Δημητρίου Ι. Νταή

ΕΙΣΑΓΩΓΙΚΗ ΑΛΓΕΒΡΑ

Σημειώσεις Παραδόσεων

ΗΡΑΚΛΕΙΟ ΚΡΗΤΗΣ, 2020-2021

Στη φιλομαθή φοιτητιώσα νεολαία

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1

Θεμελιώδεις έννοιες

Η έννοια τού *συνόλου* είναι πρωταρχική για τα Μαθηματικά. Επειδή όμως ένας αυστηρός ορισμός της δεν εντάσσεται στους στόχους των πρώτων παραδόσεων προπτυχιακού επιπέδου, θα περιορισθούμε στην «απλοϊκή» ή «αφελή» αλλά ιδιαίτερα χρήσιμη *διαισθητική* (καντοριανή[1]) σύλληψή της που μας είναι οικεία ήδη από τα σχολικά μας χρόνια. Συνήθη σύμβολα από τον προτασιακό και τον συνολοθεωρητικό λογισμό, όπως π.χ. τα σύμβολα «$\forall$», «$\exists$», «$\Longrightarrow$», «$\Longleftrightarrow$», «$=$», «$\subseteq$», «$\subsetneq$», τού «για κάθε», τού «υπάρχειν», τής απλής και αμφίπλευρης συνεπαγωγής, τού «ίσον» και τού (συνολοθεωρητικού) «εγκλεισμού» και «γνησίου εγκλεισμού», αντιστοίχως, χρησιμοποιούνται ελευθέρως (αλλά εντούτοις με αρκετή φειδώ) στις παρούσες σημειώσεις.

1.1 ΣΥΝΟΛΑ

Ως **σύνολο** εκλαμβάνουμε μια συλλογή κάποιων πλήρως καθορισμένων αντικειμένων (συνήθως μέσω μιας χαρακτηριστικής κοινής ιδιότητας). Τα αντικείμενα που απαρτίζουν ένα σύνολο A καλούνται **στοιχεία** τού A. Γράφοντας $x \in A$ (και αντιστοίχως, $y \notin A$) εννοούμε ότι το στοιχείο x ανήκει στο A (και ότι, αντιστοίχως, το στοιχείο y δεν ανήκει στο A). Επίσης, δεχόμαστε την ύπαρξη ενός συνόλου που δεν περιέχει κανένα στοιχείο, ήτοι τού **κενού συνόλου** (συμβολιζόμενου ως $\varnothing$). Ένα σύνολο δηλούται είτε μέσω αναγραφής των στοιχείων του (εντός αγκίστρων) είτε μέσω αναγραφής τής κοινής ιδιότητας των στοιχείων του (ως εξής: $\{x \mid x$ έχει την τάδε ιδιότητα$\}$).

1.1.1 Ορισμός. Ένα σύνολο A **ισούται** με ένα σύνολο B ($A = B$) όταν κάθε στοιχείο τού A είναι και στοιχείο τού B, και αντιστρόφως. Ένα σύνολο A λέγεται **υποσύνολο** ενός συνόλου B ($A \subseteq B$ ή $B \supseteq A$) όταν κάθε στοιχείο τού A είναι και στοιχείο τού B. (Σε αυτήν την περίπτωση καλούμε το B **υπερσύνολο** τού A). Εάν $A \subseteq B$, τότε το A χαρακτηρίζεται ως **γνήσιο υποσύνολο** τού B όταν υπάρχει τουλάχιστον ένα στοιχείο τού B που δεν ανήκει στο A. (Εν τοιαύτη περιπτώσει γράφουμε $A \subsetneq B$ και καλούμε το B **γνήσιο υπερσύνολο** τού A.)

1.1.2 Ορισμός. Έστω ότι τα A και B είναι δυο σύνολα. Τότε η **ένωσή** τους είναι το σύνολο

$$A \cup B := \{x \mid x \in A \text{ ή } x \in B\} \tag{1.1}$$

[1] Ο Georg Cantor (1845-1918) θεωρείται ως ο πατέρας της νεότερης Συνολοθεωρίας.

και η **τομή** τους το σύνολο

$$\boxed{A \cap B := \{x \mid x \in A \text{ και } x \in B\}.} \tag{1.2}$$

1.1.3 Πρόταση. *Ας υποθέσουμε ότι τα A, B και C είναι τυχόντα σύνολα. Τότε για την ένωση (1.1) και την τομή (1.2) ισχύουν τα εξής*:

(i) $A \cup \varnothing = A \cap A = A \cup A = A$, $A \cap \varnothing = \varnothing$,

(ii) $A \subseteq A \cup B$, $A \subseteq B \Leftrightarrow A \cup B = B$, $A \cap B \subseteq A$, $A \cap B \subseteq B$.

(iii) $A \cap B = B \cap A$, $A \cup B = B \cup A$ (Μεταθετικοί νόμοι)

(iv) $A \cap (B \cap C) = (A \cap B) \cap C$, $A \cup (B \cup C) = (A \cup B) \cup C$
(Προσεταιριστικοί νόμοι)

(v) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
(Επιμεριστικοί νόμοι)

Απόδειξη. Τα (i), (ii), (iii) και (iv) είναι προφανή βάσει των ορισμών τής ενώσεως και τής τομής συνόλων.

(v) Ένα x ανήκει στο $A \cap (B \cup C)$ εάν και μόνον εάν

$$\begin{aligned} & x \in A \text{ και } [x \in B \text{ ή } x \in C] \Longleftrightarrow [x \in A \text{ και } x \in B] \text{ ή } [x \in A \text{ και } x \in C] \\ \Longleftrightarrow \quad & x \in A \cap B \text{ ή } y \in A \cap C \Longleftrightarrow x \in (A \cap B) \cup (A \cap C)\,. \end{aligned}$$

Αναλόγως εργαζόμαστε και για τη απόδειξη τής δεύτερης ισότητας. □

1.1.4 Ορισμός. Έστω I ένα μη κενό σύνολο. Ας υποθέσουμε ότι για κάθε $i \in I$ διαθέτουμε ένα σύνολο A_i (εξαρτώμενο[2] από το i). Τότε το σύνολο

$$\boxed{\bigcup_{i \in I} A_i := \{x \mid \exists i \in I : x \in A_i\}}$$

ονομάζεται **ένωση** όλων των $A_i, i \in I$. Αντιστοίχως, το σύνολο

$$\boxed{\bigcap_{i \in I} A_i := \{x \mid x \in A_i,\ \forall i \in I\}}$$

ονομάζεται **τομή** όλων των $A_i, i \in I$. (Ένα τέτοιο I καλείται ενίοτε **σύνολο δεικτών** και τα στοιχεία του **δείκτες** τής θεωρουμένης οικογενείας συνόλων.)

1.1.5 Πρόταση. *Έστω I ένα μη κενό σύνολο. Ας υποθέσουμε ότι για κάθε $i \in I$ διαθέτουμε ένα σύνολο A_i και ότι J και K είναι δυο μη κενά υποσύνολα τού I. Τότε ισχύουν τα εξής*:

(i) *για έναν οιονδήποτε παγιωμένο δείκτη $i_0 \in I$,*

$$\bigcap_{i \in I} A_i \subseteq A_{i_0}, \quad A_{i_0} \subseteq \bigcup_{i \in I} A_i$$

(ii) $\bigcup\limits_{i \in J} A_i \subseteq \bigcup\limits_{i \in I} A_i$, $\bigcap\limits_{i \in I} A_i \subseteq \bigcap\limits_{i \in J} A_i$,

(iii) $\left(\bigcup\limits_{i \in J} A_i\right) \cup \left(\bigcup\limits_{i \in K} A_i\right) = \bigcup\limits_{i \in J \cup K} A_i$,

[2] Αργότερα, άπαξ και θα έχουμε εισαγάγει την έννοια τής απεικονίσεως (βλ. 1.2.2), η φράση «εξαρτώμενο από το i» θα σημαίνει ότι εργαζόμαστε με μια απεικόνιση $f : I \longrightarrow S$, όπου το S είναι ένα συγκεκριμένο σύνολο αποτελούμενο από σύνολα και η εικόνα καθενός $i \in I$ μέσω τής f είναι εξ ορισμού η $f(i) := A_i \in S$.

(iv) $\left(\bigcap_{i\in J} A_i\right) \cap \left(\bigcap_{i\in K} A_i\right) = \bigcap_{i\in J\cup K} A_i$.

1.1.6 Πρόταση. *Έστω I ένα μη κενό σύνολο. Ας υποθέσουμε ότι για κάθε $i \in I$ διαθέτουμε ένα σύνολο A_i και ότι το B είναι ένα τυχόν σύνολο. Τότε*

$$\left(\bigcup_{i\in I} A_i\right) \cap B = \bigcup_{i\in I} (A_i \cap B)\,, \quad \left(\bigcap_{i\in I} A_i\right) \cup B = \bigcap_{i\in I} (A_i \cup B)\,.$$

1.1.7 Σημείωση. Γενικότερα, εάν το S είναι ένα σύνολο, τα στοιχεία τού οποίου είναι *σύνολα*, τότε ως **ένωση** τού S ορίζεται το

$$\boxed{\bigcup S := \{x \mid x \in A \text{ για κάποιο } A \in S\}\,,}$$

ενώ, όταν $S \neq \varnothing$, ως **τομή** τού S ορίζεται το

$$\boxed{\bigcap S := \{x \mid x \in A \text{ για κάθε } A \in S\}\,.}$$

1.1.8 Ορισμός. Έστω ότι τα A και B είναι δυο τυχόντα σύνολα. Ορίζουμε ως **διαφορά** (τού δευτέρου από το πρώτο) το σύνολο

$$\boxed{A\smallsetminus B := \{x \mid x \in A \text{ και } x \notin B\}} \tag{1.3}$$

1.1.9 Πρόταση. *Έστω ότι τα A, B, C και D είναι τυχόντα σύνολα. Τότε*:
(i) $A\smallsetminus B \subseteq A$,
(ii) $(A\smallsetminus B) \cap B = \varnothing$,
(iii) $(A\smallsetminus B) \cup B = A \cup B$,
(iv) $A\smallsetminus (B \cap C) = (A\smallsetminus B) \cup (A\smallsetminus C)\,,$
(v) $A\smallsetminus (B \cup C) = (A\smallsetminus B) \cap (A\smallsetminus C)\,,$
(vi) $A \subseteq B$ *και* $C \subseteq D \Longrightarrow A\smallsetminus D \subseteq B\smallsetminus C$.

1.1.10 Πρόταση. *Έστω ότι τα A, B και C είναι τυχόντα σύνολα. Τότε*:
(i) $(A \cup B)\smallsetminus C = (A\smallsetminus C) \cup (B\smallsetminus C)\,,$
(ii) $(A \cap B)\smallsetminus C = (A\smallsetminus C) \cap (B\smallsetminus C)\,,$
(iii) $(A \cup B)\smallsetminus B = A\smallsetminus B = A\smallsetminus (A \cap B)\,,$
(iv) $A\smallsetminus B = A \Longleftrightarrow A \cap B = \varnothing$, $A\smallsetminus B = B\smallsetminus A \Longleftrightarrow A = B$,
(v) $(A\smallsetminus B)\smallsetminus C = A\smallsetminus (B \cup C)\,,$ $A\smallsetminus (B\smallsetminus C) = A\smallsetminus B \cup (A \cap C)\,,$
(vi) $A\smallsetminus (A\smallsetminus B) = A \cap B$,
(vii) $(A \cup B \cup C) \cap ((A \cup C)\smallsetminus B) \cap ((A \cup B)\smallsetminus C) = A\smallsetminus (B \cup C)\,.$

1.1.11 Ορισμός. Έστω ότι τα A και B είναι δυο σύνολα. Τότε το σύνολο

$$\boxed{\begin{aligned} A \times B &:= \{(x,y) \mid x \in A \text{ και } y \in B\} \\ &:= \{z \mid \exists x \in A,\ \exists y \in B \text{ με } z = (x,y)\} \end{aligned}} \tag{1.4}$$

των *διατεταγμένων ζευγών* (με το πρώτο τους στοιχείο ανήκον στο A και το δεύ-

τερο στο B) καλείται **καρτεσιανό γινόμενο** των A και B. Σημειωτέον ότι

$$(x,y)=\left(x',y'\right)\Longleftrightarrow x=x' \text{ και } y=y'.$$

(Ο ακριβής συνολοθεωρητικός ορισμός τού **διατεταγμένου ζεύγους** κατά τον Kuratowski[3] έχει ως εξής[4]: $(x,y):=\{\{x\},\{x,y\}\}$.)

1.1.12 Πρόταση. *Έστω ότι τα A,B,C και D είναι τυχόντα σύνολα. Τότε το καρτεσιανό γινόμενο* (1.4) *έχει τις ακόλουθες ιδιότητες*:
(i) $A\subseteq B$ *και* $C\subseteq D\Longrightarrow A\times C\subseteq B\times D$,
(ii) $A\times\varnothing=\varnothing\times A=\varnothing$,
(iii) $A\neq\varnothing$ *και* $B\neq\varnothing\Longrightarrow\left(A\times B=B\times A\Longleftrightarrow A=B\right)$,
(iv) $A\times(B\cap C)=(A\times B)\cap(A\times C)$, $A\times(B\cup C)=(A\times B)\cup(A\times C)$,
(v) $(A\times B)\cap(C\times D)=(A\cap C)\times(B\cap D)$,
(vi) $(A\times B)\cup(C\times D)\subseteq(A\cup C)\times(B\cup D)$, *με την ισότητα ισχύουσα εάν και μόνον εάν τα εν λόγω σύνολα πληρούν τουλάχιστον μία εκ των ακολούθων συνθηκών*:
a) $A=C$,
b) $B=D$,
c) $A\subseteq C$ *και* $B\subseteq D$,
d) $C\subseteq A$ *και* $D\subseteq B$,
(vii) $(A\times B)\smallsetminus(C\times D)=((A\smallsetminus C)\times B)\cup(C\times(B\smallsetminus D))$.

Απόδειξη. (i) Εάν $(x,y)\in A\times C$, τότε $x\in A$ και $y\in C$, οπότε $x\in B$ και $y\in D$, απ' όπου έπεται ότι $(x,y)\in B\times D$, ήτοι ότι $A\times C\subseteq B\times D$.

(ii) Εάν $A\times\varnothing\neq\varnothing$, τότε θα υπήρχε κάποιο $z=(x,y)\in A\times\varnothing$, δηλαδή $y\in\varnothing$, πράγμα προφανώς άτοπο. Κατ' αναλογίαν αποδεικνύεται ότι $\varnothing\times A=\varnothing$.

(iii) Η συνεπαγωγή "$\Longleftarrow$" είναι τετριμμένη. Εάν $A\times B=B\times A$ και εάν υποθέσουμε ότι $x\in A$, τότε, επειδή $B\neq\varnothing$, θα $\exists\, y\in B$, οπότε $(x,y)\in A\times B=B\times A$ και θα έχουμε $x\in B$. Άρα $A\subseteq B$. Κατ' αναλογίαν δείχνουμε ότι $B\subseteq A$. Τελικώς λοιπόν $A=B$.

(iv) Ο πρώτος εκ των ισχυρισμών έπεται από τις εξής αμφίπλευρες συνεπαγωγές:

$$\begin{aligned}(x,y)\in A\times(B\cap C) &\Longleftrightarrow x\in A \text{ και } y\in B\cap C\\ &\Longleftrightarrow x\in A \text{ και } [y\in B \text{ και } y\in C]\\ &\Longleftrightarrow [x\in A \text{ και } y\in B] \text{ και } [x\in A \text{ και } y\in C]\\ &\Longleftrightarrow (x,y)\in(A\times B)\cap(A\times C),\end{aligned}$$

[3] Ο Kazimierz Kuratowski (1896-1980) υπήρξε ένας εκ των κύριων εκπροσώπων τής «πολωνικής σχολής» τής Συνολοθεωρητικής Τοπολογίας, η δράση τής οποίας ήταν πολύ σημαντική κατά το πρώτο ήμισυ τού εικοστού αιώνα.

[4] Κάνοντας χρήση αυτού τού ορισμού η αμφίπλευρη συνεπαγωγή $(x,y)=(x',y')\Leftrightarrow x=x'$ και $y=y'$ αποδεικνύεται ως ακολούθως: Υποθέτουμε ότι $\{\{x\},\{x,y\}\}=\{\{x'\},\{x',y'\}\}$ και εξετάζουμε τις δύο δυνατές περιπτώσεις χωριστά.

(a) Εάν $x\neq y$, τότε το $\{\{x\},\{x,y\}\}$ έχει δύο διαφορετικά στοιχεία, ήτοι το $\{x\}$ και το $\{x,y\}$, οπότε και το $\{\{x'\},\{x',y'\}\}$ οφείλει να έχει δύο διαφορετικά στοιχεία. Αυτό σημαίνει ότι $x'\neq y'$ (διότι εάν ίσχυε $x'=y'$, τότε θα είχαμε $\{x',y'\}=\{x'\}$). Κατά συνέπειαν, είτε $\{x\}=\{x'\}$ είτε $\{x\}=\{x',y'\}$. Το δεύτερο ενδεχόμενο αποκλείεται, καθόσον η υπόθεση ότι $x'\in\{x\}$ και $y'\in\{x\}$ θα μας οδηγούσε στην αντίφαση $x'=x=y'$. Ως εκ τούτου, $\{x\}=\{x'\}\Rightarrow x=x'$. Κατ' αναλογίαν αποδεικνύεται ότι $\{x,y\}=\{x',y'\}$, κι αφού $x=x',x\neq y$ και $y\in\{x',y'\}$, συνάγεται ότι $y=y'$.

(b) Εάν $x=y$, τότε αμφότερα τα (x,y) και (x',y') περιέχουν ένα και μόνον στοιχείο, οπότε $x'=y'$. Αυτό σημαίνει ότι $x=y=x'=y'$.

Κατά τα (a) και (b) η συνεπαγωγή "$\Rightarrow$" είναι αληθής. Η αντίστροφη συνεπαγωγή "$\Leftarrow$" είναι προφανής.

ενώ ο δεύτερος έπεται από τις

$$\begin{aligned}(x,y)\in\ A\times(B\cup C) &\iff x\in A\ \text{και}\ y\in B\cup C\\ &\iff x\in A\ \text{και}\ [y\in B\ \text{ή}\ y\in C]\\ &\iff [x\in A\ \text{και}\ y\in B]\ \text{ή}\ [x\in A\ \text{και}\ y\in C]\\ &\iff (x,y)\in(A\times B)\cup(A\times C)\,.\end{aligned}$$

(v) Προφανώς έχουμε $(x,y)\in\ (A\times B)\cap(C\times D)$ εάν και μόνον εάν

$$\begin{aligned}&(x,y)\in\ A\times B\ \text{και}\ (x,y)\in C\times D\\ \iff\ &[x\in A\ \text{και}\ y\in B]\ \text{και}\ [x\in C\ \text{και}\ y\in D]\\ \iff\ &[x\in A\ \text{και}\ x\in C]\ \text{και}\ [y\in B\ \text{και}\ y\in D]\\ \iff\ &x\in A\cap C\ \text{και}\ y\in B\cap D\\ \iff\ &(x,y)\in(A\cap C)\times(B\cap D)\,.\end{aligned}$$

(vi) Έστω τυχόν $z\in(A\times B)\cup(C\times D)$. Τότε $z\in A\times B$ ή $z\in C\times D$. Στην πρώτη περίπτωση $z=(x,y)$, όπου $x\in A$ και $y\in B$, και στη δεύτερη περίπτωση $z=(x,y)$, όπου $x\in C$ και $y\in D$. Συνεπώς ($x\in A$ ή $x\in C$) και ($y\in B$ ή $y\in D$), οπότε

$$z\in(A\cup C)\times(B\cup D)\,.$$

Άρα τελικώς

$$(A\times B)\cup(C\times D)\subseteq(A\cup C)\times(B\cup D)\,.$$

Εάν ισχύει μία των συνθηκών a), b), c) ή d), τότε έχουμε ισότητα. Πράγματι· εάν ισχύει η a) ή η b), τότε το ζητούμενο έπεται από το (iv). Εάν ισχύει η c), τότε (κατά την (i))

$$(A\times B)\cup(C\times D)=C\times D=(A\cup C)\times(B\cup D)\,.$$

(Αναλόγως εργαζόμαστε και με τη συνθήκη d)). Απομένει λοιπόν να δείξουμε ότι στην περίπτωση ισότητας ισχύει μία εκ των a), b), c) ή d). Κατ' αρχάς θα αποδείξουμε τις συνεπαγωγές

(α) $A\nsubseteq C\Longrightarrow D\subseteq B$

(β) $B\nsubseteq D\Longrightarrow C\subseteq A$

Απόδειξη τής (α): Έστω ότι υπάρχει ένα $x_0\in A$ με $x_0\notin C$. Έστω τυχόν $y\in D$. Τότε

$$\begin{aligned}&(x_0,y)\in\ (A\cup C)\times(B\cup D)=(A\times B)\cup(C\times D)\\ \Longrightarrow\ &[(x_0,y)\in A\times B]\ \text{ή}\ [(x_0,y)\in C\times D]\\ \Longrightarrow\ &(x_0,y)\in A\times B\ \ (\text{επειδή}\ \ x_0\notin C)\\ \Longrightarrow\ &y\in B.\end{aligned}$$

Αναλόγως δείχνουμε και την (β). Εν συνεχεία θα προβούμε σε διάκριση περιπτώσεων και υποπεριπτώσεων. Τι μπορεί να συμβεί;

Περίπτωση I. $A\subseteq C$.
Υποπερίπτωση I.1: $B\subseteq D$. Τότε ισχύει η c).
Υποπερίπτωση I.2: $B\nsubseteq D$. Τότε $C\subseteq A$ (κατά την (β)), οπότε $A=C$ (ήτοι ισχύει η a)).

Περίπτωση II. $A\nsubseteq C$. Τότε $D\subseteq B$ (κατά την (α)).
Υποπερίπτωση II.1: $B\subseteq D$. Τότε $B=D$ (οπότε ισχύει η b)).
Υποπερίπτωση II.2: $B\nsubseteq D$. Τότε $C\subseteq A$ (κατά την (β)). Άρα ισχύει η d).

(vii) Προφανώς έχουμε $(x,y)\in\ (A\times B)\smallsetminus(C\times D)$ εάν και μόνον εάν

$$\begin{aligned}&(x,y)\in\ A\times B\ \text{και}\ (x,y)\notin C\times D\\ \iff\ &[x\in A\ \text{και}\ y\in B]\ \text{και}\ [x\notin C\ \text{ή}\ y\notin D]\\ \iff\ &[x\in A\ \text{και}\ y\in B\ \text{και}\ x\notin C]\ \text{ή}\ [x\in A\ \text{και}\ y\in B\ \text{και}\ y\notin D]\\ \iff\ &(x,y)\in(A\smallsetminus C)\times B\ \text{ή}\ [(x,y)\in C\times(B\smallsetminus D)]\\ \iff\ &(x,y)\in((A\smallsetminus C)\times B)\cup(C\times(B\smallsetminus D))\,,\end{aligned}$$

οπότε όντως $(A \times B) \smallsetminus (C \times D) = ((A \smallsetminus C) \times B) \cup (C \times (B \smallsetminus D))$. □

1.1.13 Ορισμός. Έστω A ένα σύνολο. Το

$$\mathfrak{P}(A) := \{B \mid B \subseteq A\},$$

ήτοι το σύνολο όλων των υποσυνόλων τού A, ονομάζεται **δυναμοσύνολο** τού A.

1.1.14 Παραδείγματα. (i) $\mathfrak{P}(\varnothing) = \{\varnothing\}$.
(ii) Εάν $A = \{\spadesuit\}$, τότε $\mathfrak{P}(A) = \{\varnothing, \{\spadesuit\}\}$.
(iii) Εάν $A = \{\spadesuit, \clubsuit\}$, τότε $\mathfrak{P}(A) = \{\varnothing, \{\spadesuit\}, \{\clubsuit\}, \{\spadesuit, \clubsuit\}\}$.

1.1.15 Πρόταση. *Εάν τα A, B είναι δυο τυχόντα σύνολα, τότε*
(i) $A \subseteq B \iff \mathfrak{P}(A) \subseteq \mathfrak{P}(B)$,
(ii) $\mathfrak{P}(A \cap B) = \mathfrak{P}(A) \cap \mathfrak{P}(B)$,
(iii) $\mathfrak{P}(A) \cup \mathfrak{P}(B) \subseteq \mathfrak{P}(A \cup B)$,
(iv) $\mathfrak{P}(A) \cup \mathfrak{P}(B) = \mathfrak{P}(A \cup B) \iff (A \subseteq B \text{ ή } B \subseteq A)$,
(v) $\mathfrak{P}(A \smallsetminus B) \subseteq (\mathfrak{P}(A) \smallsetminus \mathfrak{P}(B)) \cup \{\varnothing\}$.

Απόδειξη. (i) Εάν $A \subseteq B$, τότε

$$C \in \mathfrak{P}(A) \Longrightarrow C \subseteq A \Longrightarrow C \subseteq B \Longrightarrow C \in \mathfrak{P}(B).$$

Και αντιστρόφως· εάν $\mathfrak{P}(A) \subseteq \mathfrak{P}(B)$, τότε, επειδή προφανώς $A \in \mathfrak{P}(A)$, λαμβάνουμε $A \in \mathfrak{P}(B)$, οπότε $A \subseteq B$.
(ii) Ο ισχυρισμός αυτός έπεται άμεσα από τις ακόλουθες αμφίπλευρες συνεπαγωγές:

$$\begin{aligned} C \in \mathfrak{P}(A \cap B) &\iff C \subseteq A \cap B \\ &\iff C \subseteq A \cap B \text{ και } C \subseteq A \cap B \\ &\iff C \in \mathfrak{P}(A) \text{ και } C \in \mathfrak{P}(B) \\ &\iff C \in \mathfrak{P}(A) \cap \mathfrak{P}(B). \end{aligned}$$

(iii) Προφανώς έχουμε

$$\begin{aligned} C \in \mathfrak{P}(A) \cup \mathfrak{P}(B) &\iff C \in \mathfrak{P}(A) \text{ ή } C \in \mathfrak{P}(B) \\ &\iff C \subseteq A \text{ ή } C \subseteq B \\ &\Longrightarrow C \subseteq A \cup B \\ &\iff C \in \mathfrak{P}(A \cup B). \end{aligned}$$

(iv) Για οιαδήποτε σύνολα A, B έχουμε $A \cup B \in \mathfrak{P}(A \cup B)$. Υποθέτοντας ότι

$$\mathfrak{P}(A \cup B) = \mathfrak{P}(A) \cup \mathfrak{P}(B),$$

λαμβάνουμε

$$\begin{aligned} A \cup B \in \mathfrak{P}(A) \text{ ή } A \cup B \in \mathfrak{P}(B) &\Longrightarrow A \cup B \subseteq A \text{ ή } A \cup B \subseteq B \\ &\Longrightarrow A \subseteq B \text{ ή } B \subseteq A. \end{aligned}$$

Και αντιστρόφως· εάν $A \subseteq B$ ή $B \subseteq A$, τότε $A \cup B \subseteq A$ ή $A \cup B \subseteq B$, οπότε

$$[\mathfrak{P}(A \cup B) = \mathfrak{P}(A) \text{ ή } \mathfrak{P}(A \cup B) = \mathfrak{P}(B)] \Longrightarrow \mathfrak{P}(A \cup B) \subseteq \mathfrak{P}(A) \cup \mathfrak{P}(B).$$

Ο αντίστροφος εγκλεισμός έπεται από την (iii).
(v) Εάν $\varnothing \neq C \in \mathfrak{P}(A \smallsetminus B)$, τότε $C \subseteq A \smallsetminus B$, οπότε $C \in \mathfrak{P}(A)$ και $C \notin \mathfrak{P}(B)$. Κατά συνέπειαν, $\mathfrak{P}(A \smallsetminus B) \subseteq (\mathfrak{P}(A) \smallsetminus \mathfrak{P}(B)) \cup \{\varnothing\}$. □

1.1.16 Σημείωση. Υιοθετώντας τους ορισμούς ενώσεως και τομής τους εισαχθέντες στο εδάφιο 1.1.7, διαπιστώνουμε ότι για οιοδήποτε σύνολο A ισχύουν οι ισότητες

$$\bigcup \mathfrak{P}(A) = A, \quad \bigcap \mathfrak{P}(A) = \varnothing.$$

1.2 ΔΙΜΕΛΕΙΣ ΣΧΕΣΕΙΣ ΚΑΙ ΑΠΕΙΚΟΝΙΣΕΙΣ

1.2.1 Ορισμός. Έστω ότι τα A και B είναι δυο σύνολα. Μια **διμελής σχέση** μεταξύ των A και B είναι ένα υποσύνολο

$$\boxed{\mathcal{R} \subseteq A \times B}$$

τού καρτεσιανού γινομένου αυτών.

1.2.2 Ορισμός. Έστω $\mathcal{R} \subseteq A \times B$ μια διμελής σχέση μεταξύ δυο *μη κενών* συνόλων A και B. Εάν $\mathcal{R} \neq \varnothing$, η τριάδα

$$f = (\mathcal{R}, A, B)$$

ονομάζεται **απεικόνιση**[5] από το σύνολο A στο σύνολο B όταν πληροί τις ακόλουθες συνθήκες:

(i) $\forall x \in A \;\; \exists y \in B : (x, y) \in \mathcal{R}$.

(ii) $\forall\, (x, y) \in \mathcal{R}$ και $\forall\, (x', y') \in \mathcal{R} : x = x' \Longrightarrow y = y'$.

Αντί τής τριάδας $f = (\mathcal{R}, A, B)$ χρησιμοποιείται ευρέως ο συμβολισμός

$$f : A \longrightarrow B,$$

και αντί τού $(x, y) \in \mathcal{R}$ συνήθως γράφουμε[6]

$$y = f(x) \;\text{ ή }\; x \longmapsto y \;\text{ ή }\; x \longmapsto f(x).$$

Εάν η $f = (\mathcal{R}, A, B)$ είναι μια απεικόνιση από το A στο B, τότε το σύνολο

$$\Gamma_f := \{\, (x, y) \in A \times B \mid\; y = f(x) \} \;(= \mathcal{R})$$

ονομάζεται, ιδιαιτέρως, **γράφημα** τής f. Το A καλείται **πεδίο ορισμού** και το B **πεδίο τιμών**[7] τής f. Για δοθέν $x \in A$, το μονοσημάντως ορισμένο στοιχείο $y \in B$, για το οποίο $y = f(x)$, καλείται **η τιμή** που λαμβάνει η f στο x ή **η εικόνα τού** x **μέσω τής** f. Είθισται να λέμε ότι η f *στέλνει το* x *να απεικονισθεί* στο y. Επίσης, ορίζουμε ως

$$\boxed{B^A := \text{ΑΠ}(A, B) := \{\, f : A \longrightarrow B \mid\; f \text{ απεικόνιση} \}} \tag{1.5}$$

το σύνολο όλων των απεικονίσεων από το A στο B. (Δυο απεικονίσεις f, g από το $\text{ΑΠ}(A, B)$ λογίζονται ως **ίσες**, $f = g$, όταν ισχύει $f(x) = g(x)$ για κάθε $x \in A$.)

[5] Πολλές φορές αντί τού όρου **απεικόνιση** (αγγλ. map, γερμ. Abbildung) χρησιμοποιείται ο όρος **συνάρτηση** (αγγλ. function, γερμ. Funktion) ή και άλλοι όροι (**μετασχηματισμός**, **τελεστής** κ.λπ). Ωστόσο, υπάρχουν πολλοί συγγραφείς οι οποίοι διαφοροποιούν αυτές τις έννοιες και γι' αυτόν τον λόγο κανείς οφείλει να είναι ιδιαίτερα προσεκτικός.

[6] Ενίοτε, διμελείς σχέσεις που πληρούν τη συνθήκη (i) ορίζονται από «τύπους» τής μορφής $y = f(x)$ ή $x \longmapsto y$. Ωστόσο, για να είναι **καλώς ορισμένες** ως απεικονίσεις οφείλουν να πληρούν *οπωσδήποτε* **και** τη συνθήκη (ii) τού *μονοσημάντου των εικόνων*.

[7] Θα πρέπει να επιστήσουμε την προσοχή τού αναγνώστη στο ότι είναι δυνατόν η ίδια η εικόνα (ή το σύνολο των τιμών) μιας απεικονίσεως $f : A \longrightarrow B$ να είναι *γνήσιο υποσύνολο* τού B.

1.2.3 Ορισμός. Έστω $f : A \longrightarrow B$ μια απεικόνιση από το A στο B. Εάν $C \subseteq A$ και $D \subseteq B$, τότε το σύνολο

$$\boxed{f(C) := \{f(x) \mid x \in C\} \subseteq B}$$

καλείται **η εικόνα τού** C **μέσω τής** f, ενώ το σύνολο

$$\boxed{f^{-1}(D) := \{x \in A \mid f(x) \in D\}}$$

καλείται **η αντίστροφη εικόνα** ή **το αρχέτυπο τού** D **μέσω τής** f. Ιδιαιτέρως, συμβολίζουμε ως[8]

$$\boxed{\mathrm{Im}\,(f) := f(A) := \{f(x) \mid x \in A\} \subseteq B}$$

την **εικόνα** (ή το **σύνολο τιμών**) **τής** f, ενώ όταν $y \in B$ καλούμε την αντίστροφη εικόνα

$$\boxed{f^{-1}(y) := f^{-1}(\{y\}) = \{x \in A \mid f(x) = y\}}$$

ίνα τής f υπεράνω τού στοιχείου y.

1.2.4 Πρόταση. *Έστω οτι η $f : A \longrightarrow B$ είναι μια απεικόνιση, τα C, D υποσύνολα τού A, η $(C_i)_{i\in I}$ μια οικογένεια υποσυνόλων τού A, τα E, F υποσύνολα τού B, και η $(E_j)_{j\in J}$ μια οικογένεια υποσυνόλων τού B. Τότε ισχύουν τα εξής:*

(i) $f(\varnothing) = \varnothing = f^{-1}(\varnothing)$.

(ii) $C \subseteq D \Longrightarrow f(C) \subseteq f(D)$. *Και αντιστοίχως,* $E \subseteq F \Longrightarrow f^{-1}(E) \subseteq f^{-1}(F)$.

(iii) $C \subseteq f^{-1}(f(C))$ *και* $f\left(f^{-1}(E)\right) \subseteq E$.

(iv) $f(C \cup D) = f(C) \cup f(D)$ *και* $f^{-1}(E \cup F) = f^{-1}(E) \cup f^{-1}(F)$.

(v) $f(C \cap D) \subseteq f(C) \cap f(D)$, *ενώ* $f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F)$.

(vi) $f(C) \setminus f(D) \subseteq f(C \setminus D)$.

(vii) $F \subseteq E \Longrightarrow f^{-1}(E \setminus F) = f^{-1}(E) \setminus f^{-1}(F)$.

Γενικότερα,

(viii) $f(\bigcup\limits_{i\in I} C_i) = \bigcup\limits_{i\in I} f(C_i)$ *και* $f^{-1}(\bigcup\limits_{j\in J} E_j) = \bigcup\limits_{j\in J} f^{-1}(E_j)$.

(ix) $f(\bigcap\limits_{i\in I} C_i) \subseteq \bigcap\limits_{i\in I} f(C_i)$, *ενώ* $f^{-1}(\bigcap\limits_{j\in J} E_j) = \bigcap\limits_{j\in J} f^{-1}(E_j)$.

Απόδειξη. (i) Αυτό έπεται άμεσα από τους ορισμούς 1.2.2 και 1.2.3.

(ii) Επειδή $y \in f(C) \iff (\exists x \in C) : y = f(x)$ και $C \subseteq D$, το y ανήκει και στο D, οπότε $y \in f(D)$. Επομένως, $f(C) \subseteq f(D)$. Και αντιστοίχως, εάν υποθέσουμε ότι $E \subseteq F$ και ότι το x ανήκει στο αρχέτυπο τού E, τότε

$$f(x) \in E \subseteq F \Longrightarrow f(x) \subseteq F \Longrightarrow x \in f^{-1}(F),$$

οπότε $f^{-1}(E) \subseteq f^{-1}(F)$.

(iii) Εάν $x \in C$, τότε $f(x) \in f(C)$. Άρα, βάσει τού ορισμού 1.2.3), $x \in f^{-1}(f(C))$.

Εν συνεχεία υποθέτουμε ότι το E είναι υποσύνολο τού συνόλου B. Έστω τυχόν στοιχείο $y \in f\left(f^{-1}(E)\right)$. Τότε υπάρχει κάποιο x, τέτοιο ώστε $x \in f^{-1}(E)$ με

[8] Στο σύμβολο $\mathrm{Im}(f)$ το πρόθεμα "Im" προέρχεται από τα δύο αρχικά γράμματα τής λέξεως *image*.

$y = f(x)$. Επειδή όμως $x \in f^{-1}(E)$, έχουμε $f(x) \in E$. Άρα και το y οφείλει να ανήκει στο E.

(iv) Έπειδή $C \subseteq C \cup D$ και $D \subseteq C \cup D$ (βλ. 1.1.3 (i)), βάσει τής (ii) έχουμε $f(C) \subseteq f(C \cup D)$ και $f(D) \subseteq f(C \cup D)$, απ' όπου έπεται ότι ισχύει ο εγκλεισμός:

$$f(C) \cup f(D) \subseteq f(C \cup D).$$

Και αντιστρόφως· έστω τυχόν $y \in f(C \cup D)$. Τότε υπάρχει κάποιο x, τέτοιο ώστε $f(x) = y$. Αλλά αφού το x ανήκει στην ένωση $C \cup D$, έχουμε $x \in C$ ή $x \in D$. Εάν $x \in C$, τότε το $y = f(x)$ ανήκει στην εικόνα $f(C)$ τού C. Τούτο σημαίνει ότι $y \in f(C) \cup f(D)$. Παρομοίως, εάν $x \in D$, τότε το $y = f(x)$ ανήκει στην εικόνα $f(D)$ τού D, οπότε και πάλι το y οφείλει να ανήκει στην ένωση των εικόνων $f(C) \cup f(D)$. Κατά συνέπειαν, ισχύει και ο αντίστροφος εγκλεισμός

$$f(C \cup D) \subseteq f(C) \cup f(D).$$

Εν συνεχεία, υποθέτοντας ότι τα E, F είναι υποσύνολα τού B, έχουμε $E \subseteq E \cup F$ και $F \subseteq E \cup F$ (βλ. πρόταση 1.1.3 (i)). Βάσει τής (ii), $f^{-1}(E) \subseteq f^{-1}(E \cup F)$ και $f^{-1}(F) \subseteq f^{-1}(E \cup F)$, απ' όπου έπεται ότι $f^{-1}(E) \cup f^{-1}(F) \subseteq f^{-1}(E \cup F)$. Και αντιστρόφως· έστω τυχόν $x \in f^{-1}(E \cup F)$. Τότε $f(x) \in E \cup F$. Άρα $f(x) \in E$ ή $f(x) \in F$. Αυτό όμως σημαίνει ότι είτε $x \in f^{-1}(E)$ είτε $x \in f^{-1}(F)$, δηλαδή ότι $x \in f^{-1}(E) \cup f^{-1}(F)$. Επομένως ισχύει και ο αντίστροφος εγκλεισμός:

$$f^{-1}(E \cup F) \subseteq f^{-1}(E) \cup f^{-1}(F).$$

(v) Επειδή $C \cap D \subseteq C$ και $C \cap D \subseteq D$ (βλ. 1.1.3 (i)), βάσει τής (ii), $f(C \cap D) \subseteq f(C)$ και $f(C \cap D) \subseteq f(D)$, απ' όπου έπεται ότι $f(C \cap D) \subseteq f(C) \cap f(D)$. Εν συνεχεία, υποθέτοντας ότι τα E, F είναι υποσύνολα τού B, έχουμε $E \subseteq E \cup F$ και $F \subseteq E \cup F$, οπότε, βασιζόμενοι στην ίδια συλλογιστική, λαμβάνουμε

$$f^{-1}(E \cap F) \subseteq f^{-1}(E) \cap f^{-1}(F).$$

Και αντιστρόφως· έστω τυχόν στοιχείο $x \in f^{-1}(E) \cap f^{-1}(F)$. Τότε $f(x) \in E \cap F$. Άρα $f(x) \in E$ και $f(x) \in F$. Αυτό όμως σημαίνει ότι $x \in f^{-1}(E)$ και $x \in f^{-1}(F)$, δηλαδή ότι $x \in f^{-1}(E) \cap f^{-1}(F)$. Κατά συνέπειαν, ισχύει και ο αντίστροφος εγκλεισμός $f^{-1}(E) \cap f^{-1}(F) \subseteq f^{-1}(E \cap F)$.

(vi) Έστω ότι $D \subseteq C$ και ότι $y \in f(C) \setminus f(D)$. Τότε $y \in f(C)$ και $y \notin f(D)$. Άρα υπάρχει κάποιο $x \in C$, τέτοιο ώστε $y = f(x)$, και, δεδομένου ότι $y \notin f(D)$, έχουμε $x \notin D$. Συνεπώς, $x \in C \setminus D$, οπότε $y \in f(C \setminus D)$.

(vii) Έστω ότι $F \subseteq E$ και ότι το x είναι ένα τυχόντως επιλεγμένο στοιχείο τού $f^{-1}(E \setminus F)$. Τότε

$$f(x) \in E \setminus F \Longrightarrow (f(x) \in E \quad f(x) \notin F) \Longrightarrow x \in f^{-1}(E) \setminus f^{-1}(F).$$

Άρα $f^{-1}(E \setminus F) \subseteq f^{-1}(E) \setminus f^{-1}(F)$. Και αντιστρόφως· εάν $x \in f^{-1}(E) \setminus f^{-1}(F)$, τότε $f(x) \in E$ και $f(x) \notin F$, οπότε $f(x) \in E \setminus F$, πράγμα το οποίο σημαίνει ότι ισχύει $x \in f^{-1}(E \setminus F)$. Άρα $f^{-1}(E) \setminus f^{-1}(F) \subseteq f^{-1}(E \setminus F)$.

(viii) Ο πρώτος ισχυρισμός είναι αληθής επί τη βάσει των ακολούθων αμφιπλεύρων συνεπαγωγών:

$$\begin{aligned} y \in f(\bigcup_{i \in I} C_i) &\iff \left(\exists x \in \bigcup_{i \in I} C_i : y = f(x)\right) \\ &\iff ((\exists i \in I)(\exists x \in C_i) : y = f(x)) \\ &\iff ((\exists i \in I) : y \in f(C_i)) \\ &\iff y \in \bigcup_{i \in I} f(C_i). \end{aligned}$$

Κατ' αναλογίαν έχουμε

$$\begin{aligned} x \in f^{-1}(\bigcup_{j\in J} E_j) &\iff f(x) \in \bigcup_{j\in J} E_j \\ &\iff ((\exists j \in J) : f(x) \in E_j) \\ &\iff \big((\exists j \in J) : x \in f^{-1}(E_j)\big) \\ &\iff x \in \bigcup_{j\in J} f^{-1}(E_j). \end{aligned}$$

(ix) Εάν $y \in f(\bigcap_{i\in I} C_i)$, τότε

$$\begin{aligned} (\exists x \in \bigcap_{i\in I} C_i : y = f(x)) &\implies ((\forall i \in I)\,(\exists x \in C_i) : y = f(x)) \\ &\iff (y \in f(C_i), \forall i \in I) \\ &\iff y \in \bigcap_{i\in I} f(C_i). \end{aligned}$$

Επομένως, $f(\bigcap_{i\in I} C_i) \subseteq \bigcap_{i\in I} f(C_i)$. Ο δεύτερος ισχυρισμός αποδεικνύεται ως εξής:

$$\begin{aligned} x \in f^{-1}(\bigcap_{j\in J} E_j) &\iff f(x) \in \bigcap_{j\in J} E_j \\ &\iff (f(x) \in E_j, \forall j \in J) \\ &\iff \big(x \in f^{-1}(E_j), \forall j \in J\big) \\ &\iff x \in \bigcap_{j\in J} f^{-1}(E_j). \end{aligned}$$

Συνεπώς, $f^{-1}(\bigcap_{j\in J} E_j) = \bigcap_{j\in J} f^{-1}(E_j)$. □

1.2.5 Ορισμός («Περιορισμοί»). Έστω $f : A \longrightarrow B$ τυχούσα απεικόνιση. Εάν $\varnothing \neq U \subseteq A$, τότε η απεικόνιση $f|_U : U \longrightarrow B$, όπου $f|_U(x) := f(x), \forall x \in U$, λέγεται **περιορισμός** (τού πεδίου ορισμού) **τής** f **στο** U.

1.2.6 Ορισμός (Γενίκευση τής εννοίας τού «περιορισμού»). Έστω $f : A \longrightarrow B$ μια απεικόνιση. Εάν $\mathrm{Im}(f) := f(A) \subseteq V \subseteq B$, τότε η απεικόνιση

$$f|_{(A,V)} : A \longrightarrow V,\ x \longmapsto f|_{(A,V)}(x) := f(x),$$

καλείται **περιορισμός τού πεδίου τιμών τής** f **στο** V. Γενικότερα, εάν $\varnothing \neq U \subseteq A$ και $\mathrm{Im}(f|_U) \subseteq V \subseteq B$, λέμε ότι η απεικόνιση

$$f|_{(U,V)} : U \longrightarrow V,\ x \longmapsto f|_{(U,V)}(x) := f(x),$$

είναι **αμφίπλευρος περιορισμός, αφ' ενός μεν τού πεδίου ορισμού τής** f **στο σύνολο** U, **αφ' ετέρου δε τού πεδίου τιμών τής** f **στο σύνολο** V. (Προφανώς, $f|_{(A,B)} = f$ και $f|_{(U,B)} = f|_U$.)

1.2.7 Ορισμός («Επεκτάσεις»). Έστω $g : U \longrightarrow B$ μια απεικόνιση, όπου το U είναι υποσύνολο ενός συνόλου A. Κάθε απεικόνιση $f : A \longrightarrow B$, για την οποία ισχύει $g = f|_U$, ονομάζεται **επέκταση** τής g στο σύνολο A. (Οι επεκτάσεις τής g στο σύνολο A δεν είναι κατ' ανάγκην μονοσημάντως ορισμένες.)

1.2.8 Ορισμός. Μια απεικόνιση $f : A \longrightarrow B$ λέγεται

(i) **ενριπτική** (ή **ερριπτική** ή **ένα προς ένα**-απεικόνιση (1-1)), ή απλώς **ένριψη**, όταν

$$\boxed{(\forall\ x, y \in A, \quad f(x) = f(y) \Longrightarrow x = y)}$$

(ii) **επιρριπτική** (ή **επί**-απεικόνιση), ή απλώς **επίριψη**, όταν $\mathrm{Im}\,(f) = B$, δηλαδή όταν

$$\boxed{(\forall\ y \in B, \quad \exists\ x \in A : \quad y = f(x))}$$

και

(iii) **αμφιρριπτική** (ή **ένα πρός ένα και επί**-απεικόνιση), ή απλώς **αμφίριψη**, όταν είναι ταυτοχρόνως και ενριπτική και επιρριπτική[9].

1.2.9 Παραδείγματα. (i) Έστω A ένα μη κενό σύνολο. Η **ταυτοτική απεικόνιση**[10] $\mathrm{id}_A : A \longrightarrow A$, όπου $\mathrm{id}_A(x) = x$, $\forall x \in A$, είναι προφανώς αμφιρριπτική, ενώ για οιοδήποτε υποσύνολο $C \subseteq A$ η **ενθετική απεικόνιση** (ή **ένθεση**) $\mathrm{id}_A\,|_C : C \longrightarrow A$ τού C εντός τού A είναι ενριπτική.

(ii) Εάν $A = \{\spadesuit, \clubsuit\}$ και $B = \{\heartsuit, \diamondsuit\}$, τότε η απεικόνιση

$$f : A \longrightarrow B, \quad f(\spadesuit) := \diamondsuit, \quad f(\clubsuit) := \heartsuit,$$

είναι αμφιρριπτική, ενώ η απεικόνιση

$$g : A \longrightarrow B, \quad g(\spadesuit) := \heartsuit, \quad g(\clubsuit) := \heartsuit,$$

δεν είναι *ούτε* ενριπτική (αφού $\spadesuit \neq \clubsuit$) *ούτε* επιρριπτική ($\mathrm{Im}(g) = \{\heartsuit\} \subsetneqq B$).

(iii) Εάν $f : A \longrightarrow B$ είναι τυχούσα απεικόνιση, τότε η $f|_{(A,\mathrm{Im}(f))}$ αποτελεί (εκ κατασκευής) μια *επίριψη*.

Στις προτάσεις 1.2.10, 1.2.11 και 1.2.18 δίδουμε τρεις διαφορετικής φύσεως, αλλ' εντούτοις *ισοδυνάμους* χαρακτηρισμούς τής ενριπτικότητας/επιρριπτικότητας και αμφιρριπτικότητας μιας απεικονίσεως.

1.2.10 Πρόταση. *Έστω $f : A \longrightarrow B$ μια τυχούσα απεικόνιση. Τότε ισχύουν τα εξής:*

(i) *Η f είναι ενριπτική* $\Longleftrightarrow \left(\begin{array}{l} \text{Η ίνα } f^{-1}(y) \text{ τής } f \text{ υπεράνω τού } y \text{ περιέχει} \\ \text{το πολύ ένα στοιχείο, για όλα τα } y \in B \end{array}\right)$.

(ii) *Η f είναι επιρριπτική* $\Longleftrightarrow \left(\begin{array}{l} \text{Η ίνα } f^{-1}(y) \text{ τής } f \text{ υπεράνω τού } y \text{ περιέχει} \\ \text{τουλάχιστον ένα στοιχείο, για όλα τα } y \in B \end{array}\right)$.

(iii) *Η f είναι αμφιρριπτική* $\Longleftrightarrow \left(\begin{array}{l} \text{Η ίνα } f^{-1}(y) \text{ τής } f \text{ υπεράνω τού } y \text{ περιέχει} \\ \text{ακριβώς ένα στοιχείο, για όλα τα } y \in B \end{array}\right)$.

Απόδειξη. (i) Έστω ότι η f είναι ενριπτική. Για να αποδείξουμε ότι η ίνα $f^{-1}(y)$ τής f υπεράνω ενός οιουδήποτε $y \in B$ περιέχει το πολύ ένα στοιχείο, αρκεί

[9] Για μια ομογενή απόδοση τής τριάδας των όρων «injection/surjection/bijection» στα ελληνικά, αντί των «ένριψη/επίριψη/αμφίριψη», χρησιμοποιείται ενίοτε και η (σε μεγάλο βαθμό σημασιολογικά συγγενεύουσα) τριάδα «ένεση/έφεση/αμφίεση». (Το αρχαίο ρήμα *ενίημι* σήμαινε -μεταξύ άλλων- και «ενρίπτω, εγχέω, εμβάλλω», εξ ου και το λατινικό *injicio.*). Θα πρέπει επίσης να σημειωθεί ότι ορισμένοι συγγραφείς κάνουν χρήση τού «(1-1) αντιστοιχία» ή «(1-1) αντιστοίχιση» ως συνωνύμου τής «αμφιρρίψεως» (όταν, βεβαίως, τούτη η λέξη *ορισθεί* να αποδίδει ιδιαιτέρως *και* την αγγλική λέξη «(one-to-one) correspondence»). Τέλος, θα πρέπει να τονισθεί ότι στην ελληνική βιβλιογραφία δεν έχει εισέτι κατορθωθεί να οριστικοποιηθεί μια *κοινή* εννοιολόγηση τής φράσεως «αμφιμονοσήμαντη» ή «αμφιμονότιμη» απεικόνιση. Κάποιοι συγγραφείς εννοούν μέσω αυτής μόνον την ένριψη (και ίσως τούτο να είναι το σωστότερο), ενώ άλλοι πάλι εννοούν την αμφίριψη. (Φυσικά, η ιδιότητα τού «μονότιμου» ή «μονοσήμαντου» είναι ακριβώς αυτή που χαρακτηρίζει μια απεικόνιση). Κατά την προσωπική άποψη τού γράφοντος, η θέσπιση τής τριάδας «ένριψη/επίριψη/αμφίριψη» θα αποτελούσε την καταλληλότερη λύση στο προκύπτον πρόβλημα, καθότι τούτη είναι σημασιολογικώς απολύτως ορθή, αισθητώς ευφωνική, και ταυτοχρόνως δεν δημιουργεί και συνειρμικούς ενδοιασμούς σχετικούς με τη χρήση αμφισήμων λέξεων.

[10] Στο σύμβολο id_A το "id" προέρχεται από τα δύο αρχικά γράμματα τής λέξεως *identity*.

να αποδείξουμε πως δυο *τυχόντα* στοιχεία τής ίνας $f^{-1}(y)$ είναι ίσα (όταν, βεβαίως, $f^{-1}(y) \neq \varnothing$). Αλλά τούτο είναι προφανές, διότι για οιαδήποτε στοιχεία x, x' τής ίνας $f^{-1}(y)$ έχουμε

$$f(x) = y = f(x') \underset{f \text{ 1-1}}{\Longrightarrow} x = x'.$$

Και αντιστρόφως· εάν τα x_1, x_2 είναι στοιχεία τού A με $f(x_1) = f(x_2)$ και εάν θέσουμε $y = f(x_1)$, τότε λαμβάνουμε $x_1 \in f^{-1}(y)$. Άρα και $x_2 \in f^{-1}(y)$, οπότε $x_1 = x_2$ εξ υποθέσεως.

(ii) Ο ισχυρισμός αυτός είναι αληθής δυνάμει των ακολούθων αμφιπλεύρων συνεπαγωγών:

$$\left(\begin{array}{l}\text{Η ίνα } f^{-1}(y) \text{ τής } f \text{ υπεράνω}\\ \text{τού } y \text{ περιέχει τουλάχιστον}\\ \text{ένα στοιχείο, } \forall y \in B\end{array}\right) \iff \left[f^{-1}(y) \neq \varnothing, \forall y \in B\right]$$

$$\iff [(\forall y \in B)\,(\exists x \in A) : f(x) = y]$$

$$\iff \text{η } f \text{ είναι επιρριπτική.}$$

(iii) Αυτό έπεται άμεσα από τα (i) και (ii). □

1.2.11 Πρόταση. *Έστω $f : A \longrightarrow B$ μια τυχούσα απεικόνιση. Τότε ισχύουν τα εξής:*

(i) *Η f είναι ενριπτική* $\iff (f(C \cap D) = f(C) \cap f(D)$ *για όλα τα* $C, D \subseteq A)$.

(ii) *Η f είναι ενριπτική* $\iff (f(C \smallsetminus D) = f(C) \smallsetminus f(D)$ *για όλα τα* $C, D \subseteq A)$.

(iii) *Η f είναι ενριπτική* $\iff (C = f^{-1}(f(C))$ *για όλα τα* $C \subseteq A)$.

(iv) *Η f είναι επιρριπτική* $\iff (f\left(f^{-1}(E)\right) = E$ *για όλα τα* $E \subseteq B)$.

(v) *Η f είναι αμφιρριπτική* $\iff (f(A \smallsetminus M) = B \smallsetminus f(M)$ *για όλα τα* $M \subseteq A)$.

Απόδειξη. (i) Για οιαδήποτε απεικόνιση $f : A \longrightarrow B$ ισχύει ο εγκλεισμός

$$f(C \cap D) \subseteq f(C) \cap f(D)$$

για όλα τα $C, D \subseteq A$ (βλ. 1.2.4 (v)). Εάν λοιπόν η f είναι ενριπτική, τότε αρκεί (εν πρώτοις, προκειμένου να ελεγχθεί η αλήθεια τής συνεπαγωγής " $\Longrightarrow$ ") να αποδείξουμε και τον αντίστροφο εγκλεισμό. Έστω τυχόν $y \in f(C) \cap f(D)$. Τότε

$$\left[(\exists x \in C)\ \left(\exists x' \in D\right) : f(x) = y = f(x')\right] \implies x = x' \in C \cap D \text{ και } y = f(x)$$
$$\implies y \in f(C \cap D).$$

Για να δείξουμε την αλήθεια και τής αντιθέτως κατευθυνομένης συνεπαγωγής ("$\Longleftarrow$") θεωρούμε δύο στοιχεία x_1 και x_2 τού A, τέτοια ώστε $f(x_1) = f(x_2)$. Εάν (υποτιθεμένης τής ισχύος τής ισότητας $f(C \cap D) = f(C) \cap f(D)$) έχουμε $x_1 \neq x_2$ (δηλαδή η f *δεν* είναι ενριπτική), θα καταλήξουμε σε *άτοπο*. Πράγματι· εάν κάτι τέτοιο συνέβαινε, τότε θα λαμβάναμε

$$\{f(x_1)\} = f(\{x_1\}) \cap f(\{x_2\}) = f(\{x_1\} \cap \{x_2\}) = f(\varnothing) = \varnothing,$$

ήτοι κάτι αδύνατο.

(ii) Ας υποθέσουμε εν πρώτοις ότι η f είναι ενριπτική. Εν γένει (ήτοι για οιαδήποτε απεικόνιση f) ισχύει ο εγκλεισμός $f(C) \smallsetminus f(D) \subseteq f(C \smallsetminus D)$ (Βλ. 1.2.4 (vi)). Αρκεί λοιπόν να αποδειχθεί και ο αντίστροφος εγκλεισμός. Έστω ότι τα C και D είναι υποσύνολα τού A και ότι $y \in f(C \smallsetminus D)$. Τότε

$$[(\exists x \in C,\ x \notin D) : f(x) = y] \Longrightarrow y \in f(C).$$

Υποθέτοντας ότι το y ανήκει στην εικόνα $f(D)$ τού D μέσω τής f, θα υπάρχει κάποιο $x' \in D$, τέτοιο ώστε να ισχύει $f(x') = y(= f(x))$. Επειδή όμως η f είναι αμφίρριψη, τούτο σημαίνει ότι $x = x' \in D$. Άτοπο! Άρα $y \notin f(D)$ και επομένως $f(C \smallsetminus D) \subseteq f(C) \smallsetminus f(D)$.

Τώρα αντιστρόφως· υποθέτοντας ότι για οιαδήποτε υποσύνολα C και D τού A ισχύει η ισότητα $f(C \smallsetminus D) = f(C) \smallsetminus f(D)$, θα αποδείξουμε ότι η f είναι μια ένριψη. Θεωρούμε δύο στοιχεία x_1, x_2 τού A με $x_1 \neq x_2$. Θέτοντας ως $C = \{x_1, x_2\}$ και ως $D = \{x_2\}$ λαμβάνουμε

$$f(x_1) \in f(\{x_1\}) = f(\{x_1, x_2\} \smallsetminus \{x_2\}) = f(\{x_1, x_2\}) \smallsetminus f(\{x_2\}) \Longrightarrow f(x_1) \neq f(x_2).$$

Άρα η f είναι όντως μια ένριψη.

(iii) Ο εγκλεισμός $C \subseteq f^{-1}(f(C))$ ισχύει πάντοτε, $\forall C \subseteq A$ (βλ. 1.2.4 (iii)). Αρκεί λοιπόν να αποδειχθεί η ακόλουθη αμφίπλευρη συνεπαγωγή:

$$\text{Η } f \text{ είναι ενριπτική} \iff \left(f^{-1}(f(C)) \subseteq C,\ \forall C \subseteq A\right).$$

Εάν η f είναι ενριπτική και $x \in f^{-1}(f(C))$ για κάποιο $C \subseteq A$, τότε υπάρχει ένα στοιχείο $y \in f(C)$, τέτοιο ώστε $y = f(x)$. Επιπροσθέτως, επειδή $y \in f(C)$, υπάρχει και κάποιο στοιχείο $x' \in C$, τέτοιο ώστε $y = f(x')$. Εξ αυτού έπεται ότι $f(x) = f(x')$, ήτοι ότι $x = x'$ (λόγω τής προϋποτεθείσας ενριπτικότητας τής απεικονίσεως f). Άρα $x = x' \in C$ και $f^{-1}(f(C)) \subseteq C$.

Τώρα αντιστρόφως· υποθέτοντας ότι για οιοδήποτε υποσύνολο C τού A ισχύει $f^{-1}(f(C)) \subseteq C$ και ότι η f *δεν* είναι ενριπτική, θα καταλήξουμε σε *άτοπο*. Πράγματι· εάν κάτι τέτοιο συνέβαινε, τότε θα υπήρχαν δύο στοιχεία x_1 και x_2 τού A με $x_1 \neq x_2$ και $f(x_1) = f(x_2) =: y$. Θέτοντας λοιπόν $C = \{x_1\}$ θα λαμβάναμε

$$\{x_1, x_2\} \subseteq f^{-1}(y) = f^{-1}(f(x_i)) \subseteq \{x_i\},\ \forall i \in \{1, 2\},$$

ήτοι έναν μη ισχύοντα εγκλεισμό (καθότι $x_1 \neq x_2$). Επομένως η f *οφείλει* να είναι ενριπτική.

(iv) Εν γένει ισχύει ο εγκλεισμός $f\left(f^{-1}(E)\right) \subseteq E, \forall E \subseteq B$ (βλ. 1.2.4 (iii)). Αρκεί λοιπόν να αποδειχθεί η ακόλουθη αμφίπλευρη συνεπαγωγή:

$$\text{Η } f \text{ είναι επιρριπτική} \iff \left(E \subseteq f\left(f^{-1}(E)\right),\ \forall E \subseteq B\right).$$

Έστω ότι η f είναι μια επίρριψη, το E ένα οιοδήποτε υποσύνολο τού B και $y \in E$. Τότε

$$(\exists x \in A : y = f(x)) \underset{(y \in E)}{\Longrightarrow} \left(\exists x \in f^{-1}(E) : y = f(x)\right) \Longrightarrow y \in f\left(f^{-1}(E)\right).$$

Άρα $E \subseteq f\left(f^{-1}(E)\right)$. Τώρα αντιστρόφως· υποθέτοντας ότι για οιοδήποτε υποσύνολο E τού B ισχύει $E \subseteq f\left(f^{-1}(E)\right)$ και ότι η f *δεν* είναι μια επίρριψη, θα καταλήξουμε σε *άτοπο*. Πράγματι· εάν κάτι τέτοιο ίσχυε, τότε θα υπήρχε κάποιο στοιχείο $y \in B$, τέτοιο ώστε $y \neq f(x)$ *για κάθε* $x \in A$. Άρα

$$f^{-1}(y) = \varnothing \Longrightarrow f\left(f^{-1}(y)\right) = f(\varnothing) = \varnothing,$$

γεγονός το οποίο θα αντέκειτο προς την υπόθεσή μας, σύμφωνα με την οποία έχουμε $\{y\} \subseteq f\left(f^{-1}(y)\right)$. Επομένως η f *οφείλει* να είναι επιρριπτική.

(v) Έστω ότι η f είναι μια αμφίρριψη. Τότε $f(A) = B$ και εφαρμόζοντας το (ii) (για $C = A$, και τυχόν υποσύνολο $D = M$ τού A) λαμβάνουμε

$$f(A \smallsetminus M) = B \smallsetminus f(M).$$

Και αντιστρόφως· εάν $f(A \smallsetminus M) = B \smallsetminus f(M)$ για κάθε υποσύνολο M τού A, τότε, θέτοντας $M = \varnothing$, λαμβάνουμε $f(A) = B$, οπότε η f είναι επιρριπτική. Αρκεί λοιπόν να αποδείξουμε ότι η f είναι και ενριπτική. Εάν αυτό δεν συνέβαινε, τότε θα υπήρχαν δύο στοιχεία x_1, x_2 τού A με $x_1 \neq x_2$ και $f(x_1) = f(x_2) = y$. Από την υπόθεσή μας (για $M = \{x_1\}$) αυτό θα είχε ως συνέπεια τις ισότητες

$$f(A \smallsetminus \{x_1\}) = B \smallsetminus f(\{x_1\}) = B \smallsetminus \{y\},$$

πράγμα άτοπο, καθότι $y = f(x_2) \underset{x_1 \neq x_2}{\Longrightarrow} y \in f(A \smallsetminus \{x_1\})$. Άρα η f είναι όντως ενριπτική. □

1.2.12 Ορισμός. Ας υποθέσουμε πως οι $f : A \longrightarrow B$ και $g : B \longrightarrow C$ είναι δυο απεικονίσεις. Η **σύνθεση** $g \circ f$ των απεικονίσεων g και f είναι η απεικόνιση

$$\boxed{g \circ f : A \longrightarrow C} \tag{1.6}$$

η οποία ορίζεται μέσω τού τύπου $(g \circ f)(x) := g(f(x))$, $\forall x \in A$, έχοντας ως πεδίο ορισμού της το σύνολο A, ως πεδίο τιμών της το C, και ως εικόνα της την $\mathrm{Im}(g \circ f) = \mathrm{Im}\big(g\,|_{\mathrm{Im}(f)}\big)$. Ας σημειωθεί, ότι εάν $E \subseteq A$ και $F \subseteq B$, τότε

$$(g \circ f)(E) = g(f(E))$$

και $(g \circ f)^{-1}(F) = f^{-1}\left(g^{-1}(F)\right)$.

Η σύνθεση απεικονίσεων έχει την *προσεταιριστική ιδιότητα*, δηλ. εάν η $h : C \longrightarrow D$ είναι μια επιπρόσθετη απεικόνιση, τότε έχουμε:

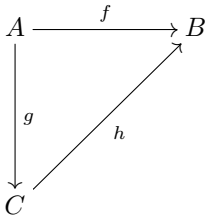
1.2.13 Πρόταση. $h \circ (g \circ f) = (h \circ g) \circ f$.

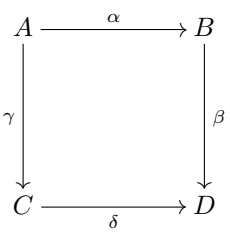
Απόδειξη. Προφανώς, τα πεδία ορισμού και τιμών των δύο αυτών απεικονίσεων συμπίπτουν. Επιπροσθέτως, για κάθε $x \in A$ έχουμε

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = (h \circ g) \circ f(x).$$

Επομένως, $h \circ (g \circ f) = (h \circ g) \circ f$. □

1.2.14 Σημείωση (Μεταθετικά διαγράμματα). Σε διάφορους κλάδους τής Άλγεβρας (αλλά και άλλων μαθηματικών περιοχών) είναι σύνηθες το να συναντά κανείς ολόκληρα *διαγράμματα συμβόλων* αποτελούμενα από γράμματα (που παριστούν μη κενά σύνολα) και βέλη (που δηλούν απεικονίσεις μεταξύ αυτών). Ένα διάγραμμα αυτού τού είδους καλείται **μεταθετικό διάγραμμα** στην περίπτωση κατά την οποία όλες οι δυνατές συνθέσεις απεικονίσεων (που προκύπτουν ακολουθώντας κατά τρόπο συνεπή τη φορά των υπαρχόντων βελών) από οιοδήποτε (πάγιο) σύνολο αφετηρίας σε οιοδήποτε (πάγιο) σύνολο απολήξεως[11] είναι ίσες μεταξύ τους. Επί παραδείγματι, διαγράμματα τής μορφής





[11] Εν προκειμένω, θεωρούμε ως **σύνολο αφετηρίας** κάποιο σύνολο το οποίο αποτελεί το πεδίο ορισμού μιας απεικονίσεως τού διαγράμματος (και από το οποίο ξεκινά, κατ' ανάγκην, ένα βέλος) και ως **σύνολο απολήξεως** κάποιο άλλο σύνολο το οποίο αποτελεί το πεδίο τιμών μιας απεικονίσεως τού διαγράμματος (και στο οποίο απολήγει, κατ' ανάγκην, ένα -ενδεχομένως διαφορετικό- βέλος).

(όπου τα $f, g, h, \alpha, \beta, \gamma, \delta$ δηλούν απεικονίσεις) είναι μεταθετικά όταν ισχύουν οι ισότητες $h \circ g = f$ και $\beta \circ \alpha = \delta \circ \gamma$, αντιστοίχως.

1.2.15 Παρατήρηση. Η σύνθεση απεικονίσεων (1.6) *δεν* έχει (εν γένει) τη *μεταθετική ιδιότητα*, πράγμα που σημαίνει ότι, δοθέντων δυο απεικονίσεων f και g, για τις οποίες ορίζονται αμφότερες οι συνθέσεις $f \circ g$ και $g \circ f$, *δεν* έχουμε κατ' ανάγκην $f \circ g = g \circ f$!

1.2.16 Πρόταση. *Ας υποθέσουμε ότι οι $f : A \longrightarrow B$ και $g : B \longrightarrow C$ είναι δυο απεικονίσεις. Τότε ισχύουν οι ακόλουθες συνεπαγωγές*:

(i) f, g *ενριπτικές* $\implies$ $g \circ f$ *ένριψη*

(ii) f, g *επιρριπτικές* $\implies$ $g \circ f$ *επίρριψη*

(iii) $g \circ f$ *ένριψη* $\implies$ f *ένριψη*

(iv) $g \circ f$ *επίρριψη* $\implies$ g *επίρριψη*

Απόδειξη. (i) Έστω ότι τα x, x' είναι στοιχεία τού A, τέτοια ώστε να ισχύει η ισότητα $(g \circ f)(x) = (g \circ f)(x')$. Τότε

$$g(f(x)) = g\left(f(x')\right) \underset{g \ \text{1-1}}{\Longrightarrow} f(x) = f(x') \underset{f \ \text{1-1}}{\Longrightarrow} x = x',$$

οπότε η $g \circ f$ είναι εξ ορισμού μια ένριψη.

(ii) Εάν οι f, g είναι επιρριπτικές, τότε $f(A) = B$ και $g(B) = C$, οπότε

$$g(f(A)) = g(B) = C.$$

(iii) Έστω ότι τα x, x' είναι στοιχεία τού A, τέτοια ώστε να ισχύει $f(x) = f(x')$. Τότε

$$(g \circ f)(x) = g(f(x)) = g\left(f(x')\right) = (g \circ f)(x') \underset{g \circ f \ \text{1-1}}{\Longrightarrow} x = x',$$

οπότε η f είναι εξ ορισμού μια ένριψη.

(iv) Εάν η $g \circ f$ είναι μια επίρριψη, τότε για κάθε $z \in C$ υπάρχει ένα στοιχείο $x \in A$, τέτοιο ώστε να ισχύει η ισότητα $(g \circ f)(x) = z$. Αυτό σημαίνει ότι υπάρχει ένα $y \in B$ (ήτοι το $y := f(x)$), τέτοιο ώστε $g(y) = z$. Κατά συνέπειαν, η g είναι μια επίρριψη. □

1.2.17 Λήμμα. *Έστω $f : A \longrightarrow B$ μια απεικόνιση. Τότε ισχύουν τα εξής*:

(i) *Εάν η f είναι ενριπτική και οι $g, h : C \longrightarrow A$ δυο απεικονίσεις, τότε*

$$f \circ g = f \circ h \Longrightarrow g = h.$$

(ii) *Εάν η f είναι επιρριπτική και οι $g, h : B \longrightarrow C$ δυο απεικονίσεις, τότε*

$$g \circ f = h \circ f \Longrightarrow g = h.$$

Απόδειξη. (i) Κατά την υπόθεσή μας, $f \circ g = f \circ h$. Επομένως, για κάθε $z \in C$,

$$f \circ g(z) = f \circ h(z) \Longrightarrow f(g(z)) = f(h(z)) \underset{f \ \text{1-1}}{\Longrightarrow} g(z) = h(z) \Longrightarrow g = h.$$

(ii) Επειδή η f είναι επιρριπτική, για κάθε $y \in B$ υπάρχει κάποιο $x \in A$, τέτοιο ώστε $f(x) = y$. Εάν $g \circ f = h \circ f$, τότε $g(y) = g(f(x)) = h(f(x)) = h(y)$, οπότε τελικώς $g = h$. □

1.2.18 Πρόταση. *Έστω $f : A \longrightarrow B$ μια απεικόνιση.*

(i) *Η f είναι ενριπτική* $\iff$ $\exists\, g : B \longrightarrow A$, *ούτως ώστε* $g \circ f = \mathrm{id}_A$.

(ii) *Η f είναι επιρριπτική* $\iff$ $\exists\, h : B \longrightarrow A$, *ούτως ώστε* $f \circ h = \mathrm{id}_B$.

(iii) *Η f είναι αμφιρριπτική* $\iff$ $\begin{cases} \exists\, \vartheta : B \longrightarrow A, \text{ούτως ώστε} \\ \vartheta \circ f = \mathrm{id}_A \text{ και } f \circ \vartheta = \mathrm{id}_B. \end{cases}$

Εν τοιαύτη περιπτώσει, η απεικόνιση ϑ είναι μοναδική (ως προς αυτήν την ιδιότητα), συμβολίζεται ιδιαιτέρως ως f^{-1} και ονομάζεται **η αντίστροφη απεικόνιση τής** f (ή απλώς **η αντίστροφος τής** f).

Απόδειξη. (i) Εάν η f είναι ενριπτική, τότε για όλα τα $y \in \mathrm{Im}\,(f) = f(A)$ οι ίνες $f^{-1}(y)$ θα αποτελούνται από ένα και μόνον στοιχείο τού A. Ας συμβολίσουμε λοιπόν για κάθε $y \in \mathrm{Im}\,(f)$ αυτό το στοιχείο ως x_y. (Για το x_y ισχύει εξ ορισμού $f(x_y) = y$). Αντιθέτως, για κάθε $y \in B \smallsetminus \mathrm{Im}(f)$ έχουμε $f^{-1}(y) = \varnothing$. Παγιώνουμε εφεξής ένα στοιχείο $x_0 \in A$ (σημειωτέον ότι το A δεν είναι κενό) και ορίζουμε μια απεικόνιση $g : B \longrightarrow A$ ως ακολούθως:

$$g\,(y) := \begin{cases} x_y, & \text{όταν } y \in \mathrm{Im}\,(f)\,, \\ x_0, & \text{όταν } y \in B \smallsetminus \mathrm{Im}(f). \end{cases}$$

Τότε για κάθε $x \in A$ λαμβάνουμε

$$(g \circ f)\,(x) = g(f(x)) = x_y, \text{ όταν θέσουμε } y := f(x)$$

οπότε (κατά το 1.2.11 (iii))

$$f^{-1}\,(\{y\}) = f^{-1}\,(\{f(x)\}) = \{x\},$$

απ' όπου έπεται ότι

$$x_y = x = \mathrm{id}_A\,(x)\,,$$

ήτοι $g \circ f = \mathrm{id}_A$. Και αντιστρόφως· εάν υπάρχει μια απεικόνιση $g : B \longrightarrow A$, τέτοια ώστε να ισχύει $g \circ f = \mathrm{id}_A$ και εάν τα x_1, x_2 είναι δυο στοιχεία τού A, ούτως ώστε $f(x_1) = f\,(x_2)$, τότε

$$x_1 = \mathrm{id}_A\,(x_1) = (g \circ f)\,(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)\,(x_2) = \mathrm{id}_A\,(x_2) = x_2.$$

Άρα η f είναι όντως ενριπτική.

(ii) Εάν η f είναι επιρριπτική, τότε για κάθε $y \in B = \mathrm{Im}(f) = f(A)$ επιλέγουμε ένα $x_y \in A$, ούτως ώστε $f(x_y) = y$, και ορίζουμε την απεικόνιση

$$h : B \longrightarrow A, \quad y \longmapsto x_y.$$

Τότε

$$(f \circ h)\,(y) = f(h(y)) = f\,(x_y) = y = \mathrm{id}_B(y) \Longrightarrow f \circ h = \mathrm{id}_B.$$

Και αντιστρόφως· εάν υπάρχει μια απεικόνιση $h : B \longrightarrow A$, τέτοια ώστε να ισχύει $f \circ h = \mathrm{id}_B$, τότε για κάθε $y \in B$ θεωρούμε την εικόνα $x := h\,(y) \in A$, οπότε έχουμε

$$y = \mathrm{id}_B(y) = (f \circ h)\,(y) = f(x) \in \mathrm{Im}(f) = f(A).$$

Άρα η f είναι όντως επιρριπτική.

(iii) Κατ' αρχάς υποθέτουμε ότι η f είναι αμφιρριπτική. Τότε για την f (που είναι, ιδιαιτέρως, επιρριπτική) υπάρχει μια απεικόνιση $\vartheta : B \longrightarrow A$, ούτως ώστε να ισχύει $f \circ \vartheta = \mathrm{id}_B$ (κατά το (ii) "$\Longrightarrow$"). Γι' αυτήν την απεικόνιση έχουμε

$$f \circ (\vartheta \circ f) = (f \circ \vartheta) \circ f = \mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A,$$

οπότε $\vartheta \circ f = \mathrm{id}_A$ (λόγω τού ότι η f είναι και ενριπτική, πρβλ. 1.2.17 (i)). Αρκεί λοιπόν να αποδειχθεί ότι οι εν λόγω ισότητες $\vartheta \circ f = \mathrm{id}_A$ και $f \circ \vartheta = \mathrm{id}_B$ καθορίζουν μονοσημάντως την ϑ. Υποθέτοντας την ύπαρξη μιας απεικονίσεως $\widetilde{\vartheta} : B \longrightarrow A$, η οποία ικανοποιεί τις ισότητες $\widetilde{\vartheta} \circ f = \mathrm{id}_A$ και $f \circ \widetilde{\vartheta} = \mathrm{id}_B$, λαμβάνουμε

$$f \circ \widetilde{\vartheta} = \mathrm{id}_B = f \circ \vartheta,$$

απ' όπου συνάγεται ότι $\widetilde{\vartheta} = \vartheta$ κατά το λήμμα 1.2.17 (ii) (καθόσον η f είναι και επιρριπτική). Η αντίστροφη συνεπαγωγή έπεται από τις αντίστροφες συνεπαγωγές των (i) και (ii). □

1.2.19 Παρατήρηση. Η αντίστροφος

$$f^{-1} : B \longrightarrow A$$

μιας απεικονίσεως $f : A \longrightarrow B$ ορίζεται *μόνον όταν* η f είναι αμφιρριπτική· αντιθέτως, η αντίστροφη εικόνα[12] $h^{-1}(D)$ οιουδήποτε υποσυνόλου $D \subseteq B$ μέσω μιας απεικονίσεως $h : A \longrightarrow B$ ορίζεται *πάντοτε* χωρίς να απαιτείται η αμφιρριπτικότητα τής h. Βεβαίως, για αμφιρριπτικές απεικονίσεις $f : A \longrightarrow B$, οι δύο (ατυχώς ομοειδείς) συμβολισμοί συμπίπτουν εννοιολογικώς, καθόσον το αρχέτυπο $f^{-1}(D)$ οιουδήποτε υποσυνόλου $D \subseteq B$ ισούται με την εικόνα $f^{-1}(D)$ τού D μέσω τής f^{-1}.

1.2.20 Πρόταση. *Εάν οι $f : A \longrightarrow B$ και $g : B \longrightarrow C$ είναι δυο αμφιρριπτικές απεικονίσεις, τότε και η σύνθεσή τους $g \circ f : A \longrightarrow C$ είναι αμφιρριπτική, έχουσα ως αντίστροφό της την*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}. \tag{1.7}$$

ΑΠΟΔΕΙΞΗ. Σύμφωνα με τα (i) και (ii) τής προτάσεως 1.2.16 η $g \circ f$ είναι αμφιρριπτική. Αρκεί λοιπόν ο προσδιορισμός τής αντιστρόφου της. Προφανώς,

$$\begin{aligned} f^{-1} \circ g^{-1} \circ (g \circ f) &= f^{-1} \circ \big(g^{-1} \circ g\big) \circ f \ \text{(βλ. πρόταση 1.2.13)} \\ &= f^{-1} \circ \mathrm{id}_B \circ f \ \text{(λόγω τού 1.2.18 (iii))} \\ &= f^{-1} \circ f \ \text{(λόγω τού ότι } \mathrm{id}_B \circ f = f\text{)} \\ &= \mathrm{id}_A \ \text{(λόγω τού 1.2.18 (iii)).} \end{aligned}$$

Παρομοίως αποδεικνύεται ότι $(g \circ f) \circ f^{-1} \circ g^{-1} = \mathrm{id}_C$. Άρα η ισότητα (1.7) είναι αληθής επί τη βάσει τού (iii) τής προτάσεως 1.2.18. □

1.2.21 Ορισμός. Εάν οι $f : A \longrightarrow C$ και $g : B \longrightarrow D$ είναι δυο απεικονίσεις, τότε ως **καρτεσιανό γινόμενο των f και g** ορίζεται η απεικόνιση

$$f \times g : A \times B \longrightarrow C \times D, \quad (x, y) \longmapsto (f \times g)(x, y) := (f(x), g(y)).$$

1.2.22 Πρόταση. *Εάν οι $f : A \longrightarrow C$ και $g : B \longrightarrow D$ είναι δυο απεικονίσεις, τότε ισχύουν τα ακόλουθα:*

(i) *Εάν οι $h : C \longrightarrow E$, $k : D \longrightarrow F$ είναι απεικονίσεις, τότε*

$$(h \times k) \circ (f \times g) = (h \circ f) \times (k \circ g). \tag{1.8}$$

(ii) *Εάν οι f και g είναι ενριπτικές, τότε και η $f \times g$ είναι ενριπτική.*

[12] Ορισμένοι συγγραφείς, για την αποφυγή συγχύσεως, χρησιμοποιούν τον (κατά τι ιδιομερή) συμβολισμό $h^{\leftarrow}(D)$ ή $h^{-}(D)$ (αντί τού $h^{-1}(D)$) για να εκφράσουν την αντίστροφη εικόνα ενός υποσυνόλου $D \subseteq B$ μέσω μιας απεικονίσεως $h : A \longrightarrow B$. Ωστόσο, επειδή ο *κλασικός συμβολισμός* $h^{-1}(D)$ είναι επικρατέστερος στη βιβλιογραφία, απαιτείται ιδιαίτερη προσοχή!

(iii) *Εάν οι f και g είναι επιρριπτικές, τότε και η $f \times g$ είναι επιριπτική.*
(iv) *Εάν οι f και g είναι αμφιριπτικές, τότε και η $f \times g$ είναι αμφιριπτική, και*

$$(f \times g)^{-1} = f^{-1} \times g^{-1}. \tag{1.9}$$

Απόδειξη. (i) Για οιοδήποτε διατεταγμένο ζεύγος $(x, y) \in A \times B$ έχουμε

$$\begin{aligned} ((h \times k) \circ (f \times g))(x, y) &= (h \times k)(f(x), g(y)) = (h(f(x)), k(g(y))) \\ &= ((h \circ f)(x), (k \circ g)(y)) = ((h \circ f) \times (k \circ g))(x, y), \end{aligned}$$

οπότε η (1.8) είναι αληθής.

(ii) Εάν οι f και g είναι ενριπτικές, τότε, σύμφωνα με το (i) τής προτάσεως 1.2.18, υπάρχουν απεικονίσεις $h : C \longrightarrow A$ και $k : D \longrightarrow B$, ούτως ώστε να ισχύουν οι ισότητες $h \circ f = \mathrm{id}_A$ και $k \circ g = \mathrm{id}_B$. Κατά συνέπειαν,

$$(h \times k) \circ (f \times g) \underset{(1.8)}{=} (h \circ f) \times (k \circ g) = \mathrm{id}_A \times \mathrm{id}_B = \mathrm{id}_{A \times B},$$

όπου η τελευταία ισότητα είναι απόρροια τού ότι για κάθε διατεταγμένο ζεύγος $(x, y) \in A \times B$ έχουμε $(\mathrm{id}_A \times \mathrm{id}_B)(x, y) = (\mathrm{id}_A(x), \mathrm{id}_B(y)) = (x, y) = \mathrm{id}_{A \times B}(x, y)$. Ως εκ τούτου, $(h \times k) \circ (f \times g) = \mathrm{id}_{A \times B}$, οπότε η $f \times g$ είναι ενριπτική λόγω τού (i) τής προτάσεως 1.2.18.

(iii) Τούτο αποδεικνύεται παρομοίως κάνοντας χρήση τού 1.2.18 (ii).

(iv) Εάν οι f και g είναι αμφιρριπτικές, τότε από τα ανωτέρω (ii) και (iii) έπεται άμεσα ότι η $f \times g$ είναι ωσαύτως αμφιρριπτική. Επιπροσθέτως,

$$\left(f^{-1} \times g^{-1}\right) \circ (f \times g) \underset{(1.8)}{=} (f^{-1} \circ f) \times (g^{-1} \circ g) = \mathrm{id}_A \times \mathrm{id}_B = \mathrm{id}_{A \times B}$$

και (κατ' αναλογίαν) $(f \times g) \circ \left(f^{-1} \times g^{-1}\right) = \mathrm{id}_{C \times D}$. Άρα η ισότητα (1.9) είναι αληθής επί τη βάσει τού (iii) τής προτάσεως 1.2.18. □

1.3 ΣΧΕΣΕΙΣ ΙΣΟΔΥΝΑΜΙΑΣ

1.3.1 Ορισμός. Έστω A ένα σύνολο. Λέμε ότι μια διμελής σχέση $\mathcal{R} \subseteq A \times A$ είναι

(i) **ανακλαστική** (ή **αυτοπαθής**) όταν

$$(x, x) \in \mathcal{R}, \ \forall x \in A,$$

(ii) **συμμετρική** όταν για οιαδήποτε $x, y \in A$ ισχύει η συνεπαγωγή

$$(x, y) \in \mathcal{R} \Longrightarrow (y, x) \in \mathcal{R},$$

(iii) **αντισυμμετρική** όταν για οιαδήποτε $x, y \in A$ ισχύει η συνεπαγωγή

$$(x, y) \in \mathcal{R} \ \text{ και } \ (y, x) \in \mathcal{R} \Longrightarrow x = y,$$

και (iv) **μεταβατική** όταν για οιαδήποτε $x, y, z \in A$ ισχύει η συνεπαγωγή

$$(x, y) \in \mathcal{R} \ \text{ και } \ (y, z) \in \mathcal{R} \Longrightarrow (x, z) \in \mathcal{R}.$$

1.3.2 Ορισμός. Έστω A ένα σύνολο. Μια διμελής σχέση $\mathcal{R} \subseteq A \times A$ καλείται **σχέση ισοδυναμίας** επί τού A όταν είναι ανακλαστική, συμμετρική και μεταβατική. Εάν η $\mathcal{R}$ είναι μια σχέση ισοδυναμίας επί τού A και $x \in A$, τότε ορίζουμε ως **κλάση ισοδυναμίας** τού x **ως προς την** $\mathcal{R}$ το σύνολο

$$\boxed{[x] := \{\, y \in A \mid (x, y) \in \mathcal{R}\}.} \tag{1.10}$$

(Όταν εργαζόμαστε με διαφορετικές σχέσεις ισοδυναμίας (1.10) και υφίσταται κίνδυνος συγχύσεως τού τι οφείλει να σημαίνει το σύμβολο $[x]$, τότε γράφουμε $[x]_{\mathcal{R}}$ αντί τού $[x]$.) Κάθε στοιχείο τού $[x]$ καλείται **εκπρόσωπος** τής κλάσεως ισοδυναμίας $[x]$. Τέλος, ως

$$\boxed{A/\mathcal{R} := \{\, [x] \mid x \in A\}}$$

συμβολίζουμε το **σύνολο των κλάσεων ισοδυναμίας** (ως προς την $\mathcal{R}$).

1.3.3 Ορισμός. Έστω A ένα μη κενό σύνολο και έστω $\varnothing \neq \mathcal{R} \subseteq A \times A$ μια σχέση ισοδυναμίας επί τού A. Τότε η επιρριπτική απεικόνιση

$$\boxed{\pi : A \longrightarrow A/\mathcal{R},\ \ x \longmapsto \pi(x) := [x]\,,} \tag{1.11}$$

καλείται **φυσική επίρριψη ως προς την** $\mathcal{R}$. (Όταν επιθυμούμε να δώσουμε έμφαση στη θεωρούμενη σχέση ισοδυναμίας, τότε γράφουμε $\pi_{\mathcal{R}}$ αντί τού π.)

1.3.4 Σημείωση (Εναλλακτικός συμβολισμός). Ενίοτε, για λόγους συμβολιστικής συντομίας, χρησιμοποιούμε το σύμβολο "$\sim$" αντί τού $\mathcal{R}$ και γράφουμε $x \sim y$ αντί τού $(x, y) \in \mathcal{R}$, $x \nsim y$ αντί τού $(x, y) \notin \mathcal{R}$, $[x]_{\sim}$ αντί τού $[x]_{\mathcal{R}}$, $A/\sim$ αντί τού $A/\mathcal{R}$ (ονομάζοντας το $A/\sim$ «σύνολο των κλάσεων ισοδυναμίας *ως προς την* "$\sim$"») και $\pi_{\sim}$ αντί τού $\pi_{\mathcal{R}}$.

1.3.5 Ορισμός. Έστω A ένα σύνολο και έστω $\mathcal{R} \subseteq A \times A$ μια σχέση ισοδυναμίας επί τού A. Εάν $C \subseteq A$, τότε το

$$\mathcal{R}|_C := \mathcal{R} \cap (C \times C) \subseteq C \times C$$

αποτελεί μια σχέση ισοδυναμίας επί τού C (όπως ελέγχεται άμεσα) η οποία καλείται **περιορισμός τής** $\mathcal{R}$ **στο** C. Σημειωτέον ότι

$$[x]_{\mathcal{R}|_C} = [x]_{\mathcal{R}} \cap C,\ \ \forall x \in C.$$

1.3.6 Πρόταση. *Έστω A ένα μη κενό σύνολο και έστω $\varnothing \neq \mathcal{R} \subseteq A \times A$ μια σχέση ισοδυναμίας επί τού A. Εάν $C \subseteq A$ και εάν θέσουμε*

$$C(\mathcal{R}) := \pi^{-1}(\pi(C)), \tag{1.12}$$

όπου $\pi : A \longrightarrow A/\mathcal{R}$ η φυσική επίρριψη (1.11) ως προς την $\mathcal{R}$, τότε ισχύουν τα ακόλουθα:

(i) $C(\mathcal{R}) = \bigcup\{[y]_{\mathcal{R}} \mid y \in C\} = \bigcup\{[y]_{\mathcal{R}} \mid y \in A : [y]_{\mathcal{R}} \cap C \neq \varnothing\}$.

(ii) $[x]_{\mathcal{R}|_{C(\mathcal{R})}} = [x]_{\mathcal{R}},\ \ \forall x \in C(\mathcal{R})$.

Αποδειξη. (i) Παρατηρούμε ότι

$$x \in C(\mathcal{R}) \Leftrightarrow \pi(x) \in \pi(C) \Leftrightarrow [x]_{\mathcal{R}} \in \{[y]_{\mathcal{R}} \mid y \in C\} \text{ (εξ ορισμού)}$$
$$\Leftrightarrow \exists y \in C : [y]_{\mathcal{R}} = [x]_{\mathcal{R}} \Leftrightarrow [x]_{\mathcal{R}} \subseteq \bigcup\{[y]_{\mathcal{R}} \mid y \in C\}$$
$$\Leftrightarrow x \in \bigcup\{[y]_{\mathcal{R}} \mid y \in C\}.$$

Άρα η πρώτη ισότητα είναι αληθής. Η δεύτερη είναι προφανής.
(ii) Επειδή για κάθε $x \in C(\mathcal{R})$ έχουμε $[x]_{\mathcal{R}|_{C(\mathcal{R})}} = [x]_{\mathcal{R}} \cap C(\mathcal{R})$ και επειδή (βάσει τού (i)) το $C(\mathcal{R})$ είναι η ένωση κάποιων κλάσεων ισοδυναμίας *ως προς την* $\mathcal{R}$, συμπεραίνουμε ότι $[x]_{\mathcal{R}} \cap C(\mathcal{R}) = [x]_{\mathcal{R}},\ \forall x \in C(\mathcal{R})$. □

1.3.7 Ορισμός. Το σύνολο $C(\mathcal{R})$ που ορίσθηκε στην (1.12) καλείται **κεκορεσμένη θήκη τού** C **ως προς την** $\mathcal{R}$.

1.3.8 Πρόταση. *Έστω A ένα μη κενό σύνολο. Εάν οι*

$$\varnothing \neq \mathcal{R} \subseteq A \times A,\ \ \varnothing \neq \mathcal{R}' \subseteq A \times A$$

είναι δυο σχέσεις ισοδυναμίας επί τού A, τότε οι ακόλουθες τρεις συνθήκες είναι ισοδύναμες:
(i) *Για οιαδήποτε $x, y \in A$ ισχύει η συνεπαγωγή $(x,y) \in \mathcal{R} \Longrightarrow (x,y) \in \mathcal{R}'$.*
(ii) $[x]_{\mathcal{R}} \subseteq [x]_{\mathcal{R}'},\ \forall x \in A$.
(iii) $C(\mathcal{R}) \subseteq C(\mathcal{R}')$ *για κάθε $C \subseteq A$.*

Αποδειξη. (i)⇒(ii): Για οιοδήποτε $x \in A$ ισχύουν οι συνεπαγωγές

$$y \in [x]_{\mathcal{R}} \Rightarrow (x,y) \in \mathcal{R} \Rightarrow (x,y) \in \mathcal{R}' \Rightarrow y \in [x]_{\mathcal{R}'},$$

οπότε $[x]_{\mathcal{R}} \subseteq [x]_{\mathcal{R}'},\ \forall x \in A$.
(ii)⇒(iii): Για κάθε $C \subseteq A$ ισχύουν (δυνάμει τού 1.3.6 (i)) οι εξής συνεπαγωγές:

$$x \in C(\mathcal{R}) \Rightarrow x \in \bigcup\{[y]_{\mathcal{R}} \mid y \in C\} \Rightarrow x \in \bigcup\{[y]_{\mathcal{R}'} \mid y \in C\} \Rightarrow x \in C(\mathcal{R}').$$

Άρα $C(\mathcal{R}) \subseteq C(\mathcal{R}')$ για κάθε $C \subseteq A$.
(iii)⇒(i): Εάν $x, y \in A$ με $(x,y) \in \mathcal{R}$, τότε για το $C := \{x\}$ έχουμε

$$\pi_{\mathcal{R}}(y) = \pi_{\mathcal{R}}(x) \in \pi_{\mathcal{R}}(C) \Rightarrow y \in C(\mathcal{R}).$$

Εξ υποθέσεως, $y \in C(\mathcal{R}')$, οπότε $\pi_{\mathcal{R}'}(y) \in \pi_{\mathcal{R}'}(C(\mathcal{R}')) = \{\pi_{\mathcal{R}'}(x)\}$. Τούτο σημαίνει ότι $\pi_{\mathcal{R}'}(y) = \pi_{\mathcal{R}'}(x)$, απ' όπου προκύπτει ότι $(x,y) \in \mathcal{R}'$. □

1.3.9 Ορισμός. Όταν ισχύει μία (και, κατ' επέκταση, και οι τρεις) εκ των συνθηκών (i), (ii) και (iii) τής προτάσεως 1.3.8, τότε λέμε ότι η $\mathcal{R}$ είναι **λεπτότερη** τής $\mathcal{R}'$ (ή ότι η $\mathcal{R}'$ είναι **αδρότερη** τής $\mathcal{R}$).

1.3.10 Ορισμός. Έστω ότι τα A, B είναι δυο σύνολα. Εάν η $\mathcal{R} \subseteq A \times A$ είναι μια διμελής σχέση επί τού A και η $\mathcal{S} \subseteq B \times B$ μια διμελής σχέση επί τού B, τότε επί τού καρτεσιανού γινομένου $A \times B$ των A και B ορίζεται μια διμελής σχέση $\mathcal{R} \times \mathcal{S}$ ως εξής:

$$\boxed{((x,x'),(y,y')) \in \mathcal{R} \times \mathcal{S} \underset{\text{ορσ}}{\Longleftrightarrow} (x,y) \in \mathcal{R} \text{ και } (x',y') \in \mathcal{S}.}$$

Η $\mathcal{R} \times \mathcal{S}$ καλείται **το καρτεσιανό γινόμενο των** $\mathcal{R}$ **και** $\mathcal{S}$.

1.3.11 Πρόταση. *Έστω ότι τα A, B είναι δυο σύνολα. Εάν η $\mathcal{R}$ είναι μια σχέση ισοδυναμίας επί τού A και η $\mathcal{S}$ μια σχέση ισοδυναμίας επί τού B, τότε η $\mathcal{R} \times \mathcal{S}$ είναι μια σχέση ισοδυναμίας επί τού $A \times B$.*

Απόδειξη. Επειδή για κάθε $x \in A$ και κάθε $y \in B$ έχουμε

$$(x, x) \in \mathcal{R} \text{ και } (y, y) \in \mathcal{S}$$

(λόγω τού ότι οι $\mathcal{R}$ και $\mathcal{S}$ είναι ανακλαστικές διμελείς σχέσεις), συνάγεται ότι

$$((x, y), (x, y)) \in \mathcal{R} \times \mathcal{S},$$

οπότε και η $\mathcal{R} \times \mathcal{S}$ είναι ανακλαστική. Το ότι η $\mathcal{R} \times \mathcal{S}$ είναι συμμετρική έπεται άμεσα από τον ορισμό της. Απομένει να αποδειχθεί ότι η $\mathcal{R} \times \mathcal{S}$ είναι μεταβατική. Προς τούτο θεωρούμε διατεταγμένα ζεύγη $(x, x'), (y, y'), (z, z')$ ανήκοντα στο καρτεσιανό γινόμενο $A \times B$ και τέτοια ώστε $((x, x'), (y, y')) \in \mathcal{R} \times \mathcal{S}$ και $((y, y'), (z, z')) \in \mathcal{R} \times \mathcal{S}$. Προφανώς,

$$\left.\begin{matrix}(x, y) \in \mathcal{R} \\ (y, z) \in \mathcal{R}\end{matrix}\right\} \Rightarrow (x, z) \in \mathcal{R} \text{ και } \left.\begin{matrix}(x', y') \in \mathcal{S} \\ (y', z') \in \mathcal{S}\end{matrix}\right\} \Rightarrow (x', z') \in \mathcal{S}$$

(λόγω τού ότι οι $\mathcal{R}$ και $\mathcal{S}$ είναι μεταβατικές διμελείς σχέσεις), οπότε

$$((x, x'), (z, z')) \in \mathcal{R} \times \mathcal{S},$$

και, ως εκ τούτου, η $\mathcal{R} \times \mathcal{S}$ είναι όντως μεταβατική. □

1.3.12 Ορισμός. Έστω A ένα μη κενό σύνολο. Ένα υποσύνολο $\mathfrak{X}$ τού $\mathfrak{P}(A)$ ονομάζεται **διαμελισμός**[13] τού συνόλου A όταν πληρούνται οι ακόλουθες συνθήκες:

(i) $B \neq \varnothing,\ \forall B \in \mathfrak{X}$.

(ii) Για οιαδήποτε $B, B' \in \mathfrak{X}$ ισχύει η αμφίπλευρη συνεπαγωγή

$$B \cap B' \neq \varnothing \Longleftrightarrow B = B'.$$

(iii) $A = \bigcup\{B \mid B \in \mathfrak{X}\}$.

1.3.13 Παραδείγματα. Έστω A ένα μη κενό σύνολο.

(i) Το $\{A\}$ αποτελεί έναν διαμελισμό τού A.

(ii) Εάν $A \supsetneq A' \neq \varnothing$, τότε το $\{A', A \smallsetminus A'\}$ είναι διαμελισμός τού A.

(iii) Εάν τα $\mathfrak{X}$ και $\mathfrak{X}'$ είναι δυο διαμελισμοί τού A, τότε και το

$$\mathfrak{Z} := \{C \mid \exists B \in \mathfrak{X},\ B' \in \mathfrak{X}' : \varnothing \neq B \cap B' = C\}$$

είναι διαμελισμός τού A.

Η επόμενη πρόταση μας πληροφορεί ότι κάθε σχέση ισοδυναμίας επί ενός μη κενού συνόλου προσδιορίζει (κατά φυσικό τρόπο) έναν διαμελισμό αυτού.

1.3.14 Πρόταση. *Έστω A ένα μη κενό σύνολο. Εάν η "$\sim$" είναι μια σχέση ισοδυναμίας επί τού A, τότε ισχύουν τα εξής:*

(i) *$[x] \neq \varnothing$ για κάθε $x \in A$.*

(ii) *Εάν $x, y \in A$, τότε $x \sim y \Longleftrightarrow [x] = [y]$.*

(iii) *Εάν $x, y \in A$, τότε $x \nsim y \Longleftrightarrow [x] \cap [y] = \varnothing$.*

(iv) *Το σύνολο $A/\sim := \{[x] \mid x \in A\}$ των κλάσεων ισοδυναμίας ως προς την "$\sim$"*

[13] Αντ' αυτού χρησιμοποιείται ενίοτε και ο όρος «διαμέριση».

είναι ένας διαμελισμός τού A.

ΑΠΟΔΕΙΞΗ. (i) Έστω τυχόν $x \in A$. Τότε, επειδή $x \sim x$, έχουμε $x \in [x] \Rightarrow [x] \neq \varnothing$.

(ii) Εάν $x \sim y$ και $z \in [x]$, τότε, λόγω τής συμμετρικής και τής μεταβατικής ιδιότητας, έχουμε

$$\left.\begin{array}{r} x \sim z \Rightarrow z \sim x \\ \text{και } x \sim y \end{array}\right\} \Longrightarrow z \sim y \Longrightarrow y \sim z \Longrightarrow z \in [y],$$

οπότε $[x] \subseteq [y]$. Εάν εναλλάξουμε τους ρόλους των x και y και εφαρμόσουμε την ίδια επιχειρηματολογία, τότε συμπεραίνουμε ότι $[y] \subseteq [x]$. Άρα τελικώς $[x] = [y]$. Και αντιστρόφως· εάν $[x] = [y]$, τότε $x \sim y$, διότι $y \in [y]$.

(iii) Εάν $x \not\sim y$ και εάν υποθέσουμε ότι $\exists z \in [x] \cap [y]$, τότε, λόγω τής συμμετρικής και τής μεταβατικής ιδιότητας, έχουμε

$$\left.\begin{array}{r} y \sim z \\ \text{και } x \sim z \Rightarrow z \sim x \end{array}\right\} \Longrightarrow y \sim x \Longrightarrow x \sim y.$$

Άτοπο! Άρα $[x] \cap [y] = \varnothing$. Και αντιστρόφως· εάν $[x] \cap [y] = \varnothing$ και εάν υποθέσουμε ότι $x \sim y$, τότε

$$x \sim y \underset{\text{(ii)}}{\Longleftrightarrow} [x] = [y] \Longrightarrow [x] \cap [y] = [x] \underset{\text{(i)}}{\neq} \varnothing.$$

Άτοπο! Κατά συνέπειαν, $x \not\sim y$.

(iv) Από τα ανωτέρω (i), (ii) και (iii) έπεται ότι το σύνολο

$$A/\sim := \{\, [x] \mid x \in A \} \subseteq \mathfrak{P}\,(A)$$

πληροί τις συνθήκες (i) και (ii) τού ορισμού 1.3.12. Από την άλλη μεριά, επειδή

$$[x] \subseteq A,\ \forall x \in A \Longrightarrow \bigcup \{\, [x] \mid x \in A \} \subseteq A$$

και *για κάθε* $z \in A$,

$$z \in [z] \in \bigcup \{\, [x] \mid x \in A \} \Longrightarrow A \subseteq \bigcup \{\, [x] \mid x \in A \}$$

συμπεραίνουμε τελικώς ότι $A = \bigcup \{\, [x] \mid x \in A \}$, οπότε το $A/\sim$ πληροί *και* τη συνθήκη (iii) τού ορισμού 1.3.12. □

1.3.15 Παρατήρηση. Η επανειλημμένως και ποικιλοτρόπως χρησιμοποιούμενη έκφραση, ότι κανείς «ταυτίζει» συγκεκριμένα στοιχεία ενός δεδομένου μη κενού συνόλου A, τα οποία έχουν κάποιες «προδιαγεγραμμένες» ιδιότητες, ισοδυναμεί με τη μετάβαση από το A στο $A/\sim$, όπου η "$\sim$" είναι μια κατάλληλη σχέση ισοδυναμίας.

1.3.16 Παράδειγμα. Έστω $A = \{$όλοι οι άνθρωποι τής γης$\}$. Εάν ορίσουμε την ακόλουθη σχέση ισοδυναμίας "$\sim$" επί τού A:

$$x \sim y \underset{\text{ορσ}}{\Longleftrightarrow} (\text{οι } x \text{ και } y \text{ γεννήθηκαν στο ίδιο κράτος}),$$

τότε το σύνολο $A/\sim$ μας παρέχει μια παραμέτρηση των κρατών τής γης (καθότι κάθε κλάση ισοδυναμίας απαρτίζεται από τους κατοίκους τής γης τους γεννηθέντες σε ένα συγκεκριμένο κράτος).

1.3.17 Παράδειγμα. Έστω A ένα μη κενό σύνολο. Εάν ορίσουμε την ακόλουθη σχέση ισοδυναμίας "$\sim$" επί τού A:

$$x \sim y \underset{\text{ορσ}}{\Longleftrightarrow} x = y,$$

τότε η κλάση ισοδυναμίας $[x]$ οιουδήποτε $x \in A$ είναι το σύνολο $\{x\}$. Άρα

$$A/\sim = \{\, \{x\} \mid x \in A \},\ \ A = \bigcup \{\, \{x\} \mid x \in A \} = \{\, x \mid x \in A \}.$$

Προσοχή! Το $A/\sim$ είναι *υποσύνολο τού* $\mathfrak{P}\,(A)$ και δεν θα πρέπει κανείς να το συγχέει, εν προκειμένω, με το ίδιο το σύνολο A.

1.3.18 Ορισμός. (i) Η ένωση $A \cup B$ δυο συνόλων A και B ονομάζεται (**συνολοθεωρητική**) **αποσυνδετή ένωση** των A και B όταν $A \cap B = \varnothing$. (Εν τοιαύτη περιπτώσει, λέμε ότι τα A και B είναι *ξένα μεταξύ τους*.)

(ii) Έστω I ένα μη κενό σύνολο. Με τον όρο (**συνολοθεωρητική**) **αποσυνδετή ένωση** των μελών μιας οικογενείας συνόλων $(A_i)_{i\in I}$ εννοούμε την ένωση $\bigcup_{i\in I} A_i$ (βλ. 1.1.4) *όταν ισχύει* $A_i \cap A_j = \varnothing$, *για κάθε* $(i,j) \in I \times I$, $i \neq j$, ήτοι όταν τα μέλη τής προκειμένης οικογενείας είναι *ανά δύο* (δηλαδή *ανά ζεύγη*) *ξένα μεταξύ τους* ή, με άλλα λόγια, (*σαφώς*) *διακεκριμένα*. Για να επισημάνουμε ότι κάποιο δοθέν σύνολο A είναι η αποσυνδετή ένωση μιας οικογενείας συνόλων $(A_i)_{i\in I}$ κάνουμε χρήση τού ειδικού συμβολισμού

$$A = \coprod_{i\in I} A_i.$$

(iii) Γενικότερα, εάν το S είναι ένα σύνολο, τα στοιχεία τού οποίου είναι *σύνολα*, τότε η ένωση $\bigcup S$ (η ορισθείσα στο εδάφιο 1.1.7) καλείται (**συνολοθεωρητική**) **αποσυνδετή ένωση** (συμβολιζόμενη, ιδιαιτέρως, ως $\coprod S$) όταν τα στοιχεία τού S είναι ανά δύο ξένα μεταξύ τους.

1.3.19 Σημείωση. Εάν η "$\sim$" είναι μια σχέση ισοδυναμίας επί ενός μη κενού συνόλου A, τότε, όπως απεδείχθη στην πρόταση 1.3.14, το $\{[x] \mid x \in A\}$ αποτελεί έναν διαμελισμό τού A. Παρότι πληρούνται οι συνθήκες 1.3.14 (i)-(iv), το *A δεν είναι κατ' ανάγκην αποσυνδετή ένωση* των μελών τής οικογενείας $\{[x] \mid x \in A\}$, διότι δεν έχουμε αποκλείσει ρητώς την (ενδεχόμενη) *επανάληψη* ορισμένων εξ αυτών! Ως εκ τούτου, για να γραφεί το A ως αποσυνδετή ένωση απαιτείται να περιορισθούμε σε ένα υποσύνολό του $\widehat{A}$ με την εξής ιδιότητα: *Για οιαδήποτε στοιχεία $x, y \in \widehat{A}$ ισχύει η συνεπαγωγή*

$$x \neq y \Longrightarrow [x] \neq [y]\,.$$

Εν τοιαύτη περιπτώσει,

$$A = \coprod \{[x] \mid x \in \widehat{A}\}.$$

Κάθε υποσύνολο τού A που έχει αυτήν την ιδιότητα καλείται **πλήρες σύστημα εκπροσώπων τού A ως προς την** "$\sim$".

Δοθέντος ενός διαμελισμού ενός μη κενού συνόλου είναι δυνατόν να ορισθεί επ' αυτού (τού συνόλου) μια σχέση ισοδυναμίας έχουσα τον εν λόγω διαμελισμό ως σύνολο των αντιστοίχων κλάσεων ισοδυναμίας.

1.3.20 Πρόταση. *Έστω $\mathfrak{X} \subseteq \mathfrak{P}(A)$ ένας διαμελισμός ενός μη κενού συνόλου A. Επί τού A ορίζουμε τη διμελή σχέση " $\sim_{\mathfrak{X}}$ " ως ακολούθως*:

$$x \sim_{\mathfrak{X}} y \underset{\text{ορσ}}{\Longleftrightarrow} (\exists B \in \mathfrak{X} : \text{αμφότερα τα } x \text{ και } y \text{ ανήκουν στο } B)\,.$$

Τότε ισχύουν τα εξής:

(i) *Η " $\sim_{\mathfrak{X}}$ "είναι μια σχέση ισοδυναμίας επί τού A.*

(ii) $A/\sim_{\mathfrak{X}} = \mathfrak{X}$.

Απόδειξη. (i) Κατά το 1.3.12 (iii) υπάρχει για κάθε $x \in A$ κάποιο $B \in \mathfrak{X}$ με $x \in B$, οπότε $x \sim_{\mathfrak{X}} x$ και η " $\sim_{\mathfrak{X}}$ " είναι ανακλαστική. Το ότι η " $\sim_{\mathfrak{X}}$ " είναι και συμμετρική είναι προφανές από τον ορισμό της. Υπολείπεται να αποδειχθεί ότι η " $\sim_{\mathfrak{X}}$ " είναι μεταβατική. Προς τούτο θεωρούμε $x, y, z \in A$ για τα οποία ισχύουν οι $x \sim_{\mathfrak{X}} y$ και $y \sim_{\mathfrak{X}} z$. Εξ ορισμού, υπάρχουν $B, B' \in \mathfrak{X}$ με $x, y \in B$ και $y, z \in B'$. Επειδή $y \in B \cap B'$, έχουμε $B \cap B' \neq \varnothing$, οπότε $B = B'$ (δυνάμει τού 1.3.12 (ii)). Επομένως, $x, z \in B \Rightarrow x \sim_{\mathfrak{X}} z$.

(ii) Έστω τυχόν $x \in A$. Θεωρούμε την κλάση ισοδυναμίας του $[x]_{\sim_{\mathfrak{X}}} \in A/\sim_{\mathfrak{X}}$. Κατά το 1.3.12 (iii) υπάρχει κάποιο $B \in \mathfrak{X}$ με $x \in B$. Προφανώς, για οιοδήποτε $y \in A$ ισχύουν οι αμφίπλευρες συνεπαγωγές

$$y \in [x]_{\sim_{\mathfrak{X}}} \Leftrightarrow x \sim_{\mathfrak{X}} y \ \text{(εξ ορισμού)} \Leftrightarrow \exists B' \in \mathfrak{X} : x, y \in B' \ \text{(εξ ορισμού)}$$
$$\Leftrightarrow y \in B \ \text{(διότι } x \in B \cap B' \Rightarrow B \cap B' \neq \varnothing \underset{\text{1.3.12 (ii)}}{\Longrightarrow} B = B').$$

Άρα $[x]_{\sim_{\mathfrak{X}}} = B \in \mathfrak{X}$ και, ως εκ τούτου, $A/\sim_{\mathfrak{X}} \subseteq \mathfrak{X}$.

Και αντιστρόφως· εάν $B \in \mathfrak{X}$, τότε (σύμφωνα με το 1.3.12 (i)) υπάρχει κάποιο $x \in B$. Χρησιμοποιώντας την προηγηθείσα επιχειρηματολογία (όταν δείχναμε τον εγκλεισμό "$\subseteq$") καταλήγουμε στο ότι $B = [x]_{\sim_{\mathfrak{X}}}$. Άρα ισχύει και ο αντίστροφος εγκλεισμός $A/\sim_{\mathfrak{X}} \supseteq \mathfrak{X}$. □

Η «ταύτιση» των σχέσεων ισοδυναμίας των οριζομένων επί ενός μη κενού συνόλου και των διαμελισμών αυτού υλοποιείται μέσω μιας κατάλληλης *αμφιρρίψεως* ως ακολούθως:

1.3.21 Θεώρημα (Αντιστοιχία μεταξύ σχέσεων ισοδυναμίας και διαμελισμών). *Έστω A ένα μη κενό σύνολο. Τότε η απεικόνιση*

$$\left\{\begin{array}{c}\text{σχέσεις ισοδυναμίας}\\ \text{οριζόμενες επί τού } A\end{array}\right\} \xrightarrow{\Phi} \left\{\begin{array}{c}\text{διαμελισμοί}\\ \text{τού } A\end{array}\right\}$$

η οριζόμενη από τον τύπο

$$\boxed{\sim \longmapsto \Phi(\sim) := A/\sim}$$

είναι μια αμφίρριψη έχουσα την απεικόνιση

$$\left\{\begin{array}{c}\text{διαμελισμοί}\\ \text{τού } A\end{array}\right\} \xrightarrow{\Psi} \left\{\begin{array}{c}\text{σχέσεις ισοδυναμίας}\\ \text{οριζόμενες επί τού } A\end{array}\right\}$$

την οριζόμενη από τον τύπο

$$\boxed{\mathfrak{X} \longmapsto \Psi(\mathfrak{X}) := \sim_{\mathfrak{X}}}$$

ως αντίστροφό της.

Απόδειξη. Σύμφωνα με το (iii) τής προτάσεως 1.2.18 αρκεί να αποδειχθεί ότι οι συνθέσεις $\Psi \circ \Phi$ και $\Phi \circ \Psi$ είναι οι ταυτοτικές απεικονίσεις. Έστω "$\sim$" *τυχούσα* σχέση ισοδυναμίας επί τού A. Τότε

$$\Psi(\Phi(\sim)) = \Psi(A/\sim) = \sim_{(A/\sim)}.$$

Θα αποδείξουμε ότι η "$\sim_{(A/\sim)}$" είναι η αρχικώς θεωρηθείσα "$\sim$" (απ' όπου έπεται ότι η $\Psi \circ \Phi$ είναι η ταυτοτική απεικόνιση). Προς τούτο είναι αρκετό να ελεγχθεί ότι για οιαδήποτε $x, y \in A$ ισχύει η αμφίπλευρη συνεπαγωγή

$$x \sim y \Longleftrightarrow x \sim_{(A/\sim)} y.$$

Εάν $x \sim y$, τότε (κατά το 1.3.14 (ii)) $[x] = [y]$, οπότε θεωρώντας ως B την κλάση ισοδυναμίας $[x] = [y] \in A/\sim$ αμφότερα τα x και y ανήκουν στο B, πράγμα που σημαίνει ότι $x \sim_{(A/\sim)} y$. Και αντιστρόφως· εάν $x \sim_{(A/\sim)} y$, τότε υπάρχει κάποιο $z \in A$, τέτοιο ώστε αμφότερα τα x και y να ανήκουν στην κλάση ισοδυναμίας του $(B :=)\ [z] \in A/\sim$. Ως εκ τούτου, $[x] = [z] = [y]$, οπότε $x \sim y$.

Εν συνεχεία θεωρούμε *τυχόντα* διαμελισμό $\mathfrak{X}$ τού A. Προφανώς,

$$\Phi(\Psi(\mathfrak{X})) = \Phi\left(\sim_{\mathfrak{X}}\right) = A/\sim_{\mathfrak{X}}.$$

Σύμφωνα με το (ii) τής προτάσεως 1.3.20 το σύνολο των κλάσεων ισοδυναμίας $A/\sim_{\mathfrak{X}}$ είναι ο αρχικώς θεωρηθείς διαμελισμός $\mathfrak{X}$ τού A. Άρα η $\Phi \circ \Psi$ είναι η ταυτοτική απεικόνιση. □

1.3.22 Ορισμός. Έστω $f : A \longrightarrow B$ μια απεικόνιση. Επί τού A ορίζουμε τη διμελή σχέση $\mathcal{R}_f \subseteq A \times A$ ως εξής:

$$\boxed{(x,y) \in \mathcal{R}_f \underset{\text{ορσ}}{\Longleftrightarrow} f(x) = f(y).}$$

Είναι άμεσος ο έλεγχος τού ότι η $\mathcal{R}_f$ είναι μια σχέση ισοδυναμίας. Λέμε, ιδιαιτέρως, ότι η $\mathcal{R}_f$ είναι **η σχέση ισοδυναμίας η επαγομένη μέσω τής** f επί τού A. Σημειωτέον ότι για κάθε $x \in A$ έχουμε

$$[x]_{\mathcal{R}_f} = \{\, y \in A \mid (x,y) \in \mathcal{R}_f \} = \{\, y \in A \mid f(x) = f(y) \} = f^{-1}(f(x)),$$

δηλαδή η κλάση ισοδυναμίας τού x ως προς την $\mathcal{R}_f$ ισούται με την ίνα τής f υπεράνω τής εικόνας $f(x)$ τού x. Κατά συνέπειαν,

$$\boxed{A/\mathcal{R}_f = \{\, f^{-1}(f(x)) \;\big|\; x \in A \}.}$$

1.3.23 Πρόταση. *Έστω A ένα μη κενό σύνολο και έστω $\varnothing \neq \mathcal{R} \subseteq A \times A$ μια σχέση ισοδυναμίας επί τού A. Τότε $\mathcal{R} = \mathcal{R}_{\pi_\mathcal{R}}$, όπου $\pi_\mathcal{R} : A \longrightarrow A/\mathcal{R}$ η φυσική επίρριψη ως προς την $\mathcal{R}$ η ορισθείσα στο εδάφιο 1.3.3.*

Απόδειξη. Εάν θεωρήσουμε τυχόντα $x, y \in A$, τότε

$$(x,y) \in \mathcal{R}_{\pi_\mathcal{R}} \Leftrightarrow \pi_\mathcal{R}(x) = \pi_\mathcal{R}(y) \Leftrightarrow [x]_\mathcal{R} = [y]_\mathcal{R} \underset{1.3.14\,\text{(ii)}}{\Longleftrightarrow} (x,y) \in \mathcal{R},$$

οπότε $\mathcal{R} = \mathcal{R}_{\pi_\mathcal{R}}$. □

1.3.24 Πρόταση. *Εάν η $\mathcal{R} \subseteq A \times A$ είναι μια σχέση ισοδυναμίας επί ενός μη κενού συνόλου A, η $\mathcal{S} \subseteq B \times B$ μια σχέση ισοδυναμίας επί ενός μη κενού συνόλου B, όπου $\mathcal{R} \neq \varnothing$, $\mathcal{S} \neq \varnothing$, και*

$$\pi_\mathcal{R} : A \longrightarrow A/\mathcal{R}, \quad \pi_\mathcal{S} : B \longrightarrow B/\mathcal{S}, \quad \pi_{\mathcal{R}\times\mathcal{S}} : A \times B \longrightarrow (A \times B)\,/\,(\mathcal{R} \times \mathcal{S})$$

οι φυσικές επιρρίψεις ως προς τις $\mathcal{R}, \mathcal{S}$ και $\mathcal{R} \times \mathcal{S}$, αντιστοίχως (βλ. 1.3.3)*, τότε*

$$\mathcal{R} \times \mathcal{S} = \mathcal{R}_{\pi_{\mathcal{R}\times\mathcal{S}}} = \mathcal{R}_{\pi_\mathcal{R} \times \pi_\mathcal{S}},$$

όπου $\pi_\mathcal{R} \times \pi_\mathcal{S}$ το καρτεσιανό γινόμενο των $\pi_\mathcal{R}$ και $\pi_\mathcal{S}$ (βλ. 1.2.21).

Απόδειξη. Εφαρμόζοντας την πρόταση 1.3.23 για την $\mathcal{R} \times \mathcal{S}$ (αντί για την ίδια την $\mathcal{R}$) λαμβάνουμε $\mathcal{R} \times \mathcal{S} = \mathcal{R}_{\pi_{\mathcal{R}\times\mathcal{S}}}$. Εξάλλου,

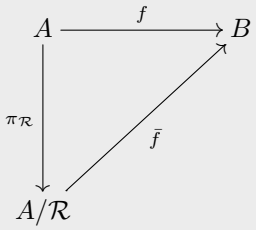
$$\begin{aligned}
&((x,x'),(y,y')) \in \mathcal{R}_{\pi_{\mathcal{R}\times\mathcal{S}}} \Leftrightarrow (\pi_\mathcal{R} \times \pi_\mathcal{S})(x,x') = (\pi_\mathcal{R} \times \pi_\mathcal{S})(y,y') \\
\Leftrightarrow\ &(\pi_\mathcal{R}(x), \pi_\mathcal{S}(x')) = (\pi_\mathcal{R}(y), \pi_\mathcal{S}(y')) \Leftrightarrow \pi_\mathcal{R}(x) = \pi_\mathcal{R}(y) \ \text{ και } \ \pi_\mathcal{S}(x') = \pi_\mathcal{S}(y') \\
\Leftrightarrow\ &[x]_\mathcal{R} = [y]_\mathcal{R} \ \text{ και } \ [x']_\mathcal{S} = [y']_\mathcal{S} \underset{1.3.14\,\text{(ii)}}{\Longleftrightarrow} (x,y) \in \mathcal{R} \ \text{ και } \ (x',y') \in \mathcal{S} \\
\Leftrightarrow\ &((x,x'),(y,y')) \in \mathcal{R} \times \mathcal{S},
\end{aligned}$$

οπότε $\mathcal{R} \times \mathcal{S} = \mathcal{R}_{\pi_\mathcal{R} \times \pi_\mathcal{S}}$. □

1.3.25 Θεώρημα (Θεμελιώδες θεώρημα περί συνόλων κλάσεων ισοδυναμίας). *Έστω $f : A \longrightarrow B$ μια απεικόνιση και έστω $\varnothing \neq \mathcal{R} \subseteq A \times A$ μια σχέση ισοδυναμίας επί τού A. Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*[14]:

(i) $\mathcal{R} \subseteq \mathcal{R}_f$.

(ii) *Υφίσταται μια απεικόνιση $\bar{f} : A/\mathcal{R} \longrightarrow B$, τέτοια ώστε $f = \bar{f} \circ \pi_{\mathcal{R}}$, δηλαδή τέτοια ώστε το διάγραμμα*



να καθίσταται μεταθετικό. Επιπροσθέτως, εάν πληρούνται οι (i), (ii), *τότε ισχύουν τα εξής*:

(a) *Η $\bar{f}$ είναι η μοναδική απεικόνιση με την ανωτέρω περιγραφείσα ιδιότητα.*

(b) $\mathrm{Im}(f) = \mathrm{Im}(\bar{f})$. *(Ως εκ τούτου, η $\bar{f}$ είναι επιρριπτική εάν και μόνον εάν η f είναι επιρριπτική.)*

(c) *Η $\bar{f}$ είναι ενριπτική εάν και μόνον εάν $\mathcal{R} = \mathcal{R}_f$.*

Απόδειξη. (i)⇒(ii): Ορίζουμε την $\bar{f} : A/\mathcal{R} \longrightarrow B$ μέσω τού τύπου

$$\bar{f}([x]_{\mathcal{R}}) := f(x),\ \forall x \in A.$$

Επειδή το σύνολο $[x]_{\mathcal{R}}$ δεν είναι μονοσημάντως ορισμένο από το x οφείλουμε εν πρώτοις να αποδείξουμε ότι η $\bar{f}$ είναι *καλώς ορισμένη*, ήτοι ότι για κάθε $x, y \in A$ ισχύει η συνεπαγωγή $[x]_{\mathcal{R}} = [y]_{\mathcal{R}} \Longrightarrow \bar{f}([x]_{\mathcal{R}}) = \bar{f}([y]_{\mathcal{R}})$. Ας υποθέσουμε λοιπόν ότι $x, y \in A$ με $[x]_{\mathcal{R}} = [y]_{\mathcal{R}}$. Τότε

$$\left.\begin{array}{c} [x]_{\mathcal{R}} = [y]_{\mathcal{R}} \underset{\text{1.3.14 (ii)}}{\Longrightarrow} (x,y) \in \mathcal{R} \\ \mathcal{R} \subseteq \mathcal{R}_f \ \ (\text{εξ υποθέσεως}) \end{array}\right\} \Rightarrow (x,y) \in \mathcal{R}_f,$$

απ' όπου έπεται ότι $f(x) = f(y)$, ήτοι ότι ισχύει η ισότητα $\bar{f}([x]_{\mathcal{R}}) = \bar{f}([y]_{\mathcal{R}})$. Εξάλλου,

$$\bar{f}(\pi_{\mathcal{R}}(x)) = \bar{f}([x]_{\mathcal{R}}) = f(x),\ \forall x \in A \Rightarrow f = \bar{f} \circ \pi_{\mathcal{R}}.$$

(ii)⇒(i): Εάν υφίσταται μια απεικόνιση $\bar{f} : A/\mathcal{R} \longrightarrow B$ με $f = \bar{f} \circ \pi_{\mathcal{R}}$, τότε για οιαδήποτε $x, y \in A$ ισχύουν οι συνεπαγωγές

$$\begin{aligned} (x,y) \ \in \ & \mathcal{R} \underset{\text{1.3.14 (ii)}}{\Longrightarrow} \pi_{\mathcal{R}}(x) = [x]_{\mathcal{R}} = [y]_{\mathcal{R}} = \pi_{\mathcal{R}}(y) \\ \Rightarrow \ & f(x) = \bar{f}(\pi_{\mathcal{R}}(x)) = \bar{f}(\pi_{\mathcal{R}}(y)) = f(y) \Rightarrow (x,y) \in \mathcal{R}_f, \end{aligned}$$

οπότε $\mathcal{R} \subseteq \mathcal{R}_f$. Εν συνεχεία υποθέτουμε ότι οι (i), (ii) πληρούνται.

(a) Έστω $g : A/\mathcal{R} \longrightarrow B$ μια απεικόνιση, τέτοια ώστε $f = g \circ \pi_{\mathcal{R}}$. Τότε

$$g([x]_{\mathcal{R}}) = g(\pi_{\mathcal{R}}(x)) = f(x) = \bar{f}([x]_{\mathcal{R}}),\ \forall x \in A \Rightarrow g = \bar{f}.$$

(b) Επειδή η $\pi_{\mathcal{R}}$ είναι επιρριπτική απεικόνιση, έχουμε

$$\mathrm{Im}(f) = (\bar{f} \circ \pi_{\mathcal{R}})(A) = \bar{f}(\pi_{\mathcal{R}}(A)) = \bar{f}(A/\mathcal{R}) = \mathrm{Im}(\bar{f}).$$

[14] Όταν η f πληροί τη συνθήκη (i), τότε η f καλείται **$\mathcal{R}$-ισομεταβλητή απεικόνιση**.

(c) Ας υποθέσουμε ότι η $\bar{f}$ είναι ενριπτική. Επειδή $\mathcal{R} \subseteq \mathcal{R}_f$, αρκεί να αποδείξουμε ότι $\mathcal{R}_f \subseteq \mathcal{R}$. Προς τούτο θεωρούμε $x, y \in A$, τέτοια ώστε $(x, y) \in \mathcal{R}_f$. Προφανώς,

$$\left.\begin{array}{r} f(x) = f(y) \Rightarrow \bar{f}([x]_{\mathcal{R}}) = \bar{f}([y]_{\mathcal{R}}) \\ \bar{f} \text{ ενριπτική (εξ υποθέσεως)} \end{array}\right\} \Rightarrow [x]_{\mathcal{R}} = [y]_{\mathcal{R}} \underset{1.3.14\,\text{(ii)}}{\Longrightarrow} (x, y) \in \mathcal{R},$$

απ' όπου προκύπτει ότι $\mathcal{R}_f \subseteq \mathcal{R}$. Άρα $\mathcal{R} = \mathcal{R}_f$. Και αντιστρόφως· εάν $\mathcal{R} = \mathcal{R}_f$ και $x, y \in A$, τέτοια ώστε $\bar{f}([x]_{\mathcal{R}}) = \bar{f}([y]_{\mathcal{R}})$, παρατηρούμε ότι

$$\left.\begin{array}{r} f(x) = f(y) \Rightarrow (x, y) \in \mathcal{R}_f \\ \mathcal{R} = \mathcal{R}_f \text{ (εξ υποθέσεως)} \end{array}\right\} \Rightarrow (x, y) \in \mathcal{R} \underset{1.3.14\,\text{(ii)}}{\Longrightarrow} [x]_{\mathcal{R}} = [y]_{\mathcal{R}}.$$

Κατά συνέπειαν, η $\bar{f}$ είναι ενριπτική. □

1.3.26 Πόρισμα (Αμφίρριψη επαγόμενη από τυχούσα απεικόνιση). *Έστω $f : A \longrightarrow B$ μια απεικόνιση. Τότε η απεικόνιση*

$$\boxed{\hat{f} : A/\mathcal{R}_f \longrightarrow \mathrm{Im}(f)}$$

η οριζόμενη από τον τύπο

$$\boxed{\hat{f}([x]_{\mathcal{R}_f}) := f(x), \ \ \forall x \in A,}$$

είναι αμφιρριπτική.

Απόδειξη. Εφαρμόζοντας το θεώρημα 1.3.25 για την $\mathcal{R} = \mathcal{R}_f$ αποκτούμε την ενριπτική απεικόνιση

$$\bar{f} : A/\mathcal{R}_f \longrightarrow B, \ \ [x]_{\mathcal{R}_f} \longmapsto \bar{f}([x]_{\mathcal{R}_f}) := f(x),$$

με $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f)$. Αρκεί λοιπόν να ορίσουμε την $\hat{f}$ ως την $\bar{f}$ ύστερα από περιορισμό τού πεδίου τιμών της B στο σύνολο $\mathrm{Im}(f) \subseteq B$. □

1.3.27 Πόρισμα (Φυσική «παραγοντοποίηση» απεικονίσεων). *Κάθε απεικόνιση $f : A \longrightarrow B$ γράφεται ως σύνθεση τριών απεικονίσεων*

$$\boxed{f = (\mathrm{id}_B|_{\mathrm{Im}(f)}) \circ \hat{f} \circ \pi_{\mathcal{R}_f},}$$

τής επιρρίψεως $\pi_{\mathcal{R}_f}$, τής αμφιρρίψεως $\hat{f}$ και τής ενρίψεως $\mathrm{id}_B|_{\mathrm{Im}(f)}$.

Απόδειξη. Εφαρμόζοντας το πόρισμα 1.3.26 κατασκευάζουμε την $\hat{f}$ και καταλήγουμε στο εξής διάγραμμα απεικονίσεων:

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & B \\ {\scriptstyle \pi_{\mathcal{R}_f}}\downarrow & & \uparrow{\scriptstyle \mathrm{id}_B|_{\mathrm{Im}(f)}} \\ A/\mathcal{R}_f & \xrightarrow[\ \hat{f}\ ]{} & \mathrm{Im}(f) \end{array}$$

Αυτό είναι μεταθετικό, διότι

$$\mathrm{id}_B|_{\mathrm{Im}(f)}\left(\hat{f}\left(\pi_{\mathcal{R}_f}(x)\right)\right) = \mathrm{id}_B|_{\mathrm{Im}(f)}\left(\hat{f}([x]_{\mathcal{R}_f})\right) = \mathrm{id}_B|_{\mathrm{Im}(f)}\left(f(x)\right) = f(x)$$

για κάθε $x \in A$. □

1.3.28 Πόρισμα (Αμφίρριψη για καρτεσιανά γινόμενα σχέσεων ισοδυναμίας). *Έστω ότι τα A, B είναι δυο μη κενά σύνολα. Εάν η $\mathcal{R} \subseteq A \times A$ είναι μια σχέση ισοδυναμίας επί τού A, η $\mathcal{S} \subseteq B \times B$ μια σχέση ισοδυναμίας επί τού B και $\mathcal{R} \neq \varnothing$, $\mathcal{S} \neq \varnothing$, τότε η*

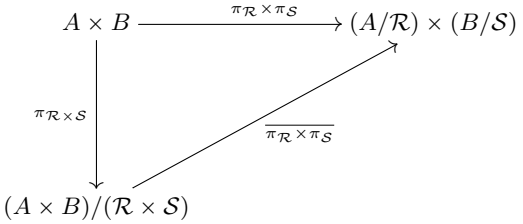
$$\boxed{\begin{array}{c}(A \times B)\,/\,(\mathcal{R} \times \mathcal{S}) \longrightarrow (A/\mathcal{R}) \times (B/\mathcal{S}) \\ [(x,y)]_{\mathcal{R}\times\mathcal{S}} \longmapsto ([x]_{\mathcal{R}}\,, [(y)]_{\mathcal{S}})\end{array}} \tag{1.13}$$

είναι μια (καλώς ορισμένη) απεικόνιση, η οποία είναι αμφίρριψη.

Απόδειξη. Κατά την πρόταση 1.3.24, $\mathcal{R} \times \mathcal{S} = \mathcal{R}_{\pi_{\mathcal{R}} \times \pi_{\mathcal{S}}}$. Εφαρμόζουμε το (i)⇒(ii) τού θεωρήματος 1.3.25 για την απεικόνιση

$$\pi_{\mathcal{R}} \times \pi_{\mathcal{S}} : A \times B \longrightarrow (A/\mathcal{R}) \times (B/\mathcal{S})\,.$$

Κατ' αυτόν τον τρόπο σχηματίζεται το μεταθετικό διάγραμμα:



όπου η $\overline{\pi_{\mathcal{R}} \times \pi_{\mathcal{S}}}$ είναι *ενριπτική* (λόγω τού 1.3.25 (c)). Σημειωτέον ότι για οιοδήποτε διατεταγμένο ζεύγος $(x, y) \in A \times B$ έχουμε

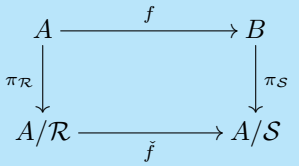
$$\overline{\pi_{\mathcal{R}} \times \pi_{\mathcal{S}}}([(x,y)]_{\mathcal{R}\times\mathcal{S}}) := (\pi_{\mathcal{R}} \times \pi_{\mathcal{S}})\,(x,y) = ([x]_{\mathcal{R}}\,, [(y)]_{\mathcal{S}})\,,$$

οπότε η (1.13) είναι η απεικόνιση $\overline{\pi_{\mathcal{R}} \times \pi_{\mathcal{S}}}$. Επιπροσθέτως, επειδή η απεικόνιση $\pi_{\mathcal{R}} \times \pi_{\mathcal{S}}$ είναι επιρριπτική (βλ. 1.2.22 (iii)), η $\overline{\pi_{\mathcal{R}} \times \pi_{\mathcal{S}}}$ είναι ωσαύτως *επιρριπτική* (βλ. 1.3.25 (b)). □

1.3.29 Πόρισμα (Επαγόμενη απεικόνιση σε επίπεδο συνόλων ισοδυναμίας). *Έστω $f : A \longrightarrow B$ μια απεικόνιση. Εάν η $\mathcal{R} \subseteq A \times A$ είναι μια σχέση ισοδυναμίας επί τού A, η $\mathcal{S} \subseteq B \times B$ μια σχέση ισοδυναμίας επί τού B και $\mathcal{R} \neq \varnothing$, $\mathcal{S} \neq \varnothing$, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) $\mathcal{R} \subseteq \mathcal{R}_{\pi_{\mathcal{S}} \circ f}$.

(ii) *Μέσω τής f επάγεται μια απεικόνιση $\check{f} : A/\mathcal{R} \longrightarrow B/\mathcal{S}$ η οποία καθιστά το διάγραμμα*



μεταθετικό, όπου οι

$$\pi_{\mathcal{R}} : A \longrightarrow A/\mathcal{R},\ \ x \longmapsto \pi_{\mathcal{R}}\,(x) := [x]_{\mathcal{R}}\,,\ \ \pi_{\mathcal{S}} : B \longrightarrow B/\mathcal{S},\ \ y \longmapsto \pi_{\mathcal{S}}\,(y) := [y]_{\mathcal{S}}\,,$$

παριστούν τις φυσικές επιρρίψεις ως προς τις $\mathcal{R}$ και $\mathcal{S}$, αντιστοίχως (βλ. 1.3.3). *Επιπροσθέτως, εάν πληρούνται οι* (i), (ii), *τότε ισχύουν τα εξής*:

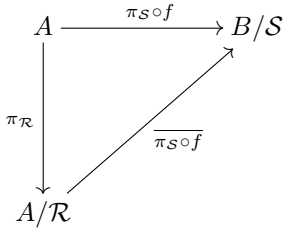
(a) *H $\check{f}$ είναι η μοναδική απεικόνιση με την ανωτέρω περιγραφείσα ιδιότητα.*

(b) $\mathrm{Im}(\pi_{\mathcal{S}} \circ f) = \mathrm{Im}(\check{f})$. *(Ως εκ τούτου, η $\check{f}$ είναι επιρριπτική εάν και μόνον εάν η*

$\pi_{\mathcal{S}} \circ f$ είναι επιριπτική).

(c) *$H\ \bar{f}$ είναι ενριπτική εάν και μόνον εάν $\mathcal{R} = \mathcal{R}_{\pi_{\mathcal{S}} \circ f}$.*

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμόσουμε την ισοδυναμία των συνθηκών (i) και (ii), καθώς και τα (a), (b), (c) (όταν αυτές πληρούνται), τού θεωρήματος 1.3.25 για τη σύνθεση $\pi_{\mathcal{S}} \circ f : A \longrightarrow B/\mathcal{S}$ (*αντί για την ίδια την* f). Προϋποτιθέμενης τής ισχύος τής (i) προκύπτει το μεταθετικό διάγραμμα:



Θέτουμε $\check{f} := \overline{\pi_{\mathcal{S}} \circ f} : A/\mathcal{R} \longrightarrow B/\mathcal{S}$ για την οποία ισχύει

$$\boxed{\check{f}([x]_{\mathcal{R}}) := \overline{\pi_{\mathcal{S}} \circ f}([x]_{\mathcal{R}}) = \pi_{\mathcal{S}}(f(x)) = [f(x)]_{\mathcal{S}}\,,\ \forall x \in A.}$$

Προφανώς, εκ κατασκευής, $\pi_{\mathcal{S}} \circ f = \check{f} \circ \pi_{\mathcal{R}}$. □

1.4 ΣΧΕΣΕΙΣ ΔΙΑΤΑΞΕΩΣ ΚΑΙ ΣΥΝΔΕΣΜΟΙ

1.4.1 Ορισμός. Έστω A ένα μη κενό σύνολο. Μια διμελής σχέση $\mathcal{R} \subseteq A \times A$ λέγεται **σχέση μερικής διατάξεως** (ή απλώς **μερική διάταξη**) επί τού A όταν η $\mathcal{R}$ είναι ανακλαστική, αντισυμμετρική και μεταβατική (βλ. 1.3.1). Σε αυτήν την περίπτωση το ζεύγος $(A, \mathcal{R})$ ονομάζεται **μερικώς διατεταγμένο σύνολο**. Συνήθως, αντί τού $\mathcal{R}$, μια σχέση μερικής διατάξεως αναπαριστάται μέσω τού συμβολισμού "$\preceq$". (Επίσης, χρησιμοποιείται συχνά και ο συμβολισμός «$\prec$» μεταξύ στοιχείων τού A, όπου $x \prec y$ αποτελεί συντομογραφία τού ($x \preceq y$ και $x \neq y$)). Ένα μερικώς διατεταγμένο σύνολο $(A, \preceq)$ λέγεται **ολικώς** (ή **γραμμικώς**) **διατεταγμένο σύνολο** (και η "$\preceq$" **σχέση ολικής διατάξεως**) όταν όλα τα στοιχεία τού A είναι μεταξύ τους ανά δύο *συγκρίσιμα*, δηλαδή όταν $(\forall x, y \in A)\ \ [x \preceq y \ \text{ ή } \ y \preceq x]$.

1.4.2 Παραδείγματα. (i) Έστω Ω ένα σύνολο. Ορίζοντας επί τού δυναμοσυνόλου του $\mathfrak{P}(\Omega)$ τη σχέση $A \preceq B \underset{\text{ορσ}}{\Longleftrightarrow} A \subseteq B,\ \ \forall\, (A, B) \in \mathfrak{P}(\Omega)^2$, διαπιστώνουμε ότι το $(\mathfrak{P}(\Omega), \preceq)$ είναι ένα μερικώς διατεταγμένο σύνολο. Σημειωτέον ότι το $(\mathfrak{P}(\Omega), \preceq)$ δεν είναι εν γένει ολικώς διατεταγμένο.

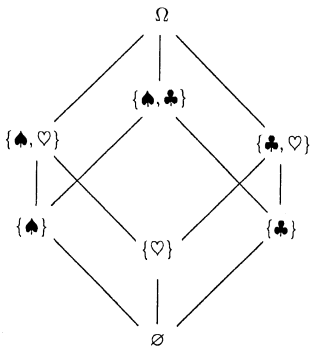
(ii) Όχι μόνον το δυναμοσύνολο ενός δοθέντος συνόλου, αλλά -γενικότερα- *κάθε* σύνολο με *σύνολα* ως στοιχεία του καθίσταται μερικώς διατεταγμένο ως προς τη σχέση εγκλεισμού "$\subseteq$".

1.4.3 Ορισμός. Έστω $(A, \preceq)$ ένα μερικώς διατεταγμένο σύνολο. Εάν υποτεθεί ότι $(x, y) \in A \times A$ με $x \prec y$, τότε το x λέγεται **προηγούμενο τού** y και το y **επόμενο τού** x (ως προς την "$\preceq$"). Εν τοιαύτη περιπτώσει το y λέγεται, ιδιαιτέρως, **αμέσως επόμενο τού** x και το x **αμέσως προηγούμενο τού** y (ως προς την "$\preceq$") όταν

$$\nexists z \in A : x \prec z \prec y.$$

1.4.4 Ορισμός. Έστω $(A, \preceq)$ ένα μερικώς διατεταγμένο σύνολο. Όταν το A είναι πεπερασμένο, τότε είθισται να «οπτικοποιούμε» τον τρόπο διατάξεως των στοιχείων του μέσω ενός ειδικού διαγράμματος, τού λεγομένου **διαγράμματος τού Hasse**[15] **για το** $(A, \preceq)$. Αυτό κατασκευάζεται ως ακολούθως: Όλα τα στοιχεία τού A τοποθετούνται στο επίπεδο σχεδιάσεως και για κάθε ζεύγος $(x, y) \in A \times A$, όπου το y είναι αμέσως επόμενο τού x (ως προς την "$\preceq$"), τα x και y συνδέονται με ένα ευθύγραμμο τμήμα, ενώ το y τίθεται *υψηλότερα* τού x. Κατ' αυτόν τον τρόπο, για κάθε ζεύγος $(z, w) \in A \times A$, όπου το w είναι επόμενο τού z (ως προς την "$\preceq$"), τα z και w συνδέονται εντός τού διαγράμματος μέσω διαδοχικών ευθυγράμμων τμημάτων.

1.4.5 Παράδειγμα. Εάν $\Omega := \{\spadesuit, \clubsuit, \heartsuit\}$, τότε το διάγραμμα τού Hasse για το $(\mathfrak{P}(\Omega), \subseteq)$ είναι το



1.4.6 Ορισμός. Έστω ότι τα $(A_1, \preceq_1)$ και $(A_2, \preceq_2)$ είναι δυο μερικώς διατεταγμένα σύνολα. Λέμε ότι μια απεικόνιση $f : A_1 \longrightarrow A_2$ είναι **ισότονη** (ή ότι *διατηρεί* τις μερικές διατάξεις αυτών) όταν για οιαδήποτε $x, y \in A_1$ ισχύει η συνεπαγωγή

$$x \preceq_1 y \Longrightarrow f(x) \preceq_2 f(y),$$

και ότι είναι **αντίτονη** (ή ότι *αντιστρέφει* τις μερικές διατάξεις αυτών) όταν για οιαδήποτε $x, y \in A_1$ ισχύει η συνεπαγωγή

$$x \preceq_1 y \Longrightarrow f(y) \preceq_2 f(x).$$

1.4.7 Παραδείγματα. Έστω Ω ένα σύνολο και έστω $X \in \mathfrak{P}(\Omega)$. Θεωρούμε το μερικώς διατεταγμένο σύνολο $(\mathfrak{P}(\Omega), \subseteq)$. Η απεικόνιση

$$f : \mathfrak{P}(\Omega) \longrightarrow \mathfrak{P}(\Omega), \quad A \longmapsto f(A) := A \cap X,$$

είναι ισότονη, ενώ η $f : \mathfrak{P}(\Omega) \longrightarrow \mathfrak{P}(\Omega), \quad A \longmapsto f(A) := \Omega \smallsetminus A$, είναι αντίτονη.

1.4.8 Ορισμός. Έστω ότι τα $(A_1, \preceq_1)$ και $(A_2, \preceq_2)$ είναι δυο μερικώς διατεταγμένα σύνολα. Μια *ισότονη αμφίρριψη* $f : A_1 \longrightarrow A_2$ έχουσα *ισότονη αντίστροφο* καλείται **ισομορφισμός μερικώς διατεταγμένων συνόλων**. Λέμε ότι δυο μερικώς διατεταγμένα σύνολα $(A_1, \preceq_1)$ και $(A_2, \preceq_2)$ είναι **ισόμορφα** όταν υφίσταται ένας τέτοιος ισομορφισμός μεταξύ αυτών.

[15] Προς τιμήν τού Γερμανού μαθηματικού Helmut Hasse (1898-1979) ο οποίος εισήγαγε και χρησιμοποίησε αυτά τα διαγράμματα.

1.4.9 Ορισμός. Έστω $(A, \preceq)$ ένα μερικώς διατεταγμένο σύνολο.

(i) Ένα στοιχείο $x \in A$ καλείται **μεγιστικό** (ή **μεγιστοτικό**) **στοιχείο** τού A (ως προς την "$\preceq$") όταν δεν είναι προηγούμενο κανενός στοιχείου τού A, ήτοι όταν για κάθε στοιχείο $y \in A$ για το οποίο ισχύει $x \preceq y$ έχουμε $x = y$.

(ii) Ένα στοιχείο $x \in A$ καλείται **ελαχιστικό** (ή **ελαχιστοτικό**) **στοιχείο** τού A (ως προς την "$\preceq$") όταν δεν είναι επόμενο κανενός στοιχείου τού A, ήτοι όταν για κάθε στοιχείο $y \in A$ για το οποίο ισχύει $y \preceq x$ έχουμε $x = y$.

1.4.10 Ορισμός. Έστω $(A, \preceq)$ ένα μερικώς διατεταγμένο σύνολο.

(i) Ένα στοιχείο $x \in A$ καλείται **μέγιστο στοιχείο** τού A (ως προς την "$\preceq$") όταν

$$y \preceq x, \ \ \forall y \in A.$$

(ii) Ένα στοιχείο $x \in A$ καλείται **ελάχιστο στοιχείο** τού A (ως προς την "$\preceq$") όταν

$$x \preceq y, \ \ \forall y \in A.$$

1.4.11 Παράδειγμα. Το $\mathfrak{P}(\Omega) \setminus \{\Omega, \varnothing\}$, όπου $\Omega := \{1, 2, 3, 4, 5\}$, δεν διαθέτει ούτε μέγιστο ούτε ελάχιστο στοιχείο (ως προς τη σχέση εγκλεισμού "$\subseteq$").

1.4.12 Πρόταση. *Ένα μερικώς διατεταγμένο σύνολο $(A, \preceq)$ διαθέτει το πολύ ένα μέγιστο και το πολύ ένα ελάχιστο στοιχείο. Δηλαδή όταν υπάρχει μέγιστο (και αντιστοίχως, ελάχιστο) στοιχείο τού $(A, \preceq)$, τότε αυτό είναι μονοσημάντως ορισμένο.* (Αυτό είθισται να συμβολίζεται ως $\max_{\preceq}(A)$ (και αντιστοίχως, ως $\min_{\preceq}(A)$) ή απλώς ως $\max(A)$ (και αντιστοίχως, ως $\min(A)$) όταν υπονοείται ποια είναι η "$\preceq$".)

Απόδειξη. Εάν ένα μερικώς διατεταγμένο σύνολο $(A, \preceq)$ διέθετε τα $x, x' \in A$ ως μέγιστα στοιχεία του, τότε $x = x'$. Πράγματι· εξ ορισμού, $y \preceq x$ για κάθε $y \in A$ και $y \preceq x'$ για κάθε $y \in A$. Εφαρμόζοντας την πρώτη εξ αυτών των συνθηκών για $y = x'$ και τη δεύτερη για $y = x$ λαμβάνουμε $x' \preceq x$ και $x \preceq x'$. Μέσω τής αντισυμμετρικής ιδιότητας τής "$\preceq$" συνάγεται ότι $x = x'$. Η απόδειξη τής μοναδικότητας τού ελαχίστου στοιχείου (όταν αυτό υπάρχει) είναι πανομοιότυπη. □

1.4.13 Παρατήρηση. (i) Εάν ένα μερικώς διατεταγμένο σύνολο $(A, \preceq)$ διαθέτει μέγιστο (και αντιστοίχως, ελάχιστο) στοιχείο, τότε αυτό είναι προφανώς *το μοναδικό* μεγιστικό (και αντιστοίχως, *το μοναδικό* ελαχιστικό) στοιχείο του (ως προς την "$\preceq$"). Όμως ένα μεγιστικό (και αντιστοίχως, ένα ελαχιστικό) στοιχείο δεν είναι κατ' ανάγκην μέγιστο (και αντιστοίχως, ελάχιστο) στοιχείο.

(ii) Προφανώς, κάθε *ολικώς* διατεταγμένο *πεπερασμένο* σύνολο διαθέτει πάντοτε *και* μέγιστο *και* ελάχιστο στοιχείο. Ωστόσο, ένα ολικώς διατεταγμένο σύνολο που διαθέτει *και* μέγιστο *και* ελάχιστο στοιχείο δεν είναι απαραιτήτως πεπερασμένο. Επίσης, σε *ολικώς* διατεταγμένα σύνολα οι έννοιες μεγιστικό και μέγιστο στοιχείο (και αντιστοίχως, οι έννοιες ελαχιστικό και ελάχιστο στοιχείο) συμπίπτουν.

1.4.14 Ορισμός. Έστω ότι το $(A, \preceq)$ είναι ένα μερικώς διατεταγμένο σύνολο και το $\mathfrak{Y}$ ένα μη κενό υποσύνολο τού A.

(i) Ένα στοιχείο $x \in A$ καλείται **άνω φράγμα** τού $\mathfrak{Y}$ εντός τού A ως προς την "$\preceq$" όταν $y \preceq x, \forall y \in \mathfrak{Y}$.

(ii) Ένα στοιχείο $x \in A$ καλείται **κάτω φράγμα** τού $\mathfrak{Y}$ εντός τού A ως προς την

"$\preceq$" όταν $x \preceq y, \forall y \in \mathfrak{Y}$. Ως

$$\text{ΑΦ}(\mathfrak{Y}; A) := \{x \in A |\, x \text{ άνω φράγμα τού } \mathfrak{Y} \text{ (εντός τού } A) \text{ ως προς την " } \preceq \text{ "}\}$$

συμβολίζουμε το σύνολο των άνω φραγμάτων τού $\mathfrak{Y}$ και ως

$$\text{ΚΦ}(\mathfrak{Y}; A) := \{x \in A |\, x \text{ κάτω φράγμα τού } \mathfrak{Y} \text{ (εντός τού } A) \text{ ως προς την " } \preceq \text{ "}\}$$

το σύνολο των κάτω φραγμάτων τού $\mathfrak{Y}$ ως προς την "$\preceq$". Όταν $\text{ΑΦ}(\mathfrak{Y}; A) \neq \varnothing$ (και αντιστοίχως, $\text{ΚΦ}(\mathfrak{Y}; A) \neq \varnothing$), τότε λέμε ότι το $\mathfrak{Y}$ είναι **φραγμένο εκ των άνω** (και αντιστοίχως, **φραγμένο εκ των κάτω**).

(iii) Εάν το μερικώς διατεταγμένο σύνολο $(\text{ΑΦ}(\mathfrak{Y}; A), \preceq|_{\text{ΑΦ}(\mathfrak{Y};A)})$ έχει ελάχιστο στοιχείο, τότε αυτό καλείται **ελάχιστο άνω φράγμα** (ή **supremum**) **τού** $\mathfrak{Y}$ εντός τού A.

(iv) Εάν το μερικώς διατεταγμένο σύνολο $(\text{ΚΦ}(\mathfrak{Y}; A), \preceq|_{\text{ΚΦ}(\mathfrak{Y};A)})$ έχει μέγιστο στοιχείο, τότε αυτό καλείται **μέγιστο κάτω φράγμα** (ή **infimum**) **τού** $\mathfrak{Y}$ εντός τού A.

1.4.15 Πρόταση. *Έστω $(A, \preceq)$ ένα μερικώς διατεταγμένο σύνολο και έστω $\mathfrak{Y}$ ένα μη κενό υποσύνολο τού A. Όταν υπάρχει ελάχιστο άνω φράγμα (και αντιστοίχως, μέγιστο κάτω φράγμα) τού $\mathfrak{Y}$ εντός τού A ως προς την "$\preceq$", τότε αυτό είναι μονοσημάντως ορισμένο* (Αυτό είθισται να συμβολίζεται ως $\sup_{\preceq}(\mathfrak{Y}; A)$ (και αντιστοίχως, ως $\inf_{\preceq}(\mathfrak{Y}; A)$) ή απλώς ως $\sup(\mathfrak{Y}; A)$ (και αντιστοίχως, ως $\inf(\mathfrak{Y}; A)$) όταν υπονοείται ποια είναι η "$\preceq$".).

ΑΠΟΔΕΙΞΗ. Αυτή έπεται άμεσα από την πρόταση 1.4.12. □

1.4.16 Ορισμός. Έστω $(A, \preceq)$ ένα μερικώς διατεταγμένο σύνολο.

(i) Κάθε υποσύνολο B τού A το οποίο είναι ολικώς διατεταγμένο ως προς την[16] "$\preceq$" καλείται **αλυσίδα** τού $(A, \preceq)$.

(ii) Το $(A, \preceq)$ λέγεται **επαγωγικώς διατεταγμένο** όταν κάθε αλυσίδα του διαθέτει ένα άνω φράγμα (εντός τού A) ως προς την "$\preceq$".

1.4.17 Παράδειγμα. Το $(\mathfrak{P}(\Omega), \subseteq)$, όπου Ω ένα σύνολο, δεν είναι κατ' ανάγκην επαγωγικώς διατεταγμένο. Ωστόσο, κάθε υποσύνολο τού $\mathfrak{P}(\Omega)$ τής μορφής $\{B, B', B'', ...\}$, όπου $B \subseteq B' \subseteq B'' \subseteq \cdots$, είναι επαγωγικώς διατεταγμένο (ως προς την "$\subseteq$").

Το ακόλουθο *λήμμα τού Zorn*[17] εφαρμόζεται σε μια πληθώρα αποδείξεων θεωρημάτων σχετιζομένων με την ύπαρξη μεγιστοτικών στοιχείων (ως προς δεδομένες σχέσεις διατάξεως):

1.4.18 Λήμμα τού Zorn. *Εάν το $(A, \preceq)$ είναι ένα επαγωγικώς διατεταγμένο σύνολο, τότε για οιοδήποτε $a \in A$ υπάρχει τουλάχιστον ένα μεγιστικό στοιχείο m εντός τού A, για το οποίο ισχύει $a \preceq m$.*

[16] Εννοείται ως προς τον περιορισμό τής διμελούς σχέσεως "$\preceq$" επί τού $B \times B$.

[17] Η ύπαρξη μεγιστικού στοιχείου αποδίδεται συνήθως στον Max August Zorn (1906-1993) λόγω τής εκ μέρους του δημοσιεύσεώς της σε ένα άρθρο στο περιοδικό Bulletin of A.M.S. το 1935 (με τίτλο: *A remark on method of trasfinite algebra*). Ωστόσο, αυτό το «λήμμα» (ή ισοδύναμες παραλλαγές του) ήταν χρόνια πριν γνωστό από εργασίες των μαθηματικών R.L. Moore (1882-1974) και K. Kuratowski (1896-1980).

1.4.19 Ορισμός. Έστω $(A, \leq)$ ένα μερικώς διατεταγμένο σύνολο. Το $(A, \leq)$ καλείται **καλώς διατεταγμένο** όταν κάθε μη κενό υποσύνολό του διαθέτει ελάχιστο στοιχείο ως προς την "$\leq$".

1.4.20 Πρόταση. *Κάθε καλώς διατεταγμένο σύνολο $(A, \leq)$ είναι ολικώς διατεταγμένο.*

Απόδειξη. Θεωρούμε τυχόντα στοιχεία $x, y \in A$ και θέτουμε $S := \{x, y\}$. Το S διαθέτει (εξ υποθέσεως) ελάχιστο στοιχείο ως προς την "$\leq$". Εάν αυτό το ελάχιστο στοιχείο είναι το x, τότε $x \leq y$. Κατ' αναλογίαν, εάν αυτό το ελάχιστο στοιχείο είναι το y, τότε $y \leq x$. Άρα το $(A, \leq)$ είναι ολικώς διατεταγμένο. □

Στο πλαίσιο τής Θεωρίας Συνόλων αποδεικνύεται ότι το λήμμα τού Zorn 1.4.18 είναι ισοδύναμο τού ακολούθου «αξιώματος»:

1.4.21 Αρχή τής καλής διατάξεως. *Κάθε σύνολο A μπορεί να εφοδιασθεί με κάποια μερική διάταξη "$\leq$", ούτως ώστε το $(A, \leq)$ να είναι καλώς διατεταγμένο.*

1.4.22 Ορισμός. Ένα μερικώς διατεταγμένο σύνολο $(A, \leq)$ καλείται **σύνδεσμος** όταν για οιαδήποτε στοιχεία $x, y \in A$ υπάρχει τόσον το μέγιστο κάτω φράγμα όσον και το ελάχιστο άνω φράγμα τού $\{x, y\}$ εντός τού A ως προς την "$\leq$". Τα φράγματα αυτά δηλούνται μέσω των συμβόλων $x \wedge y$ και $x \vee y$, αντιστοίχως.

1.4.23 Παραδείγματα. (i) Έστω Ω ένα σύνολο. Το μερικώς διατεταγμένο σύνολο $(\mathfrak{P}(\Omega), \subseteq)$ (βλ. 1.4.2 (i)) είναι σύνδεσμος. Μάλιστα, για οιαδήποτε $A, B \in \mathfrak{P}(\Omega)$ έχουμε $A \wedge B = A \cap B,\ A \vee B = A \cup B$.

(ii) Κάθε *ολικώς* διατεταγμένο σύνολο $(A, \leq)$ είναι αυτομάτως σύνδεσμος. Εν προκειμένω, εάν $x, y \in A$ και $x \leq y$, τότε $x \wedge y = x$ και $x \vee y = y$.

(iii) Έστω $(A, \leq)$ τυχών σύνδεσμος. Τότε το ανάστροφο μερικώς διατεταγμένο σύνολο $(A, \geq)$ είναι ωσαύτως σύνδεσμος (καθότι η "$\geq$" συνεπιφέρει την εναλλαγή των ρόλων των "$\wedge$" και "$\vee$") και καλείται **ανάστροφος τού συνδέσμου** $(A, \leq)$.

1.4.24 Σημείωση. (i) Εάν το $(A, \leq)$ είναι ένας σύνδεσμος και $x, y, z \in A$, τότε είναι εύκολο να αποδειχθεί ότι αυτός έχει τις εξής ιδιότητες:

	Ιδιότητες	**σε συμβολική γραφή**
1.	ταυτοδυναμία	$x \wedge x = x, \quad x \vee x = x$
2.	μεταθετικότητα	$x \wedge y = y \wedge x, \quad x \vee y = y \vee x$
3.	προσεταιριστικότητα	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$, $(x \vee y) \vee z = x \vee (y \vee z)$
4.	απορροφητικότητα	$x \wedge (x \vee y) = x, \ \ x \vee (x \wedge y) = x$

(ii) Κάθε πεπερασμένο υποσύνολο $\{x_1, x_2, ..., x_n\}$ τού υποκειμένου συνόλου A ενός συνδέσμου $(A, \leq)$ διαθέτει μέγιστο κάτω φράγμα

$$x_1 \wedge x_2 \wedge ... \wedge x_n := x_1 \wedge (x_2 \wedge ... \wedge x_n)$$

και ελάχιστο άνω φράγμα

$$x_1 \vee x_2 \vee ... \vee x_n := x_1 \vee (x_2 \vee ... \vee x_n)$$

εντός αυτού. (Επαγωγικός ορισμός.) Ωστόσο, όταν το A είναι απειροσύνολο, ένα άπειρο υποσύνολό του $\mathfrak{Y}$ δεν διαθέτει κατ' ανάγκην αυτά τα φράγματα.

(iii) Ένας σύνδεσμος $(A, \preceq)$ καλείται **πλήρης σύνδεσμος** όταν *κάθε* υποσύνολό του $\mathfrak{Y}$ διαθέτει μέγιστο κάτω φράγμα και ελάχιστο άνω φράγμα. (Εν τοιαύτη περιπτώσει τα φράγματα αυτά συμβολίζονται ως $\bigwedge \mathfrak{Y}$ και $\bigvee \mathfrak{Y}$, αντιστοίχως.)

1.4.25 Ορισμός. Έστω $(A, \preceq)$ ένας σύνδεσμος και έστω $\mathfrak{Y}$ ένα μη κενό υποσύνολο τού A. Τότε το μερικώς διατεταγμένο σύνολο $(\mathfrak{Y}, \preceq)$ (ή -ακριβέστερα- το $(\mathfrak{Y}, \preceq|_{\mathfrak{Y}\times\mathfrak{Y}})$) καλείται **υποσύνδεσμος τού** $(A, \preceq)$ όταν για οιαδήποτε $x, y \in \mathfrak{Y}$ έχουμε $x \wedge y \in \mathfrak{Y}$ και $x \vee y \in \mathfrak{Y}$.

1.4.26 Ορισμός. Έστω ότι τα $(A_1, \preceq_1)$ και $(A_2, \preceq_2)$ είναι δυο σύνδεσμοι. Ένας ισομορφισμός (των υποκειμένων) μερικώς διατεταγμένων συνόλων $f : A_1 \to A_2$ (υπό την έννοια τού ορισμού 1.4.8) καλείται **ισομορφισμός συνδέσμων**. Λέμε ότι δυο σύνδεσμοι $(A_1, \preceq_1)$ και $(A_2, \preceq_2)$ είναι **ισόμορφοι** όταν υφίσταται ένας τέτοιος ισομορφισμός μεταξύ αυτών.

1.4.27 Πρόταση. *Έστω ότι τα $(A_1, \preceq_1)$ και $(A_2, \preceq_2)$ είναι δυο σύνδεσμοι. Για μια αμφίρριψη $f : A_1 \longrightarrow A_2$ οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Η f είναι ισομορφισμός συνδέσμων.*

(ii) $f(x \wedge y) = f(x) \wedge f(y), \forall (x, y) \in A_1 \times A_1$.

(iii) $f(x \vee y) = f(x) \vee f(y), \forall (x, y) \in A_1 \times A_1$.

Απόδειξη. (i)⇒(ii) Εάν η f είναι ισομορφισμός συνδέσμων και $(x, y) \in A_1 \times A_1$, τότε

$$x \wedge y \preceq_1 x \text{ και } x \wedge y \preceq_1 y \Rightarrow f(x \wedge y) \preceq_2 f(x) \text{ και } f(x \wedge y) \preceq_2 f(y),$$

οπότε το $f(x \wedge y)$ αποτελεί ένα κάτω φράγμα τού $\{f(x), f(y)\}$ εντός τού A_2 ως προς την " $\preceq_2$ ". Έστω τώρα ξ *τυχόν* κάτω φράγμα τού $\{f(x), f(y)\}$ εντός τού A_2 ως προς την " $\preceq_2$ ". Επειδή η f είναι αμφιρριπτική απεικόνιση, υπάρχει ακριβώς ένα στοιχείο $z \in A_1$, τέτοιο ώστε να ισχύει $f(z) = \xi$. Προφανώς,

$$\xi \preceq_2 f(x) \text{ και } \xi \preceq_2 f(y) \Rightarrow z \preceq_1 f^{-1}(f(x)) = x \text{ και } z \preceq_1 f^{-1}(f(y)) = y,$$

οπότε το z αποτελεί ένα κάτω φράγμα τού $\{x, y\}$ εντός τού A_1 ως προς την " $\preceq_1$ ". Αυτό σημαίνει ότι $z \preceq_1 x \wedge y$, απ' όπου έπεται ότι

$$f(z) = \xi \preceq_2 f(x \wedge y) \Rightarrow f(x \wedge y) = f(x) \wedge f(y).$$

(ii)⇒(i) Για οιοδήποτε ζεύγος $(x, y) \in A_1 \times A_1$ με $x \preceq_1 y$ έχουμε $x \wedge y = x$, οπότε

$$f(x) = f(x \wedge y) = f(x) \wedge f(y) \Rightarrow f(x) \preceq_2 f(y).$$

Εξ αυτού έπεται ότι η f είναι ισότονη. Από την άλλη μεριά, για οιοδήποτε ζεύγη $(u, w) \in A_2 \times A_2$ με $u \preceq_2 w$ υπάρχουν μονοσημάντως ορισμένα $x, y \in A_1$, τέτοια ώστε να ισχύει $f(x) = u$ και $f(y) = w$. Κατά συνέπειαν,

$$f(x) = u = u \wedge w = f(x) \wedge f(y) = f(x \wedge y),$$

απ' όπου συμπεραίνουμε ότι

$$x = f^{-1}(f(x)) = f^{-1}(f(x \wedge y)) = x \wedge y \Rightarrow x \preceq_1 y,$$

ήτοι ότι $f^{-1}(u) \preceq_1 f^{-1}(w)$. Άρα και η αντίστροφος f^{-1} τής f είναι ισότονη και, ως εκ τούτου, η f είναι ισομορφισμός συνδέσμων. Η ισοδυναμία (i)⇔(iii) αποδεικνύεται παρομοίως. □

1.5 ΠΡΑΞΕΙΣ

1.5.1 Ορισμός. Δοθέντων δύο μη κενών συνόλων A και B, κάθε απεικόνιση

$$\psi : B \times A \longrightarrow A$$

ορίζει μια **πράξη** επί τού A. Όταν $A = B$, οι πράξεις χαρακτηρίζονται ως **εσωτερικές**· ειδάλλως ονομάζονται **εξωτερικές**. Ως **αλγεβρικές δομές** νοούνται σύνολα διάφορα τού κενού, τα οποία είναι εφοδιασμένα με μία τουλάχιστον (εσωτερική ή εξωτερική) πράξη[18].

Στο κεφάλαιο 3 θα μελετήσουμε τις κύριες ιδιότητες διαφόρων αλγεβρικών δομών που αποτελούνται από μη κενά σύνολα εφοδιασμένα με *μία και μόνον εσωτερική πράξη* (ομαδοειδή, ημιομάδες, μονοειδή και ομάδες). Στο κεφάλαιο 6 θα επεκτείνουμε αυτήν τη μελέτη για αλγεβρικές δομές που αποτελούνται από μη κενά σύνολα εφοδιασμένα με *δύο εσωτερικές πράξεις* (δακτυλίους, ακέραιες περιοχές και σώματα), οι οποίες συνδέονται «επιμεριστικώς». Στην παρούσα ενότητα θα προταχθούν οι ορισμοί χαρακτηριστικών εσωτερικών πράξεων που έχουν ιδιότητες συναντώμενες σε μια πληθώρα παραδειγμάτων.

1.5.2 Σημείωση. Έστω A ένα μη κενό σύνολο και έστω $\psi : A \times A \longrightarrow A$ μια εσωτερική πράξη επί τού A. Θεωρούμε τυχόν υποσύνολο $C \neq \varnothing$ τού A. Προφανώς, ο περιορισμός $\psi|_{C\times C} : C \times C \longrightarrow A$ τής ψ στο $C \times C$ (βλ. 1.2.5) ορίζει μια εσωτερική πράξη *επί τού* C (υπό την έννοια τού 1.5.1) εάν και μόνον εάν για την εικόνα $\mathrm{Im}(\psi|_{C\times C}) := \psi(C \times C)$ τού $C \times C$ μέσω τής ψ πληρούται η συνθήκη

$$\boxed{\mathrm{Im}(\psi|_{C\times C}) \subseteq C.} \tag{1.14}$$

Στην περίπτωση κατά την οποία ισχύει ο εγκλεισμός (1.14) λέμε ότι το C είναι **κλειστό ως προς την πράξη** ψ. (Αυτή η «συνθήκη τής κλειστότητας» μη κενών υποσυνόλων ως προς εσωτερικές πράξεις *προαπαιτείται* για τον ορισμό *υποδομών* των αλγεβρικών δομών που θα μελετηθούν στα κεφάλαια 3 και 6.)

1.5.3 Ορισμός. Έστω A ένα μη κενό σύνολο και έστω $\psi : A \times A \longrightarrow A$ μια εσωτερική πράξη επί τού A.

(i) Εάν για οιαδήποτε στοιχεία $x, y, z \in A$ ισχύει η ισότητα

$$\boxed{\psi(\psi(x, y), z) = \psi(x, \psi(y, z)),}$$

τότε λέμε ότι η ψ είναι **προσεταιριστική πράξη** (ή ότι η ψ έχει την **προσεταιριστική ιδιότητα**).

(ii) Εάν για οιαδήποτε στοιχεία $x, y \in A$ ισχύει η ισότητα

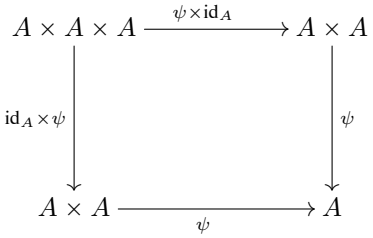
$$\boxed{\psi(x, y) = \psi(y, x),}$$

τότε λέμε ότι η ψ είναι **μεταθετική πράξη** (ή ότι η ψ έχει τη **μεταθετική ιδιότητα**).

1.5.4 Σημείωση. Η $\psi : A \times A \longrightarrow A$ είναι προσεταιριστική εάν και μόνον εάν το

[18] Επί παραδείγματι, ο αναγνώστης που έχει παρακολουθήσει παραδόσεις Γραμμικής Άλγεβρας είναι σίγουρα εξοικειωμένος με την αλγεβρική δομή τού *διανυσματικού χώρου*. Οι διανυσματικοί χώροι είναι μη κενά σύνολα εφοδιασμένα με μία εσωτερική και μία -εν γένει- εξωτερική πράξη (ήτοι την *πρόσθεση* και τον *αριθμητικό ή βαθμωτό πολλαπλασιασμό*).

ακόλουθο διάγραμμα είναι μεταθετικό:



Εν προκειμένω, υπονοείται η ταύτιση των $(A \times A) \times A$ και $A \times (A \times A)$ με το[19] $A \times A \times A$ (όπου τα στοιχεία τής μορφής $((x, y), z)$ και $(x, (y, z))$ ταυτίζονται με το (x, y, z)).

1.5.5 Παραδείγματα. Έστω Ω ένα σύνολο.

(i) Η απεικόνιση $\psi : \mathfrak{P}(\Omega) \times \mathfrak{P}(\Omega) \longrightarrow \mathfrak{P}(\Omega),\ (A, B) \longmapsto \psi(A, B) := A \cup B$, αποτελεί μια εσωτερική πράξη επί τού[20] $\mathfrak{P}(\Omega)$, η οποία είναι προσεταιριστική και μεταθετική. (Βλ. 1.1.3 (ii), (iii).)

(ii) Το ίδιο ισχύει και για την απεικόνιση

$$\psi : \mathfrak{P}(\Omega) \times \mathfrak{P}(\Omega) \longrightarrow \mathfrak{P}(\Omega),\ \ (A, B) \longmapsto \psi(A, B) := A \cap B.$$

(iii) Επί τη βάσει των (vi) και (i) τής ασκήσεως 8 τού 1ου φυλλαδίου η απεικόνιση

$$\psi : \mathfrak{P}(\Omega) \times \mathfrak{P}(\Omega) \longrightarrow \mathfrak{P}(\Omega),\ (A, B) \longmapsto \psi(A, B) := A \triangle B,$$

(όπου "$A \triangle B$" η *συμμετρική διαφορά* των A και B) είναι ωσαύτως προσεταιριστική και μεταθετική.

(iv) Η απεικόνιση $\psi : \mathfrak{P}(\Omega) \times \mathfrak{P}(\Omega) \longrightarrow \mathfrak{P}(\Omega),\ \ (A, B) \longmapsto \psi(A, B) := A \smallsetminus B$, δεν είναι (εν γένει) ούτε προσεταιριστική ούτε μεταθετική.

1.5.6 Ορισμός. Έστω A ένα μη κενό σύνολο και έστω $\psi : A \times A \longrightarrow A$ μια εσωτερική πράξη επί τού A.

(i) Ένα στοιχείο e τού A καλείται **εξ αριστερών ουδέτερο στοιχείο** τού A ως προς την πράξη ψ όταν

$$\boxed{\psi(e, a) = a,\ \forall a \in A.}$$

(ii) Ένα στοιχείο e τού A καλείται **εκ δεξιών ουδέτερο στοιχείο** τού A ως προς την πράξη ψ όταν

$$\boxed{\psi(a, e) = a,\ \forall a \in A.}$$

(iii) Ένα στοιχείο e τού A καλείται **αμφιπλεύρως ουδέτερο** ή απλώς **ουδέτερο στοιχείο** τού A ως προς την πράξη ψ όταν

$$\boxed{\psi(e, a) = a = \psi(a, e),\ \forall x \in A.}$$

1.5.7 Παράδειγμα. Εάν επί τού συνόλου $A = \{\spadesuit, \clubsuit, \heartsuit\}$ ορίσουμε την εσωτερική πράξη

$$A \times A \longrightarrow A, \quad (x, y) \longmapsto \psi(x, y) := y,$$

[19] Το $A \times A \times A$ αποτελείται από *διατεταγμένες τριάδες* (x, y, z) έχουσες στοιχεία τού A ως μέλη τους. Κατ' αναλογίαν προς ό,τι συμβαίνει με τα διατεταγμένα ζεύγη, δυο διατεταγμένες τριάδες (x, y, z) και (x', y', z') είναι ίσες εάν και μόνον εάν $x = x'$, $y = y'$ και $z = z'$.

[20] Σημειωτέον ότι το $\mathfrak{P}(\Omega)$ είναι πάντοτε μη κενό. (Εάν $\Omega = \varnothing$, τότε το $\mathfrak{P}(\Omega)$ απαρτίζεται από το *μη κενό* σύνολο $\{\varnothing\}$ που έχει το $\varnothing$ ως μοναδικό του στοιχείο!)

τότε η ψ είναι (προφανώς) μη μεταθετική αλλά είναι προσεταιριστική, διότι

$$\psi(\psi(\spadesuit,\clubsuit),\heartsuit)=\psi(\clubsuit,\heartsuit)=\heartsuit=\psi(\spadesuit,\heartsuit)=\psi(\spadesuit,\psi(\clubsuit,\heartsuit)),$$
$$\psi(\psi(\spadesuit,\heartsuit),\clubsuit)=\psi(\heartsuit,\clubsuit)=\clubsuit=\psi(\spadesuit,\clubsuit)=\psi(\spadesuit,\psi(\heartsuit,\clubsuit)),$$

και, κατ' αναλογίαν,

$$\psi(\psi(\clubsuit,\spadesuit),\heartsuit)=\psi(\clubsuit,\psi(\spadesuit,\heartsuit)),\qquad \psi(\psi(\clubsuit,\heartsuit),\spadesuit)=\psi(\clubsuit,\psi(\heartsuit,\spadesuit)),$$

$$\psi(\psi(\heartsuit,\spadesuit),\clubsuit)=\psi(\heartsuit,\psi(\spadesuit,\clubsuit)),\qquad \psi(\psi(\heartsuit,\clubsuit),\spadesuit)=\psi(\heartsuit,\psi(\clubsuit,\spadesuit)).$$

Επιπροσθέτως, *κάθε* στοιχείο τού A είναι εξ αριστερών ουδέτερο στοιχείο του ως προς αυτήν. Ωστόσο, το A δεν διαθέτει κανένα εκ δεξιών ουδέτερο στοιχείο ως προς αυτήν!

1.5.8 Πρόταση. *Έστω A ένα μη κενό σύνολο και έστω $\psi : A\times A\longrightarrow A$ μια εσωτερική πράξη επί τού A. Εάν το e είναι ένα εξ αριστερών και το e' ένα εκ δεξιών ουδέτερο στοιχείο τού A ως προς την πράξη ψ, τότε $e=e'$ (και, ως εκ τούτου, το e είναι ουδέτερο στοιχείο τού A ως προς την πράξη ψ). Κατά συνέπειαν, κάθε μη κενό σύνολο εφοδιασμένο με μια εσωτερική πράξη διαθέτει το πολύ ένα ουδέτερο στοιχείο ως προς αυτήν.*

Απόδειξη. Έχουμε $\psi(e,e')=e'$, επειδή το e είναι ένα εξ αριστερών ουδέτερο, και $\psi(e,e')=e'$, επειδή το e' είναι ένα εκ δεξιών ουδέτερο στοιχείο. Άρα τελικώς $e=e'$. Ως εκ τούτου, όταν το A διαθέτει ουδέτερο στοιχείο ως προς την ψ, τότε αυτό, όντας ουδέτερο τόσον εξ αριστερών όσον και εκ δεξιών, είναι κατ' ανάγκην μονοσημάντως ορισμένο. □

1.5.9 Παρατήρηση. Εάν η $\psi : A\times A\longrightarrow A$ είναι μια *μεταθετική* πράξη ορισμένη επί ενός μη κενού συνόλου A, τότε οι έννοιες «εξ αριστερών ουδέτερο στοιχείο», «εκ δεξιών ουδέτερο στοιχείο» και «ουδέτερο στοιχείο» τού A ως προς την ψ συμπίπτουν.

1.5.10 Παραδείγματα. Έστω Ω ένα σύνολο. Το δυναμοσύνολό του $\mathfrak{P}(\Omega)$ διαθέτει πάντοτε ουδέτερο στοιχείο ως προς τις εσωτερικές (μεταθετικές) πράξεις τις ορισθείσες επ' αυτού στα (i), (ii) και (iii) τού εδαφίου 1.5.5. Συγκεκριμένα, το ουδέτερο στοιχείο του ως προς την πράξη 1.5.5 (i) είναι το $\varnothing$ (βλ. 1.1.3 (i)), ως προς την πράξη 1.5.5 (ii) το Ω και ως προς την πράξη 1.5.5 (iii) το $\varnothing$.

1.5.11 Ορισμός. Ας υποθέσουμε ότι το A είναι ένα μη κενό σύνολο, το a ένα στοιχείο τού A, η $\psi : A\times A\longrightarrow A$ μια εσωτερική πράξη επί τού A και το e ουδέτερο στοιχείο[21] τού A ως προς την ψ.

(i) Ένα στοιχείο b τού A καλείται **εξ αριστερών συμμετρικό στοιχείο τού** a ως προς την πράξη ψ όταν

$$\boxed{\psi(b,a)=e.}$$

(ii) Ένα στοιχείο c τού A καλείται **εκ δεξιών συμμετρικό στοιχείο τού** a ως προς την πράξη ψ όταν

$$\boxed{\psi(a,c)=e.}$$

(iii) Ένα στοιχείο a' τού A καλείται **αμφιπλεύρως συμμετρικό στοιχείο** ή απλώς

συμμετρικό στοιχείο τού a ως προς την πράξη ψ όταν

$$\boxed{\psi(a', a) = e = \psi(a, a').}$$

1.5.12 Παράδειγμα. Έστω A ένα μη κενό σύνολο. Θεωρούμε το σύνολο

$$A^A = \text{ΑΠ}\,(A, A)$$

των απεικονίσεων από το A στο A (βλ. 1.2.2). Επ' αυτού ορίζουμε την εσωτερική πράξη

$$\psi : A^A \times A^A \longrightarrow A^A,\ (g, f) \longmapsto \psi(g, f) := g \circ f.$$

Η πράξη αυτή είναι προσεταιριστική αλλ' όχι κατ' ανάγκην και μεταθετική (βλ. 1.2.13 και 1.2.15). Προφανώς, η *ταυτοτική απεικόνιση* id_A (βλ. 1.2.9) αποτελεί το ουδέτερο στοιχείο τού A^A ως προς την ψ. Κατά την πρόταση 1.2.18 οι μόνες απεικονίσεις τού A^A οι οποίες διαθέτουν εξ αριστερών συμμετρικό στοιχείο ως προς την ψ είναι οι *ενριπτικές*, οι μόνες απεικονίσεις τού A^A οι οποίες διαθέτουν εκ δεξιών συμμετρικό στοιχείο ως προς την ψ είναι οι *επιριπτικές*, ενώ οι μόνες απεικονίσεις τού A^A οι οποίες διαθέτουν συμμετρικό στοιχείο ως προς την ψ είναι οι *αμφιριπτικές*.

1.5.13 Πρόταση. *Αν υποθέσουμε ότι το A είναι ένα μη κενό σύνολο, το a ένα στοιχείο τού A, η $\psi : A \times A \longrightarrow A$ μια προσεταιριστική πράξη επί τού A και το e ουδέτερο στοιχείο τού A ως προς την ψ. Εάν το a διαθέτει το a' ως εξ αριστερών συμμετρικό του και το a'' ως εκ δεξιών συμμετρικό του στοιχείο ως προς την ψ, τότε $a' = a''$. Κατά συνέπειαν, κάθε στοιχείο ενός μη κενού συνόλου εφοδιασμένου με μια προσεταιριστική πράξη διαθέτει το πολύ ένα συμμετρικό στοιχείο τού a ως προς αυτήν.*

Απόδειξη. Προφανώς,

$$\begin{aligned}
a'' &= \psi(e, a'') && \text{(διότι το } e \text{ είναι το ουδέτερο στοιχείο)}\\
&= \psi(\psi(a', a)), a'') && \text{(επειδή το } a' \text{ είναι εξ αριστερών συμμετρικό τού } a)\\
&= \psi(a', \psi(a, a'')) && \text{(διότι η πράξη } \circledcirc \text{ είναι προσεταιριστική)}\\
&= \psi(a', e) && \text{(επειδή το } a'' \text{ είναι εκ δεξιών συμμετρικό τού } a)\\
&= a'' && \text{(διότι το } e \text{ είναι το ουδέτερο στοιχείο).}
\end{aligned}$$

Ως εκ τούτου, όταν το a διαθέτει συμμετρικό στοιχείο ως προς την προσεταιριστική πράξη ψ, τότε αυτό, όντας συμμετρικό του τόσον εξ αριστερών όσον και εκ δεξιών, είναι κατ' ανάγκην μονοσημάντως ορισμένο.[21] □

1.5.14 Παρατήρηση. Εάν η $\psi : A \times A \longrightarrow A$ είναι μια *μεταθετική* πράξη ορισμένη επί ενός μη κενού συνόλου A και $a \in A$, τότε οι έννοιες «εξ αριστερών συμμετρικό στοιχείο», «εκ δεξιών συμμετρικό στοιχείο» και «συμμετρικό στοιχείο» τού a ως προς την ψ συμπίπτουν.

1.5.15 Παραδείγματα. Έστω Ω ένα σύνολο. Στο εδάφιο 1.5.10 παραθέσαμε τα ουδέτερα στοιχεία τού δυναμοσυνόλου του $\mathfrak{P}(\Omega)$ ως προς τρεις εσωτερικές (προσεταιριστικές και μεταθετικές) πράξεις ορισθείσες επ' αυτού στα (i), (ii) και (iii) τού εδαφίου 1.5.5. Είναι εύκολο να διαπιστωθεί ότι δεν υφίσταται συμμετρικό στοιχείο οιουδήποτε μη κενού συνόλου $A \in \mathfrak{P}(\Omega)$ ως προς την 1.5.5 (i), ότι δεν υφίσταται συμμετρικό στοιχείο οιουδήποτε γνησίου υποσυνόλου A τού συνόλου Ω ως προς την 1.5.5 (ii) και ότι κάθε $A \in \mathfrak{P}(\Omega)$ έχει ως (μοναδικό του) συμμετρικό στοιχείο ως προς την 1.5.5 (iii) το ίδιο το A. (Βλ. τα (i) και (iii) τής ασκ. 8 τού 1ου φυλλαδίου.)

[21] Κατά την πρόταση 1.5.8 το e είναι μονοσημάντως ορισμένο.

1.5.16 Πρόταση (Εσωτερικές πράξεις επί καρτεσιανών γινομένων). *Έστω ότι τα A και B είναι δυο μη κενά σύνολα, και ότι οι*

$$\phi : A \times A \longrightarrow A, \;\; \psi : B \times B \longrightarrow B$$

είναι εσωτερικές πράξεις επ' αυτών. Θεωρούμε την εσωτερική πράξη[22]

$$\boxed{\begin{array}{c}(\phi,\psi) : (A \times B) \times (A \times B) \longrightarrow A \times B \\ ((x,z),(y,t)) \longmapsto (\phi,\psi)\left((x,z),(y,t)\right) := \left(\phi\left(x,y\right),\psi\left(z,t\right)\right)\end{array}}$$

την οριζόμενη επί τού καρτεσιανού γινομένου $A \times B$. Τότε ισχύουν τα εξής:

(i) *Εάν οι ϕ και ψ είναι προσεταιριστικές, τότε και η (ϕ,ψ) είναι προσεταιριστική.*

(ii) *Εάν οι ϕ και ψ είναι μεταθετικές, τότε και η (ϕ,ψ) είναι μεταθετική.*

(iii) *Εάν τα e_A, e_B είναι (εξ αριστερών/εκ δεξιών/αμφιπλεύρως) ουδέτερα στοιχεία τού A και B ως προς τις πράξεις ϕ και ψ, αντιστοίχως, τότε το (e_A, e_B) είναι (εξ αριστερών/εκ δεξιών/αμφιπλεύρως) ουδέτερο στοιχείο τού $A\times B$ ως προς την πράξη (ϕ,ψ).*

(iv) *Εάν τα e_A, e_B είναι ουδέτερα στοιχεία τού A και B ως προς τις πράξεις ϕ και ψ, αντιστοίχως, και τα y' και t' (εξ αριστερών/εκ δεξιών/αμφιπλεύρως) συμμετρικά στοιχεία των $y \in A$ και $t \in B$ ως προς τις πράξεις ϕ και ψ, αντιστοίχως, τότε το (y',t') είναι (εξ αριστερών/εκ δεξιών/αμφιπλεύρως) συμμετρικό στοιχείο τού (y,t) ως προς την πράξη (ϕ,ψ).*

Απόδειξη. (i) Εάν οι ϕ και ψ είναι προσεταιριστικές, τότε για οιαδήποτε διατεταγμένα ζεύγη $(x,z),(y,t),(u,v) \in A \times B$ ισχύουν οι ισότητες

$$\begin{aligned}(\phi,\psi)\left((\phi,\psi)\left((x,z),(y,t)\right),(u,v)\right) &= (\phi,\psi)\left(\left(\phi\left(x,y\right),\psi\left(z,t\right)\right),(u,v)\right) \\ &= \left(\phi\left(\phi\left(x,y\right),u\right),\psi\left(\psi\left(z,t\right),v\right)\right) \\ &= \left(\phi(x,\phi(y,u)),\psi\left(z,\psi\left(t,v\right)\right)\right) \\ &= (\phi,\psi)\left((x,z),\left(\phi(y,u),\psi\left(t,v\right)\right)\right) \\ &= (\phi,\psi)\left((x,z),(\phi,\psi)\left((y,t),(u,v)\right)\right).\end{aligned}$$

(ii) Εάν οι ϕ και ψ είναι μεταθετικές, τότε $\forall\, ((x,z),(y,t)) \in (A \times B) \times (A \times B)$:

$$(\phi,\psi)\left((x,z),(y,t)\right) = \left(\phi\left(x,y\right),\psi\left(z,t\right)\right) = \left(\phi\left(y,x\right),\psi\left(t,z\right)\right) = (\phi,\psi)\left((y,t),(x,z)\right).$$

(iii) Εάν τα e_A, e_B είναι εξ αριστερών ουδέτερα στοιχεία τού A και B ως προς τις πράξεις ϕ και ψ, αντιστοίχως, τότε για κάθε $(y,t) \in A \times B$ έχουμε

$$(\phi,\psi)\left((e_A,e_B),(y,t)\right) = \left(\phi\left(e_A,y\right),\psi\left(e_B,t\right)\right) = (y,t),$$

οπότε το (e_A,e_B) είναι εξ αριστερών ουδέτερο στοιχείο τού $A \times B$ ως προς την πράξη (ϕ,ψ). Οι λοιπές περιπτώσεις αντιμετωπίζονται παρομοίως.

(iv) Εάν τα y' και t' είναι εξ αριστερών συμμετρικά στοιχεία των $y \in A$ και $t \in B$ ως προς τις πράξεις ϕ και ψ, αντιστοίχως, τότε

$$(\phi,\psi)\left((y',t'),(y,t)\right) = \left(\phi\left(y',y\right),\psi\left(t',t\right)\right) = (e_A,e_B).$$

Οι λοιπές περιπτώσεις αντιμετωπίζονται παρομοίως. □

[22] Σημειωτέον ότι $(\phi,\psi) = (\phi \times \psi) \circ \vartheta$, όπου $\phi \times \psi : (A \times A) \times (B \times B) \longrightarrow A \times B$ το καρτεσιανό γινόμενο των ϕ και ψ (όπως ορίσθηκε στο εδάφιο 1.2.21) και $\vartheta : (A \times B) \times (A \times B) \longrightarrow (A \times A) \times (B \times B)$ η *αμφίρριψη* η οριζόμενη από τον τύπο $\vartheta\left((x,z),(y,t)\right) := ((x,y),(z,t))$.

1.5.17 Σημείωση (Απλουστεύσεις συμβολισμών). Όταν η $\psi : A \times A \longrightarrow A$ είναι μια εσωτερική πράξη επί ενός μη κενού συνόλου A και (x, y) τυχόν στοιχείο τού $A \times A$, τότε για μια εξαπλουστευμένη αναγραφή τής εικόνας $\psi(x, y)$ τού (x, y) μέσω τής ψ χρησιμοποιούνται συνήθως διάφοροι σύντομοι συμβολισμοί, όπως π.χ. $x \star y$, $x \circledast y$, $x \circledcirc y$ κ.ά. Μια κατ' αυτόν τον τρόπο εκφραζόμενη εσωτερική πράξη, ας την πούμε "$\circledcirc$",

$$A \times A \longrightarrow A,\ (x, y) \longmapsto x \circledcirc y \tag{1.15}$$

επί τού A είναι π.χ. *προσεταιριστική* όταν

$$(x \circledcirc y) \circledcirc z = x \circledcirc (y \circledcirc z) \tag{1.16}$$

για οιαδήποτε $x, y, z \in A$, *μεταθετική* όταν[23]

$$x \circledcirc y = y \circledcirc x \tag{1.17}$$

για οιαδήποτε $x, y \in A$, κ.ο.κ.

1.5.18 Παρατήρηση. Δοθείσας μιας προσεταιριστικής πράξεως (1.15), η ισότητα (1.16) μας πληροφορεί ότι η διπλή εκτέλεση τής "$\circledcirc$" μεταξύ τριών στοιχείων x, y και z (διατηρώντας τη σειρά παραθέσεως των x, y, z αμετάβλητη) *δεν επηρεάζεται από τη μετακίνηση των παρενθέσεων*[24]. Κατά συνέπειαν, καθ' οιονδήποτε τρόπο κι αν εφαρμόσουμε την πράξη "$\circledcirc$" στα x, y, z (υπό τον όρο τής τηρήσεως τής σειράς παραθέσεως αυτών), δηλαδή καθ' οιονδήποτε τρόπο και αν σχηματίσουμε το στοιχείο

$$"x \circledcirc y \circledcirc z",$$

λαμβάνουμε πάντοτε το ίδιο αποτέλεσμα. Εδώ τίθεται το εξής ερώτημα: Εάν αντί τριών (σαφώς διατεταγμένων) στοιχείων τού A μας δοθούν τέσσερα, ας πούμε τα x, y, z, t, τότε υπάρχουν και πάλι διαφορετικοί τρόποι σχηματισμού τού

$$"x \circledcirc y \circledcirc z \circledcirc t",$$

π.χ.

$$x \circledcirc (y \circledcirc z \circledcirc t),\ (x \circledcirc y) \circledcirc (z \circledcirc t),\ (x \circledcirc y \circledcirc z) \circledcirc t,\ \ldots$$

Λαμβάνουμε, εν τοιαύτη περιπτώσει, εκ νέου το ίδιο αποτέλεσμα; Η απάντηση είναι όντως καταφατική (και μάλιστα σε πλήρη γενικότητα) και μας οδηγεί στη λεγόμενη «γενικευμένη προσεταιριστική ιδιότητα» η οποία θα αποδειχθεί στην επόμενη ενότητα (βλ. πρόταση 1.6.40).

1.5.19 Ορισμός. Έστω ότι το A είναι ένα μη κενό σύνολο, η $\varnothing \neq \mathcal{R} \subseteq A \times A$ μια σχέση ισοδυναμίας και η

$$A \times A \longrightarrow A,\ (x, y) \longmapsto x * y$$

μια εσωτερική πράξη επί τού A. Λέμε ότι η $\mathcal{R}$ είναι **συμβατή με την** "$*$" όταν για οιαδήποτε διατεταγμένα ζεύγη $(x, x'), (y, y') \in A \times A$ ισχύει η συνεπαγωγή

$$\boxed{(x, x') \in \mathcal{R} \ \text{ και } \ (y, y') \in \mathcal{R} \Longrightarrow (x * y, x' * y') \in \mathcal{R}.}$$

[23] Όταν ισχύει η (1.17), τότε λέμε ότι τα x και y **μετατίθενται αμοιβαίως** ύστερα από εφαρμογή τής πράξεως "$\circledcirc$".

[24] Ο συμβολισμός $(x \circledcirc y) \circledcirc z$ σημαίνει ότι εκτελούμε την πράξη "$\circledcirc$" μεταξύ των x και y και κατόπιν την πράξη "$\circledcirc$" μεταξύ τού (αποτελέσματος τής πρώτης) και τού z (εκ δεξιών). Ο συμβολισμός $x \circledcirc (y \circledcirc z)$ σημαίνει ότι εκτελούμε την πράξη "$\circledcirc$" μεταξύ των y και z και κατόπιν την πράξη "$\circledcirc$" μεταξύ τού (αποτελέσματος τής πρώτης) και τού x (εξ αριστερών).

1.5.20 Θεώρημα (Μεταφορά πράξεως σε σύνολο κλάσεων ισοδυναμίας). *Εάν το A είναι ένα μη κενό σύνολο, η*

$$\varnothing \neq \mathcal{R} \subseteq A \times A$$

μια σχέση ισοδυναμίας και η

$$A \times A \longrightarrow A,\ (x,y) \longmapsto x * y$$

μια εσωτερική πράξη επί τού A, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:

(i) *Η $\mathcal{R}$ είναι συμβατή με την "$*$".*

(ii) *Υφίσταται μια απεικόνιση*

$$(A/\mathcal{R}) \times (A/\mathcal{R}) \longrightarrow (A/\mathcal{R})\,,\ ([x]_{\mathcal{R}}\,,[y]_{\mathcal{R}}) \longmapsto [x]_{\mathcal{R}} \circledast [y]_{\mathcal{R}}\,,$$

ήτοι μια εσωτερική πράξη "$\circledast$" επί τού $A/\mathcal{R}$, η οποία καθιστά το διάγραμμα

$$\begin{array}{ccc} A \times A & \xrightarrow{\quad * \quad} & A \\ {\scriptstyle \pi_{\mathcal{R}} \times \pi_{\mathcal{R}}}\downarrow & & \downarrow{\scriptstyle \pi_{\mathcal{R}}} \\ (A/\mathcal{R}) \times (A/\mathcal{R}) & \xrightarrow[\quad \circledast \quad]{} & A/\mathcal{R} \end{array} \tag{1.18}$$

μεταθετικό. Επιπροσθέτως, εάν πληρούνται οι (i), (ii), *τότε ισχύουν τα εξής*:

(a) *Η "$\circledast$" είναι η μοναδική απεικόνιση με την ανωτέρω περιγραφείσα ιδιότητα και ορίζεται μέσω τού τύπου*

$$\boxed{[x]_{\mathcal{R}} \circledast [y]_{\mathcal{R}} := [x * y]_{\mathcal{R}}\,,\ \ \forall (x,y) \in A \times A.}$$

(b) *Εάν η πράξη "$*$" είναι προσεταιριστική, τότε και η "$\circledast$" είναι προσεταιριστική.*

(c) *Εάν η "$*$" είναι μεταθετική, τότε και η "$\circledast$" είναι μεταθετική.*

(d) *Εάν το e είναι (εξ αριστερών/εκ δεξιών/αμφιπλεύρως) ουδέτερο στοιχείο τού A ως προς την πράξη "$*$", τότε το $[e]_{\mathcal{R}}$ είναι (εξ αριστερών/εκ δεξιών/αμφιπλεύρως) ουδέτερο στοιχείο τού $A/\mathcal{R}$ ως προς την πράξη "$\circledast$".*

(e) *Εάν το e είναι ουδέτερο στοιχείο τού A ως προς την πράξη "$*$" και το x' είναι (εξ αριστερών/εκ δεξιών/αμφιπλεύρως) συμμετρικό στοιχείο ενός $x \in A$ ως προς αυτήν, τότε το $[x']_{\mathcal{R}}$ είναι (εξ αριστερών/εκ δεξιών/αμφιπλεύρως) συμμετρικό στοιχείο τού $[x]_{\mathcal{R}}$ ως προς την πράξη "$\circledast$".*

Απόδειξη. Κατ' αρχάς παρατηρούμε ότι ισχύει η ισοδυναμία των συνθηκών

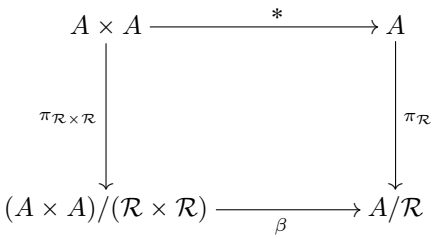
$$\text{(i)} \iff \mathcal{R} \times \mathcal{R} \subseteq \mathcal{R}_{\pi_{\mathcal{R}} \circ *},$$

όπου $\mathcal{R} \times \mathcal{R}$ το καρτεσιανό γινόμενο τής $\mathcal{R}$ με τον εαυτό της (βλ. 1.3.10, 1.3.11) και $\mathcal{R}_{\pi_{\mathcal{R}} \circ *}$ η σχέση ισοδυναμίας η επαγομένη μέσω τής συνθέσεως $\pi_{\mathcal{R}} \circ *$ επί τού $A \times A$ (βλ. 1.3.22).

(i)⇒(ii) Εφαρμόζοντας το πόρισμα 1.3.29 (με την "$*$" αντί τής f, το $A \times A$ αντί τού A, το A αντί τού B, το $\mathcal{R} \times \mathcal{R}$ αντί τού $\mathcal{R}$ και το $\mathcal{R}$ αντί τού $\mathcal{S}$) διαπιστώνουμε ότι υφίσταται (μία και μόνον) απεικόνιση

$$(\text{"}\check{*}\text{"} =:)\ \beta : (A \times A)/(\mathcal{R} \times \mathcal{R}) \longrightarrow (A/\mathcal{R})$$

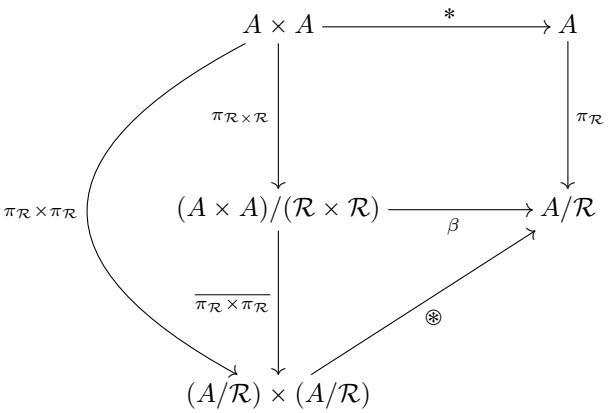
η οποία καθιστά το διάγραμμα



μεταθετικό. Συγκεκριμένα, η εν λόγω απεικόνιση είναι η αυτή που ορίζεται από τον τύπο

$$[(x,y)]_{\mathcal{R}\times\mathcal{R}} \longmapsto \beta\left([(x,y)]_{\mathcal{R}\times\mathcal{R}}\right) := [x*y]_{\mathcal{R}}\,, \quad \forall (x,y) \in A \times A.$$

Αρκεί λοιπόν να εφαρμόσουμε το πόρισμα 1.3.28 (για $A = B$, $\mathcal{S} = \mathcal{R}$), να καταλήξουμε στο επεκτεταμένο μεταθετικό διάγραμμα



(1.19)

και να θέσουμε $\circledast := \beta \circ \left(\overline{\pi_{\mathcal{R}} \times \pi_{\mathcal{R}}}\right)^{-1}$ (καθότι η $\overline{\pi_{\mathcal{R}} \times \pi_{\mathcal{R}}}$ είναι αμφιριπτική).

(ii)⇒(i) Εκκινώντας από την "$\circledast$" κατασκευάζουμε την β θέτοντας

$$\beta := \circledast \circ \left(\overline{\pi_{\mathcal{R}} \times \pi_{\mathcal{R}}}\right)$$

και επαληθεύουμε την (i) χρησιμοποιώντας τη συνεπαγωγή (ii)⇒(i) τού πορίσματος 1.3.29.

(a) Επειδή, κατά τα προαναφερθέντα, η "$\circledast$" παρίσταται ως σύνθεση δύο μονοσημάντως ορισμένων απεικονίσεων, ούτως ώστε το (1.19) (αφαιρουμένης τής ιδίας) να καθίσταται μεταθετικό (σύμφωνα με τα χρησιμοποιηθέντα πορίσματα 1.3.28 και 1.3.29), η "$\circledast$" είναι κατ' ανάγκην η *μοναδική απεικόνιση* που καθιστά το (1.18) μεταθετικό. Επιπροσθέτως, για κάθε $x, y \in A$ έχουμε

$$[x]_{\mathcal{R}} \circledast [y]_{\mathcal{R}} := \beta \circ \left(\overline{\pi_{\mathcal{R}} \times \pi_{\mathcal{R}}}\right)^{-1} ([x]_{\mathcal{R}}\,, [y]_{\mathcal{R}}) = \beta\left([(x,y)]_{\mathcal{R}\times\mathcal{R}}\right) = [x*y]_{\mathcal{R}}\,.$$

(b) Εάν η "$*$" είναι προσεταιριστική, τότε για οιαδήποτε $x, y, z \in A$ έχουμε

$$\begin{aligned} ([x]_{\mathcal{R}} \circledast [y]_{\mathcal{R}}) \circledast [z]_{\mathcal{R}} &= [x*y]_{\mathcal{R}} \circledast [z]_{\mathcal{R}} = [(x*y)*z]_{\mathcal{R}} \\ &= [x*(y*z)]_{\mathcal{R}} = [x]_{\mathcal{R}} \circledast [y*z]_{\mathcal{R}} \\ &= [x]_{\mathcal{R}} \circledast ([y]_{\mathcal{R}} \circledast [z]_{\mathcal{R}})\,. \end{aligned}$$

(c) Εάν η "$*$" είναι μεταβατική, τότε για οιαδήποτε $x, y \in A$ ισχύουν οι ισότητες

$$[x]_{\mathcal{R}} \circledast [y]_{\mathcal{R}} = [x*y]_{\mathcal{R}} = [y*x]_{\mathcal{R}} = [y]_{\mathcal{R}} \circledast [x]_{\mathcal{R}}\,.$$

(d) Εάν το e είναι εξ αριστερών ουδέτερο στοιχείο τού A ως προς την "$*$", τότε

$$[e]_{\mathcal{R}} \circledast [x]_{\mathcal{R}} = [e * x]_{\mathcal{R}} = [x]_{\mathcal{R}}\,,$$

οπότε το $[e]_{\mathcal{R}}$ είναι εξ αριστερών ουδέτερο στοιχείο τού $A/\mathcal{R}$ ως προς την πράξη "$\circledast$". Οι λοιπές περιπτώσεις αντιμετωπίζονται παρομοίως.

(e) Εάν το x' είναι εξ αριστερών συμμετρικό στοιχείο ενός $x \in A$ ως προς την πράξη "$*$", τότε

$$\left[x'\right]_{\mathcal{R}} \circledast [x]_{\mathcal{R}} = \left[x' * x\right]_{\mathcal{R}} = [e]_{\mathcal{R}}\,,$$

οπότε το $[x']_{\mathcal{R}}$ είναι εξ αριστερών συμμετρικό στοιχείο τού $[x]_{\mathcal{R}}$ ως προς την πράξη "$\circledast$". Οι λοιπές περιπτώσεις αντιμετωπίζονται παρομοίως. □

‣ **«Επιμεριστικός» συσχετισμός δύο εσωτερικών πράξεων**. Όταν ένα δοθέν μη κενό σύνολο είναι εφοδιασμένο με *δύο* εσωτερικές πράξεις, τότε ο πλέον «φυσικός» τρόπος συσχετισμού τής μίας με την άλλη περιγράφεται στον ακόλουθο ορισμό. (Θα πρέπει, ωστόσο, εξαρχής να επισημανθεί ότι η ισχύς ή μη τής λεγομένης *επιμεριστικής ιδιότητας* εξαρτάται -εν γένει- και από το ποια εκ των θεωρουμένων πράξεων εκτελείται ως *πρώτη* και ποια ως *δεύτερη*. Πρβλ. με τα (i) και (ii) τής σημειώσεως 1.6.19.)

1.5.21 Ορισμός. Έστω ότι το A είναι ένα μη κενό σύνολο και οι

$$A \times A \longrightarrow A,\ (x,y) \longmapsto x \star y, \quad A \times A \longrightarrow A,\ (x,y) \longmapsto x \circledcirc y$$

δυο εσωτερικές πράξεις οριζόμενες επ' αυτού. Θα λέμε ότι η πράξη "$\star$" είναι

(i) **εξ αριστερών επιμεριστική ως προς την** "$\circledcirc$" όταν για οιαδήποτε $x, y, z \in A$ ισχύει η ισότητα

$$\boxed{x \star (y \circledcirc z) = (x \star y) \circledcirc (x \star z)\,,}$$

(ii) **εκ δεξιών επιμεριστική ως προς την** "$\circledcirc$" όταν για οιαδήποτε $x, y, z \in A$ ισχύει η ισότητα

$$\boxed{(y \circledcirc z) \star x = (y \star x) \circledcirc (z \star x)\,,}$$

και (iii) **αμφιπλεύρως επιμεριστική ως προς την** "$\circledcirc$" ή απλώς **επιμεριστική ως προς την** "$\circledcirc$" όταν η "$\star$" είναι ταυτοχρόνως και εξ αριστερών και εκ δεξιών επιμεριστική ως προς την "$\circledcirc$".

1.5.22 Παρατήρηση. Εάν η πράξη "$\star$" είναι μεταθετική, τότε οι έννοιες «εξ αριστερών επιμεριστική», «εκ δεξιών επιμεριστική» και «επιμεριστική» ως προς την "$\circledcirc$" συμπίπτουν. Εάν η "$\star$" δεν είναι μεταθετική, τότε η εκ δεξιών επιμεριστικότητα ενδέχεται να μην συνεπάγεται την εξ αριστερών επιμεριστικότητά της ως προς κάποιες άλλες εσωτερικές (και μάλιστα μεταθετικές!) πράξεις "$\circledcirc$".

1.5.23 Παραδείγματα. Έστω Ω ένα σύνολο. Στο εδάφιο 1.5.5 ορίσθηκαν τρεις εσωτερικές (προσεταιριστικές και μεταθετικές) πράξεις επί τού δυναμοσυνόλου του $\mathfrak{P}(\Omega)$ (ένωση, τομή και συμμετρική διαφορά). Καθεμιά εκ των πράξεων «ένωση» και «τομή» είναι επιμεριστική ως προς την άλλη (βλ. 1.1.3 (iv)). Η πράξη «συμμετρική διαφορά» είναι επιμεριστική ως προς την «τομή» (βλ. το (vi) τής ασκήσεως 8 τού 1ου φυλλαδίου) αλλά δεν είναι επιμεριστική ως προς την «ένωση» όταν $\Omega \neq \varnothing$, διότι για οιαδήποτε $A, B \in \mathfrak{P}(\Omega)$ έχουμε

$$\Omega \cup (A \vartriangle B) = \Omega \neq \varnothing = \Omega \vartriangle \Omega = (\Omega \cup A) \vartriangle (\Omega \cup B)\,.$$

▸ **Μετάβαση στα «αριθμητικά σύνολα».** Στα περισσότερα εκ των προαναφερθέντων παραδειγμάτων εσωτερικών πράξεων υπεισήλθαν ενώσεις, τομές και συμμετρικές διαφορές συνόλων ανηκόντων στο δυναμοσύνολο ενός συνόλου ή συνθέσεις απεικονίσεων από ένα σύνολο στον εαυτό του. Για να αυξήσουμε το απόθεμά μας σε παραδείγματα επίκειται να χρησιμοποιήσουμε τα «αριθμητικά συστήματα» ή «αριθμητικά σύνολα» $\mathbb{N}$ των *φυσικών αριθμών*, $\mathbb{Z}$ των *ακεραίων αριθμών*, $\mathbb{Q}$ των *ρητών αριθμών*, $\mathbb{R}$ των *πραγματικών αριθμών* και $\mathbb{C}$ των *μιγαδικών αριθμών*. Παρότι οι κύριες ιδιότητες των «συνήθων πράξεων» (*προσθέσεως* και *πολλαπλασιασμού*) των οριζομένων επ' αυτών, καθώς και η ιεράρχηση (ως προς τη σχέση τού εγκλεισμού)

$$\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C} \tag{1.20}$$

και η διάταξη των στοιχείων των τεσσάρων πρώτων είναι γνωστές από το σχολείο, η ορισμολογική οικοδόμηση των προκειμένων συνόλων, διμελών σχέσεων και απεικονίσεων που έγινε εκεί ήταν ατελής (τόσον από συνολοθεωρητική όσον και από καθαρώς αλγεβρική οπτική γωνία), ούτως ώστε να μην είναι δυνατόν να ανταποκρίνεται στο περιώνυμο γνωμικό τού Kronecker[25]. Η κατά τι μακροσκελής κατασκευή των «αριθμητικών συνόλων» και η αλγεβρική ερμηνεία των εγκλειστικών σχέσεων (1.20) θα παρουσιασθούν στις επόμενες πέντε ενότητες.

1.6 ΦΥΣΙΚΟΙ ΑΡΙΘΜΟΙ

Το σύστημα των φυσικών αριθμών $(\mathbb{N}, 1, \theta)$ εισάγεται αυστηρώς μέσω *των αξιωμάτων τού Peano*[26]. Επί τού $\mathbb{N}$ ορίζονται οι *συνήθεις* (εσωτερικές) *πράξεις* τής *προσθέσεως* και τού *πολλαπλασιασμού* («συνήθεις» υπό την έννοια με την οποία αυτές χρησιμοποιούνται στο σχολείο) ως απεικονίσεις $\alpha : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$ και $\beta : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$ που πληρούν κατάλληλες συνθήκες. (Κατ' αναλογίαν, μέσω μιας άλλης απεικονίσεως $\gamma : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ εισάγεται και ο σχηματισμός «δυνάμεων»). Επίσης, το $\mathbb{N}$, εφοδιαζόμενο με τη συνήθη διάταξη, καθίσταται ένα *καλώς διατεταγμένο σύνολο*.

▸ **Αξιωματική δόμηση τού** $\mathbb{N}$. Για τη δόμηση τού $\mathbb{N}$ αρκεί κανείς να εκλάβει ως αξιώματα[27] τις στοιχειώδεις ιδιότητες τής διαδοχικής απαριθμήσεως (ξεκινώντας με κάποια «ελαχίστη» αριθμητική οντότητα ονόματι **ένα**, "1", και προσθέτοντας στο κατασκεύασμα κάθε «επόμενόν της»). Για την πλέον προσήκουσα έκφραση αυτών των ιδιοτήτων γίνεται χρήση ειδικών απεικονίσεων $\theta : \mathbb{N} \longrightarrow \mathbb{N}$.

1.6.1 Αξιώματα (Peano, 1889). *Έστω* $\mathbb{N}$ *ένα σύνολο για το οποίο υφίσταται μια απεικόνιση* $\theta : \mathbb{N} \longrightarrow \mathbb{N}$, *ούτως ώστε να πληρούνται τα κάτωθι* **αξιώματα τού Peano**:

(**A 1**) *Υπάρχει ένα στοιχείο* $1 \in \mathbb{N}$.

(**A 2**) $1 \notin \theta(\mathbb{N})$.

(**A 3**) *Η* θ *είναι ενριπτική.*

[25] Κατά τον Γερμανό μαθηματικό Leopold Kronecker (1823-1891): «Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk». Βεβαίως, όπως θα διαπιστώσει κανείς, η μόνη ενδεχόμενη «μεταφυσική συνιστώσα» τής κατασκευής τού $\mathbb{N}$ ή τού $\mathbb{Z}$ δεν θα μπορούσε να συναρτάται με τίποτα άλλο παρά με τα αξιώματα τα παρατιθέμενα στα εδάφια 1.6.1 και 1.6.4.)

[26] Ο Ιταλός μαθηματικός Giuseppe Peano (1858-1932) δημοσίευσε τα αξιώματα αυτά στο άρθρο του *Arithmetices principia nova methodo exposita*, 1889. (Βλ. Opere scelte, Vol. II, Rome 1958, σελ. 20-55.)

[27] Για διάφορους κλάδους των Μαθηματικών έχουν κατασκευασθεί συστήματα από *χαρακτηριστικές, θεμελιώδεις ιδιότητες*, στις οποίες στηρίζεται καθ' ολοκηρίαν η εκάστοτε αναπτυσσόμενη θεωρία· δηλαδή, εάν οι εν λόγω χαρακτηριστικές, θεμελιώδεις ιδιότητες, οι οποίες καλούνται **αξιώματα**, θεωρηθούν a priori αληθείς, τότε είναι δυνατή η απόδειξη οιασδήποτε άλλης ιδιότητας μέσω αυτών. Για να είναι ένα «αξιωματικό οικοδόμημα» *παραδεκτό* επιδιώκεται να έχει τα εξής τρία γνωρίσματα:
α) Να είναι **πλήρες**, δηλαδή να καλύπτει ολόκληρη τη θεωρία για την οποία έχει κατασκευασθεί.
β) Να είναι **ανεξάρτητο**, δηλαδή κανένα από τα αξιώματά του να μην είναι απόρροια των υπολοίπων.
γ) Να είναι **ελεύθερο αντιφάσεων**, δηλαδή να μην υφίστανται προτάσεις αποδεικνυόμενες μέσω των αξιωμάτων του, με τις αρνήσεις αυτών αποδεικνυόμενες ωσαύτως μέσω των αξιωμάτων.

(**A 4**) *Για κάθε υποσύνολο* $U \subseteq \mathbb{N}$ *για το οποίο ισχύει* $1 \in U$ *και* $\theta(n) \in U$, $\forall n \in U$, *έχουμε* $U = \mathbb{N}$.
Τότε η τριάδα $(\mathbb{N}, 1, \theta)$ *καλείται* **σύστημα φυσικών αριθμών**.

1.6.2 Σημείωση. (i) Οι ως άνω απεικονίσεις $\theta : \mathbb{N} \longrightarrow \mathbb{N}$ ονομάζονται **απεικονίσεις διαδοχής**, ενώ η εικόνα $\theta(n)$ οιουδήποτε $n \in \mathbb{N}$ μέσω μιας τέτοιας απεικονίσεως θ καλείται **διάδοχος** τού n ως προς την θ. (Πρβλ. 1.6.15 (i)).

(ii) Η *ύπαρξη* (τουλάχιστον) ενός συστήματος φυσικών αριθμών διασφαλίζεται μέσω τού θεωρήματος 1.6.7. Επιπροσθέτως, το θεώρημα 1.6.10 μας πληροφορεί ότι δυο *τυχόντα* συστήματα φυσικών αριθμών μπορούν να εκληφθούν (υπό μία προδιαγεγραμμένη έννοια) ως *κατ' ουσίαν ταυτιζόμενα*.

(iii) Η *εξέχουσα σημασία* τού αξιώματος (**A 4**) θα αναφανεί, μεταξύ άλλων, και στα θεωρήματα 1.6.32, 1.6.34, 1.6.36 και 1.6.38 που παρατίθενται στο τέλος τής παρούσας ενότητας.

1.6.3 Ορισμός. Ένα σύνολο $\mathcal{G}$ αποτελούμενο από σύνολα (ήτοι έχον σύνολα ως στοιχεία του) καλείται **επαγωγικώς κατασκευαζόμενο** όταν πληροί τις ακόλουθες συνθήκες[28]:
(i) $\{\varnothing\} \in \mathcal{G}$.
(ii) $A \cup \{A\} \in \mathcal{G}$, $\forall A \in \mathcal{G}$.
Ορίζουμε ως

$$\mathcal{N} := \bigcap \{\mathcal{G} | \, \mathcal{G} \text{ επαγωγικώς κατασκευαζόμενο σύνολο}\}$$

την τομή όλων των επαγωγικώς κατασκευαζόμενων συνόλων.

1.6.4 Σημείωση. Η *ύπαρξη* (τουλάχιστον) ενός επαγωγικώς κατασκευαζόμενου συνόλου είναι τόσο θεμελιώδης για τη Θεωρία Συνόλων, ώστε να πρέπει να θεσπίζεται ως *αξίωμα*, το οποίο είναι γνωστό ως **αξίωμα τού απείρου**. Βλ. P.R. Halmos: *Αφελής Συνολοθεωρία,* σε μετάφραση (από το αγγλικό πρωτότυπο υπό τον τίτλο *Naive Set Theory*, Springer-Verlag, 1960) από τον Γ. Κολέτσο, Εκδόσεις Εκκρεμές, Αθήνα, 2002, κεφ. 11.

1.6.5 Λήμμα. *Έστω ένα υποσύνολο* $\mathcal{U} \subseteq \mathcal{N}$ *για το οποίο ισχύει* $\{\varnothing\} \in \mathcal{U}$ *και*

$$A \cup \{A\} \in \mathcal{U}, \quad \forall A \in \mathcal{U}.$$

Τότε $\mathcal{U} = \mathcal{N}$.

Απόδειξη. Προφανώς, $\mathcal{U} \in \{\mathcal{G} | \, \mathcal{G} \text{ επαγωγικώς κατασκευαζόμενο σύνολο}\}$, οπότε

$$\bigcap \left\{ \mathcal{G} \,\middle|\, \begin{array}{c} \mathcal{G} \text{ επαγωγικώς} \\ \text{κατασκευαζόμενο σύνολο} \end{array} \right\} = \mathcal{N} \subseteq \mathcal{U} \subseteq \mathcal{N} \Rightarrow \mathcal{U} = \mathcal{N}$$

και ο ισχυρισμός είναι αληθής. □

1.6.6 Λήμμα. *Για κάθε* $A \in \mathcal{N}$ *ισχύουν τα εξής*:
(i) $A \neq \varnothing$.
(ii) *Εάν* $B \in A$, *τότε* $B \subseteq A$.

[28] Εν προκειμένω, απαιτείται ιδιαίτερη προσοχή, καθότι πρέπει να γίνεται σαφής διάκριση μεταξύ τού συνόλου A και τού μονοσυνόλου $\{A\}$ (ως στοιχείου τού $\mathfrak{P}(A)$)!

Απόδειξη. Έστω $\mathcal{U} := \{A \in \mathcal{N} \,|\text{το } A \text{ πληροί τις (i) και (ii)}\}$. Κατ' αρχάς παρατηρούμε ότι $\{\varnothing\} \in \mathcal{U}$, διότι

$$\{\varnothing\} \in \mathcal{N},\ \varnothing \in \{\varnothing\} \neq \varnothing, \text{ και εάν } B \in \{\varnothing\},\ \text{τότε } B = \varnothing \Rightarrow B \subseteq \{\varnothing\}.$$

Επιπροσθέτως, για οιοδήποτε $A \in \mathcal{U}$ έχουμε $A \cup \{A\} \in \mathcal{U}$, καθόσον

$$A \cup \{A\} \in \mathcal{N},\ \ A \in A \cup \{A\} \neq \varnothing$$

και εάν $B \in A \cup \{A\}$, τότε

$$[B \in A \ \text{ή}\ B = A] \Longrightarrow B \subseteq A \ \text{ή}\ B = A \ (\text{διότι } A \in \mathcal{U}) \Longrightarrow B \subseteq A.$$

Κατά συνέπειαν, σύμφωνα με το λήμμα 1.6.5, $\mathcal{U} = \mathcal{N}$. □

1.6.7 Θεώρημα (Ύπαρξη συστήματος φυσικών αριθμών.). *Υπάρχει τουλάχιστον ένα σύστημα φυσικών αριθμών.*

Απόδειξη. Θα αποδείξουμε ότι η τριάδα $(\mathcal{N}, \{\varnothing\}, \vartheta)$ αποτελεί ένα σύστημα φυσικών αριθμών, όπου

$$\vartheta : \mathcal{N} \longrightarrow \mathcal{N},\ \ \vartheta(A) := A \cup \{A\},\ \forall A \in \mathcal{N}.$$

Επειδή $\{\varnothing\} \in \mathcal{N}$, το (**A 1**) είναι προφανές. Εν συνεχεία θεωρούμε ένα υποσύνολο $\mathcal{U} \subseteq \mathcal{N}$ για το οποίο ισχύει $\{\varnothing\} \in \mathcal{U}$ και $\vartheta(A) \in \mathcal{U}$, $\forall A \in \mathcal{U}$. Τότε, σύμφωνα με το λήμμα 1.6.5, $\mathcal{U} = \mathcal{N}$, πράγμα που σημαίνει ότι πληρούται και το αξίωμα (**A 4**). Σημειωτέον ότι η ϑ είναι ενριπτική, διότι για οιαδήποτε σύνολα $A, A' \in \mathcal{N}$, για τα οποία ισχύει η ισότητα $A \cup \{A\} = A' \cup \{A'\}$, λαμβάνουμε

$$\begin{aligned}
& A \in A' \cup \{A'\} \ \text{ και } \ A' \in A \cup \{A\} \\
\Longrightarrow\ & [A \in A' \ \text{ή}\ A = A'] \ \text{ και } \ [A' \in A \ \text{ή}\ A' = A] \\
\Longrightarrow\ & [A \in A' \ \text{ και } \ A' \in A] \ \text{ή}\ A = A' \\
\Longrightarrow\ & [A \subseteq A' \ \text{ και } \ A' \subseteq A] \ \text{ή}\ A = A' \ (\text{λόγω τού (ii) τού λήμματος 1.6.6}) \\
\Longrightarrow\ & A = A'.
\end{aligned}$$

Τούτο επαληθεύει το αξίωμα (**A 3**). Απομένει η επαλήθευση τού (**A 2**). Εάν υπήρχε $A \in \mathcal{N}$, τέτοιο ώστε να ισχύει $\vartheta(A) = \{\varnothing\}$, θα είχαμε

$$A \cup \{A\} = \{\varnothing\} \Longrightarrow A = \varnothing,$$

ήτοι κάτι που θα αντέκειτο προς το (i) τού λήμματος 1.6.6. Άρα $\{\varnothing\} \notin \vartheta(\mathcal{N})$. □

1.6.8 Θεώρημα («Θεώρημα τής αναδρομικότητας», R. Dedekind, 1888).
Έστω $(\mathbb{N}, 1, \theta)$ οιοδήποτε σύστημα φυσικών αριθμών και έστω B τυχόν μη κενό σύνολο. Εάν $b \in B$ και $\psi : B \longrightarrow B$ τυχούσα απεικόνιση, τότε υφίσταται μία και μόνον απεικόνιση $f : \mathbb{N} \longrightarrow B$ η οποία ικανοποιεί τις ακόλουθες συνθήκες:
(i) $f(1) = b$.
(ii) $f(\theta(n)) = \psi(f(n)),\ \forall n \in \mathbb{N}$.

Απόδειξη. *Ύπαρξη μιας τέτοιας απεικονίσεως f.* Ορίζουμε ως **επιτρεπτό σύνολο** κάθε σύνολο $E \subseteq \mathbb{N} \times B$ που ικανοποιεί τις ακόλουθες συνθήκες:
(a) $(1, b) \in E$.
(b) $(\theta(n), \psi(m)) \in E,\ \forall (n, m) \in E$.

[Σημείωση: Επί παραδείγματι, ολόκληρο το καρτεσιανό γινόμενο $\mathbb{N} \times B$ αποτελεί καταφανώς ένα επιτρεπτό σύνολο.] Εν συνεχεία θέτουμε

$$\Gamma := \bigcap \{ E |\, E \text{ επιτρεπτό σύνολο} \} .$$

Το Γ είναι αφ' εαυτού επιτρεπτό σύνολο, διότι ικανοποιεί τις (a) και (b). (Μάλιστα, το Γ είναι το *ελάχιστο επιτρεπτό σύνολο* ως προς τον συνήθη συνολοθεωρητικό εγκλεισμό.) Αρκεί λοιπόν να αποδειχθεί ότι το Γ αποτελεί το γράφημα Γ_f μιας απεικονίσεως $f : \mathbb{N} \longrightarrow B$ (διότι τότε αυτή η f θα πληροί εκ κατασκευής τις (i) και (ii)). Προς τούτο πρέπει να δειχθεί ότι ισχύουν τα ακόλουθα:

(I) $\forall n \in \mathbb{N} \;\; \exists m \in B : (n, m) \in \Gamma$.

(II) $\forall\, (n, m) \in \Gamma$ και $\forall\, (n', m') \in \Gamma : n = n' \Longrightarrow m = m'$. (Πρβλ. 1.2.2.)

Έστω $U := \{ n \in \mathbb{N} \,|\, \exists m \in B : (n, m) \in \Gamma \}$. Προφανώς, $1 \in U$ (λόγω τού ότι το Γ, όντας επιτρεπτό, ικανοποιεί τη συνθήκη (a)). Επίσης, για κάθε στοιχείο $n \in U$ έχουμε $\theta\,(n) \in U$ (διότι το Γ, όντας επιτρεπτό, ικανοποιεί και τη συνθήκη (b)). Σύμφωνα με το αξίωμα (**A 4**), $U = \mathbb{N}$, οπότε το **(I)** είναι αληθές. Έστω τώρα

$$W := \{ n \in \mathbb{N} \,|\, \text{υπάρχει } \textit{ακριβώς ένα}\; m \in B : (n, m) \in \Gamma \} .$$

Εκ κατασκευής, $(1, b) \in \Gamma$. Ας υποθέσουμε ότι $(1, b') \in \Gamma$ για κάποιο $b' \in B \smallsetminus \{b\}$. Θέτοντας

$$\Gamma^{-} := \Gamma \smallsetminus \{(1, b')\}$$

παρατηρούμε ότι αφ' ενός μεν $(1, b) \in \Gamma^{-}$, αφ' ετέρου δε

$$(\theta\,(n)\,, \psi\,(m)) \in \Gamma^{-}, \;\; \forall\, (n, m) \in \Gamma^{-},$$

διότι (κατά το αξίωμα (**A 2**))

$$1 \notin \theta(\mathbb{N}) \Longrightarrow (\theta\,(n)\,, \psi\,(m)) \neq (1, b'), \;\; \forall\, (n, m) \in \Gamma^{-}.$$

Τούτο σημαίνει ότι το Γ^{-} είναι επιτρεπτό σύνολο, κάτι που αντιφάσκει προς το γεγονός ότι το Γ είναι το *ελάχιστο επιτρεπτό σύνολο*. Άρα $1 \in W$. Εξάλλου, για οιοδήποτε $n \in W$ υπάρχει *ακριβώς ένα* $m \in B : (n, m) \in \Gamma$ με

$$(\theta\,(n)\,, \psi\,(m)) \in \Gamma.$$

Ας υποθέσουμε ότι $(\theta\,(n)\,, c) \in \Gamma$ για κάποιο $c \in B \smallsetminus \{\psi\,(m)\}$. Θέτοντας

$$\Gamma^{\star} := \Gamma \smallsetminus \{(\theta\,(n)\,, c)\}$$

παρατηρούμε ότι

$$1 \notin \theta(\mathbb{N}) \Longrightarrow (1, b) \in \Gamma^{\star}. \tag{1.21}$$

Επιπροσθέτως, για κάθε $(k, l) \in \Gamma^{\star}$ έχουμε

$$(\theta\,(k)\,, \psi\,(l)) \in \Gamma^{\star}. \tag{1.22}$$

Πράγματι· στην περίπτωση όπου $k = n$ η (1.22) είναι αληθής, διότι $(n, m) \in \Gamma$ με $m = l$ και

$$\psi\,(m) \neq c \Rightarrow (\theta\,(k)\,, \psi\,(l)) = (\theta\,(n)\,, \psi\,(m)) \neq (\theta\,(n)\,, c)\,.$$

Εάν $k \neq n$, τότε

$$\left.\begin{array}{r} (\theta\,(k)\,, \psi\,(l)) \in \Gamma \\ (\textbf{A3}) \Rightarrow \theta\,(k) \neq \theta\,(n) \end{array}\right\} \Rightarrow (\theta\,(k)\,, \psi\,(l)) \neq (\theta\,(n)\,, c)\,.$$

Άρα η (1.22) είναι πάντοτε αληθής. Από τις (1.21) και (1.22) συμπεραίνουμε ότι το $\Gamma^\star$ είναι επιτρεπτό σύνολο, κάτι που αντιφάσκει προς το γεγονός ότι το Γ είναι το *ελάχιστο επιτρεπτό σύνολο*. Άρα $\theta(n) \in W$. Κατά το αξίωμα (**A 4**), $W = \mathbb{N}$, οπότε *και* το (II) είναι αληθές.

Μοναδικότητα μιας τέτοιας απεικονίσεως f. Ας υποθέσουμε ότι υπάρχει κάποια άλλη απεικόνιση $f' : \mathbb{N} \longrightarrow B$ με $f'(1) = b$ και $f'(\theta(n)) = \psi(f'(n))$, $\forall n \in \mathbb{N}$. Θέτοντας $Z := \{n \in \mathbb{N} \mid f(n) = f'(n)\}$ παρατηρούμε ότι

$$f(1) = b = f'(1) \Longrightarrow 1 \in Z.$$

Επιπροσθέτως, για κάθε $n \in Z$ έχουμε

$$f(n) = f'(n) \Rightarrow f(\theta(n)) = \psi(f(n)) = \psi\left(f'(n)\right) = f'(\theta(n)) \Rightarrow \theta(n) \in Z.$$

Κατά το αξίωμα (**A 4**), $Z = \mathbb{N}$, οπότε $f = f'$. □

1.6.9 Ορισμός. Λέμε ότι δυο συστήματα φυσικών αριθμών $(\mathbb{N}, 1, \theta)$ και $(\mathbb{N}', 1', \theta')$ είναι **ισόμορφα** όταν υφίσταται μια *αμφιρριπτική απεικόνιση* $f : \mathbb{N} \longrightarrow \mathbb{N}'$ η οποία ικανοποιεί τις ακόλουθες συνθήκες[29]:

(i) $f(1) = 1'$.

(ii) $f(\theta(n)) = \theta'(f(n))$, $\forall n \in \mathbb{N}$.

1.6.10 Θεώρημα (Το μονοσήμαντο τού συστήματος των φυσικών αριθμών). *Δυο τυχόντα συστήματα φυσικών αριθμών είναι ισόμορφα.*

Απόδειξη. Έστω ότι τα $(\mathbb{N}, 1, \theta)$ και $(\mathbb{N}', 1', \theta')$ είναι δυο τυχόντα συστήματα φυσικών αριθμών. Θα αποδείξουμε ότι αυτά οφείλουν να είναι ισόμορφα. Εφαρμόζοντας το θεώρημα 1.6.8 (για τα $B = \mathbb{N}'$, $b = 1'$ και $\psi = \theta'$) κατασκευάζουμε τη (μοναδική) απεικόνιση $f : \mathbb{N} \longrightarrow \mathbb{N}'$ που ικανοποιεί τις συνθήκες (i) και (ii) τού 1.6.9. Αρκεί λοιπόν να αποδειχθεί ότι η f είναι μια αμφίρριψη. Κάνοντας εκ νέου χρήση τού θεωρήματος 1.6.8 (κατόπιν εναλλαγής των ρόλων των συστημάτων αναφοράς μας) κατασκευάζουμε τη (μοναδική) απεικόνιση $g : \mathbb{N}' \longrightarrow \mathbb{N}$ με

$$g(1') = 1, \;\; g(\theta'(n')) = \theta\left(g\left(n'\right)\right), \forall n' \in \mathbb{N}'.$$

Έστω $U := \{n \in \mathbb{N} \mid g(f(n)) = n\}$. Προφανώς,

$$g(f(1)) = g(1') = 1 \Rightarrow 1 \in U,$$

και για κάθε $n \in U$ έχουμε

$$g(f(\theta(n))) = g\left(\theta'(f(n))\right) = \theta(g(f(n))) = \theta(n) \Rightarrow \theta(n) \in U.$$

Σύμφωνα με το το αξίωμα (**A 4**), $U = \mathbb{N}$, οπότε $g \circ f = \mathrm{id}_{\mathbb{N}}$. Κατ' αναλογίαν αποδεικνύεται ότι $f \circ g = \mathrm{id}_{\mathbb{N}'}$. Ως εκ τούτου, η f είναι αμφιρριπτική έχουσα την g ως αντίστροφό της. (Βλ. 1.2.18 (iii).) □

[29] Η συνθήκη (i) μας πληροφορεί ότι το «πρώτο» στοιχείο τού $\mathbb{N}$ στέλνεται να απεικονισθεί μέσω τής f στο «πρώτο» στοιχείο τού $\mathbb{N}'$. Η συνθήκη (ii) ισοδυναμεί με το ότι το διάγραμμα

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{\;f\;} & \mathbb{N}' \\ {\scriptstyle\theta}\downarrow & & \downarrow{\scriptstyle\theta'} \\ \mathbb{N} & \xrightarrow{\;f\;} & \mathbb{N}' \end{array}$$

είναι μεταθετικό (βλ. 1.2.14).

1.6.11 Σημείωση. Επί τη βάσει τού θεωρήματος 1.6.10 όλα τα συστήματα φυσικών αριθμών μπορούν να λογίζονται ως *κατ' ουσίαν ταυτιζόμενα* (υπό την περιγραφείσα έννοια). Γι' αυτόν τον λόγο θα ομιλούμε *από εδώ και στο εξής* (με μόνη εξαίρεση ό,τι εντοπίζεται στην παρατήρηση 1.6.31 και στις σημειώσεις 1.6.33 και 1.7.28) για **το** *σύνολο* $\mathbb{N}$ *των φυσικών αριθμών* [έχον το 1 ως «πρώτο του στοιχείο» (βλ. 1.6.24 (iv))] και για **την** απεικόνιση διαδοχής $\theta : \mathbb{N} \longrightarrow \mathbb{N}$. Επίσης, θα κάνουμε χρήση των «οικείων» μας συμβολισμών

$$2 := \theta(1), \;\; 3 := \theta(2), \;\; 4 := \theta(3), \;\; \ldots\ldots$$

και ονομασιών (*δύο*, *τρία*, *τέσσερα* κ.λπ.)

1.6.12 Πρόταση. *Το σύνολο των φυσικών αριθμών* $\mathbb{N}$ *έχει τις εξής ιδιότητες*:
(i) $\theta(n) \neq n, \forall n \in \mathbb{N}$.
(ii) *Για κάθε* $n \in \mathbb{N} \setminus \{1\}$ *υπάρχει ένας και μόνον* $m \in \mathbb{N}$, *ούτως ώστε να ισχύει η ισότητα* $n = \theta(m)$.
(iii) *Εάν* $n \in \mathbb{N}$, *τότε* $n = 1 \Longleftrightarrow n \notin \theta(\mathbb{N})$.

Απόδειξη. (i) Έστω $U := \{n \in \mathbb{N} \,|\, \theta(n) \neq n\}$. Το αξίωμα (**A 2**) μας πληροφορεί ότι $1 \notin \theta(\mathbb{N})$, απ' όπου έπεται ότι $1 \in U$. Έστω τυχών $n \in U$. Τότε $\theta(\theta(n)) \neq \theta(n)$, διότι εάν ίσχυε η ισότητα $\theta(\theta(n)) = \theta(n)$, θα συμπεραίναμε ότι $\theta(n) = n$ (λόγω τού αξιώματος (**A 3**)), πράγμα αδύνατο (καθόσον $n \in U$ εξ υποθέσεως). Άρα $\theta(n) \in U$. Μέσω τού αξιώματος (**A 4**) συνάγεται ότι $U = \mathbb{N}$.

(ii) Έστω $U := \{n \in \mathbb{N} \,|\, \text{είτε } n = 1 \text{ είτε } \exists m \in \mathbb{N} : n = \theta(m)\}$. Εξ ορισμού, $1 \in U$. Έστω τυχών $n \in U$. Εάν $n = 1$, τότε $\theta(n) = \theta(1) \in U$ (διότι $1 \in \mathbb{N}$). Εάν $n \neq 1$, τότε $\theta(n) \in U$ (διότι $n \in \mathbb{N}$). Άρα $\theta(n) \in U, \forall n \in U$. Κατά το αξίωμα (**A 4**), $U = \mathbb{N}$. Εξ αυτού έπεται ότι για κάθε $n \in \mathbb{N} \setminus \{1\}$ υπάρχει ένας $m \in \mathbb{N}$, ούτως ώστε να ισχύει η ισότητα $n = \theta(m)$. Η μοναδικότητα ενός τέτοιου m (με αυτήν την ιδιότητα) έπεται από το αξίωμα (**A 3**).

(iii) Η συνεπαγωγή "$\Rightarrow$" είναι αληθής λόγω τού αξιώματος (**A 2**). Εάν $n \in \mathbb{N} \setminus \theta(\mathbb{N})$, τότε ο n είναι αδύνατον να ανήκει στο $\mathbb{N} \setminus \{1\}$ (διότι, σύμφωνα με την ιδιότητα (ii), $n \in \theta(\mathbb{N})$ για κάθε $n \in \mathbb{N} \setminus \{1\}$). Ως εκ τούτου, και λαμβανομένου υπ' όψιν τού αξιώματος (**A 2**), έχουμε κατ' ανάγκην $n = 1$. Αυτό επαληθεύει και την αντίστροφη συνεπαγωγή "$\Leftarrow$". □

▸ **Οι συνήθεις εσωτερικές πράξεις επί τού** $\mathbb{N}$. Εν συνεχεία, πρόθεσή μας είναι να ορίσουμε αυστηρώς τα *αθροίσματα*, *γινόμενα* και *δυνάμεις* φυσικών αριθμών, και να αποδείξουμε τις κύριες ιδιότητές τους.

1.6.13 Πρόταση. *Υφίσταται μία και μόνον απεικόνιση* $\alpha : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ *η οποία ικανοποιεί τις ακόλουθες συνθήκες*:
(i) $\alpha(n, 1) = \theta(n), \forall n \in \mathbb{N}$.
(ii) $\alpha(n, \theta(m)) = \theta(\alpha(n, m)), \forall (n, m) \in \mathbb{N} \times \mathbb{N}$.

Απόδειξη. Έστω τυχών $n \in \mathbb{N}$. Εφαρμόζοντας το θεώρημα 1.6.8 (για τα $B = \mathbb{N}$, $b = \theta(n)$ και $\psi = \theta$) κατασκευάζουμε τη (μοναδική) απεικόνιση $\alpha_n : \mathbb{N} \longrightarrow \mathbb{N}$ με

$$\alpha_n(1) = \theta(n), \quad \alpha_n(\theta(m)) = \theta(\alpha_n(m)), \;\; \forall m \in \mathbb{N}.$$

Ύπαρξη τής α. Ορίζουμε την $\alpha : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ μέσω τού τύπου

$$\alpha(n, m) := \alpha_n(m), \;\; \forall (n, m) \in \mathbb{N} \times \mathbb{N}.$$

Αυτή είναι καλώς ορισμένη απεικόνιση, διότι εάν υπήρχε κάποιο διατεταγμένο ζεύγος $(n,m)\in\mathbb{N}\times\mathbb{N}$ με

$$\alpha\,(n,m)=l_1\ \text{ και }\ \alpha\,(n,m)=l_2$$

όπου $l_1,l_2\in\mathbb{N}$, $l_1\neq l_2$, τότε θα έπρεπε να ισχύει $\alpha_n(m)=l_1\neq l_2=\alpha_n(m)$, ήτοι κάτι που θα αντέφασκε προς το γεγονός ότι η α_n είναι (εκ κατασκευής) μια απεικόνιση. Προφανώς,

$$\alpha(n,1)=\alpha_n(1)=\theta\,(n)\,,\ \forall n\in\mathbb{N}$$

και

$$\alpha(n,\theta\,(m))=\ \alpha_n(\theta\,(m))=\theta\,(\alpha_n\,(m))=\theta\,(\alpha\,(n,m))\,,\ \forall(n,m)\in\mathbb{N}\times\mathbb{N},$$

οπότε η α πληροί τις (i) και (ii).

Μοναδικότητα τής α. Ας υποθέσουμε ότι υπάρχει κάποια άλλη απεικόνιση

$$\alpha':\mathbb{N}\times\mathbb{N}\longrightarrow\mathbb{N}$$

που πληροί τις (i) και (ii). Έστω τυχών $n\in\mathbb{N}$. Θέτοντας

$$U_n:=\left\{m\in\mathbb{N}\,|\,\alpha\,(n,m)=\alpha'\,(n,m)\right\}$$

παρατηρούμε ότι

$$\alpha(n,1)=\theta\,(n)=\alpha'(n,1)\Longrightarrow 1\in U_n.$$

Επιπροσθέτως, για κάθε $m\in U_n$ έχουμε

$$\alpha(n,\theta\,(m))=\theta\,(\alpha\,(n,m))=\theta\left(\alpha'\,(n,m)\right)=\alpha'(n,\theta\,(m))\Rightarrow\theta\,(m)\in U_n.$$

Κατά το αξίωμα (**A 4**), $U_n=\mathbb{N}$, οπότε $\alpha=\alpha'$. □

1.6.14 Ορισμός. Η εσωτερική πράξη $\alpha:\mathbb{N}\times\mathbb{N}\longrightarrow\mathbb{N}$ η ορισθείσα επί τού $\mathbb{N}$ μέσω τής προτάσεως 1.6.13 καλείται **πρόσθεση**[30] **(των φυσικών αριθμών)**. Για διευκόλυνσή μας (πρβλ. 1.5.17) θα συμβολίζουμε εφεξής την εικόνα $\alpha(n,m)$ οιουδήποτε διατεταγμένου ζεύγους $(n,m)\in\mathbb{N}\times\mathbb{N}$ μέσω τής α απλώς ως $n+_{\mathbb{N}}m$. (Το $n+_{\mathbb{N}}m$ καλείται, ιδιαιτέρως, **άθροισμα** των n και m.)

1.6.15 Πρόταση (Ιδιότητες προσθέσεως). *Η πρόσθεση φυσικών αριθμών έχει τις εξής ιδιότητες*:

(i) $\theta(n)=n+_{\mathbb{N}}1,\ \forall n\in\mathbb{N}$.

(ii) $n+_{\mathbb{N}}(m+_{\mathbb{N}}1)=(n+_{\mathbb{N}}m)+_{\mathbb{N}}1,\ \forall(n,m)\in\mathbb{N}\times\mathbb{N}$.

(iii) $1+_{\mathbb{N}}n=n+_{\mathbb{N}}1,\ \forall n\in\mathbb{N}$.

(iv) $(m+_{\mathbb{N}}1)+_{\mathbb{N}}n=(m+_{\mathbb{N}}n)+_{\mathbb{N}}1,\ \forall(n,m)\in\mathbb{N}\times\mathbb{N}$.

(v) **[Μεταθετική ιδιότητα]** $m+_{\mathbb{N}}n=n+_{\mathbb{N}}m,\ \forall(n,m)\in\mathbb{N}\times\mathbb{N}$.

(vi) **[Προσεταιριστική ιδιότητα]** *Για οιουσδήποτε* $m,n,k\in\mathbb{N}$ *ισχύει η ισότητα*

$$(m+_{\mathbb{N}}n)+_{\mathbb{N}}k=m+_{\mathbb{N}}(n+_{\mathbb{N}}k)\,.$$

(vii) $n\neq n+_{\mathbb{N}}m,\ \forall(n,m)\in\mathbb{N}\times\mathbb{N}$.

[30] Στην ιδέα που οδήγησε στον ορισμό τής απεικονίσεως α ως *προσθέσεως* περιλαμβάνεται η διαπίστωση τού ότι οι χαρακτηριστικές ιδιότητες τής α (βλ. 1.6.13 (i) και (ii)), οι οποίες αναδιατυπώνονται μέσω πιο εύληπτου συμβολισμού στα (i) και (ii) τής προτάσεως 1.6.15, είναι ακριβώς εκείνες που μας επιτρέπουν (σε συνδυασμό με το αξίωμα (**A 4**)) να αποδεικνύουμε *όλες τις άλλες* ιδιότητες (που έχει η «οικεία» μας «πρόσθεση», όπως αυτή γίνεται αντιληπτή και χρησιμοποιείται με αυτόματο τρόπο στο σχολείο). Εννοείται ότι, κατ' αντιστοιχίαν, ανάλογοι σχολιασμοί μπορούν να γίνουν και για τους ορισμούς των απεικονίσεων β και γ που ακολουθούν.

(viii) **[Νόμος τής διαγραφής**[31]**]** *Για οιουσδήποτε* $m, n, k \in \mathbb{N}$ *ισχύει η συνεπαγωγή*

$$n +_{\mathbb{N}} k = n +_{\mathbb{N}} m \Longrightarrow k = m.$$

Αποδειξη. Οι ιδιότητες (i) και (ii) αποτελούν αναδιατυπώσεις των συνθηκών (i) και (ii) τής προτάσεως 1.6.13 (που ικανοποιούνται από την εσωτερική πράξη τής προσθέσεως).

(iii) Έστω $U := \{ n \in \mathbb{N} \mid 1 +_{\mathbb{N}} n = n +_{\mathbb{N}} 1 \}$. Προφανώς, $1 \in U$. Έστω τυχών $n \in U$. Τότε

$$\begin{aligned} 1 +_{\mathbb{N}} \theta(n) &= 1 +_{\mathbb{N}} (n +_{\mathbb{N}} 1) \quad \text{(λόγω τής ιδιότητας (i))} \\ &= (1 +_{\mathbb{N}} n) +_{\mathbb{N}} 1 \quad \text{(λόγω τής ιδιότητας (ii))} \\ &= (n +_{\mathbb{N}} 1) +_{\mathbb{N}} 1 \quad \text{(επειδή } n \in U\text{)} \\ &= \theta(n) +_{\mathbb{N}} 1 \quad \text{(λόγω τής ιδιότητας (i)),} \end{aligned}$$

οπότε $\theta(n) \in U$. Από το αξίωμα (**A 4**) έπεται ότι $U = \mathbb{N}$.

(iv) Για κάθε $m \in \mathbb{N}$ ορίζουμε το σύνολο

$$U_m := \{ n \in \mathbb{N} \mid (m +_{\mathbb{N}} 1) +_{\mathbb{N}} n = (m +_{\mathbb{N}} n) +_{\mathbb{N}} 1 \}.$$

Προφανώς, $1 \in U_m,\ \forall m \in \mathbb{N}$. Εν συνεχεία, θεωρούμε τυχόν διατεταγμένο ζεύγος $(n, m) \in \mathbb{N} \times \mathbb{N}$ με $n \in U_m$ και παρατηρούμε ότι

$$\begin{aligned} (m +_{\mathbb{N}} 1) +_{\mathbb{N}} \theta(n) &= (m +_{\mathbb{N}} 1) +_{\mathbb{N}} (n +_{\mathbb{N}} 1) \quad \text{(λόγω τής ιδιότητας (i))} \\ &= ((m +_{\mathbb{N}} 1) +_{\mathbb{N}} n) +_{\mathbb{N}} 1 \quad \text{(λόγω τής ιδιότητας (ii))} \\ &= ((m +_{\mathbb{N}} n) +_{\mathbb{N}} 1) +_{\mathbb{N}} 1 \quad \text{(επειδή } n \in U_m\text{)} \\ &= (m +_{\mathbb{N}} (n +_{\mathbb{N}} 1)) +_{\mathbb{N}} 1 \quad \text{(λόγω τής ιδιότητας (ii))} \\ &= (m +_{\mathbb{N}} \theta(n)) +_{\mathbb{N}} 1 \quad \text{(λόγω τής ιδιότητας (i)).} \end{aligned}$$

Άρα $\theta(n) \in U_m,\ \forall m \in \mathbb{N}$. Από το αξίωμα (**A 4**) έπεται ότι $U_m = \mathbb{N},\ \forall m \in \mathbb{N}$.

(v) Για κάθε $m \in \mathbb{N}$ ορίζουμε το σύνολο

$$U_m := \{ n \in \mathbb{N} \mid m +_{\mathbb{N}} n = n +_{\mathbb{N}} m \}.$$

Σύμφωνα με την ήδη επαληθευθείσα ιδιότητα (iii), $1 \in U_m,\ \forall m \in \mathbb{N}$. Εν συνεχεία θεωρούμε τυχόν διατεταγμένο ζεύγος $(n, m) \in \mathbb{N} \times \mathbb{N}$ με $n \in U_m$ και παρατηρούμε ότι

$$\begin{aligned} m +_{\mathbb{N}} \theta(n) &= m +_{\mathbb{N}} (n +_{\mathbb{N}} 1) \quad \text{(λόγω τής ιδιότητας (i))} \\ &= (m +_{\mathbb{N}} n) +_{\mathbb{N}} 1 \quad \text{(λόγω τής ιδιότητας (ii))} \\ &= (n +_{\mathbb{N}} m) +_{\mathbb{N}} 1 \quad \text{(επειδή } n \in U_m\text{)} \\ &= (n +_{\mathbb{N}} 1) +_{\mathbb{N}} m \quad \text{(λόγω τής ιδιότητας (iv))} \\ &= \theta(n) +_{\mathbb{N}} m \quad \text{(λόγω τής ιδιότητας (i)).} \end{aligned}$$

Άρα $\theta(n) \in U_m,\ \forall m \in \mathbb{N}$. Από το αξίωμα (**A 4**) έπεται ότι $U_m = \mathbb{N},\ \forall m \in \mathbb{N}$.

(vi) Για κάθε $(m, n) \in \mathbb{N} \times \mathbb{N}$ ορίζουμε το σύνολο

$$U_{(m,n)} := \{ k \in \mathbb{N} \mid (m +_{\mathbb{N}} n) +_{\mathbb{N}} k = m +_{\mathbb{N}} (n +_{\mathbb{N}} k) \}.$$

[31] Εναλλακτικώς, ο *νόμος τής διαγραφής* συναντάται στη βιβλιογραφία και ως *νόμος* (ή *κανόνας*) τής *απαλοιφής* (ή τής *απλοποιήσεως*).

Λόγω τής ιδιότητας (ii) έχουμε $1 \in U_{(m,n)},\ \forall (m,n) \in \mathbb{N} \times \mathbb{N}$. Για οιουσδήποτε $(m,n) \in \mathbb{N} \times \mathbb{N}$ και $k \in U_{(m,n)}$ έχουμε

$$\begin{aligned}
&(m +_{\mathbb{N}} n) +_{\mathbb{N}} \theta(k) = (m +_{\mathbb{N}} n) +_{\mathbb{N}} (k +_{\mathbb{N}} 1) \ \text{(λόγω τής ιδιότητας (i))}\\
&= ((m +_{\mathbb{N}} n) +_{\mathbb{N}} k) +_{\mathbb{N}} 1 \ \text{(λόγω τής ιδιότητας (ii))}\\
&= (m +_{\mathbb{N}} (n +_{\mathbb{N}} k)) +_{\mathbb{N}} 1 \ \text{(επειδή } k \in U_{(m,n)}\text{)}\\
&= m +_{\mathbb{N}} ((n +_{\mathbb{N}} k) +_{\mathbb{N}} 1) \ \text{(λόγω τής ιδιότητας (ii))}\\
&= m +_{\mathbb{N}} (n +_{\mathbb{N}} (k +_{\mathbb{N}} 1)) \ \text{(λόγω τής ιδιότητας (ii))}\\
&= m +_{\mathbb{N}} (n +_{\mathbb{N}} \theta(k)) \ \text{(λόγω τής ιδιότητας (i))}.
\end{aligned}$$

Κατά συνέπειαν, $\theta(k) \in U_{(m,n)},\ \forall (m,n) \in \mathbb{N} \times \mathbb{N}$. Από το αξίωμα (**A 4**) έπεται ότι

$$U_{(m,n)} = \mathbb{N},\ \forall (m,n) \in \mathbb{N} \times \mathbb{N}.$$

(vii) Για κάθε $m \in \mathbb{N}$ ορίζουμε το σύνολο $U_m := \{ n \in \mathbb{N} \mid n \neq n +_{\mathbb{N}} m \}$. Σύμφωνα με το αξίωμα (**A 2**) και την ιδιότητα (i),

$$1 \neq \theta(m) = m +_{\mathbb{N}} 1 \Rightarrow 1 \in U_m,\ \forall m \in \mathbb{N}.$$

Εν συνεχεία, θεωρούμε τυχόν διατεταγμένο ζεύγος $(n,m) \in \mathbb{N} \times \mathbb{N}$ με $n \in U_m$ και παρατηρούμε ότι $\theta(n) \neq \theta(n +_{\mathbb{N}} m)$ (διότι $n \neq n +_{\mathbb{N}} m$ και κατά το αξίωμα (**A 3**) η θ είναι μια ένριψη.) Επιπροσθέτως,

$$\begin{aligned}
&\theta(n +_{\mathbb{N}} m) = (m +_{\mathbb{N}} n) +_{\mathbb{N}} 1 \ \text{(λόγω τής ιδιότητας (i))}\\
&= m +_{\mathbb{N}} (n +_{\mathbb{N}} 1) \ \text{(λόγω τής ιδιότητας (ii))}\\
&= (n +_{\mathbb{N}} 1) +_{\mathbb{N}} m \ \text{(λόγω τής ιδιότητας (v))}\\
&= \theta(n) +_{\mathbb{N}} m \ \text{(λόγω τής ιδιότητας (i))}.
\end{aligned}$$

Άρα $\theta(n) \in U_m,\ \forall m \in \mathbb{N}$. Από το αξίωμα (**A 4**) έπεται ότι $U_m = \mathbb{N},\ \forall m \in \mathbb{N}$.

(viii) Έστω $U := \left\{ n \in \mathbb{N} \;\middle|\; \begin{array}{c} \text{για οιουσδήποτε } k,m \in \mathbb{N} \\ \text{ισχύει η συνεπαγωγή} \\ n +_{\mathbb{N}} k = n +_{\mathbb{N}} m \Longrightarrow k = m \end{array} \right\}$. Εάν $k,m \in \mathbb{N}$ με $1 +_{\mathbb{N}} k = 1 +_{\mathbb{N}} m$, τότε

$$1 +_{\mathbb{N}} k \underset{\text{(v)}}{=} k +_{\mathbb{N}} 1 \underset{\text{(i)}}{=} \theta(k) = \theta(m) \underset{\text{(i)}}{=} m +_{\mathbb{N}} 1 \underset{\text{(v)}}{=} 1 +_{\mathbb{N}} m,$$

οπότε $k = m$ (λόγω τού αξιώματος (**A 3**)). Αυτό σημαίνει ότι $1 \in U$. Εξάλλου, εάν ο n δηλοί τυχόν στοιχείο τού U και $k,m \in \mathbb{N}$ είναι τέτοιοι ώστε να ισχύει η ισότητα

$$\theta(n) +_{\mathbb{N}} k = \theta(n) +_{\mathbb{N}} m,$$

τότε

$$\begin{aligned}
&(n +_{\mathbb{N}} 1) +_{\mathbb{N}} k = (n +_{\mathbb{N}} 1) +_{\mathbb{N}} m \ \text{(λόγω τής ιδιότητας (i))}\\
\Longrightarrow\ &k +_{\mathbb{N}} (n +_{\mathbb{N}} 1) = m +_{\mathbb{N}} (n +_{\mathbb{N}} 1) \ \text{(λόγω τής ιδιότητας (v))}\\
\Longrightarrow\ &(k +_{\mathbb{N}} n) +_{\mathbb{N}} 1 = (m +_{\mathbb{N}} n) +_{\mathbb{N}} 1 \ \text{(λόγω τής ιδιότητας (ii))}\\
\Longrightarrow\ &\theta(k +_{\mathbb{N}} n) = \theta(m +_{\mathbb{N}} n) \ \text{(λόγω τής ιδιότητας (i))}\\
\Longrightarrow\ &k +_{\mathbb{N}} n = m +_{\mathbb{N}} n \ \text{(λόγω τού αξιώματος (A3))}\\
\Longrightarrow\ &n +_{\mathbb{N}} k = n +_{\mathbb{N}} m \ \text{(λόγω τής ιδιότητας (v))}\\
\Longrightarrow\ &k = m \ \text{(επειδή } n \in U\text{)}\\
\Longrightarrow\ &\theta(n) \in U \ \text{(εξ ορισμού)}.
\end{aligned}$$

Εκ νέου χρήση τού αξιώματος (**A 4**) μας οδηγεί στο ότι $U = \mathbb{N}$. □

1.6.16 Πρόταση. *Υφίσταται μία και μόνον απεικόνιση* $\beta : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ *η οποία ικανοποιεί τις ακόλουθες συνθήκες*:
(i) $\beta(n,1) = n,\ \forall n \in \mathbb{N}$.
(ii) $\beta(n,\theta(m)) = \alpha(n,\beta(n,m)),\ \forall (n,m) \in \mathbb{N} \times \mathbb{N}$,
όπου $\alpha : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ *η πράξη τής προσθέσεως* (βλ. 1.6.13, 1.6.14).

Απόδειξη. Έστω τυχών $n \in \mathbb{N}$. Εφαρμόζοντας το θεώρημα 1.6.8 (για $B = \mathbb{N}, b = n$ και την $\psi = \alpha_n$ την ορισθείσα στην απόδειξη τής προτάσεως 1.6.13) κατασκευάζουμε τη (μοναδική) απεικόνιση $\beta_n : \mathbb{N} \longrightarrow \mathbb{N}$ με

$$\beta_n(1) = n, \quad \beta_n(\theta(m)) = \alpha_n(\beta_n(m)),\ \forall m \in \mathbb{N}.$$

Ύπαρξη τής β. Ορίζουμε την $\beta : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ μέσω τού τύπου

$$\beta(n,m) := \beta_n(m),\ \forall (n,m) \in \mathbb{N} \times \mathbb{N}.$$

Αυτή είναι καλώς ορισμένη απεικόνιση, διότι εάν υπήρχε κάποιο διατεταγμένο ζεύγος $(n,m) \in \mathbb{N} \times \mathbb{N}$ με

$$\beta(n,m) = l_1 \ \text{ και } \ \beta(n,m) = l_2$$

όπου $l_1, l_2 \in \mathbb{N}$, $l_1 \neq l_2$, τότε θα έπρεπε να ισχύει $\beta_n(m) = l_1 \neq l_2 = \beta_n(m)$, ήτοι κάτι που θα αντέφασκε προς το γεγονός ότι η β_n είναι (εκ κατασκευής) μια απεικόνιση. Προφανώς, $\beta(n,1) = \beta_n(1) = n,\ \forall n \in \mathbb{N}$ και

$$\begin{aligned} \beta(n,\theta(m)) &= \beta_n(\theta(m)) = \alpha_n(\beta_n(m)) \\ &= \alpha(n,\beta_n(m)) = \alpha(n,\beta(n,m)),\ \forall (n,m) \in \mathbb{N} \times \mathbb{N}, \end{aligned}$$

οπότε η β πληροί τις (i) και (ii).
Μοναδικότητα τής β. Ας υποθέσουμε ότι υπάρχει κάποια άλλη απεικόνιση

$$\beta' : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

που πληροί τις (i) και (ii). Έστω τυχών $n \in \mathbb{N}$. Θέτοντας

$$U_n := \left\{ m \in \mathbb{N} \mid \beta(n,m) = \beta'(n,m) \right\}$$

παρατηρούμε ότι

$$\beta(n,1) = n = \beta'(n,1) \Longrightarrow 1 \in U_n.$$

Επιπροσθέτως, για κάθε $m \in U_n$ έχουμε

$$\beta(n,\theta(m)) = \alpha(n,\beta(n,m)) = \alpha\left(n,\beta'(n,m)\right) = \beta'(n,\theta(m)) \Rightarrow \theta(m) \in U_n.$$

Κατά το αξίωμα (**A 4**), $U_n = \mathbb{N}$, οπότε $\beta = \beta'$. □

1.6.17 Ορισμός. Η εσωτερική πράξη $\beta : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ η ορισθείσα επί τού $\mathbb{N}$ μέσω τής προτάσεως 1.6.16 καλείται **πολλαπλασιασμός (των φυσικών αριθμών)**. Για διευκόλυνσή μας (πρβλ. 1.5.17) θα συμβολίζουμε εφεξής την εικόνα $\beta(n,m)$ οιουδήποτε διατεταγμένου ζεύγους $(n,m) \in \mathbb{N} \times \mathbb{N}$ μέσω τής β απλώς ως $n \cdot_{\mathbb{N}} m$. (Το $n \cdot_{\mathbb{N}} m$ καλείται, ιδιαιτέρως, **γινόμενο** των n και m.)

1.6.18 Πρόταση (Ιδιότητες πολλαπλασιασμού). *Ο πολλαπλασιασμός φυσικών αριθμών έχει τις εξής ιδιότητες*:
(i) $n \cdot_{\mathbb{N}} 1 = n,\ \forall n \in \mathbb{N}$.
(ii) $n \cdot_{\mathbb{N}} (m +_{\mathbb{N}} 1) = (n \cdot_{\mathbb{N}} m) +_{\mathbb{N}} n,\ \forall (n,m) \in \mathbb{N} \times \mathbb{N}$.
(iii) $n \cdot_{\mathbb{N}} 1 = 1 \cdot_{\mathbb{N}} n,\ \forall n \in \mathbb{N}$.

(iv) $(m +_{\mathbb{N}} 1) \cdot_{\mathbb{N}} n = (m \cdot_{\mathbb{N}} n) +_{\mathbb{N}} n, \forall (n, m) \in \mathbb{N} \times \mathbb{N}$.

(v) **[Μεταθετική ιδιότητα]** $m \cdot_{\mathbb{N}} n = n \cdot_{\mathbb{N}} m, \forall (n, m) \in \mathbb{N} \times \mathbb{N}$.

(vi) **[Επιμεριστική ιδιότητα τού πολλαπλασιασμού ως προς την πρόσθεση]** *Για οιουσδήποτε* $m, n, k \in \mathbb{N}$ *ισχύει η ισότητα*

$$m \cdot_{\mathbb{N}} (n +_{\mathbb{N}} k) = (m \cdot_{\mathbb{N}} n) +_{\mathbb{N}} (m \cdot_{\mathbb{N}} k) .$$

(vii) **[Προσεταιριστική ιδιότητα]** *Για οιουσδήποτε* $m, n, k \in \mathbb{N}$ *ισχύει η ισότητα*

$$(m \cdot_{\mathbb{N}} n) \cdot_{\mathbb{N}} k = m \cdot_{\mathbb{N}} (n \cdot_{\mathbb{N}} k) .$$

Απόδειξη. Οι ιδιότητες (i) και (ii) αποτελούν αναδιατυπώσεις των συνθηκών (i) και (ii) τής προτάσεως 1.6.16 που ικανοποιούνται από την εσωτερική πράξη τού πολλαπλασιασμού (όπου στη δεύτερη έχει ληφθεί υπ' όψιν και η ιδιότητα (i) τής προτάσεως 1.6.15).

(iii) Έστω $U := \{ n \in \mathbb{N} \mid n \cdot_{\mathbb{N}} 1 = 1 \cdot_{\mathbb{N}} n \}$. Προφανώς, $1 \in U$. Έστω τυχών $n \in U$. Τότε

$$\theta (n) \cdot_{\mathbb{N}} 1 = \theta (n) \quad \text{(λόγω τής ιδιότητας (i))}$$

$$= n +_{\mathbb{N}} 1 = (n \cdot_{\mathbb{N}} 1) +_{\mathbb{N}} 1 \quad \text{(λόγω τής ιδιότητας (i))}$$

$$= (1 \cdot_{\mathbb{N}} n) +_{\mathbb{N}} 1 \quad \text{(επειδή } n \in U\text{)}$$

$$= 1 \cdot_{\mathbb{N}} (n +_{\mathbb{N}} 1) = 1 \cdot_{\mathbb{N}} \theta (n) \quad \text{(λόγω τής ιδιότητας (ii)),}$$

οπότε $\theta (n) \in U$. Από το αξίωμα (**A 4**) έπεται ότι $U = \mathbb{N}$.

(iv) Για κάθε $m \in \mathbb{N}$ ορίζουμε το σύνολο

$$U_m := \{ n \in \mathbb{N} \mid (m +_{\mathbb{N}} 1) \cdot_{\mathbb{N}} n = (m \cdot_{\mathbb{N}} n) +_{\mathbb{N}} n \} .$$

Σύμφωνα με την ιδιότητα (i),

$$(m +_{\mathbb{N}} 1) \cdot_{\mathbb{N}} 1 = m +_{\mathbb{N}} 1 = (m \cdot_{\mathbb{N}} 1) +_{\mathbb{N}} 1 \Rightarrow 1 \in U_m, \ \forall m \in \mathbb{N}.$$

Εν συνεχεία θεωρούμε τυχόν διατεταγμένο ζεύγος $(n, m) \in \mathbb{N} \times \mathbb{N}$ με $n \in U_m$ και παρατηρούμε ότι

$$(m +_{\mathbb{N}} 1) \cdot_{\mathbb{N}} \theta (n) = (m +_{\mathbb{N}} 1) \cdot_{\mathbb{N}} (n +_{\mathbb{N}} 1) \quad \text{(λόγω τής 1.6.15 (i))}$$

$$= (m +_{\mathbb{N}} 1) \cdot_{\mathbb{N}} n +_{\mathbb{N}} (m +_{\mathbb{N}} 1) \quad \text{(λόγω τής ιδιότητας (ii))}$$

$$= (m \cdot_{\mathbb{N}} n) +_{\mathbb{N}} n +_{\mathbb{N}} m +_{\mathbb{N}} 1 \quad \text{(επειδή } n \in U_m\text{)}$$

$$= (m \cdot_{\mathbb{N}} n) +_{\mathbb{N}} m +_{\mathbb{N}} n +_{\mathbb{N}} 1 \text{ (λόγω τής 1.6.15 (v))}$$

$$= m \cdot_{\mathbb{N}} (n +_{\mathbb{N}} 1) +_{\mathbb{N}} (n +_{\mathbb{N}} 1) \quad \text{(λόγω τής ιδιότητας (ii))}$$

$$= (m \cdot_{\mathbb{N}} \theta (n)) +_{\mathbb{N}} \theta (n) \quad \text{(λόγω τής 1.6.15 (i)).}$$

Άρα $\theta (n) \in U_m, \ \forall m \in \mathbb{N}$. Από το αξίωμα (**A 4**) έπεται ότι $U_m = \mathbb{N}, \ \forall m \in \mathbb{N}$.

(v) Για κάθε $m \in \mathbb{N}$ ορίζουμε το σύνολο

$$U_m := \{ n \in \mathbb{N} \mid m \cdot_{\mathbb{N}} n = n \cdot_{\mathbb{N}} m \} .$$

Σύμφωνα με την ήδη επαληθευθείσα ιδιότητα (iii), $1 \in U_m, \ \forall m \in \mathbb{N}$. Εν συνεχεία θεωρούμε τυχόν διατεταγμένο ζεύγος $(n, m) \in \mathbb{N} \times \mathbb{N}$ με $n \in U_m$ και παρατηρούμε ότι

$$m \cdot_{\mathbb{N}} \theta (n) = m \cdot_{\mathbb{N}} (n +_{\mathbb{N}} 1) \quad \text{(λόγω τής 1.6.15 (i))}$$

$$= (m \cdot_{\mathbb{N}} n) +_{\mathbb{N}} m \quad \text{(λόγω τής ιδιότητας (iv))}$$

$$= (n \cdot_{\mathbb{N}} m) +_{\mathbb{N}} m \quad \text{(επειδή } n \in U_m\text{)}$$

$$= m \cdot_{\mathbb{N}} (n +_{\mathbb{N}} 1) \quad \text{(λόγω τής ιδιότητας (ii))}$$

$$= m \cdot_{\mathbb{N}} \theta (n) \quad \text{(λόγω τής 1.6.15 (i)).}$$

Άρα $\theta(n) \in U_m,\ \forall m \in \mathbb{N}$. Από το αξίωμα (**A 4**) έπεται ότι $U_m = \mathbb{N},\ \forall m \in \mathbb{N}$.
(vi) Για κάθε $(m,n) \in \mathbb{N} \times \mathbb{N}$ ορίζουμε το σύνολο

$$U_{(m,n)} := \{k \in \mathbb{N} \mid m \cdot_{\mathbb{N}} (n +_{\mathbb{N}} k) = (m \cdot_{\mathbb{N}} n) +_{\mathbb{N}} (m \cdot_{\mathbb{N}} k)\}.$$

Προφανώς,

$$\begin{aligned} & m \cdot_{\mathbb{N}} (n +_{\mathbb{N}} 1) = (m \cdot_{\mathbb{N}} n) +_{\mathbb{N}} m \ \text{(λόγω τής ιδιότητας (ii))} \\ & = (m \cdot_{\mathbb{N}} n) +_{\mathbb{N}} (m \cdot_{\mathbb{N}} 1) \ \text{(λόγω τής ιδιότητας (i))} \\ & \Rightarrow 1 \in U_{(m,n)},\ \forall (m,n) \in \mathbb{N} \times \mathbb{N}. \end{aligned}$$

Επιπροσθέτως, για οιουσδήποτε $(m,n) \in \mathbb{N} \times \mathbb{N}$ και $k \in U_{(m,n)}$ έχουμε

$$\begin{aligned} & m \cdot_{\mathbb{N}} (n +_{\mathbb{N}} \theta(k)) = m \cdot_{\mathbb{N}} (n +_{\mathbb{N}} (k +_{\mathbb{N}} 1)) \ \text{(λόγω τής 1.6.15 (i))} \\ & = m \cdot_{\mathbb{N}} ((n +_{\mathbb{N}} k) +_{\mathbb{N}} 1) \ \text{(λόγω τής 1.6.15 (vi))} \\ & = m \cdot_{\mathbb{N}} (n +_{\mathbb{N}} k) +_{\mathbb{N}} m \ \text{(λόγω τής ιδιότητας (ii))} \\ & = (m \cdot_{\mathbb{N}} n) +_{\mathbb{N}} (m \cdot_{\mathbb{N}} k) +_{\mathbb{N}} m \ \text{(επειδή } k \in U_{(m,n)}) \\ & = (m \cdot_{\mathbb{N}} n) +_{\mathbb{N}} (m \cdot_{\mathbb{N}} (k +_{\mathbb{N}} 1)) \ \text{(λόγω τής ιδιότητας (ii))} \\ & = (m \cdot_{\mathbb{N}} n) +_{\mathbb{N}} (m \cdot_{\mathbb{N}} \theta(k)) \ \text{(λόγω τής 1.6.15 (i)).} \end{aligned}$$

Κατά συνέπειαν, $\theta(k) \in U_{(m,n)},\ \forall (m,n) \in \mathbb{N} \times \mathbb{N}$. Από το αξίωμα (**A 4**) έπεται ότι

$$U_{(m,n)} = \mathbb{N},\ \forall (m,n) \in \mathbb{N} \times \mathbb{N}.$$

(vii) Για κάθε $(m,n) \in \mathbb{N} \times \mathbb{N}$ ορίζουμε το σύνολο

$$U_{(m,n)} := \{k \in \mathbb{N} \mid (m \cdot_{\mathbb{N}} n) \cdot_{\mathbb{N}} k = m \cdot_{\mathbb{N}} (n \cdot_{\mathbb{N}} k)\}.$$

Προφανώς,

$$\begin{aligned} & (m \cdot_{\mathbb{N}} n) \cdot_{\mathbb{N}} 1 = (m \cdot_{\mathbb{N}} n) \ \text{(λόγω τής ιδιότητας (i))} \\ & = m \cdot_{\mathbb{N}} (n \cdot_{\mathbb{N}} 1) \ \text{(λόγω τής ιδιότητας (i))} \\ & \Rightarrow 1 \in U_{(m,n)},\ \forall (m,n) \in \mathbb{N} \times \mathbb{N}. \end{aligned}$$

Επιπροσθέτως, για οιουσδήποτε $(m,n) \in \mathbb{N} \times \mathbb{N}$ και $k \in U_{(m,n)}$ έχουμε

$$\begin{aligned} & (m \cdot_{\mathbb{N}} n) \cdot_{\mathbb{N}} \theta(k) = (m \cdot_{\mathbb{N}} n) \cdot_{\mathbb{N}} (k +_{\mathbb{N}} 1) \ \text{(λόγω τής 1.6.15 (i))} \\ & = ((m \cdot_{\mathbb{N}} n) \cdot_{\mathbb{N}} k) +_{\mathbb{N}} (m \cdot_{\mathbb{N}} n) \ \text{(λόγω τής ιδιότητας (ii))} \\ & = (m \cdot_{\mathbb{N}} (n \cdot_{\mathbb{N}} k)) +_{\mathbb{N}} (m \cdot_{\mathbb{N}} n) \ \text{(επειδή } k \in U_{(m,n)}) \\ & = m \cdot_{\mathbb{N}} ((n \cdot_{\mathbb{N}} k) +_{\mathbb{N}} n) \ \text{(λόγω τής ιδιότητας (vi))} \\ & = m \cdot_{\mathbb{N}} (n \cdot_{\mathbb{N}} (k +_{\mathbb{N}} 1)) \ \text{(λόγω τής ιδιότητας (ii))} \\ & = m \cdot_{\mathbb{N}} (n \cdot_{\mathbb{N}} \theta(k)) \ \text{(λόγω τής 1.6.15 (i)).} \end{aligned}$$

Κατά συνέπειαν, $\theta(k) \in U_{(m,n)},\ \forall (m,n) \in \mathbb{N} \times \mathbb{N}$. Εκ νέου χρήση τού (**A 4**) μας οδηγεί στην ισότητα $U_{(m,n)} = \mathbb{N},\ \forall (m,n) \in \mathbb{N} \times \mathbb{N}$. □

1.6.19 Σημείωση. (i) Για την απόδειξη τής ισχύος τής επιμεριστικής ιδιότητας τού πολλαπλασιασμού "$\cdot_{\mathbb{N}}$" ως προς την πρόσθεση "$+_{\mathbb{N}}$" αρκεί ο έλεγχος τού ότι αυτός είναι εξ αριστερών επιμεριστικός, καθότι η πράξη "$\cdot_{\mathbb{N}}$", κατά το 1.6.18 (v), είναι μεταβατική (βλ. παρατήρηση 1.5.22).

(ii) Η πράξη " $+_{\mathbb{N}}$ ", παρότι είναι μεταθετική (βλ. 1.6.15 (v)), *δεν* είναι επιμεριστική ως προς τον πολλαπλασιασμό " $\cdot_{\mathbb{N}}$ ", διότι π.χ.

$$23 = 3 +_{\mathbb{N}} (5 \cdot_{\mathbb{N}} 4) \neq (3 +_{\mathbb{N}} 5) \cdot_{\mathbb{N}} (3 +_{\mathbb{N}} 4) = 56.$$

(iii) Κατά τα (i) και (v) τής προτάσεως 1.6.15 το 1 αποτελεί ουδέτερο στοιχείο ως προς τον πολλαπλασιασμό " $\cdot_{\mathbb{N}}$ ".

1.6.20 Πρόταση. *Υφίσταται μία και μόνον απεικόνιση* $\gamma : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ *η οποία ικανοποιεί τις ακόλουθες συνθήκες*:
(i) $\gamma(n, 1) = n, \forall n \in \mathbb{N}$.
(ii) $\gamma(n, \theta(m)) = \beta(n, \gamma(n, m)), \forall (n, m) \in \mathbb{N} \times \mathbb{N}$,
όπου $\beta : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ *η πράξη τού πολλαπλασιασμού* (βλ. 1.6.16, 1.6.17).

Απόδειξη. Έστω τυχών $n \in \mathbb{N}$. Εφαρμόζοντας το θεώρημα 1.6.8 (για $B = \mathbb{N}, b = n$ και την $\psi = \beta_n$ την ορισθείσα στην απόδειξη τής προτάσεως 1.6.16) κατασκευάζουμε τη (μοναδική) απεικόνιση $\gamma_n : \mathbb{N} \longrightarrow \mathbb{N}$ με

$$\gamma_n(1) = n, \quad \gamma_n(\theta(m)) = \beta_n(\gamma_n(m)), \ \forall m \in \mathbb{N}.$$

Ύπαρξη τής γ. Ορίζουμε την $\gamma : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ μέσω τού τύπου

$$\gamma(n, m) := \gamma_n(m), \ \forall (n, m) \in \mathbb{N} \times \mathbb{N}.$$

Αυτή είναι καλώς ορισμένη απεικόνιση, διότι εάν υπήρχε κάποιο διατεταγμένο ζεύγος $(n, m) \in \mathbb{N} \times \mathbb{N}$ με

$$\gamma(n, m) = l_1 \ \text{ και } \ \gamma(n, m) = l_2$$

όπου $l_1, l_2 \in \mathbb{N}$, $l_1 \neq l_2$, τότε θα έπρεπε να ισχύει $\gamma_n(m) = l_1 \neq l_2 = \gamma_n(m)$, ήτοι κάτι που θα αντέφασκε προς το γεγονός ότι η γ_n είναι (εκ κατασκευής) μια απεικόνιση. Προφανώς, $\gamma(n, 1) = \gamma_n(1) = n, \ \forall n \in \mathbb{N}$ και

$$\begin{aligned} \gamma(n, \theta(m)) &= \gamma_n(\theta(m)) = \beta_n(\gamma_n(m)) \\ &= \beta(n, \gamma_n(m)) = \beta(n, \gamma(n, m)), \ \forall (n, m) \in \mathbb{N} \times \mathbb{N}, \end{aligned}$$

οπότε η γ πληροί τις (i) και (ii).
Μοναδικότητα τής γ. Ας υποθέσουμε ότι υπάρχει κάποια άλλη απεικόνιση

$$\gamma' : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

που πληροί τις (i) και (ii). Έστω τυχών $n \in \mathbb{N}$. Θέτοντας

$$U_n := \{ m \in \mathbb{N} \mid \gamma(n, m) = \gamma'(n, m) \}$$

παρατηρούμε ότι

$$\gamma(n, 1) = n = \gamma'(n, 1) \Longrightarrow 1 \in U_n.$$

Επιπροσθέτως, για κάθε $m \in U_n$ έχουμε

$$\gamma(n, \theta(m)) = \beta(n, \gamma(n, m)) = \beta(n, \gamma'(n, m)) = \gamma'(n, \theta(m)) \Rightarrow \theta(m) \in U_n.$$

Κατά το αξίωμα (**A 4**), $U_n = \mathbb{N}$, οπότε $\gamma = \gamma'$. □

1.6.21 Ορισμός. Η εικόνα $\gamma(n,m)$ οιουδήποτε $(n,m) \in \mathbb{N}\times\mathbb{N}$ μέσω τής εσωτερικής πράξεως $\gamma : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$ τής ορισθείσας επί τού $\mathbb{N}$ στην πρόταση 1.6.20 θα συμβολίζεται εφεξής ως n^m. Επίσης, θα λέμε ότι ο n^m είναι ο n **υψωμένος στη δύναμη** m (και ότι ο n^m έχει τον m ως **εκθέτη του**).

1.6.22 Πρόταση (Ιδιότητες δυνάμεων). *Οι δυνάμεις φυσικών αριθμών έχουν τις εξής ιδιότητες*:

(i) $n^1 = n,\ \forall n \in \mathbb{N}$.

(ii) $n^{\theta(m)} = n^{m+_{\mathbb{N}}1} = n^m \cdot_{\mathbb{N}} n,\ \forall (n,m) \in \mathbb{N}\times\mathbb{N}$.

(iii) $1^n = 1,\ \forall n \in \mathbb{N}$.

(iv) *Για οιουσδήποτε* $m,n,k \in \mathbb{N}$ *ισχύει η ισότητα*

$$n^m \cdot_{\mathbb{N}} n^k = n^{m+_{\mathbb{N}}k}.$$

(v) *Για οιουσδήποτε* $m,n,k \in \mathbb{N}$ *ισχύει η ισότητα*

$$(n^m)^k = n^{m\cdot_{\mathbb{N}}k}.$$

(vi) *Για οιουσδήποτε* $m,n,k \in \mathbb{N}$ *ισχύει η ισότητα*

$$(n \cdot_{\mathbb{N}} m)^k = n^k \cdot_{\mathbb{N}} m^k.$$

Απόδειξη. Οι ιδιότητες (i) και (ii) αποτελούν αναδιατυπώσεις των συνθηκών (i) και (ii) τής προτάσεως 1.6.20 (όπου στη δεύτερη έχει ληφθεί υπ' όψιν και η ιδιότητα (v) τής προτάσεως 1.6.18).

(iii) Έστω $U := \{\, n \in \mathbb{N} \mid 1^n = 1 \,\}$. Λόγω τής ιδιότητας (i), $1 \in U$. Έστω τυχών $n \in U$. Τότε

$$\begin{aligned} 1^{\theta(n)} = 1^{(n+_{\mathbb{N}}1)} &= 1^n \cdot_{\mathbb{N}} 1 \ \text{ (λόγω τής ιδιότητας (ii))} \\ &= 1 \cdot_{\mathbb{N}} 1 \ \text{ (επειδή } n \in U\text{)} \\ &= 1 \ \text{ (λόγω τής 1.6.18 (i)),} \end{aligned}$$

οπότε $\theta\,(n) \in U$. Από το αξίωμα (**A 4**) έπεται ότι $U = \mathbb{N}$.

(iv) Για κάθε $(m,n) \in \mathbb{N}\times\mathbb{N}$ ορίζουμε το σύνολο

$$U_{(m,n)} := \left\{\, k \in \mathbb{N} \mid n^m \cdot_{\mathbb{N}} n^k = n^{m+_{\mathbb{N}}k} \right\}.$$

Προφανώς,

$$\begin{aligned} n^m \cdot_{\mathbb{N}} n^1 &= n^m \cdot_{\mathbb{N}} n \ \text{ (λόγω τής ιδιότητας (i))} \\ &= n^{m+_{\mathbb{N}}1} \ \text{ (λόγω τής ιδιότητας (ii))} \\ &\Rightarrow 1 \in U_{(m,n)},\ \forall (m,n) \in \mathbb{N}\times\mathbb{N}. \end{aligned}$$

Επιπροσθέτως, για οιουσδήποτε $(m,n) \in \mathbb{N}\times\mathbb{N}$ και $k \in U_{(m,n)}$ έχουμε

$$\begin{aligned} n^m \cdot_{\mathbb{N}} n^{\theta(k)} &= n^m \cdot_{\mathbb{N}} n^{k+_{\mathbb{N}}1} \ \text{ (λόγω τής 1.6.15 (i))} \\ &= n^m \cdot_{\mathbb{N}} n^k \cdot_{\mathbb{N}} n \ \text{ (λόγω τής ιδιότητας (ii))} \\ &= n^{m+_{\mathbb{N}}k} \cdot_{\mathbb{N}} n \ \text{ (επειδή } k \in U_{(m,n)}\text{)} \\ &= n^{m+_{\mathbb{N}}k+_{\mathbb{N}}1} \ \text{ (λόγω τής ιδιότητας (ii))} \\ &= n^{m+_{\mathbb{N}}\theta(k)} \ \text{ (λόγω τής 1.6.15 (i)).} \end{aligned}$$

Κατά συνέπειαν, $\theta\,(k) \in U_{(m,n)},\ \forall (m,n) \in \mathbb{N}\times\mathbb{N}$. Από το αξίωμα (**A 4**) έπεται ότι

$$U_{(m,n)} = \mathbb{N},\ \forall (m,n) \in \mathbb{N}\times\mathbb{N}.$$

(v) Για κάθε $(m,n)\in\mathbb{N}\times\mathbb{N}$ ορίζουμε το σύνολο

$$U_{(m,n)}:=\left\{k\in\mathbb{N}\mid (n^m)^k=n^{m\cdot_{\mathbb{N}}k}\right\}.$$

Προφανώς,

$$\begin{aligned}&(n^m)^1=n^m\ \text{(λόγω της ιδιότητας (i))}\\&=n^{m\cdot_{\mathbb{N}}1}\ \text{(λόγω της 1.6.18 (i))}\\&\Rightarrow 1\in U_{(m,n)},\ \forall(m,n)\in\mathbb{N}\times\mathbb{N}.\end{aligned}$$

Επιπροσθέτως, για οιουσδήποτε $(m,n)\in\mathbb{N}\times\mathbb{N}$ και $k\in U_{(m,n)}$ έχουμε

$$\begin{aligned}&(n^m)^{\theta(k)}=(n^m)^{k+_{\mathbb{N}}1}\ \text{(λόγω της 1.6.15 (i))}\\&=(n^m)^k\cdot_{\mathbb{N}}(n^m)^1\ \text{(λόγω της ιδιότητας (iv))}\\&=n^{m\cdot_{\mathbb{N}}k}\cdot_{\mathbb{N}}(n^m)^1\ \text{(επειδή } k\in U_{(m,n)})\\&=n^{m\cdot_{\mathbb{N}}k}\cdot_{\mathbb{N}}n^m\ \text{(λόγω της ιδιότητας (i))}\\&=n^{(m\cdot_{\mathbb{N}}k)+_{\mathbb{N}}m}\ \text{(λόγω της ιδιότητας (iv))}\\&=n^{m\cdot_{\mathbb{N}}(k+_{\mathbb{N}}1)}\ \text{(λόγω της 1.6.18 (ii))}\\&=n^{m\cdot_{\mathbb{N}}\theta(k)}\ \text{(λόγω της 1.6.15 (i)).}\end{aligned}$$

Κατά συνέπειαν, $\theta(k)\in U_{(m,n)},\ \forall(m,n)\in\mathbb{N}\times\mathbb{N}$. Από το αξίωμα (**A 4**) έπεται ότι

$$U_{(m,n)}=\mathbb{N},\ \forall(m,n)\in\mathbb{N}\times\mathbb{N}.$$

(vi) Για κάθε $(m,n)\in\mathbb{N}\times\mathbb{N}$ ορίζουμε το σύνολο

$$U_{(m,n)}:=\left\{k\in\mathbb{N}\mid (n\cdot_{\mathbb{N}}m)^k=n^k\cdot_{\mathbb{N}}m^k\right\}.$$

Προφανώς,

$$\begin{aligned}&(n\cdot_{\mathbb{N}}m)^1=n\cdot_{\mathbb{N}}m\ \text{(λόγω της ιδιότητας (i))}\\&=n^1\cdot_{\mathbb{N}}m^1\ \text{(και πάλι λόγω της ιδιότητας (i))}\\&\Rightarrow 1\in U_{(m,n)},\ \forall(m,n)\in\mathbb{N}\times\mathbb{N}.\end{aligned}$$

Επιπροσθέτως, για οιουσδήποτε $(m,n)\in\mathbb{N}\times\mathbb{N}$ και $k\in U_{(m,n)}$ έχουμε

$$\begin{aligned}&(n\cdot_{\mathbb{N}}m)^{\theta(k)}=(n\cdot_{\mathbb{N}}m)^{k+_{\mathbb{N}}1}\ \text{(λόγω της 1.6.15 (i))}\\&=(n\cdot_{\mathbb{N}}m)^k\cdot_{\mathbb{N}}(n\cdot_{\mathbb{N}}m)^1\ \text{(λόγω της ιδιότητας (ii))}\\&=n^k\cdot_{\mathbb{N}}m^k\cdot_{\mathbb{N}}(n\cdot_{\mathbb{N}}m)^1\ \text{(επειδή } k\in U_{(m,n)})\\&=n^k\cdot_{\mathbb{N}}m^k\cdot_{\mathbb{N}}n\cdot_{\mathbb{N}}m\ \text{(λόγω της ιδιότητας (i))}\\&=\left(n^k\cdot_{\mathbb{N}}n\right)\cdot_{\mathbb{N}}\left(m^k\cdot_{\mathbb{N}}m\right)\ \text{(λόγω της 1.6.18 (v))}\\&=n^{k+_{\mathbb{N}}1}\cdot_{\mathbb{N}}m^{k+_{\mathbb{N}}1}\ \text{(λόγω της ιδιότητας (ii))}\\&=n^{\theta(k)}\cdot_{\mathbb{N}}m^{\theta(k)}\ \text{(λόγω της 1.6.15 (i)).}\end{aligned}$$

Κατά συνέπειαν, $\theta(k)\in U_{(m,n)},\ \forall(m,n)\in\mathbb{N}\times\mathbb{N}$. Εκ νέου χρήση τού (**A 4**) μας οδηγεί στην ισότητα $U_{(m,n)}=\mathbb{N},\ \forall(m,n)\in\mathbb{N}\times\mathbb{N}$. □

‣ **Ο ορισμός τής συνήθους διατάξεως επί τού** $\mathbb{N}$. Τα στοιχεία τού $\mathbb{N}$ διατάσσονται κατά τον πλέον «φυσικό» τρόπο ως ακολούθως:

1.6.23 Ορισμός. Έστω $(m,n) \in \mathbb{N} \times \mathbb{N}$. Λέμε ότι ο m είναι **μικρότερος** τού n ή ότι ο n είναι **μεγαλύτερος** τού m (και γράφουμε $m < n$ ή $n > m$) όταν υπάρχει κάποιος $k \in \mathbb{N}$, ούτως ώστε να ισχύει η ισότητα $n = m +_{\mathbb{N}} k$. Επίσης, λέμε ότι ο m είναι **μικρότερος ή ίσος** τού n ή ότι ο n είναι **μεγαλύτερος ή ίσος** τού m (και γράφουμε $m \leqslant n$ ή $n \geqslant m$) όταν *είτε* $m < n$ *είτε* $m = n$.

1.6.24 Λήμμα. *Για τα στοιχεία τού* $\mathbb{N}$ *ισχύουν τα ακόλουθα*:

(i) $n +_{\mathbb{N}} 1 > n$, $\forall n \in \mathbb{N}$.

(ii) $n +_{\mathbb{N}} 1 > 1$, $\forall n \in \mathbb{N}$.

(iii) $n > 1$, $\forall n \in \mathbb{N} \setminus \{1\}$.

(iv) $n \geqslant 1$, $\forall n \in \mathbb{N}$.

Απόδειξη. Τα (i) και (ii) απορρέουν απ' ευθείας από τον δοθέντα ορισμό 1.6.23. Το (iii) έπεται από το (ii), σε συνδυασμό με τις ιδιότητες 1.6.12 (ii) και 1.6.15 (i), ενώ το (iv) έπεται άμεσα από το (iii). □

1.6.25 Θεώρημα (Νόμος τής «τριχοτομίας»). *Εάν* $(m,n) \in \mathbb{N} \times \mathbb{N}$, *τότε ισχύει ακριβώς ένα εκ των κάτωθι*:

(i) $m = n$.

(ii) $m > n$.

(iii) $n > m$.

Απόδειξη. **Βήμα 1ο**. Θα αποδείξουμε ότι ισχύει *το πολύ ένα* εκ των (i), (ii) και (iii). Ας υποθέσουμε ότι ισχύει το (i). Εάν ίσχυε (ταυτοχρόνως) και το (ii), τότε θα υπήρχε κάποιος $k \in \mathbb{N}$ με $m = n +_{\mathbb{N}} k = n$, οπότε θα καταλήγαμε σε άτοπο (καθότι η τελευταία ισότητα δεν μπορεί να είναι αληθής λόγω τής ιδιότητας 1.6.15 (vii)). Κατ' αναλογίαν θα καταλήγαμε σε άτοπο εάν υποθέταμε την ταυτόχρονη ισχύ των (i) και (iii).

Εν συνεχεία, υποθέτουμε ότι ισχύει το (ii). Τότε $\exists k \in \mathbb{N} : m = n +_{\mathbb{N}} k$. Λόγω τής ιδιότητας 1.6.15 (vii) το (i) είναι αναληθές. Εξάλλου, εάν ίσχυε το (iii), τότε θα υπήρχε κάποιος $r \in \mathbb{N}$ με

$$m +_{\mathbb{N}} r = n \Rightarrow m = (m +_{\mathbb{N}} r) +_{\mathbb{N}} k = m +_{\mathbb{N}} (r +_{\mathbb{N}} k)$$

οπότε θα καταλήγαμε εκ νέου σε άτοπο (λόγω τής ιδιότητας 1.6.15 (vii)).

Τέλος, εάν υποτεθεί ότι ισχύει το (iii), τότε κατόπιν χρήσεως ανάλογης συλλογιστικής (και εναλλαγής των ρόλων των m και n) αποδεικνύεται ότι δεν ισχύει ούτε το (i) ούτε το (ii).

Βήμα 2ο. Θα αποδείξουμε ότι ισχύει *τουλάχιστον ένα* εκ των (i), (ii) και (iii). Προς τούτο ορίζουμε το σύνολο

$$U := \{\, n \in \mathbb{N} \mid \text{τουλάχιστον ένα εκ των (i), (ii) και (iii) είναι αληθές} \,\}.$$

Προφανώς, $1 \in U$ (διότι εάν $m = 1$, τότε το (i) είναι αληθές, ενώ εάν $m \neq 1$, τότε το (ii) είναι αληθές). Έστω τυχών $n \in U$. Εξετάζουμε τις τρεις περιπτώσεις χωριστά:

• Εάν $m = n$, τότε $\theta(n) = n +_{\mathbb{N}} 1 = m +_{\mathbb{N}} 1$, οπότε το (iii) είναι αληθές για τον $\theta(n)$.

• Εάν $m > n$, τότε

$$\exists k \in \mathbb{N} : m = n +_{\mathbb{N}} k \Rightarrow m +_{\mathbb{N}} 1 = \theta(n) +_{\mathbb{N}} k.$$

Εάν $k = 1$, τότε το (i) είναι αληθές για το $\theta(n)$ (λόγω τής ιδιότητας 1.6.15 (viii)). Εάν $k \neq 1$, τότε

$$\exists l \in \mathbb{N} : k = l +_{\mathbb{N}} 1 \Rightarrow m +_{\mathbb{N}} 1 = \theta(n) +_{\mathbb{N}} l +_{\mathbb{N}} 1,$$

οπότε το (ii) είναι αληθές για το $\theta(n)$ (διότι $m = \theta(n) +_{\mathbb{N}} l$, και πάλι λόγω τής ιδιότητας 1.6.15 (viii)).
• Εάν $n > m$, τότε

$$\exists k \in \mathbb{N} : m +_{\mathbb{N}} k = n \Rightarrow m +_{\mathbb{N}} (1 +_{\mathbb{N}} k) = n +_{\mathbb{N}} 1 = \theta(n),$$

οπότε το (iii) είναι αληθές για τον $\theta(n)$. Άρα τελικώς $\theta(n) \in U$, $\forall n \in \mathbb{N}$. Από το αξίωμα (**A 4**) έπεται ότι $U = \mathbb{N}$. □

1.6.26 Θεώρημα. *Η διμελής σχέση "$\leqslant$" η ορισθείσα επί τού $\mathbb{N}$ στο εδάφιο 1.6.23 καθιστά το $\mathbb{N}$ ολικώς διατεταγμένο σύνολο.* (Βλ. 1.4.1.)

Απόδειξη. Η ανακλαστικότητα τής "$\leqslant$" είναι προφανής (διότι $n = n$, $\forall n \in \mathbb{N}$). Εάν $(m, n) \in \mathbb{N} \times \mathbb{N}$, όπου $m \leqslant n$ και (ταυτοχρόνως) $n \leqslant m$, και εάν υποθέσουμε ότι $m \neq n$, τότε $m < n$ και (ταυτοχρόνως) $n < m$, κάτι που είναι άτοπο επί τη βάσει τού νόμου τής τριχοτομίας 1.6.25. Κατ' ανάγκην λοιπόν $m = n$ και η "$\leqslant$" είναι αντισυμμετρική.

Εν συνεχεία θεωρούμε $m, n, k \in \mathbb{N}$, όπου $m \leqslant n$ και (ταυτοχρόνως) $n \leqslant k$. Εργαζόμενοι με «εις άτοπον απαγωγή» υποθέτουμε ότι η ανισοϊσότητα $m \leqslant k$ δεν είναι αληθής. Σύμφωνα με τον νόμο τής τριχοτομίας 1.6.25, $m > k$. Κατά συνέπειαν, $\exists l \in \mathbb{N} : m = k +_{\mathbb{N}} l$. Διαχωρίζουμε περιπτώσεις:

(a) Εάν $n = k$, τότε $m > n$, κάτι που αντιβαίνει στον νόμο τής τριχοτομίας 1.6.25.

(b) Εάν $n < k$, τότε

$$\exists q \in \mathbb{N} : k = n +_{\mathbb{N}} q \Rightarrow m = (n +_{\mathbb{N}} q) +_{\mathbb{N}} l = n +_{\mathbb{N}} (q +_{\mathbb{N}} l) \Rightarrow m > n,$$

κάτι που αντιβαίνει εκ νέου στον νόμο τής τριχοτομίας 1.6.25. Ως εκ τούτου, $m \leqslant k$ και η "$\leqslant$" είναι μεταβατική.

Απομένει να αποδειχθεί ότι τα στοιχεία τού $\mathbb{N}$ είναι μεταξύ τους ανά δύο συγκρίσιμα ως προς την "$\leqslant$". Θεωρούμε λοιπόν τυχόντες $m, n \in \mathbb{N}$. Εάν $m = n$, τότε εξ ορισμού $m \leqslant n$. Εάν $m \neq n$, τότε ο νόμος τής τριχοτομίας 1.6.25 επιτάσσει είτε την ισχύ τής ανισότητας $m < n$ (οπότε $m \leqslant n$) είτε την ισχύ τής ανισότητας $n < m$ (οπότε $n \leqslant m$). Κατά συνέπειαν, η διμελής σχέση "$\leqslant$" καθιστά το $\mathbb{N}$ ολικώς διατεταγμένο σύνολο. □

1.6.27 Πρόταση (Ιδιότητες διατάξεως). *Εάν $n, m, k, p \in \mathbb{N}$, τότε ισχύουν τα ακόλουθα*:

(i) *Εάν $n < m$ και $m < k$, τότε $n < k$.*

(ii) *Δεν ισχύει ποτέ η σχέση $n < n$.*

(iii) *Εάν $m \neq n$, τότε ακριβώς μία εκ των εξισώσεων*

$$x +_{\mathbb{N}} m = n \text{ και } x +_{\mathbb{N}} n = m$$

είναι επιλύσιμη (ως προς x) εντός τού $\mathbb{N}$. Επιπροσθέτως, αυτή διαθέτει μία και μόνον λύση.

(iv) $n +_{\mathbb{N}} m > n$.

(v) $m > n \iff m +_{\mathbb{N}} k > n +_{\mathbb{N}} k$.

(vi) *Εάν $m > n$ και $k > p$, τότε $m +_{\mathbb{N}} k > n +_{\mathbb{N}} p$.*

(vii) $m < n +_{\mathbb{N}} 1 \iff m \leqslant n$.

(viii) $\nexists \xi \in \mathbb{N} : n < \xi < n + 1$.

(ix) $n < m \iff n \cdot_{\mathbb{N}} p < m \cdot_{\mathbb{N}} p$.

(x) **[Νόμος τής διαγραφής]** $n \cdot_{\mathbb{N}} p = m \cdot_{\mathbb{N}} p \Longrightarrow n = m$.

(xi) *Εάν* $n < m$ *και* $k < p$, *τότε* $n \cdot_{\mathbb{N}} k < m \cdot_{\mathbb{N}} p$.
(xii) $n \cdot_{\mathbb{N}} m \geqslant n$.
(xiii) $n < m \iff n^k < m^k$.
(xiv) $(n +_{\mathbb{N}} 1)^m \geqslant 1 +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m)$.
(xv) $m \in \mathbb{N} \setminus \{1\} \Longrightarrow m^k \geqslant 1 +_{\mathbb{N}} k$.

Απόδειξη. Το (i) έπεται άμεσα από τη μεταβατικότητα τής "$\leqslant$" και το (ii) από την ιδιότητα 1.6.15 (vii).

(iii) Από τον νόμο τής τριχοτομίας 1.6.25 συνάγεται ότι ο πρώτος ισχυρισμός είναι αληθής. Απομένει λοιπόν να αποδειχθεί το μονοσήμαντο τής (όποιας) λύσεως. Εάν η $x +_{\mathbb{N}} m = n$ διαθέτει δυο λύσεις x_1, x_2 εντός τού $\mathbb{N}$, τότε

$$\left.\begin{array}{l} x_1 +_{\mathbb{N}} m = n \\ x_2 +_{\mathbb{N}} m = n \end{array}\right\} \Rightarrow x_1 +_{\mathbb{N}} m = x_2 +_{\mathbb{N}} m \underset{1.6.15\,(\text{viii})}{\Longrightarrow} x_1 = x_2.$$

Το ίδιο συμπέρασμα εξάγεται εάν υποτεθεί ότι η $x +_{\mathbb{N}} n = m$ είναι επιλύσιμη (ως προς x) εντός τού $\mathbb{N}$.

(iv) Τούτο έπεται άμεσα από τον ορισμό 1.6.23.

(v) Εάν $m > n$, τότε

$$\exists l \in \mathbb{N} : m = n +_{\mathbb{N}} l \Rightarrow m +_{\mathbb{N}} k = (n +_{\mathbb{N}} k) +_{\mathbb{N}} l > n \Rightarrow m +_{\mathbb{N}} k > n +_{\mathbb{N}} k.$$

Και αντιστρόφως· εάν $m +_{\mathbb{N}} k > n +_{\mathbb{N}} k$, τότε

$$\exists q \in \mathbb{N} : m +_{\mathbb{N}} k = n +_{\mathbb{N}} k +_{\mathbb{N}} q \underset{1.6.15\,(\text{viii})}{\Longrightarrow} m = n +_{\mathbb{N}} q \Rightarrow m > n.$$

(vi) Εάν $m > n$ και $k > p$, τότε

$$\left.\begin{array}{l} \exists l \in \mathbb{N} : m = n +_{\mathbb{N}} l \\ \exists q \in \mathbb{N} : k = p +_{\mathbb{N}} q \end{array}\right\} \Rightarrow m +_{\mathbb{N}} k = (n +_{\mathbb{N}} p) +_{\mathbb{N}} (l +_{\mathbb{N}} q) \Rightarrow m +_{\mathbb{N}} k > n +_{\mathbb{N}} p.$$

(vii) Εάν $m < n +_{\mathbb{N}} 1$ και εάν υποθέσουμε ότι $m > n$, τότε

$$\left.\begin{array}{r} \exists l \in \mathbb{N} : n +_{\mathbb{N}} 1 = m +_{\mathbb{N}} l \\ \exists q \in \mathbb{N} : m = n +_{\mathbb{N}} q \end{array}\right\} \Rightarrow n +_{\mathbb{N}} 1 +_{\mathbb{N}} m = (m +_{\mathbb{N}} l) +_{\mathbb{N}} (n +_{\mathbb{N}} q),$$

οπότε (κατά την 1.6.15 (v))

$$(n +_{\mathbb{N}} m) +_{\mathbb{N}} 1 = (n +_{\mathbb{N}} m) +_{\mathbb{N}} (l +_{\mathbb{N}} q) \underset{1.6.15\,(\text{viii})}{\Longrightarrow} l +_{\mathbb{N}} q = 1 \Rightarrow l < 1,$$

πράγμα άτοπο λόγω τού 1.6.24 (iv) και των όσων επιτάσσει ο νόμος τής τριχοτομίας 1.6.25.

(viii) Εάν υπήρχε $\xi \in \mathbb{N} : n < \xi < n + 1$, τότε θα είχαμε $n < \xi \leqslant n$, ήτοι κάτι το οποίο αντιβαίνει στον νόμο τής τριχοτομίας 1.6.25.

(ix) Εάν $n < m$, τότε

$$\exists l \in \mathbb{N} : m = n +_{\mathbb{N}} l \underset{1.6.18\,(\text{vi})}{\Longrightarrow} m \cdot_{\mathbb{N}} p = (n \cdot_{\mathbb{N}} p) +_{\mathbb{N}} (l \cdot_{\mathbb{N}} p) \Rightarrow n \cdot_{\mathbb{N}} p < m \cdot_{\mathbb{N}} p.$$

Και αντιστρόφως· εάν $n \cdot_{\mathbb{N}} p < m \cdot_{\mathbb{N}} p$, τότε αποκλείεται να ισχύει $n = m$ (διότι θα ίσχυε κατ' ανάγκην και η $n \cdot_{\mathbb{N}} p = m \cdot_{\mathbb{N}} p$, η οποία θα ήταν αδύνατη επί τη βάσει τού θεωρήματος 1.6.25). Επιπροσθέτως, αποκλείεται να ισχύει και η ανισότητα $n > m$,

διότι εν τοιαύτη περιπτώσει θα υπήρχε $q \in \mathbb{N} : n = m +_{\mathbb{N}} q$, οπότε θα συμπεραίναμε ότι

$$n \cdot_{\mathbb{N}} p = (m +_{\mathbb{N}} q) \cdot_{\mathbb{N}} p = (m \cdot_{\mathbb{N}} p) +_{\mathbb{N}} (q \cdot_{\mathbb{N}} p) \Rightarrow n \cdot_{\mathbb{N}} p > m \cdot_{\mathbb{N}} p,$$

ήτοι κάτι το άτοπο (λόγω τού θεωρήματος 1.6.25). Εκ των προαναφερθέντων και εκ τού νόμου τής τριχοτομίας 1.6.25 συνάγεται τελικώς ότι

$$n \cdot_{\mathbb{N}} p < m \cdot_{\mathbb{N}} p \Rightarrow n < m.$$

(x) Εάν $n \cdot_{\mathbb{N}} p = m \cdot_{\mathbb{N}} p$ και (ταυτοχρόνως) $n \neq m$, τότε είτε $n > m$ είτε $m > n$. Σε αμφότερες τις περιπτώσεις το (ix) μας οδηγεί στο συμπέρασμα ότι $n \cdot_{\mathbb{N}} p \neq m \cdot_{\mathbb{N}} p$. Άρα

$$n \cdot_{\mathbb{N}} p = m \cdot_{\mathbb{N}} p \Longrightarrow n = m.$$

(xi) Εάν $n < m$ και $k < p$, τότε, σύμφωνα με το (ix), έχουμε

$$\left.\begin{array}{l} n \cdot_{\mathbb{N}} k < m \cdot_{\mathbb{N}} k \\ m \cdot_{\mathbb{N}} k < m \cdot_{\mathbb{N}} p \end{array}\right\} \underset{\text{(i)}}{\Longrightarrow} n \cdot_{\mathbb{N}} k < m \cdot_{\mathbb{N}} p.$$

(xii) Τούτο ισχύει προφανώς ως ισότητα όταν $m = 1$. Στην περίπτωση όπου το m είναι $\neq 1$, υπάρχει κάποιος $l \in \mathbb{N}$ με $m = 1 +_{\mathbb{N}} l$. Ως εκ τούτου, ο ισχυρισμός είναι αληθής, διότι (βάσει τού (iv)) $n +_{\mathbb{N}} (n \cdot_{\mathbb{N}} k) \geqslant n$.

(xiii) Έστω τυχόν διατεταγμένο ζεύγος $(n, m) \in \mathbb{N} \times \mathbb{N}$. Ορίζουμε το σύνολο

$$U_{(n,m)} := \left\{ k \in \mathbb{N} \,|\, n < m \Longleftrightarrow n^k < m^k \right\}.$$

Προφανώς, $1 \in U_{(n,m)}$. Έστω τυχών $k \in U_{(n,m)}$. Εάν $n < m$, τότε

$$n^k < m^k \underset{\text{(xi)}}{\Longrightarrow} n^{k+_{\mathbb{N}}1} = n^k \cdot_{\mathbb{N}} n < m^k \cdot_{\mathbb{N}} m = m^{k+_{\mathbb{N}}1}.$$

Εν συνεχεία, ας υποθέσουμε, αντιστρόφως, ότι $n^{k+_{\mathbb{N}}1} < m^{k+_{\mathbb{N}}1}$. Θα εξετάσουμε δύο περιπτώσεις χωριστά:

(a) Εάν $n = m$, τότε από το (ix) έπεται ότι $n^k < m^k \underset{(\text{επειδή } k \in U_{(n,m)})}{\Longrightarrow} n < m$, κάτι που αντιβαίνει στον νόμο τής τριχοτομίας 1.6.25.

(b) Εάν $n > m$, τότε από το (xi) έπεται ότι

$$m \cdot_{\mathbb{N}} n^{k+_{\mathbb{N}}1} < n \cdot_{\mathbb{N}} m^{k+_{\mathbb{N}}1} \underset{\text{(ix)}}{\Longrightarrow} n^k < m^k \underset{(\text{επειδή } k \in U_{(n,m)})}{\Longrightarrow} n < m,$$

κάτι που εκ νέου αντιβαίνει στον νόμο τής τριχοτομίας 1.6.25. Κατά συνέπειαν,

$$k +_{\mathbb{N}} 1 = \theta(k) \in U_{(n,m)} \underset{(\text{αξ. } (\mathbf{A4}))}{\Longrightarrow} U_{(n,m)} = \mathbb{N}, \ \forall (n, m) \in \mathbb{N} \times \mathbb{N}.$$

(xiv) Έστω τυχών $n \in \mathbb{N}$. Ορίζουμε το σύνολο

$$U_n := \left\{ m \in \mathbb{N} \,|\, (n +_{\mathbb{N}} 1)^m \geqslant 1 +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m) \right\}.$$

Προφανώς, $1 \in U_n$. Έστω τυχών $m \in U_n$. Ας υποθέσουμε ότι

$$\begin{aligned} &(n +_{\mathbb{N}} 1)^{m+_{\mathbb{N}}1} < 1 +_{\mathbb{N}} (n \cdot_{\mathbb{N}} (m +_{\mathbb{N}} 1)) \\ &\left[\Leftrightarrow (n +_{\mathbb{N}} 1)^m \cdot_{\mathbb{N}} n +_{\mathbb{N}} (n +_{\mathbb{N}} 1)^m < 1 +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m) +_{\mathbb{N}} n\right]. \end{aligned}$$

Θα εξετάσουμε δύο περιπτώσεις χωριστά:

(a) Εάν $(n +_{\mathbb{N}} 1)^m = 1 +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m)$, τότε από το (v) έπεται ότι

$$(n +_{\mathbb{N}} 1)^m \cdot_{\mathbb{N}} n < n \underset{\text{(ix)}}{\Longrightarrow} (n +_{\mathbb{N}} 1)^{m+_{\mathbb{N}}1} < 1,$$

ήτοι κάτι που είναι αδύνατο λόγω τού (iii) τού λήμματος 1.6.24.

(b) Εάν $(n +_{\mathbb{N}} 1)^m > 1 +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m)$, τότε

$$\begin{aligned}
&(n +_{\mathbb{N}} 1)^m +_{\mathbb{N}} n > 1 +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m) +_{\mathbb{N}} n \\
&\underset{\text{(i)}}{\Longrightarrow} (n +_{\mathbb{N}} 1)^m +_{\mathbb{N}} n > (n +_{\mathbb{N}} 1)^m \cdot_{\mathbb{N}} n +_{\mathbb{N}} (n +_{\mathbb{N}} 1)^m \\
&\underset{\text{(v)}}{\Longrightarrow} n > (n +_{\mathbb{N}} 1)^m \cdot_{\mathbb{N}} n \underset{\text{(ix)}}{\Longrightarrow} 1 > (n +_{\mathbb{N}} 1)^m,
\end{aligned}$$

πράγμα το οποίο αντισφάσκει προς το (iii) τού λήμματος 1.6.24. Εκ των προαναφερθέντων και εκ τού νόμου τής τριχοτομίας 1.6.25 συνάγεται τελικώς ότι

$$m +_{\mathbb{N}} 1 = \theta(m) \in U_n \underset{(\text{αξ. } (\mathbf{A4}))}{\Longrightarrow} U_n = \mathbb{N},\ \forall n \in \mathbb{N}.$$

(xv) Επειδή $m \neq 1$ θα υπάρχει κάποιος $n \in \mathbb{N} : m = n +_{\mathbb{N}} 1$ (λόγω των ιδιοτήτων 1.6.12 (ii) και 1.6.15 (i)), οπότε

$$\begin{aligned}
m^k = (n +_{\mathbb{N}} 1)^k &\geqslant 1 +_{\mathbb{N}} (n \cdot_{\mathbb{N}} k) \ \text{ (λόγω τού (xiv))} \\
&\geqslant 1 +_{\mathbb{N}} k \ \text{ (λόγω των (ix) και (v) και τού ότι } n \geqslant 1)
\end{aligned}$$

Άρα $m^k \geqslant 1 +_{\mathbb{N}} k$, $\forall m \in \mathbb{N} \setminus \{1\}$. □

1.6.28 Σημείωση. (i) Λόγω τού νόμου τής τριχοτομίας 1.6.25 και τού (iv) τής προτάσεως 1.6.27 το $\mathbb{N}$ δεν διαθέτει ουδέτερο στοιχείο ως προς την πρόσθεση " $+_{\mathbb{N}}$ ".

(ii) Το μοναδικό στοιχείο τού $\mathbb{N}$ που διαθέτει συμμετρικό στοιχείο ως προς τον πολλαπλασιασμό " $\cdot_{\mathbb{N}}$ " είναι το 1 (με το 1 ως το μοναδικό συμμετρικό του, πρβλ. με τα 1.5.13, 1.5.14 και 1.6.18 (v)). Πράγματι· ας υποθέσουμε ότι $m, n \in \mathbb{N}$ με $m \cdot_{\mathbb{N}} n = 1$ κι ας εξετάσουμε όλες τις δυνατές περιπτώσεις χωριστά: Εάν $m > 1$ και $n > 1$, τότε $m \cdot_{\mathbb{N}} n > 1 \cdot_{\mathbb{N}} 1 = 1$ (λόγω των 1.6.18 (i) και 1.6.27 (xi)), πράγμα άτοπο. Εάν το ένα εκ των m, n είναι $= 1$ και το άλλο > 1, τότε καταλήγουμε εκ νέου σε άτοπο λόγω των (i) και (v) τής προτάσεως 1.6.18 (i) και τού (iii) τού λήμματος 1.6.24. Άρα κατ' ανάγκην $m = n = 1$.

1.6.29 Πρόταση (Αρχιμήδεια ιδιότητα). *Για οιουσδήποτε $m, n \in \mathbb{N}$ υπάρχει κάποιος $k \in \mathbb{N}$, ούτως ώστε να ισχύει η ανισότητα*

$$m \cdot_{\mathbb{N}} k > n.$$

Απόδειξη. Επιλέγοντας, για οιουσδήποτε $m, n \in \mathbb{N}$, ως k τον $\theta(n) = n +_{\mathbb{N}} 1$, παρατηρούμε ότι

$$\begin{aligned}
m \cdot_{\mathbb{N}} k = m \cdot_{\mathbb{N}} (n +_{\mathbb{N}} 1) &= (m \cdot_{\mathbb{N}} n) +_{\mathbb{N}} m \ \text{ (λόγω τής ιδιότητας 1.6.18 (ii))} \\
&\geqslant m \cdot_{\mathbb{N}} n \ \text{ (λόγω τού (iv) τής προτάσεως 1.6.27)},
\end{aligned}$$

απ' όπου έπεται ότι $m \cdot_{\mathbb{N}} k > n$ (λόγω τού (ix) τής προτάσεως 1.6.27 και τού ότι $m \geqslant 1$). □

1.6.30 Πρόταση («Εκθετική» αρχιμήδεια ιδιότητα). *Για οιουσδήποτε $m, n \in \mathbb{N}$ με $m \neq 1$ υπάρχει κάποιος $k \in \mathbb{N}$, ούτως ώστε να ισχύει η ανισότητα*

$$m^k > n.$$

Απόδειξη. Εάν $m, n \in \mathbb{N}$ με $m \neq 1$, τότε θέτοντας $k := n$ παρατηρούμε ότι

$$m^k = m^n > 1 +_{\mathbb{N}} n \ \text{ (λόγω τού (xv) τής προτάσεως 1.6.27)},$$

οπότε $m^k > n$ (λόγω τού (i) τού λήμματος 1.6.24). □

1.6.31 Παρατήρηση. Τόσον οι πράξεις προσθέσεως και πολλαπλασιασμού όσον και η σχέση διατάξεως "$\leqslant$" ορίζονται επί *οιουδήποτε* συστήματος φυσικών αριθμών. Επιπροσθέτως, εάν τα $(\mathbb{N}, 1, \theta)$ και $(\mathbb{N}', 1', \theta')$ είναι τυχόντα συστήματα φυσικών αριθμών και η $f : \mathbb{N} \longrightarrow \mathbb{N}'$ μια αμφίριψη που πληροί τις συνθήκες (i) και (ii) τις παρατεθείσες στο εδάφιο 1.6.9, τότε είναι εύκολο να αποδειχθούν οι εξής («διατηρητικές») ιδιότητες:

(i) $f(m +_{\mathbb{N}} n) = f(m) +_{\mathbb{N}'} f(n), \forall (m, n) \in \mathbb{N} \times \mathbb{N}$.

(ii) $f(m \cdot_{\mathbb{N}} n) = f(m) \cdot_{\mathbb{N}'} f(n), \forall (m, n) \in \mathbb{N} \times \mathbb{N}$.

(iii) Για οιουσδήποτε $m, n \in \mathbb{N}$ ισχύει η αμφίπλευρη συνεπαγωγή

$$m \leqslant n \Longleftrightarrow f(m) \leqslant' f(n).$$

Ως εκ τούτου, οι πράξεις προσθέσεως και πολλαπλασιασμού και η σχέση διατάξεως (καθώς και όλες οι περιγραφείσες ιδιότητές τους) *δεν επηρεάζονται* ύστερα από την εφαρμογή τής f, δηλαδή *δεν εξαρτώνται* από την επιλογή τού εκάστοτε «εκπροσώπου» τού "$\mathbb{N}$" με τον οποίον εργαζόμαστε. (Η παρούσα παρατήρηση ισχυροποιεί το θεώρημα 1.6.10, καθώς και τα προαναφερθέντα στην παρατήρηση 1.6.11.)

1.6.32 Θεώρημα («Αρχή τής καλής διατάξεως τού $\mathbb{N}$»). *Ως προς τη συνήθη σχέση διατάξεως "$\leqslant$" το $\mathbb{N}$ είναι καλώς διατεταγμένο.*

Απόδειξη. Θα εργασθούμε με «εις άτοπον απαγωγή». Υποθέτουμε ότι υφίσταται κάποιο μη κενό υποσύνολο S τού $\mathbb{N}$ το οποίο δεν διαθέτει ελάχιστο στοιχείο. Ορίζουμε το σύνολο

$$U := \{\, n \in \mathbb{N} \mid n \leqslant s,\ \forall s \in S \}\,.$$

Προφανώς, $1 \in U$ (λόγω τού (iv) τού λήμματος 1.6.24). Έστω τυχών $n \in U$. Εξ υποθέσεως, $n \notin S$ (διότι αλλιώς το n θα ήταν ελάχιστο στοιχείο τού S). Επομένως, *για κάθε* $s \in S$,

$$\exists k_s \in \mathbb{N} : s = n +_{\mathbb{N}} k_s$$

Κατά το 1.6.12 (ii) $\exists l_s \in \mathbb{N} : k_s = l_s +_{\mathbb{N}} 1$, οπότε

$$\begin{aligned} & s = n +_{\mathbb{N}} (l_s +_{\mathbb{N}} 1) = (n +_{\mathbb{N}} 1) +_{\mathbb{N}} l_s,\ \forall s \in S \\ & \Rightarrow n +_{\mathbb{N}} 1 \leqslant s,\ \forall s \in S \Rightarrow \theta\,(n) = n +_{\mathbb{N}} 1 \in U. \end{aligned}$$

Κατά συνέπειαν, σύμφωνα με το αξίωμα (**A 4**), $U = \mathbb{N}$. Επειδή $S \neq \varnothing$, θεωρώντας κάποιο $s_\bullet \in S$, έχουμε

$$s_\bullet \in \mathbb{N} = U \Rightarrow s_\bullet \leqslant s,\ \forall s \in S \Rightarrow s_\bullet = \min(S).$$

Άτοπο! Άρα κάθε μη κενό υποσύνολο τού $\mathbb{N}$ διαθέτει ελάχιστο στοιχείο. □

1.6.33 Σημείωση (Η ισοδυναμία των (A 4) και 1.6.32.). Μέχρι στιγμής (και λαμβανομένης υπ' όψιν και τής παρατηρήσεως 1.6.31) έχουμε αποδείξει ότι η *αρχή τής καλής διατάξεως* οιουδήποτε συστήματος φυσικών αριθμών $(\mathbb{N}, 1, \theta)$ (ως προς τη συνήθη σχέση διατάξεως "$\leqslant$" την ορισθείσα στο εδάφιο 1.6.23) είναι επακόλουθη τού αξιώματος (**A 4**) τού Peano. Αξίζει, όμως, να επισημανθεί ότι είναι δυνατή και η *αντιστροφή των ρόλων τους*: Εάν η αρχή τής καλής διατάξεως 1.6.32 θεωρηθεί ως *αξίωμα*[32] που πληρούται από το $(\mathbb{N}, 1, \theta)$, τότε το (**A 4**) έπεται από αυτήν και

[32] Προσοχή! Δεν θα πρέπει κανείς να συγχέει την *αρχή* (ή, κατ' άλλους, *αξίωμα*) *τής καλής διατάξεως* **τού** $\mathbb{N}$ με το *αξίωμα* 1.4.21 *τής καλής διατάξεως* τής Θεωρίας Συνόλων. Το αξίωμα 1.4.21 διασφαλίζει την ύπαρξη *κάποιας* σχέσεως διατάξεως επί *οιουδήποτε* μη κενού συνόλου, η οποία το καθιστά καλώς διατεταγμένο σύνολο. Εν προκειμένω, η "$\leqslant$" είναι μια *συγκεκριμένη* σχέση διατάξεως επί τού $\mathbb{N}$, η οποία *οφείλει* να το καθιστά καλώς διατεταγμένο.

μπορεί, ως εκ τούτου, να αφαιρεθεί από τα αξιώματα 1.6.1 αντικαθιστώμενο με αυτήν! Πράγματι· εάν υποθέσουμε ότι το U είναι ένα υποσύνολο τού $\mathbb{N}$ για το οποίο ισχύει $1 \in U$ και $\theta(n) \in U$, $\forall n \in U$, και ότι $U \subsetneq \mathbb{N}$, τότε (σύμφωνα με το 1.6.32) $\exists n_\bullet \in \mathbb{N} : n_\bullet = \min(\mathbb{N} \smallsetminus U)$ με $n_\bullet > 1$ (διότι $1 \in U$). Επιλέγουμε τον (μονοσημάντως ορισμένο) $q \in \mathbb{N}$ με $\theta(q) = q +_{\mathbb{N}} 1 = n_\bullet$ (βλ. 1.6.12 (ii) και 1.6.15 (i)). Επειδή το $n_\bullet$ είναι το ελάχιστο στοιχείο τού $\mathbb{N} \smallsetminus U$, $q \in U$. Επειδή $q \in U$, το $\theta(q) = n_\bullet$ πρέπει να ανήκει στο U (εξ υποθέσεως), πράγμα *άτοπο*, διότι δεν είναι δυνατόν να έχουμε (ταυτοχρόνως) $n_\bullet \in \mathbb{N} \smallsetminus U$ και $n_\bullet \in U$. Κατά συνέπειαν, έχουμε $U = \mathbb{N}$ και το (**A 4**) είναι αληθές.

▸ **Η μέθοδος τής μαθηματικής επαγωγής.** Ο σημαντικός ρόλος που διαδραματίζει το αξίωμα (**A 4**) στις προηγηθείσες αποδείξεις είναι εμφανής. Το αξίωμα αυτό (που ισοδυναμεί, όπως είδαμε, με την αρχή τής καλής διατάξεως) είναι γνωστό και ως «αρχή τής μαθηματικής (ή τελείας) επαγωγής» και αποτελεί το έρεισμα τής *αποδεικτικής μεθόδου* που φέρει το όνομα «μέθοδος τής μαθηματικής (ή τελείας) επαγωγής». Η εν λόγω μέθοδος εφαρμόζεται για την επαλήθευση (ή μη) προτασιακών τύπων[33] που έχουν ως σύνολα αναφοράς τους το $\mathbb{N}$ ή ορισμένα (ειδικής φύσεως) υποσύνολά του.

1.6.34 Θεώρημα (Κλασική μαθηματική επαγωγή). *Εάν ο* $\Pi(n)$ *είναι ένας προτασιακός τύπος με σύνολο αναφοράς του το* $\mathbb{N}$, *τέτοιος ώστε*

(i) *η πρόταση* $\Pi(1)$ *να είναι αληθής και*

(ii) *η συνεπαγωγή* $\Pi(k) \Rightarrow \Pi(k +_{\mathbb{N}} 1)$ *να ισχύει για κάθε* $k \in \mathbb{N}$,

τότε η πρόταση $\Pi(n)$ *είναι αληθής για κάθε* $n \in \mathbb{N}$.

Απόδειξη. Έστω $U := \{ n \in \mathbb{N} \mid \text{η } \Pi(n) \text{ είναι αληθής} \}$. Σύμφωνα με το (i), $1 \in U$. Έστω τώρα τυχών $k \in U$. Σύμφωνα με το (ii), $k +_{\mathbb{N}} 1 = \theta(k) \in U$. Επομένως, επί τη βάσει τού αξιώματος (**A 4**), $U = \mathbb{N}$. □

1.6.35 Παράδειγμα. Για κάθε $n \in \mathbb{N}$ ισχύει η ισότητα

$$2 +_{\mathbb{N}} 4 +_{\mathbb{N}} 6 +_{\mathbb{N}} \cdots +_{\mathbb{N}} (2 \cdot_{\mathbb{N}} n) = n \cdot_{\mathbb{N}} (n +_{\mathbb{N}} 1)\,. \tag{1.23}$$

Πράγματι· για $n = 1$ έχουμε $2 \cdot_{\mathbb{N}} 1 = 2 = 1 \cdot_{\mathbb{N}} (1 +_{\mathbb{N}} 1) = 1 \cdot_{\mathbb{N}} 2$ (βλ. 1.6.18 (i), (v)). Εάν ο k είναι ένας φυσικός αριθμός με

$$2 +_{\mathbb{N}} 4 +_{\mathbb{N}} 6 +_{\mathbb{N}} \cdots +_{\mathbb{N}} (2 \cdot_{\mathbb{N}} k) = k \cdot_{\mathbb{N}} (k +_{\mathbb{N}} 1)\,,$$

τότε (λόγω των ιδιοτήτων (vi) και (v) τής προτάσεως 1.6.18)

$$\begin{aligned} &2 +_{\mathbb{N}} 4 +_{\mathbb{N}} 6 +_{\mathbb{N}} \cdots +_{\mathbb{N}} (2 \cdot_{\mathbb{N}} k) +_{\mathbb{N}} (2 \cdot_{\mathbb{N}} (k +_{\mathbb{N}} 1)) \\ &= k \cdot_{\mathbb{N}} (k +_{\mathbb{N}} 1) +_{\mathbb{N}} (2 \cdot_{\mathbb{N}} (k +_{\mathbb{N}} 1)) \\ &= (k +_{\mathbb{N}} 2) \cdot_{\mathbb{N}} (k +_{\mathbb{N}} 1) = (k +_{\mathbb{N}} 1) \cdot_{\mathbb{N}} (k +_{\mathbb{N}} 2)\,. \end{aligned}$$

Κατά συνέπειαν, βάσει τού θεωρήματος 1.6.34 η (1.23) είναι αληθής.

Το επόμενο θεώρημα αποτελεί γενίκευση τού 1.6.34, καθότι μας επιτρέπει να εφαρμόζουμε τη μέθοδο τής μαθηματικής επαγωγής εκκινώντας από *τυχόντα* φυσικό αριθμό.

[33] Σε αδρές γραμμές, ένας **προτασιακός τύπος** (ή ένα **κατηγόρημα**) $\Pi(x)$ είναι μια μαθηματική έκφραση περιέχουσα κάποιο «σύμβολο» (ή «μεταβλητή») x, η οποία επιδέχεται έναν ακριβώς από τους δύο χαρακτηρισμούς: **«αληθής»**, **«ψευδής»** (**πρόταση**) και με την ίδια πάντοτε σημασία όταν αντικαθιστούμε το x με οιοδήποτε στοιχείο ενός **συνόλου αναφοράς** A.

1.6.36 Θεώρημα (Πρώτη μορφή μαθηματικής επαγωγής). *Έστω* $n_0 \in \mathbb{N}$. *Εάν ο* $\Pi(n)$ *είναι ένας προτασιακός τύπος με σύνολο αναφοράς του το* $\{n \in \mathbb{N} \mid n \geqslant n_0\}$, *τέτοιος ώστε*

(i) *η πρόταση* $\Pi(n_0)$ *να είναι αληθής και*

(ii) *η συνεπαγωγή* $\Pi(k) \Rightarrow \Pi(k +_{\mathbb{N}} 1)$ *να ισχύει για κάθε φυσικό αριθμό* $k \geqslant n_0$,

τότε η πρόταση $\Pi(n)$ *είναι αληθής για κάθε φυσικό αριθμό* $n \geqslant n_0$.

Αποδειξη. Κατ' αρχάς ορίζουμε έναν προτασιακό τύπο $\Pi'(n)$ με σύνολο αναφοράς του το $\mathbb{N}$ ως εξής:

$$\Pi'(n) := \{n \in \mathbb{N} \mid \text{Εάν } n \geqslant n_0, \text{ τότε η πρόταση } \Pi(n) \text{ είναι αληθής}\}.$$

Παρατηρούμε ότι η πρόταση $\Pi'(1)$ είναι αληθής, καθότι, στην περίπτωση όπου $1 \geqslant n_0$, έχουμε κατ' ανάγκην $n_0 = 1$ (λόγω τού (iv) τού λήμματος 1.6.24) και η πρόταση $\Pi(1)$ είναι (εξ υποθέσεως) αληθής. Έστω τώρα τυχών $n \in \mathbb{N}$ για τον οποίο η πρόταση $\Pi'(n)$ είναι αληθής. Θα δείξουμε ότι η $\Pi'(\theta(n))$ είναι ωσαύτως αληθής, ήτοι ότι για $\theta(n) \geqslant n_0$ η πρόταση $\Pi(\theta(n))$ είναι αληθής. Εάν $\theta(n) = n_0$, τότε, σύμφωνα με το (i), η πρόταση $\Pi(\theta(n))$ είναι αληθής. Εάν $\theta(n) > n_0$, τότε $n \geqslant n_0$ και σύμφωνα με το (ii) η πρόταση $\Pi(\theta(n))$ είναι αληθής. Από το θεώρημα 1.6.34 έπεται ότι η $\Pi'(n)$ είναι αληθής για κάθε $n \in \mathbb{N}$. Ως εκ τούτου, η πρόταση $\Pi(n)$ είναι αληθής για κάθε φυσικό αριθμό $n \geqslant n_0$. □

1.6.37 Παράδειγμα. Για κάθε φυσικό αριθμό $n \geqslant 3$ $(=: n_0)$ ισχύει η ανισότητα

$$3^n > (n +_{\mathbb{N}} 1)^2. \tag{1.24}$$

Πράγματι· για $n = 3$ έχουμε $3^3 = 27 > 16 = (3 +_{\mathbb{N}} 1)^2$. Εάν ο k είναι ένας φυσικός αριθμός $\geqslant 3$ με

$$3^k > (k +_{\mathbb{N}} 1)^2, \tag{1.25}$$

τότε $\left(2 \cdot_{\mathbb{N}} k^2\right) +_{\mathbb{N}} (2 \cdot_{\mathbb{N}} k) = 2 \cdot_{\mathbb{N}} k \cdot_{\mathbb{N}} (k +_{\mathbb{N}} 1) \geqslant 24 > 1$, οπότε

$$\begin{aligned} &\Rightarrow \quad \left(3 \cdot_{\mathbb{N}} k^2\right) +_{\mathbb{N}} (6 \cdot_{\mathbb{N}} k) +_{\mathbb{N}} 3 > k^2 +_{\mathbb{N}} (4 \cdot_{\mathbb{N}} k) +_{\mathbb{N}} 4 \\ &\Rightarrow \quad 3 \cdot_{\mathbb{N}} (k +_{\mathbb{N}} 1)^2 > (k +_{\mathbb{N}} 2)^2. \end{aligned} \tag{1.26}$$

Από τις (1.25) και (1.26) λαμβάνουμε

$$3^{k+_{\mathbb{N}}1} = 3 \cdot_{\mathbb{N}} 3^k > 3 \cdot_{\mathbb{N}} (k +_{\mathbb{N}} 1)^2 > (k +_{\mathbb{N}} 2)^2.$$

Κατά συνέπειαν, βάσει τού θεωρήματος 1.6.36 η (1.24) είναι αληθής. (Σημειωτέον ότι η (1.24) είναι *ψευδής* για $n = 1$ και $n = 2$.)

1.6.38 Θεώρημα (Δεύτερη μορφή μαθηματικής επαγωγής). *Έστω* $n_0 \in \mathbb{N}$. *Εάν ο* $\Pi(n)$ *είναι ένας προτασιακός τύπος με σύνολο αναφοράς του το* $\{n \in \mathbb{N} \mid n \geqslant n_0\}$, *τέτοιος ώστε*

(i) *η πρόταση* $\Pi(n_0)$ *να είναι αληθής και*

(ii) *η συνεπαγωγή*

$$\left.\begin{array}{c} \Pi(n_0), \\ \Pi(n_0 +_{\mathbb{N}} 1), \\ \vdots \\ \text{και } \Pi(k) \end{array}\right\} \Longrightarrow \Pi(k +_{\mathbb{N}} 1)$$

να ισχύει για κάθε φυσικό αριθμό $k \geqslant n_0$, *τότε η πρόταση* $\Pi(n)$ *είναι αληθής για κάθε φυσικό αριθμό* $n \geqslant n_0$.

ΑΠΟΔΕΙΞΗ. Θεωρούμε το σύνολο

$$S := \{\, n \in \mathbb{N} \mid n \geqslant n_0 \text{ και η πρόταση } \Pi(n) \text{ είναι ψευδής } \}\,.$$

Ας υποθέσουμε ότι $S \neq \varnothing$. Τότε, σύμφωνα με το θεώρημα 1.6.32,

$$\exists m \in \mathbb{N} : m = \min(S).$$

Λόγω τού (i), $n_0 \notin S$, οπότε ισχύει η ανισότητα $m > n_0$ $(\geqslant 1)$. Κατά τα 1.6.12 (ii) και 1.6.15 (i) υπάρχει (μονοσημάντως ορισμένος) $k \in \mathbb{N}$ με $\theta\,(k) = k +_{\mathbb{N}} 1 = m$. Από τον ορισμό τού m, για κάθε $j \in \mathbb{N}$ με $n_0 \leqslant j \leqslant k$ η $\Pi(j)$ είναι αληθής. Λόγω τής υποθέσεως (ii) η $\Pi(k +_{\mathbb{N}} 1)$ οφείλει να είναι ωσαύτως αληθής. Άρα

$$m = k +_{\mathbb{N}} 1 \in \{\, n \in \mathbb{N} \mid n \geqslant n_0\} \smallsetminus S.$$

Άτοπο! Ως εκ τούτου, $S = \varnothing$ και η πρόταση $\Pi(n)$ είναι αληθής για κάθε φυσικό αριθμό $n \geqslant n_0$. □

1.6.39 Σημείωση. Κατά την εφαρμογή κάποιου εκ των θεωρημάτων 1.6.34, 1.6.36 ή 1.6.38 για την επαλήθευση τής ισχύος μιας προτάσεως η (εκάστοτε) συνθήκη (ii) αναφέρεται συνήθως ως **επαγωγική υπόθεση**.

Ως εφαρμογή τού θεωρήματος 1.6.38 θα δώσουμε την απόδειξη τής «γενικευμένης προσεταιριστικής ιδιότητας» που διέπει κάθε μη κενό σύνολο A το οποίο είναι εφοδιασμένο με μια προσεταιριστική πράξη (βλ. παρατήρηση 1.5.18). Προς τούτο απαιτείται η θεώρηση *διατεταγμένων n-άδων* απαρτιζομένων από στοιχεία τού A, ήτοι στοιχείων τού *n-απλού καρτεσιανού γινομένου* A^n τού συνόλου A για κάθε $n \in \mathbb{N}$. Για $n = 1$, θέτουμε $A^1 := A$, ενώ για $n \geqslant 2$ επιλέγουμε τον (μονοσημάντως ορισμένο) $q \in \mathbb{N}$ με $\theta\,(q) = q +_{\mathbb{N}} 1 = n$ (βλ. 1.6.12 (ii) και 1.6.15 (i)) και ορίζουμε επαγωγικώς[34]:

$$A^n := A^q \times A.$$

1.6.40 Πρόταση (Γενικευμένη προσεταιριστική ιδιότητα). *Έστω ότι το A είναι ένα μη κενό σύνολο, η*

$$A \times A \longrightarrow A,\ (x, y) \longmapsto x \circledcirc y$$

μια προσεταιριστική πράξη ορισμένη επ' αυτού και

$$(a_1, a_2, \ldots, a_n) \in A^n$$

μια διατεταγμένη n-άδα στοιχείων τού A (όπου $n \in \mathbb{N}$). Τότε, καθ' οιονδήποτε τρόπο και αν εφαρμόσουμε την πράξη "$\circledcirc$" στα ως άνω στοιχεία $a_1, a_2, \ldots, a_n$, δηλαδή καθ' οιονδήποτε τρόπο και αν σχηματίσουμε το

$$\text{“}a_1 \circledcirc a_2 \circledcirc \cdots \circledcirc a_n\text{”},$$

υπό τον όρο -όμως- τής τηρήσεως τής προκειμένης σειράς παραθέσεώς τους, λαμβάνουμε πάντοτε το ίδιο αποτέλεσμα. (Απλούστερη διατύπωση: Για τον σχηματισμό τού "$a_1 \circledcirc a_2 \circledcirc \cdots \circledcirc a_n$" δεν έχουμε χρεία παρεμβολής οιωνδήποτε «παρενθέσεων».)

ΑΠΟΔΕΙΞΗ. Για *κάθε* $\nu \in \mathbb{N}$, $\nu \leqslant n$, ορίζουμε μια απεικόνιση

$$f_\nu : A^\nu \longrightarrow \mathfrak{P}\,(A)$$

μέσω τού αναδρομικού τύπου $f_1 := \mathrm{id}_A$ και

$$f_\nu\,(\xi_1, \xi_2, \ldots, \xi_\nu) := \left\{ b \circledcirc c \;\middle|\; \begin{array}{l} b \in f_l\,(\xi_1, \ldots, \xi_l)\,,\ c \in f_m\,(\xi_{l+_{\mathbb{N}}1}, \ldots, \xi_\nu) \\ \text{για κάποια } l, m \in \mathbb{N} : l +_{\mathbb{N}} m = \nu \end{array} \right\}.$$

[34] Παρομοίως ορίζεται και το καρτεσιανό γινόμενο n (όχι κατ' ανάγκην ίσων) συνόλων $A_1, \ldots, A_n$.

Τα στοιχεία τού υποσυνόλου $f_n\,(a_1, a_2, \ldots, a_n) \subseteq A$ είναι ουσιαστικώς όλοι οι δυνατοί σχηματισμοί τού "$a_1 \circledcirc \cdots \circledcirc a_n$" (με παγιωμένη τη σειρά παραθέσεως των $a_1, \ldots, a_n$) κατόπιν παρεμβολής οιωνδήποτε (δυνατών) «παρενθέσεων», όπως π.χ. είναι ο σχηματισμός

$$((a_1 \circledcirc a_2) \circledcirc (a_3 \circledcirc a_4)) \circledcirc (a_5 \circledcirc (a_6 \circledcirc a_7))$$

για $n = 7$. Ισχυριζόμαστε ότι ισχύει η ισότητα

$$f_n\,(a_1, a_2, \ldots, a_n) = \{(\cdots((a_1 \circledcirc a_2) \circledcirc a_3) \circledcirc \cdots)\cdots) \circledcirc a_n\}, \quad \forall n \in \mathbb{N}, \tag{1.27}$$

ήτοι ότι το σύνολο $f_n\,(a_1, a_2, \ldots, a_n)$ αποτελείται από το *ένα και μόνον στοιχείο* που αποκτάται ύστερα από την «πλέον συνήθη» (ήτοι *διαδοχική*, ανά δύο όρους εκτελούμενη) αναγραφή παρενθέσεων. (Εάν λοιπόν αποδειχθεί η (1.27), τότε αποδεικνύεται *αυτομάτως* και η πρόταση 1.6.40). Όταν $n \leqslant 3$, η (1.27) είναι προφανής. Για $n \geqslant 4$ εφαρμόζουμε τη δεύτερη μορφή τής μαθηματικής επαγωγής (θεώρημα 1.6.38) ως προς το n εκκινώντας από το $n_0 = 3$. Η επαγωγική μας υπόθεση είναι η εξής:

$$f_j(\xi_1, \xi_2, \ldots, \xi_j) = \{(\cdots((\xi_1 \circledcirc \xi_2) \circledcirc \xi_3) \circledcirc \cdots)\cdots) \circledcirc \xi_j\},$$

για *οιαδήποτε* $(\xi_1, \xi_2, \ldots, \xi_j) \in A^j$, όπου $j, k \in \mathbb{N}$ και $3 \leqslant j \leqslant k$. Θεωρούμε το σύνολο

$$f_{k+_{\mathbb{N}}1}\,(a_1, \ldots, a_{k+_{\mathbb{N}}1}) \subseteq A.$$

Εξ ορισμού, *οιοδήποτε* στοιχείο του $d \in f_{k+_{\mathbb{N}}1}\,(a_1, a_2, \ldots, a_{k+_{\mathbb{N}}1})$ γράφεται υπό τη μορφή

$$d = b \circledcirc c, \quad b \in f_l\,(a_1, \ldots, a_l)\,,\ c \in f_m\,(a_{l+_{\mathbb{N}}1}, \ldots, a_{k+_{\mathbb{N}}1})\,,$$

όπου $l, m \in \mathbb{N}$, τέτοιοι ώστε $l +_{\mathbb{N}} m = k +_{\mathbb{N}} 1$. Εξετάζουμε δύο περιπτώσεις χωριστά:
(a) Εάν $m = 1$, ήτοι $c = a_{k+_{\mathbb{N}}1}$, τότε, κατά την επαγωγική μας υπόθεση,

$$b = (\cdots((a_1 \circledcirc a_2) \circledcirc a_3) \circledcirc \cdots)\cdots) \circledcirc a_k,$$

οπότε

$$d = ((\cdots((a_1 \circledcirc a_2) \circledcirc a_3) \circledcirc \cdots)\cdots) \circledcirc a_k) \circledcirc a_{k+_{\mathbb{N}}1}.$$

(b) Εάν $m > 1$, τότε, σύμφωνα με το (ii) τής προτάσεως 1.6.12 και το (i) τής προτάσεως 1.6.15 υπάρχει (μονοσημάντως ορισμένος) $q \in \mathbb{N}$ με $\theta\,(q) = q +_{\mathbb{N}} 1 = m$, οπότε κατά την επαγωγική μας υπόθεση

$$c = w \circledcirc a_{k+_{\mathbb{N}}1}, \ \text{ για κάποιο } \ w \in f_q\,(a_{l+_{\mathbb{N}}1}, \ldots, a_k)\,,$$

και

$$b = (\cdots((a_1 \circledcirc a_2) \circledcirc a_3) \circledcirc \cdots)\cdots) \circledcirc a_l.$$

Τούτο σημαίνει ότι

$$\begin{aligned} d &= [(\cdots((a_1 \circledcirc a_2) \circledcirc a_3) \circledcirc \cdots)\cdots) \circledcirc a_l] \circledcirc [w \circledcirc a_{k+_{\mathbb{N}}1}] \\ &= [(\cdots((a_1 \circledcirc a_2) \circledcirc a_3) \circledcirc \cdots)\cdots) \circledcirc a_l \circledcirc w] \circledcirc a_{k+_{\mathbb{N}}1} \end{aligned}$$

όπου η τελευταία ισότητα έπεται από τη (συνήθη) προσεταιριστική ιδιότητα. Επειδή η έκφραση

$$(\cdots((a_1 \circledcirc a_2) \circledcirc a_3) \circledcirc \cdots)\cdots) \circledcirc a_l \circledcirc w$$

περιέχει τα k (το πλήθος) στοιχεία $a_1, \ldots, a_k$, εκ νέου εφαρμογή τής επαγωγικής υποθέσεώς μας μάς δίδει

$$(\cdots((a_1 \circledcirc a_2) \circledcirc a_3) \circledcirc \cdots)\cdots) \circledcirc a_l \circledcirc w = (\cdots((a_1 \circledcirc a_2) \circledcirc a_3) \circledcirc \cdots)\cdots) \circledcirc a_k,$$

οπότε τελικώς

$$d = ((\cdots((a_1 \circledcirc a_2) \circledcirc a_3) \circledcirc \cdots)\cdots) \circledcirc a_k) \circledcirc a_{k+_{\mathbb{N}}1}.$$

Από τα (a), (b) και το θεώρημα 1.6.38 συμπεραίνουμε ότι η (1.27) είναι αληθής *για κάθε* $n \in \mathbb{N}$. □

1.7 ΑΚΕΡΑΙΟΙ ΑΡΙΘΜΟΙ

Εάν $m, n \in \mathbb{N}$ και $m \neq n$, τότε (σύμφωνα με το 1.6.27 (iii)) η εξίσωση

$$\boxed{x +_{\mathbb{N}} n = m} \tag{1.28}$$

(με *άγνωστό της* τον x) διαθέτει λύση εντός τού $\mathbb{N}$ μόνον όταν $m > n$. Η αναζήτηση ενός σύνολου «ευρύτερου» τού $\mathbb{N}$, τέτοιου ώστε η (1.28) να διαθέτει πάντοτε λύση εντός αυτού (ακόμη και όταν $m \leqslant n$), μας οδηγεί στον ορισμό τού $\mathbb{Z}$.

1.7.1 Ορισμός. Επί τού καρτεσιανού γινομένου $\mathbb{N} \times \mathbb{N}$ τού συνόλου $\mathbb{N}$ των φυσικών αριθμών με τον εαυτό του ορίζουμε δύο εσωτερικές πράξεις "$+_{\mathbb{N}\times\mathbb{N}}$" και "$\cdot_{\mathbb{N}\times\mathbb{N}}$" μέσω των τύπων

$$\boxed{(m,n) +_{\mathbb{N}\times\mathbb{N}} (m',n') \quad := \quad (m +_{\mathbb{N}} m', n +_{\mathbb{N}} n')} \tag{1.29}$$

και

$$\boxed{(m,n) \cdot_{\mathbb{N}\times\mathbb{N}} (m',n') \quad := \quad ((m \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} n'), (m \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m')),} \tag{1.30}$$

αντιστοίχως, για οιαδήποτε διατεταγμένα ζεύγη $(m,n), (m',n') \in \mathbb{N} \times \mathbb{N}$.

1.7.2 Λήμμα. (i) *Η "$+_{\mathbb{N}\times\mathbb{N}}$" είναι μεταθετική και προσεταιριστική.*
(ii) *Η "$\cdot_{\mathbb{N}\times\mathbb{N}}$" είναι μεταθετική και προσεταιριστική.*

ΑΠΟΔΕΙΞΗ. (i) Για οιαδήποτε $(m,n), (m',n'), (m'',n'') \in \mathbb{N} \times \mathbb{N}$ έχουμε

$$\begin{aligned}
(m,n) +_{\mathbb{N}\times\mathbb{N}} (m',n') &= (m +_{\mathbb{N}} m', n +_{\mathbb{N}} n') \quad \text{(εξ ορισμού)} \\
&= (m' +_{\mathbb{N}} m, n' +_{\mathbb{N}} n) \quad \text{(λόγω τού 1.6.15 (v))} \\
&= (m',n') +_{\mathbb{N}\times\mathbb{N}} (m,n) \quad \text{(εξ ορισμού)}
\end{aligned}$$

και (λόγω τού 1.6.15 (vi))

$$\begin{aligned}
((m,n) +_{\mathbb{N}\times\mathbb{N}} (m',n')) +_{\mathbb{N}\times\mathbb{N}} (m'',n'') &= (m +_{\mathbb{N}} m', n +_{\mathbb{N}} n') +_{\mathbb{N}\times\mathbb{N}} (m'',n'') \\
&= ((m +_{\mathbb{N}} m') +_{\mathbb{N}} m'', (n +_{\mathbb{N}} n') +_{\mathbb{N}} n'') \\
&= (m +_{\mathbb{N}} (m' +_{\mathbb{N}} m''), n +_{\mathbb{N}} (n' +_{\mathbb{N}} n'')) \\
&= (m,n) +_{\mathbb{N}\times\mathbb{N}} ((m',n') +_{\mathbb{N}\times\mathbb{N}} (m'',n'')).
\end{aligned}$$

Άρα η "$+_{\mathbb{N}\times\mathbb{N}}$" είναι μεταθετική και προσεταιριστική.
(ii) Για οιαδήποτε $(m,n), (m',n'), (m'',n'') \in \mathbb{N} \times \mathbb{N}$ έχουμε

$$\begin{aligned}
&(m,n) \cdot_{\mathbb{N}\times\mathbb{N}} (m',n') = ((m \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} n'), (m \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m')) \quad \text{(εξ ορισμού)} \\
&= ((m' \cdot_{\mathbb{N}} m) +_{\mathbb{N}} (n' \cdot_{\mathbb{N}} n), (n' \cdot_{\mathbb{N}} m) +_{\mathbb{N}} (m' \cdot_{\mathbb{N}} n)) \quad \text{(λόγω τού 1.6.18 (v))} \\
&= ((m' \cdot_{\mathbb{N}} m) +_{\mathbb{N}} (n' \cdot_{\mathbb{N}} n), (m' \cdot_{\mathbb{N}} n) +_{\mathbb{N}} (n' \cdot_{\mathbb{N}} m)) \quad \text{(λόγω τού 1.6.15 (v))} \\
&= (m',n') \cdot_{\mathbb{N}\times\mathbb{N}} (m,n) \quad \text{(εξ ορισμού)}
\end{aligned}$$

και

$$\begin{aligned}
&((m,n) \cdot_{\mathbb{N}\times\mathbb{N}} (m',n')) \cdot_{\mathbb{N}\times\mathbb{N}} (m'',n'') \\
= \ &((m \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} n'), (m \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m')) \cdot_{\mathbb{N}\times\mathbb{N}} (m'',n'') \\
= \ &(((m \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} n')) \cdot_{\mathbb{N}} m'' +_{\mathbb{N}} ((m \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m')) \cdot_{\mathbb{N}} n'', \\
&((m \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} n')) \cdot_{\mathbb{N}} n'' +_{\mathbb{N}} ((m \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m')) \cdot_{\mathbb{N}} m'')) \\
= \ &((m \cdot_{\mathbb{N}} m') \cdot_{\mathbb{N}} m'' +_{\mathbb{N}} (n \cdot_{\mathbb{N}} n') \cdot_{\mathbb{N}} m'' +_{\mathbb{N}} (m \cdot_{\mathbb{N}} n') \cdot_{\mathbb{N}} n'' +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m') \cdot_{\mathbb{N}} n'', \\
&(m \cdot_{\mathbb{N}} m') \cdot_{\mathbb{N}} n'' +_{\mathbb{N}} (n \cdot_{\mathbb{N}} n') \cdot_{\mathbb{N}} n'' +_{\mathbb{N}} (m \cdot_{\mathbb{N}} n') \cdot_{\mathbb{N}} m'' +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m') \cdot_{\mathbb{N}} m'')),
\end{aligned}$$

καθώς και

$$\begin{aligned}
& (m,n)\cdot_{\mathbb{N}\times\mathbb{N}}\left(\left(m',n'\right)\cdot_{\mathbb{N}\times\mathbb{N}}\left(m'',n''\right)\right)\\
= \;& (m,n)\cdot_{\mathbb{N}\times\mathbb{N}}\left(\left(m'\cdot_{\mathbb{N}} m''\right)+_{\mathbb{N}}\left(n'\cdot_{\mathbb{N}} n''\right),\left(m'\cdot_{\mathbb{N}} n''\right)+_{\mathbb{N}}\left(n'\cdot_{\mathbb{N}} m''\right)\right)\\
= \;& \left(m\cdot_{\mathbb{N}}\left(\left(m'\cdot_{\mathbb{N}} m''\right)+_{\mathbb{N}}\left(n'\cdot_{\mathbb{N}} n''\right)\right)+_{\mathbb{N}} n\cdot_{\mathbb{N}}\left(\left(m'\cdot_{\mathbb{N}} n''\right)+_{\mathbb{N}}\left(n'\cdot_{\mathbb{N}} m''\right)\right),\right.\\
& \left. m\cdot_{\mathbb{N}}\left(\left(m'\cdot_{\mathbb{N}} n''\right)+_{\mathbb{N}}\left(n'\cdot_{\mathbb{N}} m''\right)\right)+_{\mathbb{N}} n\cdot_{\mathbb{N}}\left(\left(m'\cdot_{\mathbb{N}} m''\right)+_{\mathbb{N}}\left(n'\cdot_{\mathbb{N}} n''\right)\right)\right)\\
= \;& \left(m\cdot_{\mathbb{N}}\left(m'\cdot_{\mathbb{N}} m''\right)+_{\mathbb{N}} m\cdot_{\mathbb{N}}\left(n'\cdot_{\mathbb{N}} n''\right)+_{\mathbb{N}} n\cdot_{\mathbb{N}}\left(m'\cdot_{\mathbb{N}} n''\right)+_{\mathbb{N}} n\cdot_{\mathbb{N}}\left(n'\cdot_{\mathbb{N}} m''\right),\right.\\
& \left. m\cdot_{\mathbb{N}}\left(m'\cdot_{\mathbb{N}} n''\right)+_{\mathbb{N}} m\cdot_{\mathbb{N}}\left(n'\cdot_{\mathbb{N}} m''\right)+_{\mathbb{N}} n\cdot_{\mathbb{N}}\left(m'\cdot_{\mathbb{N}} m''\right)+_{\mathbb{N}} n\cdot_{\mathbb{N}}\left(n'\cdot_{\mathbb{N}} n''\right)\right)\\
= \;& \left(\left(m\cdot_{\mathbb{N}} m'\right)\cdot_{\mathbb{N}} m''+_{\mathbb{N}}\left(m\cdot_{\mathbb{N}} n'\right)\cdot_{\mathbb{N}} m''+_{\mathbb{N}}\left(m\cdot_{\mathbb{N}} n'\right)\cdot_{\mathbb{N}} n''+_{\mathbb{N}}\left(n\cdot_{\mathbb{N}} m'\right)\cdot_{\mathbb{N}} n'',\right.\\
& \left.\left(m\cdot_{\mathbb{N}} m'\right)\cdot_{\mathbb{N}} n''+_{\mathbb{N}}\left(n\cdot_{\mathbb{N}} n'\right)\cdot_{\mathbb{N}} n''+_{\mathbb{N}}\left(m\cdot_{\mathbb{N}} n'\right)\cdot_{\mathbb{N}} m''+_{\mathbb{N}}\left(n\cdot_{\mathbb{N}} m'\right)\cdot_{\mathbb{N}} m''\right),
\end{aligned}$$

(ύστερα από εφαρμογή των 1.6.18 (vii), 1.6.15 (v)), οπότε

$$\left((m,n)\cdot_{\mathbb{N}\times\mathbb{N}}\left(m',n'\right)\right)\cdot_{\mathbb{N}\times\mathbb{N}}\left(m'',n''\right)=(m,n)\cdot_{\mathbb{N}\times\mathbb{N}}\left(\left(m',n'\right)\cdot_{\mathbb{N}\times\mathbb{N}}\left(m'',n''\right)\right).$$

Ως εκ τούτου, η "$\cdot_{\mathbb{N}\times\mathbb{N}}$" είναι μεταθετική και προσεταιριστική. □

1.7.3 Ορισμός. Επί τού καρτεσιανού γινομένου $\mathbb{N}\times\mathbb{N}$ τού συνόλου $\mathbb{N}$ των φυσικών αριθμών με τον εαυτό του ορίζουμε τη διμελή σχέση "$\sim$" ως ακολούθως:

$$\boxed{(m,n)\sim(m',n')\underset{\text{ορσ}}{\Longleftrightarrow} m+_{\mathbb{N}} n'=n+_{\mathbb{N}} m'.} \tag{1.31}$$

1.7.4 Λήμμα. *Η "$\sim$" είναι μια σχέση ισοδυναμίας επί τού $\mathbb{N}\times\mathbb{N}$.*

Απόδειξη. Για οιαδήποτε $(m,n),(m',n'),(m'',n'')\in\mathbb{N}\times\mathbb{N}$ έχουμε

$$\text{1.6.15 (v)}\Rightarrow m+_{\mathbb{N}} n=n+_{\mathbb{N}} m\Rightarrow(m,n)\sim(m,n),$$

τις συνεπαγωγές

$$(m,n)\sim\left(m',n'\right)\underset{\text{1.6.15 (v)}}{\Longrightarrow} m'+_{\mathbb{N}} n=n'+_{\mathbb{N}} m\Rightarrow\left(m',n'\right)\sim(m,n),$$

καθώς και τις

$$\left.\begin{array}{rc}(m,n)\sim(m',n')\\ \text{και}\quad (m',n')\sim(m'',n'')\end{array}\right\}\Rightarrow m+_{\mathbb{N}} n'=n+_{\mathbb{N}} m'\ \text{ και }\ m'+_{\mathbb{N}} n''=n'+_{\mathbb{N}} m'',$$

οπότε προσθέτοντας τις δύο τελευταίες ισότητες κατά μέλη και κάνοντας χρήση τής μεταθετικότητας τής "$+_{\mathbb{N}}$" και τού νόμου τής διαγραφής γι' αυτήν (βλ. 1.6.15 (v) και (viii)) λαμβάνουμε $m+_{\mathbb{N}} n''=n+_{\mathbb{N}} m''\Rightarrow(m,n)\sim(m'',n'')$. Άρα η "$\sim$" είναι ανακλαστική, συμμετρική και μεταβατική. □

1.7.5 Λήμμα. *Η "$\sim$" είναι συμβατή τόσον με την "$+_{\mathbb{N}\times\mathbb{N}}$" όσον και με την "$\cdot_{\mathbb{N}\times\mathbb{N}}$".*

Απόδειξη. Εάν $(m,n),(m',n'),(k,l),(k',l')\in\mathbb{N}\times\mathbb{N}$ με

$$(m,n)\sim\left(m',n'\right)\ \text{ και }\ (k,l)\sim(k',l'), \tag{1.32}$$

τότε[35]

$$\left.\begin{array}{rc}m+_{\mathbb{N}} n'=n+_{\mathbb{N}} m'\\ k+_{\mathbb{N}} l'=l+_{\mathbb{N}} k'\end{array}\right\}\underset{\text{1.6.15 (v)}}{\Longrightarrow} m+_{\mathbb{N}} k+_{\mathbb{N}} n'+_{\mathbb{N}} l'=n+_{\mathbb{N}} l+_{\mathbb{N}} m'+_{\mathbb{N}} k',$$

[35] Εδώ προσθέτουμε τις δύο ισότητες κατά μέλη και κατόπιν εναλλάσσουμε τους προσθετέους κάνοντας χρήση τού ότι η "$+_{\mathbb{N}}$" είναι μεταθετική.

οπότε $(m,n)+_{\mathbb{N}\times\mathbb{N}}(k,l)\sim(m',n')+_{\mathbb{N}\times\mathbb{N}}(k',l')$. Εξάλλου, υπό την ίδια προϋπόθεση (1.32) συνάγεται ότι

$$k\cdot_{\mathbb{N}}(m+_{\mathbb{N}}n')=k\cdot_{\mathbb{N}}(n+_{\mathbb{N}}m'),\quad l\cdot_{\mathbb{N}}(n+_{\mathbb{N}}m')=l\cdot_{\mathbb{N}}(m+_{\mathbb{N}}n'),$$
$$m'\cdot_{\mathbb{N}}(k+_{\mathbb{N}}l')=m'\cdot_{\mathbb{N}}(l+_{\mathbb{N}}k'),\quad n'\cdot_{\mathbb{N}}(l+_{\mathbb{N}}k')=n'\cdot_{\mathbb{N}}(k+_{\mathbb{N}}l').$$

Προσθέτοντας κατά μέλη αυτές τις ισότητες, εκτελώντας τούς πολλαπλασιασμούς "$\cdot_{\mathbb{N}}$" επιμεριστικώς ως προς την πρόσθεση "$+_{\mathbb{N}}$" και κάνοντας χρήση τού νόμου τής διαγραφής για την "$+_{\mathbb{N}}$" και τής μεταθετικής ιδιότητας τής "$\cdot_{\mathbb{N}}$" (βλ. 1.6.15 (viii) και 1.6.18 (v), (vi)) καταλήγουμε στην ισότητα

$$(m\cdot_{\mathbb{N}}k)+_{\mathbb{N}}(n\cdot_{\mathbb{N}}l)+_{\mathbb{N}}(m'\cdot_{\mathbb{N}}l')+_{\mathbb{N}}(n'\cdot_{\mathbb{N}}k')=(m\cdot_{\mathbb{N}}l)+_{\mathbb{N}}(n\cdot_{\mathbb{N}}k)+_{\mathbb{N}}(m'\cdot_{\mathbb{N}}k')(n'\cdot_{\mathbb{N}}l'),$$

οπότε $(m,n)\cdot_{\mathbb{N}\times\mathbb{N}}(k,l)\sim(m',n')\cdot_{\mathbb{N}\times\mathbb{N}}(k',l')$. □

1.7.6 Ορισμός. Το **σύνολο των ακεραίων αριθμών** ορίζεται να είναι το σύνολο των κλάσεων ισοδυναμίας

$$\boxed{\mathbb{Z}:=(\mathbb{N}\times\mathbb{N})\,/\sim}\tag{1.33}$$

ως προς την ανωτέρω ορισθείσα "$\sim$" (βλ. (1.31)). Οι κλάσεις ισοδυναμίας

$$\boxed{[(m,n)]:=\{(p,q)\in\mathbb{N}\times\mathbb{N}\,|(m,n)\sim(p,q)\}}$$

των διατεταγμένων ζευγών $(m,n)\in\mathbb{N}\times\mathbb{N}$ ως προς την "$\sim$" καλούνται **ακέραιοι αριθμοί**.

1.7.7 Σημείωση. Για να αντιληφθεί κανείς την ιδέα που υποβόσκει πίσω από την κατά τι *φορμαλιστική* κατασκευή (1.33) τού $\mathbb{Z}$ θα πρέπει να ανατρέξει εκ νέου στη εξίσωση (1.28). Εάν θεωρούσαμε «διαφορές» "$m-n$" ως *άτυπες οντότητες* οι οποίες θα όφειλαν να απαρτίζουν το $\mathbb{Z}$ (ασχέτως με το εάν ισχύει $m>n$, $m=n$ ή $m<n$), τότε θα σχηματίζαμε μια (εξίσου άτυπη) επιρριπτική απεικόνιση

$$f:\mathbb{N}\times\mathbb{N}\longrightarrow\mathbb{Z},\ (m,n)\longmapsto f(m,n):=\text{“}m-n\text{”}.$$

(Κατ' αυτόν τον τρόπο κατανοείται και η ανάγκη τού να εργαζόμαστε με το καρτεσιανό γινόμενο $\mathbb{N}\times\mathbb{N}$ αντί με το ίδιο το $\mathbb{N}$.) Για τη μετάβαση από αυτήν την επίρριψη σε μια *αμφίρριψη* (που θα συσχέτιζε, κατά κάποιον φυσικό τρόπο, το $\mathbb{N}\times\mathbb{N}$ με το $\mathbb{Z}$) θα αρκούσε να θυμηθούμε το πόρισμα 1.3.26 τού θεμελιώδους θεωρήματος 1.3.25 περί συνόλων κλάσεων ισοδυναμίας. Αυτό θα μας διασφάλιζε πράγματι την ύπαρξη μιας αμφιρρίψεως $\hat{f}:(\mathbb{N}\times\mathbb{N})/\mathcal{R}_f\longrightarrow\mathrm{Im}(f)=\mathbb{Z}$ (που θα ήταν, μάλιστα, και η μοναδική απεικόνιση με την ιδιότητα $f=\hat{f}\circ\pi_{\mathcal{R}_f}$). Τι θα σήμαινε όμως ότι ένα διατεταγμένο ζεύγος στοιχείων τού $\mathbb{N}\times\mathbb{N}$ ανήκει στην $\mathcal{R}_f$; Ιδού το αποτέλεσμα:

$$\big((m,n),(m',n')\big)\in\mathcal{R}_f\underset{\text{ορσ}}{\Longleftrightarrow}f(m,n)=f(m',n')\Leftrightarrow\text{“}m-n\text{”}=\text{“}m'-n'\text{”}.$$

Μεταφέροντας (και πάλι *ατύπως*) το n τού πρώτου μέλους τής τελευταίας «εξισώσεως» στο δεύτερο, καθώς και το n' τού δευτέρου μέλους στο πρώτο, προκύπτει μια *καθ' όλα αποδεκτή ισότητα* μεταξύ αθροισμάτων φυσικών αριθμών:

$$m+_{\mathbb{N}}n'=n+_{\mathbb{N}}m'.$$

Αυτή η συλλογιστική μάς οδηγεί στον ορισμό (1.31) τής "$\sim$" και στην «ταύτιση» τής *άτυπης οντότητας* "$m-n$" με την (*τυπικώς οριζόμενη*) κλάση ισοδυναμίας $[(m,n)]$ τού (m,n).

1.7.8 Θεώρημα. *Επί τού $\mathbb{Z}$ ορίζονται δύο εσωτερικές πράξεις "$+_{\mathbb{Z}}$" και "$\cdot_{\mathbb{Z}}$":*

$$([(m,n)],[(m',n')]) \longmapsto [(m,n)] +_{\mathbb{Z}} [(m',n')],$$
$$([(m,n)],[(m',n')]) \longmapsto [(m,n)] \cdot_{\mathbb{Z}} [(m',n')],$$

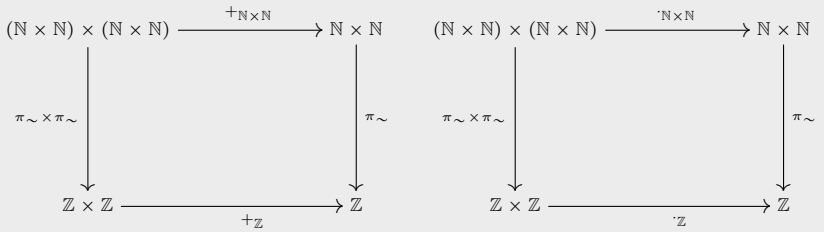
μέσω των τύπων[36]

$$\boxed{[(m,n)] +_{\mathbb{Z}} [(m',n')] \quad := \quad [(m +_{\mathbb{N}} m', n +_{\mathbb{N}} n')]} \tag{1.34}$$

και

$$\boxed{[(m,n)] \cdot_{\mathbb{Z}} [(m',n')] \quad := \quad [((m \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} n'), (m \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m'))]\,,} \tag{1.35}$$

αντιστοίχως. Αυτές είναι οι μοναδικές απεικονίσεις από το $\mathbb{Z} \times \mathbb{Z}$ στο $\mathbb{Z}$ οι οποίες καθιστούν τα διαγράμματα



μεταθετικά.

Απόδειξη. Κατά το λήμμα 1.7.5 η σχέση ισοδυναμίας "$\sim$" είναι συμβατή με αμφότερες τις πράξεις "$+_{\mathbb{N}\times\mathbb{N}}$" και "$\cdot_{\mathbb{N}\times\mathbb{N}}$". Ως εκ τούτου, είναι δυνατή η εφαρμογή τού θεωρήματος 1.5.20 για καθεμιά εξ αυτών και ο προσδιορισμός των μοναδικών απεικονίσεων (1.34) και (1.35) που καθιστούν τα ανωτέρω διαγράμματα μεταθετικά. □

1.7.9 Ορισμός. Οι εσωτερικές πράξεις "$+_{\mathbb{Z}}$" και "$\cdot_{\mathbb{Z}}$" οι ορισθείσες στο θεώρημα 1.7.8 καλούνται **πρόσθεση** και **πολλαπλασιασμός (των ακεραίων αριθμών)**, αντιστοίχως. Εάν $a, b \in \mathbb{Z}$, τότε οι ακέραιοι αριθμοί $a +_{\mathbb{Z}} b$ και $a \cdot_{\mathbb{Z}} b$ καλούνται **άθροισμα** και **γινόμενο των a και b**, αντιστοίχως. Κάθε ακέραιος αριθμός που γράφεται υπό τη μορφή $2 \cdot_{\mathbb{Z}} a$, για κάποιον $a \in \mathbb{Z}$, καλείται **άρτιος**, ενώ κάθε μη άρτιος ακέραιος αριθμός καλείται **περιττός**.

1.7.10 Λήμμα. (i) *Εάν $m, n \in \mathbb{N}$, τότε $[(m,m)] = [(n,n)]$.*

(ii) *Για οιουσδήποτε $m, n, k \in \mathbb{N}$ ισχύει η ισότητα*

$$[(n +_{\mathbb{N}} m, m)] = [(n +_{\mathbb{N}} k, k)].$$

(iii) *Για οιουσδήποτε $m, n, k \in \mathbb{N}$ ισχύει η ισότητα*

$$[(m +_{\mathbb{N}} k, n +_{\mathbb{N}} k)] = [(m,n)].$$

[36] Για να εξηγήσει κανείς τον λόγο που οδήγησε στον ορισμό των πράξεων "$+_{\mathbb{N}\times\mathbb{N}}$" και "$\cdot_{\mathbb{N}\times\mathbb{N}}$" μέσω των τύπων (1.29) και (1.30), οι οποίοι δίδουν τους (1.34) και (1.35) (λόγω τής συμβατότητας τής "$\sim$" με αυτές), θα μπορούσε να καταφύγει εκ νέου στο τέχνασμα με τις *άτυπες διαφορές* (βλ. 1.7.7). Σε επίπεδο κλάσεων ισοδυναμίας, το ζητούμενο είναι να ισχύουν οι «ισότητες»

$$\text{“}m - n\text{”} +_{\mathbb{Z}} \text{“}m' - n'\text{”} = \text{“}(m +_{\mathbb{N}} m') - (n +_{\mathbb{N}} n')\text{”},$$
$$\text{“}m - n\text{”} \cdot_{\mathbb{Z}} \text{“}m' - n'\text{”} = \text{“}((m \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} n')) - ((m \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m'))\text{”}.$$

Αποδειξη. Το (i) έπεται άμεσα από τον ορισμό (1.31).

(ii) Προφανώς,

$$1.6.15\ (\mathrm{v}) \Rightarrow n +_{\mathbb{N}} m +_{\mathbb{N}} k = m +_{\mathbb{N}} n +_{\mathbb{N}} k \Rightarrow (m, m +_{\mathbb{N}} n) \sim (k, k +_{\mathbb{N}} n)\,,$$

οπότε $[(n +_{\mathbb{N}} m, m)] = [(n +_{\mathbb{N}} k, k)]$ (βλ. 1.3.14 (ii)).

(iii) Παρομοίως,

$$m +_{\mathbb{N}} k +_{\mathbb{N}} n = n +_{\mathbb{N}} k +_{\mathbb{N}} m \Rightarrow (m +_{\mathbb{N}} k, n +_{\mathbb{N}} k) \sim (m, n)\,,$$

οπότε $[(m +_{\mathbb{N}} k, n +_{\mathbb{N}} k)] = [(m, n)]$. □

1.7.11 Ορισμός. (i) Το στοιχείο $0_{\mathbb{Z}} := [(1,1)]$ τού $\mathbb{Z}$ ονομάζεται **μηδέν** (ή, ακριβέστερα, **μηδενικό στοιχείο**) **τού** $\mathbb{Z}$. Σημειωτέον ότι δυνάμει τού 1.7.10 (i) ισχύει η ισότητα

$$0_{\mathbb{Z}} = [(m, m)]\,,\ \forall m \in \mathbb{N}. \tag{1.36}$$

(ii) Το $1_{\mathbb{Z}} := [(2,1)]$ ονομάζεται **μοναδιαίο στοιχείο τού** $\mathbb{Z}$. Κατά το 1.7.10 (ii) (εφαρμοζόμενο για $n = k = 1$) έχουμε

$$1_{\mathbb{Z}} = [(m +_{\mathbb{N}} 1, m)]\,,\ \forall m \in \mathbb{N}. \tag{1.37}$$

(iii) Εάν $a = [(m,n)] \in \mathbb{Z}$, τότε λέμε ότι ο ακέραιος αριθμός

$$-a := [(n, m)]$$

είναι **ο αντίθετος τού** a.

1.7.12 Παρατήρηση. Προφανώς, $2 +_{\mathbb{N}} 1 \neq 2 = 1 +_{\mathbb{N}} 1 \Rightarrow 1_{\mathbb{Z}} \neq 0_{\mathbb{Z}}$. (Βλ. 1.6.24 (i)).

1.7.13 Πρόταση (Ιδιότητες προσθέσεως). *Η πρόσθεση ακεραίων αριθμών έχει τις εξής ιδιότητες*:

(i) **[Μεταθετική ιδιότητα]** $a +_{\mathbb{Z}} b = b +_{\mathbb{Z}} a$, $\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}$.

(ii) **[Προσεταιριστική ιδιότητα]** *Για οιουσδήποτε* $a, b, c \in \mathbb{Z}$ *ισχύει η ισότητα*

$$(a +_{\mathbb{Z}} b) +_{\mathbb{Z}} c = a +_{\mathbb{Z}} (b +_{\mathbb{Z}} c)\,.$$

(iii) **[Νόμος τής διαγραφής]** *Για οιουσδήποτε* $a, b, c \in \mathbb{Z}$ *ισχύει η συνεπαγωγή*

$$a +_{\mathbb{Z}} c = b +_{\mathbb{Z}} c \Longrightarrow a = b.$$

(iv) **[Ύπαρξη ουδετέρου στοιχείου]** *Το* $0_{\mathbb{Z}}$ *είναι ουδέτερο στοιχείο τού* $\mathbb{Z}$ *ως προς την* "$+_{\mathbb{Z}}$" (βλ. 1.5.6), *δηλαδή*

$$0_{\mathbb{Z}} +_{\mathbb{Z}} a = a = a +_{\mathbb{Z}} 0_{\mathbb{Z}},\ \ \forall a \in \mathbb{Z}.$$

(v) **[Ύπαρξη συμμετρικού στοιχείου]** *Κάθε* $a \in \mathbb{Z}$ *έχει τον αντίθετό του ως συμμετρικό του στοιχείο ως προς την* "$+_{\mathbb{Z}}$" (βλ. 1.5.11), *δηλαδή*

$$(-a) +_{\mathbb{Z}} a = 0_{\mathbb{Z}} = a +_{\mathbb{Z}} (-a)\,.$$

Αποδειξη. Τα (i) και (ii) έπονται άμεσα από το (i) τού λήμματος 1.7.2, το θεώρημα 1.7.8 και τα (b) και (c) τού θεωρήματος 1.5.20.

(iii) Εάν οι $a = [(m,n)]$, $b = [(m',n')]$ και $c = [(m'',n'')]$ είναι τέτοιοι ώστε να ισχύει η ισότητα $a +_{\mathbb{Z}} c = b +_{\mathbb{Z}} c$, τότε

$$\begin{aligned}
&[(m +_{\mathbb{N}} m'', n +_{\mathbb{N}} n'')] = [(m' +_{\mathbb{N}} m'', n' +_{\mathbb{N}} n'')] \\
&\underset{\text{1.3.14 (ii)}}{\Longrightarrow} (m +_{\mathbb{N}} m'', n +_{\mathbb{N}} n'') \sim (m' +_{\mathbb{N}} m'', n' +_{\mathbb{N}} n'') \\
&\Longrightarrow m +_{\mathbb{N}} m'' +_{\mathbb{N}} n' +_{\mathbb{N}} n'' = n +_{\mathbb{N}} n'' +_{\mathbb{N}} m' +_{\mathbb{N}} m'' \\
&\underset{\text{1.6.15 (viii)}}{\Longrightarrow} m +_{\mathbb{N}} n' = n +_{\mathbb{N}} m' \Longrightarrow (m,n) \sim (m',n'),
\end{aligned}$$

οπότε $a = [(m,n)] = [(m',n')] = b$.

(iv) Εάν $a = [(m,n)]$, τότε

$$0_{\mathbb{Z}} +_{\mathbb{Z}} a = [(1,1)] +_{\mathbb{Z}} [(m,n)] = [(m +_{\mathbb{N}} 1, n +_{\mathbb{N}} 1)] = [(m,n)] = a,$$

όπου η προτελευταία ισότητα έπεται από το (iii) τού λήμματος 1.7.10. Άρα το $0_{\mathbb{Z}}$ είναι εξ αριστερών ουδέτερο στοιχείο τού $\mathbb{Z}$ ως προς την "$+_{\mathbb{Z}}$" και, κατ' επέκταση, (αμφιπλεύρως) ουδέτερο, διότι η "$+_{\mathbb{Z}}$" (κατά το (i)) είναι μεταθετική (βλ. 1.5.9).

(v) Εάν $a = [(m,n)]$, τότε

$$(-a) +_{\mathbb{Z}} a = [(n,m)] +_{\mathbb{Z}} [(m,n)] = [(n +_{\mathbb{N}} m, m +_{\mathbb{N}} n)] = [(m +_{\mathbb{N}} n, m +_{\mathbb{N}} n)] = 0_{\mathbb{Z}},$$

όπου η τελευταία ισότητα προκύπτει από την (1.36). Άρα το $-a$ είναι εξ αριστερών συμμετρικό στοιχείο τού a ως προς την "$+_{\mathbb{Z}}$" και, κατ' επέκταση, συμμετρικό τού a ως προς την "$+_{\mathbb{Z}}$", διότι η "$+_{\mathbb{Z}}$" (κατά το (i)) είναι μεταθετική. (Βλ. 1.5.14.) □

1.7.14 Σημείωση. Εάν $a, b \in \mathbb{Z}$, τότε ο ακέραιος $a +_{\mathbb{Z}} (-b)$ καλείται **διαφορά** τού a από τον b (σημειούμενος συνήθως ως $a - b$). Θα πρέπει να επισημανθεί ότι η εσωτερική πράξη $\mathbb{Z} \times \mathbb{Z} \ni (a,b) \longmapsto a +_{\mathbb{Z}} (-b) \in \mathbb{Z}$ επί τού $\mathbb{Z}$ **(πράξη αφαιρέσεως)** *δεν είναι ούτε* μεταθετική *ούτε* προσεταιριστική. Επίσης, το $0_{\mathbb{Z}}$ αποτελεί εκ δεξιών αλλά όχι και εξ αριστερών ουδέτερο στοιχείο τού $\mathbb{Z}$ ως προς αυτήν.

1.7.15 Πρόταση (Ιδιότητες πολλαπλασιασμού). *Ο πολλαπλασιασμός ακεραίων αριθμών έχει τις εξής ιδιότητες*:

(i) **[Μεταθετική ιδιότητα]** $a \cdot_{\mathbb{Z}} b = b \cdot_{\mathbb{Z}} a$, $\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}$.

(ii) **[Προσεταιριστική ιδιότητα]** *Για οιουσδήποτε* $a, b, c \in \mathbb{Z}$ *ισχύει η ισότητα*

$$(a \cdot_{\mathbb{Z}} b) \cdot_{\mathbb{Z}} c = a \cdot_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} c).$$

(iii) *Για οιονδήποτε* $a \in \mathbb{Z}$ *ισχύουν οι ισότητες*

$$0_{\mathbb{Z}} \cdot_{\mathbb{Z}} a = 0_{\mathbb{Z}} = a \cdot_{\mathbb{Z}} 0_{\mathbb{Z}}.$$

(iv) **[Ύπαρξη ουδετέρου στοιχείου]** *Το* $1_{\mathbb{Z}}$ *είναι ουδέτερο στοιχείο τού* $\mathbb{Z}$ *ως προς την* "$\cdot_{\mathbb{Z}}$" (βλ. 1.5.6), *δηλαδή*

$$1_{\mathbb{Z}} \cdot_{\mathbb{Z}} a = a = a \cdot_{\mathbb{Z}} 1_{\mathbb{Z}}, \quad \forall a \in \mathbb{Z}.$$

(v) *Για οιουσδήποτε* $a, b \in \mathbb{Z}$ *ισχύουν οι ισότητες*

$$(-a) \cdot_{\mathbb{Z}} b = -(a \cdot_{\mathbb{Z}} b) = a \cdot_{\mathbb{Z}} (-b), \quad (-a) \cdot_{\mathbb{Z}} (-b) = a \cdot_{\mathbb{Z}} b.$$

(vi) **[Επιμεριστική ιδιότητα τού πολλαπλασιασμού ως προς την πρόσθεση]** *Για οιουσδήποτε* $a, b, c \in \mathbb{Z}$ *ισχύουν οι ισότητες*

$$a \cdot_{\mathbb{Z}} (b +_{\mathbb{Z}} c) = (a \cdot_{\mathbb{Z}} b) +_{\mathbb{Z}} (a \cdot_{\mathbb{Z}} c), \quad (a +_{\mathbb{Z}} b) \cdot_{\mathbb{Z}} c = (a \cdot_{\mathbb{Z}} c) +_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} c).$$

(vii) *Εάν* $a, b \in \mathbb{Z}$ *με* $a \cdot_{\mathbb{Z}} b = 0_{\mathbb{Z}}$, *τότε είτε* $a = 0_{\mathbb{Z}}$ *είτε* $b = 0_{\mathbb{Z}}$.

(viii) **[Νόμος τής διαγραφής]** *Για* $a, b, c \in \mathbb{Z}$ *με* $c \neq 0_{\mathbb{Z}}$ *ισχύει η συνεπαγωγή*

$$a \cdot_{\mathbb{Z}} c = b \cdot_{\mathbb{Z}} c \Longrightarrow a = b.$$

ΑΠΟΔΕΙΞΗ. Τα (i) και (ii) έπονται άμεσα από το (ii) τού λήμματος 1.7.2, το θεώρημα 1.7.8 και τα (b) και (c) τού θεωρήματος 1.5.20.

(iii) Εάν $a = [(m, n)]$, τότε

$$\begin{aligned} 0_{\mathbb{Z}} \cdot_{\mathbb{Z}} a &= [(1,1)] \cdot_{\mathbb{Z}} [(m,n)] = [((1 \cdot_{\mathbb{N}} m) +_{\mathbb{N}} (1 \cdot_{\mathbb{N}} n), (1 \cdot_{\mathbb{N}} n) +_{\mathbb{N}} (1 \cdot_{\mathbb{N}} m))] \\ &= [(m +_{\mathbb{N}} n, n +_{\mathbb{N}} m)] = [(m +_{\mathbb{N}} n, m +_{\mathbb{N}} n)] = 0_{\mathbb{Z}} \end{aligned}$$

(λόγω των 1.6.18 (iii), 1.6.15 (v) και (1.36)). Η ισότητα $a \cdot_{\mathbb{Z}} 0_{\mathbb{Z}} = 0_{\mathbb{Z}}$ είναι προφανής, διότι η "$\cdot_{\mathbb{Z}}$" (κατά το (i)) είναι μεταθετική.

(iv) Εάν $a = [(m, n)]$, τότε

$$\begin{aligned} 1_{\mathbb{Z}} \cdot_{\mathbb{Z}} a &= [(2,1)] \cdot_{\mathbb{Z}} [(m,n)] = [((2 \cdot_{\mathbb{N}} m) +_{\mathbb{N}} (1 \cdot_{\mathbb{N}} n), (2 \cdot_{\mathbb{N}} n) +_{\mathbb{N}} (1 \cdot_{\mathbb{N}} m))] \\ &= [((2 \cdot_{\mathbb{N}} m) +_{\mathbb{N}} n, (2 \cdot_{\mathbb{N}} n) +_{\mathbb{N}} m)] = [(m,n)] = a, \end{aligned}$$

όπου η προτελευταία ισότητα έπεται από τον ορισμό (1.31) τής "$\sim$". Η ισότητα $a \cdot_{\mathbb{Z}} 1_{\mathbb{Z}} = a$ είναι προφανής, διότι η "$\cdot_{\mathbb{Z}}$" (κατά το (i)) είναι μεταθετική.

(v) Εάν $a = [(m, n)]$, $b = [(m', n')]$, τότε

$$\begin{aligned} (-a) \cdot_{\mathbb{Z}} b &= [(n,m)] \cdot_{\mathbb{Z}} \left[(m',n')\right] = \left[((n \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (m \cdot_{\mathbb{N}} n'), (n \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (m \cdot_{\mathbb{N}} m'))\right] \\ &= \left[(m \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m'), (m \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} n'))\right] = -\left(a \cdot_{\mathbb{Z}} b\right). \end{aligned}$$

Παρομοίως αποδεικνύεται ότι και οι άλλες ισότητες είναι αληθείς.

(vi) Εάν $a = [(m, n)]$, $b = [(m', n')]$ και $c = [(m'', n'')]$, τότε

$$\begin{aligned} &[(m,n)] \cdot_{\mathbb{Z}} ([(m',n')] +_{\mathbb{Z}} [(m'',n'')]) = [(m,n)] \cdot_{\mathbb{Z}} [(m' +_{\mathbb{N}} m'', n' +_{\mathbb{N}} n'')] \\ &= [(m \cdot_{\mathbb{N}} (m' +_{\mathbb{N}} m'') + n \cdot_{\mathbb{N}} (n' +_{\mathbb{N}} n''), m \cdot_{\mathbb{N}} (n' +_{\mathbb{N}} n'') + n \cdot_{\mathbb{N}} (m' +_{\mathbb{N}} m''))] \\ &= [((m \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} n'), (m \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m'))] \\ &+ [((m \cdot_{\mathbb{N}} m'') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} n''), (m \cdot_{\mathbb{N}} n'') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m''))] \end{aligned}$$

(λόγω τού 1.6.18 (vii)). Η άλλη ισότητα είναι προφανής, διότι η "$\cdot_{\mathbb{Z}}$" (κατά το (i)) είναι μεταθετική.

(vii) Εάν οι $a = [(m, n)]$, $b = [(m', n')] \in \mathbb{Z}$ είναι τέτοιοι ώστε να ισχύει η ισότητα $a \cdot_{\mathbb{Z}} b = 0_{\mathbb{Z}}$, τότε

$$\left[\left((m \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} n'), (m \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m')\right)\right] = [(1,1)],$$

οπότε $(m \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} n') = (m \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m')$. Ας υποθέσουμε, δίχως βλάβη τής γενικότητας, ότι $a \neq 0_{\mathbb{Z}}$, δηλαδή ότι $[(m, n)] \neq [(1, 1)]$. Τότε $m \neq n$. Επί τη βάσει τού νόμου τής τριχοτομίας 1.6.25 οφείλουμε να διακρίνουμε δύο περιπτώσεις:

(a) Εάν $m > n$, τότε υπάρχει κάποιος $k \in \mathbb{N}$, τέτοιος ώστε $m = n +_{\mathbb{N}} k$. Επομένως,

$$\begin{aligned} &((n +_{\mathbb{N}} k) \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} n') = ((n +_{\mathbb{N}} k) \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m') \\ &\underset{\text{1.6.18 (vii)}}{\Longrightarrow} (n \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (k \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} n') = (n \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (k \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m') \\ &\underset{\text{1.6.15 (viii)}}{\Longrightarrow} k \cdot_{\mathbb{N}} m' = k \cdot_{\mathbb{N}} n' \underset{\text{1.6.27 (x)}}{\Longrightarrow} m' = n' \Longrightarrow b = 0_{\mathbb{Z}}. \end{aligned}$$

(b) Εάν $n > m$, τότε υπάρχει κάποιος $l \in \mathbb{N}$, τέτοιος ώστε $n = m +_{\mathbb{N}} l$. Επομένως,

$$\begin{aligned} &(m \cdot_{\mathbb{N}} m') +_{\mathbb{N}} ((m +_{\mathbb{N}} l) \cdot_{\mathbb{N}} n') = (m \cdot_{\mathbb{N}} n') +_{\mathbb{N}} ((m +_{\mathbb{N}} l) \cdot_{\mathbb{N}} m')) \\ &\underset{\text{1.6.18 (vii)}}{\Longrightarrow} (m \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (m \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (l \cdot_{\mathbb{N}} n') = (m \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (m \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (l \cdot_{\mathbb{N}} m') \\ &\underset{\text{1.6.15 (viii)}}{\Longrightarrow} l \cdot_{\mathbb{N}} n' = l \cdot_{\mathbb{N}} m' \underset{\text{1.6.27 (x)}}{\Longrightarrow} m' = n' \Longrightarrow b = 0_{\mathbb{Z}}. \end{aligned}$$

(viii) Εάν οι $a, b \in \mathbb{Z}$ και $c \in \mathbb{Z} \setminus \{0_{\mathbb{Z}}\}$ είναι τέτοιοι ώστε να ισχύει η ισότητα

$$a \cdot_{\mathbb{Z}} c = b \cdot_{\mathbb{Z}} c,$$

τότε από τα (v) και (vi) λαμβάνουμε $(a +_{\mathbb{Z}} (-b)) \cdot_{\mathbb{Z}} c = (a \cdot_{\mathbb{Z}} c) +_{\mathbb{Z}} (-(b \cdot_{\mathbb{Z}} c)) = 0_{\mathbb{Z}}$. Σύμφωνα με το (vii), $a +_{\mathbb{Z}} (-b) = 0_{\mathbb{Z}}$, οπότε $a = b$. □

1.7.16 Σημείωση. Εάν $n \in \mathbb{N}$ και $a \in \mathbb{Z}$, τότε λέμε ότι ο ακέραιος

$$a^n := \underbrace{a \cdot_{\mathbb{Z}} a \cdot_{\mathbb{Z}} \cdots \cdot_{\mathbb{Z}} a}_{n \text{ φορές}}$$

είναι ο a **υψωμένος στη δύναμη** n (και ότι ο a^n έχει τον n ως **εκθέτη του**). Οι κατωτέρω ιδιότητες ακεραίων υψούμενων σε δυνάμεις που είναι φυσικοί αριθμοί αποδεικνύονται εύκολα κάνοντας χρήση τού θεωρήματος 1.6.34 τής «κλασικής» μαθηματικής επαγωγής[37]:

(i) Για οιουσδήποτε $m, n \in \mathbb{N}$ και $a \in \mathbb{Z}$ ισχύει η ισότητα

$$a^m \cdot_{\mathbb{Z}} a^n = a^{m +_{\mathbb{N}} n}.$$

(ii) Για οιουσδήποτε $m, n \in \mathbb{N}$ και $a \in \mathbb{Z}$ ισχύει η ισότητα

$$(a^m)^n = a^{m \cdot_{\mathbb{N}} n}.$$

(iii) Για οιουσδήποτε $n \in \mathbb{N}$ και $a, b \in \mathbb{Z}$ ισχύει η ισότητα

$$(a \cdot_{\mathbb{Z}} b)^n = a^n \cdot_{\mathbb{Z}} b^n.$$

▸ **Ο ορισμός τής συνήθους διατάξεως επί τού** $\mathbb{Z}$. Τα στοιχεία τού $\mathbb{Z}$ διατάσσονται κατά τον πλέον «φυσικό» τρόπο ως ακολούθως:

1.7.17 Ορισμός. Έστω $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. Εάν $a = [(m, n)]$, $b = [(m', n')]$, τότε ορίζουμε τη διμελή σχέση[38]

$$a \leqslant_{\mathbb{Z}} b \underset{\text{ορσ}}{\iff} m +_{\mathbb{N}} n' \leqslant n +_{\mathbb{N}} m',$$

όπου "$\leqslant$" η ήδη ορισθείσα σχέση ολικής διατάξεως επί τού συνόλου $\mathbb{N}$ των φυσικών αριθμών (βλ. 1.6.23 και 1.6.26).

(i) Όταν $a \leqslant_{\mathbb{Z}} b$, τότε λέμε ότι ο a είναι **μικρότερος ή ίσος** τού b ή ότι ο b είναι **μεγαλύτερος ή ίσος** τού a (και γράφουμε, εναλλακτικώς, $b \geqslant_{\mathbb{Z}} a$). Επίσης, λέμε ότι ο a είναι **μικρότερος** τού b ή ότι ο b είναι **μεγαλύτερος** τού a (και γράφουμε $a <_{\mathbb{Z}} b$ ή $b >_{\mathbb{Z}} a$) όταν $a \leqslant_{\mathbb{Z}} b$ *και* $a \neq b$.

(ii) Κάθε $a \in \mathbb{Z}$ για τον οποίο ισχύει $a >_{\mathbb{Z}} 0_{\mathbb{Z}}$ (και, αντιστοίχως, $a <_{\mathbb{Z}} 0_{\mathbb{Z}}$) καλείται **θετικός** (και, αντιστοίχως, **αρνητικός**) **ακέραιος αριθμός**.

[37] Για τις (i) και (ii) εφαρμόζουμε το θεώρημα για καθέναν των m, n *χωριστά* (δηλαδή κρατούμε τον έναν εξ αυτών σταθερό και εργαζόμαστε με τον άλλον, και κατόπιν εναλλάσσουμε τους ρόλους τους).

[38] Αυτή η διμελής σχέση *δεν εξαρτάται* από την επιλογή των εκπροσώπων (m, n) και (m', n') των (κλάσεων ισοδυναμίας) a και b, αντιστοίχως, διότι εάν $a = [(m, n)] = [(\overline{m}, \overline{n})]$ και $b = [(m', n')] = [(\overline{m}', \overline{n}')]$, τότε

$$m +_{\mathbb{N}} n' \leqslant n +_{\mathbb{N}} m' \iff \overline{m} +_{\mathbb{N}} \overline{n}' \leqslant \overline{n} +_{\mathbb{N}} \overline{m}'.$$

Πράγματι· επειδή $m +_{\mathbb{N}} \overline{n} = n +_{\mathbb{N}} \overline{m}$ και $m' +_{\mathbb{N}} \overline{n}' = n' +_{\mathbb{N}} \overline{m}'$, έχουμε (λόγω των 1.6.27 (v) και 1.6.15 (v))

$$\begin{aligned} &m +_{\mathbb{N}} n' \leqslant n +_{\mathbb{N}} m' \iff m +_{\mathbb{N}} n' +_{\mathbb{N}} \overline{n} +_{\mathbb{N}} \overline{n}' \leqslant m' +_{\mathbb{N}} n +_{\mathbb{N}} \overline{n} +_{\mathbb{N}} \overline{n}' \\ &\iff \overline{m} +_{\mathbb{N}} n +_{\mathbb{N}} n' +_{\mathbb{N}} \overline{n}' \leqslant \overline{m}' +_{\mathbb{N}} n' +_{\mathbb{N}} n +_{\mathbb{N}} \overline{n} \iff \overline{m} +_{\mathbb{N}} \overline{n}' \leqslant \overline{n} +_{\mathbb{N}} \overline{m}'. \end{aligned}$$

1.7.18 Θεώρημα (Νόμος τής «τριχοτομίας»). *Εάν* $(a,b)\in\mathbb{Z}\times\mathbb{Z}$, *τότε ισχύει ακριβώς ένα εκ των κάτωθι*:

(i) $a=b$.

(ii) $a>_{\mathbb{Z}} b$.

(iii) $a<_{\mathbb{Z}} b$.

Απόδειξη. Εάν $a=[(m,n)]$, $b=[(m',n')]$, τότε, σύμφωνα με τον νόμο τής τριχοτομίας 1.6.25 τον ισχύοντα για τα ζεύγη στοιχείων τού $\mathbb{N}$, ακριβώς ένα εκ των κάτωθι είναι αληθές:

$$m+_{\mathbb{N}} n'=n+_{\mathbb{N}} m',\quad m+_{\mathbb{N}} n'<n+_{\mathbb{N}} m',\quad m+_{\mathbb{N}} n'>n+_{\mathbb{N}} m',$$

οπότε η απόδειξη λήγει εδώ. □

1.7.19 Θεώρημα. *Η διμελής σχέση* "$\leqslant_{\mathbb{Z}}$" *η ορισθείσα επί τού* $\mathbb{Z}$ *στο εδάφιο* 1.7.17 *είναι σχέση ολικής διατάξεως.* (Βλ. 1.4.1.)

Απόδειξη. Η ανακλαστικότητα τής "$\leqslant_{\mathbb{Z}}$" είναι προφανής (διότι $a=a$, $\forall a\in\mathbb{Z}$). Εάν $(a,b)\in\mathbb{Z}\times\mathbb{Z}$, όπου $a\leqslant_{\mathbb{Z}} b$ και (ταυτοχρόνως) $b\leqslant_{\mathbb{Z}} a$, και εάν υποθέσουμε ότι $a\neq b$, τότε $a<_{\mathbb{Z}} b$ και (ταυτοχρόνως) $b<_{\mathbb{Z}} a$, κάτι που είναι άτοπο επί τη βάσει τού νόμου τής τριχοτομίας 1.7.18. Κατ' ανάγκην λοιπόν $a=b$ και η "$\leqslant_{\mathbb{Z}}$" είναι αντισυμμετρική.

Εν συνεχεία θεωρούμε ακεραίους a,b,c, όπου $a=[(m,n)]$, $b=[(m',n')]$ και $c=[(m'',n'')]$, τέτοιους ώστε $a\leqslant_{\mathbb{Z}} b$ και $b\leqslant_{\mathbb{Z}} c$. Τότε

$$\left.\begin{aligned} m+_{\mathbb{N}} n'&\leqslant n+_{\mathbb{N}} m'\\ m'+_{\mathbb{N}} n''&\leqslant n'+_{\mathbb{N}} m''\end{aligned}\right\}\Rightarrow m+_{\mathbb{N}} n'+_{\mathbb{N}} n''\leqslant n+_{\mathbb{N}} m'+_{\mathbb{N}} n''\leqslant n+_{\mathbb{N}} n'+_{\mathbb{N}} m'',$$

οπότε $m'+_{\mathbb{N}} n''\leqslant n'+_{\mathbb{N}} m''$ (λόγω τού 1.6.27 (v)). Άρα η "$\leqslant_{\mathbb{Z}}$" είναι μεταβατική.

Απομένει να αποδειχθεί ότι τα στοιχεία τού $\mathbb{Z}$ είναι μεταξύ τους ανά δύο συγκρίσιμα ως προς την "$\leqslant_{\mathbb{Z}}$". Θεωρούμε λοιπόν τυχόντες $a,b\in\mathbb{Z}$. Εάν $a=b$, τότε εξ ορισμού $a\leqslant_{\mathbb{Z}} b$. Εάν $a\neq b$, τότε ο νόμος τής τριχοτομίας 1.7.18 επιτάσσει είτε την ισχύ τής ανισότητας $a<_{\mathbb{Z}} b$ (οπότε $a\leqslant_{\mathbb{Z}} b$) είτε την ισχύ τής ανισότητας $b<_{\mathbb{Z}} a$ (οπότε $b\leqslant_{\mathbb{Z}} a$). Κατά συνέπειαν, η "$\leqslant_{\mathbb{Z}}$" αποτελεί μια σχέση ολικής διατάξεως επί τού $\mathbb{Z}$. □

1.7.20 Πρόταση (Ιδιότητες διατάξεως). *Εάν* $a,b,c\in\mathbb{Z}$, *τότε ισχύουν τα ακόλουθα*:

(i) *Εάν* $a<_{\mathbb{Z}} b$ *και* $b<_{\mathbb{Z}} c$, *τότε* $b<_{\mathbb{Z}} c$.

(ii) $a<_{\mathbb{Z}} b\Leftrightarrow -b<_{\mathbb{Z}} -a$.

(iii) $0<_{\mathbb{Z}} a\Leftrightarrow -a<_{\mathbb{Z}} 0_{\mathbb{Z}}$.

(iv) $a<_{\mathbb{Z}} b\Leftrightarrow a+_{\mathbb{Z}} c<_{\mathbb{Z}} b+_{\mathbb{Z}} c$.

(v) *Εάν* $a>_{\mathbb{Z}} 0_{\mathbb{Z}}$ *και* $b>_{\mathbb{Z}} 0_{\mathbb{Z}}$, *τότε* $a+_{\mathbb{Z}} b>_{\mathbb{Z}} 0_{\mathbb{Z}}$ *και* $a\cdot_{\mathbb{Z}} b>_{\mathbb{Z}} 0_{\mathbb{Z}}$.

(vi) *Εάν* $a<_{\mathbb{Z}} 0_{\mathbb{Z}}$ *και* $b<_{\mathbb{Z}} 0_{\mathbb{Z}}$, *τότε* $a+_{\mathbb{Z}} b<_{\mathbb{Z}} 0_{\mathbb{Z}}$ *και* $a\cdot_{\mathbb{Z}} b>_{\mathbb{Z}} 0_{\mathbb{Z}}$.

(vii) *Εάν* $a<_{\mathbb{Z}} 0_{\mathbb{Z}}$ *και* $b>_{\mathbb{Z}} 0_{\mathbb{Z}}$, *τότε* $a\cdot_{\mathbb{Z}} b<_{\mathbb{Z}} 0_{\mathbb{Z}}$.

(viii) *Εάν* $c>_{\mathbb{Z}} 0_{\mathbb{Z}}$, *τότε* $a<_{\mathbb{Z}} b\Leftrightarrow (a\cdot_{\mathbb{Z}} c)<_{\mathbb{Z}} (b\cdot_{\mathbb{Z}} c)$.

(ix) *Εάν* $c<_{\mathbb{Z}} 0_{\mathbb{Z}}$, *τότε* $a<_{\mathbb{Z}} b\Leftrightarrow (a\cdot_{\mathbb{Z}} c)>_{\mathbb{Z}} (b\cdot_{\mathbb{Z}} c)$.

Απόδειξη. (i) Τούτο αποδεικνύεται όπως και η μεταβατικότητα τής "$\leqslant_{\mathbb{Z}}$".

(ii) Εάν $a=[(m,n)]$ και $b=[(m',n')]$, τότε από το 1.6.15 (v) έπεται ότι

$$m+_{\mathbb{N}} n'<n+_{\mathbb{N}} m'\Longleftrightarrow n'+_{\mathbb{N}} m<m'+_{\mathbb{N}} n.$$

(iii) Τούτο έπεται από το (ii) και από το γεγονός ότι $0_{\mathbb{Z}} = -0_{\mathbb{Z}}$.

(iv) Εάν $a = [(m, n)]$, $b = [(m', n')]$ και $c = [(m'', n'')]$, τότε

$$m +_{\mathbb{N}} n' < n +_{\mathbb{N}} m' \Longleftrightarrow m +_{\mathbb{N}} m'' +_{\mathbb{N}} n' +_{\mathbb{N}} n'' < n +_{\mathbb{N}} n'' +_{\mathbb{N}} m' +_{\mathbb{N}} m''$$

(λόγω των 1.6.27 (v) και 1.6.15 (v)). Άρα $a <_{\mathbb{Z}} b \Leftrightarrow a +_{\mathbb{Z}} c <_{\mathbb{Z}} b +_{\mathbb{Z}} c$.

(v) Εάν $a = [(m, n)]$ και $b = [(m', n')]$, τότε $m > n$ και $m' > n$. Επομένως,

$$m +_{\mathbb{N}} m' > n +_{\mathbb{N}} n' \Rightarrow a +_{\mathbb{Z}} b >_{\mathbb{Z}} 0_{\mathbb{Z}}$$

(λόγω τού 1.6.27 (vi)). Εξάλλου, επειδή υπάρχουν $k, k' \in \mathbb{N}$, τέτοιοι ώστε

$$m = n +_{\mathbb{N}} k, \;\; m' = n' +_{\mathbb{N}} k',$$

συμπεραίνουμε ύστερα από αντικατάσταση των m, m' (υπ' αυτήν τη μορφή) στην ανισότητα

$$(m \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} n') > (m \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m'), \tag{1.38}$$

εκτέλεση πράξεων και εφαρμογή τού 1.6.27 (v) ότι η (1.38) ισοδυναμεί με την

$$\left(k \cdot_{\mathbb{N}} k'\right) + \left(k \cdot_{\mathbb{N}} n'\right) > \left(k \cdot_{\mathbb{N}} n'\right),$$

η οποία είναι αληθής λόγω τού 1.6.27 (iv). Άρα $a \cdot_{\mathbb{Z}} b >_{\mathbb{Z}} 0_{\mathbb{Z}}$. Τα (vi) και (vii) αποδεικνύονται παρομοίως.

(viii) Εάν $a = [(m, n)]$, $b = [(m', n')]$ και $c = [(m'', n'')]$, και εάν υποθέσουμε ότι $c >_{\mathbb{Z}} 0_{\mathbb{Z}}$, δηλαδή ότι $m'' > n''$, τότε η αμφίπλευρη συνεπαγωγή

$$a <_{\mathbb{Z}} b \Longleftrightarrow (a \cdot_{\mathbb{Z}} c) <_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} c) \tag{1.39}$$

ισοδυναμεί με την αμφίπλευρη συνεπαγωγή

$$k < l \Longleftrightarrow (k \cdot_{\mathbb{N}} m'') +_{\mathbb{N}} (l \cdot_{\mathbb{N}} n'') < (k \cdot_{\mathbb{N}} n'') +_{\mathbb{N}} (l \cdot_{\mathbb{N}} m''), \tag{1.40}$$

όπου $k := m +_{\mathbb{N}} n'$ και $l := n +_{\mathbb{N}} m'$. Επειδή $m'' > n''$, υπάρχει κάποιος $v \in \mathbb{N}$, τέτοιος ώστε να ισχύει $m'' = n'' +_{\mathbb{N}} v$. Εάν υποθέσουμε ότι $k < l$ και εάν λάβουμε υπ' όψιν ότι υπάρχει κάποιος $u \in \mathbb{N}$, τέτοιος ώστε να ισχύει $l = k +_{\mathbb{N}} u$, τότε

$$\begin{aligned}
(k \cdot_{\mathbb{N}} n'') +_{\mathbb{N}} (l \cdot_{\mathbb{N}} m'') &= (k \cdot_{\mathbb{N}} n'') +_{\mathbb{N}} ((k +_{\mathbb{N}} u) \cdot_{\mathbb{N}} m'') \\
&= (k \cdot_{\mathbb{N}} n'') +_{\mathbb{N}} (k \cdot_{\mathbb{N}} m'') +_{\mathbb{N}} (u \cdot_{\mathbb{N}} m'') \\
&= (k \cdot_{\mathbb{N}} n'') +_{\mathbb{N}} (k \cdot_{\mathbb{N}} m'') +_{\mathbb{N}} (u \cdot_{\mathbb{N}} (n'' +_{\mathbb{N}} v)) \\
&= (k \cdot_{\mathbb{N}} n'') +_{\mathbb{N}} (k \cdot_{\mathbb{N}} m'') +_{\mathbb{N}} (u \cdot_{\mathbb{N}} n'') +_{\mathbb{N}} (u \cdot_{\mathbb{N}} v) \\
&= (k \cdot_{\mathbb{N}} m'') +_{\mathbb{N}} (k +_{\mathbb{N}} u) \cdot_{\mathbb{N}} n'' +_{\mathbb{N}} (u \cdot_{\mathbb{N}} v) \\
&= (k \cdot_{\mathbb{N}} m'') +_{\mathbb{N}} (l \cdot_{\mathbb{N}} n'') +_{\mathbb{N}} (u \cdot_{\mathbb{N}} v)
\end{aligned}$$

(λόγω των ιδιοτήτων 1.6.18 (vi) και 1.6.15 (v)). Επειδή $u \cdot_{\mathbb{N}} v \in \mathbb{N}$, βάσει τού ορισμού 1.6.23 συνάγεται ότι

$$(k \cdot_{\mathbb{N}} m'') +_{\mathbb{N}} (l \cdot_{\mathbb{N}} n'') < (k \cdot_{\mathbb{N}} n'') +_{\mathbb{N}} (l \cdot_{\mathbb{N}} m''). \tag{1.41}$$

Και αντιστρόφως· εάν υποθέσουμε ότι ισχύει η ανισότητα (1.41), για να αποδείξουμε την αντίστροφη συνεπαγωγή στην (1.40) είναι αρκετό (λόγω τού νόμου τής τριχοτομίας 1.6.25) να αποκλείσουμε ως ενδεχόμενο το να ισχύει είτε $k = l$ είτε $l < k$. Εάν ίσχυε η ισότητα $k = l$, τότε το αριστερό μέλος τής (1.41) θα ήταν ίσο

με το δεξιό, κάτι που αποκλείεται από την ιδιότητα 1.6.27 (ii). Εάν $l < k$, τότε θα υπήρχε κάποιος $u' \in \mathbb{N}$, τέτοιος ώστε να ισχύει $k = l +_{\mathbb{N}} u'$, οπότε θα είχαμε

$$\begin{aligned}(k \cdot_{\mathbb{N}} m'') +_{\mathbb{N}} (l \cdot_{\mathbb{N}} n'') &= ((l +_{\mathbb{N}} u') \cdot_{\mathbb{N}} n'') +_{\mathbb{N}} ((l \cdot_{\mathbb{N}} m'') \\ &= (l \cdot_{\mathbb{N}} n'') +_{\mathbb{N}} (u' \cdot_{\mathbb{N}} m'') +_{\mathbb{N}} (l \cdot_{\mathbb{N}} m'') \\ &= (l \cdot_{\mathbb{N}} n'') +_{\mathbb{N}} (u' \cdot_{\mathbb{N}} (n'' +_{\mathbb{N}} v)) +_{\mathbb{N}} (l \cdot_{\mathbb{N}} m'') \\ &= (l \cdot_{\mathbb{N}} n'') +_{\mathbb{N}} (u' \cdot_{\mathbb{N}} n'') +_{\mathbb{N}} (u' \cdot_{\mathbb{N}} v) +_{\mathbb{N}} (l \cdot_{\mathbb{N}} m'') \\ &= (l +_{\mathbb{N}} u') \cdot_{\mathbb{N}} n'' +_{\mathbb{N}} (l \cdot_{\mathbb{N}} m'') +_{\mathbb{N}} (u' \cdot_{\mathbb{N}} v) \\ &= (k \cdot_{\mathbb{N}} n'') +_{\mathbb{N}} (l \cdot_{\mathbb{N}} m'') +_{\mathbb{N}} (u' \cdot_{\mathbb{N}} v).\end{aligned}$$

Επειδή $u' \cdot_{\mathbb{N}} v \in \mathbb{N}$, τούτο θα μας οδηγούσε στην ανισότητα

$$(k \cdot_{\mathbb{N}} n'') +_{\mathbb{N}} (l \cdot_{\mathbb{N}} m'') < (k \cdot_{\mathbb{N}} m'') +_{\mathbb{N}} (l \cdot_{\mathbb{N}} n''),$$

η οποία (εκ νέου λόγω τού νόμου τής τριχοτομίας 1.6.25) θα αντέκειτο προς την προϋποτεθείσα (1.41). Άρα κατ' ανάγκην $k < l$. Από τα προαναφερθέντα συμπεραίνουμε ότι η αμφίπλευρη συνεπαγωγή (1.40) είναι όντως αληθής.

(ix) Αυτό έπεται άμεσα από τον συνδυασμό τού 1.7.15 (v) και των ανωτέρω αποδειχθέντων (iii), (ii) και (viii). □

1.7.21 Πόρισμα. *Ένας ακέραιος αριθμός $a \in \mathbb{Z}$ διαθέτει συμμετρικό στοιχείο ως προς την "$\cdot_{\mathbb{Z}}$" εάν και μόνον εάν $a \in \{-1_{\mathbb{Z}}, 1_{\mathbb{Z}}\}$.*

Απόδειξη. Προφανώς, $1_{\mathbb{Z}} \cdot_{\mathbb{Z}} 1_{\mathbb{Z}} = 1_{\mathbb{Z}}$ και $(-1_{\mathbb{Z}}) \cdot_{\mathbb{Z}} (-1_{\mathbb{Z}}) = 1_{\mathbb{Z}}$. Ως εκ τούτου, καθένα εκ των $-1_{\mathbb{Z}}, 1_{\mathbb{Z}}$ έχει τον εαυτό του ως συμμετρικό του στοιχείο ως προς την "$\cdot_{\mathbb{Z}}$". Ας υποθέσουμε, αντιστρόφως, ότι ο $a = [(m, n)]$ έχει ως συμμετρικό του στοιχείο ως προς την "$\cdot_{\mathbb{Z}}$" έναν ακέραιο $b = [(m', n')]$. Τότε $a \cdot_{\mathbb{Z}} b = 1_{\mathbb{Z}}$. Επειδή (προφανώς) $1_{\mathbb{Z}} >_{\mathbb{Z}} 0_{\mathbb{Z}}$, οι a, b είναι είτε *αμφότεροι θετικοί* είτε *αμφότεροι αρνητικοί* (βλ. 1.7.20 (v), (vi) και (vii)). Στην περίπτωση κατά την οποία αμφότεροι οι a, b είναι θετικοί, έχουμε $m > n$ και $m' > n'$. Θα δείξουμε ότι $a = b = 1_{\mathbb{Z}}$. Επειδή

$$(m \cdot_{\mathbb{N}} m') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} n') = (m \cdot_{\mathbb{N}} n') +_{\mathbb{N}} (n \cdot_{\mathbb{N}} m') +_{\mathbb{N}} 1 \tag{1.42}$$

και επειδή υπάρχουν $k, k' \in \mathbb{N}$, τέτοιοι ώστε

$$m = n +_{\mathbb{N}} k, \quad m' = n' +_{\mathbb{N}} k', \tag{1.43}$$

αντικαθιστώντας τούς m, m' (υπ' αυτήν τη μορφή) στην (1.42) και εκτελώντας τις πράξεις (και τις απαλοιφές) κατά τα ειωθότα λαμβάνουμε τελικώς $k \cdot_{\mathbb{N}} k' = 1$. Εάν $k > 1$, τότε, σύμφωνα με το 1.6.27 (ix), θα ίσχυε $1 = k \cdot_{\mathbb{N}} k' > 1 \cdot_{\mathbb{N}} k' = k' \geqslant 1$, πράγμα άτοπο! Κατά συνέπειαν, $k = k' = 1$. Αυτό, σε συνδυασμό με τις ισότητες (1.43) και (1.37), μας οδηγεί στο συμπέρασμα ότι $a = b = 1_{\mathbb{Z}}$. Στην περίπτωση κατά την οποία αμφότεροι οι a, b είναι αρνητικοί, συμπεραίνουμε κατ' αναλογίαν ότι $a = b = -1_{\mathbb{Z}}$.

□

1.7.22 Ορισμός. Θεωρούμε την απεικόνιση

$$\boxed{\iota_{\mathbb{N}} : \mathbb{N} \longrightarrow \mathbb{Z}, \quad n \longmapsto \iota_{\mathbb{N}}(n) := [(n +_{\mathbb{N}} 1, 1)]}$$

Σημειωτέον ότι $\iota_{\mathbb{N}}(n) = [(n +_{\mathbb{N}} m, m)]$, $\forall\, (m, n) \in \mathbb{N} \times \mathbb{N}$ (βλ. 1.7.10 (ii)). Η $\iota_{\mathbb{N}}$ καλείται **φυσική εμφύτευση τού $\mathbb{N}$ εντός τού $\mathbb{Z}$**. Οι κύριες ιδιότητές της παρατίθενται στην επόμενη πρόταση.

1.7.23 Πρόταση. (i) *Η* $\iota_{\mathbb{N}}$ *είναι ενριπτική.*
(ii) $\iota_{\mathbb{N}}(m +_{\mathbb{N}} n) = \iota_{\mathbb{N}}(m) +_{\mathbb{Z}} \iota_{\mathbb{N}}(n), \forall (m,n) \in \mathbb{N} \times \mathbb{N}$.
(iii) $\iota_{\mathbb{N}}(m \cdot_{\mathbb{N}} n) = \iota_{\mathbb{N}}(m) \cdot_{\mathbb{Z}} \iota_{\mathbb{N}}(n), \forall (m,n) \in \mathbb{N} \times \mathbb{N}$.
(iv) *Για οιουσδήποτε* $m, n \in \mathbb{N}$ *ισχύει η αμφίπλευρη συνεπαγωγή*

$$m \leqslant n \Longleftrightarrow \iota_{\mathbb{N}}(m) \leqslant_{\mathbb{Z}} \iota_{\mathbb{N}}(n).$$

(v) $\iota_{\mathbb{N}}(1) = 1_{\mathbb{Z}}$.
(vi) *Για κάθε* $a = [(m,n)] \in \mathbb{Z}$ *ισχύει η ισότητα*[39]

$$a = \iota_{\mathbb{N}}(m) +_{\mathbb{Z}} (-\iota_{\mathbb{N}}(n)). \tag{1.44}$$

(vii) *Για οιονδήποτε* $a = [(m,n)] \in \mathbb{Z}$ *ισχύει η αμφίπλευρη συνεπαγωγή*

$$a >_{\mathbb{Z}} 0_{\mathbb{Z}} \Leftrightarrow \exists k \in \mathbb{N} : a = \iota_{\mathbb{N}}(k). \tag{1.45}$$

Κατά συνέπειαν,

$$\boxed{\mathbb{Z} = \mathrm{Im}(\iota_{\mathbb{N}}) \coprod \{0_{\mathbb{Z}}\} \coprod (-\mathrm{Im}(\iota_{\mathbb{N}}))}, \tag{1.46}$$

όπου $-\mathrm{Im}(\iota_{\mathbb{N}}) := \{-\iota_{\mathbb{N}}(l) \,|\, l \in \mathbb{N}\}$.

Απόδειξη. (i) Εάν $n, n' \in \mathbb{N}$ με $\iota_{\mathbb{N}}(n) = \iota_{\mathbb{N}}(n')$, τότε

$$[(n +_{\mathbb{N}} 1, 1)] = [(n' +_{\mathbb{N}} 1, 1)] \Rightarrow n +_{\mathbb{N}} 2 = n' +_{\mathbb{N}} 2 \underset{1.6.15\ \text{(viii)}}{\Longrightarrow} n = n',$$

οπότε η $\iota_{\mathbb{N}}$ είναι όντως ενριπτική.
(ii) Χρησιμοποιώντας το (iii) τού λήμματος 1.7.10 λαμβάνουμε

$$\begin{aligned} \iota_{\mathbb{N}}(m +_{\mathbb{N}} n) &= [(m +_{\mathbb{N}} n +_{\mathbb{N}} 1, 1)] = [(m +_{\mathbb{N}} n +_{\mathbb{N}} 2, 2)] \\ &= [(m +_{\mathbb{N}} 1, 1)] +_{\mathbb{Z}} [(n +_{\mathbb{N}} 1, 1)] \\ &= \iota_{\mathbb{N}}(m) +_{\mathbb{Z}} \iota_{\mathbb{N}}(n), \ \forall (m,n) \in \mathbb{N} \times \mathbb{N}. \end{aligned}$$

(iii) Χρησιμοποιώντας το (iii) τού λήμματος 1.7.10 λαμβάνουμε

$$\begin{aligned} \iota_{\mathbb{N}}(m \cdot_{\mathbb{N}} n) &= [((m \cdot_{\mathbb{N}} n) +_{\mathbb{N}} 1, 1)] \\ &= [((m \cdot_{\mathbb{N}} n) +_{\mathbb{N}} +_{\mathbb{N}} 1 +_{\mathbb{N}} (m +_{\mathbb{N}} n +_{\mathbb{N}} 1), 1 +_{\mathbb{N}} (m +_{\mathbb{N}} n +_{\mathbb{N}} 1))] \\ &= [((m +_{\mathbb{N}} 1) \cdot_{\mathbb{N}} (n +_{\mathbb{N}} 1) +_{\mathbb{N}} 1, m +_{\mathbb{N}} n +_{\mathbb{N}} 2)] \\ &= [(m +_{\mathbb{N}} 1, 1)] \cdot_{\mathbb{Z}} [(n +_{\mathbb{N}} 1, 1)] \\ &= \iota_{\mathbb{N}}(m) \cdot_{\mathbb{Z}} \iota_{\mathbb{N}}(n), \ \forall (m,n) \in \mathbb{N} \times \mathbb{N}. \end{aligned}$$

(iv) Προφανώς, για οιουσδήποτε $m, n \in \mathbb{N}$ ισχύουν οι αμφίπλευρες συνεπαγωγές

$$\begin{aligned} \iota_{\mathbb{N}}(m) \leqslant_{\mathbb{Z}} \iota_{\mathbb{N}}(n) &\Leftrightarrow [(m +_{\mathbb{N}} 1, 1)] \leqslant_{\mathbb{Z}} [(n +_{\mathbb{N}} 1, 1)] \\ &\Leftrightarrow m +_{\mathbb{N}} 2 \leqslant n +_{\mathbb{N}} 2 \Leftrightarrow m \leqslant n, \end{aligned}$$

όπου η τελευταία έπεται από τα 1.7.13 (iii) και 1.7.20 (iv).
(v) Προφανώς, $\iota_{\mathbb{N}}(1) = [(1 +_{\mathbb{N}} 1, 1)] = [(2,1)] = 1_{\mathbb{Z}}$.
(vi) Για κάθε $a = [(m,n)] \in \mathbb{Z}$ έχουμε

$$\begin{aligned} \iota_{\mathbb{N}}(m) +_{\mathbb{Z}} (-\iota_{\mathbb{N}}(n)) &= [(m +_{\mathbb{N}} 1, 1)] +_{\mathbb{Z}} (-[(n +_{\mathbb{N}} 1, 1)]) \\ &= [(m +_{\mathbb{N}} 1, 1)] +_{\mathbb{Z}} [(1, n +_{\mathbb{N}} 1)] \\ &= [(m +_{\mathbb{N}} 2, n +_{\mathbb{N}} 2)] \\ &= [(m,n)] = a. \end{aligned}$$

[39] Η ισότητα (1.44) προσδίδει έναν εναλλακτικό, «επίσημο» χαρακτηρισμό για τις *άτυπες διαφορές* τις αναφερθείσες στο εδάφιο 1.7.7 εντός τού *ήδη κατασκευασθέντος* $\mathbb{Z}$.

(vii) Έστω $a = [(m,n)]$ τυχών ακέραιος αριθμός. Κατά τον νόμο τής τριχοτομίας 1.7.18 ισχύει *ακριβώς ένα* εκ των ακολούθων: (α) $a >_{\mathbb{Z}} 0_{\mathbb{Z}}$, (β) $a <_{\mathbb{Z}} 0_{\mathbb{Z}}$, (γ) $a = 0_{\mathbb{Z}}$. Στην περίπτωση (α) έχουμε $m > n$. Επομένως υπάρχει κάποιος $k \in \mathbb{N}$, τέτοιος ώστε να ισχύει $m = n +_{\mathbb{N}} k$. Τούτο σημαίνει ότι

$$a = [(m,n)] = [(n +_{\mathbb{N}} k, n)] = [(k +_{\mathbb{N}} 1 +_{\mathbb{N}} n, 1 +_{\mathbb{N}} n)] = [(k +_{\mathbb{N}} 1, 1)] = \iota_{\mathbb{N}}(k)$$

(λόγω τού 1.7.10 (iii)). Ισχύει, βεβαίως, και το αντίστροφο· εάν $a \in \mathbb{Z}$ και εάν υπάρχει κάποιος $k \in \mathbb{N}$, τέτοιος ώστε $a = \iota_{\mathbb{N}}(k) = [(k +_{\mathbb{N}} 1, 1)]$, τότε $k +_{\mathbb{N}} 1 > 1$, οπότε $a >_{\mathbb{Z}} 0_{\mathbb{Z}}$ και εμπίπτουμε στην περίπτωση (α). Άρα η αμφίπλευρη συνεπαγωγή (1.45) είναι αληθής. Στην περίπτωση (β) έχουμε $n > m$. Επομένως υπάρχει κάποιος $l \in \mathbb{N}$, τέτοιος ώστε να ισχύει $n = m +_{\mathbb{N}} l$. Τούτο σημαίνει ότι

$$\begin{aligned} a &= [(m,n)] = [(m, m +_{\mathbb{N}} l)] = -[(m +_{\mathbb{N}} l, m)] \\ &= -[(l +_{\mathbb{N}} 1 +_{\mathbb{N}} m, 1 +_{\mathbb{N}} m)] = -[(l +_{\mathbb{N}} 1, 1)] = -\iota_{\mathbb{N}}(l). \end{aligned}$$

Κατ' αναλογίαν, ισχύει και το αντίστροφο, οπότε τελικώς

$$a <_{\mathbb{Z}} 0_{\mathbb{Z}} \Leftrightarrow \exists l \in \mathbb{N} : a = -\iota_{\mathbb{N}}(l). \tag{1.47}$$

Η ισότητα (1.46) έπεται από τις (1.45) και (1.47), έχοντας λάβει υπ' όψιν το τι συμβαίνει και στην περίπτωση (γ). □

1.7.24 Σημείωση (Οι συνήθεις «ταυτίσεις»). Εάν περιορίσουμε το πεδίο τιμών τής $\iota_{\mathbb{N}}$ στην εικόνα της, τότε η προκύπτουσα απεικόνιση είναι μια *αμφίρριψη* έχουσα την

$$\mathrm{Im}(\iota_{\mathbb{N}}) \ni [(n +_{\mathbb{N}} 1, 1)] \longmapsto n \in \mathbb{N}$$

ως αντίστροφό της. Προκειμένου να επανέλθουμε στον πλέον «οικείο» τρόπο αντιλήψεως τού συνόλου

$$\mathbb{Z} = \{0_{\mathbb{Z}}\} \coprod \{\pm\iota_{\mathbb{N}}(n) \,|\, n \in \mathbb{N}\} = \mathbb{N}_0 \coprod \mathbb{Z}_{<0},$$

όπου

$$\boxed{\mathbb{N}_0 := \{0_{\mathbb{Z}}\} \coprod \{\iota_{\mathbb{N}}(n) \,|\, n \in \mathbb{N}\}} \quad \text{και} \quad \boxed{\mathbb{Z}_{<0} := \{-\iota_{\mathbb{N}}(n) \,|\, n \in \mathbb{N}\},}$$

ταυτίζουμε την εικόνα $\iota_{\mathbb{N}}(n) = [(n +_{\mathbb{N}} 1, 1)]$ οιουδήποτε φυσικού αριθμού n μέσω τής $\iota_{\mathbb{N}}$ *με τον ίδιο τον* n και τον $-\iota_{\mathbb{N}}(n)$ με τον «σχολικό» "$-n$". Επιπροσθέτως, λόγω των 1.7.23 (ii) και (iii), για οιουσδήποτε $m, n \in \mathbb{N}$ *ταυτίζουμε* το $\iota_{\mathbb{N}}(m) +_{\mathbb{Z}} \iota_{\mathbb{N}}(n)$ με το $m +_{\mathbb{N}} n$ και το $\iota_{\mathbb{N}}(m) \cdot_{\mathbb{Z}} \iota_{\mathbb{N}}(n)$ με το $m \cdot_{\mathbb{N}} n$ (ήτοι τους περιορισμούς των πράξεων "$+_{\mathbb{Z}}$" και "$\cdot_{\mathbb{Z}}$" επί τής $\mathrm{Im}(\iota_{\mathbb{N}})$ με τις πράξεις "$+_{\mathbb{N}}$" και "$\cdot_{\mathbb{N}}$", αντιστοίχως). Κατ' αναλογίαν, λόγω των 1.7.23 (iv) και (v) *ταυτίζουμε* την "$\leqslant_{\mathbb{Z}}|_{\mathrm{Im}(\iota_{\mathbb{N}})}$" με τη σχέση διατάξεως "$\leqslant$" και το $1_{\mathbb{Z}}$ με το 1. Επίσης, αξίζει να επισημανθεί ότι **το σύνολο $\mathbb{N}_0$ των μη αρνητικών ακεραίων** είναι κλειστό ως προς τις πράξεις "$+_{\mathbb{Z}}$" και "$\cdot_{\mathbb{Z}}$" (βλ. 1.5.2 και 1.7.20 (v)), έχον το $0_{\mathbb{Z}}$ ως το ουδέτερό του στοιχείο ως προς την "$+_{\mathbb{Z}}$" και το $1_{\mathbb{Z}}$ ως το ουδέτερό του στοιχείο ως προς την "$\cdot_{\mathbb{Z}}$".

1.7.25 Πρόταση. *Εάν $a \in \mathbb{Z}$, τότε $\nexists b \in \mathbb{Z} : a <_{\mathbb{Z}} b <_{\mathbb{Z}} a + 1_{\mathbb{Z}}$.*

Απόδειξη. Εάν το a ανήκει στο $\mathbb{N}$, τότε λαμβάνοντας υπ' όψιν τις «ταυτίσεις» τού εδαφίου 1.7.24 και υποθέτοντας την ύπαρξη ενός τέτοιου $b \in \mathbb{Z}$, θα έπρεπε να ισχύει $b \in \mathbb{N}$, κάτι που θα αντέφασκε προς το (viii) τής προτάσεως 1.6.27. Από την άλλη μεριά, εάν το a είναι ένας μη θετικός ακέραιος αριθμός και εάν υποθέταμε την ύπαρξη ενός $b \in \mathbb{Z}$, τέτοιου ώστε $a <_{\mathbb{Z}} b <_{\mathbb{Z}} a +_{\mathbb{Z}} 1_{\mathbb{Z}}$, τότε (λόγω τού 1.7.20 (iv)) θα είχαμε

$$a +_{\mathbb{Z}} (-a +_{\mathbb{Z}} 1_{\mathbb{Z}}) <_{\mathbb{Z}} b +_{\mathbb{Z}} (-a +_{\mathbb{Z}} 1_{\mathbb{Z}}) <_{\mathbb{Z}} a +_{\mathbb{Z}} 1_{\mathbb{Z}} +_{\mathbb{Z}} (-a +_{\mathbb{Z}} 1_{\mathbb{Z}}),$$

οπότε ο $b +_{\mathbb{Z}} (-a +_{\mathbb{Z}} 1_{\mathbb{Z}})$ θα ήταν μεγαλύτερος τού $1_{\mathbb{Z}}\,(= 1)$ και μικρότερος τού 2, κάτι που θα αντέφασκε εκ νέου προς το (viii) τής προτάσεως 1.6.27. □

1.7.26 Παρατήρηση. Εν αντιθέσει προς το $(\mathbb{N}, \leqslant)$ (βλ. 1.6.32), το ολικώς διατεταγμένο σύνολο $(\mathbb{Z}, \leqslant_{\mathbb{Z}})$ *δεν είναι καλώς διατεταγμένο*[40]. Επί παραδείγματι, το

$$A := \{a +_{\mathbb{Z}} a \,|\, a \in \mathbb{Z}\} \subsetneqq \mathbb{Z}$$

είναι ένα μη κενό υποσύνολο τού $\mathbb{Z}$ το οποίο δεν διαθέτει ελάχιστο στοιχείο ως προς την "$\leqslant_{\mathbb{Z}}$". (Εάν υποθέταμε ότι το A διαθέτει ελάχιστο στοιχείο, ας πούμε το $a_\bullet +_{\mathbb{Z}} a_\bullet$, για κάποιο $a_\bullet \in \mathbb{Z}$, θα καταλήγαμε σε άτοπο, καθόσον το $(a_\bullet +_{\mathbb{Z}} (-1_{\mathbb{Z}})) +_{\mathbb{Z}} (a_\bullet +_{\mathbb{Z}} (-1_{\mathbb{Z}}))$ θα ανήκε στο A παρότι είναι μικρότερο τού $a_\bullet +_{\mathbb{Z}} a_\bullet$.) Ωστόσο, εκ των κάτω φραγμένα υποσύνολα τού $\mathbb{Z}$, ήτοι σύνολα τής μορφής $A_b = \{a \in \mathbb{Z} \,|\, a \geqslant_{\mathbb{Z}} b\}$, όπου $b \in \mathbb{Z}$, *είναι καλώς διατεταγμένα* ως προς την "$\leqslant_{\mathbb{Z}}$", όπως δείχνει η επόμενη πρόταση.

1.7.27 Πρόταση. *Έστω $b \in \mathbb{Z}$. Τότε οιοδήποτε μη κενό υποσύνολο τού συνόλου $A_b := \{a \in \mathbb{Z} \,|\, a \geqslant_{\mathbb{Z}} b\}$ διαθέτει ελάχιστο στοιχείο.*

Απόδειξη. Έστω $\varnothing \neq S \subseteq A_b$. Τότε το

$$S' := \{a +_{\mathbb{Z}} (-b) +_{\mathbb{Z}} 1_{\mathbb{Z}} \in \mathbb{Z} \,|\, a \in S\}$$

είναι υποσύνολο τού $\mathbb{N}$ (τού $\mathbb{N}$ ταυτιζομένου με την $\mathrm{Im}(\iota_{\mathbb{N}})$), διότι για κάθε στοιχείο $c = a +_{\mathbb{Z}} (-b) +_{\mathbb{Z}} 1_{\mathbb{Z}} \in S'$ (όπου $a \in S$) έχουμε (επί τη βάσει των 1.7.13 (iv), 1.7.20 (iv) και 1.7.13 (iii))

$$a \geqslant_{\mathbb{Z}} b \Rightarrow c = a +_{\mathbb{Z}} (-b) +_{\mathbb{Z}} 1_{\mathbb{Z}} \geqslant_{\mathbb{Z}} b +_{\mathbb{Z}} (-b) +_{\mathbb{Z}} 1_{\mathbb{Z}} = 0_{\mathbb{Z}} +_{\mathbb{Z}} 1_{\mathbb{Z}} = 1_{\mathbb{Z}}.$$

Κατά το θεώρημα 1.6.32 $\exists n_\bullet \in \mathbb{N} : n_\bullet = \min(S')$. Τούτο θα είναι κατ' ανάγκην τής μορφής $n_\bullet = a_\bullet +_{\mathbb{Z}} (-b) +_{\mathbb{Z}} 1_{\mathbb{Z}}$, για κάποιο $a_\bullet \in S$. Το $a_\bullet$ αποτελεί το ελάχιστο στοιχείο τού S ως προς την "$\leqslant_{\mathbb{Z}}$". Πράγματι· για οιοδήποτε $a \in S$ έχουμε

$$a +_{\mathbb{Z}} (-b) +_{\mathbb{Z}} 1_{\mathbb{Z}} \in S' \Longrightarrow a +_{\mathbb{Z}} (-b) +_{\mathbb{Z}} 1_{\mathbb{Z}} \geqslant_{\mathbb{Z}} n_\bullet,$$

οπότε $a_\bullet = n_\bullet +_{\mathbb{Z}} b +_{\mathbb{Z}} (-1_{\mathbb{Z}}) \leqslant_{\mathbb{Z}} (a +_{\mathbb{Z}} (-b) +_{\mathbb{Z}} 1_{\mathbb{Z}}) +_{\mathbb{Z}} b +_{\mathbb{Z}} (-1_{\mathbb{Z}}) = a$ και, ως εκ τούτου, $a_\bullet = \min(S)$. □

1.7.28 Σημείωση (Γενίκευση τής επαγωγικής μεθόδου). Θεωρούμε την απεικόνιση $\vartheta : A_b \longrightarrow A_b$ την οριζόμενη μέσω τού τύπου $\vartheta(a) := a +_{\mathbb{Z}} 1_{\mathbb{Z}}$. Προφανώς, η τριάδα (A_b, ϑ, b) πληροί τα αξιώματα (**A 1**), (**A 2**) και (**A 3**) τού Peano (βλ. 1.6.1, όπου το b επέχει τη θέση τού 1). Η πρόταση 1.7.27 δεν είναι τίποτε άλλο παρά μια παραλλαγή τού θεωρήματος 1.6.32 (ήτοι τής *αρχής τής καλής διατάξεως τού* $\mathbb{N}$) που «λειτουργεί» για το σύνολο A_b (μετατοπίζοντας το b στο $1_{\mathbb{Z}}$). Επειδή το 1.6.32 *ισοδυναμεί* (σύμφωνα με τη σημείωση 1.6.33) με το αξίωμα (**A 4**), η τριάδα (A_b, ϑ, b) πληροί *και* το (**A 4**), οπότε πρόκειται για ένα *σύστημα φυσικών αριθμών*. Λαμβάνοντας υπ' όψιν τα όσα προαναφέρθησαν στην παρατήρηση 1.6.31, διαπιστώνουμε ότι τα θεωρήματα 1.6.36 και 1.6.38 *εξακολουθούν να ισχύουν* όταν εφαρμόζονται για προτασιακούς τύπους $\Pi(a)$, όπου το a ανήκει στο A_b και το b παίζει τον ρόλο

[40] Προσοχή! Τούτο *δεν αντίκειται* προς το αξίωμα τής καλής διατάξεως 1.4.21. Υπάρχουν *άλλες* σχέσεις διατάξεως (*διαφορετικές* τής "$\leqslant_{\mathbb{Z}}$") που καθιστούν το $\mathbb{Z}$ καλώς διατεταγμένο. Επί παραδείγματι, εάν ορίσουμε την «ασυνήθη» σχέση διατάξεως "$\leq$" επί τού $\mathbb{Z}$ που υποχρεώνει τα στοιχεία του (όπως αυτά παριστώνται ύστερα από τη διαμεσολάβηση των συνήθων «ταυτίσεων» 1.7.24) να διατάσσονται ως εξής:

$$0_{\mathbb{Z}} < -1 < 1 < -2 < 2 < -3 < 3 < \cdots,$$

τότε το $(\mathbb{Z}, \leq)$ είναι όντως καλώς διατεταγμένο.

τού n_0 (που παρατίθεται στις διατυπώσεις τους). Εξάλλου, μια ελαφρά τροποποίηση τής ανωτέρω γενικεύσεως τής επαγωγικής μεθόδου οδηγεί σε αυτό που καλείται *επαγωγή με οπισθοπορεία*: Εάν κανείς αντικαταστήσει το εκ των κάτω φραγμένο υποσύνολο A_b τού $\mathbb{Z}$ με ένα εκ των άνω φραγμένο υποσύνολο $A'_c := \{a \in \mathbb{Z} \,|\, a \leqslant_{\mathbb{Z}} c\}$ τού $\mathbb{Z}$ (όπου $c \in \mathbb{Z}$), τότε $A'_c = -A_{-c} := \{-a \,|\, a \in A_{-c}\}$, οπότε έχουμε τη δυνατότητα να εφαρμόζουμε την επαγωγική μέθοδο κινούμενοι προς τα πίσω!

1.8 ΡΗΤΟΙ ΑΡΙΘΜΟΙ

Εάν $a \in \mathbb{Z}$ και $b \in \mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\}$, τότε η εξίσωση

$$\boxed{a = bx} \tag{1.48}$$

(με *άγνωστό της* τον x) δεν διαθέτει πάντοτε λύση εντός τού $\mathbb{Z}$. (Επί παραδείγματι, όταν $a = 1_{\mathbb{Z}}$, το πόρισμα 1.7.21 μας πληροφορεί ότι η (1.48) είναι επιλύσιμη εάν και μόνον εάν $b \in \{-1_{\mathbb{Z}}, 1_{\mathbb{Z}}\}$.) Η αναζήτηση ενός σύνολου «ευρύτερου» τού $\mathbb{Z}$, τέτοιου ώστε η (1.48) να διαθέτει πάντοτε λύση εντός αυτού, μας οδηγεί στον ορισμό τού $\mathbb{Q}$.

1.8.1 Ορισμός. Επί τού καρτεσιανού γινομένου $\mathbb{Z} \times (\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})$ ορίζουμε δύο εσωτερικές πράξεις "$+_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})}$" και "$\cdot_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})}$" μέσω των τύπων

$$\boxed{(a,b) +_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})} (a',b') \;:=\; ((a \cdot_{\mathbb{Z}} b') +_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} a'), b \cdot_{\mathbb{Z}} b')} \tag{1.49}$$

και

$$\boxed{(a,b) \cdot_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})} (a',b') \;:=\; (a \cdot_{\mathbb{Z}} a', b \cdot_{\mathbb{Z}} b')} \tag{1.50}$$

αντιστοίχως, για οιαδήποτε διατεταγμένα ζεύγη $(a,b), (a',b') \in \mathbb{Z} \times (\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})$.

1.8.2 Λήμμα. (i) *Η* "$+_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})}$" *είναι μεταθετική και προσεταιριστική, και το* $(0_{\mathbb{Z}}, 1_{\mathbb{Z}})$ *είναι το ουδέτερο στοιχείο τού* $\mathbb{Z} \times (\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})$ *ως προς αυτήν.*
(ii) *Η* "$\cdot_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})}$" *είναι μεταθετική και προσεταιριστική, και το* $(1_{\mathbb{Z}}, 1_{\mathbb{Z}})$ *είναι το ουδέτερο στοιχείο τού* $\mathbb{Z} \times (\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})$ *ως προς αυτήν.*

Απόδειξη. (i) Για οιαδήποτε $(a,b), (a',b'), (a'',b'') \in \mathbb{Z} \times (\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})$ έχουμε

$$\begin{aligned}
&(a,b) +_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})} (a',b') = ((a \cdot_{\mathbb{Z}} b') +_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} a'), b \cdot_{\mathbb{Z}} b') \quad \text{(εξ ορισμού)}\\
&= ((b \cdot_{\mathbb{Z}} a') +_{\mathbb{Z}} (a \cdot_{\mathbb{Z}} b'), b \cdot_{\mathbb{Z}} b') \quad \text{(λόγω τού 1.7.13 (i))}\\
&= ((a' \cdot_{\mathbb{Z}} b) +_{\mathbb{Z}} (b' \cdot_{\mathbb{Z}} a), b' \cdot_{\mathbb{Z}} b) \quad \text{(λόγω τού 1.7.15 (i))}\\
&= (a',b') +_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})} (a,b) \quad \text{(εξ ορισμού)}
\end{aligned}$$

και (λόγω των 1.7.15 (i), (ii) και (vi))

$$\begin{aligned}
&\big((a,b) +_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})} (a',b')\big) +_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})} (a'',b'')\\
=\;& \big((a \cdot_{\mathbb{Z}} b') +_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} a'), b \cdot_{\mathbb{Z}} b'\big) +_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})} (a'',b'')\\
=\;& \big(\big((a \cdot_{\mathbb{Z}} b') +_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} a')\big) \cdot_{\mathbb{Z}} b'' +_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} b') \cdot_{\mathbb{Z}} a'', (b \cdot_{\mathbb{Z}} b') \cdot_{\mathbb{Z}} b''\big)\\
=\;& \big(\big((a \cdot_{\mathbb{Z}} b') +_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} a')\big) \cdot_{\mathbb{Z}} b'' +_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} b') \cdot_{\mathbb{Z}} a'', (b \cdot_{\mathbb{Z}} b') \cdot_{\mathbb{Z}} b''\big)\\
=\;& \big(a \cdot_{\mathbb{Z}} (b' \cdot_{\mathbb{Z}} b'') +_{\mathbb{Z}} b \cdot_{\mathbb{Z}} ((a' \cdot_{\mathbb{Z}} b'') +_{\mathbb{Z}} (b' \cdot_{\mathbb{Z}} a'')), b \cdot_{\mathbb{Z}} (b' \cdot_{\mathbb{Z}} b'')\big)\\
=\;& (a,b) +_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})} \big((a' \cdot_{\mathbb{Z}} b'') +_{\mathbb{Z}} (b' \cdot_{\mathbb{Z}} a''), b' \cdot_{\mathbb{Z}} b''\big)\\
=\;& (a,b) +_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})} \big((a',b') +_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})} (a'',b'')\big).
\end{aligned}$$

Επίσης, λόγω των 1.7.15 (iii) και (iv),

$$\begin{aligned}(a,b)+_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})}(0_{\mathbb{Z}},1_{\mathbb{Z}}) &= ((a\cdot_{\mathbb{Z}}1_{\mathbb{Z}})+_{\mathbb{Z}}(b\cdot_{\mathbb{Z}}0_{\mathbb{Z}}),b\cdot_{\mathbb{Z}}1_{\mathbb{Z}})\\ &= ((a\cdot_{\mathbb{Z}}1_{\mathbb{Z}}),b\cdot_{\mathbb{Z}}1_{\mathbb{Z}})=(a,b),\end{aligned}$$

οπότε το $(0_{\mathbb{Z}},1_{\mathbb{Z}})$ είναι όντως το ουδέτερο στοιχείο τού $\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})$ ως προς την "$+_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})}$" (διότι αυτή είναι μεταθετική πράξη , βλ. 1.7.13 (i), 1.5.8 και 1.5.9).
(ii) Για οιαδήποτε $(a,b),(a',b'),(a'',b'')\in\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})$ έχουμε

$$\begin{aligned}&(a,b)\cdot_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})}(a',b')=(a\cdot_{\mathbb{Z}}a',b\cdot_{\mathbb{Z}}b') \quad \text{(εξ ορισμού)}\\ &=(a'\cdot_{\mathbb{Z}}a,b'\cdot_{\mathbb{Z}}b) \quad \text{(λόγω τού 1.7.15 (i))}\\ &=(a',b')\cdot_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})}(a,b) \quad \text{(εξ ορισμού)}\end{aligned}$$

και (λόγω τού 1.7.15 (ii))

$$\begin{aligned}&\big((a,b)\cdot_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})}(a',b')\big)\cdot_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})}(a'',b'')\\ =\;&\big(a\cdot_{\mathbb{Z}}a',b\cdot_{\mathbb{Z}}b'\big)\cdot_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})}(a'',b'')\\ =\;&\big((a\cdot_{\mathbb{Z}}a')\cdot_{\mathbb{Z}}a'',(b\cdot_{\mathbb{Z}}b')\cdot_{\mathbb{Z}}b''\big)\\ =\;&\big(a\cdot_{\mathbb{Z}}(a'\cdot_{\mathbb{Z}}a''),b\cdot_{\mathbb{Z}}(b'\cdot_{\mathbb{Z}}b'')\big)\\ =\;&(a,b)\cdot_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})}\big((a',b')\cdot_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})}(a'',b'')\big).\end{aligned}$$

Επίσης, λόγω τού 1.7.15 (iv),

$$(a,b)\cdot_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})}(1_{\mathbb{Z}},1_{\mathbb{Z}})=(a\cdot_{\mathbb{Z}}1_{\mathbb{Z}},b\cdot_{\mathbb{Z}}1_{\mathbb{Z}})=(a,b)$$

οπότε το $(1_{\mathbb{Z}},1_{\mathbb{Z}})$ είναι όντως το ουδέτερο στοιχείο τού $\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})$ ως προς την "$\cdot_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})}$" (διότι αυτή είναι μεταθετική, βλ. 1.7.15 (i), 1.5.8 και 1.5.9). □

1.8.3 Ορισμός. Επί τού καρτεσιανού γινομένου $\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})$ ορίζουμε τη διμελή σχέση "$\sim$" ως ακολούθως[41]:

$$\boxed{(a,b)\sim(a',b')\underset{\text{ορσ}}{\Longleftrightarrow}a\cdot_{\mathbb{Z}}b'=b\cdot_{\mathbb{Z}}a'.} \tag{1.51}$$

1.8.4 Λήμμα. *Η "$\sim$" είναι μια σχέση ισοδυναμίας επί τού $\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})$.*

Απόδειξη. Για οιαδήποτε $(a,b),(a',b'),(a'',b'')\in\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})$ έχουμε

$$1.7.15\text{ (i)}\Rightarrow a\cdot_{\mathbb{Z}}b=b\cdot_{\mathbb{Z}}a\Rightarrow(a,b)\sim(a,b),$$

τις συνεπαγωγές

$$(a,b)\sim\big(a',b'\big)\underset{1.7.15\text{ (i)}}{\Longrightarrow}a'\cdot_{\mathbb{Z}}b=b'\cdot_{\mathbb{Z}}a\Rightarrow\big(a',b'\big)\sim(a,b),$$

καθώς και τις

$$\left.\begin{aligned}(a,b)&\sim(a',b')\\ \text{και}\quad(a',b')&\sim(a'',b'')\end{aligned}\right\}\Rightarrow\left\{\begin{aligned}a\cdot_{\mathbb{Z}}b'&=b\cdot_{\mathbb{Z}}a'\\ a'\cdot_{\mathbb{Z}}b''&=b'\cdot_{\mathbb{Z}}a''\end{aligned}\right\}$$

[41] Το κίνητρο για τη θέσπιση τού ορισμού αυτού είναι ο «σχολικός» κανόνας χειρισμού τής ισότητας δύο «κλασμάτων» μέσω τού *χιαστί πολλαπλασιασμού*, ήτοι μέσω τού πολλαπλασιασμού τού αριθμητή τού πρώτου με τον παρονομαστή τού δεύτερου και την εξίσωση τού γινομένου τους με το γινόμενο τού παρονομαστή τού πρώτου με τον αριθμητή τού δεύτερου.

$$\Rightarrow \left\{ \begin{array}{l} b'' \cdot_{\mathbb{Z}} (a \cdot_{\mathbb{Z}} b') = b'' \cdot_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} a') \\ b \cdot_{\mathbb{Z}} (b' \cdot_{\mathbb{Z}} a'') = b \cdot_{\mathbb{Z}} (a' \cdot_{\mathbb{Z}} b'') \end{array} \right\} \Rightarrow b' \cdot_{\mathbb{Z}} \left(a \cdot_{\mathbb{Z}} b''\right) = b' \cdot_{\mathbb{Z}} \left(b \cdot_{\mathbb{Z}} a''\right)$$

(λόγω των 1.7.15 (i) και (ii)), οπότε μέσω τού νόμου τής διαγραφής 1.7.15 (viii) (που εφαρμόζεται επειδή $b' \neq 0_{\mathbb{Z}}$) λαμβάνουμε

$$a \cdot_{\mathbb{Z}} b'' = b \cdot_{\mathbb{Z}} a'' \Rightarrow (a, b) \sim (a'', b'').$$

Άρα η "$\sim$" είναι ανακλαστική, συμμετρική και μεταβατική. □

1.8.5 Λήμμα. *Η "$\sim$" είναι συμβατή τόσον με την πράξη "$+_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})}$" όσον και με την πράξη "$\cdot_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})}$".*

Απόδειξη. Εάν $(a, b), (a', b'), (c, d), (c', d') \in \mathbb{Z} \times (\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})$, τέτοιοι ώστε να ισχύει

$$(a, b) \sim \left(a', b'\right) \quad \text{και} \quad (c, d) \sim (c', d'), \tag{1.52}$$

ή -ισοδυνάμως- $a \cdot_{\mathbb{Z}} b' = b \cdot_{\mathbb{Z}} a'$ και $c \cdot_{\mathbb{Z}} d' = d \cdot_{\mathbb{Z}} c'$, τότε (λόγω των 1.7.15 (vi) και (i)) έχουμε

$$\begin{array}{rcl} (a \cdot_{\mathbb{Z}} d +_{\mathbb{Z}} b \cdot_{\mathbb{Z}} c) \cdot_{\mathbb{Z}} (b' \cdot_{\mathbb{Z}} d') & = & (a \cdot_{\mathbb{Z}} b') \cdot_{\mathbb{Z}} (d \cdot_{\mathbb{Z}} d') +_{\mathbb{Z}} (c \cdot_{\mathbb{Z}} d') \cdot_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} b') \\ & = & (b \cdot_{\mathbb{Z}} a') \cdot_{\mathbb{Z}} (d \cdot_{\mathbb{Z}} d') +_{\mathbb{Z}} (d \cdot_{\mathbb{Z}} c') \cdot_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} b') \\ & = & \left(a' \cdot_{\mathbb{Z}} d' +_{\mathbb{Z}} b' \cdot_{\mathbb{Z}} c'\right) \cdot_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} d), \end{array}$$

οπότε $(a, b) +_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})} (c, d) \sim (a', b') +_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})} (c', d')$. Εξάλλου, υπό την ίδια προϋπόθεση (1.52) συνάγεται ότι

$$\begin{array}{rcl} (a \cdot_{\mathbb{Z}} c) \cdot_{\mathbb{Z}} (b' \cdot_{\mathbb{Z}} d') & = & \left(a \cdot_{\mathbb{Z}} b'\right) \cdot_{\mathbb{Z}} (c \cdot_{\mathbb{Z}} d') \\ & = & \left(b \cdot_{\mathbb{Z}} a'\right) \cdot_{\mathbb{Z}} (d \cdot_{\mathbb{Z}} c') \\ & = & \left(a' \cdot_{\mathbb{Z}} c'\right) \cdot_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} d), \end{array}$$

οπότε $(a, b) \cdot_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})} (c, d) \sim (a', b') \cdot_{\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})} (c', d')$. □

1.8.6 Ορισμός. Το **σύνολο των ρητών αριθμών** ορίζεται να είναι το σύνολο των κλάσεων ισοδυναμίας

$$\boxed{\mathbb{Q} := (\mathbb{Z} \times (\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})) \,/\, \sim}$$

ως προς την ανωτέρω ορισθείσα "$\sim$" (βλ. (1.51)). Οι κλάσεις ισοδυναμίας

$$\boxed{\frac{a}{b} := [(a, b)] := \{(c, d) \in \mathbb{Z} \times (\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\}) \,|\, (a, b) \sim (c, d)\}}$$

των διατεταγμένων ζευγών $(a, b) \in \mathbb{Z} \times (\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})$ ως προς την "$\sim$" καλούνται **ρητοί αριθμοί**. Από εδώ και στο εξής θα υιοθετήσουμε τον συμβολισμό $\frac{a}{b}$ αντί τού $[(a, b)]$ για να εκφράζουμε την κλάση ισοδυναμίας τού (a, b) ως προς την "$\sim$", ούτως ώστε να την εκλαμβάνουμε εξαρχής ως (*τυπικώς οριζόμενο*) **κλάσμα** με **αριθμητή** του τον a και **παρονομαστή** του τον b.

1.8.7 Θεώρημα. *Επί τού $\mathbb{Q}$ ορίζονται δύο εσωτερικές πράξεις "$+_{\mathbb{Q}}$" και "$\cdot_{\mathbb{Q}}$":*

$$\left(\frac{a}{b}, \frac{a'}{b'}\right) \longmapsto \frac{a}{b} +_{\mathbb{Q}} \frac{a'}{b'}, \quad \left(\frac{a}{b}, \frac{a'}{b'}\right) \longmapsto \frac{a}{b} \cdot_{\mathbb{Q}} \frac{a'}{b'}$$

μέσω των τύπων

$$\boxed{\frac{a}{b} +_{\mathbb{Q}} \frac{a'}{b'} := \frac{(a \cdot_{\mathbb{Z}} b') +_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} a')}{b \cdot_{\mathbb{Z}} b'}} \tag{1.53}$$

και

$$\boxed{\frac{a}{b} \cdot_{\mathbb{Q}} \frac{a'}{b'} := \frac{a \cdot_{\mathbb{Z}} a'}{b \cdot_{\mathbb{Z}} b'}} \tag{1.54}$$

αντιστοίχως. Αυτές είναι οι μοναδικές απεικονίσεις από το $\mathbb{Q} \times \mathbb{Q}$ *στο* $\mathbb{Q}$ *οι οποίες καθιστούν τα διαγράμματα*

$$\begin{array}{ccc} (\mathbb{Z} \times (\mathbb{Z}\backslash\{0_{\mathbb{Z}}\}))^2 & \xrightarrow{+_{\mathbb{Z}\times(\mathbb{Z}\backslash\{0_{\mathbb{Z}}\})}} & \mathbb{Z} \times (\mathbb{Z}\backslash\{0_{\mathbb{Z}}\}) \\ \downarrow{\scriptstyle \pi_\sim \times \pi_\sim} & & \downarrow{\scriptstyle \pi_\sim} \\ \mathbb{Q} \times \mathbb{Q} & \xrightarrow[+_{\mathbb{Q}}]{} & \mathbb{Q} \end{array}$$

και

$$\begin{array}{ccc} (\mathbb{Z} \times (\mathbb{Z}\backslash\{0_{\mathbb{Z}}\}))^2 & \xrightarrow{\cdot_{\mathbb{Z}\times(\mathbb{Z}\backslash\{0_{\mathbb{Z}}\})}} & \mathbb{Z} \times (\mathbb{Z}\backslash\{0_{\mathbb{Z}}\}) \\ \downarrow{\scriptstyle \pi_\sim \times \pi_\sim} & & \downarrow{\scriptstyle \pi_\sim} \\ \mathbb{Q} \times \mathbb{Q} & \xrightarrow[\cdot_{\mathbb{Q}}]{} & \mathbb{Q} \end{array}$$

μεταθετικά.

Απόδειξη. Κατά το λήμμα 1.8.5 η σχέση ισοδυναμίας "$\sim$" είναι συμβατή με αμφότερες τις πράξεις "$+_{\mathbb{Z}\times(\mathbb{Z}\setminus\{0_{\mathbb{Z}}\})}$" και "$\cdot_{\mathbb{Z}\times(\mathbb{Z}\setminus\{0_{\mathbb{Z}}\})}$". Ως εκ τούτου, είναι δυνατή η εφαρμογή τού θεωρήματος 1.5.20 για καθεμιά εξ αυτών και ο προσδιορισμός των μοναδικών απεικονίσεων (1.53) και (1.54) που καθιστούν τα ανωτέρω διαγράμματα μεταθετικά. □

1.8.8 Ορισμός. Οι εσωτερικές πράξεις "$+_{\mathbb{Q}}$" και "$\cdot_{\mathbb{Q}}$" οι ορισθείσες στο θεώρημα 1.8.7 καλούνται **πρόσθεση** και **πολλαπλασιασμός (των ρητών αριθμών)**, αντιστοίχως. Εάν $r, s \in \mathbb{Q}$, τότε οι ρητοί αριθμοί $r +_{\mathbb{Q}} s$ και $r \cdot_{\mathbb{Q}} s$ καλούνται **άθροισμα** και **γινόμενο των** r **και** s, αντιστοίχως.

1.8.9 Ορισμός. (i) Το στοιχείο $0_{\mathbb{Q}} := \dfrac{0_{\mathbb{Z}}}{1_{\mathbb{Z}}}$ τού $\mathbb{Q}$ ονομάζεται **μηδέν** (ή, ακριβέστερα, **μηδενικό στοιχείο) τού** $\mathbb{Q}$.

(ii) Το $1_{\mathbb{Q}} := \dfrac{1_{\mathbb{Z}}}{1_{\mathbb{Z}}}$ ονομάζεται **μοναδιαίο στοιχείο τού** $\mathbb{Q}$.

(iii) Εάν $r = \dfrac{a}{b} \in \mathbb{Q}$, τότε λέμε ότι ο ρητός αριθμός

$$-r := \frac{-a}{b}$$

είναι **ο αντίθετος τού** r.

(iv) Εάν $r = \dfrac{a}{b} \in \mathbb{Q}\setminus\{0_{\mathbb{Q}}\}$, τότε λέμε ότι ο ρητός αριθμός

$$r^{-1} := \frac{b}{a}$$

είναι **ο αντίστροφος τού** r.

1.8.10 Παρατήρηση. Προφανώς, $0_{\mathbb{Z}} \cdot_{\mathbb{Z}} 1_{\mathbb{Z}} = 0_{\mathbb{Z}} \neq 1_{\mathbb{Z}} \Rightarrow 1_{\mathbb{Q}} \neq 0_{\mathbb{Q}}$. (Βλ. 1.6.24 (i)). Επίσης,

$$0_{\mathbb{Q}} = \frac{0_{\mathbb{Z}}}{b}, \quad 1_{\mathbb{Q}} = \frac{b}{b}, \ \forall b \in \mathbb{Z}\setminus\{0_{\mathbb{Z}}\}, \quad \frac{a}{b} = \frac{-a}{-b}, \ \forall (a,b) \in \mathbb{Z} \times (\mathbb{Z}\setminus\{0_{\mathbb{Z}}\}).$$

1.8.11 Πρόταση (Ιδιότητες προσθέσεως). *Η πρόσθεση ρητών αριθμών έχει τις εξής ιδιότητες*:

(i) **[Μεταθετική ιδιότητα]** $r +_{\mathbb{Q}} s = s +_{\mathbb{Q}} r, \forall (r,s) \in \mathbb{Q} \times \mathbb{Q}$.

(ii) **[Προσεταιριστική ιδιότητα]** *Για οιουσδήποτε* $r, s, t \in \mathbb{Q}$ *ισχύει η ισότητα*

$$(r +_{\mathbb{Q}} s) +_{\mathbb{Q}} t = r +_{\mathbb{Q}} (s +_{\mathbb{Q}} t)\,.$$

(iii) **[Νόμος τής διαγραφής]** *Για οιουσδήποτε* $r, s, t \in \mathbb{Q}$ *ισχύει η συνεπαγωγή*

$$r +_{\mathbb{Q}} t = s +_{\mathbb{Q}} t \Longrightarrow r = s.$$

(iv) **[Ύπαρξη ουδετέρου στοιχείου]** *Το* $0_{\mathbb{Q}}$ *είναι ουδέτερο στοιχείο τού* $\mathbb{Q}$ *ως προς την* "$+_{\mathbb{Q}}$" (βλ. 1.5.6), *δηλαδή*

$$0_{\mathbb{Q}} +_{\mathbb{Q}} r = r = r +_{\mathbb{Q}} 0_{\mathbb{Q}}, \quad \forall r \in \mathbb{Q}.$$

(v) **[Ύπαρξη συμμετρικού στοιχείου]** *Κάθε* $r \in \mathbb{Q}$ *έχει τον αντίθετό του ως συμμετρικό του στοιχείο ως προς την* "$+_{\mathbb{Q}}$" (βλ. 1.5.11), *δηλαδή*

$$(-r) +_{\mathbb{Q}} r = 0_{\mathbb{Q}} = r +_{\mathbb{Q}} (-r)\,.$$

Απόδειξη. Τα (i) (ii) και (iv) έπονται άμεσα από το (i) τού λήμματος 1.8.2, το θεώρημα 1.8.7 και τα (b), (c) και (d) τού θεωρήματος 1.5.20.

(iii) Εάν οι $r = \dfrac{a}{b}$, $s = \dfrac{a'}{b'}$ και $t = \dfrac{a''}{b''} \in \mathbb{Q}$ είναι τέτοιοι ώστε να ισχύει η ισότητα $r +_{\mathbb{Q}} t = s +_{\mathbb{Q}} t$, τότε δυνάμει των (i), (vi) και (viii) τής προτάσεως 1.7.15 συνάγεται ότι

$$\begin{aligned}
&\frac{(a \cdot_{\mathbb{Z}} b'') +_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} a'')}{b \cdot_{\mathbb{Z}} b''} = \frac{(a' \cdot_{\mathbb{Z}} b'') +_{\mathbb{Z}} (b' \cdot_{\mathbb{Z}} a'')}{b' \cdot_{\mathbb{Z}} b''} \\
&\Rightarrow ((a \cdot_{\mathbb{Z}} b'') +_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} a'')) \cdot_{\mathbb{Z}} (b' \cdot_{\mathbb{Z}} b'') = (b \cdot_{\mathbb{Z}} b'') \cdot_{\mathbb{Z}} ((a' \cdot_{\mathbb{Z}} b'') +_{\mathbb{Z}} (b' \cdot_{\mathbb{Z}} a'')) \\
&\Rightarrow ((a \cdot_{\mathbb{Z}} b'') +_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} a'')) \cdot_{\mathbb{Z}} b' = b \cdot_{\mathbb{Z}} ((a' \cdot_{\mathbb{Z}} b'') +_{\mathbb{Z}} (b' \cdot_{\mathbb{Z}} a'')) \\
&\Rightarrow ((a \cdot_{\mathbb{Z}} b'') \cdot_{\mathbb{Z}} b') +_{\mathbb{Z}} ((b \cdot_{\mathbb{Z}} a'') \cdot_{\mathbb{Z}} b') = b \cdot_{\mathbb{Z}} (a' \cdot_{\mathbb{Z}} b'') +_{\mathbb{Z}} b \cdot_{\mathbb{Z}} (b' \cdot_{\mathbb{Z}} a'') \\
&\Rightarrow (a \cdot_{\mathbb{Z}} b') \cdot_{\mathbb{Z}} b'' = (b \cdot_{\mathbb{Z}} a') \cdot_{\mathbb{Z}} b'' \Rightarrow a \cdot_{\mathbb{Z}} b' = b \cdot_{\mathbb{Z}} a'
\end{aligned}$$

οπότε $r = \dfrac{a}{b} = \dfrac{a'}{b'} = s$.

(v) Εάν $r = \dfrac{a}{b} \in \mathbb{Q}$, τότε, σύμφωνα με το 1.7.13 (iv) και τα 1.7.15 (i) και (v),

$$\begin{aligned}
(-r) +_{\mathbb{Q}} r &= \frac{-a}{b} +_{\mathbb{Q}} \frac{a}{b} = \frac{((-a) \cdot_{\mathbb{Z}} b) +_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} a)}{b^2} \\
&= \frac{-(a \cdot_{\mathbb{Z}} b) +_{\mathbb{Z}} (a \cdot_{\mathbb{Z}} b)}{b^2} = \frac{0_{\mathbb{Z}}}{b^2} = \frac{0_{\mathbb{Z}}}{1_{\mathbb{Z}}} = 0_{\mathbb{Q}},
\end{aligned}$$

Άρα ο $-r$ είναι εξ αριστερών συμμετρικό στοιχείο τού r ως προς την "$+_{\mathbb{Q}}$" και, κατ' επέκταση, συμμετρικό τού r ως προς την "$+_{\mathbb{Q}}$", διότι αυτή (κατά το (i)) είναι μεταθετική (βλ. 1.5.14). □

1.8.12 Σημείωση. Εάν $r, s \in \mathbb{Q}$, τότε ο ρητός αριθμός $r +_{\mathbb{Q}} (-s)$ καλείται **διαφορά** τού r από τον s (σημειούμενος συνήθως ως $r - s$). Η εσωτερική πράξη

$$\mathbb{Q} \times \mathbb{Q} \ni (r, s) \longmapsto r +_{\mathbb{Q}} (-s) \in \mathbb{Q}$$

επί τού $\mathbb{Q}$ (**πράξη αφαιρέσεως**), όπως και στην περίπτωση που εργαζόμασταν μόνον με ακεραίους (βλ. 1.7.14), *δεν είναι ούτε* μεταθετική *ούτε* προσεταιριστική. Επίσης, το $0_{\mathbb{Q}}$ αποτελεί εκ δεξιών αλλά όχι και εξ αριστερών ουδέτερο στοιχείο τού $\mathbb{Q}$ ως προς αυτήν.

1.8.13 Πρόταση (Ιδιότητες πολλαπλασιασμού). *Ο πολλαπλασιασμός ρητών αριθμών έχει τις εξής ιδιότητες*:

(i) **[Μεταθετική ιδιότητα]** $r \cdot_{\mathbb{Q}} s = s \cdot_{\mathbb{Q}} r, \forall (r, s) \in \mathbb{Q} \times \mathbb{Q}$.

(ii) **[Προσεταιριστική ιδιότητα]** *Για οιουσδήποτε* $r, s, t \in \mathbb{Q}$ *ισχύει η ισότητα*

$$(r \cdot_{\mathbb{Q}} s) \cdot_{\mathbb{Q}} t = r \cdot_{\mathbb{Q}} (s \cdot_{\mathbb{Q}} t)\,.$$

(iii) *Για οιονδήποτε* $r \in \mathbb{Q}$ *ισχύουν οι ισότητες*

$$0_{\mathbb{Q}} \cdot_{\mathbb{Q}} r = 0_{\mathbb{Q}} = r \cdot_{\mathbb{Q}} 0_{\mathbb{Q}}.$$

(iv) **[Ύπαρξη ουδετέρου στοιχείου]** *Το* $1_{\mathbb{Q}}$ *είναι ουδέτερο στοιχείο τού* $\mathbb{Q}$ *ως προς την* "$\cdot_{\mathbb{Q}}$" (βλ. 1.5.6), *δηλαδή*

$$1_{\mathbb{Q}} \cdot_{\mathbb{Q}} r = r = r \cdot_{\mathbb{Q}} 1_{\mathbb{Q}},\ \forall r \in \mathbb{Q}.$$

(v) **[Ύπαρξη συμμετρικού στοιχείου για** $r \neq 0_{\mathbb{Q}}$**]** *Κάθε* $r \in \mathbb{Q} \setminus \{0_{\mathbb{Q}}\}$ *έχει τον αντίστροφό του ως συμμετρικό του στοιχείο ως προς την* "$\cdot_{\mathbb{Q}}$" (βλ. 1.5.11), *δηλαδή*

$$r^{-1} \cdot_{\mathbb{Q}} r = 1_{\mathbb{Q}} = r \cdot_{\mathbb{Q}} r^{-1}.$$

(vi) *Για οιουσδήποτε* $r, s \in \mathbb{Q}$ *ισχύουν οι ισότητες*

$$(-r) \cdot_{\mathbb{Q}} s = -(r \cdot_{\mathbb{Q}} s) = r \cdot_{\mathbb{Q}} (-s),\ \ (-r) \cdot_{\mathbb{Q}} (-s) = r \cdot_{\mathbb{Q}} s.$$

(vii) **[Επιμεριστική ιδιότητα τού πολλαπλασιασμού ως προς την πρόσθεση]** *Για οιουσδήποτε* $r, s, t \in \mathbb{Q}$ *ισχύουν οι ισότητες*

$$r \cdot_{\mathbb{Q}} (s +_{\mathbb{Q}} t) = (r \cdot_{\mathbb{Q}} s) +_{\mathbb{Q}} (r \cdot_{\mathbb{Q}} t)\,,\ \ (r +_{\mathbb{Q}} s) \cdot_{\mathbb{Q}} t = (r \cdot_{\mathbb{Q}} t) +_{\mathbb{Q}} (s \cdot_{\mathbb{Q}} t)\,.$$

(viii) *Εάν* $r, s \in \mathbb{Q}$ *με* $r \cdot_{\mathbb{Q}} s = 0_{\mathbb{Q}}$, *τότε είτε* $r = 0_{\mathbb{Q}}$ *είτε* $s = 0_{\mathbb{Q}}$.

(ix) **[Νόμος τής διαγραφής]** *Για* $r, s, t \in \mathbb{Q}$ *με* $t \neq 0_{\mathbb{Q}}$ *ισχύει η συνεπαγωγή*

$$r \cdot_{\mathbb{Q}} t = s \cdot_{\mathbb{Q}} t \Longrightarrow r = s.$$

Απόδειξη. Τα (i) (ii) και (iv) έπονται άμεσα από το (ii) τού λήμματος 1.8.2, το θεώρημα 1.8.7 και τα (b), (c) και (d) τού θεωρήματος 1.5.20.

(iii) Εάν $r = \dfrac{a}{b} \in \mathbb{Q}$, τότε κάνοντας χρήση των 1.7.15 (iii) και (iv) λαμβάνουμε

$$0_{\mathbb{Q}} \cdot_{\mathbb{Q}} r = \frac{0_{\mathbb{Z}}}{1_{\mathbb{Z}}} \cdot_{\mathbb{Q}} \frac{a}{b} = \frac{0_{\mathbb{Z}} \cdot_{\mathbb{Z}} a}{1_{\mathbb{Z}} \cdot_{\mathbb{Z}} b} = \frac{0_{\mathbb{Z}}}{b} = 0_{\mathbb{Q}}.$$

Λόγω τής μεταθετικότητας τής " $\cdot_{\mathbb{Q}}$ " έχουμε $0_{\mathbb{Q}} \cdot_{\mathbb{Q}} r = 0_{\mathbb{Q}} = r \cdot_{\mathbb{Q}} 0_{\mathbb{Q}},\ \forall r \in \mathbb{Q}$.

(v) Για κάθε $r = \dfrac{a}{b} \in \mathbb{Q} \setminus \{0_{\mathbb{Q}}\}$ συνάγεται ότι

$$r^{-1} \cdot_{\mathbb{Q}} r = \frac{b}{a} \cdot_{\mathbb{Q}} \frac{a}{b} = \frac{b \cdot_{\mathbb{Z}} a}{a \cdot_{\mathbb{Z}} b} = \frac{a \cdot_{\mathbb{Z}} b}{a \cdot_{\mathbb{Z}} b} = 1_{\mathbb{Q}}.$$

Η ισότητα $1_{\mathbb{Q}} = r \cdot_{\mathbb{Q}} r^{-1}$ είναι προφανής λόγω τής μεταθετικότητας τής " $\cdot_{\mathbb{Q}}$ ".

(vi) Εάν $r = \dfrac{a}{b}$, $s = \dfrac{a'}{b'} \in \mathbb{Q}$, τότε

$$(-r) \cdot_{\mathbb{Q}} s = \frac{-a}{b} \cdot_{\mathbb{Q}} \frac{a'}{b'} \quad := \frac{(-a) \cdot_{\mathbb{Z}} a'}{b \cdot_{\mathbb{Z}} b'} = \frac{-(a \cdot_{\mathbb{Z}} a')}{b \cdot_{\mathbb{Z}} b'} = -\left(r \cdot_{\mathbb{Q}} s\right).$$

Οι λοιπές ισότητες αποδεικνύονται παρομοίως.

(vii) Εάν $r = \dfrac{a}{b}$, $s = \dfrac{a'}{b'}$ και $t = \dfrac{a''}{b''} \in \mathbb{Q}$, τότε, λόγω τού 1.7.15 (vi),

$$\begin{aligned}
r \cdot_{\mathbb{Q}} (s +_{\mathbb{Q}} t) &= \frac{a}{b} \cdot_{\mathbb{Q}} \frac{(a' \cdot_{\mathbb{Z}} b'') +_{\mathbb{Z}} (b' \cdot_{\mathbb{Z}} a'')}{b' \cdot_{\mathbb{Z}} b''} \\
&= \frac{a \cdot_{\mathbb{Z}} ((a' \cdot_{\mathbb{Z}} b'') +_{\mathbb{Z}} (b' \cdot_{\mathbb{Z}} a''))}{b \cdot_{\mathbb{Z}} b' \cdot_{\mathbb{Z}} b''} \\
&= \frac{(a \cdot_{\mathbb{Z}} a' \cdot_{\mathbb{Z}} b'') +_{\mathbb{Z}} (a \cdot_{\mathbb{Z}} a'' \cdot_{\mathbb{Z}} b')}{b \cdot_{\mathbb{Z}} b' \cdot_{\mathbb{Z}} b''} \\
&= \frac{(a \cdot_{\mathbb{Z}} a' \cdot_{\mathbb{Z}} b \cdot_{\mathbb{Z}} b'') +_{\mathbb{Z}} (a \cdot_{\mathbb{Z}} a'' \cdot_{\mathbb{Z}} b \cdot_{\mathbb{Z}} b')}{(b \cdot_{\mathbb{Z}} b') \cdot_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} b'')} \\
&= \frac{a \cdot_{\mathbb{Z}} a'}{b \cdot_{\mathbb{Z}} b'} +_{\mathbb{Q}} \frac{a \cdot_{\mathbb{Z}} a''}{b \cdot_{\mathbb{Z}} b''} = (r \cdot_{\mathbb{Q}} s) +_{\mathbb{Q}} (r \cdot_{\mathbb{Q}} t).
\end{aligned}$$

Η δεύτερη ισότητα είναι προφανής (βλ. 1.5.22).

(viii) Εάν $r = \dfrac{a}{b}$, $s = \dfrac{a'}{b'} \in \mathbb{Q}$, τότε ισχύει η συνεπαγωγή

$$\frac{a \cdot_{\mathbb{Z}} a'}{b \cdot_{\mathbb{Z}} b'} = \frac{0_{\mathbb{Z}}}{1_{\mathbb{Z}}} \Rightarrow a \cdot_{\mathbb{Z}} a' = \left(a \cdot_{\mathbb{Z}} a'\right) \cdot_{\mathbb{Z}} 1_{\mathbb{Z}} = (b \cdot_{\mathbb{Z}} b') \cdot_{\mathbb{Z}} 0_{\mathbb{Z}} = 0_{\mathbb{Z}},$$

οπότε, βάσει τού 1.7.15 (vii), είτε $a = 0_{\mathbb{Z}}$ είτε $a' = 0_{\mathbb{Z}}$. Κατ' επέκταση, είτε $r = 0_{\mathbb{Q}}$ είτε $s = 0_{\mathbb{Q}}$.

(ix) Εάν οι $r = \dfrac{a}{b}, s = \dfrac{a'}{b'}$ και $t = \dfrac{a''}{b''} \in \mathbb{Q}$ είναι τέτοιοι ώστε $r \cdot_{\mathbb{Q}} t = s \cdot_{\mathbb{Q}} t$, τότε δυνάμει των (ii) και (viii) τής προτάσεως 1.7.15, και τής προτάσεως 1.6.40, συνάγεται ότι

$$\begin{aligned}
&\frac{a \cdot_{\mathbb{Z}} a''}{b \cdot_{\mathbb{Z}} b''} = \frac{a' \cdot_{\mathbb{Z}} a''}{b' \cdot_{\mathbb{Z}} b''} \\
&\Rightarrow (a \cdot_{\mathbb{Z}} a'') \cdot_{\mathbb{Z}} (b' \cdot_{\mathbb{Z}} b'') = (b \cdot_{\mathbb{Z}} b'') \cdot_{\mathbb{Z}} (a' \cdot_{\mathbb{Z}} a'') \\
&\Rightarrow (a \cdot_{\mathbb{Z}} b') \cdot_{\mathbb{Z}} (a'' \cdot_{\mathbb{Z}} b'') = (b \cdot_{\mathbb{Z}} a') \cdot_{\mathbb{Z}} (a'' \cdot_{\mathbb{Z}} b'') \\
&\Rightarrow a \cdot_{\mathbb{Z}} b' = b \cdot_{\mathbb{Z}} a'
\end{aligned}$$

οπότε ισχύει και ο νόμος τής διαγραφής στο $\mathbb{Q}$. □

1.8.14 Σημείωση (Κλάσματα με ρητούς αριθμητές και παρονομαστές). Σε ορισμένες περιπτώσεις είθισται, για λόγους συντομίας, να γράφουμε κάποιους ρητούς αριθμούς υπό τη μορφή «κλασμάτων» $\frac{r}{s}$ με *ρητούς* αριθμητές r και (μη μηδενικούς) *ρητούς* παρονομαστές s. Συγκεκριμένα, εάν $r = \dfrac{a}{b} \in \mathbb{Q}$ και εάν $s = \dfrac{c}{d} \in \mathbb{Q} \setminus \{0_{\mathbb{Q}}\}$, τότε χρησιμοποιώντας τό σύμβολο $\dfrac{r}{s}$ εννοούμε τον ρητό αριθμό

$$\boxed{\frac{r}{s} := r \cdot_{\mathbb{Q}} s^{-1} = \frac{a}{b} \cdot_{\mathbb{Q}} \frac{d}{c} = \frac{a \cdot_{\mathbb{Z}} d}{b \cdot_{\mathbb{Z}} c}.}$$

1.8.15 Σημείωση (Ρητοί υψούμενοι σε ακέραιες δυνάμεις). Εάν $a \in \mathbb{Z}$ και εάν υποτεθεί ότι $r \in \mathbb{Q}\smallsetminus\{0_{\mathbb{Q}}\}$, τότε λέμε ότι ο ρητός αριθμός[42]

$$r^a := \begin{cases} 1_{\mathbb{Q}}, & \text{όταν } a = 0_{\mathbb{Z}}, \\ r^{a+_{\mathbb{Z}}(-1_{\mathbb{Z}})} \cdot_{\mathbb{Q}} r, & \text{όταν } a >_{\mathbb{Z}} 0_{\mathbb{Z}}, \\ (r^{-a})^{-1}, & \text{όταν } a <_{\mathbb{Z}} 0_{\mathbb{Z}}, \end{cases}$$

είναι ο r **υψωμένος στη δύναμη** a και ότι ο r^a έχει τον a ως **εκθέτη του**. (Ο ορισμός αυτός είναι επεκτάσιμος και για $r = 0_{\mathbb{Q}}$ αλλά *μόνον για θετικές δυνάμεις*, θέτοντας $0^a_{\mathbb{Q}} := 0_{\mathbb{Q}}$ για κάθε ακέραιο $a >_{\mathbb{Z}} 0_{\mathbb{Z}}$.) Οι ακόλουθες ιδιότητες αποδεικνύονται εύκολα κάνοντας κατάλληλη χρήση τής μεθόδου μαθηματικής επαγωγής (κατά περίπτωση):

(i) Για οιουσδήποτε $a, b \in \mathbb{Z}$ και $r \in \mathbb{Q}\smallsetminus\{0_{\mathbb{Q}}\}$ ισχύει η ισότητα

$$r^a \cdot_{\mathbb{Q}} r^b = r^{a+_{\mathbb{Z}}b} = r^b \cdot_{\mathbb{Q}} r^a.$$

(ii) Για οιουσδήποτε $a, b \in \mathbb{Z}$ και $r \in \mathbb{Q}\smallsetminus\{0_{\mathbb{Q}}\}$ έχουμε

$$(r^a)^b = r^{a\cdot_{\mathbb{Z}}b}.$$

(iii) Για οιουσδήποτε $a \in \mathbb{Z}$ και $r, s \in \mathbb{Q}\smallsetminus\{0_{\mathbb{Q}}\}$ ισχύει η ισότητα

$$(r \cdot_{\mathbb{Q}} s)^a = r^a \cdot_{\mathbb{Q}} s^a.$$

(iv) Για οιονδήποτε $a \in \mathbb{Z}$ και οιονδήποτε $r \in \mathbb{Q}\smallsetminus\{0_{\mathbb{Q}}\}$ έχουμε

$$r^{-a} = (r^{-1})^a = (r^a)^{-1}.$$

(Ως εκ τούτου, ο r^{-a}είναι ο αντίστροφος τού r^a.)

▸ **Ο ορισμός τής συνήθους διατάξεως επί τού** $\mathbb{Q}$. Τα στοιχεία τού $\mathbb{Q}$ διατάσσονται κατά τον πλέον «φυσικό» τρόπο ως ακολούθως:

1.8.16 Ορισμός. Επί τού $\mathbb{Q}$ ορίζουμε τη διμελή σχέση[43]

$$r \leqslant_{\mathbb{Q}} s \underset{\text{ορσ}}{\iff} ((a' \cdot_{\mathbb{Z}} b) +_{\mathbb{Z}} (-b' \cdot_{\mathbb{Z}} a)) \cdot_{\mathbb{Z}} b \cdot_{\mathbb{Z}} b' \geqslant_{\mathbb{Z}} 0_{\mathbb{Z}}. \tag{1.55}$$

όπου $r = \dfrac{a}{b}$, $s = \dfrac{a'}{b'} \in \mathbb{Q}$ και "$\leqslant_{\mathbb{Z}}$" η ήδη ορισθείσα σχέση ολικής διατάξεως επί τού συνόλου $\mathbb{Z}$ των ακεραίων αριθμών (βλ. 1.7.17 και 1.7.19).

(i) Όταν $r \leqslant_{\mathbb{Q}} s$, τότε λέμε ότι ο r είναι **μικρότερος ή ίσος** τού s ή ότι ο s είναι **μεγαλύτερος ή ίσος** τού r (και γράφουμε, εναλλακτικώς, $s \geqslant_{\mathbb{Q}} r$). Επίσης, λέμε ότι ο r είναι **μικρότερος** τού s ή ότι ο s είναι **μεγαλύτερος** τού r (και γράφουμε $r <_{\mathbb{Q}} s$ ή $s >_{\mathbb{Q}} r$) όταν $r \leqslant_{\mathbb{Q}} s$ *και* $r \neq s$.

(ii) Κάθε $r \in \mathbb{Q}$ για τον οποίο ισχύει $r >_{\mathbb{Q}} 0_{\mathbb{Q}}$ (και αντιστοίχως, $r <_{\mathbb{Q}} 0_{\mathbb{Q}}$) καλείται **θετικός** (και αντιστοίχως, **αρνητικός**) **ρητός αριθμός**. Το σύνολο των θετικών (και αντιστοίχως, των αρνητικών) ρητών αριθμών συμβολίζεται ως $\mathbb{Q}_{>0}$ (και αντιστοίχως, ως $\mathbb{Q}_{<0}$). Προφανώς, $r <_{\mathbb{Q}} s \iff s +_{\mathbb{Q}} (-r) >_{\mathbb{Q}} 0_{\mathbb{Q}}$.

[42] Εν προκειμένω, για $a >_{\mathbb{Z}} 0_{\mathbb{Z}}$ ο ορισμός είναι επαγωγικώς υλοποιήσιμος.

[43] Αυτή η διμελής σχέση *δεν εξαρτάται* από την επιλογή των εκπροσώπων (a, b) και (a', b') των (κλάσεων ισοδυναμίας) r και s, αντιστοίχως, διότι εάν $r = \frac{a}{b} = \frac{c}{d}$ και $s = \frac{a'}{b'} = \frac{c'}{d'}$, τότε

$$s +_{\mathbb{Q}} (-r) = \frac{(a' \cdot_{\mathbb{Z}} b) +_{\mathbb{Z}} (-b' \cdot_{\mathbb{Z}} a)}{b \cdot_{\mathbb{Z}} b'} = \frac{(c' \cdot_{\mathbb{Z}} d) +_{\mathbb{Z}} (-d' \cdot_{\mathbb{Z}} c)}{d \cdot_{\mathbb{Z}} d'},$$

οπότε $\big((a' \cdot_{\mathbb{Z}} b) +_{\mathbb{Z}} (-b' \cdot_{\mathbb{Z}} a)\big) \cdot_{\mathbb{Z}} \big(d \cdot_{\mathbb{Z}} d'\big) = \big((c' \cdot_{\mathbb{Z}} d) +_{\mathbb{Z}} (-d' \cdot_{\mathbb{Z}} c)\big) \cdot_{\mathbb{Z}} \big(b \cdot_{\mathbb{Z}} b'\big)$. Το να είναι αυτός ο ακέραιος *γνησίως θετικός* ισοδυναμεί με το ότι οι παράγοντες των ανωτέρω παραστάσεών του ως γινομένου οφείλουν να είναι είτε *αμφότεροι γνησίως θετικοί* είτε *αμφότεροι γνησίως αρνητικοί* ακέραιοι (βλ. 1.7.20 (v), (vi) και (vii)).

1.8.17 Θεώρημα (Νόμος τής «τριχοτομίας»). *Εάν* $(r,s)\in\mathbb{Q}\times\mathbb{Q}$, *τότε ισχύει ακριβώς ένα εκ των κάτωθι*:

(i) $r=s$.

(ii) $r<_{\mathbb{Q}}s$.

(iii) $r>_{\mathbb{Q}}s$.

Απόδειξη. Εάν $r=\frac{a}{b}$, $s=\frac{a'}{b'}$, για κάποια $(a,b),(a',b')\in\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0_{\mathbb{Z}}\})$, τότε, σύμφωνα με τον νόμο τής τριχοτομίας 1.7.18 τον ισχύοντα για τα ζεύγη στοιχείων τού $\mathbb{Z}$, ακριβώς ένα εκ των κάτωθι είναι αληθές:

$$\begin{cases}((a'\cdot_{\mathbb{Z}}b)+_{\mathbb{Z}}(-b'\cdot_{\mathbb{Z}}a))\cdot_{\mathbb{Z}}b\cdot_{\mathbb{Z}}b'=0_{\mathbb{Z}},\\ ((a'\cdot_{\mathbb{Z}}b)+_{\mathbb{Z}}(-b'\cdot_{\mathbb{Z}}a))\cdot_{\mathbb{Z}}b\cdot_{\mathbb{Z}}b'>0_{\mathbb{Z}},\\ ((a'\cdot_{\mathbb{Z}}b)+_{\mathbb{Z}}(-b'\cdot_{\mathbb{Z}}a))\cdot_{\mathbb{Z}}b\cdot_{\mathbb{Z}}b'<0_{\mathbb{Z}}.\end{cases}$$

Επειδή (εξ υποθέσεως) $b\cdot_{\mathbb{Z}}b'\neq 0_{\mathbb{Z}}$, η ισότητα τής πρώτης περιπτώσεως ισοδυναμεί με την

$$((a'\cdot_{\mathbb{Z}}b)+_{\mathbb{Z}}(-b'\cdot_{\mathbb{Z}}a))=0_{\mathbb{Z}}\Leftrightarrow a\cdot_{\mathbb{Z}}b'=b'\cdot_{\mathbb{Z}}a\Leftrightarrow r=s.$$

Στη δεύτερη περίπτωση λαμβάνουμε (εξ ορισμού) $r<_{\mathbb{Q}}s$. Τέλος, στην τρίτη περίπτωση, αρκεί να γίνει εναλλαγή των ρόλων των r και s και να εφαρμοσθεί εκ νέου ο ορισμός 1.8.16. □

1.8.18 Πόρισμα. *Το σύνολο* $\mathbb{Q}$ *των ρητών αριθμών γράφεται ως αποσυνδετή ένωση*

$$\boxed{\mathbb{Q}=\mathbb{Q}_{<0}\coprod\{0_{\mathbb{Q}}\}\coprod\mathbb{Q}_{>0}.}$$

Απόδειξη. Αρκεί να εφαρμοσθεί το θεώρημα 1.8.17 για το (r,s), όπου r τυχών ρητός αριθμός και $s=0_{\mathbb{Q}}$. □

1.8.19 Λήμμα. *Εάν* $(r,s)\in\mathbb{Q}\times\mathbb{Q}$, *τότε*

$$\boxed{r\leqslant_{\mathbb{Q}}s\Longleftrightarrow\exists\,(m,n)\in\mathbb{N}_0\times\mathbb{N}:s+_{\mathbb{Q}}(-r)=\tfrac{m}{n},}\tag{1.56}$$

(όπου $r=s$ *εάν και μόνον εάν* $m=0_{\mathbb{Z}}$*).*

Απόδειξη. Επειδή $r=s\Leftrightarrow s+_{\mathbb{Q}}(-r)=0_{\mathbb{Q}}$, αρκεί να αποδείξουμε την (1.56) όταν $r=\frac{a}{b}<_{\mathbb{Q}}s=\frac{a'}{b'}$. Υπό αυτήν την προϋπόθεση, $s+_{\mathbb{Q}}(-r)=\frac{(a'\cdot_{\mathbb{Z}}b)+_{\mathbb{Z}}(-b'\cdot_{\mathbb{Z}}a)}{b\cdot_{\mathbb{Z}}b'}$ και (σύμφωνα με την (1.55))

$$\text{είτε }[(a'\cdot_{\mathbb{Z}}b)+_{\mathbb{Z}}(-b'\cdot_{\mathbb{Z}}a)>_{\mathbb{Z}}0_{\mathbb{Z}}\ \text{ και }b\cdot_{\mathbb{Z}}b'>_{\mathbb{Z}}0_{\mathbb{Z}}]$$

$$\text{είτε }[(a'\cdot_{\mathbb{Z}}b)+_{\mathbb{Z}}(-b'\cdot_{\mathbb{Z}}a)<_{\mathbb{Z}}0_{\mathbb{Z}}\ \text{ και }b\cdot_{\mathbb{Z}}b'<_{\mathbb{Z}}0_{\mathbb{Z}}].$$

Στην πρώτη περίπτωση θέτουμε $m:=(a'\cdot_{\mathbb{Z}}b)+_{\mathbb{Z}}(-b'\cdot_{\mathbb{Z}}a)$ και $n:=b\cdot_{\mathbb{Z}}b'$, ενώ στη δεύτερη περίπτωση θέτουμε $m:=(-a'\cdot_{\mathbb{Z}}b)+_{\mathbb{Z}}(b'\cdot_{\mathbb{Z}}a)$ και $n:=-b\cdot_{\mathbb{Z}}b'$, και λαμβάνουμε υπ' όψιν την παρατήρηση 1.9.8. Και αντιστρόφως· εάν υπάρχουν $m,n\in\mathbb{N}$ με $s+_{\mathbb{Q}}(-r)=\frac{m}{n}$, τότε

$$\big((a'\cdot_{\mathbb{Z}}b)+_{\mathbb{Z}}(-b'\cdot_{\mathbb{Z}}a)\big)\cdot_{\mathbb{Z}}n=\big(b\cdot_{\mathbb{Z}}b'\big)\cdot_{\mathbb{Z}}m,$$

οπότε οι όροι $(a'\cdot_{\mathbb{Z}}b)+_{\mathbb{Z}}(-b'\cdot_{\mathbb{Z}}a)$ και $b\cdot_{\mathbb{Z}}b'$ είναι είτε *αμφότεροι θετικοί* είτε *αμφότεροι αρνητικοί*. Εξ αυτού έπεται ότι το γινόμενό τους είναι θετικός ακέραιος (βλ. 1.7.20 (v), (vi)) και ότι $r<_{\mathbb{Q}}s$. □

1.8.20 Θεώρημα. *Η διμελής σχέση "$\leqslant_{\mathbb{Q}}$" η ορισθείσα επί τού $\mathbb{Q}$ στο εδάφιο 1.8.16 είναι σχέση ολικής διατάξεως.* (Βλ. 1.4.1.)

Απόδειξη. Η ανακλαστικότητα τής "$\leqslant_{\mathbb{Q}}$" είναι προφανής. Εάν $(r,s)\in\mathbb{Q}\times\mathbb{Q}$, όπου $r\leqslant_{\mathbb{Q}} s$ και (ταυτοχρόνως) $s\leqslant_{\mathbb{Q}} r$, και εάν υποθέσουμε ότι $r\neq s$, τότε $r<_{\mathbb{Q}} s$ και (ταυτοχρόνως) $s<_{\mathbb{Q}} r$, κάτι που είναι άτοπο επί τη βάσει τού νόμου τής τριχοτομίας 1.8.17. Κατ' ανάγκην λοιπόν $r=s$ και η "$\leqslant_{\mathbb{Q}}$" είναι αντισυμμετρική.

Εν συνεχεία θεωρούμε ρητούς αραιθμούς $r=\dfrac{a}{b}$, $s=\dfrac{a'}{b'}$ και $t=\dfrac{a''}{b''}\in\mathbb{Q}$, τέτοιους ώστε $r\leqslant_{\mathbb{Q}} s$ και $s\leqslant_{\mathbb{Q}} t$. Τότε, λόγω τής αμφίπλευρης συνεπαγωγής (1.56), συμπεραίνουμε ότι

$$\left.\begin{array}{r}\exists\,(m,n)\in\mathbb{N}_0\times\mathbb{N}: s+_{\mathbb{Q}}(-r)=\frac{m}{n}\\ \exists\,(m',n')\in\mathbb{N}_0\times\mathbb{N}: t+_{\mathbb{Q}}(-s)=\frac{m'}{n'}\end{array}\right\}\Rightarrow t+_{\mathbb{Q}}(-r)=\frac{m}{n}+_{\mathbb{Q}}\frac{m'}{n'}=\frac{(m\cdot_{\mathbb{Z}}n')+_{\mathbb{Z}}(n\cdot_{\mathbb{Z}}m')}{n\cdot_{\mathbb{Z}}n'},$$

οπότε $r\leqslant_{\mathbb{Q}} t$ (και πάλι λόγω τής (1.56)). Άρα η "$\leqslant_{\mathbb{Q}}$" είναι μεταβατική.

Απομένει να αποδειχθεί ότι τα στοιχεία τού $\mathbb{Q}$ είναι μεταξύ τους ανά δύο συγκρίσιμα ως προς την "$\leqslant_{\mathbb{Q}}$". Θεωρούμε λοιπόν τυχόντες $r,s\in\mathbb{Q}$. Εάν $r=s$, τότε εξ ορισμού $r\leqslant_{\mathbb{Q}} s$. Εάν $r\neq s$, τότε ο νόμος τής τριχοτομίας 1.8.17 επιτάσσει είτε την ισχύ τής ανισότητας $r<_{\mathbb{Q}} s$ (οπότε $r\leqslant_{\mathbb{Q}} s$) είτε την ισχύ τής ανισότητας $s<_{\mathbb{Q}} r$ (οπότε $s\leqslant_{\mathbb{Q}} r$). Κατά συνέπειαν, η "$\leqslant_{\mathbb{Q}}$" αποτελεί μια σχέση ολικής διατάξεως επί τού $\mathbb{Q}$. □

1.8.21 Πρόταση (Ιδιότητες διατάξεως). *Εάν $r,s,r',s',t\in\mathbb{Q}$, τότε ισχύουν τα ακόλουθα*:

(i) *Εάν $r<_{\mathbb{Q}} s$ και $s<_{\mathbb{Q}} t$, τότε $s<_{\mathbb{Q}} t$.*

(ii) $r<_{\mathbb{Q}} s\Leftrightarrow -s<_{\mathbb{Q}} -r$.

(iii) $0<_{\mathbb{Q}} r\Leftrightarrow -r<_{\mathbb{Q}} 0_{\mathbb{Q}}$.

(iv) $r<_{\mathbb{Q}} s\Leftrightarrow r+_{\mathbb{Q}} t<_{\mathbb{Q}} s+_{\mathbb{Q}} t$ *και*

$$[r<_{\mathbb{Q}} s\ \text{ και }\ r'<_{\mathbb{Q}} s']\Rightarrow r+_{\mathbb{Q}} r'<_{\mathbb{Q}} s+_{\mathbb{Q}} s'.$$

(v) *Εάν $r,s\in\mathbb{Q}_{>0}$, τότε $r+_{\mathbb{Q}} s>_{\mathbb{Q}} 0_{\mathbb{Q}}$ και $r\cdot_{\mathbb{Q}} s>_{\mathbb{Q}} 0_{\mathbb{Q}}$.*

(vi) *Εάν $r,s\in\mathbb{Q}_{<0}$, τότε $r+_{\mathbb{Q}} s<_{\mathbb{Q}} 0_{\mathbb{Q}}$ και $r\cdot_{\mathbb{Q}} s>_{\mathbb{Q}} 0_{\mathbb{Q}}$.*

(vii) *Εάν $r\in\mathbb{Q}_{<0}$ και $s\in\mathbb{Q}_{>0}$, τότε $r\cdot_{\mathbb{Q}} s<_{\mathbb{Q}} 0_{\mathbb{Q}}$.*

(viii) *Εάν $t\in\mathbb{Q}_{>0}$, τότε $r<_{\mathbb{Q}} s\Leftrightarrow (r\cdot_{\mathbb{Q}} t)<_{\mathbb{Q}}(s\cdot_{\mathbb{Q}} t)$ και*

$$[0_{\mathbb{Q}}<_{\mathbb{Q}} r<_{\mathbb{Q}} s\ \text{ και }\ 0_{\mathbb{Q}}<_{\mathbb{Q}} r'<_{\mathbb{Q}} s']\Rightarrow (r\cdot_{\mathbb{Q}} r')<_{\mathbb{Q}}(s\cdot_{\mathbb{Q}} s').$$

(ix) *Εάν $t\in\mathbb{Q}_{<0}$, τότε $r<_{\mathbb{Q}} s\Leftrightarrow (r\cdot_{\mathbb{Q}} t)>_{\mathbb{Q}}(s\cdot_{\mathbb{Q}} t)$.*

Απόδειξη. (i) Τούτο αποδεικνύεται όπως και η μεταβατικότητα τής "$\leqslant_{\mathbb{Q}}$".

(ii) Εάν $r=\dfrac{a}{b}$, $s=\dfrac{a'}{b'}\in\mathbb{Q}$, τότε το 1.7.20 (iii) και η (1.55) δίδουν

$$\begin{aligned} r<_{\mathbb{Q}} s&\Leftrightarrow((a'\cdot_{\mathbb{Z}} b)+_{\mathbb{Z}}(-b'\cdot_{\mathbb{Z}} a))\cdot_{\mathbb{Z}} b\cdot_{\mathbb{Z}} b'\geqslant_{\mathbb{Z}} 0_{\mathbb{Z}}\\ &\Leftrightarrow((-a\cdot_{\mathbb{Z}} b')+_{\mathbb{Z}}(-b'\cdot_{\mathbb{Z}} a'))\cdot_{\mathbb{Z}} b'\cdot_{\mathbb{Z}} b\leqslant_{\mathbb{Z}} 0_{\mathbb{Z}}\Leftrightarrow -s<_{\mathbb{Q}} -r.\end{aligned}$$

(iii) Τούτο έπεται άμεσα από το (ii).

(iv) Κατά την (1.56),

$$\begin{aligned} r<_{\mathbb{Q}} s&\Leftrightarrow\exists\,(m,n)\in\mathbb{N}\times\mathbb{N}: s+_{\mathbb{Q}}(-r)=\frac{m}{n}\\ &\Leftrightarrow\exists\,(m,n)\in\mathbb{N}\times\mathbb{N}:(s+_{\mathbb{Q}} t)+_{\mathbb{Q}}(-(r+_{\mathbb{Q}} t))=\frac{m}{n}\Leftrightarrow r+_{\mathbb{Q}} t<_{\mathbb{Q}} s+_{\mathbb{Q}} t.\end{aligned}$$

Επιπροσθέτως, εάν $r <_{\mathbb{Q}} s$ και $r' <_{\mathbb{Q}} s'$, τότε

$$\left.\begin{array}{r}\exists\,(m,n)\in\mathbb{N}\times\mathbb{N}: s+_{\mathbb{Q}}(-r)=\frac{m}{n}\\ \exists\,(m,n)\in\mathbb{N}\times\mathbb{N}: s'+_{\mathbb{Q}}(-r)=\frac{m'}{n'}\end{array}\right\}\Rightarrow\left(s+_{\mathbb{Q}}s'\right)-\left(r+_{\mathbb{Q}}r'\right)=\tfrac{(m\cdot_{\mathbb{Z}}n')+_{\mathbb{Z}}(n\cdot_{\mathbb{Z}}m')}{n\cdot_{\mathbb{Z}}n'},$$

οπότε $r+_{\mathbb{Q}}r' <_{\mathbb{Q}} s+_{\mathbb{Q}}s'$.
(v) Εάν $r,s\in\mathbb{Q}_{>0}$, τότε

$$\left.\begin{array}{r}\exists\,(m,n)\in\mathbb{N}\times\mathbb{N}: r=\frac{m}{n}\\ \exists\,(m',n')\in\mathbb{N}\times\mathbb{N}: s=\frac{m'}{n'}\end{array}\right\}\Rightarrow r+_{\mathbb{Q}}s=\tfrac{(m\cdot_{\mathbb{Z}}n')+_{\mathbb{Z}}(n\cdot_{\mathbb{Z}}m')}{n\cdot_{\mathbb{Z}}n'},\ r\cdot_{\mathbb{Q}}s=\tfrac{m\cdot_{\mathbb{Z}}m'}{n\cdot_{\mathbb{Z}}n'},$$

οπότε $r+_{\mathbb{Q}}s >_{\mathbb{Q}} 0_{\mathbb{Q}}$ και $r\cdot_{\mathbb{Q}}s >_{\mathbb{Q}} 0_{\mathbb{Q}}$ (βλ. (1.56)). Τα (vi) και (vii) αποδεικνύονται παρομοίως.
(viii) Προφανώς, $t\in\mathbb{Q}_{>0}\Leftrightarrow\exists\,(m,n)\in\mathbb{N}\times\mathbb{N}: t=\frac{m}{n}$, οπότε

$$\begin{aligned}&r <_{\mathbb{Q}} s\Leftrightarrow\exists\,(m',n')\in\mathbb{N}\times\mathbb{N}: s+_{\mathbb{Q}}(-r)=\tfrac{m'}{n'}\\ \Rightarrow\ &\exists\,(m',n')\in\mathbb{N}\times\mathbb{N}:(s\cdot_{\mathbb{Q}}t)+_{\mathbb{Q}}(-(r\cdot_{\mathbb{Q}}t))=(s+_{\mathbb{Q}}(-r))\cdot_{\mathbb{Q}}t=\tfrac{m\cdot_{\mathbb{Z}}m'}{n\cdot_{\mathbb{Z}}n'}\\ &\underset{(1.56)}{\Longrightarrow}(r\cdot_{\mathbb{Q}}t) <_{\mathbb{Q}}(s\cdot_{\mathbb{Q}}t).\end{aligned}$$

Και αντιστρόφως· εάν $(r\cdot_{\mathbb{Q}}t) <_{\mathbb{Q}}(s\cdot_{\mathbb{Q}}t)$, τότε

$$\begin{aligned}&\exists\,(k,l)\in\mathbb{N}\times\mathbb{N}:(s\cdot_{\mathbb{Q}}t)+_{\mathbb{Q}}(-(r\cdot_{\mathbb{Q}}t))=(s+_{\mathbb{Q}}(-r))\cdot_{\mathbb{Q}}t=\tfrac{k}{l}\\ \Rightarrow\ &\exists\,(k,l)\in\mathbb{N}\times\mathbb{N}:(s+_{\mathbb{Q}}(-r))=(s+_{\mathbb{Q}}(-r))\cdot_{\mathbb{Q}}t\cdot_{\mathbb{Q}}t^{-1}=\tfrac{k}{l}\cdot_{\mathbb{Q}}t^{-1}=\tfrac{k\cdot_{\mathbb{Z}}n}{l\cdot_{\mathbb{Z}}m},\end{aligned}$$

οπότε $r <_{\mathbb{Q}} s$. Επιπροσθέτως, εάν $0_{\mathbb{Q}} <_{\mathbb{Q}} r <_{\mathbb{Q}} s$ και $0_{\mathbb{Q}} <_{\mathbb{Q}} r' <_{\mathbb{Q}} s'$, τότε

$$(r\cdot_{\mathbb{Q}}r') <_{\mathbb{Q}}(s\cdot_{\mathbb{Q}}r')=(r'\cdot_{\mathbb{Q}}s) <_{\mathbb{Q}}(s'\cdot_{\mathbb{Q}}s)=(s\cdot_{\mathbb{Q}}s').$$

Το (ix) αποδεικνύεται παρομοίως. □

1.8.22 Παρατήρηση. Αξίζει να επισημανθεί ότι το σύνολο $\mathbb{Q}_{>0}$ των *θετικών ρητών αριθμών* είναι κλειστό ως προς τις "$+_{\mathbb{Q}}$" και "$\cdot_{\mathbb{Q}}$" (βλ. 1.5.2 και 1.8.21 (v)), έχον το $0_{\mathbb{Q}}$ ως το ουδέτερό του στοιχείο ως προς την "$+_{\mathbb{Q}}$" και το $1_{\mathbb{Q}}$ ως το ουδέτερό του στοιχείο ως προς την "$\cdot_{\mathbb{Q}}$", καθώς και το ότι το σύνολο $\mathbb{Q}\setminus\{0_{\mathbb{Q}}\}$ των *μη μηδενικών ρητών αριθμών* είναι κλειστό ως προς την "$\cdot_{\mathbb{Q}}$" έχον το $1_{\mathbb{Q}}$ ως ουδέτερό του στοιχείο.

1.8.23 Ορισμός. Θεωρούμε την απεικόνιση

$$\boxed{\iota_{\mathbb{Z}}:\mathbb{Z}\longrightarrow\mathbb{Q},\ \ a\longmapsto\iota_{\mathbb{Z}}(a):=\frac{a}{1_{\mathbb{Z}}}.}$$

Η $\iota_{\mathbb{Z}}$ καλείται **φυσική εμφύτευση τού** $\mathbb{Z}$ **εντός τού** $\mathbb{Q}$. Οι κύριες ιδιότητές της παρατίθενται στην επόμενη πρόταση.

1.8.24 Πρόταση. (i) *Η* $\iota_{\mathbb{Z}}$ *είναι ενριπτική.*
(ii) $\iota_{\mathbb{Z}}(a+_{\mathbb{Z}}b)=\iota_{\mathbb{Z}}(a)+_{\mathbb{Q}}\iota_{\mathbb{Z}}(b),\ \forall\,(a,b)\in\mathbb{Z}\times\mathbb{Z}$.
(iii) $\iota_{\mathbb{Z}}(a\cdot_{\mathbb{Z}}b)=\iota_{\mathbb{Z}}(a)\cdot_{\mathbb{Q}}\iota_{\mathbb{Z}}(b),\ \forall\,(a,b)\in\mathbb{Z}\times\mathbb{Z}$.
(iv) *Για οιουσδήποτε* $a,b\in\mathbb{Z}$ *ισχύει η αμφίπλευρη συνεπαγωγή*

$$a\leqslant_{\mathbb{Z}}b\Longleftrightarrow\iota_{\mathbb{Z}}(a)\leqslant_{\mathbb{Q}}\iota_{\mathbb{Z}}(b).$$

(v) $\iota_{\mathbb{Z}}(0_{\mathbb{Z}})=0_{\mathbb{Q}}$ *και* $\iota_{\mathbb{Z}}(1_{\mathbb{Z}})=1_{\mathbb{Q}}$.

Αποδειξη. (i) Εάν $a, b \in \mathbb{Z}$ με $\iota_{\mathbb{Z}}(a) = \iota_{\mathbb{Z}}(b)$, τότε

$$\frac{a}{1_{\mathbb{Z}}} = \frac{b}{1_{\mathbb{Z}}} \underset{1.8.13\,\text{(iv)}}{\Longrightarrow} a = a \cdot_{\mathbb{Z}} 1_{\mathbb{Z}} = 1_{\mathbb{Z}} \cdot_{\mathbb{Z}} b = b,$$

οπότε η $\iota_{\mathbb{Z}}$ είναι όντως ενριπτική.
(ii) Προφανώς, για οιοδήποτε $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ λαμβάνουμε

$$\begin{aligned} \iota_{\mathbb{Z}}(a) +_{\mathbb{Q}} \iota_{\mathbb{Z}}(b) &= \frac{a}{1_{\mathbb{Z}}} +_{\mathbb{Q}} \frac{b}{1_{\mathbb{Z}}} = \frac{(a \cdot_{\mathbb{Z}} 1_{\mathbb{Z}}) +_{\mathbb{Z}} (1_{\mathbb{Z}} \cdot_{\mathbb{Z}} b)}{1_{\mathbb{Z}} \cdot_{\mathbb{Z}} 1_{\mathbb{Z}}} \\ &= \frac{a +_{\mathbb{Z}} b}{1_{\mathbb{Z}}} = \iota_{\mathbb{Z}}(a +_{\mathbb{Z}} b). \end{aligned}$$

(iii) Κατ' αναλογίαν, για οιοδήποτε $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ λαμβάνουμε

$$\begin{aligned} \iota_{\mathbb{Z}}(a) \cdot_{\mathbb{Q}} \iota_{\mathbb{Z}}(b) &= \frac{a}{1_{\mathbb{Z}}} \cdot_{\mathbb{Q}} \frac{b}{1_{\mathbb{Z}}} = \frac{a \cdot_{\mathbb{Z}} b}{1_{\mathbb{Z}} \cdot_{\mathbb{Z}} 1_{\mathbb{Z}}} \\ &= \frac{a \cdot_{\mathbb{Z}} b}{1_{\mathbb{Z}}} = \iota_{\mathbb{Z}}(a \cdot_{\mathbb{Z}} b). \end{aligned}$$

(iv) Για οιουσδήποτε $a, b \in \mathbb{Z}$ ισχύουν οι αμφίπλευρες συνεπαγωγές

$$\iota_{\mathbb{Z}}(a) \leqslant_{\mathbb{Q}} \iota_{\mathbb{Z}}(b) \Leftrightarrow \tfrac{a}{1_{\mathbb{Z}}} \leqslant_{\mathbb{Q}} \tfrac{b}{1_{\mathbb{Z}}} \Leftrightarrow b +_{\mathbb{Z}} (-a) \geqslant_{\mathbb{Z}} 0_{\mathbb{Z}} \Leftrightarrow a \leqslant_{\mathbb{Z}} b.$$

(v) Προφανώς, $\iota_{\mathbb{Z}}(0_{\mathbb{Z}}) = \dfrac{0_{\mathbb{Z}}}{1_{\mathbb{Z}}} = 0_{\mathbb{Q}}$ και $\iota_{\mathbb{Z}}(1_{\mathbb{Z}}) = \dfrac{1_{\mathbb{Z}}}{1_{\mathbb{Z}}} = 1_{\mathbb{Q}}$. □

1.8.25 Σημείωση (Οι συνήθεις «ταυτίσεις»). Εάν περιορίσουμε το πεδίο τιμών τής $\iota_{\mathbb{Z}}$ στην εικόνα της, τότε η προκύπτουσα απεικόνιση είναι μια *αμφίρριψη* έχουσα την

$$\mathrm{Im}(\iota_{\mathbb{Z}}) \ni \frac{a}{1_{\mathbb{Z}}} \longmapsto a \in \mathbb{Z}$$

ως αντίστροφό της. Ως εκ τούτου, είθισται να *ταυτίζουμε* την εικόνα $\iota_{\mathbb{Z}}(a) = \dfrac{a}{1_{\mathbb{Z}}}$ οιουδήποτε ακεραίου αριθμού a μέσω τής $\iota_{\mathbb{Z}}$ *με τον ίδιο τον* a. Επιπροσθέτως, λόγω των 1.8.24 (ii) και (iii), για οιουσδήποτε $a, b \in \mathbb{Z}$ *ταυτίζουμε* το $\iota_{\mathbb{Z}}(a) +_{\mathbb{Q}} \iota_{\mathbb{Z}}(b)$ με το $a +_{\mathbb{Z}} b$ και το $\iota_{\mathbb{Z}}(a) \cdot_{\mathbb{Q}} \iota_{\mathbb{Z}}(b)$ με το $a \cdot_{\mathbb{Z}} b$ (ήτοι τους περιορισμούς των πράξεων "$+_{\mathbb{Q}}$" και "$\cdot_{\mathbb{Q}}$" επί τής $\mathrm{Im}(\iota_{\mathbb{Z}})$ με τις πράξεις "$+_{\mathbb{Z}}$" και "$\cdot_{\mathbb{Z}}$", αντιστοίχως). Κατ' αναλογίαν, λόγω των 1.8.24 (iv) και (v) *ταυτίζουμε* την "$\leqslant_{\mathbb{Q}}|_{\mathrm{Im}(\iota_{\mathbb{Z}})}$" με τη σχέση διατάξεως "$\leqslant_{\mathbb{Z}}$", το $0_{\mathbb{Q}}$ με το $0_{\mathbb{Z}}$ και το $1_{\mathbb{Q}}$ με το $1_{\mathbb{Z}}$ (που το έχουμε ταυτίσει μέσω τής $\iota_{\mathbb{N}}$ με το $1 \in \mathbb{N}$ στο εδάφιο 1.7.24).

1.8.26 Πρόταση (Αρχιμήδεια ιδιότητα). *Για οιουσδήποτε ρητούς αριθμούς r, s με $s \geqslant_{\mathbb{Q}} r >_{\mathbb{Q}} 0_{\mathbb{Q}}$ υπάρχει κάποιος $k \in \mathbb{N}$, ούτως ώστε να ισχύει η ανισότητα*

$$k \cdot_{\mathbb{Q}} r >_{\mathbb{Q}} s$$

(όπου ο k ταυτίζεται, όπως προείπαμε, με τον $\iota_{\mathbb{Z}}(k) := \frac{k}{1_{\mathbb{Z}}}$).

Αποδειξη. Επειδή εξ υποθέσεως $r, s \in \mathbb{Q}_{>0}$, υπάρχουν $m, n, m', n' \in \mathbb{N}$, τέτοιοι ώστε $r = \frac{m}{n}$ και $s = \frac{m'}{n'}$. Επειδή $m \cdot_{\mathbb{N}} n', n \cdot_{\mathbb{N}} m' \in \mathbb{N}$, η αρχιμήδεια ιδιότητα η ισχύουσα στο $\mathbb{N}$ (βλ. πρόταση 1.6.29) μας διασφαλίζει την ύπαρξη ενός $k \in \mathbb{N}$, ούτως ώστε να ισχύει η ανισότητα

$$k \cdot_{\mathbb{N}} (m \cdot_{\mathbb{N}} n') > n \cdot_{\mathbb{N}} m' \underset{1.7.24}{\Longrightarrow} k \cdot_{\mathbb{Z}} (m \cdot_{\mathbb{Z}} n') >_{\mathbb{Z}} (n \cdot_{\mathbb{Z}} m').$$

Κατά συνέπειαν,

$$k \cdot_{\mathbb{Q}} r = \frac{k \cdot_{\mathbb{Z}} m}{n} = \frac{k \cdot_{\mathbb{Z}} (m \cdot_{\mathbb{Z}} n')}{n \cdot_{\mathbb{Z}} n'} >_{\mathbb{Q}} \frac{n \cdot_{\mathbb{Z}} m'}{n \cdot_{\mathbb{Z}} n'} = \frac{m'}{n'} = s,$$

και η απόδειξη λήγει εδώ. □

1.8.27 Πρόταση. *Για κάθε $r \in \mathbb{Q}$ υπάρχει ένας και μόνον ακέραιος a, τέτοιος ώστε*

$$a \leqslant_{\mathbb{Q}} r <_{\mathbb{Q}} a +_{\mathbb{Z}} 1_{\mathbb{Z}}.$$

Απόδειξη. Έστω $A := \left\{ \xi \in \mathbb{Z} \,|\, \xi \leqslant_{\mathbb{Q}} r \right\}$. Εάν $r \geqslant_{\mathbb{Q}} 0_{\mathbb{Q}}$, τότε το $0_{\mathbb{Z}}$ (που το έχουμε ταυτίσει με το $0_{\mathbb{Q}}$) ανήκει στο A. Εάν $r <_{\mathbb{Q}} 0_{\mathbb{Q}}$, τότε, σύμφωνα με το (iii) τής προτάσεως 1.8.21, $-r >_{\mathbb{Q}} 0_{\mathbb{Q}}$ και, κατ' επέκταση, $-r \geqslant_{\mathbb{Q}} 1_{\mathbb{Q}}$, και η πρόταση 1.8.26 (εφαρμοζόμενη για τα $1_{\mathbb{Q}}$ και $-r$ στη θέση των εκεί παρατιθέμενων r και s, αντιστοίχως) μας πληροφορεί ότι υπάρχει κάποιος $k \in \mathbb{N}$, ούτως ώστε να ισχύει

$$k = k \cdot_{\mathbb{Q}} 1_{\mathbb{Q}} >_{\mathbb{Q}} -r \Rightarrow r >_{\mathbb{Q}} -k \Rightarrow -k \in A.$$

Άρα το A είναι σε κάθε περίπτωση ένα *μη κενό* υποσύνολο τού $\mathbb{Z}$, το οποίο είναι προφανώς και *εκ των άνω φραγμένο* από κάποιον ακέραιο αριθμό. Τούτο σημαίνει ότι υφίσταται μέγιστο στοιχείο $a := \max(A) \in \mathbb{Z}$ τού A (ως προς την "$\leqslant_{\mathbb{Z}}$"). Λαμβάνοντας υπ' όψιν τις «ταυτίσεις» τις θεσπισθείσες στο εδάφιο 1.8.25, έχουμε εκ κατασκευής $a \leqslant_{\mathbb{Q}} r <_{\mathbb{Q}} a +_{\mathbb{Z}} 1_{\mathbb{Z}}$. Μάλιστα, υποθέτοντας την ύπαρξη κάποιου $b \in \mathbb{Z}$ με την ίδια ιδιότητα, έχουμε $b \leqslant_{\mathbb{Z}} a \Rightarrow b \leqslant_{\mathbb{Q}} a$, οπότε

$$b \leqslant_{\mathbb{Q}} a \leqslant_{\mathbb{Q}} r <_{\mathbb{Q}} b +_{\mathbb{Z}} 1_{\mathbb{Z}},$$

απ' όπου συμπεραίνουμε ότι $b = a$ (καθόσον, σύμφωνα με την πρόταση 1.7.25, δεν υπάρχει ακέραιος μεγαλύτερος τού b που να είναι -ταυτοχρόνως- μικρότερος τού $b +_{\mathbb{Z}} 1_{\mathbb{Z}}$). □

1.8.28 Παρατήρηση. (i) Εν αντιθέσει προς το $(\mathbb{N}, \leqslant)$ (βλ. 1.6.32), το ολικώς διατεταγμένο σύνολο $(\mathbb{Q}, \leqslant_{\mathbb{Q}})$, όπως και το $(\mathbb{Z}, \leqslant_{\mathbb{Z}})$, *δεν είναι καλώς διατεταγμένο*. (Πρβλ. 1.7.26.)

(ii) Εν αντιθέσει προς ό,τι συμβαίνει με τα στοιχεία των $\mathbb{N}$ και $\mathbb{Z}$ (βλ. 1.6.27 (viii) και 1.7.25), τα στοιχεία τού $\mathbb{Q}$ είναι «πυκνώς διατεταγμένα», όπως δείχνει η επόμενη πρόταση.

1.8.29 Πρόταση («Πυκνή διάταξη» των στοιχείων τού $\mathbb{Q}$). *Εάν οι r, s είναι δυο ρητοί αριθμοί και $r <_{\mathbb{Q}} s$, τότε*

$$\exists t \in \mathbb{Q} : r <_{\mathbb{Q}} t <_{\mathbb{Q}} s.$$

Απόδειξη. Επειδή $r <_{\mathbb{Q}} s$, το (iv) τής προτάσεως 1.8.21 (σε συνδυασμό με τις «ταυτίσεις» τις θεσπισθείσες στο εδάφιο 1.8.25) δίδει

$$\left.\begin{array}{l} 2 \cdot_{\mathbb{Q}} r = r +_{\mathbb{Q}} r <_{\mathbb{Q}} r +_{\mathbb{Q}} s \\ r +_{\mathbb{Q}} s <_{\mathbb{Q}} s +_{\mathbb{Q}} s = 2 \cdot_{\mathbb{Q}} s \end{array}\right\} \Rightarrow 2 \cdot_{\mathbb{Q}} r <_{\mathbb{Q}} r +_{\mathbb{Q}} s <_{\mathbb{Q}} 2 \cdot_{\mathbb{Q}} s.$$

Θέτοντας $t := \frac{1}{2} \cdot_{\mathbb{Q}} (r +_{\mathbb{Q}} s)$ και πολλαπλασιάζοντας τα μέλη των δύο τελευταίων ανισοτήτων με το $\frac{1}{2} \in \mathbb{Q}_{>0}$ λαμβάνουμε $r <_{\mathbb{Q}} t <_{\mathbb{Q}} s$ μέσω τού (viii) τής προτάσεως 1.8.21. □

1.8.30 Ορισμός. Ως **απόλυτη τιμή** ενός $r \in \mathbb{Q}$ ορίζουμε τον μη αρνητικό ρητό αριθμό

$$\boxed{|r| := \text{sign}\,(r) \cdot_{\mathbb{Q}} r,}$$

όπου

$$\operatorname{sign}(r) := \begin{cases} 1_{\mathbb{Q}}, & \text{όταν } r \geqslant_{\mathbb{Q}} 0_{\mathbb{Q}}, \\ -1_{\mathbb{Q}}, & \text{όταν } r <_{\mathbb{Q}} 0_{\mathbb{Q}}, \end{cases}$$

ο **προσημασμένος άσος** τού r.

1.8.31 Πρόταση (Ιδιότητες απολύτων τιμών). (i) *Για κάθε $r \in \mathbb{Q}$ ισχύουν οι αμφίπλευρες συνεπαγωγές*

$$|r| >_{\mathbb{Q}} 0_{\mathbb{Q}} \Leftrightarrow r \neq 0_{\mathbb{Q}} \ \textit{και} \quad |r| =_{\mathbb{Q}} 0_{\mathbb{Q}} \Leftrightarrow r = 0_{\mathbb{Q}}.$$

(ii) *Για κάθε $r \in \mathbb{Q}$ ισχύουν οι αμφίπλευρες συνεπαγωγές*

$$|r| = r \Leftrightarrow r \geqslant_{\mathbb{Q}} 0_{\mathbb{Q}} \ \textit{και} \quad |r| = -r \Leftrightarrow r \leqslant_{\mathbb{Q}} 0_{\mathbb{Q}}.$$

(iii) *Για οιουσδήποτε $r, s \in \mathbb{Q}$ ισχύουν οι ισότητες*

$$|r| = |-r| \ \textit{και} \quad |r - s| = |s - r|\,.$$

(iv) *Για κάθε $r \in \mathbb{Q}$ έχουμε*

$$-|r| \leqslant_{\mathbb{Q}} r \leqslant_{\mathbb{Q}} |r| \ \textit{και} \ \varepsilon \in \mathbb{Q}_{>0} \Rightarrow [|r| \leqslant_{\mathbb{Q}} \varepsilon \Leftrightarrow -\varepsilon \leqslant_{\mathbb{Q}} r \leqslant_{\mathbb{Q}} \varepsilon].$$

(v) *Για οιουσδήποτε $r, s \in \mathbb{Q}$ έχουμε*

$$|r \cdot_{\mathbb{Q}} s| = |r| \cdot_{\mathbb{Q}} |s| \ \textit{και} \ s \neq 0_{\mathbb{Q}} \Rightarrow \left|\frac{r}{s}\right| = \frac{|r|}{|s|}.$$

(vi) *Εάν $\nu \in \mathbb{N}, \nu \geqslant 2$, και $r_1, r_2, \ldots, r_\nu \in \mathbb{Q}$, τότε*

$$|r_1 \cdot_{\mathbb{Q}} r_2 \cdot_{\mathbb{Q}} \cdots \cdot_{\mathbb{Q}} r_\nu| = |r_1| \cdot_{\mathbb{Q}} |r_2| \cdot_{\mathbb{Q}} \cdots \cdot_{\mathbb{Q}} |r_\nu|\,.$$

(vii) *Για κάθε $r \in \mathbb{Q} \setminus \{0_{\mathbb{Q}}\}$ ισχύει η ισότητα*

$$|r^a| = |r|^a\,,\ \forall a \in \mathbb{Z}.$$

(viii) *Για οιουσδήποτε $r, s \in \mathbb{Q}$ έχουμε*

$$\left\{ \begin{array}{c} ||r| - |s|| \leqslant_{\mathbb{Q}} |r +_{\mathbb{Q}} s| \leqslant_{\mathbb{Q}} |r| +_{\mathbb{Q}} |s|\,, \\ ||r| - |s|| \leqslant_{\mathbb{Q}} |r - s| \leqslant_{\mathbb{Q}} |r| +_{\mathbb{Q}} |s|\,. \end{array} \right\}$$

(ix) *Εάν $\nu \in \mathbb{N}, \nu \geqslant 2$, και $r_1, r_2, \ldots, r_\nu \in \mathbb{Q}$, τότε*

$$|r_1 +_{\mathbb{Q}} r_2 +_{\mathbb{Q}} \cdots +_{\mathbb{Q}} r_\nu| \leqslant_{\mathbb{Q}} |r_1| +_{\mathbb{Q}} |r_2| +_{\mathbb{Q}} \cdots +_{\mathbb{Q}} |r_\nu|\,.$$

Απόδειξη. Τα (i)-(v) είναι άμεσες συνέπειες τού ορισμού 1.8.30. Το (vi) αποδεικνύεται κάνοντας χρήση τής κλασικής μαθηματικής επαγωγής 1.6.34 ως προς τον ν (αφού, λόγω τού (v), η ισότητα αυτή ισχύει για $\nu = 2$).

(vii) Για $a \in \{0_{\mathbb{Z}}, 1_{\mathbb{Z}}\}$ η ισότητα είναι προφανής. Για $a \geqslant_{\mathbb{Z}} 2$ αρκεί να εφαρμοσθεί το (vi) για $\nu := a$ και $r_1 = \cdots = r_\nu = r$. Για οιονδήποτε αρνητικό ακέραιο a, ο αντίθετός του $-a$ είναι θετικός, το 1.8.15 (iv) συνδυαζόμενο με το ανωτέρω (v) μας δίδει

$$\begin{aligned} |r^a| &= \left|\left(r^{-1}\right)^{-a}\right| = \left|\left(r^{-1}\right)\right|^{-a} = \left|\tfrac{1_{\mathbb{Z}}}{r}\right|^{-a} \\ &= \left(\tfrac{|1_{\mathbb{Z}}|}{|r|}\right)^{-a} = \left(|r|^{-1}\right)^{-a} = |r|^a\,. \end{aligned}$$

(viii) Λαμβάνοντας υπ' όψιν το (iv) συμπεραίνουμε ότι

$$\left.\begin{array}{l} -|r| \leqslant_{\mathbb{Q}} r \leqslant_{\mathbb{Q}} |r| \\ -|s| \leqslant_{\mathbb{Q}} s \leqslant_{\mathbb{Q}} |s| \end{array}\right\} \Rightarrow -\left(|r| +_{\mathbb{Q}} |s|\right) \leqslant_{\mathbb{Q}} r +_{\mathbb{Q}} s \leqslant_{\mathbb{Q}} |r| +_{\mathbb{Q}} |s|\,,$$

απ' όπου έπεται ότι $|r +_{\mathbb{Q}} s| \leqslant_{\mathbb{Q}} |r| +_{\mathbb{Q}} |s|$ και (αντικαθιστώντας τό s με το $-s$)

$$|r - s| \leqslant_{\mathbb{Q}} |r| +_{\mathbb{Q}} |-s| \underset{\text{(iii)}}{=} |r| +_{\mathbb{Q}} |s|\,.$$

Εν συνεχεία, δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $|r| \geqslant_{\mathbb{Q}} |s|$ (καθόσον $||r| - |s|| = ||s| - |r||$). Θέτοντας $t := r +_{\mathbb{Q}} s$ και $t' := r - s$, λαμβάνουμε

$$\left.\begin{array}{r} r = t - s \\ r = t' +_{\mathbb{Q}} s \end{array}\right\} \Rightarrow \left\{\begin{array}{c} |r| = |t - s| \leqslant_{\mathbb{Q}} |t| +_{\mathbb{Q}} |s| \\ |r| = |t' +_{\mathbb{Q}} s| \leqslant_{\mathbb{Q}} |t'| +_{\mathbb{Q}} |s| \end{array}\right\} \Rightarrow \left\{\begin{array}{c} |r| - |s| \leqslant_{\mathbb{Q}} |t| \\ |r| - |s| \leqslant_{\mathbb{Q}} |t'| \end{array}\right\},$$

οπότε από την $|r| - |s| \geqslant_{\mathbb{Q}} 0_{\mathbb{Q}}$ και το (ii) έπεται ότι

$$||r| - |s|| \leqslant_{\mathbb{Q}} |t| = |r +_{\mathbb{Q}} s| \quad \text{και} \quad ||r| - |s|| \leqslant_{\mathbb{Q}} |t'| = |r - s|\,.$$

(ix) Τούτο αποδεικνύεται μέσω κλασικής μαθηματικής επαγωγής 1.6.34 ως προς τον ν (αφού, λόγω τού (viii), η ισότητα αυτή ισχύει για $\nu = 2$). □

1.8.32 Ορισμός. Μια ακολουθία ρητών αριθμών $(r_n)_{n\in\mathbb{N}}$ καλείται **ακολουθία Cauchy** (ή **θεμελιώδης ακολουθία**) όταν για κάθε $\varepsilon \in \mathbb{Q}_{>0}$ υπάρχει δείκτης $n_0 = n_0(\varepsilon) \in \mathbb{N}$ (ήτοι δείκτης *γενικώς εξαρτώμενος* από τον ε), ούτως ώστε να ισχύει

$$|r_m - r_n| <_{\mathbb{Q}} \varepsilon, \text{ για οιουσδήποτε φυσικούς αριθμούς } m, n \geqslant n_0.$$

Το σύνολο των ακολουθιών Cauchy ρητών αριθμών συμβολίζεται ως $\mathrm{CS}(\mathbb{Q})$.

1.8.33 Ορισμός. Μια ακολουθία ρητών αριθμών $(r_n)_{n\in\mathbb{N}}$ καλείται **μηδενική ακολουθία** όταν για κάθε $\varepsilon \in \mathbb{Q}_{>0}$ υπάρχει δείκτης $n_0 = n_0(\varepsilon) \in \mathbb{N}$, ούτως ώστε να ισχύει

$$|r_n| <_{\mathbb{Q}} \varepsilon, \text{ για οιονδήποτε φυσικό αριθμό } n \geqslant n_0.$$

Το σύνολο των μηδενικών ακολουθιών ρητών αριθμών συμβολίζεται ως[44] $\mathrm{NS}(\mathbb{Q})$.

1.8.34 Ορισμός. Μια ακολουθία ρητών αριθμών $(r_n)_{n\in\mathbb{N}}$ καλείται **φραγμένη ακολουθία** όταν υπάρχει κάποιος $s \in \mathbb{Q}_{>0}$, ούτως ώστε να ισχύει

$$|r_n| \leqslant_{\mathbb{Q}} s, \text{ για οιονδήποτε } n \in \mathbb{N}.$$

1.8.35 Πρόταση. *Κάθε μηδενική ακολουθία ρητών αριθμών είναι ακολουθία Cauchy, δηλαδή* $\mathrm{NS}(\mathbb{Q}) \subseteq \mathrm{CS}(\mathbb{Q})$.

Απόδειξη. Εάν $(r_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q})$, τότε $\forall \varepsilon \in \mathbb{Q}_{>0}$, άρα και για τον $\frac{\varepsilon}{2} \in \mathbb{Q}_{>0}$,

$$\exists n_0 = n_0(\tfrac{\varepsilon}{2}) \in \mathbb{N} : |r_n| <_{\mathbb{Q}} \frac{\varepsilon}{2},\ \forall n,\ n \geqslant n_0,$$

απ' όπου προκύπτει ότι για οιουσδήποτε φυσικούς αριθμούς $m, n \geqslant n_0$ ισχύει

$$|r_m - r_n| \leqslant_{\mathbb{Q}} |r_m| +_{\mathbb{Q}} |r_n| <_{\mathbb{Q}} \frac{\varepsilon}{2} +_{\mathbb{Q}} \frac{\varepsilon}{2} = \varepsilon$$

λόγω των 1.8.31 (viii) και 1.8.21 (iv). Άρα $(r_n)_{n\in\mathbb{N}} \in \mathrm{CS}(\mathbb{Q})$. □

[44] Η επιλογή των προθεμάτων "CS" και "NS" για τα σύμβολα $\mathrm{CS}(\mathbb{Q})$ και $\mathrm{NS}(\mathbb{Q})$ έχει γίνει κατά τέτοιον τρόπο, ώστε να θυμίζει τα αρχικά γράμματα των «**C**auchy **s**equences» και «**n**ull **s**equences», αντιστοίχως.

1.8.36 Πρόταση. *Κάθε ακολουθία Cauchy ρητών αριθμών είναι φραγμένη.*

ΑΠΟΔΕΙΞΗ. Εάν $(r_n)_{n\in\mathbb{N}} \in \mathrm{CS}(\mathbb{Q})$, τότε για κάθε $\varepsilon \in \mathbb{Q}_{>0}$

$$(\exists n_0 = n_0(\varepsilon) \in \mathbb{N} : |r_m - r_n| <_{\mathbb{Q}} \varepsilon, \text{ για οιουσδήποτε φυσικούς } m, n \geqslant n_0),$$

οπότε $|r_n| - |r_{n_0}| \leqslant_{\mathbb{Q}} |r_n - r_{n_0}| = |r_{n_0} - r_n| <_{\mathbb{Q}} \varepsilon$, $\forall n \geqslant n_0$ (βλ. 1.8.31 (viii)). Εξ αυτού έπεται ότι για τον $s := \max\{|r_1|, |r_2|, \ldots, |r_{n_0-1}|, |r_{n_0}| +_{\mathbb{Q}} \varepsilon\} \in \mathbb{Q}_{>0}$ ισχύει

$$|r_n| \leqslant_{\mathbb{Q}} s, \text{ για οιονδήποτε } n \in \mathbb{N}.$$

Κατά συνέπειαν, η $(r_n)_{n\in\mathbb{N}}$ είναι φραγμένη. □

1.8.37 Πρόταση. *Επί του συνόλου* $\mathrm{CS}(\mathbb{Q})$ *ορίζονται δυο εσωτερικές πράξεις* (**προσθέσεως** *και* **πολλαπλασιασμού**)

$$\begin{cases} \boxplus_{\mathbb{Q}} : \mathrm{CS}(\mathbb{Q}) \times \mathrm{CS}(\mathbb{Q}) \longrightarrow \mathrm{CS}(\mathbb{Q}), \\ \boxdot_{\mathbb{Q}} : \mathrm{CS}(\mathbb{Q}) \times \mathrm{CS}(\mathbb{Q}) \longrightarrow \mathrm{CS}(\mathbb{Q}), \end{cases}$$

μέσω των τύπων:

$$\boxed{\begin{array}{c} ((r_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}}) \longmapsto (r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}} := (r_n +_{\mathbb{Q}} s_n)_{n\in\mathbb{N}}, \\ ((r_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}}) \longmapsto (r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}} := (r_n \cdot_{\mathbb{Q}} s_n)_{n\in\mathbb{N}}. \end{array}}$$

ΑΠΟΔΕΙΞΗ. Εάν $(r_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}} \in \mathrm{CS}(\mathbb{Q})$, τότε οι

$$(r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}, \quad (r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}$$

είναι ακολουθίες ρητών αριθμών και για κάθε $\varepsilon \in \mathbb{Q}_{>0}$, άρα και για τον $\frac{\varepsilon}{2} \in \mathbb{Q}_{>0}$,

$$\left\{ \begin{array}{l} \exists n_1 = n_1(\frac{\varepsilon}{2}) \in \mathbb{N} : |r_m - r_n| <_{\mathbb{Q}} \frac{\varepsilon}{2}, \ \forall m,\ m \geqslant n_1 \text{ και } \forall n,\ n \geqslant n_1, \\ \exists n_2 = n_2(\frac{\varepsilon}{2}) \in \mathbb{N} : |s_m - s_n| <_{\mathbb{Q}} \frac{\varepsilon}{2}, \ \forall m,\ m \geqslant n_2 \text{ και } \forall n,\ n \geqslant n_2. \end{array} \right\}$$

Επιπροσθέτως, επειδή (λόγω τής προτάσεως 1.8.36)

$$\exists t, v \in \mathbb{Q}_{>0} : |r_n| \leqslant_{\mathbb{Q}} t \ \text{ και } \ |s_n| \leqslant_{\mathbb{Q}} v, \ \ \forall n \in \mathbb{N},$$

για κάθε $\varepsilon \in \mathbb{Q}_{>0}$, άρα και για τους $\frac{\varepsilon}{2v}, \frac{\varepsilon}{2t} \in \mathbb{Q}_{>0}$,

$$\left\{ \begin{array}{l} \exists n_1' = n_1(\frac{\varepsilon}{2v}) \in \mathbb{N} : |r_m - r_n| <_{\mathbb{Q}} \frac{\varepsilon}{2v}, \ \forall m,\ m \geqslant n_1' \text{ και } \forall n,\ n \geqslant n_1', \\ \exists n_2' = n_2(\frac{\varepsilon}{2t}) \in \mathbb{N} : |s_m - s_n| <_{\mathbb{Q}} \frac{\varepsilon}{2t}, \ \forall m,\ m \geqslant n_2' \text{ και } \forall n,\ n \geqslant n_2'. \end{array} \right\}$$

Επομένως, για οιονδήποτε φυσικό $n \geqslant n_0 := \max\{n_1, n_2\}$ (λόγω των 1.8.31 (viii) και 1.8.21 (iv)) έχουμε

$$|(r_m +_{\mathbb{Q}} s_m) - (r_n +_{\mathbb{Q}} s_n)| \leqslant_{\mathbb{Q}} |r_m - r_n| +_{\mathbb{Q}} |s_m - s_n| <_{\mathbb{Q}} \frac{\varepsilon}{2} +_{\mathbb{Q}} \frac{\varepsilon}{2} = \varepsilon,$$

και για οιουσδήποτε φυσικούς αριθμούς $m, n \geqslant n_0' := \max\{n_1', n_2'\}$,

$$\begin{aligned} |(r_m \cdot_{\mathbb{Q}} s_m) - (r_n \cdot_{\mathbb{Q}} s_n)| &= |((r_m - r_n) \cdot_{\mathbb{Q}} s_m) +_{\mathbb{Q}} r_n \cdot_{\mathbb{Q}} (s_m - s_n)| \\ &\leqslant_{\mathbb{Q}} (|r_m - r_n| \cdot_{\mathbb{Q}} |s_m|) +_{\mathbb{Q}} (|r_n| \cdot_{\mathbb{Q}} |s_m - s_n|) \\ &<_{\mathbb{Q}} \left(\tfrac{\varepsilon}{2v} \cdot_{\mathbb{Q}} v\right) +_{\mathbb{Q}} \left(\tfrac{\varepsilon}{2t} \cdot_{\mathbb{Q}} t\right) = \varepsilon. \end{aligned}$$

Συνεπώς, $(r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}, (r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}} \in \mathrm{CS}(\mathbb{Q})$. □

1.8.38 Ορισμός. (i) Εάν $(r_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}} \in \mathrm{CS}(\mathbb{Q})$, τότε οι $(r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}$ και $(r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}$ καλούνται **άθροισμα** και **γινόμενο των** $(r_n)_{n\in\mathbb{N}}$ **και** $(s_n)_{n\in\mathbb{N}}$, αντιστοίχως.

(ii) Μια ακολουθία ρητών αριθμών $(r_n)_{n\in\mathbb{N}}$ καλείται **σταθερή ακολουθία** όταν υπάρχει κάποιος $r \in \mathbb{Q}$, τέτοιος ώστε

$$r_n = r, \text{ για οιονδήποτε } n \in \mathbb{N}. \tag{1.57}$$

Από εδώ και στο εξής θα γράφουμε $(r)_{n\in\mathbb{N}}$ για τον συμβολισμό μιας σταθερής ακολουθίας (υπονοώντας ότι πληρούται η συνθήκη (1.57)). Ιδιαιτέρως, χρησιμοποιούμε τις βραχυγραφίες

$$0_{\mathrm{CS}(\mathbb{Q})} := (0_{\mathbb{Q}})_{n\in\mathbb{N}}, \quad 1_{\mathrm{CS}(\mathbb{Q})} := (1_{\mathbb{Q}})_{n\in\mathbb{N}}.$$

Προφανώς, κάθε σταθερή ακολουθία είναι ακολουθία Cauchy.

1.8.39 Πρόταση (Ιδιότητες προσθέσεως). *Η πρόσθεση ακολουθιών Cauchy ρητών αριθμών έχει τις εξής ιδιότητες*:

(i) **[Μεταθετική ιδιότητα]** *Για κάθε* $((r_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}}) \in \mathrm{CS}(\mathbb{Q}) \times \mathrm{CS}(\mathbb{Q})$ *έχουμε*

$$(r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}} = (s_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (r_n)_{n\in\mathbb{N}}.$$

(ii) **[Προσεταιριστική ιδιότητα]** *Για οιεσδήποτε* $(r_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}}, (t_n)_{n\in\mathbb{N}} \in \mathrm{CS}(\mathbb{Q})$ *ισχύει η ισότητα*

$$((r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}) \boxplus_{\mathbb{Q}} (t_n)_{n\in\mathbb{N}} = (r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} ((s_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (t_n)_{n\in\mathbb{N}}).$$

(iii) **[Νόμος τής διαγραφής]** *Για οιεσδήποτε* $(r_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}}, (t_n)_{n\in\mathbb{N}} \in \mathrm{CS}(\mathbb{Q})$ *ισχύει η συνεπαγωγή*

$$(r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (t_n)_{n\in\mathbb{N}} = (s_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (t_n)_{n\in\mathbb{N}} \Longrightarrow (r_n)_{n\in\mathbb{N}} = (s_n)_{n\in\mathbb{N}}.$$

(iv) **[Ύπαρξη ουδετέρου στοιχείου]** *Η* $0_{\mathrm{CS}(\mathbb{Q})}$ *είναι ουδέτερο στοιχείο τού* $\mathrm{CS}(\mathbb{Q})$ *ως προς την* "$\boxplus_{\mathbb{Q}}$" (βλ. 1.5.6), *δηλαδή*

$$0_{\mathrm{CS}(\mathbb{Q})} \boxplus_{\mathbb{Q}} (r_n)_{n\in\mathbb{N}} = (r_n)_{n\in\mathbb{N}} = (r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} 0_{\mathrm{CS}(\mathbb{Q})}.$$

(v) **[Ύπαρξη συμμετρικού στοιχείου]** *Κάθε* $(r_n)_{n\in\mathbb{N}} \in \mathrm{CS}(\mathbb{Q})$ *έχει την* $(-r_n)_{n\in\mathbb{N}}$ *ως συμμετρικό της στοιχείο ως προς την* "$\boxplus_{\mathbb{Q}}$" (βλ. 1.5.11), *δηλαδή*

$$(-r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (r_n)_{n\in\mathbb{N}} = 0_{\mathrm{CS}(\mathbb{Q})} = (r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (-r_n)_{n\in\mathbb{N}}.$$

Απόδειξη. Έπεται άμεσα από τον ορισμό τής "$\boxplus_{\mathbb{Q}}$" και την πρόταση 1.8.11. □

1.8.40 Πρόταση (Ιδιότητες πολλαπλασιασμού). *Ο πολλαπλασιασμός ακολουθιών Cauchy ρητών αριθμών έχει τις εξής ιδιότητες*:

(i) **[Μεταθετική ιδιότητα]** *Για κάθε* $((r_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}}) \in \mathrm{CS}(\mathbb{Q}) \times \mathrm{CS}(\mathbb{Q})$ *έχουμε*

$$(r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}} = (s_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (r_n)_{n\in\mathbb{N}}.$$

(ii) **[Προσεταιριστική ιδιότητα]** *Για οιεσδήποτε* $(r_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}}, (t_n)_{n\in\mathbb{N}} \in \mathrm{CS}(\mathbb{Q})$ *ισχύει η ισότητα*

$$((r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}) \boxdot_{\mathbb{Q}} (t_n)_{n\in\mathbb{N}} = (r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} ((s_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (t_n)_{n\in\mathbb{N}}).$$

(iii) *Για οιαδήποτε* $(r_n)_{n\in\mathbb{N}} \in \mathrm{CS}(\mathbb{Q})$ *ισχύουν οι ισότητες*

$$0_{\mathrm{CS}(\mathbb{Q})} \boxdot_{\mathbb{Q}} (r_n)_{n\in\mathbb{N}} = (r_n)_{n\in\mathbb{N}} = (r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} 0_{\mathrm{CS}(\mathbb{Q})}.$$

(iv) **[Ύπαρξη ουδετέρου στοιχείου]** *Η* $1_{\mathrm{CS}(\mathbb{Q})}$ *είναι ουδέτερο στοιχείο τού* $\mathrm{CS}(\mathbb{Q})$ *ως προς την* "$\boxdot_{\mathbb{Q}}$" (βλ. 1.5.6), *δηλαδή*

$$1_{\mathrm{CS}(\mathbb{Q})} \boxdot_{\mathbb{Q}} (r_n)_{n\in\mathbb{N}} = (r_n)_{n\in\mathbb{N}} = (r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} 1_{\mathrm{CS}(\mathbb{Q})}.$$

(v) *Για οιεσδήποτε* $(r_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}} \in \mathrm{CS}(\mathbb{Q})$ *ισχύουν οι ισότητες*

$$(-r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}} = -\left((r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}\right) = (r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (-s_n)_{n\in\mathbb{N}},$$
$$(-r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (-s_n)_{n\in\mathbb{N}} = (r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}.$$

(vi) **[Επιμεριστική ιδιότητα τού πολλαπλασιασμού ως προς την πρόσθεση]** *Για οιεσδήποτε* $(r_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}}, (t_n)_{n\in\mathbb{N}} \in \mathrm{CS}(\mathbb{Q})$ *ισχύουν οι ισότητες*

$$(r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} \left((s_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (t_n)_{n\in\mathbb{N}}\right) = \left((r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}\right) \boxplus_{\mathbb{Q}} \left((r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (t_n)_{n\in\mathbb{N}}\right),$$
$$\left((r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}\right) \boxdot_{\mathbb{Q}} (t_n)_{n\in\mathbb{N}} = \left((r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (t_n)_{n\in\mathbb{N}}\right) \boxplus_{\mathbb{Q}} \left((s_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (t_n)_{n\in\mathbb{N}}\right).$$

Απόδειξη. Έπεται άμεσα από τον ορισμό τής "$\boxdot_{\mathbb{Q}}$" και τα (i), (ii), (iii), (iv), (vi) και (vii) τής προτάσεως 1.8.13. □

1.8.41 Λήμμα. *Εάν η* $(r_n)_{n\in\mathbb{N}}$ *είναι μια φραγμένη ακολουθία ρητών αριθμών και* $(s_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q})$, *τότε* $(r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q})$.

Απόδειξη. Επειδή η $(r_n)_{n\in\mathbb{N}}$ είναι φραγμένη ακολουθία,

$$\exists t \in \mathbb{Q}_{>0} : |r_n| \leqslant_{\mathbb{Q}} t,\ \forall n \in \mathbb{N}. \tag{1.58}$$

Επειδή $(s_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q})$, για κάθε $\varepsilon \in \mathbb{Q}_{>0}$, άρα και για το $\frac{\varepsilon}{t} \in \mathbb{Q}_{>0}$,

$$\exists n_0 = n_0(\tfrac{\varepsilon}{t}) \in \mathbb{N} : |s_n| <_{\mathbb{Q}} \tfrac{\varepsilon}{t},\ \forall n,\ n \geqslant n_0. \tag{1.59}$$

Άρα για κάθε φυσικό αριθμό $n \geqslant n_0$ οι (1.58) και (1.59) μας δίδουν

$$|r_n \cdot_{\mathbb{Q}} s_n| = |r_n| \cdot_{\mathbb{Q}} |s_n| <_{\mathbb{Q}} t \cdot_{\mathbb{Q}} \left(\tfrac{\varepsilon}{t}\right) = \varepsilon$$

λόγω τού 1.8.21 (viii). Κατά συνέπειαν, $(r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q})$. □

1.8.42 Πρόταση. *Για τις μηδενικές ακολουθίες ρητών αριθμών ισχύουν οι ακόλουθες συνεπαγωγές*:
(i) $(r_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q}) \Longrightarrow (r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q})$.
(ii) $(r_n)_{n\in\mathbb{N}} \in \mathrm{CS}(\mathbb{Q})$ *και* $(s_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q}) \Longrightarrow (r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q})$.

Απόδειξη. (i) Εάν $(r_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q})$, τότε για κάθε $\varepsilon \in \mathbb{Q}_{>0}$, άρα και για τον $\frac{\varepsilon}{2} \in \mathbb{Q}_{>0}$,

$$\left\{ \begin{array}{l} \exists n_1 = n_1(\frac{\varepsilon}{2}) \in \mathbb{N} : |r_n| <_{\mathbb{Q}} \frac{\varepsilon}{2},\ \forall n,\ n \geqslant n_1, \\ \exists n_2 = n_2(\frac{\varepsilon}{2}) \in \mathbb{N} : |s_n| <_{\mathbb{Q}} \frac{\varepsilon}{2},\ \forall n,\ n \geqslant n_2, \end{array} \right\},$$

οπότε για κάθε φυσικό αριθμό $n \geqslant n_0 := \max\{n_1, n_2\}$ έχουμε (λόγω των 1.8.31 (viii) και 1.8.21 (iv))

$$|r_n +_{\mathbb{Q}} s_n| \leqslant_{\mathbb{Q}} |r_n| +_{\mathbb{Q}} |s_n| <_{\mathbb{Q}} \tfrac{\varepsilon}{2} +_{\mathbb{Q}} \tfrac{\varepsilon}{2} = \varepsilon,$$

κάτι που σημαίνει ότι $(r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q})$.
(ii) Τούτο έπεται άμεσα από την πρόταση 1.8.36 και το λήμμα 1.8.41. □

1.9 ΠΡΑΓΜΑΤΙΚΟΙ ΑΡΙΘΜΟΙ

Εάν θεωρήσουμε ένα ορθογώνιο τρίγωνο, καθεμιά των καθέτων πλευρών τού οποίου έχει μήκος 1, τότε, σύμφωνα με το *πυθαγόρειο θεώρημα*, το μήκος x τής υποτείνουσάς του οφείλει να πληροί την εξίσωση

$$\boxed{x^2 = 2.} \tag{1.60}$$

Η (1.60) (με *άγνωστό της* τον x) δεν διαθέτει καμία λύση εντός τού $\mathbb{Q}$. Πράγματι· εάν υπήρχε $x \in \mathbb{Q}$, τέτοιος ώστε να ικανοποιείται η (1.60), τότε θα υπήρχαν $a \in \mathbb{Z}$ και $b \in \mathbb{Z}\smallsetminus\{0\}$ με $x = \frac{a}{b}$, οπότε θα είχαμε

$$x^2 = (\tfrac{a}{b})^2 = \tfrac{a^2}{b^2} = 2 \Longrightarrow a^2 = 2 \cdot_{\mathbb{Z}} b^2. \tag{1.61}$$

Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι οι a, b δεν διαθέτουν κάποιον κοινό διαιρέτη[45] πέραν των 1 και -1. (Πρβλ. σημείωση[46] 1.8.14.) Λόγω τής (1.61) ο a^2 θα ήταν ένας *άρτιος* αριθμός. (Βλ. εδ. 1.7.9.) Επειδή το γινόμενο δύο περιττών ακεραίων αριθμών είναι περιττός, *ο ίδιος ο* a θα όφειλε να είναι *άρτιος*, ήτοι τής μορφής $a = 2 \cdot_{\mathbb{Z}} c$, για κάποιον $c \in \mathbb{Z}$, οπότε θα είχαμε

$$2 \cdot_{\mathbb{Z}} (2 \cdot_{\mathbb{Z}} c^2) = 4 \cdot_{\mathbb{Z}} c^2 = (2 \cdot_{\mathbb{Z}} c)^2 = a^2 = 2 \cdot_{\mathbb{Z}} b^2$$

και (εξαιτίας τού νόμου τής διαγραφής 1.7.15 (viii))

$$b^2 = 2 \cdot_{\mathbb{Z}} c^2,$$

απ' όπου θα έπετο (με την ίδια συλλογιστική) ότι ο b^2 και, κατ' επέκταση, και ο ίδιος ο b, θα ήταν *άρτιος*, κάτι που θα μας οδηγούσε σε *άτοπο* (διότι το 2 θα ήταν κοινός διαιρέτης των a, b). Η αναζήτηση ενός σύνολου «ευρύτερου» τού $\mathbb{Q}$, τέτοιου ώστε εξισώσεις όπως η (1.60) να διαθέτουν πάντοτε λύσεις εντός αυτού, μας οδηγεί στον ορισμό τού $\mathbb{R}$. Υπάρχουν διάφοροι (αλλ' εντούτοις, «ισοδύναμοι») τρόποι αυστηρής κατασκευής των λεγομένων *πραγματικών αριθμών*. Οι κυριότεροι είναι οι ακόλουθοι:

- Κατασκευή τού $\mathbb{R}$ μέσω ακολουθιών Cauchy ρητών αριθμών (1872).
- Κατασκευή πραγματικών αριθμών μέσω εγκιβωτισμών ρητών κλειστών διαστημάτων (1892).
- Κατασκευή πραγματικών αριθμών μέσω τομών Dedekind[47] (1872).
- Κατασκευή πραγματικών αριθμών μέσω (πεπερασμένων και άπειρων) ακολουθιών δυαδικών κλασμάτων[48].

Εδώ θα παρουσιασθεί μόνον ο *πρώτος*, ήτοι ο «αλγεβρικότερος» εξ αυτών.

1.9.1 Ορισμός. Επί τού συνόλου $\mathrm{CS}(\mathbb{Q})$ των ακολουθιών Cauchy ρητών αριθμών ορίζουμε τη διμελή σχέση "$\sim_{\mathrm{C}}$" ως ακολούθως:

$$\boxed{(r_n)_{n\in\mathbb{N}} \sim_{\mathrm{C}} (s_n)_{n\in\mathbb{N}} \underset{\text{ορσ}}{\Longleftrightarrow} (r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (-s_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q}).} \tag{1.62}$$

[45] Ένας $k \in \mathbb{Z}$ καλείται **κοινός διαιρέτης** των a και b όταν υπάρχουν $\lambda, \mu \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει $a = k \cdot_{\mathbb{Z}} \lambda$ και $b = k \cdot_{\mathbb{Z}} \mu$.

[46] Εάν, εν προκειμένω, οι a, b διέθεταν κάποιους κοινούς διαιρέτες πέραν των 1 και -1, τότε θα αρκούσε στη θέση των a, b να θεωρήσουμε τους $\frac{a}{m}, \frac{b}{m}$, όπου m ο *μέγιστος* των κοινών τους διαιρετών ως προς την "$\leqslant_{\mathbb{Z}}$". Προφανώς, το κλάσμα με αριθμητή τον $\frac{a}{m}$ και παρονομαστή τον $\frac{b}{m}$ θα ισούται με τον x.

[47] Βλ., π.χ., E.D. Bloch: *The Real Numbers and Real Analysis*, Springer-Verlag, 2011, §1.6-§1.8, σελ. 33-60.

[48] Βλ. Ch. Blatter: *Ein konkretes Modell der reellen Zahlen*, Elemente der Mathematik **65** (2010), 49-61, European Mathematical Society.

1.9.2 Λήμμα. *Η "$\sim_{\mathrm{C}}$" είναι μια σχέση ισοδυναμίας επί τού* $\mathrm{CS}(\mathbb{Q})$.

Απόδειξη. Για οιεσδήποτε $(r_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}}, (t_n)_{n\in\mathbb{N}} \in \mathrm{CS}(\mathbb{Q})$ έχουμε

$$1.8.39\ (\mathrm{v}) \Rightarrow (r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (-r_n)_{n\in\mathbb{N}} = 0_{\mathrm{CS}(\mathbb{Q})} \in \mathrm{NS}(\mathbb{Q}) \Rightarrow (r_n)_{n\in\mathbb{N}} \sim_{\mathrm{C}} (r_n)_{n\in\mathbb{N}},$$

τις συνεπαγωγές

$$\begin{aligned}(r_n)_{n\in\mathbb{N}} \sim_{\mathrm{C}} (s_n)_{n\in\mathbb{N}} &\underset{1.8.39\,(\mathrm{i})}{\Longrightarrow} (s_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (r_n)_{n\in\mathbb{N}} = (r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q})\\ &\Rightarrow (s_n)_{n\in\mathbb{N}} \sim_{\mathrm{C}} (r_n)_{n\in\mathbb{N}},\end{aligned}$$

καθώς και τις

$$\left.\begin{array}{rl} & (r_n)_{n\in\mathbb{N}} \sim_{\mathrm{C}} (s_n)_{n\in\mathbb{N}}\\ \text{και} & (s_n)_{n\in\mathbb{N}} \sim_{\mathrm{C}} (t_n)_{n\in\mathbb{N}}\end{array}\right\} \Rightarrow \left\{\begin{array}{l}(r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (-s_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q})\\ (s_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (-t_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q})\end{array}\right\}$$

$$\begin{aligned}&\underset{1.8.42}{\Longrightarrow} \big((r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (-s_n)_{n\in\mathbb{N}}\big) \boxplus_{\mathbb{Q}} \big((s_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (-t_n)_{n\in\mathbb{N}}\big)\\ &= (r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (-t_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q}) \Rightarrow (s_n)_{n\in\mathbb{N}} \sim_{\mathrm{C}} (t_n)_{n\in\mathbb{N}}.\end{aligned}$$

Άρα η "$\sim_{\mathrm{C}}$" είναι ανακλαστική, συμμετρική και μεταβατική. □

1.9.3 Λήμμα. *Η "$\sim_{\mathrm{C}}$" είναι συμβατή τόσον με την "$\boxplus_{\mathbb{Q}}$" όσον και με την "$\boxdot_{\mathbb{Q}}$".*

Απόδειξη. Θεωρώντας διατεταγμένα ζεύγη ακολουθιών Cauchy ρητών αριθμών $((r_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}}), ((r'_n)_{n\in\mathbb{N}}, (s'_n)_{n\in\mathbb{N}}) \in \mathrm{CS}(\mathbb{Q}) \times \mathrm{CS}(\mathbb{Q})$, τέτοια ώστε να ισχύει $(r_n)_{n\in\mathbb{N}} \sim_{\mathrm{C}} (r'_n)_{n\in\mathbb{N}}$ και $(s_n)_{n\in\mathbb{N}} \sim_{\mathrm{C}} (s'_n)_{n\in\mathbb{N}}$, ή -ισοδυνάμως-

$$(r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (-r'_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q}) \ \text{ και } \ (s_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (-s'_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q}), \tag{1.63}$$

έχουμε (λόγω των 1.8.39 (i) και 1.8.42 (i))

$$\begin{aligned}&\big((r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}\big) \boxplus_{\mathbb{Q}} \big(-((r'_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (s'_n)_{n\in\mathbb{N}})\big)\big)\\ = \ &\big((r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}\big) \boxplus_{\mathbb{Q}} \big((-r'_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (-s'_n)_{n\in\mathbb{N}}\big)\\ = \ &\big((r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (-r'_n)_{n\in\mathbb{N}}\big) \boxplus_{\mathbb{Q}} \big((s_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (-s'_n)_{n\in\mathbb{N}}\big) \in \mathrm{NS}(\mathbb{Q}),\end{aligned}$$

οπότε $(r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}} \sim_{\mathrm{C}} (r'_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (s'_n)_{n\in\mathbb{N}}$. Εξάλλου, υπό την ίδια προϋπόθεση (1.63) συνάγεται (μέσω των 1.8.39 (v), 1.8.40 (i), (vi)) ότι

$$\begin{aligned}&\big((r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}\big) \boxplus_{\mathbb{Q}} \big(-((r'_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s'_n)_{n\in\mathbb{N}})\big)\big)\\ &= \big((r_n \cdot_{\mathbb{Q}} s_n)_{n\in\mathbb{N}}\big) \boxplus_{\mathbb{Q}} \big((-r'_n \cdot_{\mathbb{Q}} s'_n)_{n\in\mathbb{N}}\big)\\ &= \big((r_n \cdot_{\mathbb{Q}} s_n)_{n\in\mathbb{N}}\big) \boxplus_{\mathbb{Q}} \big((-r'_n \cdot_{\mathbb{Q}} s_n)_{n\in\mathbb{N}}\big) \boxplus_{\mathbb{Q}} \big((r'_n \cdot_{\mathbb{Q}} s_n)_{n\in\mathbb{N}}\big) \boxplus_{\mathbb{Q}} \big((-r'_n \cdot_{\mathbb{Q}} s'_n)_{n\in\mathbb{N}}\big)\\ &= \big(\underbrace{\big((r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (-r'_n)_{n\in\mathbb{N}}\big)}_{\in \mathrm{NS}(\mathbb{Q})} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}\big) \boxplus_{\mathbb{Q}} \big((r'_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} \big(\underbrace{\big((r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (-r'_n)_{n\in\mathbb{N}}\big)}_{\in \mathrm{NS}(\mathbb{Q})}\big)\big),\end{aligned}$$

οπότε $(r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}} \sim_{\mathrm{C}} (r'_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s'_n)_{n\in\mathbb{N}}$ λόγω των 1.8.42 (i) και (ii). □

1.9.4 Ορισμός. Το **σύνολο των πραγματικών αριθμών** ορίζεται να είναι το σύνολο

$$\boxed{\mathbb{R} := \mathrm{CS}(\mathbb{Q})/\sim_{\mathrm{C}}} \tag{1.64}$$

Οι κλάσεις ισοδυναμίας

$$\boxed{[(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}} := \{(s_n)_{n\in\mathbb{N}} \in \mathrm{CS}(\mathbb{Q}) \,|\, (r_n)_{n\in\mathbb{N}} \sim_{\mathrm{C}} (s_n)_{n\in\mathbb{N}}\}}$$

των $(r_n)_{n\in\mathbb{N}} \in \mathrm{CS}(\mathbb{Q})$ ως προς την "$\sim_{\mathrm{C}}$" καλούνται **πραγματικοί αριθμοί**.

1.9.5 Θεώρημα. *Επί τού* $\mathbb{R}$ *ορίζονται δύο εσωτερικές πράξεις* "$+_{\mathbb{R}}$" *και* "$\cdot_{\mathbb{R}}$":

$$\begin{aligned}([(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}}, [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}}) &\longmapsto [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}} +_{\mathbb{R}} [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}},\\ ([(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}}, [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}}) &\longmapsto [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \cdot_{\mathbb{R}} [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}},\end{aligned}$$

μέσω των τύπων

$$\boxed{[(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}} +_{\mathbb{R}} [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}} := [(r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}]_{\mathrm{C}}} \tag{1.65}$$

και

$$\boxed{[(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \cdot_{\mathbb{R}} [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}} := [(r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}]_{\mathrm{C}}} \tag{1.66}$$

αντιστοίχως. Αυτές είναι οι μοναδικές απεικονίσεις από το $\mathbb{R}\times\mathbb{R}$ *στο* $\mathbb{R}$ *οι οποίες καθιστούν τα διαγράμματα*

$$\begin{array}{ccc} \mathrm{CS}(\mathbb{Q})\times\mathrm{CS}(\mathbb{Q}) & \xrightarrow{\boxplus_{\mathbb{Q}}} & \mathrm{CS}(\mathbb{Q}) \\ \downarrow{\scriptstyle \pi_{\sim_{\mathrm{C}}}\times\pi_{\sim_{\mathrm{C}}}} & & \downarrow{\scriptstyle \pi_{\sim_{\mathrm{C}}}} \\ \mathbb{R}\times\mathbb{R} & \xrightarrow[+_{\mathbb{R}}]{} & \mathbb{R} \end{array}$$

και

$$\begin{array}{ccc} \mathrm{CS}(\mathbb{Q})\times\mathrm{CS}(\mathbb{Q}) & \xrightarrow{\boxdot_{\mathbb{Q}}} & \mathrm{CS}(\mathbb{Q}) \\ \downarrow{\scriptstyle \pi_{\sim_{\mathrm{C}}}\times\pi_{\sim_{\mathrm{C}}}} & & \downarrow{\scriptstyle \pi_{\sim_{\mathrm{C}}}} \\ \mathbb{R}\times\mathbb{R} & \xrightarrow[\cdot_{\mathbb{R}}]{} & \mathbb{R} \end{array}$$

μεταθετικά.

Απόδειξη. Κατά το λήμμα 1.9.3 η σχέση ισοδυναμίας "$\sim_{\mathrm{C}}$" είναι συμβατή με αμφότερες τις πράξεις "$\boxplus_{\mathbb{Q}}$" και "$\boxdot_{\mathbb{Q}}$". Ως εκ τούτου, είναι δυνατή η εφαρμογή τού θεωρήματος 1.5.20 για καθεμιά εξ αυτών και ο προσδιορισμός των μοναδικών απεικονίσεων (1.65) και (1.66) που καθιστούν τα ανωτέρω διαγράμματα μεταθετικά. □

1.9.6 Ορισμός. Οι εσωτερικές πράξεις "$+_{\mathbb{R}}$" και "$\cdot_{\mathbb{R}}$" οι ορισθείσες στο θεώρημα 1.9.5 καλούνται **πρόσθεση** και **πολλαπλασιασμός (των πραγματικών αριθμών)**, αντιστοίχως. Εάν $x, y \in \mathbb{R}$, τότε οι πραγματικοί αριθμοί $x +_{\mathbb{R}} y$ και $x \cdot_{\mathbb{R}} y$ καλούνται **άθροισμα** και **γινόμενο των** x **και** y, αντιστοίχως.

1.9.7 Ορισμός. (i) Το στοιχείο $0_{\mathbb{R}} := [0_{\mathrm{CS}(\mathbb{Q})}]_{\mathrm{C}} = [(0_{\mathbb{Q}})_{n\in\mathbb{N}}]_{\mathrm{C}}$ τού $\mathbb{R}$ ονομάζεται **μηδέν** (ή, ακριβέστερα, **μηδενικό στοιχείο) τού** $\mathbb{R}$.

(ii) Το $1_{\mathbb{R}} := [1_{\mathrm{CS}(\mathbb{Q})}]_{\mathrm{C}} = [(1_{\mathbb{Q}})_{n\in\mathbb{N}}]_{\mathrm{C}}$ ονομάζεται **μοναδιαίο στοιχείο τού** $\mathbb{R}$.

(iii) Εάν $x = [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \in \mathbb{R}$, τότε λέμε ότι ο πραγματικός αριθμός

$$-x := [(-r_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$$

είναι **ο αντίθετος τού** r.

1.9.8 Παρατήρηση. Προφανώς, κάθε σταθερή ακολουθία ρητών αριθμών $(r)_{n\in\mathbb{N}}$ με $r \neq 0_{\mathbb{Q}}$ είναι μη μηδενική (υπό την έννοια τού ορισμού 1.8.33). Ιδιαιτέρως έχουμε $0_{\mathrm{CS}(\mathbb{Q})} \neq 1_{\mathrm{CS}(\mathbb{Q})}$.

1.9.9 Πρόταση (Ιδιότητες προσθέσεως). *Η πρόσθεση πραγματικών αριθμών έχει τις εξής ιδιότητες*:

(i) **[Μεταθετική ιδιότητα]** $x +_{\mathbb{R}} y = y +_{\mathbb{R}} x, \forall (x, y) \in \mathbb{R} \times \mathbb{R}$.

(ii) **[Προσεταιριστική ιδιότητα]** *Για οιουσδήποτε* $u, x, y \in \mathbb{R}$ *ισχύει η ισότητα*

$$(u +_{\mathbb{R}} x) +_{\mathbb{R}} y = u +_{\mathbb{R}} (x +_{\mathbb{R}} y)\,.$$

(iii) **[Νόμος τής διαγραφής]** *Για οιουσδήποτε* $u, x, y \in \mathbb{R}$ *ισχύει η συνεπαγωγή*

$$x +_{\mathbb{R}} u = y +_{\mathbb{R}} u \Longrightarrow x = y.$$

(iv) **[Ύπαρξη ουδετέρου στοιχείου]** *Το* $0_{\mathbb{R}}$ *είναι ουδέτερο στοιχείο τού* $\mathbb{R}$ *ως προς την* "$+_{\mathbb{R}}$" (βλ. 1.5.6), *δηλαδή*

$$0_{\mathbb{R}} +_{\mathbb{R}} x = x = x +_{\mathbb{R}} 0_{\mathbb{R}}, \quad \forall x \in \mathbb{R}.$$

(v) **[Ύπαρξη συμμετρικού στοιχείου]** *Κάθε* $x \in \mathbb{R}$ *έχει τον αντίθετό του ως συμμετρικό του στοιχείο ως προς την* "$+_{\mathbb{R}}$" (βλ. 1.5.11), *δηλαδή*

$$(-x) +_{\mathbb{R}} x = 0_{\mathbb{R}} = x +_{\mathbb{R}} (-x)\,.$$

Απόδειξη. Τα (i), (ii), (iv) και (v) έπονται από τα (i), (ii), (iv) και (v) τής προτάσεως 1.8.39, το θεώρημα 1.9.5 και τα (b), (c), (d) και (e) τού θεωρήματος 1.5.20.

(iii) Εάν οι $x = [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$, $y = [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$ και $u = [(t_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \in \mathbb{R}$ είναι τέτοιοι ώστε να ισχύει η ισότητα $x +_{\mathbb{R}} u = y +_{\mathbb{R}} u$, τότε

$$[(r_n +_{\mathbb{Q}} t_n)_{n\in\mathbb{N}}]_{\mathrm{C}} = [(s_n +_{\mathbb{Q}} t_n)_{n\in\mathbb{N}}]_{\mathrm{C}},$$

κάτι που ισοδυναμεί με τη συνθήκη

$$((r_n +_{\mathbb{Q}} t_n) - (s_n +_{\mathbb{Q}} t_n))_{n\in\mathbb{N}} = (r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (-s_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q}),$$

απ' όπου έπεται ότι $(r_n)_{n\in\mathbb{N}} \sim_{\mathrm{C}} (s_n)_{n\in\mathbb{N}} \Rightarrow x = y$. □

1.9.10 Σημείωση. Εάν $x, y \in \mathbb{R}$, τότε ο πραγματικός αριθμός $x +_{\mathbb{R}} (-y)$ καλείται **διαφορά** τού x από τον y (σημειούμενος συνήθως ως $x - y$). Η εσωτερική πράξη

$$\mathbb{R} \times \mathbb{R} \ni (x, y) \longmapsto x +_{\mathbb{R}} (-y) \in \mathbb{R}$$

επί τού $\mathbb{R}$ (**πράξη αφαιρέσεως**), όπως και στην περίπτωση που εργαζόμασταν μόνον με ακεραίους ή με ρητούς (βλ. 1.7.14 και 1.8.12), *δεν είναι ούτε* μεταθετική *ούτε* προσεταιριστική. Επίσης, το $0_{\mathbb{R}}$ αποτελεί εκ δεξιών αλλά όχι και εξ αριστερών ουδέτερο στοιχείο τού $\mathbb{R}$ ως προς αυτήν.

Τής παραθέσεως των ιδιοτήτων τού πολλαπλασιασμού πραγματικών αριθμών προηγείται μια βοηθητική σημείωση.

1.9.11 Σημείωση (Κατασκευή αντιστρόφου ενός $x \in \mathbb{R}\setminus\{0_{\mathbb{R}}\}$**.).** Έστω τυχών πραγματικός αριθμός $x = [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \in \mathbb{R}\setminus\{0_{\mathbb{R}}\}$. Επειδή η ακολουθία $(r_n)_{n\in\mathbb{N}}$ δεν είναι μηδενική, υπάρχει κάποιος $\varepsilon \in \mathbb{Q}_{>0}$, καθώς και κάποιος $n_1 \in \mathbb{N}$, ούτως ώστε να ισχύει

$$|r_n| \geqslant_{\mathbb{Q}} \varepsilon, \text{ για οιονδήποτε φυσικό αριθμό } n \geqslant n_1.$$

Επιπροσθέτως, επειδή η $(r_n)_{n\in\mathbb{N}}$ είναι εξ ορισμού ακολουθία Cauchy ρητών αριθμών, για τον $\frac{\varepsilon}{2} \in \mathbb{Q}_{>0}$ υπάρχει δείκτης $n_2 = n_2(\frac{\varepsilon}{2}) \in \mathbb{N}$, ούτως ώστε να ισχύει

$$|r_m - r_n| <_{\mathbb{Q}} \frac{\varepsilon}{2}, \text{ για οιουσδήποτε φυσικούς αριθμούς } m, n \geqslant n_2.$$

Έστω $n_0 := \max\{n_1, n_2\}$. Τότε για κάθε $m \geqslant n_0$ υφίσταται κάποιος $n \geqslant n_0$, ούτως ώστε να έχουμε ταυτοχρόνως

$$\left.\begin{aligned} |r_n| &\geqslant_{\mathbb{Q}} \varepsilon \\ |r_m - r_n| &<_{\mathbb{Q}} \tfrac{\varepsilon}{2} \end{aligned}\right\} \Rightarrow |r_m| >_{\mathbb{Q}} \frac{\varepsilon}{2}.$$

Η τελευταία ανισότητα είναι αληθής, διότι εάν υποθέταμε ότι $|r_m| \leqslant_{\mathbb{Q}} \frac{\varepsilon}{2}$, τότε θα συμπεραίναμε ότι

$$|r_n| = |(r_n - r_m) +_{\mathbb{Q}} r_m| \leqslant_{\mathbb{Q}} |(r_n - r_m)| +_{\mathbb{Q}} |r_m| <_{\mathbb{Q}} \varepsilon,$$

πράγμα άτοπο. (Σημειωτέον ότι $r_m \neq 0_{\mathbb{Q}}$ για κάθε $m \geqslant n_0$.) Κατόπιν τούτου ορίζουμε την ακολουθία ρητών αριθμών $(r'_n)_{n\in\mathbb{N}}$ μέσω τού τύπου

$$r'_n := \begin{cases} 0_{\mathbb{Q}}, & \text{όταν } n < n_0, \\ r_n^{-1}, & \text{όταν } n \geqslant n_0. \end{cases}$$

Η $(r'_n)_{n\in\mathbb{N}}$ είναι ακολουθία Cauchy. Πράγματι· επειδή η $(r_n)_{n\in\mathbb{N}}$ ακολουθία Cauchy, για κάθε $\delta \in \mathbb{Q}_{>0}$, άρα και για τον $\delta \cdot_{\mathbb{Q}} \varepsilon^2 \in \mathbb{Q}_{>0}$, υπάρχει δείκτης $n'_0 = n'_0(\delta \cdot_{\mathbb{Q}} \varepsilon^2) \in \mathbb{N}$, ούτως ώστε να ισχύει

$$|r_m - r_n| <_{\mathbb{Q}} \delta \cdot_{\mathbb{Q}} \varepsilon^2, \text{ για οιουσδήποτε φυσικούς αριθμούς } m, n \geqslant n'_0.$$

Κατά συνέπειαν, για οιουσδήποτε φυσικούς $m, n \geqslant \max\{n_0, n'_0\}$ έχουμε

$$\left|r'_m - r'_n\right| = \left|r_m^{-1} - r_n^{-1}\right| = \tfrac{|r_m - r_n|}{|r_m| \cdot_{\mathbb{Q}} |r_n|} <_{\mathbb{Q}} \tfrac{\delta \cdot_{\mathbb{Q}} \varepsilon^2}{\varepsilon^2} = \delta,$$

οπότε $(r'_n)_{n\in\mathbb{N}} \in \mathrm{CS}(\mathbb{Q})$. Επειδή (εκ κατασκευής)

$$r_n \cdot_{\mathbb{Q}} r'_n := \begin{cases} 0_{\mathbb{Q}}, & \text{όταν } n < n_0, \\ 1_{\mathbb{Q}}, & \text{όταν } n \geqslant n_0, \end{cases}$$

συνάγεται ότι

$$(r_n \cdot_{\mathbb{Q}} r'_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (-1_{\mathbb{Q}})_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q}) \Rightarrow [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \cdot_{\mathbb{R}} [(r'_n)_{n\in\mathbb{N}}]_{\mathrm{C}} = 1_{\mathbb{R}}.$$

1.9.12 Ορισμός. Εάν $x = [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \in \mathbb{R} \setminus \{0_{\mathbb{R}}\}$, τότε λέμε ότι ο

$$x^{-1} := [(r'_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \in \mathbb{R} \setminus \{0_{\mathbb{R}}\},$$

(όπου $(r'_n)_{n\in\mathbb{N}} \in \mathrm{CS}(\mathbb{Q})$ η ακολουθία η κατασκευασθείσα στο εδάφιο 1.9.11) είναι **ο αντίστροφος τού** x.

1.9.13 Πρόταση (Ιδιότητες πολλαπλασιασμού). *Ο πολλαπλασιασμός πραγματικών αριθμών έχει τις εξής ιδιότητες*:

(i) **[Μεταθετική ιδιότητα]** $x \cdot_{\mathbb{R}} y = y \cdot_{\mathbb{R}} x, \forall (x, y) \in \mathbb{R} \times \mathbb{R}$.

(ii) **[Προσεταιριστική ιδιότητα]** *Για οιουσδήποτε* $w, x, y \in \mathbb{R}$ *ισχύει η ισότητα*

$$(w \cdot_{\mathbb{R}} x) \cdot_{\mathbb{R}} y = w \cdot_{\mathbb{R}} (x \cdot_{\mathbb{R}} y).$$

(iii) *Για οιονδήποτε* $x \in \mathbb{R}$ *ισχύουν οι ισότητες*

$$0_{\mathbb{R}} \cdot_{\mathbb{R}} x = 0_{\mathbb{R}} = x \cdot_{\mathbb{R}} 0_{\mathbb{R}}.$$

(iv) **[Ύπαρξη ουδετέρου στοιχείου]** *Το* $1_{\mathbb{R}}$ *είναι ουδέτερο στοιχείο τού* $\mathbb{R}$ *ως προς την* "$\cdot_{\mathbb{R}}$" (βλ. 1.5.6), *δηλαδή*

$$1_{\mathbb{R}} \cdot_{\mathbb{R}} x = x = x \cdot_{\mathbb{R}} 1_{\mathbb{R}},\ \forall x \in \mathbb{R}.$$

(v) **[Ύπαρξη συμμετρικού στοιχείου για** $x \neq 0_{\mathbb{R}}$**]** *Κάθε* $x \in \mathbb{R} \setminus \{0_{\mathbb{R}}\}$ *έχει τον αντίστροφό του ως συμμετρικό του στοιχείο ως προς την* "$\cdot_{\mathbb{R}}$" (βλ. 1.5.11), *δηλαδή*

$$x^{-1} \cdot_{\mathbb{R}} x = 1_{\mathbb{R}} = x \cdot_{\mathbb{R}} x^{-1}.$$

(vi) *Για οιουσδήποτε* $x, y \in \mathbb{R}$ *ισχύουν οι ισότητες*

$$(-x) \cdot_{\mathbb{R}} y = -\left(x \cdot_{\mathbb{R}} y\right) = x \cdot_{\mathbb{R}} (-y),\ \ (-x) \cdot_{\mathbb{R}} (-y) = x \cdot_{\mathbb{R}} y.$$

(vii) **[Επιμεριστική ιδιότητα τού πολλαπλασιασμού ως προς την πρόσθεση]** *Για οιουσδήποτε* $u, x, y \in \mathbb{R}$ *ισχύουν οι ισότητες*

$$u \cdot_{\mathbb{R}} (x +_{\mathbb{R}} y) = (u \cdot_{\mathbb{R}} x) +_{\mathbb{R}} (u \cdot_{\mathbb{R}} y)\,,\ \ (x +_{\mathbb{R}} y) \cdot_{\mathbb{R}} u = (x \cdot_{\mathbb{R}} u) +_{\mathbb{R}} (y \cdot_{\mathbb{R}} u)\,.$$

(viii) *Εάν* $x, y \in \mathbb{R}$ *με* $x \cdot_{\mathbb{R}} y = 0_{\mathbb{R}}$, *τότε είτε* $x = 0_{\mathbb{R}}$ *είτε* $y = 0_{\mathbb{R}}$.

(ix) **[Νόμος τής διαγραφής]** *Για* $u, x, y, \in \mathbb{R}$ *με* $u \neq 0_{\mathbb{R}}$ *ισχύει η συνεπαγωγή*

$$x \cdot_{\mathbb{R}} u = y \cdot_{\mathbb{R}} u \Longrightarrow x = y.$$

Απόδειξη. Τα (i), (ii) και (iv) έπονται άμεσα από τα (i), (ii) και (iv) τής προτάσεως 1.8.40, το θεώρημα 1.9.5 και τα (b), (c) και (d) τού θεωρήματος 1.5.20.

(iii) Για οιονδήποτε $x = [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \in \mathbb{R}$ έχουμε

$$\begin{aligned} 0_{\mathbb{R}} \cdot_{\mathbb{R}} x &= [0_{\mathrm{CS}(\mathbb{Q})}]_{\mathrm{C}} \cdot_{\mathbb{R}} [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}} = [(0_{\mathbb{Q}})_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (r_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \\ &= [(0_{\mathbb{Q}} \cdot_{\mathbb{Q}} r_n)_{n\in\mathbb{N}}] = [(0_{\mathbb{Q}})_{n\in\mathbb{N}}] = [0_{\mathrm{CS}(\mathbb{Q})}]_{\mathrm{C}} = 0_{\mathbb{R}}. \end{aligned}$$

Η δεύτερη ισότητα είναι προφανής, διότι η "$\cdot_{\mathbb{R}}$" (κατά το (i)) είναι μεταθετική.

(v) Τούτο έπεται από όσα προαναφέρθησαν στο εδάφιο 1.9.11.

(vi) Εάν $x = [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$ και $y = [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \in \mathbb{R}$, τότε το 1.8.40 (v) μας δίδει

$$\begin{aligned} (-x) \cdot_{\mathbb{R}} y &= [(-r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \\ &= [-\left((r_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}\right)]_{\mathrm{C}} = -\left(x \cdot_{\mathbb{R}} y\right). \end{aligned}$$

Οι λοιπές ισότητες αποδεικνύονται παρομοίως.

(vii) Εάν $x = [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$, $y = [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$ και $u = [(t_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \in \mathbb{R}$, τότε μέσω τού (vi) τής προτάσεως 1.8.40 συνάγεται ότι

$$\begin{aligned} u \cdot_{\mathbb{R}} (x +_{\mathbb{R}} y) &= [(t_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \cdot_{\mathbb{R}} [(r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \\ &= [(t_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} ((r_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}})]_{\mathrm{C}} \\ &= [((t_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (r_n)_{n\in\mathbb{N}}) \boxplus_{\mathbb{Q}} ((t_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}})]_{\mathrm{C}} \\ &= [(t_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (r_n)_{n\in\mathbb{N}}]_{\mathrm{C}} +_{\mathbb{R}} [(t_n)_{n\in\mathbb{N}} \boxdot_{\mathbb{Q}} (s_n)_{n\in\mathbb{N}})]_{\mathrm{C}} \\ &= ([(t_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \cdot_{\mathbb{R}} [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}}) +_{\mathbb{R}} ([(t_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \cdot_{\mathbb{R}} [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}}) \\ &= (u \cdot_{\mathbb{R}} x) +_{\mathbb{R}} (u \cdot_{\mathbb{R}} y) \end{aligned}$$

Η δεύτερη ισότητα είναι προφανής λόγω τής μεταθετικότητας τής "$\cdot_{\mathbb{R}}$".

(viii) Ας υποθέσουμε ότι $x, y \in \mathbb{R}$ με $x \cdot_{\mathbb{R}} y = 0_{\mathbb{R}}$. Εάν $x \neq 0_{\mathbb{R}}$, τότε εφαρμόζοντας κατά σειράν τα (iv), (v), (ii) και (iii) λαμβάνουμε

$$y = 1_{\mathbb{R}} \cdot_{\mathbb{R}} y = (x^{-1} \cdot_{\mathbb{R}} x) \cdot_{\mathbb{R}} y = x^{-1} \cdot_{\mathbb{R}} (x \cdot_{\mathbb{R}} y) = x^{-1} \cdot_{\mathbb{R}} 0_{\mathbb{R}} = 0_{\mathbb{R}}.$$

Κατ' αναλογίαν, εάν $y \neq 0_{\mathbb{R}}$, τότε $x = 0_{\mathbb{R}}$.

(ix) Λόγω τής επιμεριστικής ιδιότητας (vii) έχουμε

$$x \cdot_{\mathbb{R}} u = y \cdot_{\mathbb{R}} u \Rightarrow (x-y) \cdot_{\mathbb{R}} u = 0_{\mathbb{R}}.$$

Εξ υποθέσεως, $u \neq 0_{\mathbb{R}}$. Από το (viii) προκύπτει ότι $x - y = 0_{\mathbb{R}} \Rightarrow x = y$. □

1.9.14 Σημείωση (Κλάσματα με πραγματικούς αριθμητές και παρονομαστές). Σε ορισμένες περιπτώσεις είθισται, για λόγους συντομίας, να γράφουμε κάποιους πραγματικούς αριθμούς υπό τη μορφή «κλασμάτων» $\frac{x}{y}$ με *πραγματικούς* αριθμητές x και (μη μηδενικούς) *πραγματικούς* παρονομαστές y. Συγκεκριμένα, εάν $x = [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$ και $y = [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \in \mathbb{R}$, τότε χρησιμοποιώντας τό σύμβολο $\dfrac{x}{y}$ εννοούμε τον πραγματικό αριθμό

$$\boxed{\frac{x}{y} := x \cdot_{\mathbb{R}} y^{-1} = [(\tfrac{r_n}{s_n})_{n\in\mathbb{N}}]_{\mathrm{C}}.}$$

▸ **Ο ορισμός τής συνήθους διατάξεως επί τού** $\mathbb{R}$. Τα στοιχεία τού $\mathbb{R}$ διατάσσονται κατά τον πλέον «φυσικό» τρόπο ως ακολούθως:

1.9.15 Ορισμός. Επί τού $\mathbb{R}$ ορίζουμε τη διμελή σχέση

$$\boxed{x \leqslant_{\mathbb{R}} y \underset{\text{ορσ}}{\Longleftrightarrow} \text{είτε } x = y \text{ είτε } \left\{ \begin{array}{l} \exists q \in \mathbb{Q}_{>0} \text{ και } \exists n_0 = n_0(q) \in \mathbb{N} : \\ s_n - r_n >_{\mathbb{Q}} q, \ \forall \text{φυσικό } n \geqslant n_0. \end{array} \right\}} \tag{1.67}$$

όπου $x = [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$ και $y = [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \in \mathbb{R}$. Αυτή *δεν εξαρτάται* από την επιλογή των εκπροσώπων $(r_n)_{n\in\mathbb{N}}$ και $(s_n)_{n\in\mathbb{N}}$ των (κλάσεων ισοδυναμίας) x και y, αντιστοίχως. Πράγματι· εάν υποτεθεί ότι $x = [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}} = [(r'_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$ και $y = [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}} = [(s'_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$, με $x \leqslant_{\mathbb{R}} y$ και $x \neq y$, τότε αφ' ενός μεν

$$\exists q \in \mathbb{Q}_{>0} \text{ και } \exists n_0 = n_0(q) \in \mathbb{N} : s_n - r_n >_{\mathbb{Q}} q, \text{ για κάθε φυσικό } n \geqslant n_0,$$

αφ' ετέρου δε $(r_n - r'_n)_{n\in\mathbb{N}}, (s_n - s'_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q})$, οπότε

$$(s_n - s'_n)_{n\in\mathbb{N}} \boxplus_{\mathbb{Q}} (-(r_n - r'_n)_{n\in\mathbb{N}}) = ((s_n - r_n) - (s'_n - r'_n))_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q})$$

(βάσει τού θεωρήματος 1.9.5), απ' όπου έπεται ότι

$$\exists n'_0 = n'_0(\tfrac{q}{2}) \in \mathbb{N} : \left|(s_n - r_n) - (s'_n - r'_n)\right| <_{\mathbb{Q}} \tfrac{q}{2}, \text{ για κάθε φυσικό } n \geqslant n'_0.$$

Άρα για κάθε $n \geqslant \max\{n_0, n'_0\}$ έχουμε (λόγω τού 1.8.31 (iv))

$$q - (s'_n - r'_n) <_{\mathbb{Q}} (s_n - r_n) - (s'_n - r'_n) \leqslant_{\mathbb{Q}} \left|(s_n - r_n) - (s'_n - r'_n)\right| <_{\mathbb{Q}} \tfrac{q}{2},$$

απ' όπου προκύπτει ότι $s'_n - r'_n > q - \frac{q}{2} = \frac{q}{2}$.

(i) Όταν $x \leqslant_{\mathbb{R}} y$, τότε λέμε ότι ο x είναι **μικρότερος ή ίσος** τού y ή ότι ο y είναι **μεγαλύτερος ή ίσος** τού x (και γράφουμε, εναλλακτικώς, $y \geqslant_{\mathbb{R}} x$). Επίσης, λέμε ότι ο x είναι **μικρότερος** τού y ή ότι ο y είναι **μεγαλύτερος** τού x (και γράφουμε $x <_{\mathbb{R}} y$ ή $y >_{\mathbb{R}} x$) όταν $x \leqslant_{\mathbb{R}} y$ *και* $x \neq y$.

(ii) Κάθε $x \in \mathbb{R}$ για τον οποίο ισχύει $x >_{\mathbb{R}} 0_{\mathbb{R}}$ (και αντιστοίχως, $x <_{\mathbb{R}} 0_{\mathbb{R}}$) καλείται **θετικός** (και αντιστοίχως, **αρνητικός**) **πραγματικός αριθμός**. Το σύνολο των θετικών (και αντιστοίχως, των αρνητικών) πραγματικών αριθμών συμβολίζεται ως $\mathbb{R}_{>0}$ (και αντιστοίχως, ως $\mathbb{R}_{<0}$). Προφανώς, $x <_{\mathbb{R}} y \Longleftrightarrow y +_{\mathbb{R}} (-x) >_{\mathbb{R}} 0_{\mathbb{R}}$.

1.9.16 Θεώρημα (Νόμος τής «τριχοτομίας»). *Εάν* $(x, y) \in \mathbb{R} \times \mathbb{R}$, *τότε ισχύει ακριβώς ένα εκ των κάτωθι*:

(i) $x = y$.

(ii) $x <_{\mathbb{R}} y$.
(iii) $x >_{\mathbb{R}} y$.

ΑΠΟΔΕΙΞΗ. Αυτή θα γίνει σε τρία (εν συνόλω) βήματα. Έστω $x = [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$ και έστω $y = [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$.

Βήμα 1ο. Ας υποθέσουμε εν πρώτοις ότι $x \neq y$. Τότε η $(s_n - r_n)_{n\in\mathbb{N}}$ είναι μη μηδενική ακολουθία Cauchy, οπότε αφ' ενός μεν

$$\exists q \in \mathbb{Q}_{>0} \text{ και } \exists n_1 = n_1(q) \in \mathbb{N} : |s_n - r_n| \geqslant_{\mathbb{Q}} q, \ \forall \text{φυσικό } n \geqslant n_1,$$

αφ' ετέρου δε για το $\frac{q}{2} \in \mathbb{Q}_{>0}$,

$$\exists n_2 = n_2(\tfrac{q}{2}) \in \mathbb{N} : |(s_m - r_m) - (s_n - r_n)| <_{\mathbb{Q}} \tfrac{q}{2},$$

για οιουσδήποτε φυσικούς $m, n \geqslant n_2$. Έστω $n_0 := \max\{n_1, n_2\}$. Για οιουσδήποτε φυσικούς αριθμούς $m, n \geqslant n_0$ έχουμε

$$|s_n - r_n| \geqslant_{\mathbb{Q}} q \ \text{ και } \ |(s_m - r_m) - (s_n - r_n)| <_{\mathbb{Q}} \tfrac{q}{2}.$$

Ιδιαιτέρως, $|s_{n_0} - r_{n_0}| \geqslant_{\mathbb{Q}} q$, και για οιονδήποτε φυσικό αριθμό $n \geqslant n_0$ έχουμε

$$|(s_n - r_n) - (s_{n_0} - r_{n_0})| <_{\mathbb{Q}} \tfrac{q}{2} \Rightarrow -\tfrac{q}{2} <_{\mathbb{Q}} (s_n - r_n) - (s_{n_0} - r_{n_0}) <_{\mathbb{Q}} \tfrac{q}{2}.$$

ήτοι

$$(s_{n_0} - r_{n_0}) - \tfrac{q}{2} <_{\mathbb{Q}} (s_n - r_n) <_{\mathbb{Q}} (s_{n_0} - r_{n_0}) +_{\mathbb{Q}} \tfrac{q}{2}.$$

Επειδή $|s_{n_0} - r_{n_0}| \geqslant_{\mathbb{Q}} q$, εξετάζουμε δύο περιπτώσεις χωριστά.

Περίπτωση πρώτη. Εάν $n \geqslant n_0$ και $s_{n_0} - r_{n_0} \geqslant_{\mathbb{Q}} q$, τότε

$$s_n - r_n >_{\mathbb{Q}} (s_{n_0} - r_{n_0}) - \tfrac{q}{2} \geqslant_{\mathbb{Q}} q - \tfrac{q}{2} = \tfrac{q}{2} \Rightarrow x <_{\mathbb{R}} y.$$

Περίπτωση δεύτερη. Εάν $n \geqslant n_0$ και $s_{n_0} - r_{n_0} \leqslant_{\mathbb{Q}} -q$, τότε

$$r_n - s_n >_{\mathbb{Q}} (r_{n_0} - s_{n_0}) - \tfrac{q}{2} \geqslant_{\mathbb{Q}} q - \tfrac{q}{2} = \tfrac{q}{2} \Rightarrow x >_{\mathbb{R}} y.$$

Άρα απεδείχθη η συνεπαγωγή $x \neq y \Rightarrow$ είτε $x <_{\mathbb{R}} y$ είτε $x >_{\mathbb{R}} y$.

Βήμα 2ο. Εάν $x \neq y$ και $x <_{\mathbb{R}} y$, τότε

$$\exists q \in \mathbb{Q}_{>0} \text{ και } \exists n_\bullet = n_\bullet(q) \in \mathbb{N} : s_n - r_n >_{\mathbb{Q}} q, \ \forall \text{φυσικό } n \geqslant n_\bullet,$$

οπότε $r_n - s_n <_{\mathbb{Q}} -q <_{\mathbb{Q}} 0_{\mathbb{Q}}$ για κάθε φυσικό αριθμό $n \geqslant n_\bullet$. Τούτο σημαίνει ότι είναι αδύνατον να ισχύει $x >_{\mathbb{R}} y$. Κατ' αναλογίαν, εάν $x \neq y$ και $x >_{\mathbb{R}} y$, τότε είναι αδύνατον να ισχύει $x <_{\mathbb{R}} y$.

Βήμα 3ο. Εάν $x = y$, τότε $(s_n - r_n)_{n\in\mathbb{N}} \in \mathrm{NS}(\mathbb{Q})$, οπότε για κάθε $\varepsilon \in \mathbb{Q}_{>0}$ υπάρχει δείκτης $n_\star = n_\star(\varepsilon) \in \mathbb{N}$, ούτως ώστε

$$|s_n - r_n| <_{\mathbb{Q}} \varepsilon, \text{ για οιονδήποτε φυσικό αριθμό } \ n \geqslant n_\star.$$

Επομένως, $s_n - r_n \leqslant_{\mathbb{Q}} |s_n - r_n| <_{\mathbb{Q}} \varepsilon$ για κάθε φυσικό αριθμό $n \geqslant n_\star$. Αυτό σημαίνει ότι είναι αδύνατον να ισχύει *ταυτοχρόνως* $x = y$ και $x <_{\mathbb{R}} y$. Επιπροσθέτως, επειδή $x - y = 0_{\mathbb{R}} \Leftrightarrow y - x = 0_{\mathbb{R}}$, επαναλαμβάνοντας κατόπιν εναλλαγής των ρόλων των $(r_n)_{n\in\mathbb{N}}$ και $(s_n)_{n\in\mathbb{N}}$ την ίδια επιχειρηματολογία συμπεραίνουμε ότι είναι αδύνατον να ισχύει *ταυτοχρόνως* $x = y$ και $x >_{\mathbb{R}} y$. □

1.9.17 Πόρισμα. *Το σύνολο $\mathbb{R}$ των πραγματικών αριθμών γράφεται ως αποσυνδετή ένωση*

$$\boxed{\mathbb{R} = \mathbb{R}_{<0} \coprod \{0_{\mathbb{R}}\} \coprod \mathbb{R}_{>0}.}$$

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμοσθεί το θεώρημα 1.9.16 για το (x, y), όπου x τυχών πραγματικός αριθμός και $y = 0_{\mathbb{R}}$. □

1.9.18 Θεώρημα. *Η διμελής σχέση "$\leqslant_{\mathbb{R}}$" η ορισθείσα επί τού $\mathbb{R}$ στο εδάφιο 1.9.15 είναι σχέση ολικής διατάξεως.* (Βλ. 1.4.1.)

ΑΠΟΔΕΙΞΗ. Η ανακλαστικότητα τής "$\leqslant_{\mathbb{R}}$" είναι προφανής. Εάν $(x, y) \in \mathbb{R}\times\mathbb{R}$, όπου $x \leqslant_{\mathbb{R}} y$ και (ταυτοχρόνως) $y \leqslant_{\mathbb{R}} x$, και εάν υποθέσουμε ότι $x \neq y$, τότε $x <_{\mathbb{R}} y$ και (ταυτοχρόνως) $y <_{\mathbb{R}} x$, κάτι που είναι άτοπο επί τη βάσει τού νόμου τής τριχοτομίας 1.9.16. Κατ' ανάγκην λοιπόν $x = y$ και η "$\leqslant_{\mathbb{R}}$" είναι αντισυμμετρική.

Εν συνεχεία θεωρούμε $x = [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$, $y = [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$ και $u = [(t_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \in \mathbb{R}$, τέτοιους ώστε $x \leqslant_{\mathbb{R}} y$ και $y \leqslant_{\mathbb{R}} u$. Τότε

$$\text{είτε (i) } x = y \ \text{ είτε (i}') \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Q}_{>0} \text{ και } \exists n_1 = n_1(q) \in \mathbb{N} : \\ s_n - r_n >_{\mathbb{Q}} q_1, \ \forall \text{φυσικό } n \geqslant n_1 \end{array} \right\}$$

και

$$\text{είτε (ii) } y = u \ \text{ είτε (ii}'') \left\{ \begin{array}{l} \exists q_2 \in \mathbb{Q}_{>0} \text{ και } \exists n_2 = n_2(q) \in \mathbb{N} : \\ t_n - s_n >_{\mathbb{Q}} q_2, \ \forall \text{φυσικό } n \geqslant n_2. \end{array} \right\}$$

Εάν ισχύουν τα (i) και (ii), τότε προφανώς $x = u$. Εάν ισχύουν τα (i) και (ii″), τότε

$$\exists n_3 = n_3(\tfrac{q_2}{2}) \in \mathbb{N} : |s_n - r_n| <_{\mathbb{Q}} \tfrac{q_2}{2}, \text{ για κάθε φυσικό } n \geqslant n_3,$$

οπότε για κάθε φυσικό αριθμό $n \geqslant \max\{n_2, n_3\}$ έχουμε

$$\left.\begin{array}{l} s_n - r_n >_{\mathbb{Q}} -\frac{q_2}{2} \\ t_n - s_n >_{\mathbb{Q}} q_2 \end{array}\right\} \Longrightarrow t_n - r_n >_{\mathbb{Q}} \tfrac{q_2}{2} \Rightarrow x <_{\mathbb{R}} u.$$

Εάν ισχύουν τα (i′) και (ii), τότε

$$\exists n_4 = n_4(\tfrac{q_1}{2}) \in \mathbb{N} : |t_n - s_n| <_{\mathbb{Q}} \tfrac{q_1}{2}, \text{ για κάθε φυσικό } n \geqslant n_4,$$

οπότε για κάθε φυσικό αριθμό $n \geqslant \max\{n_1, n_4\}$ έχουμε

$$\left.\begin{array}{l} s_n - r_n >_{\mathbb{Q}} q_1 \\ t_n - s_n >_{\mathbb{Q}} -\frac{q_1}{2} \end{array}\right\} \Longrightarrow t_n - r_n >_{\mathbb{Q}} \tfrac{q_1}{2} \Rightarrow x <_{\mathbb{R}} u.$$

Εάν ισχύουν τα (i′) και (ii″), τότε για κάθε φυσικό αριθμό $n \geqslant \max\{n_1, n_2\}$ έχουμε

$$\left.\begin{array}{l} s_n - r_n >_{\mathbb{Q}} q_1 \\ t_n - s_n >_{\mathbb{Q}} q_2 \end{array}\right\} \Longrightarrow t_n - r_n >_{\mathbb{Q}} q_1 +_{\mathbb{Q}} q_2 \Rightarrow x <_{\mathbb{R}} u.$$

Άρα σε κάθε περίπτωση $x \leqslant_{\mathbb{R}} u$ και η "$\leqslant_{\mathbb{R}}$" είναι μεταβατική.

Απομένει να αποδειχθεί ότι τα στοιχεία τού $\mathbb{R}$ είναι μεταξύ τους ανά δύο συγκρίσιμα ως προς την "$\leqslant_{\mathbb{R}}$". Θεωρούμε λοιπόν τυχόντες $x, y \in \mathbb{R}$. Εάν $x = y$, τότε εξ ορισμού $x \leqslant_{\mathbb{R}} y$. Εάν $x \neq y$, τότε ο νόμος τής τριχοτομίας 1.9.16 επιτάσσει είτε την ισχύ τής ανισότητας $x <_{\mathbb{R}} y$ (οπότε $x \leqslant_{\mathbb{R}} y$) είτε την ισχύ τής ανισότητας $y <_{\mathbb{R}} x$ (οπότε $y \leqslant_{\mathbb{R}} x$). Κατά συνέπειαν, η "$\leqslant_{\mathbb{R}}$" αποτελεί μια σχέση ολικής διατάξεως επί τού $\mathbb{R}$. □

1.9.19 Πρόταση (Ιδιότητες διατάξεως). *Εάν $x, y, x', y', u \in \mathbb{R}$, τότε ισχύουν τα ακόλουθα*:

(i) *Εάν $x <_{\mathbb{R}} y$ και $y <_{\mathbb{R}} u$, τότε $y <_{\mathbb{R}} u$.*

(ii) $x <_{\mathbb{R}} y \Leftrightarrow -y <_{\mathbb{R}} -x$.

(iii) $0 <_{\mathbb{R}} x \Leftrightarrow -x <_{\mathbb{R}} 0_{\mathbb{R}}$.

(iv) $x <_{\mathbb{R}} y \Leftrightarrow x +_{\mathbb{R}} u <_{\mathbb{R}} y +_{\mathbb{R}} u$ *και*

$$[x <_{\mathbb{R}} y \text{ και } x' <_{\mathbb{R}} y'] \Rightarrow x +_{\mathbb{R}} x' <_{\mathbb{R}} y +_{\mathbb{R}} y'.$$

(v) *Εάν* $x, y \in \mathbb{R}_{>0}$, *τότε* $x +_{\mathbb{R}} y >_{\mathbb{R}} 0_{\mathbb{R}}$ *και* $x \cdot_{\mathbb{R}} y >_{\mathbb{R}} 0_{\mathbb{R}}$.
(vi) *Εάν* $x, y \in \mathbb{R}_{<0}$, *τότε* $x +_{\mathbb{R}} y <_{\mathbb{R}} 0_{\mathbb{R}}$ *και* $x \cdot_{\mathbb{R}} y >_{\mathbb{R}} 0_{\mathbb{R}}$.
(vii) *Εάν* $x \in \mathbb{R}_{<0}$ *και* $y \in \mathbb{R}_{>0}$, *τότε* $x \cdot_{\mathbb{R}} y <_{\mathbb{R}} 0_{\mathbb{R}}$.
(viii) *Εάν* $u \in \mathbb{R}_{>0}$, *τότε* $x <_{\mathbb{R}} y \Leftrightarrow (x \cdot_{\mathbb{R}} u) <_{\mathbb{R}} (y \cdot_{\mathbb{R}} u)$ *και*

$$[0_{\mathbb{R}} <_{\mathbb{R}} x <_{\mathbb{R}} y \text{ και } 0_{\mathbb{R}} <_{\mathbb{R}} x' <_{\mathbb{R}} y'] \Rightarrow (x \cdot_{\mathbb{R}} x') <_{\mathbb{R}} (y \cdot_{\mathbb{R}} y').$$

(ix) *Εάν* $u \in \mathbb{R}_{<0}$, *τότε* $x <_{\mathbb{R}} y \Leftrightarrow (x \cdot_{\mathbb{R}} u) >_{\mathbb{R}} (y \cdot_{\mathbb{R}} u)$.

ΑΠΟΔΕΙΞΗ. Το (i) αποδεικνύεται βάσει των προαναφερθέντων στην απόδειξη τού θεωρήματος 1.9.18 περί τής μεταβατικότητας τής "$\leqslant_{\mathbb{R}}$". Το (ii) είναι προφανές από τον ορισμό 1.9.15. Το (iii) έπεται άμεσα από το (ii).
(iv) Εάν $x = [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$, $y = [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$ και $u = [(t_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \in \mathbb{R}$, τότε

$$x <_{\mathbb{R}} y \Leftrightarrow \left\{ \begin{array}{l} \exists q \in \mathbb{Q}_{>0} \text{ και } \exists n_0 = n_0(q) \in \mathbb{N} : \\ s_n - r_n >_{\mathbb{Q}} q, \ \forall \text{φυσικό } n \geqslant n_0. \end{array} \right\}$$

$\Leftrightarrow x +_{\mathbb{R}} u <_{\mathbb{R}} y +_{\mathbb{R}} u$, διότι $s_n - r_n = (s_n +_{\mathbb{Q}} t_n) - (r_n +_{\mathbb{Q}} t_n)$. Επιπροσθέτως, εάν $x' = [(r'_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$, $y' = [(s'_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$ με $x <_{\mathbb{R}} y$ και $x' <_{\mathbb{R}} y'$, τότε

$$\left\{ \begin{array}{l} \exists q_1, q_2 \in \mathbb{Q}_{>0} \text{ και } \exists n_1 = n_1(q_1), n_2 = n_2(q_2) \in \mathbb{N} : \\ s_n - r_n >_{\mathbb{Q}} q_1, \ \forall \text{φυσικό } n \geqslant n_1 \text{ και } s'_n - r'_n >_{\mathbb{Q}} q_2, \ \forall \text{φυσικό } n \geqslant n_2 \end{array} \right\}.$$

Άρα για κάθε φυσικό αριθμό $n \geqslant \max\{n_1, n_2\}$ έχουμε

$$\left(s_n +_{\mathbb{Q}} s'_n\right) - \left(r_n +_{\mathbb{Q}} r'_n\right) >_{\mathbb{Q}} q_1 +_{\mathbb{Q}} q_2 \Rightarrow x +_{\mathbb{R}} x' <_{\mathbb{R}} y +_{\mathbb{R}} y'.$$

(v) Εάν $x = [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$, $y = [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \in \mathbb{R}_{>0}$, τότε $x +_{\mathbb{R}} y >_{\mathbb{R}} 0_{\mathbb{R}}$ κατά το (iv) και

$$\left\{ \begin{array}{l} \exists q_1, q_2 \in \mathbb{Q}_{>0} \text{ και } \exists n_1 = n_1(q_1), n_2 = n_2(q_2) \in \mathbb{N} : \\ r_n >_{\mathbb{Q}} q_1, \ \forall \text{φυσικό } n \geqslant n_1 \text{ και } s_n >_{\mathbb{Q}} q_2, \ \forall \text{φυσικό } n \geqslant n_2 \end{array} \right\}$$

Άρα για κάθε φυσικό αριθμό $n \geqslant \max\{n_1, n_2\}$ έχουμε (λόγω τού (viii) τής προτάσεως 1.8.21)

$$r_n >_{\mathbb{Q}} q_1 >_{\mathbb{Q}} 0_{\mathbb{Q}} \text{ και } s_n >_{\mathbb{Q}} q_2 >_{\mathbb{Q}} 0_{\mathbb{Q}} \Rightarrow (r_n \cdot_{\mathbb{Q}} s_n) >_{\mathbb{Q}} (q_1 \cdot_{\mathbb{Q}} q_2),$$

οπότε $x \cdot_{\mathbb{R}} y >_{\mathbb{R}} 0_{\mathbb{R}}$. Τα (vi) και (vii) αποδεικνύονται παρομοίως.
(viii) Εάν $x = [(r_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$, $y = [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \in \mathbb{R}$ και $u = [(t_n)_{n\in\mathbb{N}}]_{\mathrm{C}} \in \mathbb{R}_{>0}$, τότε

$$x <_{\mathbb{R}} y \Leftrightarrow \left\{ \begin{array}{l} \exists q \in \mathbb{Q}_{>0} \text{ και } \exists n_0 = n_0(q) \in \mathbb{N} : \\ s_n - r_n >_{\mathbb{Q}} q, \ \forall \text{φυσικό } n \geqslant n_0. \end{array} \right\}$$

$\Leftrightarrow (x \cdot_{\mathbb{R}} u) <_{\mathbb{R}} (y \cdot_{\mathbb{R}} u)$, διότι $(s_n - r_n) \cdot_{\mathbb{Q}} t_n = (s_n \cdot_{\mathbb{Q}} t_n) - (r_n \cdot_{\mathbb{Q}} t_n) >_{\mathbb{Q}} (q \cdot_{\mathbb{Q}} u)$ (βλ. 1.8.13 (vii) και 1.8.21 (viii)). Επιπροσθέτως, εάν $x' = [(r'_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$, $y' = [(s'_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$ με $x <_{\mathbb{R}} y$ και $x' <_{\mathbb{R}} y'$, τότε $(x \cdot_{\mathbb{R}} x') <_{\mathbb{R}} (y \cdot_{\mathbb{R}} x') = (x' \cdot_{\mathbb{R}} y) <_{\mathbb{R}} (x \cdot_{\mathbb{R}} x') <_{\mathbb{R}} (y \cdot_{\mathbb{R}} y')$. Το (ix) αποδεικνύεται παρομοίως. □

1.9.20 Παρατήρηση. Αξίζει να επισημανθεί ότι το σύνολο $\mathbb{R}_{>0}$ των *θετικών πραγματικών αριθμών* είναι κλειστό ως προς τις "$+_{\mathbb{R}}$" και "$\cdot_{\mathbb{R}}$" (βλ. 1.5.2 και 1.9.19 (v)), έχον το $0_{\mathbb{R}}$ ως το ουδέτερό του στοιχείο ως προς την "$+_{\mathbb{R}}$" και το $1_{\mathbb{R}}$ ως το ουδέτερό του στοιχείο ως προς την "$\cdot_{\mathbb{R}}$", καθώς και το ότι το σύνολο $\mathbb{R}\setminus\{0_{\mathbb{R}}\}$ των *μη μηδενικών πραγματικών αριθμών* είναι κλειστό ως προς την "$\cdot_{\mathbb{R}}$" έχον το $1_{\mathbb{R}}$ ως ουδέτερό του στοιχείο.

1.9.21 Ορισμός. Θεωρούμε την απεικόνιση

$$\boxed{\iota_{\mathbb{Q}} : \mathbb{Q} \longrightarrow \mathbb{R},\ \ r \longmapsto \iota_{\mathbb{Q}}(r) := [(r)_{n\in\mathbb{N}}]_{\mathrm{C}}}$$

(βλ. 1.8.38 (ii)). Η $\iota_{\mathbb{Q}}$ καλείται **φυσική εμφύτευση τού $\mathbb{Q}$ εντός τού $\mathbb{R}$**. Οι κύριες ιδιότητές της παρατίθενται στην επόμενη πρόταση.

1.9.22 Πρόταση. (i) *Η $\iota_{\mathbb{Q}}$ είναι ενριπτική.*
(ii) $\iota_{\mathbb{Q}}(r +_{\mathbb{Q}} s) = \iota_{\mathbb{Q}}(r) +_{\mathbb{R}} \iota_{\mathbb{Q}}(s)\,,\ \forall\,(r,s) \in \mathbb{Q}\times\mathbb{Q}$.
(iii) $\iota_{\mathbb{Q}}(r \cdot_{\mathbb{Q}} s) = \iota_{\mathbb{Q}}(r) \cdot_{\mathbb{R}} \iota_{\mathbb{Q}}(s)\,,\ \forall\,(r,s) \in \mathbb{Q}\times\mathbb{Q}$.
(iv) *Για οιουσδήποτε $r, s \in \mathbb{Q}$ ισχύει η αμφίπλευρη συνεπαγωγή*

$$r \leqslant_{\mathbb{Q}} s \iff \iota_{\mathbb{Q}}(r) \leqslant_{\mathbb{R}} \iota_{\mathbb{Q}}(s)\,.$$

(v) $\iota_{\mathbb{Q}}(0_{\mathbb{Q}}) = 0_{\mathbb{R}}$ *και* $\iota_{\mathbb{Q}}(1_{\mathbb{Q}}) = 1_{\mathbb{R}}$.

Απόδειξη. (i) Εάν $r, s \in \mathbb{Q}$ με $\iota_{\mathbb{Q}}(r) = \iota_{\mathbb{Q}}(s)$, τότε $[(r)_{n\in\mathbb{N}}]_{\mathrm{C}} = [(s)_{n\in\mathbb{N}}]_{\mathrm{C}}$, οπότε *για κάθε* $\varepsilon \in \mathbb{Q}_{>0}$ ισχύει $|s-r| <_{\mathbb{Q}} \varepsilon$, απ' όπου έπεται ότι $r = s$ (διότι εάν $|s-r| >_{\mathbb{Q}} 0_{\mathbb{Q}}$, τότε θα καταλήγαμε σε άτοπο θέτοντας, π.χ., $\varepsilon := \frac{|s-r|}{2}$). Άρα η $\iota_{\mathbb{Q}}$ είναι όντως ενριπτική.
(ii) Προφανώς, για οιοδήποτε $(r,s) \in \mathbb{Q}\times\mathbb{Q}$ λαμβάνουμε

$$\iota_{\mathbb{Q}}(r) +_{\mathbb{R}} \iota_{\mathbb{Q}}(s) = [(r)_{n\in\mathbb{N}}]_{\mathrm{C}} +_{\mathbb{R}} [(s)_{n\in\mathbb{N}}]_{\mathrm{C}} = [(r +_{\mathbb{Q}} s)_{n\in\mathbb{N}}]_{\mathrm{C}} = \iota_{\mathbb{Q}}(r +_{\mathbb{Q}} s)\,.$$

(iii) Κατ' αναλογίαν, για οιοδήποτε $(r,s) \in \mathbb{Q}\times\mathbb{Q}$ λαμβάνουμε

$$\iota_{\mathbb{Q}}(r) \cdot_{\mathbb{R}} \iota_{\mathbb{Q}}(s) = [(r)_{n\in\mathbb{N}}]_{\mathrm{C}} \cdot_{\mathbb{R}} [(s)_{n\in\mathbb{N}}]_{\mathrm{C}} = [(r \cdot_{\mathbb{Q}} s)_{n\in\mathbb{N}}]_{\mathrm{C}} = \iota_{\mathbb{Q}}(r \cdot_{\mathbb{Q}} s)\,.$$

(iv) Για οιουσδήποτε $r, s \in \mathbb{Q}$ ισχύουν οι αμφίπλευρες συνεπαγωγές

$$\begin{aligned} \iota_{\mathbb{Q}}(r) \quad &\leqslant \quad {}_{\mathbb{R}}\iota_{\mathbb{Q}}(s) \Leftrightarrow [(r)_{n\in\mathbb{N}}]_{\mathrm{C}} \leqslant_{\mathbb{R}} [(s)_{n\in\mathbb{N}}]_{\mathrm{C}} \\ &\Leftrightarrow \quad \text{είτε } r = s \ \text{ είτε } \{\exists q \in \mathbb{Q} : s - r >_{\mathbb{Q}} q >_{\mathbb{Q}} 0_{\mathbb{Q}}\} \\ &\Leftrightarrow \quad r \leqslant_{\mathbb{Q}} s. \end{aligned}$$

(v) Προφανώς, $\iota_{\mathbb{Q}}(0_{\mathbb{Q}}) = [(0_{\mathbb{Q}})_{n\in\mathbb{N}}]_{\mathrm{C}} = 0_{\mathbb{R}}$ και $\iota_{\mathbb{Q}}(1_{\mathbb{Q}}) = [(1_{\mathbb{Q}})_{n\in\mathbb{N}}]_{\mathrm{C}} = 1_{\mathbb{R}}$. □

1.9.23 Σημείωση (Οι συνήθεις «ταυτίσεις»). Εάν περιορίσουμε το πεδίο τιμών τής $\iota_{\mathbb{Q}}$ στην εικόνα της, τότε η προκύπτουσα απεικόνιση είναι μια *αμφίρριψη* έχουσα την

$$\mathrm{Im}(\iota_{\mathbb{Q}}) \ni [(r)_{n\in\mathbb{N}}]_{\mathrm{C}} \longmapsto r \in \mathbb{Q}$$

ως αντίστροφό της. Ως εκ τούτου, είθισται να *ταυτίζουμε* την εικόνα $\iota_{\mathbb{Q}}(r)$ οιουδήποτε ρητού αριθμού r μέσω τής $\iota_{\mathbb{Q}}$ *με τον ίδιο τον* r. Επιπροσθέτως, λόγω των 1.9.22 (ii) και (iii), για οιουσδήποτε $r, s \in \mathbb{Q}$ *ταυτίζουμε* το $\iota_{\mathbb{Q}}(r) +_{\mathbb{R}} \iota_{\mathbb{Q}}(s)$ με το $r +_{\mathbb{Q}} s$ και το $\iota_{\mathbb{Q}}(r) \cdot_{\mathbb{R}} \iota_{\mathbb{Q}}(s)$ με το $r \cdot_{\mathbb{Q}} s$ (ήτοι τους περιορισμούς των πράξεων "$+_{\mathbb{R}}$" και "$\cdot_{\mathbb{R}}$" επί τής $\mathrm{Im}(\iota_{\mathbb{Q}})$ με τις πράξεις "$+_{\mathbb{Q}}$" και "$\cdot_{\mathbb{Q}}$", αντιστοίχως). Κατ' αναλογίαν, λόγω των 1.9.22 (iv) και (v) *ταυτίζουμε* την "$\leqslant_{\mathbb{R}}|_{\mathrm{Im}(\iota_{\mathbb{Q}})}$" με τη σχέση διατάξεως "$\leqslant_{\mathbb{Q}}$", το $0_{\mathbb{R}}$ με το $0_{\mathbb{Q}}$ και το $1_{\mathbb{R}}$ με το $1_{\mathbb{Q}}$ (που το έχουμε ήδη ταυτίσει με το $1_{\mathbb{Z}}$ μέσω τής $\iota_{\mathbb{Z}}$ και με το $1 \in \mathbb{N}$ μέσω τής $\iota_{\mathbb{N}}$ στα εδάφια 1.8.25 και 1.7.24, αντιστοίχως). Κάθε πραγματικός αριθμός που ανήκει στο σύνολο $\mathbb{R}\smallsetminus\mathrm{Im}(\iota_{\mathbb{Q}})$ καλείται **άρρητος αριθμός**.

1.9.24 Θεώρημα (Το $\mathbb{Q}$ είναι «πυκνό» υποσύνολο τού συνόλου $\mathbb{R}$). *Για οιουσδήποτε πραγματικούς αριθμούς x, y με $x <_{\mathbb{R}} y$ υπάρχει $r \in \mathbb{Q}$, ούτως ώστε*

$$x <_{\mathbb{R}} r <_{\mathbb{R}} y$$

(όπου ο r ταυτίζεται, όπως προαναφέραμε, με την $\iota_{\mathbb{Q}}(r) := [(r)_{n\in\mathbb{N}}]_{\mathrm{C}}$).

Απόδειξη. Έστω $x = [(s_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$ και έστω $y = [(t_n)_{n\in\mathbb{N}}]_{\mathrm{C}}$ με $x <_{\mathbb{R}} y$. Τότε

$$\exists q \in \mathbb{Q}_{>0} \text{ και } \exists n_1 = n_1(q) \in \mathbb{N} : t_n - s_n >_{\mathbb{Q}} q, \ \forall \text{φυσικό } n \geqslant n_1.$$

Επειδή οι $(s_n)_{n\in\mathbb{N}}$ και $(t_n)_{n\in\mathbb{N}}$ είναι ακολουθίες Cauchy ρητών αριθμών, υπάρχουν δείκτες $n_2 = n_2(\frac{q}{3}) \in \mathbb{N}$ και $n_3 = n_3(\frac{q}{3}) \in \mathbb{N}$, ούτως ώστε να ισχύει

$$|s_m - s_n| <_{\mathbb{Q}} \tfrac{q}{3}, \text{ για οιουσδήποτε φυσικούς αριθμούς } m, n \geqslant n_2.$$

και

$$|t_m - t_n| <_{\mathbb{Q}} \tfrac{q}{3}, \text{ για οιουσδήποτε φυσικούς αριθμούς } m, n \geqslant n_3.$$

Έστω $n_0 := \max\{n_1, n_2, n_3\}$. Τότε για κάθε φυσικό αριθμό $n \geqslant n_0$ ισχύουν ταυτοχρόνως οι σχέσεις

$$|s_n - s_{n_0}| <_{\mathbb{Q}} \tfrac{q}{3}, \quad |t_n - t_{n_0}| <_{\mathbb{Q}} \tfrac{q}{3}, \quad t_n - s_n >_{\mathbb{Q}} q$$

$$\Longrightarrow s_{n_0} - \tfrac{q}{3} <_{\mathbb{Q}} s_n <_{\mathbb{Q}} s_{n_0} +_{\mathbb{Q}} \tfrac{q}{3}, \quad t_{n_0} - \tfrac{q}{3} <_{\mathbb{Q}} t_n <_{\mathbb{Q}} t_{n_0} +_{\mathbb{Q}} \tfrac{q}{3}, \quad t_n - s_n >_{\mathbb{Q}} q,$$

οπότε θέτοντας $r := \frac{s_{n_0} +_{\mathbb{Q}} t_{n_0}}{2}$ λαμβάνουμε

$$r - s_n = \frac{(t_{n_0} - s_n) +_{\mathbb{Q}} (s_{n_0} - s_n)}{2} >_{\mathbb{Q}} \frac{\left(t_{n_0} - s_{n_0} - \frac{q}{3}\right) - \frac{q}{3}}{2} >_{\mathbb{Q}} \frac{\left(q - \frac{q}{3}\right) - \frac{q}{3}}{2} = \frac{q}{6}$$

και

$$t_n - r = \frac{(t_n - t_{n_0}) +_{\mathbb{Q}} (t_n - s_{n_0})}{2} >_{\mathbb{Q}} \frac{-\frac{q}{3} +_{\mathbb{Q}} \left(t_{n_0} - \frac{q}{3} - s_{n_0}\right)}{2} >_{\mathbb{Q}} \frac{-\frac{q}{3} +_{\mathbb{Q}} \left(-\frac{q}{3} +_{\mathbb{Q}} q\right)}{2} = \frac{q}{6}.$$

Επομένως, $x <_{\mathbb{R}} r$ και $r <_{\mathbb{R}} y$. □

1.9.25 Πρόταση (Αρχιμήδεια ιδιότητα). *Για οιουσδήποτε πραγματικούς αριθμούς x, y με $y \geqslant_{\mathbb{R}} x >_{\mathbb{R}} 0_{\mathbb{R}}$ υπάρχει κάποιος $k \in \mathbb{N}$, ούτως ώστε να ισχύει η ανισότητα*

$$k \cdot_{\mathbb{R}} x >_{\mathbb{R}} y$$

(όπου ο k ταυτίζεται, όπως προαναφέραμε, με την $\iota_{\mathbb{Q}}(k) := [(k)_{n\in\mathbb{N}}]_{\mathrm{C}}$).

Απόδειξη. Σύμφωνα με το θεώρημα 1.9.24,

$$\exists r \in \mathbb{Q} : 0_{\mathbb{R}} <_{\mathbb{R}} r <_{\mathbb{R}} x \text{ και } \exists s \in \mathbb{Q} : x \leqslant_{\mathbb{R}} y <_{\mathbb{R}} s <_{\mathbb{R}} y +_{\mathbb{R}} 1_{\mathbb{R}}.$$

Επειδή $r, s \in \mathbb{Q}$ και $r <_{\mathbb{R}} s$, η αρχιμήδεια ιδιότητα η ισχύουσα στο $\mathbb{Q}$ (βλ. πρόταση 1.8.26) μας διασφαλίζει την ύπαρξη ενός $k \in \mathbb{N}$, ούτως ώστε να ισχύει η ανισότητα $k \cdot_{\mathbb{Q}} r >_{\mathbb{Q}} s$. Κατά συνέπειαν, λαμβάνοντας υπ' όψιν τις «ταυτίσεις» τις θεσπισθείσες στο εδάφιο 1.9.23 και το (viii) τής προτάσεως 1.9.19, διαπιστώνουμε ότι

$$(k \cdot_{\mathbb{R}} x) >_{\mathbb{R}} (k \cdot_{\mathbb{R}} r) >_{\mathbb{R}} s >_{\mathbb{R}} y,$$

οπότε η απόδειξη λήγει εδώ. □

1.10 ΜΙΓΑΔΙΚΟΙ ΑΡΙΘΜΟΙ

Εάν a είναι ένας *αρνητικός* πραγματικός αριθμός, τότε η εξίσωση

$$\boxed{x^2 = a} \tag{1.68}$$

(με *άγνωστό της* τον x) δεν διαθέτει καμία λύση εντός τού $\mathbb{R}$ (διότι το τετράγωνο ενός πραγματικού αριθμού είναι πάντοτε ένας *μη αρνητικός* πραγματικός αριθμός). Η αναζήτηση ενός σύνολου «ευρύτερου» τού $\mathbb{R}$, τέτοιου ώστε εξισώσεις όπως η (1.68) να έχουν πάντοτε λύσεις εντός αυτού, μας οδηγεί στον ορισμό τού $\mathbb{C}$. Το **σύνολο** $\mathbb{C}$ **των μιγαδικών αριθμών** μπορεί να εκληφθεί ως το $\mathbb{R}^2 := \mathbb{R} \times \mathbb{R}$, εφοδιασμένο με δύο εσωτερικές πράξεις "$+_{\mathbb{R}^2}$" και "$\cdot_{\mathbb{R}^2}$" που ορίζονται μέσω των τύπων

$$\boxed{(x,y) +_{\mathbb{R}^2} (u,v) \quad := \quad (x +_{\mathbb{R}} u, y +_{\mathbb{R}} v)} \tag{1.69}$$

και

$$\boxed{(x,y) \cdot_{\mathbb{R}^2} (u,v) \quad := \quad ((x \cdot_{\mathbb{R}} u) +_{\mathbb{R}} (-(y \cdot_{\mathbb{R}} v)), (x \cdot_{\mathbb{R}} v) +_{\mathbb{R}} (y \cdot_{\mathbb{R}} u)),} \tag{1.70}$$

αντιστοίχως, για οιαδήποτε διατεταγμένα ζεύγη $(x,y)\,, (u,v) \in \mathbb{R}^2$. Ταυτίζοντας το $\mathbb{R}$ με την εικόνα του μέσω τής **φυσικής εμφυτεύσεως**

$$\boxed{\iota_{\mathbb{R}} : \mathbb{R} \hookrightarrow \mathbb{C}, \;\; x \longmapsto \iota_{\mathbb{R}}(x) := (x, 0_{\mathbb{R}})}$$

παρατηρούμε ότι

$$\iota_{\mathbb{R}}(x +_{\mathbb{R}} y) = \iota_{\mathbb{R}}(x) +_{\mathbb{R}^2} \iota_{\mathbb{R}}(y), \;\; \iota_{\mathbb{R}}(x \cdot_{\mathbb{R}} y) = \iota_{\mathbb{R}}(x) \cdot_{\mathbb{R}^2} \iota_{\mathbb{R}}(y).$$

Εξάλλου, επειδή

$$(0_{\mathbb{R}}, 1_{\mathbb{R}}) \cdot_{\mathbb{R}^2} (0_{\mathbb{R}}, 1_{\mathbb{R}}) \quad := \quad ((0_{\mathbb{R}} \cdot_{\mathbb{R}} 0_{\mathbb{R}}) +_{\mathbb{R}} (-(1_{\mathbb{R}} \cdot_{\mathbb{R}} 1_{\mathbb{R}})), (0_{\mathbb{R}} \cdot_{\mathbb{R}} 1_{\mathbb{R}}) +_{\mathbb{R}} (1_{\mathbb{R}} \cdot_{\mathbb{R}} 0_{\mathbb{R}})) = (-1_{\mathbb{R}}, 0_{\mathbb{R}}),$$

ταυτίζοντας το $\iota_{\mathbb{R}}(-1_{\mathbb{R}}) := (-1_{\mathbb{R}}, 0_{\mathbb{R}})$ με το $-1_{\mathbb{R}}$ και θέτοντας $i := (0_{\mathbb{R}}, 1_{\mathbb{R}})\,$, λαμβάνουμε

$$\boxed{i^2 = -1_{\mathbb{R}}.}$$

Αυτό το i καλείται **φανταστική μονάδα**, αποτελεί μια λύση τής (1.68) όταν $a = -1_{\mathbb{R}}$ και μέσω αυτής μπορούμε να εκφράσουμε κάθε στοιχείο $(x,y) \in \mathbb{C}$ υπό τη μορφή

$$\begin{aligned}
&(x,y) = (x, 0_{\mathbb{R}}) +_{\mathbb{R}^2} (0_{\mathbb{R}} y) = \\
&= (x, 0_{\mathbb{R}}) +_{\mathbb{R}^2} ((0_{\mathbb{R}} \cdot_{\mathbb{R}} y) +_{\mathbb{R}} (-(1_{\mathbb{R}} \cdot_{\mathbb{R}} 0_{\mathbb{R}})), (0_{\mathbb{R}} \cdot_{\mathbb{R}} 0_{\mathbb{R}}) +_{\mathbb{R}} (1_{\mathbb{R}} \cdot_{\mathbb{R}} y)) \\
&= (x, 0_{\mathbb{R}}) +_{\mathbb{R}^2} ((0_{\mathbb{R}}, 1_{\mathbb{R}}) \cdot_{\mathbb{R}} (y, 0_{\mathbb{R}})) = \text{“}x + iy\text{”},
\end{aligned}$$

όπου ο **μιγαδικός αριθμός** $z = x + iy$ έχει τον x **ως πραγματικό του** και τον y **ως φανταστικό του μέρος**[49]. Έτσι, αντί των (1.69) και (1.70) έχουμε τη δυνατότητα να γράψουμε

$$\boxed{(x + iy) +_{\mathbb{C}} (u + iv) \quad := \quad (x +_{\mathbb{R}} u) + i(y +_{\mathbb{R}} v)\,,} \tag{1.71}$$

και

$$\boxed{(x + iy) \cdot_{\mathbb{C}} (u + iv) \quad := \quad (x \cdot_{\mathbb{R}} u) +_{\mathbb{R}} (-(y \cdot_{\mathbb{R}} v)) + i((x \cdot_{\mathbb{R}} v) +_{\mathbb{R}} (y \cdot_{\mathbb{R}} u)).} \tag{1.72}$$

Οι αποδείξεις των προτάσεων 1.10.1, 1.10.2, 1.10.4 και 1.10.6 αφήνονται ως ασκήσεις.

[49] Προφανώς, $x + iy = x' + iy' \Leftrightarrow [x = x' \text{ και } y = y']$.

1.10.1 Πρόταση (Ιδιότητες προσθέσεως). *Η πρόσθεση μιγαδικών αριθμών έχει τις εξής ιδιότητες*:

(i) **[Μεταθετική ιδιότητα]** *Για* $(x,y),(u,v)\in\mathbb{R}^2$ *ισχύει η ισότητα*

$$(x+iy)+_{\mathbb{C}}(u+iv)=(u+iv)+_{\mathbb{C}}(x+iy).$$

(ii) **[Προσεταιριστική ιδιότητα]** *Για* $(x,y),(u,v),(s,t)\in\mathbb{R}^2$ *ισχύει η ισότητα*

$$((x+iy)+_{\mathbb{C}}(u+iv))+_{\mathbb{C}}(s+it)=(x+iy)+_{\mathbb{C}}((u+iv)+_{\mathbb{C}}(s+it)).$$

(iii) **[Νόμος τής διαγραφής]** *Για* $(x,y),(x',y'),(u,v)\in\mathbb{R}^2$ *ισχύει η συνεπαγωγή*

$$(x+iy)+_{\mathbb{C}}(u+iv)=(x'+iy')+_{\mathbb{C}}(u+iv)\Longrightarrow x+iy=x'+iy'.$$

(iv) **[Ύπαρξη ουδετέρου στοιχείου]** *Το* $0_{\mathbb{C}}:=0_{\mathbb{R}}+i0_{\mathbb{R}}$ *είναι ουδέτερο στοιχείο τού* $\mathbb{C}$ *ως προς την* "$+_{\mathbb{C}}$" (βλ. 1.5.6), *δηλαδή*

$$0_{\mathbb{C}}+_{\mathbb{C}}z=z=z+_{\mathbb{C}}0_{\mathbb{C}},\ \ \forall z\in\mathbb{C}.$$

(v) **[Ύπαρξη συμμετρικού στοιχείου]** *Κάθε* $z=x+iy\in\mathbb{C}$ *έχει τον αντίθετό του* $-z:=(-x)+i(-y)\in\mathbb{C}$ *ως συμμετρικό του στοιχείο ως προς την* "$+_{\mathbb{C}}$" (βλ. 1.5.11), *δηλαδή*

$$(-z)+_{\mathbb{C}}z=0_{\mathbb{C}}=z+_{\mathbb{C}}(-z).$$

1.10.2 Πρόταση (Ιδιότητες πολλαπλασιασμού). *Ο πολλαπλασιασμός μιγαδικών αριθμών έχει τις εξής ιδιότητες*:

(i) **[Μεταθετική ιδιότητα]** $z\cdot_{\mathbb{C}}w=w\cdot_{\mathbb{C}}z,\forall(z,w)\in\mathbb{C}\times\mathbb{C}$.

(ii) **[Προσεταιριστική ιδιότητα]** *Για οιουσδήποτε* $z_1,z_2,z_3\in\mathbb{C}$ *ισχύει η ισότητα*

$$(z_1\cdot_{\mathbb{C}}z_2)\cdot_{\mathbb{C}}z_3=z_1\cdot_{\mathbb{C}}(z_2\cdot_{\mathbb{C}}z_3).$$

(iii) *Για οιονδήποτε* $z\in\mathbb{C}$ *ισχύουν οι ισότητες*

$$0_{\mathbb{C}}\cdot_{\mathbb{C}}z=0_{\mathbb{C}}=z\cdot_{\mathbb{C}}0_{\mathbb{C}}.$$

(iv) **[Ύπαρξη ουδετέρου στοιχείου]** *Το* $1_{\mathbb{C}}:=1_{\mathbb{R}}+i0_{\mathbb{R}}$ *είναι ουδέτερο στοιχείο τού* $\mathbb{C}$ *ως προς την* "$\cdot_{\mathbb{C}}$" (βλ. 1.5.6), *δηλαδή*

$$1_{\mathbb{C}}\cdot_{\mathbb{C}}z=z=z\cdot_{\mathbb{C}}1_{\mathbb{C}},\ \forall z\in\mathbb{C}.$$

(v) **[Ύπαρξη συμμετρικού στοιχείου για** $z\neq0_{\mathbb{C}}$**]** *Κάθε* $z=x+iy\in\mathbb{C}\setminus\{0_{\mathbb{C}}\}$ *έχει τον αντίστροφό του*

$$z^{-1}:=\tfrac{x}{x^2+y^2}+i\tfrac{(-y)}{x^2+y^2}$$

ως συμμετρικό του στοιχείο ως προς την "$\cdot_{\mathbb{C}}$" (βλ. 1.5.11), *δηλαδή*

$$z^{-1}\cdot_{\mathbb{C}}z=1_{\mathbb{C}}=z\cdot_{\mathbb{C}}z^{-1}.$$

(vi) *Για οιουσδήποτε* $z,w\in\mathbb{C}$ *ισχύουν οι ισότητες*

$$(-z)\cdot_{\mathbb{C}}w=-(z\cdot_{\mathbb{C}}w)=z\cdot_{\mathbb{C}}(-w),\ \ (-z)\cdot_{\mathbb{C}}(-w)=z\cdot_{\mathbb{C}}w.$$

(vii) **[Επιμεριστική ιδιότητα τού πολλαπλασιασμού ως προς την πρόσθεση]** *Για οιουσδήποτε* $z_1, z_2, z_3 \in \mathbb{C}$ *ισχύουν οι ισότητες*

$$z_1 \cdot_{\mathbb{C}} (z_2 +_{\mathbb{C}} z_3) = (z_1 \cdot_{\mathbb{C}} z_2) +_{\mathbb{C}} (z_1 \cdot_{\mathbb{C}} z_3)\,,$$
$$(z_1 +_{\mathbb{C}} z_2) \cdot_{\mathbb{C}} z_3 = (z_1 \cdot_{\mathbb{C}} z_3) +_{\mathbb{C}} (z_2 \cdot_{\mathbb{C}} z_3)\,.$$

(viii) *Εάν* $z, w \in \mathbb{C}$ *με* $z \cdot_{\mathbb{C}} w = 0_{\mathbb{C}}$, *τότε είτε* $z = 0_{\mathbb{C}}$ *είτε* $w = 0_{\mathbb{C}}$.

(ix) **[Νόμος τής διαγραφής]** *Για* $z, z', w \in \mathbb{C}$ *με* $w \neq 0_{\mathbb{C}}$ *ισχύει η συνεπαγωγή*

$$z \cdot_{\mathbb{C}} w = z' \cdot_{\mathbb{C}} w \Longrightarrow z = z'.$$

1.10.3 Ορισμός. Εάν $z = x + iy \in \mathbb{C}$, τότε ως **συζυγής τού** z ορίζεται να είναι ο μιγαδικός αριθμός:

$$\overline{z} := x - iy.$$

1.10.4 Πρόταση (Ιδιότητες συζυγών). *Για* $z_1, z_2 \in \mathbb{C}$ *και* $z \in \mathbb{C} \setminus \{0_{\mathbb{C}}\}$ *ισχύουν τα εξής*:

(i) $\overline{z_1 +_{\mathbb{C}} z_2} = \overline{z_1} +_{\mathbb{C}} \overline{z_2}$.

(ii) $\overline{z_1 \cdot_{\mathbb{C}} z_2} = \overline{z_1} \cdot_{\mathbb{C}} \overline{z_2}$.

(iii) $\overline{z^{-1}} = (\overline{z})^{-1}$.

1.10.5 Ορισμός. Εάν $z = x + iy \in \mathbb{C}$, τότε ως **απόλυτη τιμή τού** z ορίζεται να είναι ο πραγματικός αριθμός:

$$|z| := \sqrt{x^2 + y^2}.$$

1.10.6 Πρόταση (Ιδιότητες απόλυτης τιμής). *Για* $z, z_1, z_2 \in \mathbb{C}$ *ισχύουν τα εξής*:

(i) $|z| \geqslant_{\mathbb{R}} 0_{\mathbb{R}}$ *και* $|z| = 0_{\mathbb{R}} \Leftrightarrow z = 0_{\mathbb{C}}$.

(ii) $|z_1 \cdot_{\mathbb{C}} z_2| = |z_1| \cdot_{\mathbb{R}} |z_2|$.

(iii) $||z_1| +_{\mathbb{R}} (-|z_2|)| \leqslant |z_1 +_{\mathbb{C}} z_2| \leqslant |z_1| +_{\mathbb{R}} |z_2|$.

(iv) *Εάν* $z \in \mathbb{C} \setminus \{0_{\mathbb{C}}\}$, *τότε* $\left|z^{-1}\right| = |z|^{-1}$.

(v) $|z|^2 = z \cdot_{\mathbb{C}} \overline{z}$.

1.10.7 Παρατήρηση («Απλούστευση συμβολισμών»). Κατά την προηγηθείσα δόμηση των αριθμητικών συνόλων[50]

$$\mathbb{N} \underset{\iota_{\mathbb{N}}}{\hookrightarrow} \mathbb{Z} \underset{\iota_{\mathbb{Z}}}{\hookrightarrow} \mathbb{Q} \underset{\iota_{\mathbb{Q}}}{\hookrightarrow} \mathbb{R} \underset{\iota_{\mathbb{R}}}{\hookrightarrow} \mathbb{C}$$

η πρόσθεση "$+_{\mathbb{C}}$" και ο πολλαπλασιασμός "$\cdot_{\mathbb{C}}$" επί τού $\mathbb{C}$ αποτελεί (φυσική) επέκταση των αντιστοίχων πράξεων επί τού $\mathbb{R}$, η πρόσθεση "$+_{\mathbb{R}}$" και ο πολλαπλασιασμός "$\cdot_{\mathbb{R}}$" επί τού $\mathbb{R}$ αποτελεί επέκταση των αντιστοίχων πράξεων επί τού $\mathbb{Q}$, η πρόσθεση "$+_{\mathbb{Q}}$" και ο πολλαπλασιασμός "$\cdot_{\mathbb{Q}}$" επί τού $\mathbb{Q}$ αποτελεί επέκταση των αντιστοίχων πράξεων επί τού $\mathbb{Z}$, και η πρόσθεση "$+_{\mathbb{Z}}$" και ο πολλαπλασιασμός "$\cdot_{\mathbb{Z}}$" επί τού $\mathbb{Z}$ αποτελεί επέκταση των αντιστοίχων πράξεων επί τού $\mathbb{N}$. Γι' αυτόν τον λόγο μπορούμε εφεξής να *εξαπλουστεύουμε* αυτές τις **συνήθεις πράξεις** γράφοντας "$+$" και "$\cdot$", παραλείποντας τους υποδείκτες. (Κατ' αναλογίαν, επειδή η "$\leqslant_{\mathbb{R}}$" είναι φυσική επέκταση τής "$\leqslant_{\mathbb{Q}}$", η "$\leqslant_{\mathbb{Q}}$" τής "$\leqslant_{\mathbb{Z}}$" και η "$\leqslant_{\mathbb{Z}}$" τής "$\leqslant_{\mathbb{N}}$", μπορούμε εφεξής να γράφουμε απλώς "$\leqslant$".)

[50] Στις διαδοχικές αυτές επεκτάσεις θα προστεθεί άλλη μία στο εδ. 8.1.21.

1.11 ΓΕΝΙΚΕΥΜΕΝΑ ΚΑΡΤΕΣΙΑΝΑ ΓΙΝΟΜΕΝΑ ΚΑΙ ΤΟ ΑΞΙΩΜΑ ΤΗΣ ΕΠΙΛΟΓΗΣ

1.11.1 Ορισμός. Έστω ότι ο n είναι ένας φυσικός αριθμός και ότι τα $A_1, A_2, \ldots, A_n$ είναι τυχόντα σύνολα. Τότε το **καρτεσιανό γινόμενο** αυτών των συνόλων, κατ' αναλογίαν προς την περίπτωση όπου $n = 2$ (βλ. 1.1.11), ορίζεται μέσω *διατεταγμένων*[51] n*-άδων* ως εξής:

$$\mathsf{X}_{i=1}^{n} A_i := \{ (x_1, x_2, \ldots, x_n) \mid x_i \in A_i, \forall i \in \{1, 2, \ldots, n\} \} \tag{1.73}$$

(Στην ειδική περίπτωση όπου $A_1 = \cdots = A_n = A$, γράφουμε A^n αντί τού $\mathsf{X}_{i=1}^{n} A_i$.)

1.11.2 Σημείωση. Το καρτεσιανό γινόμενο (1.73) n συνόλων $A_1, \ldots, A_n$ εισήχθη με τη βοήθεια διατεταγμένων n-άδων. Στο σημείο αυτό παραθέτουμε μια διαφορετική (αλλά λίαν χρήσιμη) θεωρητική πρόσβαση στην έννοια τού καρτεσιανού γινομένου. Δοθέντων n συνόλων $A_1, \ldots, A_n$ (όπου $n \in \mathbb{N}$) υποθέτουμε ότι

$$(x_1, \ldots, x_n) \in \mathsf{X}_{i=1}^{n} A_i, \quad (y_1, \ldots, y_n) \in \mathsf{X}_{i=1}^{n} A_i.$$

Ορίζοντας τις απεικονίσεις

$$f : \{1, 2, \ldots, n\} \longrightarrow \bigcup_{i=1}^{n} A_i$$

και

$$g : \{1, 2, \ldots, n\} \longrightarrow \bigcup_{i=1}^{n} A_i,$$

όπου

$$f(i) = x_i, \quad g(i) = y_i, \quad \forall i \in \{1, 2, \ldots, n\},$$

λαμβάνουμε

$$f(i) \in A_i, \quad g(i) \in A_i, \quad \forall i \in \{1, 2, \ldots, n\},$$

και

$$x_i = y_i \Longleftrightarrow f(i) = g(i), \quad \forall i \in \{1, 2, \ldots, n\} \tag{1.74}$$

Και αντιστρόφως· εάν διατίθενται απεικονίσεις

$$f : \{1, 2, \ldots, n\} \longrightarrow \bigcup_{i=1}^{n} A_i, \quad g : \{1, 2, \ldots, n\} \longrightarrow \bigcup_{i=1}^{n} A_i,$$

τότε, θέτοντας $x_i := f(i)$ και $y_i := g(i)$, ορίζονται n-άδες $(x_1, \ldots, x_n)$ και $(y_1, \ldots, y_n)$ που ικανοποιούν την (1.74). Εξ αυτού καθίσταται σαφές ότι θα μπορούσαμε εξαρχής να είχαμε ορίσει διατεταγμένες n-άδες *με τη βοήθεια απεικονίσεων*. Ως εκ τούτου, ορίζοντας το σύνολο

$$\prod_{i=1}^{n} A_i := \left\{ f \;\middle|\; f : \{1, .., n\} \longrightarrow \bigcup_{i=1}^{n} A_i \text{ απεικονίσεις με } f(i) \in A_i, \forall i \in \{1, .., n\} \right\}$$

[51] Η ύπαρξη διατεταγμένων ζευγών αρκεί για τον ορισμό *διατεταγμένων n-άδων* (μέσω μαθηματικής επαγωγής ως προς το n).

διαπιστώνουμε την ύπαρξη δύο απεικονίσεων

$$\begin{array}{ccc} \Phi : \prod_{i=1}^{n} A_i & \longrightarrow & \mathsf{X}_{i=1}^{n} A_i \\ f & \longmapsto & (f(1), \ldots, f(n)) =: \Phi(f) \end{array}$$

και

$$\begin{array}{ccc} \Psi : \mathsf{X}_{i=1}^{n} A_i & \longrightarrow & \prod_{i=1}^{n} A_i \\ (x_1, \ldots, x_n) & \longmapsto & \Psi\left((x_1, \ldots, x_n)\right)(i) := x_i \end{array}$$

για τις οποίες ισχύει

$$\Phi \circ \Psi = \mathrm{id}_{\mathsf{X}_{i=1}^{n} A_i} \quad \text{και} \quad \Psi \circ \Phi = \mathrm{id}_{\prod_{i=1}^{n} A_i}.$$

Βάσει τής προτάσεως 1.2.18 (iii) οι Φ και Ψ είναι αμφιρριπτικές και $\Phi = \Psi^{-1}$. Εφεξής θα *ταυτίζουμε* τα $\mathsf{X}_{i=1}^{n} A_i$ και $\prod_{i=1}^{n} A_i$ μέσω των απεικονίσεων Φ και Ψ.

1.11.3 Ορισμός. Έστω τώρα I *οιοδήποτε* μη κενό σύνολο και έστω $(A_i)_{i\in I}$ μια οικογένεια συνόλων με τους δείκτες της ειλημμένους από το I. Γενικεύοντας την προαναφερθείσα κατασκευή τού (νέου) καρτεσιανού γινομένου (όπου είχαμε $I = \{1, .., n\}$) μπορούμε να ορίσουμε ως **καρτεσιανό γινόμενο** των μελών τής ανωτέρω οικογενείας συνόλων το

$$\prod_{i\in I} A_i := \left\{ f \;\middle|\; f : I \longrightarrow \bigcup_{i\in I} A_i \text{ απεικονίσεις με } f(i) \in A_i, \forall i \in I \right\}.$$

Εάν για κάποιον δείκτη i_0 ισχύει $A_{i_0} = \varnothing$, τότε προφανώς $\prod_{i\in I} A_i = \varnothing$ (διότι εάν υπήρχε κάποιο στοιχείο $f \in \prod_{i\in I} A_i$, τότε θα είχαμε $f(i_0) \in A_{i_0}$, πράγμα άτοπο). Αλλά τι συμβαίνει στην περίπτωση κατά την οποία $A_i \neq \varnothing, \forall i \in I$; Η απάντηση σε αυτό το ερώτημα (στην πλήρη του γενικότητα) είναι τόσο θεμελιώδης για τη Θεωρία Συνόλων, ώστε να πρέπει να θεσπίζεται ως ένα (ιδιάζουσας σημασίας) *αξίωμα*.

1.11.4 Αξίωμα («Αξίωμα τής επιλογής»). *Εάν το I είναι ένα μη κενό σύνολο και η $(A_i)_{i\in I}$ οιαδήποτε οικογένεια συνόλων με τους δείκτες της ειλημμένους από το I, τότε*

$$(A_i \neq \varnothing, \;\; \forall i \in I) \Longrightarrow \prod_{i\in I} A_i \neq \varnothing.$$

1.12 ΠΕΠΕΡΑΣΜΕΝΑ ΚΑΙ ΑΠΕΙΡΑ ΣΥΝΟΛΑ

1.12.1 Ορισμός. Λέμε πως δυο σύνολα A και B **έχουν την ίδια ισχύ** (συμβολίζοντάς τα ως $A \approx B$) όταν υπάρχει μια αμφίρριψη $f : A \longrightarrow B$ από το A επί τού B. Προφανώς, υπό αυτήν την προϋπόθεση, έχουμε και $B \approx A$, διότι η $f^{-1} : B \longrightarrow A$ είναι αμφιρριπτική. Όμως η "$\approx$" δεν έχει μόνον τη συμμετρική και (προδήλως) την ανακλαστική ιδιότητα, αλλά *και* τη μεταβατική, καθότι η σύνθεση δύο αμφιρρίψεων αποτελεί μια αμφίρριψη (πρβλ. 1.2.16 (i), (ii)). Ως εκ τούτου, η "$\approx$" ορίζει μια σχέση ισοδυναμίας επί τής «κλάσεως[52]» $\mathcal{C}$ όλων των

συνόλων. Όλα τα σύνολα που είναι ισοδύναμα με ένα παγιωμένο σύνολο A (ως προς την "$\approx$") ορίζουν μια κλάση ισοδυναμίας. Η "$\approx$" διαμελίζει την $\mathcal{C}$ σε κλάσεις ισοδυναμίας και σε κάθε κλάση ισοδυναμίας αντιστοιχούμε έναν **απόλυτο** ή **πληθικό αριθμό** που χαρακτηρίζει -κατά κάποιον τρόπο- το «μέγεθος» κάθε στοιχείου της. (Ο αριθμός αυτός για ένα σύνολο A σημειώνεται ως $\mathrm{card}(A)$). Ένα μη κενό[53] σύνολο A ονομάζεται **πεπερασμένο** (με πληθικό αριθμό ίσο με $n = \mathrm{card}(A) \in \mathbb{N}$) όταν $A \approx \{1, \ldots, n\}$. Κάθε μη κενό και -ταυτοχρόνως- μη πεπερασμένο σύνολο καλείται **απέραντο** ή **άπειρο σύνολο** ή -απλώς- **απειροσύνολο**. Ένα σύνολο A ονομάζεται **αριθμήσιμο σύνολο** όταν $A \approx \mathbb{N}$. Κάθε σύνολο το οποίο είναι ή πεπερασμένο ή αριθμήσιμο λέγεται **το πολύ αριθμήσιμο σύνολο**. Κάθε μη κενό και -ταυτοχρόνως- μη αριθμήσιμο σύνολο λέγεται **υπεραριθμήσιμο σύνολο**.

1.12.2 Λήμμα. *Το καρτεσιανό γινόμενο πεπερασμένου πλήθους πεπερασμένων συνόλων αποτελεί ένα πεπερασμένο σύνολο. Μάλιστα, εάν τα $A_1, A_2, \ldots, A_n$ είναι πεπερασμένα σύνολα, τότε*

$$\mathrm{card}\,(A_1 \times A_2 \times \cdots \times A_n) = \mathrm{card}\,(A_1) \cdot \mathrm{card}\,(A_2) \cdot \cdots \cdot \mathrm{card}\,(A_n)\,. \tag{1.75}$$

1.12.3 Λήμμα. *Η ένωση πεπερασμένου πλήθους πεπερασμένων συνόλων αποτελεί ένα πεπερασμένο σύνολο. Μάλιστα, εάν τα $A_1, A_2, \ldots, A_n$ είναι πεπερασμένα σύνολα, τότε*

$$\mathrm{card}\,(A_1 \cup \cdots \cup A_n) = \sum_{k=1}^{n} \sum_{1 \leqslant j_1 < \cdots < j_k \leqslant n} (-1)^{k-1}\, \mathrm{card}\,(A_{j_1} \cap \cdots \cap A_{j_k})\,. \tag{1.76}$$

Ιδιαιτέρως, εάν τα $A_1, A_2, \ldots, A_n$ είναι πεπερασμένα σύνολα και ανα δύο ξένα, τότε

$$\mathrm{card}\,(A_1 \cup \cdots \cup A_n) = \mathrm{card}(\coprod_{j=1}^{n} A_j) = \mathrm{card}\,(A_1) + \cdots + \mathrm{card}\,(A_n)\,. \tag{1.77}$$

1.12.4 Λήμμα. *Έστω A ένα πεπερασμένο σύνολο και έστω $f : A \longrightarrow A$ μια τυχούσα απεικόνιση. Τότε τα ακόλουθα είναι ισοδύναμα*:

(i) *Η f είναι μια ένριψη.*

(ii) *Η f είναι μια επίριψη.*

(iii) *Η f είναι μια αμφίριψη.*

Απόδειξη. Προφανώς αρκεί να δειχθεί η αμφίπλευρη συνεπαγωγή (ii)$\Longleftrightarrow$(i).

(ii)$\Longrightarrow$(i). Έστω ότι η f είναι μια επιριπτική απεικόνιση. Τότε καθένα εκ των $\mathrm{card}(A)$ στοιχείων τού A θα διαθέτει *τουλάχιστον ένα* αρχέτυπο (= αντίστροφη εικόνα), ενώ παραλλήλως (από τον ορισμό μιας απεικονίσεως) δεν υπάρχουν διαφορετικά στοιχεία τού A με κοινό αρχέτυπο. Όμως υπάρχουν μόνον $\mathrm{card}(A)$ διαθέσιμα αρχέτυπα, οπότε κάθε $x \in A$ έχει *το πολύ ένα* εξ αυτών. Άρα η f οφείλει να είναι και ενριπτική (κατά την πρόταση 1.2.10 (i)).

(i)$\Longrightarrow$(ii). Έστω ότι η f είναι μια ενριπτική απεικόνιση. Τότε οι εικόνες των $\mathrm{card}(A)$ στοιχείων τού A πρέπει να είναι ανά ζεύγη διαφορετικές, διότι η f ποτέ δεν απει-

[52] Εδώ χρησιμοποιείται ο όρος *κλάση* αντί τού *συνόλου*, διότι στη Θεωρία Συνόλων η αποδοχή τής υπάρξεως «συνόλου όλων των συνόλων» οδηγεί στην εμφάνιση τού «παραδόξου τού Russel». (Εάν θα μπορούσε να σχηματισθεί το σύνολο όλων των συνόλων τα οποία δεν είναι στοιχεία τού εαυτού τους, τότε αυτό θα έπρεπε **και** να ανήκει **και** να μην ανήκει στον εαυτό του!)

[53] Όταν $A = \varnothing$, τότε ορίζουμε $\mathrm{card}(A) := 0$.

κονίζει δύο διαφορετικά στοιχεία στο ίδιο στοιχείο. Κατά συνέπειαν, υπάρχουν ακριβώς $\text{card}(A)$ εικόνες που καλύπτουν ολόκληρο το A (ήτοι ισχύει $f(A) = A$). □

1.12.5 Λήμμα. *Ας υποθέσουμε ότι τα A και B είναι δυο πεπερασμένα σύνολα. Τότε ισχύουν τα εξής*: (i) $\text{card}(A) \leqslant \text{card}(B) \Longleftrightarrow$ (*υπάρχει μια ένριψη* $f : A \longrightarrow B$),
(ii) $\text{card}(A) \geqslant \text{card}\,(B) \Longleftrightarrow$ (*υπάρχει μια επίριψη* $f : A \longrightarrow B$), *και*
(iii) $\text{card}(A) = \text{card}\,(B) \Longleftrightarrow$ (*υπάρχει μια αμφίριψη* $f : A \longrightarrow B$).

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι $A = \{x_1, .., x_m\}$ και $B = \{y_1, .., y_n\}$, όπου

$$x_i \neq x_j,\ \left[\forall\,(i,j) \in \{1,2,\ldots,m\}^2 : i \neq j\right],$$

και

$$y_i \neq y_j,\ \left[\forall\,(i,j) \in \{1,2,\ldots,n\}^2 : i \neq j\right].$$

Τότε $\text{card}(A) = m$ και $\text{card}(B) = n$.
(i) Εάν $m \leqslant n$, τότε ορίζουμε την απεικόνιση

$$f : A \longrightarrow B, \quad f\,(x_i) = y_i, \ \ \forall i \in \{1,2,\ldots,m\}.$$

Τότε για κάθε $(i,j) \in \{1,2,\ldots,m\}^2$ με $i \neq j$ έχουμε

$$f\,(x_i) = y_i \neq y_j = f(x_j),$$

οπότε η f είναι μια ένριψη. Και αντιστρόφως· εάν υποθέσουμε ότι η $f : A \longrightarrow B$ είναι μια ένριψη, τότε η εικόνα $f(A) = \{f(x_1), ..., f(x_m)\} \subseteq B$ συνίσταται από m ανα ζεύγη διαφορετικά στοιχεία. Άρα το B περιέχει τουλάχιστον m στοιχεία και $m \leqslant n$.
(ii) Εάν $m \geqslant n$, τότε ορίζουμε την απεικόνιση

$$f : A \longrightarrow B, \quad f\,(x_i) = \begin{cases} y_i, & \forall i \in \{1,2,\ldots,n\}, \\ y_1, & \forall i \in \{n+1,2,\ldots,m\}. \end{cases}$$

Τότε $f(A) = \{y_1, ..., y_n\} = B$, οπότε η f είναι όντως μια επίριψη. Και αντιστρόφως· εάν υποθέσουμε ότι η $f : A \longrightarrow B$ είναι μια επίριψη, τότε

$$\{y_1, ..., y_n\} = B = f(A) = \{f(x_1), ..., f(x_m)\}.$$

Κατά συνέπειαν, το σύνολο $\{f(x_1), ..., f(x_m)\}$ περιέχει ακριβώς n διαφορετικά στοιχεία, οπότε $m \geqslant n$.
(iii) Τούτο έπεται άμεσα από τα (i) και (ii). □

1.12.6 Παρατήρηση. Εάν A και B είναι δυο πεπερασμένα σύνολα και $A \subsetneqq B$, τότε -κατά το λήμμα 1.12.5- έχουμε $\text{card}(A) < \text{card}(B)$, οπότε τα A και B δεν μπορούν να έχουν την ίδια ισχύ. Αυτή η ιδιότητα δεν ισχύει και για απειροσύνολα. Π.χ. $\mathbb{N} \subsetneqq \mathbb{Z}$, αλλά $\mathbb{Z} \approx \mathbb{N}$, διότι η απεικόνιση $h : \mathbb{Z} \longrightarrow \mathbb{N}$,

$$a \longmapsto h(a) := \begin{cases} 2a, & \text{όταν } a \in \mathbb{N}, \\ 1 - 2a, & \text{όταν } a \in \mathbb{Z} \setminus \mathbb{N}, \end{cases}$$

είναι αμφιρριπτική[54]. Ωστόσο, για *τυχόντα σύνολα* A, B ισχύει μια ασθενέστερη συνθήκη, η οποία αποτυπώνεται στο θεώρημα που ακολουθεί.

[54] Ο πληθικός αριθμός τού $\mathbb{N}$ συμβολίζεται ως $\aleph_0$ και καλείται **άλεφ μηδέν**, ενώ ο πληθικός αριθμός τού $\mathbb{R}$ συμβολίζεται ως $\mathfrak{c}$ και είθισται να λέγεται **ισχύς τού συνεχούς**.

1.12.7 Θεώρημα (Schröder & Bernstein). *Εάν A, B είναι δυο σύνολα, τότε ισχύει η συνεπαγωγή*

$$[\mathrm{card}(A) \leqslant \mathrm{card}(B) \text{ και } \mathrm{card}(B) \leqslant \mathrm{card}(A)] \Rightarrow \mathrm{card}(A) = \mathrm{card}(B).$$

1.12.8 Πρόταση. *Η ένωση μιας το πολύ αριθμήσιμης οικογενείας το πολύ αριθμησίμων συνόλων είναι σύνολο το πολύ αριθμήσιμο.*

Απόδειξη. Έστω $(A_i)_{i\in\mathbb{N}}$ μια αριθμήσιμη οικογένεια το πολύ αριθμησίμων συνόλων

$$A_i = \{x_{i1}, x_{i2}, x_{i3}, \ldots\}.$$

Γράφουμε τα εν λόγω σύνολα ως εξής:

$$\begin{array}{lccccccccc}
A_1: & x_{11} & & x_{12} & \longrightarrow & x_{13} & & x_{14} & \cdots \\
 & \downarrow & \nearrow & & \swarrow & & \nearrow & & \\
A_2: & x_{21} & & x_{22} & & x_{23} & & x_{24} & \cdots \\
 & & \swarrow & & \nearrow & & & & \\
A_3: & x_{31} & & x_{32} & & x_{33} & & x_{34} & \cdots \\
 & \downarrow & \nearrow & & & & & & \\
A_4: & x_{41} & & x_{42} & & x_{43} & & x_{44} & \cdots \\
 & \vdots & & \vdots & & \vdots & & \vdots &
\end{array}$$

Κάνοντας (καντοριανή) απαρίθμηση όπως υποδεικνύουν τα βέλη και λαμβάνοντας υπ' όψιν μόνον την πρώτη φορά εμφανίσεως καθενός των στοιχείων που συναντούμε, κατασκευάζουμε μια απεικόνιση

$$\mathbb{N} \longrightarrow \bigcup_{i\in\mathbb{N}} A_i$$

η οποία είναι αμφιρριπτική. □

1.12.9 Πόρισμα. *Το σύνολο των ρητών αριθμών $\mathbb{Q}$ είναι σύνολο αριθμήσιμο.*

Απόδειξη. Επειδή το σύνολο $\mathbb{Z}$ των ακεραίων είναι αριθμήσιμο και

$$\mathbb{Q} = \bigcup_{\mu\in\mathbb{N}} \frac{1}{\mu}\mathbb{Z} = \bigcup_{\mu\in\mathbb{N}} \left\{ \frac{\lambda}{\mu} \middle| \lambda \in \mathbb{Z} \right\},$$

ο ισχυρισμός είναι αληθής δυνάμει τής προτάσεως 1.12.8. □

1.12.10 Πόρισμα. *Το καρτεσιανό γινόμενο μιας πεπερασμένης οικογενείας το πολύ αριθμησίμων συνόλων είναι σύνολο το πολύ αριθμήσιμο.*

Απόδειξη. Εάν τα A, B είναι δυο το πολύ αριθμήσιμα σύνολα, τότε

$$A \times B = \bigcup_{x\in A} (\{x\} \times B).$$

Επειδή η απεικόνιση

$$B \longrightarrow \{x\} \times B, \quad y \longmapsto (x, y),$$

είναι αμφιρριπτική, το $\{x\} \times B$ είναι σύνολο το πολύ αριθμήσιμο, οπότε και το $A \times B$ οφείλει να είναι το πολύ αριθμήσιμο βάσει τής προτάσεως 1.12.8. Η γενική περίπτωση έπεται άμεσα κάνοντας χρήση μαθηματικής επαγωγής. □

1.12.11 Πρόταση. *Το σύνολο $\mathbb{R}$ των πραγματικών αριθμών είναι υπεραριθμήσιμο.*

Απόδειξη. Επειδή $\mathbb{R} \approx (0,1)$ (βλ. το (ii) της ασκήσεως 15 τού 2ου φυλλαδίου), αρκεί να δείξουμε την υπεραριθμησιμότητα τού ανοικτού διαστήματος $(0,1)$. Εάν υποθέσουμε ότι το $(0,1)$ είναι αριθμήσιμο, τότε μπορούμε να γράψουμε τα στοιχεία του ως στοιχεία μιας ακολουθίας:

$$(0,1) = \{r_1, r_2, \ldots, r_n, r_{n+1}, \ldots\}.$$

Όμως κάθε πραγματικός αριθμός που ανήκει στο $(0,1)$ μπορεί να γραφεί υπό τη δεκαδική του μορφή, ούτως ώστε αυτή να περιέχει άπειρα στοιχεία. (Στην περίπτωση που αυτά τερματίζονται κάπου, τα συμπληρώνουμε επάπειρον με μηδενικά). Ως εκ τούτου,

$$r_i = 0, x_{i1}x_{i2}x_{i3}\ldots$$

όπου $x_{ij} \in \{0,1,2,3,4,5,6,7,8,9\}$. Ορίζοντας π.χ. τον αριθμό

$$y_i := \begin{cases} 7, & \text{όταν } x_{ii} \neq 7, \\ 3, & \text{όταν } x_{ii} = 7, \end{cases}$$

έχουμε $y_i \neq x_{ii}$ για όλους τους δείκτες i. Επομένως, ο

$$r := 0, y_1y_2y_3\ldots$$

θα είναι *διάφορος* τού r_i για όλους τους δείκτες i, καθότι τα δεκαδικά αναπτύγματα των r και r_i θα διαφέρουν (τουλάχιστον στην i-οστή θέση). Άρα ο εν λόγω αριθμός r ανήκει στο ανοικτό διάστημα $(0,1)$ χωρίς -ταυτοχρόνως- να ανήκει και στην ακολουθία $\{r_1, r_2, r_3, \ldots\}$. Άτοπο! Άρα τελικώς το $\mathbb{R}$ είναι όντως υπεραριθμήσιμο. □

1.12.12 Σημείωση. Στο παρόν κεφάλαιο περιεγράφησαν μόνον εκείνες οι έννοιες τής Στοιχειώδους Θεωρίας Συνόλων και παρετέθησαν μόνον εκείνα τα αποτελέσματα που θα μας διευκολύνουν στα κατοπινά κεφάλαια των σημειώσεων. Για μια ολοκληρωμένη εισαγωγή σε αυτού τού είδους τη Θεωρία Συνόλων ο ενδιαφερόμενος αναγνώστης παραπέμπεται στο κλασικό βιβλίο τού P.R. Halmos: *Αφελής Συνολοθεωρία,* σε μετάφραση (από το αγγλικό πρωτότυπο υπό τον τίτλο *Naive Set Theory*, Springer-Verlag, 1960) από τον Γ. Κολέτσο, Εκδόσεις Εκκρεμές, Αθήνα, 2002. Ένα άλλο αξιομνημόνευτο σύγγραμμα, το οποίο είναι υψηλοτέρου επιπέδου, συνοδεύεται από εκτενή σχόλια που αφορούν στην Αξιωματική Θεωρία Συνόλων από τη σκοπιά τής Θεωρίας Προτύπων (Μοντέλων) και είναι διαθέσιμο *και* στα ελληνικά, είναι αυτό τού Γ.Ν. Μοσχοβάκη: *Σημειώσεις στη Συνολοθεωρία*, Εκδόσεις «Νεφέλη», Αθήνα, 1993.

ΚΕΦΑΛΑΙΟ 2

Υπομνήσεις από τη Στοιχειώδη Θεωρία Αριθμών

Σκοπός τού παρόντος κεφαλαίου είναι η υπενθύμιση κάποιων αποτελεσμάτων τής Στοιχειώδους Θεωρίας Αριθμών, ορισμένα εκ των οποίων είναι ήδη γνωστά από το σχολείο (και τα λοιπά από προηγηθείσες παραδόσεις άλλων συναφών εισαγωγικών μαθημάτων) και χρησιμοποιούνται κατ' επανάληψη στο κυρίως κείμενο. Μεταξύ αυτών συγκαταλέγονται η ταυτότητα τής ευκλειδείου διαιρέσεως, οι κύριες ιδιότητες και ο τρόπος υπολογισμού τού μεγίστου κοινού διαιρέτη και τού ελαχίστου κοινού πολλαπλασίου (δύο ή περισσότερων ακεραίων), η μονοσήμαντη παράσταση ενός φυσικού αριθμού $\geqslant 2$ ως γινομένου πρώτων αριθμών, το θεώρημα τού Euler περί ισοτιμίων και η περιγραφή των λύσεων γραμμικών ισοτιμιών με έναν άγνωστο.

2.1 ΔΙΑΙΡΕΣΗ ΑΚΕΡΑΙΩΝ

Η έννοια τής «διαιρέσεως» ήταν γνωστή και κατανοητή ήδη από αρχαιοτάτων χρόνων. Ο Ευκλείδης στο βιβλίο VII των «Στοιχείων» την περιγράφει με περισσή σαφήνεια (βασιζόμενος στη γεωμετρική-ανθυφαιρετική μέθοδο).

2.1.1 Ορισμός. Έστω ότι οι a, b είναι δυο ακέραιοι αριθμοί. Εάν υπάρχει ένας ακέραιος αριθμός c, τέτοιος ώστε να ισχύει η ισότητα $b = ac$, τότε λέμε ότι ο a **διαιρεί** (ακριβώς) **τον** b και ότι ο b **είναι διαιρέσιμος διά τού** a ή -ισοδυνάμως- ότι ο b είναι **πολλαπλάσιο τού** a και ότι ο a είναι **διαιρέτης** ή **παράγοντας** τού b. Για να δηλούμε ότι ο a διαιρεί τον b γράφουμε $a \mid b$, ενώ για να δηλούμε ότι ο a δεν διαιρεί τον b γράφουμε $a \nmid b$.

2.1.2 Παράδειγμα. Οι *άρτιοι* (και αντιστοίχως, οι *περιττοί*) ακέραιοι αριθμοί είναι εκείνοι οι ακέραιοι αριθμοί οι οποίοι είναι διαιρέσιμοι (και αντιστοίχως, δεν είναι διαιρέσιμοι) διά τού 2.

2.1.3 Πρόταση. (i) $a \mid 0$ *για κάθε* $a \in \mathbb{Z}$.
(ii) $\pm 1 \mid a$ *για κάθε* $a \in \mathbb{Z}$.
(iii) *Εάν* $0 \mid b$, *για κάποιον* $b \in \mathbb{Z}$, *τότε* $b = 0$.
(iv) *Εάν* $b \mid \pm 1$, *για κάποιον* $b \in \mathbb{Z}$, *τότε* $b = \pm 1$.
(v) $a \mid a$ *για κάθε* $a \in \mathbb{Z}$.

Αποδειξη. (i) Προφανώς, $0 = a \cdot 0$.

(ii) Επειδή $a = 1 \cdot a = (-1) \cdot (-a)$, έχουμε $\pm 1 \mid a$ για οιονδήποτε $a \in \mathbb{Z}$.

(iii) Εάν $0 \mid b$, τότε $b = 0 \cdot c$ για κάποιον $c \in \mathbb{Z}$, οπότε κατ' ανάγκην $b = 0$.

(iv) Εάν $b \mid \pm 1$, τότε $\pm 1 = bc$ για κάποιον ακέραιο αριθμό c, οπότε κατ' ανάγκην έχουμε $(b, c) \in \{(\pm 1, \pm 1), (\pm 1, \mp 1)\}$.

(v) Προφανώς, $a = a \cdot 1$ για κάθε $a \in \mathbb{Z}$. □

2.1.4 Σημείωση. Σε ό,τι ακολουθεί σημειώνουμε ως $|a| = \text{sign}(a)\, a$ την *απόλυτη τιμή* ενός ακεραίου a (όπου $\text{sign}(a) := 1$, όταν $a \geqslant 0$ και $\text{sign}(a) := -1$, όταν $a < 0$).

2.1.5 Πρόταση. *Εάν $a, b, c, d \in \mathbb{Z}$, τότε ισχύουν τα ακόλουθα*:

(i) $a \mid b \iff -a \mid b \iff a \mid -b \iff |a| \mid |b|$.

(ii) *Εάν $a \mid b$ και $b \neq 0$, τότε $|a| \leqslant |b|$.*

(iii) *Εάν $a \mid b$ και $b \mid a$, τότε $|a| = |b|$.*

(iv) *Εάν $a \mid b$ και $c \mid d$, τότε $ac \mid bd$.*

(v) *Εάν $a \mid b$ και $b \mid c$, τότε $a \mid c$.*

(vi) *Εάν $a \mid b$ και $a \mid c$, τότε $a \mid bx + cy$ για κάθε $x, y \in \mathbb{Z}$.*

(Γενικότερα, εάν $n \in \mathbb{N}$, $b_1, \ldots, b_n \in \mathbb{Z}$, και $a \mid b_j$ για κάθε $j \in \{1, \ldots, n\}$, τότε ακολουθώντας την ίδια συλλογιστική έχουμε $a \mid \sum_{j=1}^{n} x_j b_j$ για οιουσδήποτε $x_1, \ldots, x_n \in \mathbb{Z}$.)

Αποδειξη. (i) Προφανές επί τη βάσει τού ορισμού 2.1.1.

(ii) Εάν $a \mid b$ και $b \neq 0$, τότε υπάρχει μη μηδενικός ακέραιος a' με $b = aa'$. Επομένως, $|b| = |a|\,|a'|$, απ' όπου έπεται ότι $|a| \leqslant |b|$.

(iii) Εάν οι a και b είναι αμφότεροι μη μηδενικοί, τότε -λόγω τού (ii)- $|a| \leqslant |b|$ και $|a| \geqslant |b|$, οπότε $|a| = |b|$. Εάν $a = 0$, τότε από τη σχέση διαιρετότητας $a \mid b$ λαμβάνουμε $b = 0$ (βλ. 2.1.3 (iii)). Παρομοίως εάν $b = 0$, τότε από την $b \mid a$ λαμβάνουμε $a = 0$. Άρα σε κάθε περίπτωση $|a| = |b|$.

(iv) Υποθέτοντας ότι $a \mid b$ και $c \mid d$, θα υπάρχουν ακέραιοι e, f, τέτοιοι ώστε να ισχύουν οι ισότητες $b = ae$ και $d = cf$. Κατά συνέπειαν,

$$bd = acef \Longrightarrow ac \mid bd.$$

(v) Υποθέτοντας ότι $a \mid b$ και $c \mid d$, θα υπάρχουν ακέραιοι e, f, τέτοιοι ώστε να ισχύουν οι ισότητες $b = ae$ και $c = bf$. Επομένως, $c = bf = aef \Longrightarrow a \mid c$.

(vi) Εάν $a \mid b$ και $a \mid c$, θα υπάρχουν ακέραιοι e, f, τέτοιοι ώστε να ισχύουν οι ισότητες $b = ae$ και $c = af$. Συνεπώς,

$$bx + cy = aex + afy = a(ex + fy) \Longrightarrow a \mid bx + cy$$

για οιουσδήποτε $x, y \in \mathbb{Z}$. □

2.1.6 Θεώρημα (Η ταυτότητα τής ευκλείδειας διαιρέσεως).
Εάν υποθέσουμε ότι $a \in \mathbb{Z}$ και ότι $b \in \mathbb{Z} \setminus \{0\}$, τότε υπάρχει ένα μονοσημάντως ορισμένο *ζεύγος $(q, r) \in \mathbb{Z} \times \mathbb{Z}$, ούτως ώστε*

$$\boxed{a = qb + r, \text{ όπου } 0 \leqslant r < |b|\,.} \tag{2.1}$$

Αποδειξη. Εν πρώτοις θα αποδείξουμε την *ύπαρξη* ενός τέτοιου ζεύγους ακεραίων (q, r). Θεωρούμε τα σύνολα

$$A := \{\, a - xb \mid x \in \mathbb{Z} \} \quad \text{και} \quad S := \{\, y \in A \mid y \geqslant 0 \}\,.$$

Το S δεν είναι κενό, διότι θέτοντας $x = -|a|\text{sign}(b)$ λαμβάνουμε

$$a - xb = a + |a|\,|b| \geqslant 0,$$

δεδομένου -εξ υποθέσεως- ότι $|b| \geqslant 1$. Ως εκ τούτου, το S διαθέτει ένα ελάχιστο στοιχείο[1] $r \geqslant 0$. Αυτό σημαίνει ότι $r = a - qb$ για κάποιον $q \in \mathbb{Z}$, οπότε $a = qb + r$. Υποθέτοντας ότι το r δεν ικανοποιεί την $r < |b|$, θα είχαμε

$$r \geqslant |b| > 0 \Longrightarrow 0 \leqslant r - |b| < r \Longrightarrow r - |b| = a - qb - |b| = a - (q + \text{sign}\,(b))b,$$

ήτοι ότι $r - |b| \in S$, κάτι το οποίο θα αντέφασκε προς την επιλογή τού r. Κατά συνέπειαν, οι ανισότητες $0 \leqslant r < |b|$ είναι όντως αληθείς. Απομένει λοιπόν να δείξουμε ότι το ανωτέρω ζεύγος (q, r) που ικανοποιεί την (2.1) είναι, επιπροσθέτως, και *μονοσημάντως ορισμένο*. Ας υποθέσουμε ότι

$$a = qb + r = q'b + r',$$

όπου $(q', r') \in \mathbb{Z} \times \mathbb{Z}$, και ότι $0 \leqslant r, r' < |b|$. Τότε

$$\left.\begin{array}{c} |r - r'| = |b|\,|q - q'| \\ \text{και} \\ 0 \leqslant |r - r'| < |b| \end{array}\right\} \Longrightarrow |b|\,|q - q'| < |b| \Longrightarrow |q - q'| < 1 \underset{q,q' \in \mathbb{Z}}{\Longrightarrow} q = q'.$$

Άρα $r = a - qb = a - q'b = r'$, δηλαδή κατ' ανάγκην $(q, r) = (q', r')$. □

2.1.7 Ορισμός. Τα q και r τής ταυτότητας (2.1) ονομάζονται το **πηλίκο** και, αντιστοίχως, το **υπόλοιπο** τής **διαιρέσεως τού** a **διά τού** b. Σημειωτέον ότι το b διαιρεί (ακριβώς) το a, δηλαδή $b \mid a$, εάν και μόνον εάν $r = 0$.

▸ **Παράσταση φυσικού αριθμού σε μια κλίμακα.** Η εξοικείωση με την παράσταση ενός φυσικού αριθμού στο *δεκαδικό σύστημα* (στην «κλίμακα τού 10») λαμβάνει χώρα στα αρχικά στάδια τής πρωτοβάθμιας εκπαιδεύσεως. Το θεώρημα 2.1.9 μας πληροφορεί ότι, αντί τού 10, είναι δυνατόν να χρησιμοποιηθεί και οιοσδήποτε άλλος ακέραιος $\geqslant 2$.

2.1.8 Λήμμα. *Έστω $s \in \mathbb{N}$, $s \geqslant 2$. Εάν $n \in \mathbb{N}_0$ και ισχύει η ισότητα*

$$b_n s^n + b_{n-1} s^{n-1} + \cdots + b_1 s + b_0 = 0, \tag{2.2}$$

όπου $b_i \in \mathbb{Z}$ και $|b_i| \leqslant s - 1$, $\forall i \in \{0, 1, ..., n\}$, τότε $b_i = 0$, $\forall i \in \{0, 1, ..., n\}$.

Απόδειξη. Η (2.2) γράφεται ως $b_0 = k_0 s$, όπου $k_0 := -(b_n s^{n-1} + \cdots + b_1)$. Άρα είτε $|b_0| \geqslant s$ είτε $k_0 = 0$. Το πρώτο ενδεχόμενο αποκλείεται από την υπόθεσή μας. Επομένως,

$$\left.\begin{array}{r} k_0 = 0 \Rightarrow b_0 = 0 \\ s \neq 0 \end{array}\right\} \underset{(2.2)}{\Longrightarrow} b_n s^{n-1} + b_{n-1} s^{n-2} + \cdots + b_1 = 0.$$

Επαναλαμβάνοντας τον ίδιο συλλογισμό συμπεραίνουμε ότι $b_1 = 0$. Συνεχίζοντας αυτήν τη διαδικασία καταλήγουμε στο ότι $b_0 = b_1 = \cdots = b_n = 0$ (ύστερα από n βήματα). □

2.1.9 Θεώρημα. *Εάν $s \in \mathbb{N}$, $s \geqslant 2$, τότε κάθε $a \in \mathbb{N}$ μπορεί να γραφεί μονοσημάντως υπό τη μορφή*

$$\boxed{a = c_n s^n + c_{n-1} s^{n-1} + \cdots + c_1 s + c_0,} \tag{2.3}$$

όπου $n \in \mathbb{N}_0$, $c_i \in \{0, 1, ..., s - 1\}$ για κάθε $i \in \{0, ..., n - 1\}$ και $c_n \in \{1, ..., s - 1\}$.

[1] Κατά την «αρχή τής καλής διατάξεως», κάθε μη κενό υποσύνολο τού $\mathbb{N}$ ή τού $\mathbb{N}_0$ διαθέτει ελάχιστο στοιχείο.

(Επειδή $s^n \leqslant c_n s^n \leqslant a$, έχουμε $n \leqslant \frac{\ln(a)}{\ln(s)}$.)

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς, κάνοντας χρήση τής μαθηματικής επαγωγής (δεύτερης μορφής), θα δείξουμε ότι κάθε $a \in \mathbb{N}$ διαθέτει μια τέτοιου είδους παράσταση. Εάν $a = 1$, τότε η $a = 1$ είναι μια παράσταση τής μορφής (2.3) θέτοντας $n := 0$ και $c_0 := 1$. Εάν $a < s$, τότε η $a = a$ είναι μια τέτοιου είδους παράσταση, εάν θέσουμε $n := 0$ και $c_0 := a$. Εάν $a \geqslant s$, υποθέτουμε ότι κάθε φυσικός αριθμός $< a$ διαθέτει μια παράσταση τής μορφής (2.3) και γράφουμε τον a (μέσω τής (2.1)) ως

$$a = qs + r, \quad \text{όπου} \quad (q, r) \in \mathbb{Z} \times \mathbb{Z}$$

και $q > 0$, $r \in \{0, 1, ..., s-1\}$ (διότι $a \geqslant s$). Επειδή $q < a$, το q διαθέτει (λόγω τής επαγωγικής μας υποθέσεως) μια παράσταση τής μορφής

$$q = d_m s^m + d_{m-1} s^{m-1} + \cdots + d_1 s + d_0,$$

όπου $m \in \mathbb{N}_0$, $d_j \in \{0, 1, ..., s-1\}$ για κάθε $j \in \{0, ..., m-1\}$ και $d_m \in \{1, ..., s-1\}$. Άρα

$$a = qs + r = c_n s^n + c_{n-1} s^{n-1} + \cdots + c_1 s + c_0,$$

όπου $n := m + 1$, $c_i := d_{i-1}$ για κάθε $i \in \{1, ..., n\}$ και $c_0 := r$.

Εν συνεχεία, θα αποδείξουμε τη *μοναδικότητα* τής παραστάσεως (2.3) τού a. Ας υποθέσουμε ότι ο a, πέραν τής (2.3), έχει και την παράσταση

$$a = c'_k s^k + c'_{k-1} s^{n-1} + \cdots + c'_1 s + c'_0, \tag{2.4}$$

όπου $k \in \mathbb{N}_0$, $c'_\varrho \in \{0, 1, ..., s-1\}$ για κάθε $\varrho \in \{0, ..., k-1\}$ και $c'_k \in \{1, ..., s-1\}$. Εάν $k > n$, τότε οι (2.3) και (2.4) δίδουν

$$c'_k s^k + \cdots + c'_{n+1} s^{n+1} + \left(c'_n - c_n\right) s^n + \cdots + \left(c'_1 - c_1\right) s + \left(c'_0 - c_0\right) = 0. \tag{2.5}$$

Επειδή $|c'_i - c_i| \leqslant s - 1, \forall i \in \{0, 1, ..., n\}$, το λήμμα 2.1.8 μας πληροφορεί ότι όλοι οι συντελεστές τού αριστερού μέλους τής (2.5) είναι ίσοι με το 0. Τούτο όμως είναι άτοπο, διότι $c'_k > 0$. Άρα δεν μπορεί να ισχύει η ανισότητα $k > n$. Παρομοίως (με εναλλαγή των ρόλων των k και n) αποδεικνύουμε ότι δεν μπορεί να ισχύει ούτε η ανισότητα $k < n$. Κατά συνέπειαν, $k = n$ και

$$\left(c'_n - c_n\right) s^n + \cdots + \left(c'_1 - c_1\right) s + \left(c'_0 - c_0\right) = 0,$$

οπότε από το λήμμα 2.1.8 έπεται ότι $c'_i = c_i, \forall i \in \{0, 1, ..., n\}$. □

2.1.10 Ορισμός. Η παράσταση (2.3) καλείται **παράσταση τού a στην κλίμακα τού s** (και ο s **βάση τής κλίμακας**).

2.1.11 Συμβολισμός. Εάν ένας $a \in \mathbb{N}$ έχει στην κλίμακα τού s την παράσταση (2.3), τότε συνήθως γράφουμε εν συντομία

$$\boxed{a = (c_n c_{n-1} \ \ldots \ c_1 c_0)_s.}$$

2.1.12 Παραδείγματα. (i) Για τον $a = 456$ έχουμε προφανώς

$$456 = (456)_{10} = 4 \cdot 10^2 + 5 \cdot 10 + 6 = 7 \cdot 8^2 + 1 \cdot 8 + 0 = (710)_8.$$

(ii) Ο φυσικός αριθμός $a = 375$ στην κλίμακα τού 2 (ήτοι *στο δυαδικό σύστημα*) γράφεται ως $(101110111)_2$.

2.2 ΜΕΓΙΣΤΟΣ ΚΟΙΝΟΣ ΔΙΑΙΡΕΤΗΣ ΚΑΙ ΕΛΑΧΙΣΤΟ ΚΟΙΝΟ ΠΟΛΛΑΠΛΑΣΙΟ

2.2.1 Ορισμός. Εάν $n \in \mathbb{N},\ n \geqslant 2$, και εάν οι $a_1, \ldots, a_n$ είναι ακέραιοι με έναν τουλάχιστον εξ αυτών $\neq 0$, τότε κάθε ακέραιος που διαιρεί καθέναν εκ των $a_1, \ldots, a_n$ καλείται **κοινός διαιρέτης** των $a_1, \ldots, a_n$. Έστω S το σύνολο των θετικών κοινών διαιρετών των $a_1, \ldots, a_n$. Προφανώς το S είναι μη κενό, καθότι $1 \in S$. Επειδή $a_k \neq 0$ για κάποιον $k \in \{1, ..., n\}$, έχουμε $\delta \mid a_k$ και, ως εκ τούτου, $\delta \leqslant |a_k|\,, \forall \delta \in S$. Κατά συνέπειαν, το S είναι πεπερασμένο. Το μέγιστο στοιχείο τού συνόλου S (ως προς την " $\leqslant$ ") καλείται **μέγιστος κοινός διαιρέτης** των $a_1, \ldots, a_n$ και συμβολίζεται ως μκδ$(a_1, \ldots, a_n)$. Σημειωτέον ότι για κάθε $a \in \mathbb{Z}$ το σύνολο των θετικών διαιρετών τού a συμπίπτει με το σύνολο των θετικών διαιρετών τού $-a$. Επομένως,

$$\text{μκδ}(a_1, \ldots, a_n) = \text{μκδ}(|a_1|\,, \ldots, |a_n|),$$

δηλαδή ο μέγιστος κοινός διαιρέτης των $a_1, \ldots, a_n$ είναι *ανεξάρτητος* των προσήμων τους. Επίσης, επειδή κάθε ακέραιος διαιρεί το μηδέν, έχουμε

$$\text{μκδ}(0, a_1, \ldots, a_n) = \text{μκδ}(a_1, \ldots, a_n)$$

και, ειδικότερα[2], μκδ$(0, a) = $ μκδ$(a, 0) = 0,\ \forall a \in \mathbb{Z}\setminus\{0\}$. (Γι' αυτόν τον λόγο μπορούμε εφεξής να υποθέτουμε ότι κανείς εκ των εκάστοτε θεωρουμένων ακεραίων $a_1, \ldots, a_n$ δεν είναι μηδέν.)

2.2.2 Ορισμός. Δυο ακέραιοι $a, b \in \mathbb{Z}\setminus\{0\}$ καλούνται **σχετικώς πρώτοι** όταν μκδ$(a, b) = 1$. (Επίσης, εναλλακτικώς, σε αυτήν την περίπτωση, λέμε ότι ο a είναι **πρώτος προς τον** b ή -ισοδυνάμως- ότι ο b είναι **πρώτος προς τον** a).

2.2.3 Ορισμός. Εάν $n \in \mathbb{N},\ n \geqslant 2$, και $a_1, .., a_n \in \mathbb{Z}\setminus\{0\}$ με μκδ$(a_1, \ldots, a_n) = 1$, τότε λέμε ότι οι $a_1, \ldots, a_n$ είναι **σχετικώς πρώτοι** ή ότι είναι **πρώτοι μεταξύ τους**. Εάν μκδ$(a_j, a_k) = 1$ για οιουσδήποτε $j, k \in \{1, ..., n\}$ με $j \neq k$, τότε λέμε ότι οι $a_1, \ldots, a_n$ είναι **ανά δύο (ή ανά ζεύγη) σχετικώς πρώτοι** ή, εναλλακτικώς, ότι είναι **ανά δύο (ή ανά ζεύγη) πρώτοι μεταξύ τους**.

2.2.4 Παρατήρηση. Εάν οι $a_1, \ldots, a_n$ είναι ανά δύο σχετικώς πρώτοι, τότε είναι και σχετικώς πρώτοι (ως ολότητα). Αντιθέτως, το να είναι οι ακέραιοι $a_1, \ldots, a_n$ σχετικώς πρώτοι δεν σημαίνει ότι αυτοί είναι κατ' ανάγκην και ανά δύο σχετικώς πρώτοι. Π.χ., μκδ$(5, 6, 10) = 1$, με μκδ$(5, 6) = 1$, αλλά μκδ$(5, 10) = 5$ και μκδ$(6, 10) = 2$.

2.2.5 Θεώρημα. *Εάν* $n \in \mathbb{N},\ n \geqslant 2,\ a_1, \ldots, a_n \in \mathbb{Z}\setminus\{0\}$ *και* $d := \text{μκδ}(a_1, \ldots, a_n)$, *τότε υπάρχουν* $k_1, \ldots, k_n \in \mathbb{Z}$, *τέτοιοι ώστε να ισχύει η ισότητα*

$$\boxed{d = k_1 a_1 + \cdots + k_n a_n.} \tag{2.6}$$

(Είθισται να λέμε ότι μέσω τής (2.6) ο d εκφράζεται ως *ακέραιος γραμμικός συνδυασμός* των $a_1, \ldots, a_n$ με *συντελεστές* του τους $k_1, \ldots, k_n$.)

[2] *Σύμβαση*: Ακόμη και όταν $a = 0$, θέτουμε μκδ$(0, 0) := 0$.

ΑΠΟΔΕΙΞΗ. Θεωρούμε το σύνολο $S := \left\{ \sum_{j=1}^{n} \lambda_j a_j \;\middle|\; \lambda_1, \ldots, \lambda_n \in \mathbb{Z} \right\}$. Θέτοντας

$$\varepsilon_{j,l} := \begin{cases} 1, & \text{όταν } j = l, \\ 0, & \text{όταν } j \neq l, \end{cases}$$

για κάθε $j, l \in \{1, \ldots, n\}$, έχουμε προφανώς $a_l = \sum_{j=1}^{n} \varepsilon_{j,l} a_j \in S, \;\; \forall l \in \{1, \ldots, n\}$. Εάν κάποιος εκ των $a_1, \ldots, a_n$ είναι > 0, τότε $S \cap \mathbb{N} \neq \varnothing$. Ωστόσο, το ότι $S \cap \mathbb{N} \neq \varnothing$ είναι *πάντοτε* αληθές, διότι ακόμη και εάν $a_l < 0$ για *κάθε* $l \in \{1, \ldots, n\}$, έχουμε

$$-a_l = \sum_{j=1}^{n} (-\varepsilon_{j,l})\, a_j \in S \cap \mathbb{N}.$$

Ως εκ τούτου, το $S \cap \mathbb{N}$ διαθέτει *ελάχιστο* στοιχείο (καθώς το $\mathbb{N}$ είναι καλώς διατεταγμένο), ας πούμε το $d' = \sum_{j=1}^{n} k_j a_j$. Θα αποδείξουμε ότι $d' = d$. Πράγματι· για οιοδήποτε στοιχείο $m = \sum_{j=1}^{n} \lambda_j a_j$ τού S υπάρχει (κατά το θεώρημα 2.1.6) ένα μονοσημάντως ορισμένο ζεύγος $(q, r) \in \mathbb{Z} \times \mathbb{Z}$, ούτως ώστε να ισχύει

$$m = qd' + r, \text{ όπου } \; 0 \leqslant r < d'.$$

Υποθέτοντας ότι $r > 0$ καταλήγουμε σε κάτι το άτοπο, καθόσον

$$d' > r = \sum_{j=1}^{n} (\lambda_j - k_j q)\, a_j \in S.$$

Άρα $r = 0 \Longrightarrow d' \mid m$ και, ειδικότερα, $d' \mid a_j$ για κάθε $j \in \{1, \ldots, n\}$. Επιπροσθέτως, για οιονδήποτε $\delta \in \mathbb{N}$, για τον οποίο ισχύει $\delta \mid a_1, \ldots, \delta \mid a_n$, έχουμε

$$[\delta \mid k_1 a_1, \ldots, \delta \mid k_n a_n] \Longrightarrow \delta \mid d' \Longrightarrow \delta \leqslant d'$$

(βλ. 2.1.5 (vi) και (ii)), οπότε τελικώς $d' = d$. □

2.2.6 Πόρισμα. *Εάν $n \in \mathbb{N}, \; n \geqslant 2$, και $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$, τότε ένας $d \in \mathbb{N}$ ισούται με τον* μκδ$(a_1, \ldots, a_n)$ *εάν και μόνον εάν ισχύουν τα ακόλουθα*:
(i) $d \mid a_1, \ldots, d \mid a_n$,
(ii) *για οιονδήποτε $\delta \in \mathbb{N}$, για τον οποίο ισχύει $\delta \mid a_1, \ldots, \delta \mid a_n$, έχουμε $\delta \mid d$.*

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το θεώρημα 2.2.5 υπάρχουν $k_1, \ldots, k_n \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει η ισότητα μκδ$(a_1, \ldots, a_n) = k_1 a_1 + \cdots + k_n a_n$. Το (i) ισχύει εξ ορισμού. Για την απόδειξη τού (ii) αρκεί να θεωρήσουμε τυχόντα θετικό κοινό διαιρέτη δ των $a_1, \ldots, a_n$ και να αποδείξουμε ότι αυτός διαιρεί τον μέγιστο κοινό διαιρέτη τους. Επειδή $\delta \mid a_j \Longrightarrow \delta \mid k_j a_j, \; \forall j \in \{1, \ldots, n\}$, διαπιστώνουμε πράγματι ότι $\delta \mid$μκδ$(a_1, \ldots, a_n)$ (πρβλ. 2.1.5 (vi)). Και αντιστρόφως· εάν υποθέσουμε ότι ο d είναι ένας θετικός ακέραιος ο οποίος ικανοποιεί τα (i) και (ii), τότε ο d είναι κοινός διαιρέτης των $a_1, \ldots, a_n$ (λόγω τού (i)) και *οιοσδήποτε* θετικός κοινός διαιρέτης δ των $a_1, \ldots, a_n$ διαιρεί τον d (λόγω τού (ii)), οπότε $\delta \leqslant d$ (βλ. 2.1.5 (ii)). Επομένως έχουμε $d =$ μκδ$(a_1, \ldots, a_n)$. □

2.2.7 Πόρισμα. *Έστω ότι $n \in \mathbb{N}, \; n \geqslant 2$, και ότι οι $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$. Εάν ο d είναι ένας θετικός κοινός διαιρέτης των $a_1, \ldots, a_n$ που γράφεται υπό τη μορφή $d = k_1 a_1 + \cdots + k_n a_n, k_1, \ldots, k_n \in \mathbb{Z}$, τότε $d =$* μκδ$(a_1, \ldots, a_n)$.

ΑΠΟΔΕΙΞΗ. Εάν δ είναι ένας θετικός κοινός διαιρέτης των $a_1, \ldots, a_n$, τότε

$$\delta \mid a_j \Rightarrow [\delta \mid k_j a_j, \; \forall j \in \{1, \ldots, n\}] \Rightarrow \delta \mid d.$$

(Βλ. 2.1.5 (vi).) Άρα $d =$ μκδ$(a_1, \ldots, a_n)$ βάσει τού πορίσματος 2.2.7. □

2.2.8 Πόρισμα. *Εάν* $n \in \mathbb{N},\ n \geqslant 2$, *και* $a_1, \ldots, a_n \in \mathbb{Z}\setminus\{0\}$, *τότε οι* $a_1, \ldots, a_n$ *είναι πρώτοι μεταξύ τους εάν και μόνον εάν υπάρχουν* $k_1, \ldots, k_n \in \mathbb{Z}$, *τέτοιοι ώστε να ισχύει η ισότητα*

$$\boxed{k_1a_1 + \cdots + k_na_n = 1.}$$

Απόδειξη. Εάν οι $a_1, \ldots, a_n$ είναι πρώτοι μεταξύ τους, τότε η ως άνω ισότητα είναι προφανής από το θεώρημα 2.2.5. Εάν, αντιστρόφως, $k_1a_1 + \cdots + k_na_n = 1$ για κάποιους ακεραίους $k_1, \ldots, k_n$, έχουμε $1 \mid a_j$ για κάθε $j \in \{1, \ldots, n\}$, οπότε $\text{μκδ}(a_1, \ldots, a_n) = 1$ δυνάμει τού πορίσματος 2.2.7. □

2.2.9 Πόρισμα. *Εάν* $a, b, c \in \mathbb{Z}\setminus\{0\}$, $\text{μκδ}(a, b) = 1$ *και* $a \mid bc$, *τότε* $a \mid c$.

Απόδειξη. Επειδή $\text{μκδ}(a, b) = 1$, βάσει τού 2.2.8 υπάρχουν $k, l \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει η ισότητα $ka + lb = 1$. Ως εκ τούτου, $kac + lbc = c$, και επειδή $a \mid ac$ και $a \mid bc$, έχουμε $a \mid c$ (βλ. 2.1.5(vi)). □

2.2.10 Πόρισμα. *Εάν* $a, b, c \in \mathbb{Z}\setminus\{0\}$, *τότε ισχύει η συνεπαγωγή*

$$[\text{μκδ}(a, b) = 1,\ a \mid c \ \text{ και } \ b \mid c] \Longrightarrow ab \mid c.$$

Απόδειξη. Επειδή $\text{μκδ}(a, b) = 1$, βάσει τού 2.2.8 υπάρχουν $k, l \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει η ισότητα $ka + lb = 1$. Επομένως,

$$[c = kac + lbc,\ ab \mid ac \ \text{ και } \ ab \mid bc] \Longrightarrow ab \mid c$$

λόγω των (iv) και (vi) τής προτάσεως 2.1.5. □

2.2.11 Πόρισμα. *Εάν* $a, b \in \mathbb{N}$ *με* $\text{μκδ}(a, b) = 1$, *τότε υπάρχουν* $\kappa, \lambda \in \mathbb{N}$, *τέτοιοι ώστε να ισχύει* $\kappa a - \lambda b = 1$.

Απόδειξη. Σύμφωνα με το πόρισμα 2.2.8 υπάρχουν $k, l \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει η ισότητα $ka + lb = 1$. Επιλέγουμε έναν ακέραιο αριθμό t με $t > -\frac{k}{b}$ και $t > \frac{l}{a}$, και θέτουμε $\kappa := k + bt$ και $\lambda := -(l - at)$. Προφανώς έχουμε $\kappa \geqslant 1$, $\lambda \geqslant 1$, και $\kappa a - \lambda b = ka + lb = 1$. □

2.2.12 Πόρισμα. *Εάν* $a, b, c \in \mathbb{Z}\setminus\{0\}$, *τότε*

$$\text{μκδ}(a, bc) = 1 \Longleftrightarrow [\text{μκδ}(a, b) = 1 \text{ και } \text{μκδ}(a, c) = 1.]$$

Απόδειξη. Εάν $\text{μκδ}(a, bc) = 1$, τότε κατά το πόρισμα 2.2.8 υπάρχουν $k, l \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει η ισότητα $ka + lbc = 1$. Με εκ νέου εφαρμογή τού πορίσματος 2.2.8 (και, συγκεκριμένα, τής αντίστροφης συνεπαγωγής που δηλοί το «μόνον εάν») συμπεραίνουμε ότι $\text{μκδ}(a, b) = 1$ και $\text{μκδ}(a, c) = 1$. Και αντιστρόφως· υποθέτοντας ότι $\text{μκδ}(a, b) = 1$ και $\text{μκδ}(a, c) = 1$, θα υπάρχουν $r, s, t, u \in \mathbb{Z}$, τέτοιοι ώστε

$$\left.\begin{aligned} ra + sb &= 1 \\ ta + uc &= 1 \end{aligned}\right\} \Longrightarrow ra + sb\,(ta + uc) = 1 = (r + stb)\,a + (su)bc,$$

οπότε και πάλι μέσω τού 2.2.8 προκύπτει ότι $\text{μκδ}(a, bc) = 1$. □

2.2.13 Πόρισμα. *Εάν $a, b \in \mathbb{Z}\setminus\{0\}$ με $\text{μκδ}(a,b) = 1$, τότε $\text{μκδ}(a^m, b^n) = 1$ για κάθε ζεύγος $(m,n) \in \mathbb{N}\times\mathbb{N}$.*

ΑΠΟΔΕΙΞΗ. **Βήμα 1ο**. Υποθέτουμε ότι $m = 1$. Θα αποδείξουμε μέσω μαθηματικής επαγωγής ως προς τον n ότι $\text{μκδ}(a, b^n) = 1$. Για $n = 1$ αυτή η ισότητα είναι (εξ υποθέσεως) αληθής. Εάν υποθέσουμε ότι $n \geqslant 2$ και ότι $\text{μκδ}(a, b^{n-1}) = 1$, τότε

$$\left[\text{μκδ}(a,b) = 1 \text{ και } \text{μκδ}(a, b^{n-1}) = 1\right] \underset{2.2.12}{\Longrightarrow} \text{μκδ}(a, b^n) = 1.$$

Βήμα 2ο. Θα αποδείξουμε μέσω μαθηματικής επαγωγής ως προς τον m ότι ισχύει $\text{μκδ}(a^m, b^n) = 1$. Για $m = 1$ η εν λόγω ισότητα είναι αληθής (βάσει των προαναφερθέντων στο 1ο βήμα). Εάν υποθέσουμε ότι $m \geqslant 2$ και ότι $\text{μκδ}(a^{m-1}, b^n) = 1$, τότε $\left[\text{μκδ}(a, b^n) = 1 \text{ και } \text{μκδ}(a^{m-1}, b^n) = 1\right] \underset{2.2.12}{\Longrightarrow} \text{μκδ}(a^m, b^n) = 1$. □

2.2.14 Πρόταση. *Εάν $n \in \mathbb{N}$, $n \geqslant 2$, και εάν οι $\lambda, a_1, \ldots, a_n$ είναι μη μηδενικοί ακέραιοι,τότε ισχύουν τα ακόλουθα*:

(i) $\text{μκδ}(\lambda a_1, \ldots, \lambda a_n) = |\lambda|\ \text{μκδ}(a_1, \ldots, a_n)$,

(ii) *εάν* $\text{μκδ}(a_1, \ldots, a_n) = d$, *τότε* $\text{μκδ}(\frac{a_1}{d}, \ldots, \frac{a_n}{d}) = 1$, *και*

(iii) $\text{μκδ}(a_1, \ldots, a_n) = \text{μκδ}(a_1 + \nu_2 a_2 + \cdots + \nu_n a_n, a_2, ..., a_n)$, *για οιουσδήποτε* $\nu_2, .., \nu_n \in \mathbb{Z}$.

ΑΠΟΔΕΙΞΗ. (i) Εάν $\text{μκδ}(a_1, \ldots, a_n) = d$, τότε κατά το θεώρημα 2.2.5 υπάρχουν ακέραιοι $k_1, \ldots, k_n$, τέτοιοι ώστε να ισχύει η ισότητα $d = k_1 a_1 + \cdots + k_n a_n$. Επομένως,

$$d\,|\lambda| = \sum_{j=1}^{n} k_j a_j\,|\lambda| = \sum_{j=1}^{n} (\text{sign}\,(\lambda)\,k_j)\ a_j\lambda,$$

και επειδή $d \mid a_j \Rightarrow d\,|\lambda| \mid a_j\lambda$, για κάθε $j \in \{1, \ldots, n\}$, ο μ.κ.δ. των $\lambda a_1, \ldots, \lambda a_n$ είναι ο $d\,|\lambda|$ δυνάμει τού πορίσματος 2.2.7.

(ii) $d = \text{μκδ}(a_1, \ldots, a_n) = \text{μκδ}(d\,\frac{a_1}{d}, \ldots, d\,\frac{a_n}{d}) = d\ \text{μκδ}(\frac{a_1}{d}, \ldots, \frac{a_n}{d})$ (σύμφωνα με το (i)), οπότε λαμβάνουμε $\text{μκδ}(\frac{a_1}{d}, \ldots, \frac{a_n}{d}) = 1$.

(iii) Κατόπιν εισαγωγής των συντομογραφιών

$$\text{μκδ}(a_1, \ldots, a_n) =: d, \qquad \text{μκδ}(a_1 + \nu_2 a_2 + \cdots + \nu_n a_n, a_2, ..., a_n) =: d',$$

παρατηρούμε ότι $[d \mid a_j \Rightarrow d \mid \nu_j a_j, \forall j \in \{2, .., n\}] \Rightarrow d \mid a_1 + \nu_2 a_2 + \cdots + \nu_n a_n$. Κατά το πόρισμα 2.2.6, $d \mid d'$. Και αντιστρόφως· επειδή

$$d' \mid a_1 + \nu_2 a_2 + \cdots + \nu_n a_n \quad \text{και} \quad \left[d' \mid a_j \Longrightarrow d' \mid \nu_j a_j,\ \forall j \in \{2, \ldots, n\}\right],$$

έχουμε $d' \mid a_1 + \nu_2 a_2 + \cdots + \nu_n a_n - (\nu_2 a_2 + \cdots + \nu_n a_n)$, ήτοι $d' \mid a_1$, οπότε $d' \mid a_j$, για κάθε $j \in \{1, 2, \ldots, n\}$, απ' όπου έπεται ότι $d' \mid d$ (βλ. 2.2.6). Επειδή $d, d' \in \mathbb{N}$, οι σχέσεις διαιρετότητας $d \mid d'$ και $d' \mid d$ δίδουν $d = d'$ (βλ. 2.1.5 (iii)). □

2.2.15 Πόρισμα. *Εάν $m, n \in \mathbb{N}$ και $a \in \mathbb{N}$, $a \geqslant 2$, τότε*

$$\text{μκδ}(a^m - 1, a^n - 1) = a^{\text{μκδ}(m,n)} - 1.$$

ΑΠΟΔΕΙΞΗ. Θέτοντας $d := \text{μκδ}(a^m - 1, a^n - 1)$, $\delta := \text{μκδ}(m, n)$ και $\mathfrak{d} := \text{μκδ}(d, a)$ παρατηρούμε εν πρώτοις ότι

$$a^m - 1 = (a^\delta)^{\frac{m}{\delta}} - 1 = (a^\delta - 1)((a^\delta)^{\frac{m}{\delta}-1} + (a^\delta)^{\frac{m}{\delta}-2} + \cdots + 1),$$

οπότε $a^\delta - 1 \mid a^m - 1$. Κατ' αναλογίαν, $a^\delta - 1 \mid a^n - 1$. Από το πόρισμα 2.2.6 έπεται ότι $a^\delta - 1 \mid d$. Εν συνεχεία, παρατηρούμε ότι μκδ$(\frac{m}{\delta}, \frac{n}{\delta}) = 1$ (βλ. 2.2.14 (ii)), οπότε (κατόπιν εφαρμογής τού πορίσματος 2.2.11) υπάρχουν $\kappa, \lambda \in \mathbb{N}$, τέτοιοι ώστε να ισχύει

$$\kappa\tfrac{m}{\delta} - \lambda\tfrac{n}{\delta} = 1 \Longrightarrow \kappa m - \lambda n = \delta.$$

Σημειωτέον ότι

$$[d \mid a^m - 1 \text{ και } a^m - 1 \mid a^{\kappa m} - 1] \underset{2.1.5\,(v)}{\Longrightarrow} d \mid a^{\kappa m} - 1$$

και, παρομοίως, $d \mid a^{\lambda n} - 1$. Εξ αυτών προκύπτει ότι

$$d \mid ((a^{\kappa m} - 1) - (a^{\lambda n} - 1)) = a^{\kappa m} - a^{\lambda n} = a^{\lambda n}(a^{\kappa m - \lambda n} - 1) = a^{\lambda n}(a^\delta - 1).$$

(Βλ. 2.1.5 (vi).) Επειδή $\mathfrak{d} \mid a \Rightarrow \mathfrak{d} \mid a^m$ και $[\mathfrak{d} \mid d \text{ και } d \mid a^m - 1] \underset{2.1.5\,(v)}{\Longrightarrow} \mathfrak{d} \mid a^m - 1$, έχουμε $\mathfrak{d} \mid a^m - (a^m - 1) = 1 \Rightarrow \mathfrak{d} = 1$ και

$$\left.\begin{array}{r} d \mid a^{\lambda n}(a^\delta - 1) \\ \mathfrak{d} = \text{μκδ}(d, a) = 1 \underset{2.2.13}{\Longrightarrow} \text{μκδ}(d, a^{\lambda n}) = 1 \end{array}\right\} \underset{2.2.9}{\Longrightarrow} d \mid a^\delta - 1.$$

Άρα τελικώς, $d = a^\delta - 1$. □

2.2.16 Πρόταση. *Εάν $n \in \mathbb{N}$, $n \geqslant 3$, και εάν $a_1, \ldots, a_n \in \mathbb{Z}\setminus\{0\}$, τότε για κάθε $k \in \mathbb{Z}$, $1 \leqslant k \leqslant n-2$, ισχύει η ισότητα*

$$\boxed{\text{μκδ}(a_1, \ldots, a_n) = \text{μκδ}(a_1, \ldots, a_k,\ \text{μκδ}(a_{k+1}, \ldots, a_n)).} \tag{2.7}$$

Απόδειξη. Επειδή μκδ$(a_1, \ldots, a_n) \mid a_j$ για κάθε $j \in \{k+1, \ldots, n\}$ έχουμε

$$\text{μκδ}(a_1, \ldots, a_n) \mid \text{μκδ}(a_{k+1}, \ldots, a_n).$$

Κατά συνέπειαν, μκδ$(a_1, \ldots, a_n) \mid a_j$ για οιονδήποτε δείκτη $j \in \{1, \ldots, n\}$ και μκδ$(a_1, \ldots, a_n) \mid$μκδ$(a_{k+1}, \ldots, a_n)$, απ' όπου συνάγεται ότι

$$\text{μκδ}(a_1, \ldots, a_n) \mid \text{μκδ}(a_1, \ldots, a_k, \text{μκδ}(a_{k+1}, \ldots, a_n)). \tag{2.8}$$

Και αντιστρόφως· μκδ$(a_1, \ldots, a_k,$ μκδ$(a_{k+1}, \ldots, a_n)) \mid a_j$ για κάθε $j \in \{1, \ldots, k\}$ και

$$\text{μκδ}(a_1, \ldots, a_k, \text{μκδ}(a_{k+1}, \ldots, a_n)) \mid \text{μκδ}(a_{k+1}, \ldots, a_n),$$

οπότε μκδ$(a_1, \ldots, a_k,$ μκδ$(a_{k+1}, \ldots, a_n)) \mid a_j$ για κάθε $j \in \{1, \ldots, n\}$, που σημαίνει ότι

$$\text{μκδ}(a_1, \ldots, a_k, \text{μκδ}(a_{k+1}, \ldots, a_n)) \mid \text{μκδ}(a_1, \ldots, a_n). \tag{2.9}$$

Επειδή οι προκείμενοι μέγιστοι κοινοί διαιρέτες είναι > 0, από τις (2.8), (2.9) και το (iii) τής προτάσεως 2.1.5 συμπεραίνουμε την ισχύ τής ισότητας (2.7). □

2.2.17 Παρατήρηση. Θέτοντας $k = 1$ και εφαρμόζοντας τον τύπο (2.7) $n - 1$ φορές είναι δυνατή η αναγωγή τής ευρέσεως τού μεγίστου κοινού διαιρέτη $n \geqslant 3$ μη μηδενικών ακεραίων αριθμών $a_1, \ldots, a_n$ στην εύρεση τού μεγίστου κοινού διαιρέτη $n - 1$ *ζευγών* μη μηδενικών ακεραίων.

▸ **Ευκλείδειος αλγόριθμος προσδιορισμού μκδ.** Ο υπολογισμός τού μεγίστου κοινού διαιρέτη *δύο* τυχόντων μη μηδενικών ακεραίων $r_0 = a$, $r_1 = b$ μπορεί να εκτελεσθεί με τη βοήθεια τού λεγομένου *Ευκλειδείου αλγορίθμου*, ο οποίος βασίζεται στη χρήση πεπερασμένου πλήθους ταυτοτήτων τής Ευκλειδείου διαιρέσεως (2.1) ως ακολούθως: Επειδή

$$\text{μκδ}(a,b) = \text{μκδ}(|a|,|b|)$$

μπορούμε -χωρίς βλάβη τής γενικότητας- να υποθέσουμε ότι $a \geqslant b > 0$. Κατά το θεώρημα 2.1.6 υπάρχουν μονοσημάντως ορισμένα ζεύγη ακεραίων αριθμών (q_j, r_j), $1 \leqslant j \leqslant n+1$, ούτως ώστε να ισχύουν οι ισότητες:

$$\begin{cases} r_0 = r_1 q_1 + r_2, & 0 \leqslant r_2 < r_1 \\ r_1 = r_2 q_2 + r_3, & 0 \leqslant r_3 < r_2 \\ r_2 = r_3 q_3 + r_4, & 0 \leqslant r_4 < r_3 \\ \cdots\cdots & \cdots\cdots \\ r_{n-2} = r_{n-1} q_{n-1} + r_n, & 0 \leqslant r_n < r_{n-1} \\ r_{n-1} = r_n q_n + r_{n+1}, & 0 \leqslant r_{n+1} < r_n. \end{cases} \tag{2.10}$$

(Εάν υπάρχει r_j, $j \geqslant 2$, με $r_j = 0$, τότε σταματούμε). Εξ αυτών συνάγεται -ιδιαιτέρως- ότι $0 \leqslant r_{n+1} < r_n < r_{n-1} < \cdots < r_3 < r_2 < r_1 \leqslant r_0$. Εάν υποθέταμε ότι για *κάθε* φυσικό αριθμό n το υπόλοιπο r_{n+1} είναι $\neq 0$, θα καταλήγαμε στο συμπέρασμα ότι μεταξύ τού 0 και τού $r_0 = a$ υπάρχουν *άπειροι* (σαφώς διακεκριμένοι) φυσικοί αριθμοί, κάτι που θα ήταν άτοπο. Ως εκ τούτου, υπάρχει (κατ' ανάγκην) κάποιος φυσικός αριθμός, ας τον πούμε n_*, για τον οποίο $r_{n_*} \neq 0$ και $r_{n_*+1} = 0$.

2.2.18 Πρόταση (Ευκλείδειος αλγόριθμος). *Ο μέγιστος κοινός διαιρέτης των a και b είναι ο*

$$\boxed{\text{μκδ}(a,b) = r_{n_*}.} \tag{2.11}$$

Απόδειξη. Σύμφωνα με την πρόταση 2.2.14 (iii) έχουμε

$$\text{μκδ}(a,b) = \text{μκδ}(r_0,r_1) = \text{μκδ}(r_1,r_0) = \text{μκδ}(r_1, r_1q_1 + r_2) = \text{μκδ}(r_1,r_2)$$

και $\text{μκδ}(r_1,r_2) = \text{μκδ}(r_2,r_3) = \cdots = \text{μκδ}(r_{n_*-1}, r_{n_*}) = \text{μκδ}(r_{n_*}q_{n_*}, r_{n_*}) = r_{n_*}$, απ' όπου έπεται η ισότητα (2.11). □

2.2.19 Παράδειγμα. Ο μέγιστος κοινός διαιρέτης των $a = 240$ και $b = 50$, λαμβανομένου υπ' όψιν ότι $240 = 50 \cdot 4 + 40$, $50 = 40 \cdot 1 + 10$, $40 = 10 \cdot 4 + 0$, υπολογίζεται μέσω των ισοτήτων $\text{μκδ}(240,50) = \text{μκδ}(50,40) = \text{μκδ}(40,10) = 10$.

2.2.20 Σημείωση. Το θεώρημα 2.2.5 μας πληροφορεί ότι ο μέγιστος κοινός διαιρέτης n μη μηδενικών ακεραίων αριθμών (όπου $n \geqslant 2$) εκφράζεται ως ακέραιος γραμμικός συνδυασμός αυτών των αριθμών. Ωστόσο, εξαιτίας τής καθαρώς «υπαρξιακής» αποδείξεώς του, δεν μας παρέχει καμία πληροφορία για τον τρόπο *υπολογισμού* των συντελεστών τού εν λόγω γραμμικού συνδυασμού. Αντιθέτως, όταν $n = 2$, ο Ευκλείδειος αλγόριθμος μας διασφαλίζει κατά τρόπο *κατασκευαστικό* ένα *φυσικό ζεύγος* ακεραίων, οι οποίοι παίζουν τον ρόλο συντελεστών τού $\text{μκδ}(a,b)$ ως ακεραίου γραμμικού συνδυασμού των a και b, ως ακολούθως:

2.2.21 Πρόταση. *Εάν $a, b \in \mathbb{Z} \setminus \{0\}$ και $a \geqslant b$, τότε*

$$\boxed{\text{μκδ}(a,b) = s_{n_*}a + t_{n_*}b,} \tag{2.12}$$

με $s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$ και $s_j = s_{j-2} - q_{j-1}s_{j-1}$, $t_j = t_{j-2} - q_{j-1}t_{j-1}$,

για κάθε $j \in \{2, \dots, n_*\}$, όπου τα $q_1, q_2, \dots, q_{n_*-1}$ είναι τα πηλίκα των διαιρέσεων (2.10) των εμφανιζομένων κατά την εκτέλεση τού Ευκλειδείου αλγορίθμου για τον προσδιορισμό τού μκδ(a, b) *και n_* ο ληκτικός του φυσικός αριθμός (για τον οποίο $r_{n_*} \neq 0$ και $r_{n_*+1} = 0$).*

Αποδειξη. Χρησιμοποιώντας τις διαιρέσεις (2.10) θα αποδείξουμε τις ισότητες

$$r_j = s_j a + t_j b, \quad \forall j \in \{0, 1, \dots, n_*\}, \tag{2.13}$$

απ' όπου προκύπτει η (2.12), λόγω τού ότι μκδ$(a, b) = r_{n_*}$. Αρκεί να εργασθούμε επαγωγικώς ως προς τον j. Για $j = 0$ έχουμε $a = r_0 = 1 \cdot a + 0 \cdot b = s_0 a + t_0 b$, ενώ για $j = 1$, $b = r_1 = 0 \cdot a + 1 \cdot b = s_1 a + t_1 b$. Υποθέτοντας ότι $r_j = s_j a + t_j b$ για κάθε $j \in \{1, \dots, k-1\}$, όπου $1 \leqslant k \leqslant n_*$, έχουμε $r_k = r_{k-2} - r_{k-1} q_{k-1}$, οπότε, λόγω τής επαγωγικής υποθέσεώς μας,

$$\begin{aligned} r_k &= (s_{k-2} a + t_{k-2} b) - (s_{k-1} a + t_{k-1} b)\, q_{k-1} \\ &= (s_{k-2} - s_k q_{k-1})\, a + (t_{k-2} - t_{k-1} q_{k-1})\, b = s_k a + t_k b, \end{aligned}$$

απ' όπου έπεται το ζητούμενο[3]. □

2.2.22 Παρατήρηση. (i) Χρησιμοποιώντας $n - 1$ φορές την (2.7) (για $k = 1$, βλ. παρατήρηση 2.2.17) και την ισότητα (2.12) είναι δυνατός ο υπολογισμός *συγκεκριμένων* συντελεστών $k_1, \dots, k_n \in \mathbb{Z}$ τού $d =$ μκδ$(a_1, \dots, a_n)$ για την έκφρασή του ως γραμμικού συνδυασμού (2.6). Ωστόσο, θα πρέπει εδώ να τονισθεί ότι η επιλογή ακεραίων $k_1, \dots, k_n$, τέτοιων ώστε να ισχύει η (2.6) δεν είναι κατά κανέναν τρόπο μονοσημάντως ορισμένη!

(ii) Για να καταστεί περισσότερο σαφές το ότι η επιλογή των ως άνω συντελεστών δεν είναι μονοσημάντως ορισμένη *ακόμη και για* $n = 2$, θεωρούμε δυο ακεραίους $a, b \in \mathbb{Z} \setminus \{0\}$ και θέτουμε $d :=$ μκδ(a, b). Εάν $d = sa + tb$ για κατάλληλους $s, t \in \mathbb{Z}$, τότε

$$d = (s + k\left(\tfrac{b}{d}\right))a + (t - k\left(\tfrac{a}{d}\right))b, \quad \forall k \in \mathbb{Z}.$$

2.2.23 Ορισμός. Έστω ότι $n \in \mathbb{N}$ και ότι οι $a_1, \dots, a_n$ είναι ακέραιοι αριθμοί. Ένας ακέραιος l καλείται **κοινό πολλαπλάσιο** των $a_1, .., a_n$ όταν $a_1 \mid l, .., a_n \mid l$. (Σημειωτέον ότι εάν ένας εκ των $a_1, \dots, a_n$ είναι ίσος με το 0, τότε το μοναδικό πολλαπλάσιό τους είναι το 0).

2.2.24 Ορισμός. Έστω ότι $n \in \mathbb{N}$ και ότι $a_1, \dots, a_n \in \mathbb{Z} \setminus \{0\}$. Προφανώς, ο φυσικός αριθμός $|a_1 \cdots a_n|$ είναι ένα κοινό πολλαπλάσιο των $a_1, \dots, a_n$. Ως εκ τούτου, το σύνολο των θετικών πολλαπλασίων των $a_1, \dots, a_n$ είναι μη κενό και διαθέτει ένα και μόνον *ελάχιστο* στοιχείο. Το στοιχείο αυτό καλείται **ελάχιστο κοινό πολλαπλάσιο** των $a_1, \dots, a_n$ και συμβολίζεται ως εκπ$(a_1, \dots, a_n)$. Επειδή το σύνολο των θετικών πολλαπλασίων των $a_1, \dots, a_n$ ισούται με το σύνολο των θετικών πολλαπλασίων των $|a_1|, \dots, |a_n|$, συμπεραίνουμε ότι

$$\text{εκπ}(a_1, \dots, a_n) = \text{εκπ}(|a_1|, \dots, |a_n|).$$

(*Σύμβαση*: Είναι δυνατή η επέκταση τής εννοίας τού ελαχίστου κοινού πολλαπλασίου ακόμη και όταν *τουλάχιστον ένας* εκ των $a_1, \dots, a_n$ είναι $= 0$. Εν τοιαύτη περιπτώσει θέτουμε εκπ$(a_1, \dots, a_n) := 0$.)

[3] Για τον συσχετισμό αυτών των πεπερασμένων ακολουθιών με την κατά αρκετά κομψό τρόπο παράσταση τού πηλίκου τού $\frac{a}{b} = \frac{a/\text{μκδ}(a,b)}{b/\text{μκδ}(a,b)}$ ως *πεπερασμένου συνεχούς κλάσματος*, πρβλ. D. Burton: *Elementary Number Theory*, seventh ed., McGraw-Hill Co., 2011, εν. 15.2, σελ. 315-317.

2.2.25 Πρόταση. *Εάν* $n \in \mathbb{N}$ *και εάν* $a_1, \ldots, a_n \in \mathbb{Z}\setminus\{0\}$, *τότε ένας* $m \in \mathbb{N}$ *ισούται με το* εκπ$(a_1, \ldots, a_n)$ *εάν και μόνον εάν ισχύουν τα ακόλουθα*:
(i) $a_1 \mid m, \ldots, a_n \mid m$,
(ii) *για οιονδήποτε* $l \in \mathbb{N}$, *για τον οποίο ισχύει* $a_1 \mid l, \ldots, a_n \mid l$, *έχουμε* $m \mid l$.

Απόδειξη. Εάν $m = \text{εκπ}(a_1, \ldots, a_n)$, τότε εξ ορισμού $a_1 \mid m, \ldots, a_n \mid m$, οπότε ισχύει το (i). Εξάλλου, για οιονδήποτε $l \in \mathbb{N}$, για τον οποίο ισχύει $a_1 \mid l, \ldots, a_n \mid l$, υπάρχει (κατά το 2.1.6) ένα μονοσημάντως ορισμένο ζεύγος $(q, r) \in \mathbb{Z} \times \mathbb{Z}$, ούτως ώστε να ισχύει $l = qm + r$, όπου $0 \leqslant r < m$. Επειδή

$$[a_1 \mid m, \ldots, a_n \mid m \text{ και } a_1 \mid l, \ldots, a_n \mid l] \Rightarrow a_1 \mid r, \ldots, a_n \mid r,$$

το r είναι ένα κοινό πολλαπλάσιο των $a_1, \ldots, a_n$. Άρα $r = 0$ (διότι εάν $r > 0$, θα είχαμε $r \geqslant m$, ήτοι κάτι το άτοπο), οπότε ισχύει και το (ii).

Και αντιστρόφως· υποθέτοντας την ισχύ των ιδιοτήτων (i) και (ii) για έναν θετικό ακέραιο m, ο m είναι ένα κοινό πολλαπλάσιο των $a_1, \ldots, a_n$ και για οιοδήποτε κοινό πολλαπλάσιο l των ακεραίων $a_1, \ldots, a_n$ έχουμε $m \mid l$, απ' όπου συμπεραίνουμε ότι $m \leqslant l$, ήτοι ότι ισχύει $m = \text{εκπ}(a_1, \ldots, a_n)$. □

2.2.26 Πρόταση. *Εάν* $n \in \mathbb{N}$ *και* $\lambda, a_1, \ldots, a_n \in \mathbb{Z}\setminus\{0\}$, *τότε ισχύουν τα εξής*:
(i) $\text{εκπ}(\lambda a_1, \ldots, \lambda a_n) = |\lambda|\ \text{εκπ}(a_1, \ldots, a_n)$.
(ii) *Εάν* $\text{εκπ}(a_1, \ldots, a_n) = m$, *τότε* $\text{μκδ}(\frac{m}{a_1}, \ldots, \frac{m}{a_n}) = 1$.

Απόδειξη. (i) Εάν $\text{εκπ}(a_1, \ldots, a_n) = m$, τότε για κάθε $j \in \{1, \ldots, n\}$

$$a_j \mid m \Longrightarrow \lambda a_j \mid |\lambda|\, m,$$

οπότε, δυνάμει τής προτάσεως 2.2.25, $\text{εκπ}(\lambda a_1, \ldots, \lambda a_n) \mid |\lambda|\, m$. Επιπροσθέτως,

$$\lambda a_j \mid \text{εκπ}(\lambda a_1, \ldots, \lambda a_n) \Longrightarrow a_j \mid \tfrac{\text{εκπ}(\lambda a_1, \ldots, \lambda a_n)}{|\lambda|},\ \forall j \in \{1, \ldots, n\},$$

οπότε $m \mid \frac{\text{εκπ}(\lambda a_1, \ldots, \lambda a_n)}{|\lambda|} \Longrightarrow |\lambda|\, m \mid \text{εκπ}\,(\lambda a_1, \ldots, \lambda a_n)$. Επομένως,

$$\left.\begin{array}{l} |\lambda|\, m \mid \text{εκπ}(\lambda a_1, \ldots, \lambda a_n) \\ \text{εκπ}(\lambda a_1, \ldots, \lambda a_n) \mid |\lambda|\, m \end{array}\right\} \Longrightarrow \text{εκπ}(\lambda a_1, \ldots, \lambda a_n) = |\lambda|\, m.$$

(ii) Επειδή $\text{μκδ}(\frac{m}{a_1}, \ldots, \frac{m}{a_n}) \mid \frac{m}{a_j}$ για κάθε $j \in \{1, \ldots, n\}$, έχουμε

$$\exists b_j \in \mathbb{Z} : m = \text{μκδ}(\tfrac{m}{a_1}, \ldots, \tfrac{m}{a_n}) a_j b_j \Rightarrow \text{μκδ}(\tfrac{m}{a_1}, \ldots, \tfrac{m}{a_n}) a_j \mid m$$

για κάθε $j \in \{1, \ldots, n\}$, οπότε (λόγω τής προτάσεως 2.2.25)

$$\text{εκπ}\left(a_1 \text{μκδ}(\tfrac{m}{a_1}, \ldots, \tfrac{m}{a_n}), \ldots, a_n \text{μκδ}(\tfrac{m}{a_1}, \ldots, \tfrac{m}{a_n})\right) \mid m.$$

Επειδή (λόγω τού (i))

$$\text{εκπ}\left(a_1 \text{μκδ}(\tfrac{m}{a_1}, \ldots, \tfrac{m}{a_n}), \ldots, a_n \text{μκδ}(\tfrac{m}{a_1}, \ldots, \tfrac{m}{a_n})\right) = \text{μκδ}(\tfrac{m}{a_1}, \ldots, \tfrac{m}{a_n}) m$$

λαμβάνουμε $\text{εκπ}(\frac{m}{a_1}, \ldots, \frac{m}{a_n}) m \mid m$, οπότε $\text{μκδ}(\frac{m}{a_1}, \ldots, \frac{m}{a_n}) = 1$. □

2.2.27 Πρόταση. *Εάν* $n \in \mathbb{N},\ n \geqslant 3$, *και εάν* $a_1, \ldots, a_n \in \mathbb{Z}\setminus\{0\}$, *τότε για κάθε* $k \in \mathbb{Z}$, $1 \leqslant k \leqslant n-2$, *ισχύει η ισότητα*:

$$\boxed{\text{εκπ}(a_1, \ldots, a_n) = \text{εκπ}(a_1, \ldots, a_k, \text{εκπ}(a_{k+1}, \ldots, a_n)).} \tag{2.14}$$

Απόδειξη. Επειδή $a_j \mid \text{εκπ}(a_1, \ldots, a_n)$ για κάθε $j \in \{k+1, \ldots, n\}$ έχουμε

$$\text{εκπ}(a_{k+1}, \ldots, a_n) \mid \text{εκπ}(a_1, \ldots, a_n).$$

Άρα $a_j \mid \text{εκπ}(a_1, \ldots, a_n), \forall j \in \{1, .., n\}$ και $\text{εκπ}(a_{k+1}, \ldots, a_n) \mid \text{εκπ}(a_1, \ldots, a_n)$, απ' όπου συνάγεται ότι

$$\text{εκπ}(a_1, \ldots, a_k, \text{εκπ}(a_{k+1}, \ldots, a_n)) \mid \text{εκπ}(a_1, \ldots, a_n). \tag{2.15}$$

Και αντιστρόφως· $\text{μκδ}(a_1, \ldots, a_k, \text{μκδ}(a_{k+1}, \ldots, a_n)) \mid a_j$ για κάθε $j \in \{1, \ldots, k\}$ και

$$\text{εκπ}(a_{k+1}, \ldots, a_n) \mid \text{εκπ}(a_1, \ldots, a_k, \text{εκπ}(a_{k+1}, \ldots, a_n)),$$

οπότε $a_j \mid \text{εκπ}(a_1, \ldots, a_k, \text{εκπ}(a_{k+1}, \ldots, a_n))$ για κάθε $j \in \{1, \ldots, n\}$, που σημαίνει ότι

$$\text{εκπ}(a_1, \ldots, a_n) \mid \text{εκπ}(a_1, \ldots, a_k, \text{εκπ}(a_{k+1}, \ldots, a_n)). \tag{2.16}$$

Επειδή τα προκείμενα ελάχιστα κοινά πολλαπλάσια είναι θετικοί ακέραιοι, από τις (2.15), (2.16) και το (iii) τής προτάσεως 2.1.5 συμπεραίνουμε την ισχύ τής ισότητας (2.14). □

2.2.28 Παρατήρηση. Θέτοντας $k = 1$ και εφαρμόζοντας τον τύπο (2.14) $n-1$ φορές είναι εμφανώς δυνατή η αναγωγή τής ευρέσεως τού ελαχίστου κοινού πολλαπλασίου $n \geqslant 3$ μη μηδενικών ακεραίων αριθμών $a_1, \ldots, a_n$ στην εύρεση τού ελαχίστου κοινού πολλαπλασίου $n-1$ *ζευγών* μη μηδενικών ακεραίων. Επιπροσθέτως, ο υπολογισμός τού ελαχίστου κοινού πολλαπλασίου *δύο* μη μηδενικών ακεραίων μπορεί να αναχθεί απευθείας στον υπολογισμό τού μεγίστου κοινού διαιρέτη τους, εάν ληφθεί υπ' όψιν ο τύπος (2.17), τον οποίο αποδεικνύουμε στην επομένη πρόταση.

2.2.29 Πρόταση. *Για οιουσδήποτε* $a, b \in \mathbb{Z}\setminus\{0\}$ *έχουμε*

$$\boxed{\text{μκδ}(a,b)\ \text{εκπ}(a,b) = |ab|\,.} \tag{2.17}$$

Απόδειξη. Επειδή $\text{μκδ}(a,b) \mid a$ και $\text{μκδ}(a,b) \mid b$, έχουμε

$$\text{μκδ}(a,b) \mid |ab|\,.$$

Αρκεί λοιπόν να αποδείξουμε ότι ο θετικός ακέραιος αριθμός $\frac{|ab|}{\text{μκδ}(a,b)}$ ισούται με το $\text{εκπ}(a,b)$. Προς τούτο θα χρησιμοποιήσουμε την πρόταση 2.2.25. Κατ' αρχάς, $a \mid \frac{|ab|}{\text{μκδ}(a,b)}$ και $b \mid \frac{|ab|}{\text{μκδ}(a,b)}$. Ας υποθέσουμε ότι ο l είναι ενας θετικός ακέραιος, για τον οποίο ισχύει $a \mid l$ και $b \mid l$. Κατά το θεώρημα 2.2.5, υπάρχουν ακέραιοι αριθμοί s, t, τέτοιοι ώστε να ισχύει η ισότητα:

$$\text{μκδ}(a,b) = sa + tb.$$

Συνεπώς,

$$\frac{l}{\frac{|ab|}{\text{μκδ}(a,b)}} = \frac{\text{μκδ}(a,b)l}{|ab|} = \frac{(sa+tb)\,l}{|ab|} = \left(\text{sign}\,(a)\,\tfrac{l}{|b|}\right)s + \left(\text{sign}\,(b)\,\tfrac{l}{|a|}\right)t \in \mathbb{Z},$$

πράγμα που σημαίνει ότι $\frac{|ab|}{\text{μκδ}(a,b)} \mid l$, οπότε κατ' ανάγκην $\frac{|ab|}{\text{μκδ}(a,b)} = \text{εκπ}(a,b)$. □

‣ **Περί των συνδέσμων** $(\mathbb{N}, |), (\mathbb{N}_0, |)$. Μέσω τής σχέσεως διαιρετότητας τα σύνολα των φυσικών και των μη αρνητικών ακεραίων καθίστανται *σύνδεσμοι*.

2.2.30 Πρόταση. *Τα ζεύγη $(\mathfrak{X}, |)$, όπου $\mathfrak{X} \in \{\mathbb{N}, \mathbb{N}_0\}$ και " $|$ " η συνήθης σχέση διαιρετότητας*

$$[a \mid b \underset{\text{ορσ}}{\iff} \exists c \in \mathbb{Z} : b = ac],\ \forall (a,b) \in \mathfrak{X} \times \mathfrak{X},$$

αποτελούν μερικώς (μη ολικώς) διατεταγμένα σύνολα.

(Εάν $(a,b) \in \mathfrak{X} \times \mathfrak{X}$ και εάν $\exists c \in \mathbb{Z} : b = ac$, τότε κατ' ανάγκην $c \in \mathfrak{X}$. Κατά συνέπειαν, $[a \mid b \Leftrightarrow \exists c \in \mathfrak{X} : b = ac]$ για κάθε ζεύγος $(a,b) \in \mathfrak{X} \times \mathfrak{X}$.)

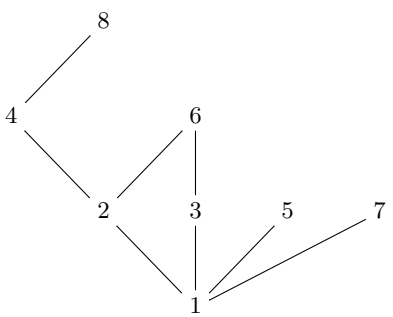
Απόδειξη. Η αυτοπάθεια και η μεταβατικότητα τής " $|$ " έπεται από το (v) τής προτάσεως 2.1.3 και το (v) τής προτάσεως 2.1.5. Επιπροσθέτως, για κάθε ζεύγος $(a,b) \in \mathfrak{X} \times \mathfrak{X}$ με $a \mid b$ και $b \mid a$, ισχύει $a = |a| = |b| = b$ (λόγω τού (iii) τής προτάσεως 2.1.5). Άρα η " $|$ " είναι *και* αντισυμμετρική επί τού $\mathfrak{X}$. Ωστόσο, το $(\mathfrak{X}, |)$ δεν είναι ολικώς διατεταγμένο σύνολο, διότι π.χ. $2 \nmid 3$. □

2.2.31 Παρατήρηση. Προσοχή! Το ζεύγος $(\mathbb{Z}, |)$ δεν είναι μερικώς διατεταγμένο σύνολο, καθότι η " $|$ " δεν είναι αντισυμμετρική επί τού $\mathbb{Z}$. Π.χ., $2 \mid -2$ και $-2 \mid 2$, αλλά $2 \neq -2$.

2.2.32 Παράδειγμα. Θεωρούμε τα μερικώς διατεταγμένα σύνολα $(\mathbb{N}, |)$, $(\mathbb{N}, \leqslant)$ (βλ. 2.2.30). Η ταυτοτική απεικόνιση id: $(\mathbb{N}, |) \longrightarrow (\mathbb{N}, \leqslant)$ είναι αμφιρριπτική και ισότονη από το ένα επί τού άλλου (διότι για $k, n \in \mathbb{N}$ ισχύει η συνεπαγωγή $k \mid n \Rightarrow k \leqslant n$) αλλά *δεν είναι* ισομορφισμός μερικώς διατεταγμένων συνόλων (υπό την έννοια τού ορισμού 1.4.8), διότι π.χ. $2 \leqslant 3$ και $2 \nmid 3$.

2.2.33 Σημείωση. Πολλά χρήσιμα (αριθμοθεωρητικά) παραδείγματα μερικώς διατεταγμένων συνόλων παρέχονται από *πεπερασμένα* υποσύνολα τού $\mathbb{N}$ (εφοδιαζόμενα με τη μερική διάταξη διαιρετότητας την επαγομένη επ' αυτών). Ενδεικτικώς αναφέρονται τα ακόλουθα:

(i) Θεωρούμε το $(\mathfrak{X}, |)$, όπου $\mathfrak{X} := \{1,2,3,4,5,6,7,8\}$. Οι αριθμοί $5, 6, 7$ και 8 είναι τα μεγιστικά στοιχεία τού $\mathfrak{X}$, ενώ το 1 είναι το ελάχιστο στοιχείο του (ως προς την " $|$ "). Το $\mathfrak{X}$ *δεν διαθέτει* μέγιστο στοιχείο. Το αντίστοιχο διάγραμμα τού Hasse για το $(\mathfrak{X}, |)$ είναι το



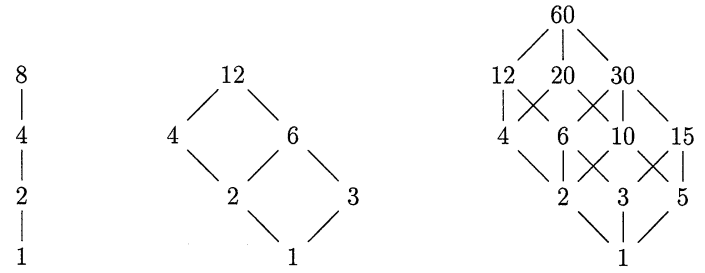
(ii) Θεωρούμε το μερικώς διατεταγμένο σύνολο $(\mathfrak{X}, |)$, όπου $\mathfrak{X} = \{3, 5, 30, 45\}$, καθώς και το $\mathfrak{Y} := \{3, 5\}$. Εν προκειμένω, $\mathrm{A}\Phi(\mathfrak{Y}; \mathfrak{X}) = \{30, 45\}$, αλλά το $\mathfrak{Y}$ δεν διαθέτει ελάχιστο άνω φράγμα εντός τού $\mathfrak{X}$ ως προς την "$|$".

2.2.34 Παράδειγμα. Έστω $m \in \mathbb{N}$. Το σύνολο

$$\boxed{\mathfrak{D}_m := \{d \in \mathbb{N} : d \mid m\}}$$

όλων των θετικών ακεραίων διαιρετών τού m καθίσταται μερικώς διατεταγμένο μέσω τής σχέσεως διαιρετότητας " $|$ " την επαγομένη από το $(\mathbb{N}, |)$ (βλ. 2.2.30).

(i) Τα διαγράμματα τού Hasse για τα $(\mathfrak{D}_8, |)$, $(\mathfrak{D}_{12}, |)$ και $(\mathfrak{D}_{60}, |)$, αντιστοίχως, είναι τα ακόλουθα:



(ii) Τα μερικώς διατεταγμένα σύνολα $(\mathfrak{D}_{30}, |)$ και $(\mathfrak{P}(\Omega), \subseteq)$, όπου $\Omega := \{\spadesuit, \clubsuit, \heartsuit\}$ (όπως στο 1.4.5), είναι ισόμορφα, καθότι η αμφίρριψη

$$1 \longmapsto \varnothing,\ 2 \longmapsto \{\spadesuit\},\ 3 \longmapsto \{\heartsuit\},\ 5 \longmapsto \{\clubsuit\},$$
$$6 \longmapsto \{\spadesuit, \heartsuit\},\ 10 \longmapsto \{\spadesuit, \clubsuit\},\ 15 \longmapsto \{\clubsuit, \heartsuit\},\ 30 \longmapsto \Omega$$

είναι ισότονη και έχει ισότονη αντίστροφο.

2.2.35 Πρόταση. *Το μερικώς διατεταγμένο σύνολο* $(\mathfrak{X}, |)$, *όπου* $\mathfrak{X} \in \{\mathbb{N}, \mathbb{N}_0\}$, *αποτελεί έναν σύνδεσμο με* $m \wedge n = \text{μκδ}(m,n),\ m \vee n = \text{εκπ}(m,n),\ \forall (m,n) \in \mathfrak{X} \times \mathfrak{X}$.

(Σημειωτέον ότι για $\mathfrak{X} = \mathbb{N}_0$ έχουμε $m \wedge 0 = 0 \wedge m = m$ και $m \vee 0 = 0 \vee m = 0$, για κάθε $m \in \mathbb{N}_0$.)

Απόδειξη. Επειδή $\text{μκδ}(m,n) \mid m$ και $\text{μκδ}(m,n) \mid n$, για κάθε $(m,n) \in \mathfrak{X} \times \mathfrak{X}$, ο μέγιστος κοινός διαιρέτης $\text{μκδ}(m,n)$ των m και n αποτελεί κάτω φράγμα τού $\{m,n\}$ εντός τού $\mathfrak{X}$ ως προς την "|", και μάλιστα το *μέγιστο κάτω φράγμα*, διότι για οιονδήποτε $\delta \in \mathfrak{X}$, για τον οποίο ισχύει $\delta \mid m$ και $\delta \mid n$, έχουμε $\delta \mid \text{μκδ}(m,n)$. (Τούτο έπεται από το (iii) τής προτάσεως 2.1.3 όταν $\mathfrak{X} = \mathbb{N}_0$ και $\delta = 0$, και από το πόρισμα 2.2.6 όταν $\delta > 0$.) Κατ' αναλογίαν, επειδή $m \mid \text{εκπ}(m,n)$ και $n \mid \text{εκπ}(m,n)$, για κάθε $(m,n) \in \mathfrak{X} \times \mathfrak{X}$, το ελάχιστο κοινό πολλαπλάσιο $\text{εκπ}(m,n)$ των m και n αποτελεί άνω φράγμα τού $\{m,n\}$ εντός τού $\mathfrak{X}$ ως προς την "|", και μάλιστα *ελάχιστο άνω φράγμα*, διότι για οιονδήποτε $l \in \mathfrak{X}$, για τον οποίο ισχύει $m \mid l$ και $n \mid l$, έχουμε $\text{εκπ}(m,n) \mid l$. (Τούτο έπεται από το (i) τής προτάσεως 2.1.3 όταν $\mathfrak{X} = \mathbb{N}_0$ και $mn = 0$, και από την πρόταση 2.2.25 όταν $mn \neq 0$.) □

2.2.36 Πόρισμα. *Έστω* $m \in \mathbb{N}$. *Το μερικώς διατεταγμένο σύνολο* $(\mathfrak{D}_m, |)$ (το ορισθέν στο εδάφιο 2.2.34) *είναι ένας υποσύνδεσμος τού* $(\mathbb{N}, |)$, *διότι*

$$\text{μκδ}(k,l) \in \mathfrak{D}_m, \quad \text{εκπ}(k,l) \in \mathfrak{D}_m, \quad \forall (k,l) \in \mathfrak{D}_m \times \mathfrak{D}_m.$$

Απόδειξη. Εάν $(k,l) \in \mathfrak{D}_m \times \mathfrak{D}_m$, τότε $[\text{μκδ}(k,l) \mid k \text{ και } k \mid m] \underset{2.1.5\,(v)}{\Longrightarrow} \text{μκδ}(k,l) \mid m$ και $\text{εκπ}(k,l) \mid m$ (βλ. πόρισμα 2.3.22). □

2.2.37 Πρόταση. *Εάν* $m_1, \ldots, m_r \in \mathbb{N}$ $(r \in \mathbb{N})$, *τότε*

$$\mathfrak{D}_{\text{μκδ}(m_1,\ldots,m_r)} = \mathfrak{D}_{m_1} \cap \cdots \cap \mathfrak{D}_{m_r}.$$

Απόδειξη. Έπεται άμεσα από το πόρισμα 2.2.6. □

2.3 ΠΡΩΤΟΙ ΑΡΙΘΜΟΙ

2.3.1 Ορισμός. Ένας θετικός ακέραιος αριθμός $p > 1$ καλείται **πρώτος** όταν οι μόνοι διαιρέτες του είναι οι ± 1 και $\pm p$. Ένας πρώτος αριθμός που είναι διαιρέτης ενός ακεραίου m καλείται **πρώτος διαιρέτης** ή **πρώτος παράγοντας** τού m. Ένας φυσικός αριθμός $n \geqslant 2$, ο οποίος δεν είναι πρώτος, καλείται **σύνθετος αριθμός**. Εάν ο n είναι σύνθετος, τότε υπάρχουν φυσικοί αριθμοί n_1, n_2, τέτοιοι ώστε να ισχύει $1 < n_1 \leqslant n_2 < n$ και $n = n_1 n_2$.

2.3.2 Πρόταση. *Κάθε $n \in \mathbb{N}$, $n \geqslant 2$, διαθέτει τουλάχιστον έναν πρώτο διαιρέτη.*

Απόδειξη. Έστω $k := \min\{ m \in \mathbb{N} \mid \ m \geqslant 2 \text{ και } m \mid n\}$. Εάν ο k ήταν σύνθετος αριθμός, τότε θα υπήρχαν $k_1, k_2 \in \mathbb{N}$, τέτοιοι ώστε $2 \leqslant k_1 \leqslant k_2 < k$ και $k = k_1 k_2$, πράγμα άτοπο (αφού $k_1 \mid k$ και $k_2 \mid k$), διότι ο k είναι εξ υποθέσεως ο *ελάχιστος* φυσικός $\geqslant 2$ με αυτήν την ιδιότητα. Άρα ο k είναι πρώτος αριθμός. □

2.3.3 Θεώρημα. *Το σύνολο των πρώτων αριθμών είναι ένα απειροσύνολο.*

Απόδειξη. Ας υποθέσουμε ότι το σύνολο των πρώτων αριθμών είναι πεπερασμένο, ας πούμε το $\{p_1, p_2, \ldots, p_k\}$, κι ας θεωρήσουμε τον $m := p_1 p_2 \cdots p_k + 1$. Τότε ισχύει

$$p_1 \nmid m,\ p_2 \nmid m, \ldots,\ p_k \nmid m$$

(διότι εάν υπήρχε κάποιος $j \in \{1, ..., k\}$ με $p_j \mid m$, θα είχαμε $p_j \mid p_1 p_2 \cdots p_k$, απ' όπου θα προέκυπτε ότι $p_j \mid m - p_1 p_2 \cdots p_k$, ήτοι $p_j \mid 1$, κάτι που θα αντέφασκε προς την ανισότητα $p_j > 1$). Τούτο όμως είναι άτοπο[4] λόγω τής 2.3.2. □

2.3.4 Παρατήρηση. Το σύνολο των πρώτων αριθμών, όντας υποσύνολο τού $\mathbb{N}$, είναι προφανώς *αριθμήσιμο*.

2.3.5 Θεώρημα. *Κάθε $n \in \mathbb{N}$, $n \geqslant 2$, γράφεται ως γινόμενο πρώτων αριθμών.*

Απόδειξη[5]. Θα γίνει χρήση τής δεύτερης μορφής τής μαθηματικής επαγωγής. Για $n = 2$ το θεώρημα είναι αληθές. Υποθέτουμε ότι αυτό συμβαίνει και για τους $2, 3, \ldots, n-1$ και θεωρούμε τον n. Εάν ο n είναι πρώτος, τότε το θεώρημα είναι προφανώς αληθές. Εάν ο n είναι σύνθετος, τότε υπάρχουν φυσικοί αριθμοί n_1, n_2, τέτοιοι ώστε $1 < n_1 \leqslant n_2 < n$ και $n = n_1 n_2$. Λογω τής επαγωγικής υποθέσεώς μας αμφότεροι οι n_1, n_2 παριστώνται ως γινόμενα πρώτων αριθμών. Άρα *και* σε αυτήν την περίπτωση ο n γράφεται ως γινόμενο πρώτων. □

Στην επόμενη ενότητα (και συγκεκριμένα στο θεώρημα 2.4.50) θα δοθεί μια ικανή και αναγκαία συνθήκη, ούτως ώστε ένας ακέραιος > 1 να είναι *πρώτος*.

2.3.6 Λήμμα. *Εάν $m, n \in \mathbb{Z} \setminus \{0, \pm 1\}$ και p είναι ένας πρώτος αριθμός με $p \mid mn$, τότε είτε $p \mid m$ είτε $p \mid n$.*

Απόδειξη. Εάν υποθέσουμε, χωρίς βλάβη τής γενικότητας, ότι $p \nmid m$, τότε μκδ$(p, m) = 1$, οπότε κατ' ανάγκην $p \mid n$ βάσει τού πορίσματος 2.2.9. □

[4] Βλ. Ευκλείδου «Στοιχεία», βιβλίο IX, εδ. 20: «Οι πρώτοι αριθμοί πλείους εισί παντός τού προτεθέντος πλήθους πρώτων». (Πρβλ. Μετάφραση-σχόλια-επεξηγήσεις Ε. Σταμάτη, ΟΕΔΒ, Αθήνα, 1953, σελ. 250-253 και 358-359.)

[5] Βλ. Ευκλείδου «Στοιχεία», βιβλίο VII, εδ. 31: «Άπας σύνθετος αριθμός υπό πρώτου τινός αριθμού μετρείται». (Πρβλ. Μετάφραση-σχόλια-επεξηγήσεις Ε. Σταμάτη, ΟΕΔΒ, Αθήνα, 1953, σελ. 168-171 και 322.)

2.3.7 Λήμμα. *Εάν $k \in \mathbb{N}$ και οι $p, p_1, \dots, p_k$ είναι πρώτοι αριθμοί, τέτοιοι ώστε να ισχύει $p \mid p_1 \cdots p_k$, τότε υπάρχει κάποιος δείκτης $j \in \{1, ..., k\}$, με $p = p_j$.*

Απόδειξη. Επειδή $p \mid p_1 \cdots p_k$, είτε $p \mid p_1$ είτε $p \mid p_2 p_3 \cdots p_k$ (βλ. 2.3.6). Εάν $p \nmid p_1$, τότε $p \mid p_2 p_3 \cdots p_k$, οπότε και πάλι είτε $p \mid p_2$ είτε $p \mid p_3 \cdots p_k$. Κατ' αναλογίαν, εάν $p \nmid p_2$, τότε $p \mid p_3 \cdots p_k$, οπότε ύστερα από την επανάληψη τού ιδίου συλλογισμού (το πολύ $k-1$ φορές) συμπεραίνουμε ότι $p \mid p_j$ για κάποιον δείκτη $j \in \{1, ..., k\}$. Επειδή οι p, p_j είναι πρώτοι, συνάγεται ότι $p = p_j$. □

2.3.8 Θεώρημα (Θεμελιώδες Θεώρημα τής Αριθμητικής). *Κάθε $n \in \mathbb{N}$, $n \geqslant 2$, γράφεται* μονοσημάντως *ως γινόμενο πρώτων αριθμών (μη λαμβανομένης υπ' όψιν τής διατάξεως των εμφανιζομένων παραγόντων εντός αυτού).*

Απόδειξη. Κάτα το θεώρημα 2.3.5 κάθε $n \in \mathbb{N}$, $n \geqslant 2$, μπορεί να παρασταθεί ως γινόμενο πρώτων αριθμών. Αρκεί λοιπόν να αποδειχθεί το *μονοσήμαντο* τής παραστάσεως (μη λαμβανομένης υπ' όψιν τής διατάξεως των εμφανιζομένων παραγόντων εντός αυτής). Προς τούτο υποθέτουμε ότι

$$n = p_1 \cdots p_k = q_1 \cdots q_l, \tag{2.18}$$

όπου $k, l \in \mathbb{N}$ και $p_1, \dots, p_k, q_1, \dots, q_l$ πρώτοι αριθμοί. Επιπροσθέτως, δίχως βλάβη τής γενικότητας, υποθέτουμε ότι $p_1 \leqslant \cdots \leqslant p_k$ και $q_1 \leqslant \cdots \leqslant q_l$. Χρησιμοποιώντας τή δεύτερη μορφή τής μαθηματικής επαγωγής ως προς τον n θα δείξουμε ότι $k = l$ και $p_j = q_j$ για κάθε $j \in \{1, \dots, k\}$. Για $n = 2$ το θεώρημα είναι αληθές. Υποθέτουμε ότι αυτό είναι αληθές και για κάθε φυσικό t, με $2 \leqslant t < n$, όπου n οιοσδήποτε παγιωμένος φυσικός $\geqslant 3$. Εάν ο n είναι πρώτος, τότε ο ισχυρισμός είναι αληθής. Εάν ο n είναι σύνθετος, τότε στην (2.18) έχουμε $k \geqslant 2$ και $l \geqslant 2$. Επειδή ισχύει $p_1 \mid q_1 \cdots q_l$ και $q_1 \mid p_1 \cdots p_k$, υπάρχουν κάποιοι $j \in \{1, ..., k\}$, $\varrho \in \{1, ..., l\}$ με $q_1 = p_j$ και $p_1 = q_\varrho$ (κατά το λήμμα 2.3.7). Εξ αυτού έπεται ότι

$$[p_1 \leqslant p_j = q_1 \text{ και } q_1 \leqslant q_\varrho = p_1] \Longrightarrow p_1 = q_1,$$

οπότε $1 < \frac{n}{p_1} < n$ και

$$\frac{n}{p_1} = p_2 \cdots p_k = q_2 \cdots q_l.$$

Λόγω τής επαγωγικής υποθέσεώς μας έχουμε $k - 1 = l - 1$ και $p_j = q_j$, για κάθε δείκτη $j \in \{2, \dots, k\}$. Ως εκ τούτου, $k = l$ και $p_j = q_j$, για κάθε $j \in \{1, \dots, k\}$. □

2.3.9 Ορισμός. Από το θεώρημα 2.3.8 έπεται ότι κάθε φυσικός αριθμός $n \geqslant 2$ μπορεί να γραφεί *μονοσημάντως* ως

$$\boxed{n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},} \tag{2.19}$$

όπου $k \in \mathbb{N}$, οι $p_1, p_2, \dots, p_k$ είναι σαφώς διακεκριμένοι πρώτοι αριθμοί με

$$p_1 < p_2 < \cdots < p_k$$

(όταν $k \geqslant 2$) και οι $\alpha_1, \alpha_2, \dots, \alpha_k$ φυσικοί αριθμοί. Η έκφραση (2.19) καλείται **κανονική παράσταση τού n ως γινομένου πρώτων αριθμών** ή **κανονική αποσύνθεση τού n σε γινόμενο πρώτων αριθμών** (ή **πρώτων παραγόντων**).

2.3.10 Παράδειγμα. Το 1, καθώς και οι κανονικές παραστάσεις (2.19) όλων των φυσικών αριθμών n, όπου $2 \leqslant n \leqslant 100$, περιλαμβάνονται στον κατάλογο

n	Παρ.	n	Παρ.	n	Παρ.	n	Παρ.	n	Παρ.
1	1	11	11	21	$3 \cdot 7$	31	31	41	41
2	2	12	$2^2 \cdot 3$	22	$2 \cdot 11$	32	2^5	42	$2 \cdot 3 \cdot 7$
3	3	13	13	23	23	33	$3 \cdot 11$	43	43
4	2^2	14	$2 \cdot 7$	24	$2^3 \cdot 3$	34	$2 \cdot 17$	44	$2^2 \cdot 11$
5	5	15	$3 \cdot 5$	25	5^2	35	$5 \cdot 7$	45	$3^2 \cdot 5$
6	$2 \cdot 3$	16	2^4	26	$2 \cdot 13$	36	$2^2 \cdot 3^2$	46	$2 \cdot 23$
7	7	17	17	27	3^3	37	37	47	47
8	2^3	18	$2 \cdot 3^2$	28	$2^2 \cdot 7$	38	$2 \cdot 19$	48	$2^4 \cdot 3$
9	3^2	19	19	29	29	39	$3 \cdot 13$	49	7^2
10	$2 \cdot 5$	20	$2^2 \cdot 5$	30	$2 \cdot 3 \cdot 5$	40	$2^3 \cdot 5$	50	$2 \cdot 5^2$

όταν $n \leqslant 50$ και στον κατάλογο

n	Παρ.	n	Παρ.	n	Παρ.	n	Παρ.	n	Παρ.
51	$3 \cdot 17$	61	61	71	71	81	3^4	91	$7 \cdot 13$
52	$2^2 \cdot 13$	62	$2 \cdot 31$	72	$2^3 \cdot 3^2$	82	$2 \cdot 41$	92	$2^2 \cdot 23$
53	53	63	$3^2 \cdot 7$	73	73	83	83	93	$3 \cdot 31$
54	$2 \cdot 3^3$	64	2^6	74	$2 \cdot 37$	84	$2^2 \cdot 3 \cdot 7$	94	$2 \cdot 47$
55	$5 \cdot 11$	65	$5 \cdot 13$	75	$3 \cdot 5^2$	85	$5 \cdot 17$	95	$5 \cdot 19$
56	$2^3 \cdot 7$	66	$2 \cdot 3 \cdot 11$	76	$2^2 \cdot 19$	86	$2 \cdot 43$	96	$2^5 \cdot 3$
57	$3 \cdot 19$	67	67	77	$7 \cdot 11$	87	$3 \cdot 29$	97	97
58	$2 \cdot 29$	68	$2^2 \cdot 17$	78	$2 \cdot 3 \cdot 13$	88	$2^3 \cdot 11$	98	$2 \cdot 7^2$
59	59	69	$3 \cdot 23$	79	79	89	89	99	$3^2 \cdot 11$
60	$2^2 \cdot 3 \cdot 5$	70	$2 \cdot 5 \cdot 7$	80	$2^4 \cdot 5$	90	$2 \cdot 3^2 \cdot 5$	100	$2^2 \cdot 5^2$

όταν $51 \leqslant n \leqslant 100$.

2.3.11 Παρατήρηση. Προφανώς, κάθε *ακέραιος* $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ μπορεί να γραφεί *μονοσημάντως* ως

$$n = \text{sign}\,(n)\ p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \tag{2.20}$$

όπου $k \in \mathbb{N}$, οι $p_1, p_2, \ldots, p_k$ πρώτοι αριθμοί με $p_1 < \cdots < p_k$ και οι $\alpha_1, \ldots, \alpha_k$ φυσικοί αριθμοί. Αλλά ακόμη και κάθε $n \in \mathbb{Q} \setminus \{0, \pm 1\}$ μπορεί να παρασταθεί *μονοσημάντως* υπό τη μορφή (2.20), όπου -εν προκειμένω- $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{Z} \setminus \{0\}$. Από το θεώρημα 2.3.8 και τις (2.19), (2.20) έχει γίνει πλέον αντιληπτό το γιατί οι πρώτοι αριθμοί θεωρούνται *δομικοί λίθοι* μέσω των οποίων «κτίζονται» τα σύνολα $\mathbb{N}, \mathbb{Z}$ και $\mathbb{Q}$. Εντούτοις, η κατανομή τους εντός τού $\mathbb{N}$ είναι αξιοπερίεργη, ελέγχεται δε (όπως δείχνει το λεγόμενο *θεώρημα των πρώτων αριθμών*) μόνον ασυμπτωτικώς.

2.3.12 Θεώρημα («Θεώρημα των πρώτων αριθμών»). *Το πλήθος των πρώτων αριθμών που είναι μικρότεροι ή ίσοι ενός θετικού πραγματικού αριθμού x πλησιάζει ασυμπτωτικώς τον λόγο $x/\ln(x)$ (τού x τείνοντος στο ∞), ήτοι*

$$\lim_{x \to \infty} \left(\frac{\text{card}(\{p \text{ πρώτος} | \, p \leqslant x\})}{x/\ln(x)} \right) = 1.$$

Οι πρώτες δύο (αναλυτικές) αποδείξεις[6] τού θεωρήματος 2.3.12 (βασιζόμενες σε ιδιότητες τής συναρτήσεως ζήτα τού Riemann) εδόθησαν από τους Charles Jean de la

[6] Για «στοιχειωδέστερες» (αλλά μακροσκελείς) αποδείξεις βλ.

Vallée-Poussin (1866-1962) και Jacques Hadamard (1865-1963) και δημοσιεύθηκαν το έτος 1896. Σημειωτέον ότι εντός τού $\mathbb{N}$ υφίστανται *μεγάλα* διαστήματα στα οποία δεν συναντούμε πρώτους αριθμούς[7]. Η ύπαρξη *αυθαιρέτως μεγάλων* «χασμάτων» μεταξύ *κάποιων* διαδοχικών πρώτων αριθμών προκύπτει από την ακόλουθη:

2.3.13 Πρόταση. *Δοθέντος ενός $n \in \mathbb{N}$, $n \geqslant 2$, υπάρχουν πάντοτε n διαδοχικοί σύνθετοι αριθμοί.*

Απόδειξη. Οι n διαδοχικοί φυσικοί αριθμοί

$$m_k := (n+1)! + k,\ k \in \{2, 3, ..., n+1\},$$

είναι σύνθετοι, διότι $k \mid (n+1)! \Rightarrow k \mid m_k$ για κάθε $k \in \{2, 3, ..., n+1\}$. □

Στο άλλο άκρο, τώρα, υπάρχουν στοιχειωδώς περιγραφόμενα *ευδιάκριτα* γνήσια υποσύνολα τού $\mathbb{N}$ τα οποία περιέχουν *άπειρους* πρώτους αριθμούς. Είναι, μάλιστα, εντυπωσιακό το ότι μεταξύ αυτών συγκαταλέγονται και τα σύνολα των όρων *κατάλληλων αριθμητικών προόδων*.

2.3.14 Θεώρημα (G.L. Dirichlet, 1837). *Εάν $a, b \in \mathbb{N}$ με μκδ$(a, b) = 1$, τότε εντός τού συνόλου $\{a + nb | n \in \mathbb{N}\}$ υπάρχουν άπειροι πρώτοι αριθμοί.*

Ο G.L. Dirichlet[8] (1805-1859) απέδειξε το θεώρημα 2.3.14 με αναλυτικά μέσα, κάνοντας χρήση των λεγομένων L-*σειρών*. Διαφορετικές αποδείξεις οφείλονται στους H. Zassenhaus[9], A. Selberg[10], H.N. Shapiro[11] κ.ά. Για την ειδική περίπτωση όπου $a = 1$, υπάρχουν και στοιχειωδέστερες αποδείξεις. (Κατ' ουσίαν, αρκούν κατάλληλοι χειρισμοί των ιδιοτήτων είτε τού *κυκλοτομικού πολυωνύμου*[12] είτε τής *συναρτήσεως* 2.4.30 *τού Möbius*[13].)

P. Erdös: *A new method in elementary number theory which leads to an elementary proof of the prime number theorem*, Proc. Nat. Acad. Sci. U.S.A. **35** (1949), 374-384, και

A. Selberg: *An elementary proof of the prime number theory*, Annals of Math. **50** (1949), 305-313.

▸ Για την ιστορική διαδρομή αυτού τού θεωρήματος, βλ.

L.J. Goldstein: *A History of the Prime Number Theorem*, American Math. Monthly **80** (1973), 599-741, και

P.T. Bateman & H.G. Diamond: *A hundred years of prime numbers*, American Math. Monthly **103** (1996), 729-741.

▸ Για μια λεπτομερή απόδειξή του (στο πλαίσιο τής Αναλυτικής Θεωρίας Αριθμών) βλ.

G.J.O. Jameson: *The Prime Number Theorem*, London Math. Soc. Student Texts, Vol. **53**, Cambridge Un. Press, 2003.

[7] Επί παραδείγματι, ο πρώτος αριθμός 370261 ακολουθείται από 111 σύνθετους αριθμούς και καθένας εκ των 209 φυσικών αριθμών που βρίσκονται μεταξύ των 20831323 και 20831533 είναι σύνθετος.

[8] G.L. Dirichlet: *Beweis des Satzes, daß jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält*, Abhandlungen der Königlichen Preußischen Akademie der Wissenschaften zu Berlin (1837), 45-81. Για πιο σύγχρονες παρουσιάσεις βλ.

E. Landau: *Elementary Number Theory*, translated by J.E. Goodman, Chealsea Pub. Co., 1958, Ch. III, σελ. 104-125,

H. Hasse: *Vorlesungen über Zahlentheorie*, zweite Aufl., Springer-Verlag, 1964, σελ. 176-283,

Z.I. Borevich & I.R. Shafarevich: *Number Theory*, transl. by N. Greenleaf, Academic Press, 1966, σελ. 339-341,

J.-P. Serre: *A Course in Arithmetic*, GTM, Vol. **7**, Springer-Verlag, 1973, Ch. VI, σελ. 61-76, και

T. Apostol: *Εισαγωγή στην Αναλυτική Θεωρία των Αριθμών*, σε μετ. των A. και E. Ζαχαρίου, και επιμ. Γ. Λεγάτου, εκδόσεις Gutenberg, Αθήνα 1986, Κεφ. 7, σελ. 198-208.

[9] H. Zassenhaus: *Über die Existenz von Primzahlen in arithmetischen Progressionen*, Commentarii Mathematici Helvetici **22** (1949), 232-259.

[10] A.Selberg: *An elementary proof of Dirichlet's theorem about primes in an arithmetic progression*, Annals of Mathematics **50** (1949), 297-304.

[11] H.N. Shapiro: *On primes in arithmetic progressions I, II*, Annals of Mathematics **52** (1950), 217-243.

[12] Βλ. P. Ribenboim: *The New Book of Prime Number Records*, Springer-Verlag, 1996, σελ. 268.

[13] Βλ. H. Gauchman: *A special case of Dirichlet's theorem on primes in an arithmetic progression*, Mathematics Magazine **74** (2001), 397-399.

2.3.15 Λήμμα. *Έστω n ένας φυσικός αριθμός γραφόμενος υπό τη μορφή*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

όπου $k \in \mathbb{N}$, οι $p_1, p_2, \ldots, p_k$ πρώτοι αριθμοί σαφώς διακεκριμένοι (για $k > 1$) και οι $\alpha_1, \alpha_2, \ldots, \alpha_k$ μη αρνητικοί ακέραιοι αριθμοί. Τότε ένας φυσικός αριθμός m διαιρεί τον n εάν και μόνον εάν

$$m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

όπου $\beta_1, \beta_2, \ldots, \beta_k \in \mathbb{N}_0$ με $0 \leqslant \beta_j \leqslant \alpha_j$, για κάθε $j \in \{1, ..., k\}$.

Απόδειξη. Επειδή για $n = 1$ ο ισχυρισμός είναι προφανής, μπορούμε, δίχως βλάβη τής γενικότητας, να υποθέσουμε ότι $n \geqslant 2$ και ότι η ανωτέρω έκφραση είναι η αποσύνθεση τού n σε γινόμενο πρώτων αριθμών. Εάν

$$m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

με $0 \leqslant \beta_j \leqslant \alpha_j$ για κάθε $j \in \{1, ..., k\}$, τότε

$$n = m \left(p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \cdots p_k^{\alpha_k - \beta_k} \right) \Longrightarrow m \mid n.$$

Και αντιστρόφως· εάν ο m είναι ένας φυσικός αριθμός $\geqslant 2$, ο οποίος διαιρεί τον n και έχει ως αποσύνθεσή του σε γινόμενο πρώτων την

$$m = q_1^{\gamma_1} q_2^{\gamma_2} \cdots q_l^{\gamma_l},$$

τότε υπάρχει $r \in \mathbb{N}$, τέτοιος ώστε να ισχύει η ισότητα

$$n = mr \Longrightarrow n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = (q_1^{\gamma_1} q_2^{\gamma_2} \cdots q_l^{\gamma_l})\, r.$$

Από τη μοναδικότητα τής παραστάσεως τού n ως γινομένου πρώτων παραγόντων λαμβάνουμε $l \leqslant k$ και $q_\varrho = p_{j_\varrho}$, $0 < \gamma_\varrho \leqslant \alpha_{j_\varrho}$, $\forall \varrho \in \{1, ..., l\}$, για κάποιο υποσύνολο δεικτών $\{j_1, \ldots, j_\varrho\} \subseteq \{1, ..., k\}$. Ως εκ τούτου, οιοσδήποτε φυσικός αριθμός $m \geqslant 1$ διαιρεί τον n θα γράφεται υπό την επιθυμητή μορφή. □

2.3.16 Πρόταση. *Έστω $n \in \mathbb{N}$. Εάν $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, όπου $k \in \mathbb{N}$, $p_1, p_2, \ldots, p_k$ πρώτοι αριθμοί σαφώς διακεκριμένοι (για $k > 1$) και $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}_0$, τότε ισχύουν τα ακόλουθα*:

(i) *Για τον πληθικό αριθμό τού συνόλου $\mathfrak{D}_n$ των θετικών ακεραίων διαιρετών τού n* (βλ. 2.2.34) *έχουμε*

$$\boxed{\operatorname{card}(\mathfrak{D}_n) = \prod_{j=1}^{k} (\alpha_j + 1).}$$

(ii) *Το άθροισμα των θετικών ακεραίων διαιρετών τού n δίδεται από τον τύπο*

$$\boxed{\sum_{d \in \mathfrak{D}_n} d = \prod_{j=1}^{k} \left(\frac{p_j^{\alpha_j + 1} - 1}{p_j - 1} \right).} \tag{2.21}$$

Απόδειξη. (i) Κατά το λήμμα 2.3.15 οι θετικοί ακέραιοι διαιρέτες τού n είναι τής μορφής

$$p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \quad \text{όπου } 0 \leqslant \beta_j \leqslant \alpha_j, \ \forall j \in \{1, ..., k\}.$$

Επομένως υπάρχουν ακριβώς $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$ θετικοί διαιρέτες τού n.

(ii) Θα χρησιμοποιήσουμε μαθηματική επαγωγή ως προς τον k. Εάν $k = 1$, τότε (κατά το λήμμα 2.3.15) οι θετικοί ακέραιοι διαιρέτες τού n είναι οι $1, p_1, p_1^2, ..., p_1^{\alpha_1}$ και το άθροισμά τους ισούται με

$$1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1} = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}.$$

Εάν $k > 1$, θέτουμε $l := p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{k-1}^{\alpha_{k-1}}$. Σύμφωνα με την επαγωγική μας υπόθεση,

$$\sum_{d \in \mathfrak{D}_l} d = \prod_{j=1}^{k-1} \left(\frac{p_j^{\alpha_j+1} - 1}{p_j - 1} \right). \tag{2.22}$$

Επειδή $\mathfrak{D}_n = \left\{ cp_k^{\beta_k} \,\middle|\, c \in \mathfrak{D}_l, \beta_k \in \{0, 1, ..., \alpha_k\} \right\}$, έχουμε

$$\sum_{d \in \mathfrak{D}_n} d = \sum_{d \in \mathfrak{D}_l} d + \left(\sum_{d \in \mathfrak{D}_l} d \right) p_k + \left(\sum_{d \in \mathfrak{D}_l} d \right) p_k^2 + \cdots + \left(\sum_{d \in \mathfrak{D}_l} d \right) p_k^{\alpha_k},$$

οπότε

$$\sum_{d \in \mathfrak{D}_n} d = \left(\sum_{d \in \mathfrak{D}_l} d \right) \left(1 + p_k + p_k^2 + \cdots + p_k^{\alpha_j} \right) = \left(\sum_{d \in \mathfrak{D}_l} d \right) \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}. \tag{2.23}$$

Η (2.21) προκύπτει άμεσα από τις (2.22) και (2.23). □

2.3.17 Πρόταση. *Εάν $n \in \mathbb{N},\ n \geqslant 2$, και $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ με*

$$|a_1| = p_1^{\alpha_{1,1}} \cdots p_k^{\alpha_{1,k}}, \ldots\ldots, \ |a_n| = p_1^{\alpha_{n,1}} \cdots p_k^{\alpha_{n,k}},$$

όπου $p_1, \ldots, p_k$ είναι πρώτοι αριθμοί σαφώς διακεκριμένοι (όταν $k > 1$) και οι $\alpha_{j,l}$, $j \in \{1, ..., n\},\ l \in \{1, ..., k\}$, μη αρνητικοί ακέραιοι αριθμοί, τότε

$$\boxed{\text{μκδ}(a_1, \ldots, a_n) = \prod_{l=1}^{k} p_l^{\min\{\alpha_{1,l}, \ldots, \alpha_{n,l}\}}.} \tag{2.24}$$

Απόδειξη. Επειδή $\text{μκδ}(a_1, \ldots, a_n) = \text{μκδ}(|a_1|, \ldots, |a_n|)$, μπορούμε -δίχως βλάβη τής γενικότητας- να υποθέσουμε ότι οι $a_1, \ldots, a_n$ είναι θετικοί. Επειδή

$$\min\{\alpha_{1,l}, ..., \alpha_{n,l}\} \leqslant \alpha_{j,l}, \quad \forall j \in \{1, ..., n\} \ \text{ και } \ \forall l \in \{1, ..., k\},$$

έχουμε $\prod_{l=1}^{k} p_l^{\min\{\alpha_{1,l}, \ldots, \alpha_{n,l}\}} \mid a_j$, για κάθε $j \in \{1, ..., n\}$ (βλ. 2.3.15). Επιπροσθέτως, εάν δ είναι οιοσδήποτε φυσικός αριθμός, για τον οποίο ισχύει $\delta \mid a_1, \ldots, \delta \mid a_n$, τότε, κατά το λήμμα 2.3.15,

$$\delta = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k},$$

όπου

$$0 \leqslant \delta_l \leqslant \alpha_{j,l}, \quad \forall j \in \{1, ..., n\} \ \text{ και } \ \forall l \in \{1, ..., k\},$$

οπότε $\delta_l \leqslant \min\{\alpha_{1,l}, ..., \alpha_{n,l}\}, \ \ \forall l \in \{1, ..., k\} \Rightarrow \delta \mid \prod_{l=1}^{k} p_l^{\min\{\alpha_{1,l}, \ldots, \alpha_{n,l}\}}$. Επομένως η (2.24) είναι αληθής λόγω τού πορίσματος 2.2.6. □

2.3.18 Πόρισμα. *Εάν* $n \in \mathbb{N},\ n \geqslant 2$, *και* $a, b_1, \ldots, b_n \in \mathbb{Z}\setminus\{0\}$ *με τους* $b_1, \ldots, b_n$ *ανά δύο σχετικώς πρώτους, τότε*

$$\text{μκδ}(a, \prod_{j=1}^{n} b_j) = \prod_{j=1}^{n} \text{μκδ}(a, b_j). \tag{2.25}$$

Απόδειξη. Αρκεί να αποδείξουμε την ισότητα (2.25) στην περίπτωση κατά την οποία οι ως άνω αριθμοί είναι φυσικοί $\geqslant 2$. Εφαρμόζουμε την πρώτη μορφή τής μαθηματικής επαγωγής ως προς τον n θεωρώντας ως αφετηρία μας τον $n = 2$. Εάν $n = 2$ και εάν οι αποσυνθέσεις των b_1, b_2 σε γινόμενα πρώτων παραγόντων είναι οι $b_1 = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, $b_2 = q_1^{\gamma_1} q_2^{\gamma_2} \cdots q_l^{\gamma_l}$, τότε οι $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_l$ είναι σαφώς διακεκριμένοι πρώτοι αριθμοί, καθόσον $\text{μκδ}(b_1, b_2) = 1$. Γράφοντας τον a ως γινόμενο σαφώς διακεκριμένων πρώτων αριθμών υπό τη μορφή

$$a = \left(p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}\right) \left(q_1^{\varepsilon_1} q_2^{\varepsilon_2} \cdots q_l^{\varepsilon_l}\right) \left(r_1^{\zeta_1} r_2^{\zeta_2} \cdots r_m^{\zeta_m}\right),$$

όπου δ_1,$\delta_2, \ldots, \delta_k, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_l \in \mathbb{N}_0$ κατάλληλοι εκθέτες των πρώτων που εμφανίζονται στις αποσυνθέσεις των b_1, b_2 και $r_1, r_2, \ldots, r_m$ οι πρώτοι που εμφανίζονται στην αποσύνθεση τού a, αλλά δεν περιέχονται στις αποσυνθέσεις των b_1, b_2, υψωμένοι σε κατάλληλες δυνάμεις $\zeta_1, \zeta_2, \ldots, \zeta_m \in \mathbb{N}$. Εφαρμόζοντας την (2.24) λαμβάνουμε

$$\text{μκδ}\,(a, b_1 b_2) = \left(\prod_{j=1}^{k} p_j^{\min\{\beta_j, \delta_j\}}\right) \left(\prod_{\varrho=1}^{l} p_\varrho^{\min\{\gamma_\varrho, \varepsilon_\varrho\}}\right) = \text{μκδ}\,(a, b_1)\ \text{μκδ}\,(a, b_2)\,.$$

Υποθέτοντας ότι η (2.25) είναι αληθής για κάποιον $n = k \geqslant 2$, θα την αποδείξουμε και για $n = k + 1$. Παρατηρούμε ότι $\text{μκδ}(b_1 b_2 \cdots b_k, b_{k+1}) = 1$ (Πράγματι· εάν ο p είναι ένας πρώτος αριθμός ο οποίος διαιρεί αμφοτέρους τους $b_1 b_2 \cdots b_k$ και b_{k+1}, τότε υπάρχει κάποιος δείκτης $j \in \{1, \ldots, k\}$ με $p \mid b_j$, οπότε $p \mid \text{μκδ}(b_j, b_{k+1}) = 1$, πράγμα άτοπο.) Βάσει των όσων αποδείξαμε για δύο παράγοντες,

$$\text{μκδ}(a, \prod_{j=1}^{k+1} b_j) = \text{μκδ}(a, \prod_{j=1}^{k} b_j)\ \text{μκδ}\,(a, b_{k+1})\,.$$

Εξάλλου, από την επαγωγική μας υπόθεση, $\text{μκδ}(a, \prod_{j=1}^{k} b_j) = \prod_{j=1}^{k} \text{μκδ}(a, b_j)$, οπότε η (2.25) είναι αληθής και για $n = k + 1$. □

2.3.19 Πόρισμα. *Εστω ότι* $n \in \mathbb{N},\ n \geqslant 2$, *και ότι* $a, b_1, \ldots, b_n \in \mathbb{Z}\setminus\{0\}$ *με τους* $b_1, \ldots, b_n$ *ανά δύο σχετικώς πρώτους. Εάν* $b_j \mid a, \forall j \in \{1, ..., n\}$, *τότε* $\prod_{j=1}^{n} b_j \mid a$.

Απόδειξη. Σύμφωνα με το πόρισμα 2.3.18 έχουμε

$$\text{μκδ}(a, \prod_{j=1}^{n} b_j) = \prod_{j=1}^{n} \text{μκδ}(a, b_j) = \prod_{j=1}^{n} |b_j|\,,$$

οπότε $\prod_{j=1}^{n} b_j \mid a$. □

2.3.20 Πόρισμα. *Εάν* $n \in \mathbb{N},\ n \geqslant 2$, *και οι* $a_1, \ldots, a_n$ *είναι μη μηδενικοί ακέραιοι, ανά δύο σχετικώς πρώτοι, τότε* $\text{εκπ}(a_1, \ldots, a_n) = |a_1 \cdots a_n|$.

ΑΠΟΔΕΙΞΗ. Επειδή $a_j \mid |a_1 \cdots a_n|$ για κάθε $j \in \{1, \ldots, n\}$ έχουμε

$$\text{εκπ}(a_1, \ldots, a_n) \mid |a_1 \cdots a_n|$$

(βλ. 2.2.25 (ii)). Εξάλλου επειδή εξ ορισμού $a_j \mid \text{εκπ}(a_1, \ldots, a_n), \forall j \in \{1, \ldots, n\}$, και οι $a_1, \ldots, a_n$ είναι σχετικώς πρώτοι ανά δύο,

$$a_1 \cdots a_n \mid \text{εκπ}(a_1, \ldots, a_n) \Longrightarrow |a_1 \cdots a_n| \mid \text{εκπ}(a_1, \ldots, a_n)$$

(βλ. 2.3.19 και 2.1.5 (i)). Επειδή τόσο το $\text{εκπ}(a_1, \ldots, a_n)$ όσο και ο $|a_1 \cdots a_n|$ είναι θετικοί ακέραιοι, από το (iii) τής προτάσεως 2.1.5 συμπεραίνουμε ότι οφείλουν να είναι ίσοι. □

2.3.21 Πρόταση. *Εάν* $n \in \mathbb{N},\ n \geqslant 2$, *και* $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ *με*

$$|a_1| = p_1^{\alpha_{1,1}} \cdots p_k^{\alpha_{1,k}}, \ldots\ldots, \ |a_n| = p_1^{\alpha_{n,1}} \cdots p_k^{\alpha_{n,k}},$$

όπου $p_1, \ldots, p_k$ *είναι πρώτοι αριθμοί σαφώς διακεκριμένοι (όταν* $k > 1$*) και οι* $\alpha_{j,l}$, $j \in \{1, ..., n\},\ l \in \{1, ..., k\}$, *μη αρνητικοί ακέραιοι αριθμοί, τότε*

$$\boxed{\text{εκπ}(a_1, \ldots, a_n) = \prod_{l=1}^{k} p_l^{\max\{\alpha_{1,l}, \ldots, \alpha_{n,l}\}}.} \tag{2.26}$$

ΑΠΟΔΕΙΞΗ. Επειδή $\text{εκπ}(a_1, \ldots, a_n) = \text{εκπ}(|a_1|, \ldots, |a_n|)$, μπορούμε -χωρίς βλάβη τής γενικότητας- να υποθέσουμε ότι οι $a_1, \ldots, a_n$ είναι θετικοί. Επειδή

$$\alpha_{j,l} \leqslant \max\{\alpha_{1,l}, ..., \alpha_{n,l}\}, \ \ \forall j \in \{1, ..., n\} \ \text{ και } \ \forall l \in \{1, ..., k\},$$

έχουμε $a_j \mid \prod_{l=1}^{k} p_l^{\max\{\alpha_{1,l}, \ldots, \alpha_{n,l}\}}$, για κάθε $j \in \{1, ..., n\}$ (βλ. 2.3.15). Επιπροσθέτως, εάν μ είναι οιοσδήποτε φυσικός αριθμός, για τον οποίο ισχύει $a_1 \mid \mu$, $\ldots$, $a_n \mid \mu$, τότε, κατά το λήμμα 2.3.15, $\mu = (p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k})\, p_{k+1}^{\gamma_{k+1}} \cdots p_\xi^{\gamma_\xi}$, όπου οι $p_1, p_2, \ldots, p_k, \ldots, p_\xi$ είναι διακεκριμένοι πρώτοι αριθμοί και οι $\gamma_1, \gamma_2, \ldots, \gamma_k, \ldots, \gamma_\xi$ κατάλληλοι φυσικοί αριθμοί με

$$\alpha_{j,l} \leqslant \gamma_l, \quad \forall j \in \{1, ..., n\} \ \text{ και } \ \forall l \in \{1, ..., k\},$$

οπότε $[\max\{\alpha_{1,l}, ..., \alpha_{n,l}\} \leqslant \gamma_l, \ \ \forall l \in \{1, ..., k\}] \Longrightarrow \prod_{l=1}^{k} p_l^{\max\{\alpha_{1,l}, \ldots, \alpha_{n,l}\}} \mid \mu$. Επομένως η (2.26) είναι αληθής λόγω τής προτάσεως 2.2.25. □

2.3.22 Πόρισμα. *Εάν* $m \in \mathbb{N}$, *τότε* $\text{εκπ}(k, l) \in \mathfrak{D}_m, \forall (k, l) \in \mathfrak{D}_m \times \mathfrak{D}_m$.

ΑΠΟΔΕΙΞΗ. Εάν $(k, l) \in \mathfrak{D}_m \times \mathfrak{D}_m$ και εάν (δίχως βλάβη τής γενικότητας) υποθέσουμε ότι

$$k = p_1^{\alpha_1} \cdots p_\nu^{\alpha_\nu},\ l = p_1^{\beta_1} \cdots p_\nu^{\beta_\nu},\ m = p_1^{\gamma_1} \cdots p_\nu^{\gamma_\nu},\ (\nu \in \mathbb{N})$$

όπου οι $p_1, \ldots, p_\nu$ είναι πρώτοι αριθμοί σαφώς διακεκριμένοι (για $\nu > 1$) και οι $\alpha_1, \ldots, \alpha_\nu, \beta_1, \ldots, \beta_\nu$ και $\gamma_1, \ldots, \gamma_\nu$ μη αρνητικοί ακέραιοι αριθμοί, τότε

$$\left.\begin{array}{l} k \mid m \Rightarrow \alpha_j \leqslant \gamma_j,\ \forall j \in \{1, ..., \nu\} \\ l \mid m \Rightarrow \beta_j \leqslant \gamma_j,\ \forall j \in \{1, ..., \nu\} \end{array}\right\} \Rightarrow \max\{\alpha_j, \beta_j\} \leqslant \gamma_j,\ \forall j \in \{1, ..., \nu\},$$

οπότε $\text{εκπ}(k, l) \in \mathfrak{D}_m$ (μέσω τού λήμματος 2.3.15 και τής προτάσεως 2.3.21). □

2.4 ΙΣΟΤΙΜΙΕΣ

2.4.1 Ορισμός. Έστω m ένας φυσικός αριθμός. Ένας ακέραιος a ορίζεται να είναι **ισότιμος** ενός ακεραίου b **κατά μόδιο** m (ή **modulo** m), συμβολιζόμενος ως[14]

$$\boxed{a \equiv b (\text{mod } m),}$$

όταν $m \mid a-b$. Ο m καλείται, εν προκειμένω, **το μόδιο**[15] τής ισοτιμίας. Όταν $m \nmid a-b$, τότε λέμε ότι ο a είναι **ανισότιμος** τού b κατά μόδιο m και γράφουμε $a \not\equiv b (\text{mod}\, m)$.

2.4.2 Παρατήρηση. Οι κατωτέρω ιδιότητες τής διμελούς σχέσεως "$\equiv$" (επί τού $\mathbb{Z}$) απορρέουν άμεσα από τον ορισμό 2.4.1:

(i) $a \equiv 0 (\text{mod } m) \iff m \mid a$.

(ii) Για οιουσδήποτε ακεραίους a, b έχουμε $a \equiv b (\text{mod } 1)$.

(iii) Ο ακέραιος a είναι άρτιος $\iff a \equiv 0 (\text{mod } 2)$.

(iv) Ο ακέραιος a είναι περιττός $\iff a \equiv 1 (\text{mod } 2)$.

(v) Εάν $a \equiv b (\text{mod } m)$ και $n \mid m$, για κάποιον $n \in \mathbb{N}$, τότε $a \equiv b (\text{mod } n)$.

Όταν $a \equiv b (\text{mod } m)$ οι a και b ονομάζονται ενίοτε και **ισοϋπόλοιποι** κατά μόδιο m, λόγω τής επομένης προτάσεως:

2.4.3 Πρόταση. *Έχουμε $a \equiv b (\text{mod } m)$ εάν και μόνον εάν οι a και b, διαιρούμενοι διά τού m, αφήνουν το ίδιο υπόλοιπο.*

Απόδειξη. Εκτελώντας τή διαίρεση των a και b διά τού m λαμβάνουμε

$$a = \kappa m + \nu,\ b = \lambda m + \rho, \quad \text{όπου} \quad \kappa, \lambda, \nu, \rho \in \mathbb{Z} \ \text{ με } \ 0 \leqslant \nu, \rho < m.$$

Παρατηρούμε ότι $a \equiv b (\text{mod}\, m) \iff m \mid a-b \iff m \mid \nu - \rho$. Επειδή όμως έχουμε $|\nu - \rho| < m$, βάσει τού 2.1.5 (ii) συμπεραίνουμε ότι $m \mid \nu - \rho \Leftrightarrow \nu = \rho$. □

2.4.4 Πρόταση (Θεμελιώδεις ιδιότητες ισοτιμιών). *Έστω ότι ο m είναι ένας φυσικός αριθμός και οι a, b, c, d ακέραιοι αριθμοί. Τότε ισχύουν τα ακόλουθα*:

(i) *Εάν $a \equiv b (\text{mod } m)$ και $c \equiv d (\text{mod } m)$, τότε*

$$a \pm c \equiv b \pm d (\text{mod } m) \quad \text{και} \quad ac \equiv bd (\text{mod } m).$$

(ii) *Εάν $a \equiv b (\text{mod } m)$, τότε $a \pm c \equiv b \pm c (\text{mod} m)$ και $ac \equiv bc (\text{mod} m)$.*

(iii) *Εάν $a \equiv b (\text{mod } m)$, τότε $a^k \equiv b^k (\text{mod } m),\ \forall k \in \mathbb{N}$.*

(iv) *Εάν $c \neq 0$, τότε $a \equiv b (\text{mod } m) \iff ac \equiv bc (\text{mod } mc)$.*

(v) *Εάν $c \neq 0$, τότε $ac \equiv bc (\text{mod } m) \iff a \equiv b (\text{mod } \frac{m}{\text{μκδ}(m,c)})$.*

Απόδειξη. (i) Εάν $a \equiv b (\text{mod } m)$ και $c \equiv d (\text{mod } m)$, τότε υπάρχουν $k_1, k_2 \in \mathbb{Z}$, τέτοιοι ώστε

$$\left.\begin{array}{l} a-b = k_1 m \\ c-d = k_2 m \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} (a \pm c) - (b \pm d) = (a-b) \pm (c-d) = (k_1 \pm k_2)m, \\ ac - bd = (bk_2 + dk_1 + k_1 k_2 m)m, \end{array}\right.$$

[14] Ο συμβολισμός αυτός εισήχθη από τον C.-F. Gauss (1777-1855) το έτος 1801 στο έργο του «Disquisitiones Arithmeticae», στο οποίο αναπτύσσεται με σαφήνεια και αυστηρότητα ο *λογισμός των ισοτιμιών*.

[15] Άλλοι συγγραφείς προτιμούν να καλούν το μόδιο **μέτρο** τής (εκάστοτε θεωρούμενης) ισοτιμίας. Προσοχή! Μη συγχέετε το (ουδέτερο) ουσιαστικό: **το μόδιο** (γερμ. **das** Modul) με το (αρσενικό) ουσιαστικό: **ο μόδιος** (γερμ. **der** Modul) που είναι όρος χρησιμοποιούμενος για να εκφράζει έναν *γενικευμένο* διανυσματικό χώρο (με τα βαθμωτά του μεγέθη ανήκοντα σε έναν δακτύλιο που δεν είναι κατ' ανάγκην σώμα.)

οπότε $a \pm c \equiv b \pm d (\text{mod } m)$ και $ac \equiv bd (\text{mod } m)$.
(ii) Επειδή $c \equiv c (\text{mod } m)$, οι ισοτιμίες αυτές έπονται από το (i).
(iii) Τούτο αποδεικνύεται κάνοντας χρήση μαθηματικής επαγωγής. Για $k = 1$, ο ισχυρισμός είναι προφανής. Υποθέτοντας ότι αυτός είναι αληθής για κάποιον ακέραιο $k > 1$, έχουμε

$$\underbrace{\begin{array}{ll} a \equiv b (\text{mod } m) & (\text{εξ υποθέσεως}) \text{ και} \\ a^k \equiv b^k (\text{mod } m) & (\text{από την επαγωγική μας υπόθεση}) \end{array}}_{\begin{array}{c} \Downarrow \text{(i)} \\ a^{k+1} \equiv b^{k+1} (\text{mod } m). \end{array}}$$

(iv) Αρκεί να παρατηρήσουμε ότι $m \mid a - b \iff mc \mid (a - b)\, c$.
(v) Εάν $ac \equiv bc (\text{mod } m)$, τότε, εφαρμόζοντας το (ii) της προτάσεως 2.2.14 και το πόρισμα 2.2.9, λαμβάνουμε

$$\left.\begin{array}{rl} m \mid (a-b)c \Longrightarrow & \frac{m}{\text{μκδ}(m,c)} \mid (a-b)\frac{c}{\text{μκδ}(m,c)} \\ & \text{μκδ}(\frac{m}{\text{μκδ}(m,c)}, \frac{c}{\text{μκδ}(m,c)}) = 1 \end{array}\right\} \Longrightarrow \frac{m}{\text{μκδ}(m,c)} \mid a - b,$$

ήτοι $a \equiv b (\text{mod } \frac{m}{\text{μκδ}(m,c)})$. Και αντιστρόφως· υποθέτοντας ότι $a \equiv b (\text{mod } \frac{m}{\text{μκδ}(m,c)})$, τότε -σύμφωνα με το (iv)- $\text{μκδ}(m, c)\, a \equiv \text{μκδ}(m, c)\, b (\text{mod } m)$. Επιπροσθέτως,

$$\text{μκδ}(m, c) \mid c \Longrightarrow (\exists c' \in \mathbb{Z} : c = \text{μκδ}(m, c)c').$$

Εάν λοιπόν εφαρμόσουμε το (ii), λαμβάνουμε

$$\text{μκδ}(m, c)\, c'\, a \equiv \text{μκδ}(m, c)\, c'\, b (\text{mod } m),$$

ήτοι $ac \equiv bc (\text{mod } m)$. □

2.4.5 Πόρισμα. *Έστω ότι ο m είναι ένας φυσικός αριθμός και οι a, b, c ακέραιοι αριθμοί. Εάν $c \neq 0$, $ac \equiv bc (\text{mod } m)$ και $\text{μκδ}(m, c) = 1$, τότε έχουμε $a \equiv b (\text{mod } m)$.*

Απόδειξη. Αρκεί να εφαρμόσουμε το (v) της προτάσεως 2.4.4. □

2.4.6 Πόρισμα. *Έστω ότι ο p είναι ένας πρώτος αριθμός και οι a, b, c ακέραιοι αριθμοί. Εάν $c \neq 0$, $ac \equiv bc (\text{mod } p)$ και $p \nmid c$, τότε $a \equiv b (\text{mod } p)$.*

Απόδειξη. Επειδή $p \nmid c$ και ο p είναι πρώτος, έχουμε $\text{μκδ}(p, c) = 1$. Επομένως, $a \equiv b (\text{mod } p)$ βάσει τού πορίσματος 2.4.5. □

2.4.7 Πρόταση. *Έστω ότι οι m_1, m_2 είναι δυο φυσικοί αριθμοί και ότι οι a, b, c είναι τρεις ακέραιοι αριθμοί για τους οποίους ισχύουν οι ισοτιμίες*

$$a \equiv b (\text{mod } m_1), \qquad a \equiv c (\text{mod } m_2).$$

Τότε έχουμε $b \equiv c (\text{mod } \text{μκδ}(m_1, m_2))$.

Απόδειξη. Εάν $m_1 \mid a - b$ και $m_2 \mid a - c$, τότε, θέτοντας σε εφαρμογή το (v) της προτάσεως 2.1.5, λαμβάνουμε

$$[m_1 \mid a - b \text{ και } \text{μκδ}(m_1, m_2) \mid m_1] \Rightarrow \text{μκδ}(m_1, m_2) \mid a - b,$$

και $[m_2 \mid a - c \text{ και } \text{μκδ}(m_1, m_2) \mid m_2] \Rightarrow \text{μκδ}(m_1, m_2) \mid a - c$. Ως εκ τούτου, λόγω τής ιδιότητας (vi) τής 2.1.5, μπορούμε να συμπεράνουμε ότι

$$\text{μκδ}(m_1, m_2) \mid (a - b) - (a - c) \Longrightarrow \text{μκδ}(m_1, m_2) \mid b - c,$$

ήτοι ότι $b \equiv c (\text{mod } \text{μκδ}(m_1, m_2))$. □

2.4.8 Πρόταση. *Υποθέτουμε ότι $s \in \mathbb{N},\ s \geqslant 2$, ότι οι $m_1, ..., m_s$ είναι φυσικοί αριθμοί και ότι οι a, b είναι δυο ακέραιοι αριθμοί. Τότε*

$$(a \equiv b (\mathrm{mod}\, m_j),\ \ \forall j \in \{1, ..., s\}) \Longleftrightarrow a \equiv b (\mathrm{mod}\ \ \text{εκπ}(m_1, ..., m_s))$$

Απόδειξη. Εάν $a \equiv b (\mathrm{mod}\, m_j)$ για κάθε δείκτη $j \in \{1, ..., s\}$, τότε (κατά την πρόταση 2.2.25) $(m_j \mid a - b,\ \ \forall j \in \{1, ..., s\}) \Longrightarrow$ εκπ$(m_1, ..., m_s) \mid a - b$. Και αντιστρόφως· εάν υποθέσουμε ότι εκπ$(m_1, ..., m_s) \mid a - b$ και λάβουμε υπ' όψιν ότι

$$m_j \mid \text{εκπ}(m_1, ..., m_s),\ \ \forall j \in \{1, ..., s\},$$

συμπεραίνουμε ότι $a \equiv b (\mathrm{mod}\, m_j)$ για κάθε $j \in \{1, ..., s\}$ (πρβλ. 2.1.5 (v)). □

2.4.9 Πόρισμα. *Υποθέτουμε ότι $s \in \mathbb{N},\ s \geqslant 2$, ότι οι $m_1, ..., m_s$ είναι φυσικοί αριθμοί, σχετικώς πρώτοι ανά δύο, και ότι $a, b \in \mathbb{Z}$. Τότε ισχύει η συνεπαγωγή*

$$[a \equiv b (\mathrm{mod}\, m_j), \forall j \in \{1, ..., s\}] \Longrightarrow a \equiv b\ (\mathrm{mod}\ \ (\prod_{j=1}^{s} m_j)).$$

Απόδειξη. Είναι αρκετό να εφαρμόσει κανείς την πρόταση 2.4.8 και να λάβει υπ' όψιν ότι εκπ$(m_1, ..., m_s) = \prod_{j=1}^{s} m_j$ (βλ. 2.3.20). □

2.4.10 Λήμμα. *Για κάθε αριθμό $n \in \mathbb{N}_0$ ας συμβολίσουμε ως $n! = 1 \cdot 2 \cdots n$ το παραγοντικό τού n, όταν $n \geqslant 1$, θέτοντας $0! = 1$, και ως $\binom{n}{i} = \frac{n!}{i!(n-i)!}$ τον διωνυμικό συντελεστή τού n υπεράνω τού i, όπου $i \in \mathbb{Z}$, $0 \leqslant i \leqslant n$. Έστω p ένας πρώτος αριθμός. Τότε*

$$\binom{p}{i} \equiv 0\ (\mathrm{mod}\, p), \quad \forall i \in \{1, ..., p-1\}. \tag{2.27}$$

Απόδειξη. Επειδή για κάθε $i \in \{1, ..., p-1\}$,

$$\underbrace{\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i!}}$$
$$\Downarrow$$
$$p(p-1)\cdots(p-i+1) = 1 \cdot 2 \cdot 3 \cdots i \cdot \tbinom{p}{i},$$

έχουμε

$$\left.\begin{array}{r} p \mid 1 \cdot 2 \cdot 3 \cdots i \cdot \binom{p}{i} \\ \text{μκδ}(p, 1 \cdot 2 \cdot 3 \cdots i) = 1 \end{array}\right\} \underset{2.2.9}{\Longrightarrow} p \mid \tbinom{p}{i},$$

το οποίο ισοδυναμεί με την ισοτιμία (2.27). □

2.4.11 Πρόταση. *Εάν $a, b \in \mathbb{Z}$ και p είναι πρώτος αριθμός, τότε*

$$(a+b)^p \equiv a^p + b^p (\mathrm{mod}\, p). \tag{2.28}$$

Απόδειξη. Κατά τον διωνυμικό τύπο,

$$(a+b)^p = \sum_{i=0}^{p} \tbinom{p}{i} a^i b^{p-i}.$$

Και επειδή ισχύει η ισοτιμία $\binom{p}{i} \equiv 0 (\mathrm{mod}\, p)$ για κάθε $i \in \{1, ..., p-1\}$ (βλ. λήμμα 2.4.10), η (2.28) είναι αληθής. □

2.4.12 Πόρισμα. *Εάν ο p είναι ένας πρώτος αριθμός, τότε*

$$\boxed{a^p \equiv a (\mathrm{mod}\, p), \quad \forall a \in \mathbb{Z}.} \tag{2.29}$$

Απόδειξη. Κατ' αρχάς παρατηρούμε ότι, όταν $a = 0$ ή $a = 1$, η (2.29) είναι προφανής. Εν συνεχεία αποδεικνύουμε την (2.29) για οιονδήποτε $a \geqslant 1$ μέσω κλασικής μαθηματικής επαγωγής. Πράγματι· υποθέτοντας ότι η (2.29) είναι αληθής για κάποιον $a \geqslant 1$, αυτή ισχύει και για τον $a+1$, καθότι

$$\underbrace{\begin{array}{ll} (a+1)^p \equiv a^p + 1 (\mathrm{mod}\, p) & \text{(δυνάμει τής ισοτιμίας (2.28)) και} \\ a^p \equiv a (\mathrm{mod}\, p) & \text{(από την επαγωγική μας υπόθεση)} \end{array}}$$
$$\Downarrow$$
$$(a+1)^p \equiv a + 1 (\mathrm{mod}\, p),$$

πρβλ. 2.4.4 (ii). Απομένει η απόδειξη τού πορίσματος και για οιονδήποτε ακέραιο $a < 0$. Όμως, σε αυτήν την περίπτωση, διαιρώντας τό a διά τού p, λαμβάνουμε $a \equiv r (\mathrm{mod}\, p)$ για κάποιον $r \in \mathbb{Z}$, για τον οποίο $0 \leqslant r \leqslant p-1$. Ως εκ τούτου, κάνοντας χρήση τού (iii) τής προτάσεως 2.4.4, σε συνδυασμό με ό,τι αποδείξαμε προηγουμένως, λαμβάνουμε

$$\left.\begin{array}{l} a^p \equiv r^p (\mathrm{mod}\, p) \\ r^p \equiv r (\mathrm{mod}\, p) \\ a \equiv r (\mathrm{mod}\, p) \end{array}\right\} \Longrightarrow a^p \equiv a (\mathrm{mod}\, p).$$

Συνεπώς η (2.29) είναι όντως αληθής *για κάθε* ακέραιο a. □

2.4.13 Πόρισμα («Μικρό θεώρημα» τού Fermat, 1640.). *Εάν ο p είναι ένας πρώτος αριθμός και ο a ένας ακέραιος, τέτοιος ώστε $p \nmid a$, τότε $a \neq 0$* (βλ. 2.1.3) *και*

$$\boxed{a^{p-1} \equiv 1 (\mathrm{mod}\, p).} \tag{2.30}$$

Απόδειξη[16] . Προφανής λόγω τής (2.29) και τού πορίσματος 2.4.6 (αφού έχουμε μκδ$(p, a) = 1$). □

2.4.14 Παράδειγμα. Δοθέντος ενός πρώτου αριθμού $p \geqslant 3$ υπάρχουν άπειροι φυσικοί αριθμοί n, ούτως ώστε να πληρούται η συνθήκη $p \mid n2^n + 1$. Πράγματι· θέτοντας $n = (p-1)^{2k+1}$, $k = 0, 1, 2, \ldots$ διαπιστώνουμε μέσω τής σχέσεως (2.30) για $a = 2$ ότι

$$n2^n + 1 \equiv (p-1)^{2k+1} \left(2^{p-1}\right)^{(p-1)^{2k}} + 1 \equiv (-1)^{2k+1} 1^{2k} + 1 \equiv 0 (\mathrm{mod}\, p).$$

▸ **Η κατά Euler γενίκευση τού «μικρού θεωρήματος» τού Fermat**. Ο Leonhard Euler (1707-1783) παρουσίασε κατά το έτος 1760 μια γενίκευση τού θεωρήματος 2.4.13 (βλ. 2.4.22), η οποία έμελλε να παίξει καθοριστικό ρόλο για μια πληθώρα εφαρμογών, τόσον στη Θεωρία Αριθμών όσον και στην Άλγεβρα. Η απόδειξη που παρατίθεται εδώ χρησιμοποιεί μόνον στοιχειώδη τεχνικά μέσα και ορισμένα λήμματα που αφορούν στη λεγομένη *συνάρτηση φι*.

2.4.15 Ορισμός. Η απεικόνιση $\phi : \mathbb{N} \longrightarrow \mathbb{N}$ η οριζόμενη μέσω τού τύπου

$$\boxed{\phi(n) := \mathrm{card}\{\ell \in \mathbb{N} \mid \ell \leqslant n \text{ και μκδ}(\ell, n) = 1\}.}$$

[16] Ο Pierre de Fermat (1601-1665) έγραψε επ' αυτού σε ένα γράμμα του προς τον Frenicle (τον Οκτώβριο τού 1640), αλλ' ουδέποτε έδωσε μια λεπτομερή απόδειξη.

καλείται **συνάρτηση φι τού Euler**. Επί παραδείγματι, $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, $\phi(6) = 2$, $\phi(7) = 6$, $\phi(8) = 4$. Η τιμή $\phi(n)$ τού n μέσω τής ϕ εκφράζεται προφανώς και ως το άθροισμα

$$\boxed{\phi(n) = \sum_{\ell=1}^{n} \left\lfloor \frac{1}{\text{μκδ}(\ell, n)} \right\rfloor}, \tag{2.31}$$

όπου για κάθε $x \in \mathbb{R}$ θέτουμε: $\lfloor x \rfloor := \max\{ n \in \mathbb{Z} \mid n \leqslant x \}$.

2.4.16 Λήμμα. *Η συνάρτηση φι τού Euler είναι «πολλαπλασιαστική», ήτοι για οιουσδήποτε $m, n \in \mathbb{N}$ ισχύει η συνεπαγωγή*

$$\text{μκδ}(m, n) = 1 \Longrightarrow \phi(mn) = \phi(m)\,\phi(n)\,. \tag{2.32}$$

Απόδειξη. Εάν $m = 1$ ή $n = 1$, τότε η ως άνω ισότητα είναι προφανής. Γι' αυτόν τον λόγο, υποθέτουμε από εδώ και στο εξής ότι $m \geqslant 2$ και $n \geqslant 2$. Θέτοντας

$$S := \{1, 2, ..., mn\} \quad \text{και} \quad S' := \{ \ell \in S \mid \text{μκδ}(\ell, mn) = 1 \},$$

και εφαρμόζοντας το πόρισμα 2.2.12 λαμβάνουμε

$$\phi(mn) = \text{card}\left(S'\right) = \text{card}\{ \ell \in S \mid \text{μκδ}(\ell, m) = 1 \text{ και } \text{μκδ}(\ell, n) = 1 \}. \tag{2.33}$$

Τοποθετώντας τά στοιχεία τού S σε έναν κατάλογο m στηλών και n γραμμών ως ακολούθως:

$$\begin{array}{ccccccc}
1 & 2 & \cdots & j & \cdots & m-1 & m \\
m+1 & m+2 & \cdots & m+j & \cdots & m+(m-1) & 2m \\
2m+1 & 2m+2 & \cdots & 2m+j & \cdots & 2m+(m-1) & 3m \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
(n-1)\,m+1 & (n-1)\,m+2 & \cdots & (n-1)\,m+j & \cdots & (n-1)\,m+(m-1) & nm
\end{array}$$

διαπιστώνουμε ότι κάθε στοιχείο τού S γράφεται μονοσημάντως υπό την μορφή $mq + j$, όπου $0 \leqslant q \leqslant n-1$ και $0 \leqslant j \leqslant m-1$. Βάσει τού 2.2.14 (iii),

$$\text{μκδ}(mq + j, m) = \text{μκδ}(j, m),$$

οπότε οι αριθμοί τής j-οστής στήλης τού ανωτέρω καταλόγου είναι πρώτοι προς τον m εάν και μόνον εάν ο ίδιος ο j είναι πρώτος προς τον m. Ως εκ τούτου, μόνον $\phi(m)$ στήλες περιέχουν φυσικούς αριθμούς πρώτους προς τον m, και κάθε στοιχείο καθεμιάς εξ αυτών είναι πρώτο προς τον m. Το πρόβλημα λοιπόν είναι να αποδειχθεί ότι σε καθεμιά εξ αυτών των $\phi(m)$ στηλών υπάρχουν ακριβώς $\phi(n)$ αριθμοί, οι οποίοι είναι πρώτοι προς τον n (διότι τότε θα υπάρχουν εν συνόλω $\phi(m)\,\phi(n)$ αριθμοί από τον κατάλογό μας, οι οποίοι θα είναι πρώτοι τόσο προς τον m όσο και προς τον n, οπότε ο ισχυρισμός θα είναι αληθής).

Ας υποθέσουμε ότι οι $\phi(m)$ στήλες, οι οποίες περιέχουν φυσικούς αριθμούς πρώτους προς τον m, είναι οι $j_1, j_2, ..., j_{\phi(m)}$, κι ας θεωρήσουμε το σύνολο

$$S_\kappa := \{ x_q = mq + j_\kappa \mid 0 \leqslant q \leqslant n-1 \}$$

των εν συνόλω n στοιχείων τής στήλης j_κ, για κάθε $\kappa \in \{1, 2, ..., \phi(m)\}$. Καθένας εκ των x_q είναι πρώτος προς τον m. Επιπροσθέτως, εάν $q, \widehat{q} \in \{0, 1, ..., n-1\}$ και

$q \neq \widehat{q}$, τότε $n \nmid x_q - x_{\widehat{q}}$, διότι, υποθέτοντας ότι $n \mid x_q - x_{\widehat{q}}$ ($\Longleftrightarrow x_q \equiv x_{\widehat{q}} (\mathrm{mod}\ n)$), θα είχαμε

$$\left.\begin{array}{r} n \mid m(q-\widehat{q}) \\ \text{μκδ}(m,n) = 1 \end{array}\right\} \underset{2.2.9}{\Longrightarrow} n \mid q - \widehat{q},$$

ήτοι κάτι το άτοπο, αφού $|q - \widehat{q}\,| \leqslant n-1$ (βλ. 2.1.5 (ii)). Κατά συνέπειαν, τα x_q και $x_{\widehat{q}}$ διαιρούμενα διά τού n αφήνουν (σύμφωνα με την πρόταση 2.4.3) *διαφορετικά* υπόλοιπα, οπότε τα n στοιχεία τού S_κ μπορούν να γραφούν υπό τη μορφή

$$n\lambda_\varrho + \varrho, \quad \forall \varrho \in \mathbb{N}_0, \ \ 0 \leqslant \varrho \leqslant n-1,$$

όπου $\lambda_0, \lambda_1, ..., \lambda_{n-1}$ είναι κατάλληλοι μη αρνητικοί ακέραιοι αριθμοί. Βάσει τού (iii) τής προτάσεως 2.2.14, $\text{μκδ}(n\lambda_\varrho + \varrho, n) = \text{μκδ}(\varrho, n)$, οπότε

$$\text{μκδ}(n\lambda_\varrho + \varrho, n) = 1 \Longleftrightarrow \text{μκδ}(\varrho, n) = 1.$$

Θέτοντας

$$S'_\kappa := \{\ell \in S_\kappa \mid \text{μκδ}\,(\ell, mn) = 1\}$$

και λαμβάνοντας υπ' όψιν ότι $\text{card}(S'_\kappa) = \phi\,(n)$ για κάθε $\kappa \in \{1, 2, ..., \phi\,(m)\}$, καθώς και ότι

$$S_{\kappa_1} \cap S_{\kappa_2} = \varnothing \Longrightarrow S'_{\kappa_1} \cap S'_{\kappa_2} = \varnothing,$$

για οιουσδήποτε $\kappa_1, \kappa_2 \in \{1, 2, ..., \phi\,(m)\}$ με $\kappa_1 \neq \kappa_2$, συμπεραίνουμε ότι

$$S' = \coprod_{\kappa=1}^{\phi(m)} S'_\kappa \Longrightarrow \text{card}\,(S') = \sum_{\kappa=1}^{\phi(m)} \text{card}\,(S'_\kappa) = \phi\,(m)\,\phi\,(n)\,. \tag{2.34}$$

Η (2.34), συνδυαζόμενη με την (2.33), δίδει τη ζητούμενη ισότητα (2.32). □

2.4.17 Θεώρημα. *Εάν $s \in \mathbb{N}$, $s \geqslant 2$, και εάν οι $m_1, m_2, \ldots, m_s$ είναι s σχετικώς πρώτοι ανά δύο φυσικοί αριθμοί, τότε*

$$\boxed{\phi\left(\prod_{j=1}^{s} m_j\right) = \prod_{j=1}^{s} \phi\,(m_j)\,.}$$

Απόδειξη. Έπεται άμεσα κάνοντας χρήση μαθηματικής επαγωγής ως προς το πλήθος s των παραγόντων τού γινομένου και τού λήμματος 2.4.16. □

2.4.18 Λήμμα. *Εάν ο p είναι πρώτος και $k \in \mathbb{N}$, τότε*

$$\boxed{\phi\left(p^k\right) = p^k - p^{k-1} = p^{k-1}\,(p-1) = p^k\left(1 - \frac{1}{p}\right).}$$

Απόδειξη. Επειδή

$$\begin{array}{rcl} \phi\left(p^k\right) & = & \text{card}(\{\ell \in \mathbb{N} \mid \ell \leqslant p^k \text{ και μκδ } \left(\ell, p^k\right) = 1\}) \\ & = & \text{card}(\{\ell \in \mathbb{N} \mid \ell \leqslant p^k \text{ και } p \nmid \ell\}) \end{array}$$

και $\{\ell \in \mathbb{N} \mid \ell \leqslant p^k \text{ και } p \nmid \ell\} = \{1, 2, \ldots, p^k\} \setminus \{p, 2p, 3p, \ldots, \left(p^{k-1}\right) p\}$, έχουμε προφανώς $\phi\left(p^k\right) = p^k - p^{k-1}$. □

2.4.19 Πρόταση. *Εάν $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ είναι η κανονική παράσταση (2.19) ενός*

$n \in \mathbb{N}$, $n \geqslant 2$, ως γινομένου πρώτων αριθμών, τότε

$$\boxed{\phi(n) = \prod_{j=1}^{k} \left(p_j^{\alpha_j} - p_j^{\alpha_j - 1}\right) = n \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right).} \tag{2.35}$$

ΑΠΟΔΕΙΞΗ. Από το λήμμα 2.4.16 λαμβάνουμε

$$\begin{aligned} \phi(n) &= \phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \phi(p_1^{\alpha_1})\, \phi(p_2^{\alpha_2} \cdots p_k^{\alpha_k}) \\ &= \phi(p_1^{\alpha_1})\, \phi(p_2^{\alpha_2})\, \phi(p_3^{\alpha_3} \cdots p_k^{\alpha_k}) = \cdots = \prod_{j=1}^{k} \phi(p_j^{\alpha_j}). \end{aligned}$$

Ως εκ τούτου, από το λήμμα 2.4.18 συνάγεται ότι

$$\prod_{j=1}^{k} \phi\left(p_j^{\alpha_j}\right) = \prod_{j=1}^{k} (p_j^{\alpha_j} - p_j^{\alpha_j - 1}) = \prod_{j=1}^{k} p_j^{\alpha_j} \left(1 - p_j^{-1}\right) = n \prod_{j=1}^{k} \left(1 - p_j^{-1}\right),$$

απ' όπου έπονται οι τύποι (2.35) για τη συνάρτηση φι τού Euler. □

2.4.20 Παράδειγμα. Όταν $n = 304920$, ο δεύτερος τύπος εκ των (2.35) μας παρέχει την τιμή $\phi(n)$ ως ακολούθως:

$$\begin{aligned} \phi(304920) &= \phi\left(2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11^2\right) \\ &= 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11^2 \left(\tfrac{2-1}{2}\right)\left(\tfrac{3-1}{3}\right)\left(\tfrac{5-1}{5}\right)\left(\tfrac{7-1}{7}\right)\left(\tfrac{11-1}{11}\right) \\ &= 2^2 \cdot 3 \cdot 11 \cdot 2 \cdot 4 \cdot 6 \cdot 10 = 63360. \end{aligned}$$

2.4.21 Πόρισμα. *$\phi(d) \mid \phi(n)$, $\forall n \in \mathbb{N}$ και $\forall d \in \mathfrak{D}_n$* (βλ. 2.2.34).

ΑΠΟΔΕΙΞΗ. Εάν $n = 1$, τότε αυτό είναι προφανές. Εάν $n \geqslant 2$ και $n = \prod_{j=1}^{k} p_j^{\alpha_j}$ είναι η κανονική παράσταση (2.19) τού n σε γινόμενο πρώτων παραγόντων, όπου $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$, τότε

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},\ \forall d \in \mathfrak{D}_n,$$

όπου $\beta_1, \beta_2, \ldots, \beta_k \in \mathbb{N}_0$ με $0 \leqslant \beta_j \leqslant \alpha_j$, για κάθε $j \in \{1, \ldots, k\}$ (βλ. 2.3.15). Στην περίπτωση όπου $d = 1$, έχουμε προφανώς $\phi(1) = 1 \mid \phi(n)$. Εάν $d \geqslant 2$, τότε υπάρχει υποσύνολο δεικτών $\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, k\}$, $r \in \mathbb{N}$, με $\beta_{i_j} > 0$ για κάθε $j \in \{1, \ldots, r\}$. Εν τοιαύτη περιπτώσει, θέτοντας $A := \{p_1, \ldots, p_k\} \setminus \{p_{i_1}, \ldots, p_{i_r}\}$ λαμβάνουμε (ύστερα από εφαρμογή τού τύπου (2.35))

$$\begin{aligned} &\phi(n) = n \left(1 - \tfrac{1}{p_1}\right) \cdots \left(1 - \tfrac{1}{p_k}\right) \\ &= \left(d \left(1 - \tfrac{1}{p_{i_1}}\right) \cdots \left(1 - \tfrac{1}{p_{i_r}}\right)\right) \left(\tfrac{n}{d} \prod_{p \in A} \left(1 - \tfrac{1}{p}\right)\right) = \phi(d) \left(\tfrac{n}{d} \prod_{p \in A} \left(1 - \tfrac{1}{p}\right)\right), \end{aligned}$$

όπου $\prod_{p \in A} \left(1 - \frac{1}{p}\right) := 1$ όταν $A = \varnothing$. Εάν $A \neq \varnothing$ και $p \in A$, τότε $p \mid \frac{n}{d}$, διότι $p \mid n$ και $p \nmid d$, απ' όπου έπεται ότι $\frac{n}{d} \prod_{p \in A} \left(1 - \frac{1}{p}\right) \in \mathbb{N}$ και $\phi(d) \mid \phi(n)$. □

2.4.22 Θεώρημα (Θεώρημα τού Euler περί ισοτιμιών). *Έστω $n \in \mathbb{N}$, $n \geqslant 2$, και έστω a ένας ακέραιος με* μκδ$(a, n) = 1$. *Τότε*

$$\boxed{a^{\phi(n)} \equiv 1 (\text{mod } n).} \tag{2.36}$$

ΑΠΟΔΕΙΞΗ. Αρχικώς θα αποδείξουμε μέσω μαθηματικής επαγωγής ότι

$$a^{\phi(p^k)} \equiv 1 (\text{mod } p^k) \tag{2.37}$$

για οιονδήποτε *πρώτο* p, ο οποίος δεν διαιρεί τον a, και για οιονδήποτε φυσικό αριθμό k. Η ισοτιμία (2.37) είναι αληθής για $k = 1$, καθότι εκφράζει την ισοτιμία (2.30) τού «μικρού θεωρήματος» τού Fermat. Ας προϋποθέσουμε την ισχύ τής (2.37) για κάποιον παγιωμένο $k \geqslant 1$, κι ας γράψουμε τον $a^{\phi\left(p^k\right)}$ ως

$$a^{\phi\left(p^k\right)} = 1 + qp^k$$

για κάποιον ακέραιο q. Επειδή $\phi\left(p^{k+1}\right) = p^{k+1} - p^k = p(p^k - p^{k-1})$, έχουμε

$$\phi\left(p^{k+1}\right) = p\phi\left(p^k\right).$$

Το διωνυμικό ανάπτυγμα, σε συνδυασμό με το λήμμα 2.4.10 και το (iv) τής προτάσεως 2.4.4, μας δίδει

$$\begin{aligned} a^{\phi\left(p^{k+1}\right)} &= a^{p\phi\left(p^k\right)} = \left(a^{\phi\left(p^k\right)}\right)^p = \left(1 + qp^k\right)^p \\ &= 1 + \tbinom{p}{1}\left(qp^k\right) + \tbinom{p}{2}\left(qp^k\right)^2 + \cdots + \tbinom{p}{p-1}\left(qp^k\right)^{p-1} + \left(qp^k\right)^p \\ &\equiv 1 + \tbinom{p}{1}\left(qp^k\right) (\mathrm{mod}\ p^{k+1}). \end{aligned}$$

Δεδομένου ότι $p \mid \binom{p}{1} \Longrightarrow p^{k+1} \mid \binom{p}{1}\left(qp^k\right)$, η τελευταία αυτή ισοτιμία μας οδηγεί στη ζητουμένη: $a^{\phi\left(p^{k+1}\right)} \equiv 1 (\mathrm{mod}\ p^{k+1})$. Εν συνεχεία, υποθέτοντας ότι ισχύει μκδ$(n, a) = 1$ και ότι $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ είναι η κανονική παράσταση (2.19) τού n ως γινομένου πρώτων αριθμών, έχουμε

$$a^{\phi\left(p_j^{\alpha_j}\right)} \equiv 1 (\mathrm{mod}\ p_j^{\alpha_j}), \quad \forall j \in \{1, ..., s\} \tag{2.38}$$

(βάσει τού ό,τι έχουμε αποδείξει προηγουμένως). Παρατηρώντας ότι το $\phi(n)$ διαιρείται διά τού $\phi(p_j^{\alpha_j})$ (βάσει τού πορίσματος 2.4.21) έχουμε τη δυνατότητα υψώσεως αμφοτέρων των μελών τής (2.38) στη δύναμη $\frac{\phi(n)}{\phi(p_j^{\alpha_j})}$ (βλ. 2.4.4 (iii)), οπότε λαμβάνουμε

$$a^{\phi(n)} \equiv 1 (\mathrm{mod}\ p_j^{\alpha_j}), \quad \forall j \in \{1, ..., s\}.$$

Εάν $s = 1$, τότε η (2.36) είναι αληθής. Ας υποθέσουμε λοιπόν ότι $s \geqslant 2$. Επειδή μκδ$(p_j^{\alpha_j}, p_\varrho^{\alpha_\varrho}) = 1$, για κάθε $j, \varrho \in \{1, ..., s\}$ με $j \neq \varrho$, το πόρισμα 2.4.9 μας δίδει

$$a^{\phi(n)} \equiv 1 (\mathrm{mod}\ (\prod_{j=1}^{s} p_j^{\alpha_j})),$$

ήτοι την (2.36). □

2.4.23 Παράδειγμα. Ας υπολογίσουμε το υπόλοιπο τής διαιρέσεως τού 3^{256} διά τού 100. Επειδή μκδ$(3, 100) = 1$ και

$$\phi(100) = \phi\left(2^2 \cdot 5^2\right) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40,$$

η σχέση (2.36) μας πληροφορεί ότι $3^{40} \equiv 1 (\mathrm{mod}\, 100)$. Διαιρώντας τό 256 διά τού 40 λαμβάνουμε $256 = (6 \cdot 40) + 16$, οπότε $3^{256} \equiv \left(3^{40}\right)^6 \cdot 3^{16} \equiv 3^{16} (\mathrm{mod}\, 100)$. Ως εκ τούτου,

$$3^{16} \equiv (81)^4 \equiv (-19)^4 \equiv (361)^2 \equiv (61)^2 \equiv 21 (\mathrm{mod}\, 100),$$

απ' όπου έπεται ότι το 3^{256} διαιρούμενο διά τού 100 αφήνει ως υπόλοιπο το 21.

▸ **Περαιτέρω ιδιότητες τής ϕ και η συνάρτηση μ.** Επειδή η συνάρτηση φι τού Euler χρησιμοποιείται κατά κόρον στη Θεωρία Πεπερασμένων Ομάδων, θα παρατεθούν και κάποιες επιπρόσθετες ιδιότητές της, συμπεριλαμβανομένης τής εκφράσεώς της τη βοηθεία τής συναρτήσεως μι τού Möbius. (Βλ. πρόταση 2.4.32.)

2.4.24 Πρόταση. *Ο $\phi(n)$ είναι άρτιος για κάθε $n \geqslant 3$.*

Απόδειξη. Εάν $n = \prod_{j=1}^{k} p_j^{\alpha_j}$ είναι η κανονική παράσταση (2.19) ενός $n \geqslant 3$ ως γινομένου πρώτων αριθμών, τότε ο τύπος (2.35) γράφεται ως εξής:

$$\phi(n) = \prod_{j=1}^{k} \left(p_j^{\alpha_j} - p_j^{\alpha_j - 1} \right) = \prod_{j=1}^{k} p_j^{\alpha_j - 1} (p_j - 1). \tag{2.39}$$

Περίπτωση πρώτη. Εάν ο n είναι *περιττός*, τότε οι $p_1, \ldots, p_k$ είναι κατ' ανάγκην περιττοί και, ως εκ τούτου, οι $p_1 - 1, \ldots, p_k - 1$ άρτιοι. Άρα και ο $\phi(n)$ είναι άρτιος (λόγω τής (2.39)).

Περίπτωση δεύτερη. Εάν ο n είναι *άρτιος*, τότε $n = 2^{\nu} m$, για κάποιους $m, \nu \in \mathbb{N}$, όπου ο m είναι περιττός. (Όταν $\nu = 1$, έχουμε $m \geqslant 3$, διότι εξ υποθέσεως $n \geqslant 3$.) Συνεπώς,

$$\phi(n) = \begin{cases} 2^{\nu-1}, & \text{όταν } m = 1 \text{ και } \nu \geqslant 2, \\ 2^{\nu-1}\phi(m), & \text{όταν } m \geqslant 3 \text{ και } \nu \geqslant 2, \\ \phi(m), & \text{όταν } m \geqslant 3 \text{ και } \nu = 1. \end{cases}$$

Στις δύο πρώτες υποπεριπτώσεις ο $\phi(n)$ είναι προδήλως άρτιος. Στην τρίτη υποπερίπτωση, $\phi(n) = \phi(m)$, όπου ο m είναι περιττός και $m \geqslant 3$, οπότε αρκεί να ληφθούν υπ' όψιν (γι' αυτόν) όσα προαναφέρθησαν στην πρώτη περίπτωση. □

2.4.25 Πρόταση. $\phi(n) = 2 \iff n \in \{3, 4, 6\}$.

Απόδειξη. Επειδή $\phi(1) = \phi(2) = 1$, θεωρούμε τυχόντα φυσικό αριθμό $n \geqslant 3$. Εάν υποθέσουμε ότι $\phi(n) = 2$, τότε για κάθε πρώτο διαιρέτη p τού n έχουμε (μέσω τού λήμματος 2.4.18 και τού πορίσματος 2.4.21) $\phi(p) = p - 1 \mid 2 (= \phi(n))$, οπότε $p \in \{2, 3\}$. Άρα είτε $n = 2^a$ είτε $n = 2^a \cdot 3^b$ είτε $n = 3^b$, για κάποιους $a, b \in \mathbb{N}$. Στην πρώτη περίπτωση, $a \geqslant 2$ και $2 = \phi(n) = 2^{a-1}$, οπότε $a = 2$. Στη δεύτερη περίπτωση, $2 = \phi(n) = 2^a \cdot 3^{b-1}$, οπότε $a = b = 1$. Στην τρίτη περίπτωση έχουμε $2 = \phi(n) = 2 \cdot 3^{b-1}$, οπότε $b = 1$. Κατά συνέπειαν, $n \in \{3, 4, 6\}$. (Το αντίστροφο είναι προφανές.) □

2.4.26 Πρόταση. *Εάν $m, n, \nu \in \mathbb{N}$, και $m \mid n$, τότε $\phi(m^{\nu} n) = m^{\nu} \phi(n)$.*

Απόδειξη. Εάν $n = 1$, τότε $m = 1$, οπότε η ανωτέρω ισότητα είναι προδήλως αληθής. Εάν $n \geqslant 2$ και $n = \prod_{j=1}^{k} p_j^{\alpha_j}$ είναι η κανονική παράσταση (2.19) τού n ως γινομένου πρώτων αριθμών, τότε (σύμφωνα με το λήμμα 2.3.15) $m = \prod_{j=1}^{k} p_j^{\beta_j}$, όπου $\beta_j \in \{0, 1, ..., \alpha_j\}$ για κάθε $j \in \{1, ..., k\}$, οπότε

$$m^{\nu} n = \prod_{j=1}^{k} p_j^{\alpha_j + \nu\beta_j} \Rightarrow \phi(m^{\nu} n) = m^{\nu} n \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right) = m^{\nu} \phi(n)$$

επί τη βάσει τού τύπου (2.35). □

2.4.27 Πρόταση. *Για οιουσδήποτε $m, n \in \mathbb{N}$ ισχύει η ισότητα*

$$\boxed{\phi(mn)\,\phi(\text{μκδ}(m, n)) = \phi(m)\,\phi(n)\,\text{μκδ}(m, n).} \tag{2.40}$$

Απόδειξη. Θέτοντας $d := \text{μκδ}(m, n)$, παρατηρούμε ότι για $d = 1$ η (2.40) είναι η ήδη αποδειχθείσα (2.32), διότι $\phi(1) = 1$. Ας υποθέσουμε ότι $d \geqslant 2$. Διακρίνουμε τρεις περιπτώσεις:

Περίπτωση πρώτη. Εάν $m \mid n$, τότε $d = m$ και η (2.40) είναι αληθής λόγω τής προτάσεως 2.4.26.

Περίπτωση δεύτερη. Παρομοίως, η (2.40) είναι αληθής όταν $n \mid m$.

Περίπτωση τρίτη. Εάν $m \nmid n$ και $n \nmid m$, και εάν υποτεθεί ότι οι $r_1, \ldots, r_t$ ($t \in \mathbb{N}$) είναι οι (σαφώς διακεκριμένοι για $t > 1$) πρώτοι διαιρέτες τού d,τότε οι m, n γράφονται υπό τη μορφή

$$n = \left(\prod_{j=1}^{k} p_j^{\alpha_j}\right)\left(\prod_{s=1}^{t} r_s^{\gamma_s}\right),\ m = \left(\prod_{\varrho=1}^{l} q_\varrho^{\beta_\varrho}\right)\left(\prod_{s=1}^{t} r_s^{\gamma_s}\right),\ \ k, l \in \mathbb{N},$$

όπου $\alpha_1, ..., \alpha_k, \beta_1, ..., \beta_l, \gamma_1, ..., \gamma_t \in \mathbb{N}$, $d = \prod_{s=1}^{t} r_s^{\gamma_s}$ και $p_1, \ldots, p_k, q_1, ..., q_l$ πρώτοι αριθμοί (σαφώς διακεκριμένοι, όταν $k > 1$ ή/και $l > 1$) με

$$\{p_1, \ldots, p_k, q_1, ..., q_l\} \cap \{r_1, \ldots, r_t\} = \varnothing.$$

Επομένως, $mn = \left(\prod_{j=1}^{k} p_j^{\alpha_j}\right)\left(\prod_{\varrho=1}^{l} q_\varrho^{\beta_\varrho}\right)\left(\prod_{s=1}^{t} r_s^{2\gamma_s}\right)$,

$$\phi(mn) = mn\left(\prod_{j=1}^{k}\left(1 - \tfrac{1}{p_j}\right)\right)\left(\prod_{\varrho=1}^{l}\left(1 - \tfrac{1}{q_\varrho}\right)\right)\left(\prod_{s=1}^{t}\left(1 - \tfrac{1}{r_s}\right)\right)$$

(βάσει τού τύπου (2.35)) και

$$\begin{aligned}\phi(mn)\,\phi(d) &= \phi(mn)\, d \prod_{s=1}^{t}\left(1 - \tfrac{1}{r_s}\right)\\ &= mn\left(\prod_{j=1}^{k}\left(1 - \tfrac{1}{p_j}\right)\right)\left(\prod_{\varrho=1}^{l}\left(1 - \tfrac{1}{q_\varrho}\right)\right)\left(\prod_{s=1}^{t}\left(1 - \tfrac{1}{r_s}\right)\right)^2 d\\ = m\left(\prod_{j=1}^{k}\left(1 - \tfrac{1}{p_j}\right)\right)\left(\prod_{s=1}^{t}\left(1 - \tfrac{1}{r_s}\right)\right) &n\left(\prod_{\varrho=1}^{l}\left(1 - \tfrac{1}{q_\varrho}\right)\right)\left(\prod_{s=1}^{t}\left(1 - \tfrac{1}{r_s}\right)\right) d,\end{aligned}$$

όπου το τελευταίο γινόμενο ισούται με $\phi(m)\,\phi(n)\,d$. □

2.4.28 Πόρισμα. *Για οιουσδήποτε $m, n \in \mathbb{N}$ ισχύει η ισότητα*

$$\boxed{\phi(m)\,\phi(n) = \phi(\text{μκδ}(m,n))\,\phi(\text{εκπ}(m,n))\,.} \tag{2.41}$$

Απόδειξη. Κατά την πρόταση 2.4.27,

$$\frac{\phi(m)\,\phi(n)}{\phi(\text{μκδ}(m,n))} = \frac{\phi(mn)}{\text{μκδ}(m,n)}. \tag{2.42}$$

Επειδή $mn = \text{μκδ}(m,n)\text{εκπ}(m,n)$ (βλ. 2.2.29) και

$$[\text{μκδ}(m,n) \mid m \text{ και } m \mid \text{εκπ}(m,n)] \Rightarrow \text{μκδ}(m,n) \mid \text{εκπ}(m,n),$$

εφαρμόζοντας την πρόταση 2.4.26 (για $\nu = 1$ και με τους $\text{μκδ}(m,n)$ και $\text{εκπ}(m,n)$ στη θέση των εκεί παρατεθέντων m και n) λαμβάνουμε

$$\phi(mn) = \phi(\text{μκδ}(m,n)\text{εκπ}(m,n)) = \text{μκδ}(m,n)\phi(\text{εκπ}(m,n))\,. \tag{2.43}$$

Η (2.41) έπεται άμεσα από τις (2.42) και (2.43). □

2.4.29 Πρόταση. *Για κάθε $n \in \mathbb{N}$ ισχύει η ισότητα*

$$\boxed{\sum_{d \in \mathfrak{D}_n} \phi(d) = n.} \tag{2.44}$$

Απόδειξη. Εάν $n = 1$, τότε η (2.44) είναι προφανής. Εάν $n \geqslant 2$ και εάν

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad k \in \mathbb{N},$$

είναι η κανονική παράσταση (2.19) τού n ως γινομένου πρώτων αριθμών, τότε (βάσει τού λήμματος 2.3.15) κάθε διαιρέτης $d \in \mathbb{N}$ τού n είναι τής μορφής

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},\ \beta_1, \ldots, \beta_k \in \mathbb{N}_0,\ \beta_j \leqslant \alpha_j,\ \forall j \in \{1, \ldots, k\},$$

οπότε μέσω τού θεωρήματος 2.4.17 (εφαρμοζόμενου για καθέναν εκ των διαιρετών d τού n) και τού τύπου (2.35) λαμβάνουμε

$$\sum_{d \in \mathfrak{D}_n} \phi(d) = \sum_{0 \leqslant \beta_1 \leqslant \alpha_1, \ldots, 0 \leqslant \beta_k \leqslant \alpha_k} \phi(p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k})$$

$$= \sum_{0 \leqslant \beta_1 \leqslant \alpha_1, \ldots, 0 \leqslant \beta_k \leqslant \alpha_k} \phi(p_1^{\beta_1}) \phi(p_2^{\beta_2}) \cdots \phi(p_k^{\beta_k})$$

$$= \left(\sum_{\beta_1=0}^{\alpha_1} \phi(p_1^{\beta_1}) \right) \left(\sum_{\beta_2=0}^{\alpha_2} \phi(p_2^{\beta_2}) \right) \cdots \left(\sum_{\beta_k=0}^{\alpha_k} \phi(p_k^{\beta_k}) \right) = \prod_{j=1}^{k} \left(\sum_{\beta_j=0}^{\alpha_j} \phi(p_j^{\beta_j}) \right)$$

$$= \prod_{j=1}^{k} \left(1 + (p_j - 1) + (p_j^2 - p_j) + \cdots + (p_j^{\alpha_j} - p_j^{\alpha_j - 1}) \right) = \prod_{j=1}^{k} p_j^{\alpha_j},$$

όπου το τελευταίο γινόμενο είναι το n. □

2.4.30 Ορισμός. Η απεικόνιση $\mu : \mathbb{N} \to \mathbb{N}$ η οριζόμενη μέσω των τύπων $\mu(1) := 1$ και

$$\boxed{\mu(n) := \begin{cases} (-1)^k, & \text{όταν } \alpha_1 = \alpha_2 = \cdots = \alpha_k = 1, \\ 0, & \text{όταν } \exists j \in \{1, ..., k\} : \alpha_j > 1, \end{cases}}$$

όπου $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $k \in \mathbb{N}$, η κανονική παράσταση τού n ως γινομένου πρώτων αριθμών για $n \geqslant 2$, καλείται **συνάρτηση μι τού Möbius**.

2.4.31 Πρόταση. *Για κάθε $n \in \mathbb{N}$ ισχύει η ισότητα*

$$\boxed{\sum_{d \in \mathfrak{D}_n} \mu(d) = \begin{cases} 1, & \text{όταν } n = 1, \\ 0, & \text{όταν } n \geqslant 2. \end{cases}} \tag{2.45}$$

Απόδειξη. Η (2.45) είναι προδήλως αληθής όταν $n = 1$. Ας υποθέσουμε ότι $n \geqslant 2$ και ότι $n = \prod_{j=1}^{k} p_j^{\alpha_j}$ είναι η κανονική παράσταση (2.19) τού n ως γινομένου πρώτων αριθμών. Εν τοιαύτη περιπτώσει, το πλήθος όλων των θετικών ακεραίων διαιρετών τού n που διαιρούνται διά i εκ των $p_1, \ldots, p_k$ ($i \in \{1, ..., k\}$) και που (ταυτοχρόνως) δεν διαιρούνται διά $p_j^{\beta_j}$, όπου $\beta_j \in \{2, \ldots, \alpha_j\}$ για κάποιον $j \in \{1, ..., k\}$ με

$\alpha_j \geqslant 2$, είναι ίσο με $\binom{k}{i}$. Επομένως,

$$\begin{aligned}\sum_{d\in\mathfrak{D}_n}\mu(d) &= 1+\sum_{d\in\mathfrak{D}_n\smallsetminus\{1\}}\mu(d) = 1+\sum_{i=1}^{k}\binom{k}{i}(-1)^i\\ &= \sum_{i=0}^{k}\binom{k}{i}(-1)^i = (1-1)^k = 0\end{aligned}$$

(από τον δυωνυμικό τύπο). Άρα η (2.45) είναι αληθής και για $n \geqslant 2$. □

2.4.32 Πρόταση. *Για κάθε $n \in \mathbb{N}$ ισχύει η ισότητα*

$$\boxed{\phi(n) = \sum_{d\in\mathfrak{D}_n}\mu(d)\,\frac{n}{d}.} \tag{2.46}$$

Απόδειξη. Εκκινώντας από την (2.31), η (2.45) δίδει

$$\phi(n) = \sum_{\ell=1}^{n}\left\lfloor\frac{1}{\mu\kappa\delta(\ell,n)}\right\rfloor = \sum_{\ell=1}^{n}\left(\sum_{d\in\mathfrak{D}_{\mu\kappa\delta(\ell,n)}}\mu(d)\right) = \sum_{\ell=1}^{n}\left(\sum_{d\in\mathfrak{D}_n,d\in\mathfrak{D}_\ell}\mu(d)\right).$$

Για κάθε παγιωμένον $d \in \mathfrak{D}_n$ η άθροιση περιλαμβάνει όλους τους $\ell \in \{1,...,n\}$ για τους οποίους υπάρχει κάποιος $j \in \mathbb{N}$ με $\ell = jd$. Επομένως, $1 \leqslant j \leqslant \frac{n}{d}$ και

$$\phi(n) = \sum_{d\in\mathfrak{D}_n}\left(\sum_{j=1}^{\frac{n}{d}}\mu(d)\right) = \sum_{d\in\mathfrak{D}_n}\mu(d)\left(\sum_{j=1}^{\frac{n}{d}}1\right) = \sum_{d\in\mathfrak{D}_n}\mu(d)\,\frac{n}{d},$$

οπότε η ισότητα (2.46) είναι αληθής. □

▸ **Το σύνολο $\mathbb{Z}_m$ και οι συνήθεις εσωτερικές πράξεις οι οριζόμενες επ' αυτού.** Το να είναι δυο ακέραιοι a, b ισοϋπόλοιποι κατά μόδιο m ($m \in \mathbb{N}$) αποτελεί μια σχέση ισοδυναμίας. Επί τού συνόλου $\mathbb{Z}_m$ των οριζομένων κλάσεων ισοδυναμίας κληρονομούνται πράξεις *προσθέσεως* και *πολλαπλασιασμού* από τις αντίστοιχες (συνήθεις) πράξεις τις θεσπισθείσες επί τού ιδίου τού $\mathbb{Z}$.

2.4.33 Πρόταση. *Η διμελής σχέση ισοτιμίας (κατά παγιωμένο μόδιο $m \in \mathbb{N}$):*

$$\boxed{a \sim_m b \underset{\text{ορσ}}{\Longleftrightarrow} a \equiv b (\mathrm{mod}\, m)}$$

αποτελεί μια σχέση ισοδυναμίας επί τού συνόλου $\mathbb{Z}$ των ακεραίων.

Απόδειξη. . Θεωρούμε τυχόντες $a, b, c \in \mathbb{Z}$. Η διμελής σχέση "$\sim_m$" είναι αυτοπαθής, διότι $a - a = 0 = 0 \cdot m$, συμμετρική, διότι $a - b = km \Rightarrow b - a = (-k)\,m$, και μεταβατική λόγω τής συνεπαγωγής

$$[a - b = k_1 m \text{ και } b - c = k_2 m] \Rightarrow a - c = (k_1 + k_2)\,m,$$

όπου $k, k_1, k_2 \in \mathbb{Z}$, οπότε $a \equiv a (\mathrm{mod}\, m)$, $a \equiv b (\mathrm{mod}\, m) \Longrightarrow b \equiv a (\mathrm{mod}\, m)$, και εάν $a \equiv b (\mathrm{mod}\, m)$ και $b \equiv c (\mathrm{mod}\, m)$, τότε $a \equiv c (\mathrm{mod}\, m)$. □

2.4.34 Σημείωση. (i) Όταν $a \equiv b (\mathrm{mod}\, m)$, λόγω τής συμμετρικότητας τής διμελούς σχέσεως "$\sim_m$" μπορούμε να χαρακτηρίζουμε τους a, b ως *ισοτίμους* κατά μόδιο m, χωρίς να καταφεύγουμε σε διάκριση προτεραιότητας, ήτοι στο ποιος εξ αυτών

προηγείται ή έπεται τού άλλου.

(ii) Για να δώσουμε έμφαση στην εξάρτηση από το m συμβολίζουμε ως

$$\dots, [-2]_m, [-1]_m, [0]_m, [1]_m, [2]_m, \dots$$

τις κλάσεις ισοδυναμίας των ακεραίων (ως προς την "$\sim_m$") και ως

$$\boxed{\mathbb{Z}_m := \mathbb{Z}/\sim_m}$$

το **σύνολο των κλάσεων υπολοίπων (ή κλάσεων ισοτιμίας) των ακεραίων κατά μόδιο** m (ή **modulo** m).

2.4.35 Πρόταση. *Το ανωτέρω σύνολο των κλάσεων υπολοίπων γράφεται σε «ανηγμένη» μορφή ως ακολούθως:*

$$\boxed{\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}.} \tag{2.47}$$

(Τούτο σημαίνει ότι τα εντός των αγκίστρων αναγραφόμενα στοιχεία είναι *σαφώς διακεκριμένα* (ήτοι ανά δύο διαφορετικά, αποκλείοντας την επανάληψη κάποιου εξ αυτών).)

ΑΠΟΔΕΙΞΗ. Επειδή *κάθε* $a \in \mathbb{Z}$ μπορεί να γραφεί υπό τη μορφή $a = qm+r$, όπου τα q και r είναι κατάλληλοι ακέραιοι αριθμοί και $0 \leqslant r < m$ (ήτοι το r είναι το υπόλοιπο τής διαιρέσεως τού a διά τού m, βλ. (2.1)), λαμβάνουμε την ισότητα $[a]_m = [r]_m$. Εξ αυτού συνάγεται ότι οι *σαφώς διακεκριμένες* κλάσεις ισοδυναμίας που διαθέτουμε είναι οι μόνον οι $[0]_m, [1]_m, \dots, [m-1]_m$. □

2.4.36 Σημείωση. Χρησιμοποιώντας τήν ορολογία που εισήχθη στο 1.3.19 διαπιστώνουμε μέσω τής προτάσεως 2.4.35 ότι το σύνολο $\{0, 1, \dots, m-1\}$ είναι ένα *πλήρες σύστημα εκπροσώπων*[17] *τού* $\mathbb{Z}$ *ως προς την* "$\sim_m$", οπότε

$$\mathbb{Z} = \coprod \{[j]_m \,|\, j \in \{0, 1, \dots, m-1\}\}.$$

Προσοχή! Για κάθε $j \in \{0, 1, \dots, m-1\}$ το $[j]_m$ είναι *ένα* στοιχείο τού $\mathbb{Z}_m$ αλλά ως υποσύνολο τού $\mathbb{Z}$ αποτελείται από *όλους τους ακεραίους που διαιρούμενοι* διά τού m *αφήνουν υπόλοιπο* j.

2.4.37 Παραδείγματα. (i) Πέραν τού $\{0, 1, \dots, m-1\}$, *και* τα $\{1, \dots, m\}$ και

$$\left\{ \begin{array}{ll} \left\{-\left(\frac{m}{2}-1\right), \dots, -1, 0, 1, \dots, \frac{m}{2}\right\}, & \text{όταν } m \equiv 0 (\mathrm{mod}\, 2) \\ \left\{-\frac{m-1}{2}, \dots, -1, 0, 1, \dots, \frac{m-1}{2}\right\}, & \text{όταν } m \equiv 1 (\mathrm{mod}\, 2) \end{array} \right\}$$

αποτελούν «φυσικώς κατασκευαζόμενα» πλήρη συστήματα εκπροσώπων τού $\mathbb{Z}$ ως προς την "$\sim_m$".

(ii) Το $\{14, 24, 9, -11, 34, 68, -21, 87\}$ αποτελεί ένα πλήρες σύστημα εκπροσώπων τού $\mathbb{Z}$ ως προς την "$\sim_8$", διότι

$$\begin{array}{llll} 24 \equiv 0 (\mathrm{mod}\, 8), & 9 \equiv 1 (\mathrm{mod}\, 8), & 34 \equiv 2 (\mathrm{mod}\, 8), & -21 \equiv 3 (\mathrm{mod}\, 8), \\ 68 \equiv 4 (\mathrm{mod}\, 8), & -11 \equiv 5 (\mathrm{mod}\, 8), & 14 \equiv 6 (\mathrm{mod}\, 8), & 87 \equiv 7 (\mathrm{mod}\, 8). \end{array}$$

(iii) Όταν $m \geqslant 3$, το $\{1, 2^2, 3^2, \dots, m^2\}$ δεν αποτελεί ένα πλήρες (παρά μόνον ένα *μερικό*) σύστημα εκπροσώπων τού $\mathbb{Z}$ ως προς την "$\sim_m$", διότι προφανώς ισχύει

$$(m-1)^2 - 1 = m(m-2) \Longrightarrow (m-1)^2 \equiv 1 (\mathrm{mod}\, m).$$

[17] Προφανώς, κάθε πλήρες σύστημα εκπροσώπων τού $\mathbb{Z}$ ως προς την "$\sim_m$" είναι τής μορφής $\{a_0, a_1, \dots, a_{m-1}\}$, όπου $a_j \in \mathbb{Z}$ και $a_j \equiv j (\mathrm{mod}\, m)$, $\forall j \in \{0, 1, \dots, m-1\}$.

Επί τού $\mathbb{Z}_m$ ορίζονται δύο εσωτερικές πράξεις "$+_{\mathbb{Z}_m}$" και "$\cdot_{\mathbb{Z}_m}$":

$$([a]_m, [b]_m) \longmapsto [a]_m +_{\mathbb{Z}_m} [b]_m, \quad ([a]_m, [b]_m) \longmapsto [a]_m \cdot_{\mathbb{Z}_m} [b]_m$$

(*προσθέσεως* και *πολλαπλασιασμού*, αντιστοίχως) μέσω των τύπων

$$\boxed{\begin{array}{c} [a]_m +_{\mathbb{Z}_m} [b]_m := [a+b]_m, \\ [a]_m \cdot_{\mathbb{Z}_m} [b]_m := [ab]_m. \end{array}} \tag{2.48}$$

2.4.38 Σημείωση. (i) Η απόδειξη τού ότι οι "$+_{\mathbb{Z}_m}$" και "$\cdot_{\mathbb{Z}_m}$" είναι *καλώς ορισμένες* πράξεις μέσω των τύπων (2.48), ήτοι τού ότι ισχύει η συνεπαγωγή

$$\left.\begin{array}{l} [a]_m = [a']_m \\ [b]_m = [b']_m \end{array}\right\} \Rightarrow \left\{\begin{array}{c} [a]_m +_{\mathbb{Z}_m} [b]_m = [a']_m +_{\mathbb{Z}_m} [b']_m \\ \text{και } [a]_m \cdot_{\mathbb{Z}_m} [b]_m = [a']_m \cdot_{\mathbb{Z}_m} [b']_m \end{array}\right\},$$

είναι εύκολη και αφήνεται ως άσκηση.

(ii) Επειδή κατά την εφαρμογή των ορισμών (2.48) οι ακέραιοι $a+b$ και ab ενδέχεται να είναι $\geqslant m$ (ακόμη και όταν οι a και b είναι ειλημμένοι από το σύνολο $\{0, 1, ..., m-1\}$), για να παραμείνουμε στην περιγραφή (2.47) τού $\mathbb{Z}_m$ επιλέγουμε ως εκπροσώπους των κλάσεων ισοδυναμιών τους ως προς την "$\sim_m$" τα υπόλοιπα που αφήνουν αφού διαιρεθούν διά τού m. Επί παραδείγματι, όταν $m = 6$, οι υπονοούμενοι εκπρόσωποι των *αθροισμάτων* δύο τυχόντων στοιχείων ειλημμένων από το $\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$ έχουν καταχωρισθεί στον ακόλουθο κατάλογο:

$+_{\mathbb{Z}_6}$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$
$[2]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$
$[3]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$
$[4]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$
$[5]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$

Ο αντίστοιχος κατάλογος που περιλαμβάνει τα *γινόμενα* είναι ο εξής:

$\cdot_{\mathbb{Z}_6}$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$
$[1]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[2]_6$	$[0]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
$[4]_6$	$[0]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$
$[5]_6$	$[0]_6$	$[5]_6$	$[4]_6$	$[3]_6$	$[2]_6$	$[1]_6$

Οι κύριες ιδιότητες των πράξεων "$+_{\mathbb{Z}_m}$" και "$\cdot_{\mathbb{Z}_m}$" περιγράφονται στις προτάσεις 2.4.39 και 2.4.40. (Οι αποδείξεις τους βασίζονται στις γνωστές ιδιότητες τής προσθέσεως και τού πολλαπλασιασμού ακεραίων, και αφήνονται ως άσκηση.)

2.4.39 Πρόταση (Ιδιότητες προσθέσεως). *Η πράξη "$+_{\mathbb{Z}_m}$" έχει τις εξής ιδιότητες*:

(i) **[Μεταθετική ιδιότητα]** $[a]_m +_{\mathbb{Z}_m} [b]_m = [b]_m +_{\mathbb{Z}_m} [a]_m, \forall (a, b) \in \mathbb{Z} \times \mathbb{Z}$.

(ii) **[Προσεταιριστική ιδιότητα]** *Για οιουσδήποτε $a, b, c \in \mathbb{Z}$ ισχύει η ισότητα*

$$([a]_m +_{\mathbb{Z}_m} [b]_m) +_{\mathbb{Z}_m} [c]_m = [a]_m +_{\mathbb{Z}_m} ([b]_m +_{\mathbb{Z}_m} [c]_m).$$

(iii) **[Νόμος τής διαγραφής]** *Για οιουσδήποτε* $a, b, c \in \mathbb{Z}$ *ισχύει η συνεπαγωγή*

$$[a]_m +_{\mathbb{Z}_m} [c]_m = [b]_m +_{\mathbb{Z}_m} [c]_m \Longrightarrow [a]_m = [b]_m.$$

(iv) **[Ύπαρξη ουδετέρου στοιχείου]** *Το* $[0]_m$ *είναι ουδέτερο στοιχείο τού* $\mathbb{Z}_m$ *ως προς την* "$+_{\mathbb{Z}_m}$" (βλ. 1.5.6), *δηλαδή* $[0]_m +_{\mathbb{Z}_m} [a]_m = [a]_m = [a]_m +_{\mathbb{Z}_m} [0]_m$.

(v) **[Ύπαρξη συμμετρικού στοιχείου]** *Κάθε* $[a]_m \in \mathbb{Z}_m$ *έχει την κλάση ισοτιμίας* $[-a]_m$ *ως συμμετρικό του στοιχείο ως προς την* "$+_{\mathbb{Z}_m}$" (βλ. 1.5.11), *δηλαδή*

$$[-a]_m +_{\mathbb{Z}_m} [a]_m = [0]_m = [a]_m +_{\mathbb{Z}_m} [-a]_m.$$

2.4.40 Πρόταση (Ιδιότητες πολλαπλασιασμού). *Η πράξη* "$\cdot_{\mathbb{Z}_m}$" *έχει τις εξής ιδιότητες*:

(i) **[Μεταθετική ιδιότητα]** *Για οιουσδήποτε* $a, b \in \mathbb{Z}$ *ισχύει η ισότητα*

$$[a]_m \cdot_{\mathbb{Z}_m} [b]_m = [b]_m \cdot_{\mathbb{Z}_m} [a]_m.$$

(ii) **[Προσεταιριστική ιδιότητα]** *Για οιουσδήποτε* $a, b, c \in \mathbb{Z}$ *ισχύει η ισότητα*

$$([a]_m \cdot_{\mathbb{Z}_m} [b]_m) \cdot_{\mathbb{Z}_m} [c]_m = [a]_m \cdot_{\mathbb{Z}_m} ([b]_m \cdot_{\mathbb{Z}_m} [c]_m).$$

(iii) *Για οιονδήποτε* $a \in \mathbb{Z}$ *ισχύουν οι ισότητες*

$$[0]_m \cdot_{\mathbb{Z}_m} [a]_m = [0]_m = [a]_m \cdot_{\mathbb{Z}_m} [0]_m.$$

(iv) **[Ύπαρξη ουδετέρου στοιχείου]** *Το* $[1]_m$ *είναι ουδέτερο στοιχείο τού* $\mathbb{Z}_m$ *ως προς την* "$\cdot_{\mathbb{Z}_m}$" (βλ. 1.5.6), *δηλαδή* $[1]_m \cdot_{\mathbb{Z}_m} [a]_m = [a]_m = [a]_m \cdot_{\mathbb{Z}_m} [1]_m$.

(v) *Για οιουσδήποτε* $a, b \in \mathbb{Z}$ *ισχύουν οι ισότητες*

$$[-a]_m \cdot_{\mathbb{Z}_m} [b]_m = [-ab]_m = [a]_m \cdot_{\mathbb{Z}_m} [-b]_m.$$

(vi) **[Επιμεριστική ιδιότητα τού πολλαπλασιασμού ως προς την πρόσθεση]** *Για οιουσδήποτε* $a, b, c \in \mathbb{Z}$ *ισχύουν οι ισότητες*

$$[a]_m \cdot_{\mathbb{Z}_m} ([b]_m +_{\mathbb{Z}_m} [c]_m) = ([a]_m \cdot_{\mathbb{Z}_m} [b]_m) +_{\mathbb{Z}_m} ([a]_m \cdot_{\mathbb{Z}_m} [c]_m),$$
$$([a]_m +_{\mathbb{Z}_m} [b]_m) \cdot_{\mathbb{Z}_m} [c]_m = ([a]_m \cdot_{\mathbb{Z}_m} [c]_m) +_{\mathbb{Z}_m} ([b]_m \cdot_{\mathbb{Z}_m} [c]_m).$$

2.4.41 Πρόταση. *Ένα στοιχείο* $[a]_m$ *τού* $\mathbb{Z}_m$ *διαθέτει αντίστροφο (ήτοι συμμετρικό στοιχείο ως προς την* "$\cdot_{\mathbb{Z}_m}$" *εάν και μόνον εάν* $\text{μκδ}(a, m) = 1$.

Απόδειξη[18]. Έστω ότι το $[a]_m$ διαθέτει το $[b]_m$ ως αντίστροφό του στοιχείο ως προς την "$\cdot_{\mathbb{Z}_m}$". Τότε $[a]_m \cdot_{\mathbb{Z}_m} [b]_m = [ab]_m = [1]_m \Rightarrow \exists k \in \mathbb{Z} : ab = mk+1$. Τούτο, σύμφωνα με το πόρισμα 2.2.8, σημαίνει ότι $\text{μκδ}(a, m) = 1$. Και αντιστρόφως· υποθέτοντας ότι $\text{μκδ}(a, m) = 1$, θα υπάρχουν $c, d \in \mathbb{Z}$, τέτοιοι ώστε

$$ac + md = 1 \Rightarrow [ac + md]_m = ([a]_m \cdot_{\mathbb{Z}_m} [c]_m) +_{\mathbb{Z}_m} ([m]_m \cdot_{\mathbb{Z}_m} [d]_m) = [1]_m$$
$$\Longrightarrow ([a]_m \cdot_{\mathbb{Z}_m} [c]_m) = [1]_m \text{ (λόγω τού 2.4.40 (iii) και τού ότι } [m]_m = [0]_m),$$

απ' όπου έπεται ότι το στοιχείο $[a]_m$ διαθέτει το $[c]_m$ ως αντίστροφό του στοιχείο ως προς την "$\cdot_{\mathbb{Z}_m}$". □

[18] Εάν το $[a]_m$ διαθέτει συμμετρικό στοιχείο ως προς την "$\cdot_{\mathbb{Z}_m}$", τότε αυτό θα είναι μονοσημάντως ορισμένο επί τη βάσει τής προτάσεως 1.5.13. Εξάλλου, επειδή η "$\cdot_{\mathbb{Z}_m}$" είναι μεταθετική (βλ. 2.4.40 (i)), αρκεί κανείς να περιορισθεί στην εξέταση υπάρξεως εκ δεξιών συμμετρικού στοιχείου τού $[a]_m$ (βλ. 1.5.14).

2.4.42 Σημείωση (Απλούστευση συμβολισμών). Υιοθετώντας, για λόγους χρηστικότητας, την «ελάφρυνση» των συμβολισμών των πράξεών μας, θα γράφουμε απλώς $[a]_m + [b]_m$ και $[a]_m \cdot [b]_m$ (ή $[a]_m[b]_m$) αντί των $[a]_m +_{\mathbb{Z}_m} [b]_m$ και $[a]_m \cdot_{\mathbb{Z}_m} [b]_m$, αντιστοίχως.

▸ **Γραμμικές ισοτιμίες.** Έστω ότι $m \in \mathbb{N}$ και $a, b \in \mathbb{Z}$. Κάθε ισοτιμία τής μορφής

$$\boxed{ax \equiv b (\mathrm{mod}\, m),} \tag{2.49}$$

με το x προσδιοριστέο εντός τού συνόλου των ακεραίων αριθμών, καλείται **γραμμική ισοτιμία** (με *άγνωστό της* τον x). Λέμε ότι ένας $x_0 \in \mathbb{Z}$ *πληροί* (ή *επαληθεύει*) την (2.49) όταν $ax_0 \equiv b (\mathrm{mod}\, m)$. Εν τοιαύτη περιπτώσει, *και οιοσδήποτε άλλος* εκπρόσωπος τής κλάσεως υπολοίπων $[x_0]_m$ τού x_0 επαληθεύει την (2.49). Πράγματι· εάν $y \in [x_0]_m$, τότε $[y]_m = [x_0]_m$, απ' όπου έπεται ότι $y \equiv x_0 (\mathrm{mod}\, m)$, οπότε $ay \equiv ax_0 \equiv b (\mathrm{mod}\, m)$. Ως εκ τούτου, όταν ομιλούμε για μια **λύση** $x_0 \in \mathbb{Z}$ **τής** (2.49) **κατά μόδιο** m, εννοούμε ολόκληρη[19] την κλάση $[x_0]_m$, όπου ο x_0 πληροί την (2.49). Επίσης, όταν εργαζόμαστε με συγκεκριμένα παραδείγματα και συναντούμε μια λύση $[x_0]_m$, για να εμπίπτουμε στην περιγραφή που δώσαμε για το σύνολο $\mathbb{Z}_m$ μέσω τής προτάσεως 2.4.35 προτιμούμε να παραθέτουμε τον *μοναδικό* εκπρόσωπο x_0' τής κλάσεως υπολοίπων $[x_0]_m$ ο οποίος ανήκει στο σύνολο $\{0, 1, \ldots, m-1\}$, ήτοι να καταφεύγουμε σε *αναγωγή* τού x_0 κατά μόδιο m κατόπιν διαιρέσεώς του διά τού m (βλ. απόδειξη τής 2.4.35).

Σημειωτέον ότι υπάρχουν γραμμικές ισοτιμίες οι οποίες δεν δέχονται καμία ακεραία λύση, όπως π.χ. η $2x \equiv 3 (\mathrm{mod}\, 4)$, αφού για κάθε $k \in \mathbb{Z}$ ο ακέραιος $2k-3$ είναι περιττός και επομένως $4 \nmid 2k-3$. Η πρόταση που ακολουθεί μας γνωστοποιεί την ικανή και αναγκαία συνθήκη για την ύπαρξη ακεραίων λύσεων τής (2.49) και, επιπροσθέτως, περιγράφει τη μορφή όλων των δυνατών λύσεων.

2.4.43 Πρόταση. *Δοθέντων ενός $m \in \mathbb{N}$ και δυο ακεραίων a, b, $a \neq 0$, η γραμμική ισοτιμία* (2.49) *διαθέτει λύσεις $x \in \mathbb{Z}$ κατά μόδιο m εάν και μόνον εάν $\mathrm{μκδ}\,(a, m) \mid b$. Επιπροσθέτως, όταν $\mathrm{μκδ}\,(a, m) \mid b$, η ισοτιμία* (2.49) *διαθέτει ακριβώς $\mathrm{μκδ}(a, m)$ σαφώς διακεκριμένες λύσεις $x \in \mathbb{Z}$ κατά μόδιο m, οι οποίες είναι τής μορφής*[20]

$$\boxed{x = x_0 + k\,\frac{m}{\mathrm{μκδ}\,(a, m)}, \quad k \in \{0, 1, \ldots, \mathrm{μκδ}\,(a, m) - 1\},} \tag{2.50}$$

όπου x_0 μια ειδική λύση τής (2.49).

Απόδειξη. Εάν η (2.49) δέχεται μια λύση $x \in \mathbb{Z}$ κατά μόδιο m, τότε

$$ax \equiv b (\mathrm{mod}\ m) \Longrightarrow m \mid ax - b \Longrightarrow (\exists k \in \mathbb{Z} : b = ax - km)\,.$$

Επομένως,

$$\left.\begin{array}{l} \mathrm{μκδ}\,(a, m) \mid a \\ \mathrm{μκδ}\,(a, m) \mid m \end{array}\right\} \underset{(\text{βλ. } 2.1.5\ (\text{vi}))}{\Longrightarrow} \mathrm{μκδ}\,(a, m) \mid ax - km\ (= b).$$

Και αντιστρόφως· εάν $\mathrm{μκδ}(a, m) \mid b$, τότε $b = \mathrm{μκδ}(a, m)\, b'$ για κάποιον $b' \in \mathbb{Z}$. Επειδή, κατά το (ii) τής προτάσεως 2.2.14, ισχύει η

$$\mathrm{μκδ}\left(\tfrac{a}{\mathrm{μκδ}(a,m)}, \tfrac{m}{\mathrm{μκδ}(a,m)}\right) = 1 \underset{(\text{βλ. } 2.2.8)}{\Longrightarrow} \left(\exists \kappa, \lambda \in \mathbb{Z} : \kappa \tfrac{a}{\mathrm{μκδ}(a,m)} + \lambda \tfrac{m}{\mathrm{μκδ}(a,m)} = 1\right),$$

[19] Γι' αυτόν τον λόγο, δυο ακέραιες λύσεις x_1 και x_2 τής (2.49) λογίζονται ως *διαφορετικές* όταν $x_1 \not\equiv x_2 (\mathrm{mod}\, m)$.

[20] Βλ., π.χ., https://www.a-calculator.com/congruence/ για έναν online calulator για τον προσδιορισμό αυτών των λύσεων.

λαμβάνουμε

$$b = \kappa \tfrac{ab}{\text{μκδ}(a,m)} + \lambda \tfrac{mb}{\text{μκδ}(a,m)} = a\left(\kappa b'\right) + m\left(\lambda b'\right) \Longrightarrow a\left(\kappa b'\right) \equiv b(\text{mod } m),$$

οπότε η κλάση ισοτιμίας τού $\kappa b'$ κατά μόδιο m είναι μια λύση τής (2.49).

Εν συνεχεία υποθέτουμε οτι το x_0 (ή, ακριβέστερα, η κλάση $[x_0]_m$) είναι μια παγιωμένη (ειδική) λύση τής (2.49). Προφανώς,

$$a\left(x_0 + k\frac{m}{\text{μκδ}\,(a,m)}\right) = ax_0 + \left(\frac{ak}{\text{μκδ}\,(a,m)}\right) m \equiv b(\text{mod } m),$$

οπότε οι ακέραιοι (2.50) αποτελούν πράγματι λύσεις τής (2.49). Οι ακέραιοι αυτοί είναι ανά δύο ανισότιμοι κατά μόδιο m, καθότι για οιουσδήποτε $k, k' \in \{0, 1, \ldots, \text{μκδ}(a,m) - 1\}$ με $k \neq k'$, έχουμε

$$\left|\left(x_0 + \tfrac{mk}{\text{μκδ}(a,m)}\right) - \left(x_0 + \tfrac{mk'}{\text{μκδ}(a,m)}\right)\right| = \left|k - k'\right| \tfrac{m}{\text{μκδ}(a,m)} < m,$$

αφού $|k - k'| < \text{μκδ}(a,m)$. Συνεπώς, λόγω τού (ii) τής προτάσεως 2.1.5, έχουμε

$$\begin{gathered} m \nmid \left(x_0 + \tfrac{mk}{\text{μκδ}(a,m)}\right) - \left(x_0 + \tfrac{mk'}{\text{μκδ}(a,m)}\right) \\ \Downarrow \\ \left(x_0 + \tfrac{mk}{\text{μκδ}(a,m)}\right) \not\equiv \left(x_0 + \tfrac{mk'}{\text{μκδ}(a,m)}\right) (\text{mod } m). \end{gathered}$$

Απομένει λοιπόν να αποδειχθεί ότι και κάθε άλλη λύση $y \in \mathbb{Z}$ τής (2.49) είναι ισότιμη με κάποια εκ των (2.50) κατά μόδιο m. Επειδή

$$\left.\begin{aligned} ax_0 &\equiv b(\text{mod } m) \\ ay &\equiv b(\text{mod } m) \end{aligned}\right\} \Longrightarrow ax_0 \equiv ay(\text{mod } m) \Longrightarrow m \mid a\,(y - x_0)\,,$$

συμπεραίνουμε ότι

$$\left.\begin{aligned} \tfrac{m}{\text{μκδ}(a,m)} &\mid \tfrac{a}{\text{μκδ}(a,m)}\,(y - x_0) \\ \text{μκδ}\left(\tfrac{a}{\text{μκδ}(a,m)}, \tfrac{m}{\text{μκδ}(a,m)}\right) &= 1 \end{aligned}\right\} \Longrightarrow \begin{gathered} \tfrac{m}{\text{μκδ}(a,m)} \mid y - x_0 \\ \Downarrow \\ \left(\exists \nu \in \mathbb{Z} : y - x_0 = \tfrac{m\nu}{\text{μκδ}(a,m)}\right). \end{gathered}$$

Διαιρώντας τον ν διά τού $\text{μκδ}(a,m)$ λαμβάνουμε μονοσημάντως ορισμένο ζεύγος $(q,r) \in \mathbb{Z}^2$ με $\nu = \text{μκδ}(a,m)\,q + r$, $0 \leqslant r \leqslant \text{μκδ}(a,m) - 1$. Ως εκ τούτου,

$$y - x_0 = \tfrac{m(\text{μκδ}(a,m)q + r)}{\text{μκδ}(a,m)} = mq + \tfrac{rm}{\text{μκδ}(a,m)} \equiv \tfrac{rm}{\text{μκδ}(a,m)} (\text{mod } m),$$

οπότε $y \equiv x_0 + r\frac{m}{\text{μκδ}(a,m)} (\text{mod } m)$, $\forall r \in \{0, 1, \ldots, \text{μκδ}(a,m) - 1\}$. □

2.4.44 Παρατήρηση. (i) Αντί τού $k \in \{0, 1, \ldots, \text{μκδ}(a,m) - 1\}$ μπορούμε στην (2.50) (επειδή εργαζόμαστε mod m) να γράψουμε $k \in \{1, \ldots, \text{μκδ}(a,m)\}$.

(ii) Όταν $b = 0$, τότε θέτουμε $x_0 := 0$.

2.4.45 Πόρισμα. *Δοθέντων ενός $m \in \mathbb{N}$ και δυο ακεραίων a, b, $a \neq 0$, η γραμμική ισοτιμία (2.49) διαθέτει ακριβώς μία λύση x_0 κατά μόδιο m εάν και μόνον εάν* $\text{μκδ}\,(a,m) = 1$.

2.4.46 Σημείωση. Όταν μκδ$(a,m)=1$, υπάρχουν *τρεις* τρόποι υπολογισμού τής λύσεως x_0 κατά μόδιο m.

Πρώτος τρόπος υπολογισμού. Αυτός διασφαλίζεται μέσω τής προσφυγής μας στον κλασικό *ευκλείδειο αλγόριθμο* (ήτοι στον προσδιορισμό ενός ζεύγους $(x_0^*, y_0^*) \in \mathbb{Z}^2$ για το οποίο ισχύει

$$ax_0^* - my_0^* = 1,$$

ορίζοντας ως x_0 το $x_0 := bx_0^*$, πρβλ. πρόταση 2.2.21).

Δεύτερος τρόπος υπολογισμού. Ένας άλλος τρόπος υπολογισμού τής λύσεως x_0 είναι δυνατός κατόπιν εφαρμογής τού θεωρήματος 2.4.22 τού Euler περί ισοτιμιών. Σύμφωνα με αυτό, (λόγω τής συνθήκης μκδ$(a,m)=1$) έχουμε $a^{\phi(m)} \equiv 1 (\mathrm{mod}\ m)$, όπου ϕ η συνάρτηση φι τού Euler (βλ. 2.4.15). Ως εκ τούτου, αρκεί να θέσουμε

$$\boxed{x_0 := a^{\phi(m)-1} b,} \tag{2.51}$$

να εφαρμόσουμε τον τύπο (2.35) για την εύρεση τού $\phi(m)$ για τον δοθέντα φυσικό αριθμό m και να διενεργήσουμε αναγωγή κατά μόδιο m.

Τρίτος τρόπος υπολογισμού (υποθέτοντας ότι $a \geqslant 2$). Μέσω τού λεγομένου **τύπου**[21] (2.53) **τού G. Voronoi**[22] για την εύρεση τού αντιστρόφου $[a]_m^{-1} = [a']_m$ τού $[a]_m$ (βλ. πρόταση 2.4.41). Θέτουμε

$$\boxed{x_0 := a'b} \tag{2.52}$$

και διενεργούμε αναγωγή κατά μόδιο m, όπου

$$\boxed{[a']_m = \left[3 - 2a + 6 \sum_{j=1}^{a-1} \left\lfloor \tfrac{mj}{a} \right\rfloor^2\right]_m .} \tag{2.53}$$

2.4.47 Παράδειγμα. Επειδή μκδ$(5,24)=1$, η γραμμική ισοτιμία $5x \equiv 3 (\mathrm{mod}\ 24)$ διαθέτει ακριβώς μία λύση x_0 κατά μόδιο 24. Γράφοντας $24 = 2^3 \cdot 3$, ο τύπος (2.35) μας δίδει την τιμή $\phi(24) = (2^3 - 2^2)(3-1) = 8$. Κατά τον (2.51), μπορούμε να θέσουμε ως $x_0 := 5^7 \cdot 3 = 234\,375$. Επειδή ισχύει $234\,375 = 9765 \cdot 24 + 15$, έχουμε $[x_0]_{24} = [15]_{24}$, οπότε $5 \cdot 15 \equiv 3 (\mathrm{mod}\ 24)$. Από την άλλη μεριά, η (2.53) δίδει

$$5' \equiv 3 - 2 \cdot 5 + 6 \left(\left\lfloor \tfrac{24}{5} \right\rfloor^2 + \left\lfloor \tfrac{48}{5} \right\rfloor^2 + \left\lfloor \tfrac{72}{5} \right\rfloor^2 + \left\lfloor \tfrac{96}{5} \right\rfloor^2 \right) = 3917 \equiv 5 (\mathrm{mod}\, 24),$$

διότι $3917 = 63 \cdot 24 + 5$, οπότε μέσω τής (2.52) λαμβάνουμε εκ νέου $[x_0]_{24} = [15]_{24}$ (αφού εδώ $b=3$).

Η εύρεση των λύσεων τής γενικής γραμμικής ισοτιμίας (2.49) ανάγεται -κατ' ουσίαν- στην ειδική περίπτωση που περιγράψαμε στα 2.4.45 και 2.4.46, ως ακολούθως:

2.4.48 Πόρισμα. *Δοθέντων ενός $m \in \mathbb{N}$ και δυο ακεραίων αριθμών a, b, $a \neq 0$, με* μκδ$(a,m) \mid b$, *η γραμμική ισοτιμία* (2.49) *διαθέτει* μκδ(a,m) *λύσεις $x \in \mathbb{Z}$ κατά μόδιο m, οι οποίες είναι τής μορφής* (2.50), *όπου x_0 η μοναδική λύση κατά μόδιο $\frac{m}{\text{μκδ}(a,m)}$ τής*

$$\left(\tfrac{a}{\text{μκδ}(a,m)}\right) x \equiv \left(\tfrac{b}{\text{μκδ}(a,m)}\right) (\mathrm{mod}\ \left(\tfrac{m}{\text{μκδ}(a,m)}\right)). \tag{2.54}$$

[21] Για την απόδειξή του βλ. J.V. Uspensky & M.A. Heaslet: *Elementary Number Theory*, McGraw-Hill Book Co., 1939, σελ. 183.

[22] *Georgy Voronoi* (1868-1908). Ρώσος μαθηματικός. Φοίτησε στο Πανεπιστήμιο τής Αγίας Πετρουπόλεως υπό τον A. Markov. Καθηγητής τού Πανεπιστημίου τής Βαρσοβίας από το 1894. Η έρευνά του ήταν επικεντρωμένη στην Αλγεβρική Θεωρία Αριθμών.

ΑΠΟΔΕΙΞΗ. Θέτοντας $\widetilde{a} := \frac{a}{\text{μκδ}(a,m)}$, $\widetilde{b} := \frac{b}{\text{μκδ}(a,m)}$ και $\widetilde{m} := \frac{m}{\text{μκδ}(a,m)}$, έχουμε $\text{μκδ}(\widetilde{a},\widetilde{m}) = 1$ (βλ. 2.2.14 (ii)), καθώς και τις ακόλουθες αμφίπλευρες συνεπαγωγές:

$$ax \equiv b \,(\text{mod } m) \quad \Leftrightarrow \text{μκδ}\,(a,m)\,\widetilde{a}x \equiv \text{μκδ}\,(a,m)\,\widetilde{b} \,(\text{mod}\,\text{μκδ}\,(a,m)\,\widetilde{m})$$

$$\Leftrightarrow \widetilde{a}x \equiv \widetilde{b}\,(\text{mod } \widetilde{m}) \Leftrightarrow \left(\tfrac{a}{\text{μκδ}(a,m)}\right) x \equiv \left(\tfrac{b}{\text{μκδ}(a,m)}\right) \,(\text{mod } \left(\tfrac{m}{\text{μκδ}(a,m)}\right)),$$

διότι $\text{μκδ}(a,m) \neq 0$ (βλ. 2.4.4 (iv)), οπότε η (2.54) ισοδυναμεί με την (2.49). □

2.4.49 Παράδειγμα. Η γραμμική ισοτιμία $6x \equiv 3 (\text{mod}\, 21)$ διαθέτει $\text{μκδ}(6,21) = 3$ λύσεις κατά μόδιο 21 τής μορφής $x_0, x_0 + 7, x_0 + 14$, όπου σύμφωνα με το πόρισμα 2.4.48 το x_0 είναι η μοναδική λύση τής $2x \equiv 1 (\text{mod}\, 7)$ κατά μόδιο 7. Εφαρμόζοντας τον τύπο (2.51) θέτουμε

$$x_0 = 2^{\phi(7)-1} = 2^5 = 32 \equiv 4 (\text{mod}\, 7).$$

Άρα οι λύσεις τής αρχικής ισοτιμίας είναι οι $4, 11, 18$ κατά μόδιο 21.

Κλείνουμε το παρόν κεφάλαιο παραθέτοντας μια απλή ικανή και αναγκαία συνθήκη[23], ούτως ώστε ένας ακέραιος > 1 να είναι *πρώτος*[24] .

2.4.50 Θεώρημα (J. Wilson). *Ένας ακέραιος $p > 1$ είναι πρώτος εάν και μόνον εάν*

$$\boxed{(p-1)! \equiv -1 \,(\text{mod } p)\,.} \tag{2.55}$$

ΑΠΟΔΕΙΞΗ. Έστω p ένας πρώτος αριθμός. Εάν $p = 2$ ή $p = 3$, τότε η (2.55) είναι προφανώς αληθής. Εάν ο p είναι πρώτος $\geqslant 5$, θεωρούμε ένα $a \in \{1, 2, \ldots, p-1\}$ και τη γραμμική ισοτιμία $ax \equiv 1 \,(\text{mod } p)$. Επειδή $\text{μκδ}(a,p) = 1$, η εν λόγω ισοτιμία έχει μοναδική λύση κατά μόδιο p, οπότε υπάρχει μονοσημάντως ορισμένος ακέραιος a', για τον οποίο ισχύει $0 \leqslant a' \leqslant p-1$ και $aa' \equiv 1 \,(\text{mod } p)$. Επειδή ο p είναι πρώτος, έχουμε

$$a = a' \Longleftrightarrow (\text{είτε } a = 1 \text{ είτε } a = p-1)\,. \tag{2.56}$$

Πράγματι· από την ισοτιμία $a^2 \equiv 1 \,(\text{mod } p)$ συνάγεται ότι

$$p \mid (a-1)(a+1) \Longrightarrow (\text{είτε } p \mid a-1 \text{ είτε } p \mid a+1)\,,$$

απ' όπου προκύπτει η συνεπαγωγή "⇒" τής (2.56), αφού $1 \leqslant a \leqslant p-1$ και $1 \leqslant a' \leqslant p-1$. Και αντιστρόφως· εάν $a = 1$, τότε

$$\left.\begin{array}{r} a' \equiv 1 \,(\text{mod } p) \Longrightarrow p \mid a'-1 \\ 1 \leqslant a' \leqslant p-1 \end{array}\right\} \underset{\text{(βλ. 2.1.5 (ii))}}{\Longrightarrow} a'-1 = 0 \Longrightarrow a' = 1,$$

και εάν $a = p-1$, τότε

$$(p-1)\,a' \equiv 1 \,(\text{mod } p) \Longrightarrow pa' \equiv a'+1 \,(\text{mod } p)\,,$$

[23] Παρά το γεγονός ότι η (2.55) αποτελεί μια ικανή και αναγκαία συνθήκη για να είναι ένας ακέραιος $p > 1$ πρώτος, είναι πρακτικώς μη αποδοτική για τον προσδιορισμό *μεγάλων πρώτων*, καθόσον εμπεριέχει το παραγοντικό. Για μια πρώτη γνωριμία με αποδοτικούς αλγορίθμους ευρέσεως πρώτων ή ελέγχου τού κατά πόσον κάποιος φυσικός αριθμός είναι πρώτος, οι ενδιαφερόμενοι αναγνώστες παραπέμπονται στο βιβλίο τού D.M. Bressoud: *Factorization and Primality Testing*, UTM, Springer-Verlag, 1989, καθώς και στα τρία βιβλία τού P. Ribenboim:
The Book of Prime Number Records, second. ed., Springer-Verlag, 1989.
The Little Book of Big Primes, Springer-Verlag, 1991.
The Little Book of Bigger Primes, second. ed., Springer-Verlag, 2004.

[24] Ο John Wilson (1741-1793) υπήρξε μαθητής τού Edward Waring (1734-1798), αλλά εγκατέλειψε αρκετά σύντομα τα Μαθηματικά. Υπηρέτησε ως δικαστικός και κατόπιν (περί το 1786) έλαβε και τον τίτλο τού ιππότη. Στο σύγγραμμά του με τον τίτλο *Meditationes algebraicae* (που δημοσιεύθηκε το 1770) ο Waring διατείνεται ότι ο Wilson είχε *εικάσει* την ισχύ τής ισοτιμίας (2.55). Ωστόσο, ο Wilson δεν μπόρεσε να την αποδείξει και πιθανώς να αρκέσθηκε σε κάποια απλά παραδείγματα. Ο Leibnitz (1646-1716) είχε επίσης εικάσει την ισχύ αυτής τής ισοτιμίας (και μάλιστα πριν το 1683), χωρίς όμως να έχει καταφέρει να την αποδείξει. Ο Lagrange (1736-1813), ορμώμενος από όσα ανέφερε ο Waring στο *Meditationes algebraicae*, εργάσθηκε σκληρά επί τού προβλήματος και τελικώς έδωσε μια ορθή απόδειξη το 1771.

οπότε

$$\left.\begin{aligned} pa' &\equiv a'+1 \,(\mathrm{mod}\ p) \\ pa' &\equiv p \,(\mathrm{mod}\ p) \end{aligned}\right\} \Longrightarrow p \equiv a'+1 \,(\mathrm{mod}\ p)\,,$$

και, ως εκ τούτου,

$$\left.\begin{aligned} p \equiv a'+1 \,(\mathrm{mod}\ p) &\Longrightarrow p \mid p-(a'+1) \\ 0 \leqslant p-(a'+1) &\leqslant p-2 \end{aligned}\right\} \underset{(\beta\lambda.\ 2.1.5\ (\mathrm{ii}))}{\Longrightarrow} a' = p-1,$$

και η συνεπαγωγή "$\Leftarrow$" τής (2.56) είναι όντως αληθής. Ομαδοποιούμε, εν συνεχεία, τους εναπομένοντες φυσικούς αριθμούς

$$\{1,2,\ldots,p-1\} \smallsetminus \{1,p-1\} = \{2,3,\ldots,p-2\}$$

κατά ζεύγη (a,a'), για τα οποία ισχύει $a \neq a'$ και $aa' \equiv 1 \,(\mathrm{mod}\ p)$. Πολλαπλασιάζοντας κατά μέλη τις κατ' αυτόν τον τρόπο σχηματιζόμενες $\frac{p-3}{2}$ ισοτιμίες λαμβάνουμε

$$2 \cdot 3 \cdot \cdots \cdot (p-2) \equiv 1 \,(\mathrm{mod}\ p) \Longrightarrow (p-1)! \equiv p-1 \,(\mathrm{mod}\ p)\,.$$

Επειδή $p-1 \equiv -1 \,(\mathrm{mod}\ p)$, η (2.55) προκύπτει από το 2.1.5 (v). Αντιστρόφως τώρα· υποθέτοντας ότι $(n-1)! \equiv -1 \,(\mathrm{mod}\ n)$, για κάποιον *σύνθετο* φυσικό αριθμό $n \geqslant 2$, θα υπάρχει διαιρέτης n' τού n με $1 < n' < n$, οπότε $n' \mid (n-1)!$. Επειδή

$$\left.\begin{aligned} n' &\mid n \\ n &\mid (n-1)!+1 \end{aligned}\right\} \Longrightarrow n' \mid (n-1)!+1,$$

ο n' θα διαιρεί και τη διαφορά $(n-1)!+1-(n-1)! = 1$, οπότε $n' = 1$, πράγμα άτοπο. Συνεπώς ο n οφείλει να είναι *πρώτος* προκειμένου να πληροί την ως άνω ισοτιμία. □

ΚΕΦΑΛΑΙΟ 3

Ομάδες και υποομάδες

Οι *ομάδες* είναι σύνολα (διάφορα τού κενού) εφοδιασμένα με μία και μόνον εσωτερική πράξη και τρεις συνοδευτικές χαρακτηριστικές ιδιότητες: την προσεταιριστικότητα, την ύπαρξη ουδετέρου στοιχείου και την ύπαρξη συμμετρικού («αντιστρόφου») οιουδήποτε στοιχείου τους. Τα *ομαδοειδή*, οι *ημιομάδες* και τα *μονοειδή* υπάγονται στους «προπομπούς» τους.

Θα μπορούσε κανείς να ισχυρισθεί με βάσιμα επιχειρήματα ότι η έννοια τής *ομάδας* «ενυπήρχε» ήδη (εμμέσως πλην σαφώς) σε διάφορες εργασίες των μαθηματικών τής αρχαιότητας. Ως *αλγεβρική δομή* πρωτοπαρουσιάσθηκε σε αριθμοθεωρητικές εργασίες των L. Euler (1707-1783), C.-F. Gauss (1777-1855) κ.ά. κατά τα τέλη τού 18ου και τις αρχές τού 19ου αιώνα, και, εν συνεχεία, στη θεωρία μετατάξεων των θέσεων μηδενισμού αλγεβρικών εξισώσεων των J.-L. Lagrange (1736-1813), E. Galois (1811-1832) κ.ά. Ωστόσο, ο τελικώς καθιερωθείς «ορισμός» της, όπως τον αντιλαμβανόμαστε στις ημέρες μας, αποκρυσταλλώθηκε σε ένα άρθρο[1] τού A. Cayley (1821-1895) το οποίο δημοσιεύθηκε το 1854, καθώς και σε κατοπινές δημοσιεύσεις[2] του περί τα μέσα τής δεκαετίας τού 1870. (Αρκετοί ιστορικοί υπογραμμίζουν και την πολύτιμη συμβολή των R. Dedekind (1831-1916), C. Jordan (1838-1922) και W. von Dyck (1856-1934) στην παγίωση αυτού τού ορισμού.)

3.1 ΟΜΑΔΟΕΙΔΗ, ΗΜΙΟΜΑΔΕΣ ΚΑΙ ΜΟΝΟΕΙΔΗ

3.1.1 Ορισμός. Κάθε ζεύγος $(A, \circledcirc)$, αποτελούμενο από ένα μη κενό σύνολο A και μία εσωτερική πράξη

$$A \times A \longrightarrow A, \quad (x, y) \longmapsto x \circledcirc y,$$

επί τού A, ονομάζεται **ομαδοειδές**[3]. (Το A καλείται **υποκείμενο σύνολο** τού ομαδοειδούς $(A, \circledcirc)$.)

3.1.2 Ορισμός. Έστω $(A, \circledcirc)$ ένα ομαδοειδές. Το $(A, \circledcirc)$ καλείται

(i) **προσεταιριστικό ομαδοειδές** ή **ημιομάδα** όταν η πράξη "$\circledcirc$" είναι *προσεταιριστική* (βλ. 1.5.3 (i)),

[1] Cayley A.: *On the theory of groups, as depending in the symbolic equation* $\Theta^n = 1$, Phil. Magazine, Vol. **7** (1854).

[2] Πρβλ. Scholz E. (Hrsg.): *Geschichte der Algebra*, B.I., Mannheim, 1990, σελ. 309.

[3] Αντ' αυτού χρησιμοποιείται ενίοτε και ο όρος **μάγμα**.

(ii) **μεταθετικό ομαδοειδές** ή **αβελιανό ομαδοειδές** όταν η πράξη "$\circledcirc$" είναι *μεταθετική* (βλ. 1.5.3 (ii)), και

(iii) **αβελιανή ημιομάδα** όταν αυτό είναι ταυτοχρόνως προσεταιριστικό και αβελιανό ομαδοειδές.

3.1.3 Ορισμός. Κάθε ημιομάδα (και αντιστοίχως, κάθε αβελιανή ημιομάδα) η οποία διαθέτει *ουδέτερο στοιχείο* ως προς την πράξη την ορισθείσα επ' αυτής (βλ. 1.5.6 (iii)) ονομάζεται **μονοειδές** (και αντιστοίχως, **αβελιανό μονοειδές**).

3.1.4 Σημείωση. Εάν μια ημιομάδα (ή, γενικότερα, ένα ομαδοειδές) διαθέτει ουδέτερο στοιχείο, τότε αυτό, σύμφωνα με την πρόταση 1.5.8, είναι μονοσημάντως ορισμένο.

3.1.5 Παραδείγματα. (i) Εάν $A \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, τότε το ζεύγος $(A, -)$, όπου "$-$" η πράξη τής αφαιρέσεως, είναι ένα *μη προσεταιριστικό*, *μη μεταθετικό* ομαδοειδές.

(ii) Παρομοίως, εάν το Ω είναι ένα σύνολο, τότε το ζεύγος $(\mathfrak{P}(\Omega), \smallsetminus)$ είναι (εν γένει) ένα *μη προσεταιριστικό*, *μη μεταθετικό* ομαδοειδές (βλ. 1.5.5(iv)).

(iii) Το ζεύγος $(\mathbb{Z}, \circledcirc)$, όπου

$$\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z},\ (a, b) \longmapsto a \circledcirc b := b,$$

αποτελεί μια *μη αβελιανή* ημιομάδα, διότι

$$a \circledcirc b \neq b \circledcirc a$$

όταν $a \neq b$, ενώ για οιαδήποτε $a, b, c \in \mathbb{Z}$ ισχύουν οι ισότητες

$$(a \circledcirc b) \circledcirc c = b \circledcirc c = c = a \circledcirc c = a \circledcirc (b \circledcirc c)\,.$$

Επιπροσθέτως, είναι προφανές ότι το $(\mathbb{Z}, \circledcirc)$ δεν είναι μονοειδές.

(iv) Το ζεύγος $(\mathbb{Z}, \circledast)$, όπου

$$\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z},\ \ (a, b) \longmapsto a \circledast b := a^2 + b^2,$$

αποτελεί ένα αβελιανό ομαδοειδές που *δεν είναι ημιομάδα*, διότι

$$a \circledast b = b \circledast a$$

για οιαδήποτε $a, b \in \mathbb{Z}$ και

$$(2 \circledast 1) \circledast 1 = 26 \neq 8 = 2 \circledast (1 \circledast 1)\,.$$

(v) Έστω A ένα μη κενό σύνολο. Το σύνολο $A^A = \text{ΑΠ}(A, A)$ των απεικονίσεων από το A στο A, εφοδιασμένο με την εσωτερική πράξη

$$A^A \times A^A \longrightarrow A^A,\ (g, f) \longmapsto g \circ f,$$

είναι ένα (εν γένει *μη αβελιανό*) μονοειδές με την ταυτοτική απεικόνιση id_A ως ουδέτερο στοιχείο του (βλ. 1.5.12).

(vi) Το ζεύγος $(\mathbb{N}, +)$, όπου "$+$" η συνήθης πρόσθεση φυσικών αριθμών, είναι μια αβελιανή ημιομάδα που δεν είναι μονοειδές.

(vii) Εάν $A \in \{\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ και $B \in \{\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, τότε τα ζεύγη $(A, +)$ και $(B, \cdot)$ (ως προς τις συνήθεις πράξεις προσθέσεως και πολλαπλασιασμού) αποτελούν αβελιανά μονοειδή με ουδέτερά τους στοιχεία τα 0 και 1, αντιστοίχως.

(viii) Επί τού $\mathbb{Z}_m$, $m \in \mathbb{N}$, ορίζονται δύο εσωτερικές πράξεις[4] "$+$" και "$\cdot$":

$$([a]_m, [b]_m) \longmapsto [a]_m + [b]_m, \quad ([a]_m, [b]_m) \longmapsto [a]_m \cdot [b]_m. \tag{3.1}$$

Τα ζεύγη $(\mathbb{Z}_m, +)$ και $(\mathbb{Z}_m, \cdot)$, $m \in \mathbb{N}$, ως προς τις ανωτέρω πράξεις προσθέσεως και πολλαπλασιασμού είναι αβελιανά μονοειδή με ουδέτερά τους στοιχεία τα $[0]_m$ και $[1]_m$, αντιστοίχως. (Βλ. προτάσεις 2.4.39 και 2.4.40.)

(ix) Εάν το Ω είναι ένα σύνολο, τότε τα ζεύγη $(\mathfrak{P}(\Omega), \cup)$, $(\mathfrak{P}(\Omega), \cap)$ και $(\mathfrak{P}(\Omega), \triangle)$ είναι αβελιανά μονοειδή με ουδέτερά τους στοιχεία τα $\varnothing, \Omega$ και $\varnothing$, αντιστοίχως. (Βλ. 1.5.5 (i), (ii) και (iii), και 1.5.10.)

3.1.6 Παράδειγμα. Εάν οι m και n είναι δυο φυσικοί αριθμοί και το A ένα μη κενό σύνολο, τότε κάθε απεικόνιση

$$f : \{1, 2, \ldots, m\} \times \{1, 2, \ldots, n\} \longrightarrow A \tag{3.2}$$

ονομάζεται $(m \times n)$-**πίνακας** με τις «εγγραφές[5]» του ειλημμένες από το A. Αντί τού σχετικώς δύσχρηστου συμβολισμού (3.2) γράφουμε απλώς

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1\,n-1} & a_{1\,n} \\ a_{21} & a_{22} & \cdots & a_{2\,n-1} & a_{2\,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m-1\,1} & a_{m-1\,2} & \cdots & a_{m-1\,n-1} & a_{m-1\,n} \\ a_{m\,1} & a_{m\,2} & \cdots & a_{m\,n-1} & a_{m\,n} \end{pmatrix}$$

ή $(a_{jk})_{1 \leqslant j \leqslant m, 1 \leqslant k \leqslant n}$, όπου

$$a_{jk} := f(j,k), \ \forall (j,k) \in \{1, 2, \ldots, m\} \times \{1, 2, \ldots, n\}.$$

Επίσης, ως $\mathrm{Mat}_{m\times n}(A)$ συμβολίζουμε το σύνολο όλων των $(m \times n)$-πινάκων (ήτοι πινάκων με m *γραμμές* και n *στήλες*) με τις εγγραφές τους ειλημμένες από το A. Εάν επί τού A ορίσουμε μια εσωτερική πράξη

$$A \times A \longrightarrow A, \ \ (x, y) \longmapsto x \circledcirc y,$$

τότε το ομαδοειδές $(A, \circledcirc)$ καθορίζει ένα ομαδοειδές

$$(\mathrm{Mat}_{m\times n}(A), \widehat{\circledcirc}),$$

όπου

$$(a_{jk})_{1 \leqslant j \leqslant m, 1 \leqslant k \leqslant n} \,\widehat{\circledcirc}\, (b_{jk})_{1 \leqslant j \leqslant m, 1 \leqslant k \leqslant n} := (a_{jk} \circledcirc b_{jk})_{1 \leqslant j \leqslant m, 1 \leqslant k \leqslant n},$$

για κάθε ζεύγος

$$((a_{jk})_{1 \leqslant j \leqslant m, 1 \leqslant k \leqslant n}, (b_{jk})_{1 \leqslant j \leqslant m, 1 \leqslant k \leqslant n}) \in \mathrm{Mat}_{m\times n}(A) \times \mathrm{Mat}_{m\times n}(A).$$

Εάν το $(A, \circledcirc)$ είναι προσεταιριστικό (και αντιστοίχως, αβελιανό), τότε και το $(\mathrm{Mat}_{m\times n}(A), \widehat{\circledcirc})$ είναι προσεταιριστικό (και αντιστοίχως, αβελιανό). Επιπροσθέτως, εάν το $(A, \circledcirc)$ είναι μονοειδές έχον το e_A ως ουδέτερο στοιχείο του, τότε και το $(\mathrm{Mat}_{m\times n}(A), \widehat{\circledcirc})$ είναι μονοειδές με ουδέτερο στοιχείο του τον $(m \times n)$-πίνακα, όλες οι εγγραφές τού οποίου είναι ίσες με το e_A. Επί παραδείγματι, εάν το $A \in \{\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_k\}$ (όπου $k \in \mathbb{N}$) εφοδιασθεί με την πράξη τής προσθέσεως "$+$", τότε είθισται να γράφουμε απλώς "$+$" αντί τού "$\widehat{+}$" για τον συμβολισμό τής επαγομένης πράξεως επί τού $\mathrm{Mat}_{m\times n}(A)$ και να την καλούμε **πρόσθεση πινάκων**. Εν προκειμένω, το $(\mathrm{Mat}_{m\times n}(A), +)$ είναι *αβελιανό μονοειδές*.

[4] Επειδή κατά την εφαρμογή των ορισμών (2.48) οι ακέραιοι $a + b$ και ab ενδέχεται να είναι $\geqslant m$ (ακόμη και όταν οι a και b είναι ειλημμένοι από το σύνολο $\{0, 1, \ldots, m-1\}$), εάν επιθυμούμε να παραμείνουμε στην περιγραφή (2.47) τού $\mathbb{Z}_m$ επιλέγουμε ως εκπροσώπους των κλάσεων ισοδυναμιών τους ως προς την "$\sim_m$" τα υπόλοιπα που αφήνουν αφού διαιρεθούν διά τού m.

[5] Οι **εγγραφές** (αγγλ. entries) ενός πίνακα (3.2) είναι οι $m \times n$ εικόνες τής f.

3.2 ΘΕΜΕΛΙΩΔΕΙΣ ΟΡΙΣΜΟΙ ΚΑΙ ΙΔΙΟΤΗΤΕΣ

3.2.1 Ορισμός. Ένα μονοειδές $(G, \circledcirc)$ (με το G ως υποκείμενο σύνολό του) καλείται **ομάδα**[6] όταν για κάθε στοιχείο τού G υπάρχει το συμμετρικό του ως προς την $\circledcirc$ (πρβλ. πρόταση 1.5.8). Η **τάξη** $|G|$ μιας ομάδας $(G, \circledcirc)$ είναι εξ ορισμού ο πληθικός αριθμός $\mathrm{card}(G)$ τού συνόλου G. Εάν η $|G|$ είναι πεπερασμένη, τότε λέμε ότι η G έχει **πεπερασμένη τάξη** ή απλώς ότι η G είναι μια **πεπερασμένη ομάδα** και γράφουμε $|G| < \infty$. (Ειδάλλως λέμε ότι η G είναι μια **άπειρη ομάδα** και γράφουμε[7] $|G| = \infty$). Μια ομάδα G λέγεται **μεταθετική** ή **αβελιανή** (ή **ομάδα τού Abel**[8]) όταν η πράξη, με την οποία είναι εφοδιασμένη, είναι μεταθετική.

3.2.2 Παραδείγματα. (i) Τα ζεύγη $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ των ακεραίων, των ρητών, των πραγματικών και των μιγαδικών αριθμών, αντιστοίχως, μαζί με τη συνήθη πρόσθεση, αποτελούν τα πιο οικεία παραδείγματα αβελιανών ομάδων. Το αβελιανό μονοειδές $(\mathbb{N}_0, +)$ δεν είναι ομάδα, διότι κανένας $n \in \mathbb{N}$ δεν διαθέτει αντίθετο (= συμμετρικό) στοιχείο *εντός* τού συνόλου $\mathbb{N}_0$.

(ii) Το μονοειδές $(\mathbb{Z}_m, +)$, $m \in \mathbb{N}$, (βλ. 3.1.5 (viii)) αποτελεί (σύμφωνα με την πρόταση 2.4.39) μια αβελιανή ομάδα με ουδέτερό της στοιχείο το $[0]_m$ και αντίθετο στοιχείο καθενός $[k]_m \in \mathbb{Z}_m$ το $[-k]_m$.

(iii) Τα ζεύγη $(\mathbb{Q}\setminus\{0\}, \cdot), (\mathbb{R}\setminus\{0\}, \cdot), (\mathbb{Q}_{>0}, \cdot), (\mathbb{R}_{>0}, \cdot), (\mathbb{C}\setminus\{0\}, \cdot)$ των μη μηδενικών ρητών, των μη μηδενικών πραγματικών, των θετικών ρητών, των θετικών πραγματικών και των μη μηδενικών μιγαδικών αριθμών, μαζί με τον συνήθη πολλαπλασιασμό, είναι αβελιανές ομάδες (με το 1 ως ουδέτερο στοιχείο τους). Αντιθέτως, το αβελιανό μονοειδές $(\mathbb{Z}\setminus\{0\}, \cdot)$ δεν είναι ομάδα, διότι μόνον οι ± 1 διαθέτουν αντίστροφο (= συμμετρικό) στοιχείο εντός τού $\mathbb{Z}\setminus\{0\}$.

(iv) Το ζεύγος $(\mathbb{Q}_{>0}, *)$, όπου $r * s := \frac{rs}{2}$, $\forall\,(r, s) \in \mathbb{Q}_{>0} \times \mathbb{Q}_{>0}$, είναι μια αβελιανή ομάδα η οποία έχει το 2 (!) ως ουδέτερό της στοιχείο και το $\frac{4}{r}$ ως συμμετρικό στοιχείο οιουδήποτε $r \in \mathbb{Q}_{>0}$.

(v) Το αβελιανό μονοειδές $(\mathbb{Z}_m, \cdot)$, $m \in \mathbb{N}$, (βλ. 3.1.5 (viii)), με ουδέτερό του στοιχείο το $[1]_m$, δεν είναι ομάδα όταν $m \geqslant 2$, διότι (τουλάχιστον) το $[0]_m$ δεν διαθέτει αντίστροφο.

(vi) Εάν το Ω είναι ένα σύνολο, τότε το ζεύγος $(\mathfrak{P}(\Omega), \triangle)$ αποτελεί μια αβελιανή ομάδα. Αντιθέτως, για οιοδήποτε $\Omega \neq \varnothing$ τα αβελιανά μονοειδή $(\mathfrak{P}(\Omega), \cup)$ και $(\mathfrak{P}(\Omega), \cap)$ δεν είναι ομάδες. (Βλ. 1.5.15 και 3.1.5 (ix).)

(vii) Εάν $m, n \in \mathbb{N}$ και εάν το $A \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_k\}$ (όπου $k \in \mathbb{N}$) εφοδιασθεί με την πράξη τής συνήθους προσθέσεως, τότε το αβελιανό μονοειδές $(\mathrm{Mat}_{m\times n}(A), +)$ το ορισθέν στο εδάφιο 3.1.6 αποτελεί μια ομάδα, καθότι κάθε

$$(a_{jk})_{1\leqslant j\leqslant m, 1\leqslant k\leqslant n} \in \mathrm{Mat}_{m\times n}(A)$$

έχει τον πίνακα $(-a_{jk})_{1\leqslant j\leqslant m, 1\leqslant k\leqslant n}$ ως συμμετρικό του στοιχείο ως προς την "+".

3.2.3 Σημείωση. Ορισμένες φορές, όταν μελετούμε μια πεπερασμένη ομάδα $(G, \circledcirc)$ που έχει είτε μικρή τάξη είτε στοιχεία διασυνδεόμενα μέσω ειδικών σχέσεων, είναι χρήσιμο να εργαζόμαστε με τον **πολλαπλασιαστικό κατάλογο τής** $(G, \circledcirc)$ (που ονομάζεται, εναλλακτικώς, και **κατάλογος τής πράξεως** "$\circledcirc$" ή **κατάλογος τού Cayley**

[6] Σε πολλές περιπτώσεις όπου δεν υφίσταται κίνδυνος συγχύσεως (για το ποια πράξη υπονοείται) συμβολίζουμε τις ομάδες μόνον με κεφαλαία (λατινικά) γράμματα.

[7] Εν κανείς χρησιμοποιήσει τον συνήθη τρόπο συγκρίσεως πληθικών αριθμών (στο πλαίσιο τής Θεωρίας Συνόλων), η συνθήκη $|G| = \infty$ ισοδυναμεί με την $|G| \geqslant \aleph_0 := \mathrm{card}(\mathbb{N})$, όπου $\aleph_0$ είναι το «άλεφ μηδέν».

[8] Προς τιμήν τού Νορβηγού μαθηματικού Niels Henrik Abel (1802-1829).

για την $(G, \circledcirc)$). Εάν $G = \{g_1, \ldots, g_k\}$, $k \in \mathbb{N}$, τότε αυτός είναι ο εξής:

$\circledcirc$	g_1	g_2	$\cdots$	$\cdots$	g_k
g_1	$g_1 \circledcirc g_1$	$g_1 \circledcirc g_2$	$\cdots$	$\cdots$	$g_1 \circledcirc g_k$
g_2	$g_2 \circledcirc g_1$	$g_2 \circledcirc g_2$	$\cdots$	$\cdots$	$g_2 \circledcirc g_k$
$\vdots$	$\vdots$	$\vdots$			$\vdots$
$\vdots$	$\vdots$	$\vdots$			$\vdots$
g_k	$g_k \circledcirc g_1$	$g_k \circledcirc g_2$	$\cdots$	$\cdots$	$g_k \circledcirc g_k$

Στην i-οστή γραμμή και στην j-οστή στήλη τού καταλόγου τοποθετείται το στοιχείο $g_i \circledcirc g_j$, $1 \leqslant i, j \leqslant k$. Κάθε στοιχείο τής ομάδας εμφανίζεται *μόνον μία φορά* σε κάθε γραμμή και σε κάθε στήλη.

3.2.4 Σημείωση. Η ιεράρχηση των (NBG-) κλάσεων των δομών που έχουμε συναντήσει μέχρι στιγμής έχει ως εξής:

$$\boxed{\{\text{ομάδες}\} \subsetneqq \{\text{μονοειδή}\} \subsetneqq \{\text{ημιομάδες}\} \subsetneqq \{\text{ομαδοειδή}\}.}$$

Από τα προηγηθέντα παραδείγματα 3.1.5 και 3.2.2 καθίσταται σαφές ότι οι ανωτέρω εγκλεισμοί είναι *γνήσιοι*. Επισημαίνεται -ιδιαιτέρως- ότι, δοθέντος ενός *μονοειδούς*, υπάρχει πάντοτε η δυνατότητα σχηματισμού μιας *ομάδας*, όπως περιγράφεται στην πρόταση 3.2.6.

3.2.5 Ορισμός. Έστω $(M, \cdot)$ ένα μονοειδές έχον το e_M ως ουδέτερο στοιχείο του. Τότε συμβολίζουμε ως

$$\boxed{M^\times := \{x \in M \,|\exists y \in M : xy = e_M = yx\}}$$

το σύνολο όλων των $x \in M$ που διαθέτουν συμμετρικό στοιχείο ως προς την "$\cdot$".

3.2.6 Πρόταση. *Έστω $(M, \cdot)$ ένα μονοειδές. Τότε το ζεύγος $(M^\times, \cdot)$ αποτελεί μια ομάδα.*

Απόδειξη. Κατ' αρχάς, επειδή $e_M e_M = e_M$, έχουμε $e_M \in M^\times$. Εάν $x, x' \in M^\times$, τότε $[\exists y \in M : xy = e_M = yx]$ και $[\exists y' \in M : x'y' = e_M = y'x']$, οπότε

$$(y'y)(xx') = y'(yx)x' = y'e_M x' = y'x' = e_M.$$

και, κατ' αναλογίαν, $(xx')(y'y) = e_M$. Τούτο σημαίνει ότι ισχύει $xx' \in M^\times$, δηλαδή ότι το $M^\times$ είναι κλειστό ως προς την "$\cdot$" (βλ. 1.5.2). Επιπροσθέτως, εάν το x είναι τυχόν στοιχείο τού $M^\times$ και το y συμμετρικό στοιχείο του, τότε το y (λόγω τής προτάσεως 1.5.13) είναι το μόνο στοιχείο τού M με αυτήν ιδιότητα και (εξ ορισμού) $y \in M^\times$ (διότι το x είναι, με τη σειρά του, το συμμετρικό στοιχείο τού y). Κατά συνέπειαν, το ζεύγος $(M^\times, \cdot)$ αποτελεί μια ομάδα. □

3.2.7 Παραδείγματα. (i) Μέσω των αβελιανών μονοειδών $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ και $(\mathbb{C}, \cdot)$ (όπου "$\cdot$" ο συνήθης πολλαπλασιασμός) δημιουργούνται οι πολλαπλασιαστικές ομάδες $(\mathbb{Q}\setminus\{0\}, \cdot)$, $(\mathbb{R}\setminus\{0\}, \cdot)$ και $(\mathbb{C}\setminus\{0\}, \cdot)$, αντιστοίχως.

(ii) Μέσω τού αβελιανού μονοειδούς $(\mathbb{Z}, \cdot)$ (όπου "$\cdot$" ο συνήθης πολλαπλασιασμός) δημιουργείται η πολλαπλασιαστική ομάδα με υποκείμενο σύνολο το $\mathbb{Z}^\times = \{\pm 1\}$.

(iii) Μέσω τού αβελιανού μονοειδούς $(\mathbb{Z}_m, \cdot)$, $m \in \mathbb{N}$, δημιουργείται η πολλαπλασιαστική ομάδα που έχει ως υποκείμενο σύνολό της το[9]

$$\boxed{\mathbb{Z}_m^\times = \{[k]_m \in \mathbb{Z}_m \mid k \in \mathbb{N},\ \ k \leqslant m,\ \ \text{μκδ}\,(k,m) = 1\}}$$

και τάξη $\phi\,(m)$, όπου $\phi : \mathbb{N} \longrightarrow \mathbb{N}$ η *συνάρτηση φι τού Euler*

$$m \longmapsto \phi\,(m) := \text{card}\{\,k \in \mathbb{N} \mid\ k \leqslant m \text{ και } \text{μκδ}\,(k,m) = 1\}. \tag{3.3}$$

(Πρβλ. 2.4.15 και 2.4.41.) Η $(\mathbb{Z}_m^\times, \cdot)$ καλείται **ομάδα των αντιστρέψιμων κλάσεων υπολοίπων κατά το μόδιο** m. (Ιδιαιτέρως, για οιονδήποτε πρώτο αριθμό p έχουμε $\mathbb{Z}_p^\times = \mathbb{Z}_p \smallsetminus \{[0]_p\}$.)

(iv) Έστω $(R, \cdot)$ το αβελιανό μονοειδές με $R \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, όπου "$\cdot$" ο συνήθης πολλαπλασιασμός. Το σύνολο $\text{Mat}_{n\times n}\,(R)$ των $(n \times n)$-πινάκων καθίσταται μονοειδές (μη αβελιανό για $n \geqslant 2$) μέσω τής (συνήθους) πράξεως τού *πολλαπλασιασμού πινάκων*:

$$\mathbf{AB} := (a_{j\,1}b_{1\,k} + a_{j\,2}b_{2\,k} + \cdots + a_{j\,n}b_{n\,k})_{1\leqslant j,k\leqslant n}\,,$$

για οιουσδήποτε $\mathbf{A} = (a_{jk})_{1\leqslant j,k\leqslant n}$, $\mathbf{B} = (b_{jk})_{1\leqslant j,k\leqslant n} \in \text{Mat}_{n\times n}\,(R)$, με μοναδιαίο του στοιχείο τον *μοναδιαίο* $(n \times n)$-πίνακα

$$\mathbf{I}_n := \begin{pmatrix} 1_R & 0_R & \cdots & 0_R & 0_R \\ 0_R & 1_R & \cdots & 0_R & 0_R \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0_R & 0_R & \cdots & 1_R & 0_R \\ 0_R & 0_R & \cdots & 0_R & 1_R \end{pmatrix}.$$

Μέσω τού μονοειδούς $(\text{Mat}_{n\times n}\,(R)\,, \cdot)$ ορίζεται η **γενική γραμμική ομάδα**

$$\boxed{\text{GL}_n\,(R) := (\text{Mat}_{n\times n}(R))^\times = \{\mathbf{A} \in\ \text{Mat}_{n\times n}(R) \mid \det(\mathbf{A}) \neq 0\}\,,}$$

(**βαθμού** n **υπεράνω τού** R), όπου $\det(\mathbf{A})$ η *ορίζουσα* τού $\mathbf{A}$.

3.2.8 Σημείωση (Χρηστικός τρόπος συμβολισμού ομάδων). Από εδώ και στο εξής, όταν αναφερόμαστε σε *τυχούσες* ομάδες, θα υιοθετούμε ως επί το πλείστον τον *πολλαπλασιαστικό* και (κάπως σπανιότερα) τον *προσθετικό* συμβολισμό για τις εκάστοτε θεωρούμενες πράξεις (γράφοντας π.χ. $g_1g_2, g_1 \cdot g_2$ ή $g_1 * g_2$ και, αντιστοίχως, $g_1 + g_2$, αντί τού $g_1 \circledcirc g_2$, για δυο στοιχεία g_1, g_2 μιας ομάδας G, ακόμη και όταν οι πράξεις δεν υπονοούν κάποιους «οικείους» πολλαπλασιασμούς και προσθέσεις, αντιστοίχως) και θα συμβολίζουμε το ουδέτερο στοιχείο μιας ομάδας G ως e_G και το συμμετρικό στοιχείο ενός $g \in G$ ως g^{-1} («αντίστροφο» τού g) και, αντιστοίχως, $-g$ («αντίθετο» τού g).

3.2.9 Πρόταση. *Έστω $(G, \cdot)$ μια ομάδα. Τότε ισχύουν τα ακόλουθα*:
(i) *Για κάθε $a, b, g \in G$ έχουμε*

$$\left.\begin{array}{rcl} ag = bg & \Longrightarrow & a = b \\ ga = gb & \Longrightarrow & a = b \end{array}\right\} \quad \text{(Νόμοι διαγραφής)}$$

(ii) $\left(g^{-1}\right)^{-1} = g$, *για κάθε $g \in G$.*
(iii) *Εάν $k \in \mathbb{N}$ και $g_1, \ldots, g_k \in G$, τότε $(g_1g_2\cdots g_k)^{-1} = g_k^{-1}\cdots g_2^{-1}g_1^{-1}$.*
(iv) *Για οιαδήποτε $a, b \in G$ οι εξισώσεις $ax = b$ και $ya = b$ επιδέχονται τις $x = a^{-1}b$*

[9] Επειδή $[0]_m = [m]_m$, ισχύει και η ισότητα $\mathbb{Z}_m^\times = \{[k]_m \in \mathbb{Z}_m \mid k \in \mathbb{Z},\ \ 0 \leqslant k \leqslant m-1,\ \ \text{μκδ}\,(k,m) = 1\}$. (Σημειωτέον ότι ορισμένοι συγγραφείς συμβολίζουν την ομάδα $\mathbb{Z}_m^\times$ ως $U(\mathbb{Z}_m)$ ή απλώς ως U_m, όπου το "U" προέρχεται από το πρώτο γράμμα τής λέξεως unit (= αντιστρέψιμο στοιχείο).)

και $y = ba^{-1}$, αντιστοίχως, ως μοναδικές τους λύσεις.

Απόδειξη. (i) Πολλαπλασιάζοντας την πρώτη εξίσωση (εκ δεξιών) με το αντίστροφο (= συμμετρικό) στοιχείο g^{-1} τού g, λαμβάνουμε

$$(ag)\,g^{-1} = (bg)\,g^{-1} \Longrightarrow a\left(gg^{-1}\right) = b\left(gg^{-1}\right) \Longrightarrow ae_G = be_G \Longrightarrow a = b.$$

Κατ' αναλογίαν (κατόπιν πολλαπλασιασμού με g^{-1} εξ αριστερών) αποδεικνύουμε και τον δεύτερο νόμο τής διαγραφής.

(ii) Επειδή $\left(g^{-1}\right)^{-1} g^{-1} = e_G = g^{-1}\left(g^{-1}\right)^{-1}$ και $gg^{-1} = e_G = g^{-1}g$, έχουμε $\left(g^{-1}\right)^{-1} = g$, για κάθε $g \in G$, λόγω τής μοναδικότητας τού συμμετρικού στοιχείου (βλ. πρόταση 1.5.8).

(iii) Έστω $k = 2$. Αρκεί (και πάλι λόγω τής μοναδικότητας τού συμμετρικού στοιχείου) να δείξουμε ότι $(g_1g_2)\left(g_2^{-1}g_1^{-1}\right) = e_G = \left(g_2^{-1}g_1^{-1}\right)(g_1g_2)$. Θέτοντας σε εφαρμογή τον γενικευμένο προσεταιριστικό νόμο 1.6.40 λαμβάνουμε

$$(g_1g_2)\left(g_2^{-1}g_1^{-1}\right) = \left(g_1\left(g_2g_2^{-1}\right)\right)g_1^{-1} = (g_1e_G)\,g_1^{-1} = g_1g_1^{-1} = e_G.$$

Αναλόγως δείχνουμε ότι

$$\left(g_2^{-1}g_1^{-1}\right)(g_1g_2) = e_G.$$

Για $k \geqslant 3$ το ζητούμενο έπεται μέσω μαθηματικής επαγωγής.

(iv) Κατ' αρχάς, $a\left(a^{-1}b\right) = \left(aa^{-1}\right)b = e_Gb = b$, οπότε το $a^{-1}b$ είναι όντως μια λύση τής εξισώσεως $ax = b$. Έστω $g \in G$ μια τυχούσα λύση της. Τότε

$$a^{-1}(ag) = a^{-1}b \Longrightarrow \left(a^{-1}a\right)g = a^{-1}b \Longrightarrow e_Gg = g = a^{-1}b.$$

Αναλόγως αποδεικνύεται και η μοναδικότητα τής λύσεως τής 2ης εξισώσεως. □

3.2.10 Ορισμός («Δυνάμεις» στοιχείων). Έστω $(G, \cdot)$ μια ομάδα. Για κάθε $n \in \mathbb{Z}$ εισάγουμε τη βραχυγραφία

$$g^n := \begin{cases} \underbrace{g\,g\,\cdots\,g}_{n\ \text{φορές}}, & \text{όταν} \quad n > 0, \\ \left(g^{-n}\right)^{-1}, & \text{όταν} \quad n < 0, \\ e_G\,, & \text{όταν} \quad n = 0, \end{cases}$$

εν είδει[10] «δυνάμεως».

3.2.11 Πρόταση. *Έστω $(G, \cdot)$ μια ομάδα. Τότε για κάθε στοιχείο $g \in G$ και κάθε $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ ισχύουν τα ακόλουθα:*

(i) $g^mg^n = g^{m+n} = g^ng^m$,

(ii) $(g^m)^n = g^{mn}$,

(iii) $g^{-m} = \left(g^{-1}\right)^m = (g^m)^{-1}$. (Το g^{-m} είναι το αντίστροφο τού g^m.)

[10] Όταν χρησιμοποιείται *προσθετικός συμβολισμός* για την G, τότε για κάθε $n \in \mathbb{Z}$ ορίζουμε κατ' αναλογίαν

$$ng := \begin{cases} \underbrace{g + g + \cdots + g}_{n\ \text{φορές}}, & \text{όταν} \quad n > 0, \\ -((-n)g), & \text{όταν} \quad n < 0, \\ e_G\,, & \text{όταν} \quad n = 0, \end{cases}$$

εν είδει «πολλαπλασίου».

Απόδειξη. (i) Κατ' αρχάς υποθέτουμε ότι αμφότεροι οι m, n είναι θετικοί. Διατηρώντας τόν n παγιωμένο, θα εφαρμόσουμε κλασική μαθηματική επαγωγή ως προς τον m. (Αναλόγως επιχειρηματολογεί κανείς και με τον n). Εάν $m = 1$, τότε -εξ ορισμού- $gg^n = g^{1+n}$. Υποθέτοντας ότι $g^m g^n = g^{m+n}$, λαμβάνουμε

$$g^{m+1}g^n = (gg^m)\,g^n = g\,(g^m g^n) = gg^{m+n} = g^{m+n+1}.$$

Τώρα υποθέτουμε ότι ένας εκ των m, n είναι $= 0$. Εάν $m = 0$, τότε

$$g^0 g^n = e_G g^n = g^n = g^{0+n}.$$

(Αναλόγως, $g^m g^0 = g^m e_G = g^m = g^{m+0}$, όταν $n = 0$). Εν συνεχεία, υποθέτουμε ότι αμφότεροι οι m, n είναι αρνητικοί. Σύμφωνα με τα 3.2.9 (ii) και (iii),

$$g^m g^n = \left(g^{-m}\right)^{-1}\left(g^{-n}\right)^{-1} = \left(g^{-n}g^{-m}\right)^{-1} = \left(g^{-(n+m)}\right)^{-1} = \left(g^{-(m+n)}\right)^{-1} = g^{m+n}.$$

Εξάλλου, επειδή $m + n = n + m$, έχουμε $g^m g^n = g^n g^m$. Ως εκ τούτου, υπολείπεται μόνον η εξέταση τής περιπτώσεως κατά την οποία ο ένας εκ των m, n είναι αρνητικός και ο άλλος θετικός. Επειδή οι αποδείξεις είναι πανομοιότυπες, θα εξετάσουμε τι συμβαίνει μόνον όταν $m > 0$ και $n < 0$. Διακρίνουμε τις τρεις διαφορετικές περιπτώσεις:

(α) $m + n > 0$. Κάνοντας χρήση των όσων ισχύουν στην περίπτωση όπου αμφότεροι είναι θετικοί, λαμβάνουμε $g^{m+n}g^{-n} = g^{(m+n)-n} = g^m$. Επειδή το g^{-n} είναι -εξ ορισμού- το αντίστροφο τού g^n, μπορούμε να πολλαπλασιάσουμε αμφότερες τις πλευρές (εκ δεξιών) με το g^n και να καταλήξουμε στο ζητούμενο: $g^{m+n} = g^m g^n$.

(β) $m + n = 0$. Σε αυτήν την περίπτωση, $n = -m$, οπότε το g^n είναι -εξ ορισμού- το αντίστροφο τού g^m και $g^m g^n = g^0 = e_G$.

(γ) $m + n < 0$. Κάνοντας εκ νέου χρήση των όσων ισχύουν στην περίπτωση όπου αμφότεροι είναι θετικοί, λαμβάνουμε $g^{-(m+n)}g^m = g^{-m-n+m} = g^{-n}$. Επειδή το g^{-m} είναι -εξ ορισμού- το αντίστροφο τού g^m, μπορούμε να πολλαπλασιάσουμε αμφότερες τις πλευρές (εκ δεξιών) με το g^{-m} και να καταλήξουμε στο ζητούμενο:

$$g^{-(m+n)} = g^{-n}g^{-m} = g^{-m}g^{-n}.$$

(ii) Η απόδειξη είναι παρόμοια και γι' αυτό αφήνεται ως άσκηση.

(iii) Εάν $m > 0$, τότε -εξ ορισμού- $g^{-m} = (g^m)^{-1}$. Χρησιμοποιώντας κλασική μαθηματική επαγωγή ως προς τον m δείχνουμε εύκολα ότι το $\left(g^{-1}\right)^m$ είναι το αντίστροφο τού g^m. Εάν $m = 0$, τότε $g^{-m} = \left(g^{-1}\right)^m = (g^m)^{-1} = e_G$. Τέλος, στην περίπτωση κατά την οποία $m < 0$, χρησιμοποιούμε εκ νέου μαθηματική επαγωγή, αλλ' αυτήν τη φορά με *οπισθοπορεία ως προς τον* m, με σύνολο αναφοράς μας το $\{k \in \mathbb{Z} \,|\, k \leqslant -1\}$, εκκινώντας από τον $m = -1$. Όταν $m = -1$, ο ισχυρισμός είναι προφανώς αληθής λόγω τού 3.2.9 (ii). Έχοντας τις $g^{-m} = \left(g^{-1}\right)^m = (g^m)^{-1}$ ως επαγωγική μας υπόθεση, μέσω τού (i) και των 3.2.9 (ii), (iii) λαμβάνουμε

$$g^{-(m-1)} = g^{-m}g = \left(g^{-1}\right)^m (g^{-1})^{-1} = \left(g^{-1}\right)^{m-1}$$

και

$$g^{-(m-1)} = g^{-m}g = (g^m)^{-1}(g^{-1})^{-1} = (g^{-1}g^m)^{-1} = \left(g^{m-1}\right)^{-1}.$$

Τούτο ολοκληρώνει την απόδειξη. □

3.2.12 Παρατήρηση. Όταν ένα στοιχείο $g \in G$ γράφεται ως «γινόμενο» $g = xy$ δυο στοιχείων x, y τής G, το «τετράγωνό του» $g^2 = (xy)^2 = (xy)(xy)$ *δεν ισούται* κατ' ανάγκην με το x^2y^2! Ωστόσο, είναι εύκολο να αποδειχθεί (επαγωγικώς) ότι ισχύουν οι ισότητες

$$(xy)^n = x^n y^n,\ \forall n \in \mathbb{Z}, \quad \text{και} \quad x^m y^n = y^n x^m,\ \forall (m, n) \in \mathbb{Z} \times \mathbb{Z},$$

για οιαδήποτε στοιχεία x, y τής G *για τα οποία ισχύει η ισότητα* $xy = yx$.

▸ **Υποομάδες**. Η υποδομή που αντιστοιχεί στην αλγεβρική δομή τής ομάδας είναι η *υποομάδα*.

3.2.13 Ορισμός. Ένα μη κενό υποσύνολο H τού υποκειμένου συνόλου G μιας ομάδας $(G,\cdot)$ καλείται **υποομάδα** τής G όταν το H είναι κλειστό ως προς την πράξη τής G (βλ. 1.5.2) και καθίσταται αφ' εαυτού μια ομάδα (ως προς τον περιορισμό της $\cdot|_{H\times H}$). Για να δηλούμε εν συντομία ότι το ζεύγος $(H,\cdot|_{H\times H})$ αποτελεί μια υποομάδα τής $(G,\cdot)$ θα χρησιμοποιούμε συχνά και τον συμβολισμό[11] $H\sqsubseteq G$.

3.2.14 Ορισμός. Όταν $H\sqsubseteq G$ και $H\neq G$, τότε η H λέγεται, ιδιαιτέρως, **γνήσια υποομάδα** τής G. Χρησιμοποιούμενος συμβολισμός (όταν επιθυμούμε να δώσουμε *έμφαση* στο ότι η H είναι γνήσια): $H\sqsubset G$.

3.2.15 Παρατήρηση. (i) Κάθε υποομάδα H μιας *πεπερασμένης* ομάδας $(G,\cdot)$ είναι πεπερασμένη, διότι $|H|\leqslant|G|<\infty$. (Φυσικά, μια *άπειρη* ομάδα διαθέτει πάντοτε[12] τόσον πεπερασμένες όσον και άπειρες υποομάδες.)

(ii) Κάθε υποομάδα H μιας *αβελιανής* ομάδας $(G,\cdot)$ είναι αβελιανή, διότι για κάθε ζεύγος $(x,y)\in H\times H$ έχουμε αυτομάτως $(x,y)\in G\times G$, οπότε $xy=yx$. (Φυσικά, μια *μη αβελιανή* ομάδα διαθέτει πάντοτε[13] τόσον αβελιανές όσον και μη αβελιανές υποομάδες.).

(iii) Για τον έλεγχο τού κατά πόσον ένα μη κενό υποσύνολο H τού υποκειμένου συνόλου G μιας ομάδας $(G,\cdot)$ καθίσταται υποομάδα τής $(G,\cdot)$ *δεν* απαιτείται ο έλεγχος τής ισχύος τής προσεταιριστικής ιδιότητας, διότι για κάθε $(x,y,z)\in H\times H\times H$ έχουμε αυτομάτως $(x,y,z)\in G\times G\times G$, οπότε $x(yz)=(xy)z$. Η επομένη πρόταση μας πληροφορεί για το ποιες (ικανές και αναγκαίες) συνθήκες οφείλουν να πληρούνται, ούτως ώστε ένα δεδομένο υποσύνολο $H\subseteq G$ να είναι υποομάδα τής ομάδας $(G,\cdot)$.

3.2.16 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H\subseteq G$. Τότε τα* (i), (ii) *και* (iii) *είναι ισοδύναμα*:

(i) $H\sqsubseteq G$.

(ii) *Το H πληροί τις εξής συνθήκες*:

(a) *Το ουδέτερο στοιχείο τής G ανήκει στο H.*

(b) $xy\in H,\ \forall(x,y)\in H\times H$.

(c) $h^{-1}\in H,\ \forall h\in H$.

(iii) *Το H πληροί τις εξής συνθήκες*:

(a) *Το ουδέτερο στοιχείο τής G ανήκει στο H.*

(b) $ab^{-1}\in H,\ \forall(a,b)\in H\times H$.

Απόδειξη. (i)⇒(ii). Εάν $H\sqsubseteq G$, τότε $H\neq\varnothing$ και οι (b) και (c) ικανοποιούνται. Εξάλλου, η H διαθέτει ουδέτερο στοιχείο e_H για το οποίο ισχύει

$$e_Hh=he_H=h,\quad\forall h\in H.$$

[11] Κατ' αντιστοιχίαν, ο συμβολισμός "$H\ \sqsubsetneq\ G$" θα σημαίνει ότι το υποσύνολο H τού G *δεν είναι υποομάδα* τής ομάδας $(G,\cdot)$ (ως προς την $\cdot|_{H\times H}$).

[12] Επειδή το μονοσύνολο $\{e_G\}$ αποτελεί πάντοτε υποομάδα οιασδήποτε ομάδας $(G,\cdot)$ (πρβλ. 3.2.21 (i)) και $G\sqsubseteq G$, εάν υποθέσουμε ότι $|G|=\infty$, τότε το $\{e_G\}$ έχει πληθικό αριθμό 1, ενώ το υποκείμενο σύνολο τής ομάδας αναφοράς μας είναι απειροπληθές.

[13] Εάν η $(G,\cdot)$ είναι μη αβελιανή, τότε η $\{e_G\}$ είναι προφανώς *αβελιανή* υποομάδα της.

Επειδή κάθε $h \in H$ ανήκει και στην G, έχουμε $he_G = h$, οπότε το μονοσήμαντο τής επιλύσεως των προκειμένων εξισώσεων (βλ. 3.2.9 (iv)) δίδει $e_G = e_H$.

(ii)⇒(iii). Αρκεί να αποδειχθεί η ισχύς τής (b) τού (iii). Εάν $(a, b) \in H \times H$, τότε (κατά την (ii) (c)) $b^{-1} \in H$, οπότε $ab^{-1} \in H$ (δυνάμει τής (ii) (b)).

(iii)⇒(i). Όπως προείπαμε, ο έλεγχος τής ισχύος τής προσεταιριστικής ιδιότητας περιττεύει. Εξάλλου, $H \neq \varnothing$ λόγω τής (iii) (a). Υποθέτοντας λοιπόν ότι $ab^{-1} \in H$ για *κάθε* $(a, b) \in H \times H$, επιχειρηματολογούμε ως εξής: εάν $a \in H$, τότε έχουμε $e_G = aa^{-1} \in H$ και $a^{-1} = e_G a^{-1} \in H$. Τούτο σημαίνει ότι η ύπαρξη *αντιστρόφου* εντός τής H είναι διασφαλισμένη. Απομένει ο έλεγχος τής «κλειστότητας» τής πράξεως, ήτοι ότι $xy \in H,\ \forall (x, y) \in H \times H$. Θέτοντας $a = x \in H$ και $b = y^{-1}$ (το οποίο ανήκει, όπως διαπιστώσαμε, στο H), λαμβάνουμε μέσω εφαρμογής τής (iii) (b): $x\left(y^{-1}\right)^{-1} = xy \in H$, ήτοι το ζητούμενο. Άρα $H \sqsubseteq G$. □

3.2.17 Παρατήρηση. Οι συνθήκες (ii) (a) και (iii) (a) συμπεριελήφθησαν στην πρόταση 3.2.16 μόνον για να μας εγγυηθούν ότι το θεωρούμενο σύνολο H δεν είναι κενό. Εάν προϋποθέσουμε ότι το H διαθέτει τουλάχιστον ένα στοιχείο, τότε, εφαρμόζοντας τη συνθήκη (ii) (c) για κάποιο στοιχείο, ας πούμε h_0, τού H, λαμβάνουμε $h_0^{-1} \in H$, οπότε μέσω τής (ii) (b) συνάγεται ότι $h_0 h_0^{-1} = e_G \in H$. Κατ' αναλογίαν, εφαρμόζοντας τη συνθήκη (iii) (b) για $a = b$ λαμβάνουμε εκ νέου $e_G \in H$.

3.2.18 Πόρισμα. *Έστω $(G, \cdot)$ μια ομάδα. Τότε για κάθε $H \sqsubseteq G$ έχουμε $e_H = e_G$.*

3.2.19 Πόρισμα. *Έστω $(G, \cdot)$ μια ομάδα και έστω $\varnothing \neq H \subseteq G$. Εάν το H είναι πεπερασμένο σύνολο, τότε τα* (i) *και* (ii) *είναι ισοδύναμα*:

(i) $H \sqsubseteq G$.

(ii) $ab \in H,\ \forall (a, b) \in H \times H$.

Απόδειξη. Η συνεπαγωγή (i)⇒(ii) είναι προφανής (λόγω τής συνεπαγωγής (i)⇒(ii) (b) στην πρόταση 3.2.16). Επειδή $H \neq \varnothing$, για να ισχύει η αντίστροφη συνεπαγωγή[14] (ii)⇒(i) αρκεί να ελεγχθεί ότι $h^{-1} \in H,\ \forall h \in H$ (βλ. 3.2.17). Προς τούτο θεωρούμε *τυχόν* στοιχείο $h \in H$. Εάν $h = e_G$, τότε προφανώς $e_G^{-1} = e_G \in H$. Εάν $h \neq e_G$, τότε $h^2 \in H$ (λόγω τής (ii)). Κάνοντας χρήση κλασικής μαθηματικής επαγωγής αποδεικνύουμε (μέσω τής (ii)) ότι $h^n = \left(h^{n-1}\right) h \in H$ *για κάθε* $n \in \mathbb{N}$. Κατά συνέπειαν,

$$\left.\begin{array}{r} \{h^n \mid n \in \mathbb{N}\} \subseteq H \\ \mathrm{card}(H) < \infty \ \text{(εξ υποθέσεως)} \end{array}\right\} \Rightarrow \exists i, j \in \mathbb{N},\ i > j : h^i = h^j.$$

Εξ αυτού έπεται ότι

$$\left.\begin{array}{r} h^{i-j} = e_G,\ h \neq e_G \Rightarrow i - j > 1 \\ h^{i-j} = h(h^{i-j-1}) = e_G \end{array}\right\} \Rightarrow h^{-1} = h^{i-j-1} \in H,$$

οπότε ισχύει πράγματι ότι $h^{-1} \in H$. □

3.2.20 Πόρισμα. *Έστω $(G, \cdot)$ μια ομάδα. Εάν $H \sqsubseteq G$ και $\varnothing \neq K \subseteq H$, τότε*

$$K \sqsubseteq G \Longleftrightarrow K \sqsubseteq H.$$

[14] Η συνεπαγωγή (ii)⇒(i) ενδέχεται να μην ισχύει όταν το H δεν είναι πεπερασμένο σύνολο. Π.χ., για την $(\mathbb{Z}, +)$ και για $H := \mathbb{N}$ έχουμε $m + n \in H,\ \forall (m, n) \in H \times H$ αλλά $H \not\sqsubseteq G$ (διότι $-n \notin H,\ \forall n \in H$).

ΑΠΟΔΕΙΞΗ. Εάν $K \sqsubseteq G$ και εάν θεωρήσουμε τυχόντα στοιχεία $x_1, x_2 \in K$, τότε $x_1 x_2^{-1} \in K \subseteq H$, οπότε $K \sqsubseteq H$ (επί τη βάσει τού (iii) τής προτάσεως 3.2.16 και τής παρατηρήσεως 3.2.17). Και αντιστρόφως· εάν $K \sqsubseteq H$ και εάν $x_1, x_2 \in K$, τότε $x_1 x_2^{-1} \in K \subseteq G$, οπότε $K \sqsubseteq G$ (για τον ίδιο λόγο). □

3.2.21 Παραδείγματα. (i) Κάθε ομάδα $(G, \cdot)$ έχει πάντοτε δύο προφανείς υποομάδες, ήτοι τον εαυτό της και την **τετριμμένη υποομάδα** $\{e_G\}$ που αποτελείται -εξ ορισμού- μόνον από το ουδέτερο στοιχείο της.

(ii) Η ομάδα $(\mathbb{Z}^\times = \{1, -1\}, \cdot)$ είναι υποομάδα τής $(\mathbb{Q}\setminus\{0\}, \cdot)$ (όπως έπεται άμεσα από την πρόταση 3.2.16).

(iii) Έστω $n \in \mathbb{Z}$ και έστω $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$ το σύνολο όλων των ακεραίων πολλαπλασίων του. Τότε, εφαρμόζοντας την πρόταση 3.2.16, διαπιστώνουμε ότι το $(n\mathbb{Z}, +)$ είναι μια υποομάδα τής $(\mathbb{Z}, +)$.

(iv) Οι εγκλεισμοί $\mathbb{Z} \subsetneqq \mathbb{Q}$, $\mathbb{Z} \subsetneqq \mathbb{R}$, $\mathbb{Z} \subsetneqq \mathbb{C}$, $\mathbb{Q} \subsetneqq \mathbb{R}$, $\mathbb{Q} \subsetneqq \mathbb{C}$ και $\mathbb{R} \subsetneqq \mathbb{C}$ καθιστούν αυτά τα υποσύνολα υποομάδες ως προς την πράξη τής συνήθους προσθέσεως.

(v) Οι εγκλεισμοί $\mathbb{Q}\setminus\{0\} \subsetneqq \mathbb{R}\setminus\{0\}$, $\mathbb{Q}\setminus\{0\} \subsetneqq \mathbb{C}\setminus\{0\}$ και $\mathbb{R}\setminus\{0\} \subsetneqq \mathbb{C}\setminus\{0\}$ καθιστούν αυτά τα υποσύνολα υποομάδες ως προς την πράξη τού συνήθους πολλαπλασιασμού.

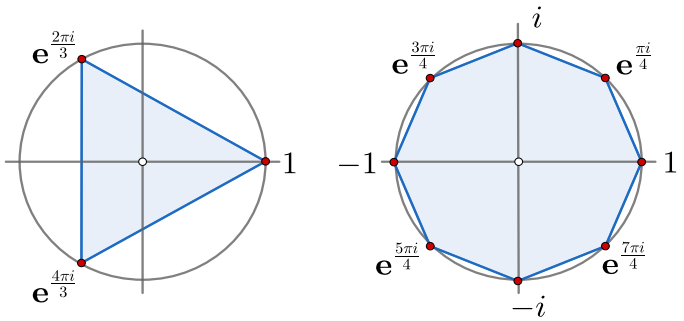
(vi) Ο **μοναδιαίος κύκλος**

$$\boxed{\mathbb{S}^1 := \{z \in \mathbb{C} \mid |z| = 1\},}$$

εφοδιασμένος με τον συνήθη πολλαπλασιασμό μιγαδικών αριθμών, αποτελεί υποομάδα τής $(\mathbb{C}\setminus\{0\}, \cdot)$. Επίσης, το σύνολο των n-**οστών ριζών τής μονάδας**[15]

$$\boxed{\mathcal{E}_n := \{z \in \mathbb{C} \mid z^n = 1\}, \quad n \in \mathbb{N},}$$

είναι μια (γνήσια) υποομάδα τής $(\mathbb{S}^1, \cdot)$, καθότι $1 \in \mathcal{E}_n$ και για οιαδήποτε στοιχεία $z_1, z_2 \in \mathcal{E}_n$ έχουμε $\left(z_1 z_2^{-1}\right)^n = z_1^n z_2^{-n} = 1 \Rightarrow z_1 z_2^{-1} \in \mathcal{E}_n$. Θέτοντας $\zeta_n := \exp\left(\frac{2\pi i}{n}\right)$, λαμβάνουμε[16] $\mathcal{E}_n = \left\{\zeta_n^k \mid k \in \{0, 1, ..., n-1\}\right\}$. Όταν $n \geqslant 3$, τα στοιχεία τής ομάδας $\mathcal{E}_n$ (ιδωμένα ως σημεία τού μιγαδικού επιπέδου $\mathbb{C}$) αποτελούν τις κορυφές ενός κανονικού n-γώνου[17] P_n (εγγεγραμμένου εντός τού μοναδιαίου κύκλου $\mathbb{S}^1$). Επί παραδείγματι, το ισόπλευρο τρίγωνο P_3 και το κανονικό οκτάγωνο P_8 εικονογραφούνται ως εξής:



[15] Το σύμβολο "$\mathcal{E}$" προέρχεται από το πρώτο γράμμα τής (γερμανικής) λέξεως Einheitswurzel (= ρίζα τής μονάδας).

[16] Εάν $z = r\mathbf{e}^{i\theta}$, $r \in \mathbb{R}_{>0}$, $0 \leqslant \theta < 2\pi$, είναι ένα στοιχείο τής $\mathcal{E}_n$, τότε

$$z^n = 1 \Leftrightarrow r^n = \mathbf{e}^{in\theta} = 1 \Leftrightarrow r = 1,\ \theta \in \left\{\frac{2\pi k i}{n} \,\middle|\, k \in \{0, 1, ..., n-1\}\right\}.$$

[17] Έστω $n \in \mathbb{N}$, $n \geqslant 3$. Ένα κυρτό πολύγωνο καλείται **κανονικό** n-**γωνο** όταν διαθέτει n ισομήκεις πλευρές (και, κατ' επέκταση, n ίσες γωνίες).

(vii) Έστω $(R,\cdot)$ το αβελιανό μονοειδές με $R\in\{\mathbb{Q},\mathbb{R},\mathbb{C}\}$, όπου "$\cdot$" ο συνήθης πολλαπλασιασμός. Το σύνολο

$$\boxed{\mathrm{SL}_n(R):=\{\mathbf{A}\in\mathrm{GL}_n(R)\mid \det(\mathbf{A})=1_R\},}$$

εφοδιασμένο με τον πολλαπλασιασμό $(n\times n)$-πινάκων, αποτελεί μια υποομάδα τής $(\mathrm{GL}_n(R),\cdot)$ (βλ. 3.2.7 (iv)) που είναι, μάλιστα, *γνήσια* υποομάδα της. Η $(\mathrm{SL}_n(R),\cdot)$ καλείται **ειδική γραμμική ομάδα** (βαθμού n υπεράνω τού R).

(viii) Έστω $n\in\mathbb{N}$. Από τη θεωρία πινάκων με τις εγγραφές τους ειλημμένες από τους πραγματικούς αριθμούς προκύπτει ο ακόλουθος «πύργος» πολλαπλασιαστικών υποομάδων

$$\boxed{\begin{array}{c}\mathrm{GL}_n(\mathbb{R})=\{\mathbf{A}\in\mathrm{Mat}_{n\times n}(\mathbb{R})\mid\det(\mathbf{A})\neq 0\}\quad\supset\mathrm{SL}_n(\mathbb{R})\\ \bigsqcup\\ \mathrm{O}_n(\mathbb{R}):=\left\{\mathbf{A}\in\mathrm{GL}_n(\mathbb{R})\;\middle|\;\mathbf{A}^{\intercal}=\mathbf{A}^{-1}\right\}\\ \bigsqcup\\ \mathrm{SO}_n(\mathbb{R}):=\mathrm{O}_n(\mathbb{R})\cap\mathrm{SL}_n(\mathbb{R}),\end{array}}$$

όπου $\mathbf{A}^{\intercal}$ ο ανάστροφος[18] ενός $\mathbf{A}\in\mathrm{GL}_n(\mathbb{R})$. (Για $n=1$ έχουμε $\mathrm{GL}_1(\mathbb{R})=\mathbb{R}\smallsetminus\{0\}$, $\mathrm{O}_1(\mathbb{R})=\{1,-1\}$ και $\mathrm{SL}_1(\mathbb{R})=\mathrm{SO}_1(\mathbb{R})=\{1\}$.) Η ομάδα $\mathrm{O}_n(\mathbb{R})$ καλείται **ορθογώνια** και η $\mathrm{SO}_n(\mathbb{R})$ **ειδική ορθογώνια ομάδα**.

(ix) Κατ' αναλογίαν, από τη θεωρία πινάκων με τις εγγραφές τους ειλημμένες από τους μιγαδικούς αριθμούς προκύπτει ο ακόλουθος «πύργος» πολλαπλασιαστικών υποομάδων

$$\boxed{\begin{array}{c}\mathrm{GL}_n(\mathbb{C})=\{\mathbf{A}\in\mathrm{Mat}_{n\times n}(\mathbb{C})\mid\det(\mathbf{A})\neq 0\}\quad\supset\mathrm{SL}_n(\mathbb{C})\\ \bigsqcup\\ \mathrm{U}_n(\mathbb{C}):=\left\{\mathbf{A}\in\mathrm{GL}_n(\mathbb{C})\;\middle|\;\overline{\mathbf{A}}^{\intercal}=\mathbf{A}^{-1}\right\}\\ \bigsqcup\\ \mathrm{SU}_n(\mathbb{C}):=\mathrm{U}_n(\mathbb{C})\cap\mathrm{SL}_n(\mathbb{C}),\end{array}}$$

όπου $\overline{\mathbf{A}}^{\intercal}$ ο αναστροφοσυζυγής ενός $\mathbf{A}\in\mathrm{GL}_n(\mathbb{C})$. (Όταν $n=1$, τότε έχουμε

$$\mathrm{GL}_1(\mathbb{C})=\mathbb{C}\smallsetminus\{0\},\ \mathrm{U}_1(\mathbb{C})=\mathbb{S}^1\ \text{ και }\ \mathrm{SL}_1(\mathbb{C})=\mathrm{SU}_1(\mathbb{C})=\{1\}.)$$

Η ομάδα $\mathrm{U}_n(\mathbb{C})$ καλείται **μοναδιακή** και η $\mathrm{SU}_n(\mathbb{C})$ **ειδική μοναδιακή ομάδα**.

3.2.22 Πρόταση. *Έστω ότι η $(G,\cdot)$ είναι μια ομάδα και οι H,H_1,H_2,H_3 υποομάδες της. Τότε ισχύουν τα ακόλουθα*:

(i) $H\sqsubseteq H$.

(ii) *Εάν* $H_1\sqsubseteq H_2$ *και* $H_2\sqsubseteq H_1$, *τότε* $H_1=H_2$.

(iii) *Εάν* $H_1\sqsubseteq H_2$ *και* $H_2\sqsubseteq H_3$, *τότε* $H_1\sqsubseteq H_3$.

Απόδειξη. Το (i) είναι προφανές. Τα (ii)-(iii) έπονται άμεσα από τις αντίστοιχες ιδιότητες τού συνολοθεωρητικού εγκλεισμού " $\subseteq$ ", την πρόταση 3.2.16 και το πόρισμα 3.2.20. □

3.2.23 Πρόταση. *Η τομή $\bigcap_{j\in J}H_j$ των μελών οιασδήποτε οικογενείας υποομάδων $(H_j)_{j\in J}$ μιας ομάδας $(G,\cdot)$ αποτελεί μια υποομάδα τής G.*

[18] Ο **ανάστροφος** ενός τετραγωνικού πίνακα είναι αυτός που προκύπτει όταν καθιστούμε τις γραμμές του στήλες (και τις στήλες του γραμμές).

ΑΠΟΔΕΙΞΗ. Επειδή $e_G \in H_j$ για κάθε $j \in J$, έχουμε $e_G \in \bigcap_{j\in J} H_j$, οπότε η τομή αυτή δεν είναι κενή. Εάν $h_1, h_2 \in \bigcap_{j\in J} H_j$, τότε

$$[h_1, h_2 \in H_j,\ \forall j \in J] \Longrightarrow \left[h_1 h_2^{-1} \in H_j,\ \forall j \in J\right] \Longrightarrow h_1 h_2^{-1} \in \bigcap_{j\in J} H_j.$$

Άρα $\bigcap_{j\in J} H_j \sqsubseteq G$ (βλ. 3.2.16 (iii)). □

3.2.24 Σημείωση. Εάν $H, K \sqsubseteq G$, τότε η ένωση $H \cup K$ δεν είναι πάντοτε υποομάδα τής G. Επί παραδείγματι, στην ομάδα $(\mathbb{Z}, +)$ έχουμε

$$2\mathbb{Z} \sqsubseteq \mathbb{Z},\ 3\mathbb{Z} \sqsubseteq \mathbb{Z},\ 2 \in 2\mathbb{Z},\ 3 \in 3\mathbb{Z},$$

αλλά $5 = 2 + 3 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$, οπότε $2\mathbb{Z} \cup 3\mathbb{Z} \not\sqsubseteq \mathbb{Z}$.

3.2.25 Πρόταση. *Εάν οι H, K είναι δυο υποομάδες μιας ομάδας $(G, \cdot)$, τότε ισχύει η αμφίπλευρη συνεπαγωγή*:

$$H \cup K \sqsubseteq G \Leftrightarrow \textit{είτε}\quad H \sqsubseteq K\ \ \textit{είτε}\quad K \sqsubseteq H.$$

ΑΠΟΔΕΙΞΗ. "⇒" Ας υποθέσουμε ότι $H \not\sqsubseteq K$ και $K \not\sqsubseteq H$. Τότε υπάρχει $x \in H \smallsetminus K$ και υπάρχει $y \in K \smallsetminus H$. Προφανώς, $x \in H \cup K$ και $y \in H \cup K$. Εάν η ένωση $H \cup K$ ήταν υποομάδα τής G, θα έπρεπε (λόγω τής κλειστότητας τής πράξεως) να ισχύει $xy \in H \cup K$, δηλαδή είτε $xy \in H$ είτε $xy \in K$, πράγμα αδύνατο, διότι τότε θα είχαμε είτε

$$\left.\begin{array}{r} xy \in H \\ x \in H \Rightarrow x^{-1} \in H \end{array}\right\} \Rightarrow x^{-1}(xy) = y \in H$$

είτε

$$\left.\begin{array}{r} xy \in K \\ y \in K \Rightarrow y^{-1} \in K \end{array}\right\} \Rightarrow (xy)y^{-1} = x \in K.$$

Άρα $H \cup K \not\sqsubseteq G$. Η αντίστροφη συνεπαγωγή "⇐" είναι προφανής, διότι εν τοιαύτη περιπτώσει είτε $H \cup K = H$ είτε $H \cup K = K$. □

▸ **Διαγράμματα τού Hasse για σύνολα υποομάδων μιας ομάδας**. Οιοδήποτε υποσύνολο τού συνόλου των υποομάδων μιας ομάδας είναι μερικώς διατεταγμένο ως προς την " $\sqsubseteq$ ". (Μάλιστα, το σύνολο *όλων των υποομάδων* μιας ομάδας καθίσταται *σύνδεσμος* ως προς αυτήν.) Ως εκ τούτου, τα διαγράμματα τού Hasse (βλ. 1.4.4) είναι υποβοηθητικά στη μελέτη ενός πεπερασμένου υποσυνόλου υποομάδων δοθείσας ομάδας (και, ειδικότερα, τού συνόλου *όλων* των υποομάδων δοθείσας *πεπερασμένης* ομάδας).

3.2.26 Πρόταση. *Έστω $(G, \cdot)$ μια ομάδα. Τότε το ζεύγος $(\mathbf{Subg}(G), \sqsubseteq)$, όπου*

$$\boxed{\mathbf{Subg}(G) := \{H \in \mathfrak{P}(G) \mid H \sqsubseteq G\},}$$

και, γενικότερα, το ζεύγος $(\mathfrak{X}, \sqsubseteq)$, όπου $\varnothing \neq \mathfrak{X} \subseteq \mathbf{Subg}(G)$, αποτελεί μερικώς διατεταγμένο σύνολο.

ΑΠΟΔΕΙΞΗ.[19] Αυτή έπεται άμεσα από την πρόταση 3.2.22. □

[19] Προσοχή! Στην καταγραφή ή στην απαρίθμηση των μελών τού συνόλου $\mathbf{Subg}(G)$ περιλαμβάνονται *όλες* οι *σαφώς διακεκριμένες* (ήτοι οι *ανά δύο διαφορετικές*) υποομάδες τής G (ασχέτως με το αν κάποιες εξ αυτών ενδέχεται να είναι *ισόμορφες* υπό την έννοια τού ορισμού 3.5.7).

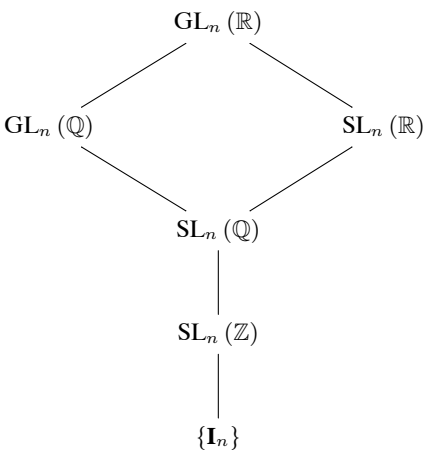
3.2.27 Παραδείγματα. Τα διαγράμματα τού Hasse για τα μερικώς διατεταγμένα σύνολα $(\mathbf{Subg}(\mathbb{Z}_2), \sqsubseteq)$ και $(\mathbf{Subg}(\mathbb{Z}_4), \sqsubseteq)$ των ομάδων $(\mathbb{Z}_2, +)$ και $(\mathbb{Z}_4, +)$ είναι τα εξής:

(Ένας γενικότερος χαρακτηρισμός των $(\mathbf{Subg}(\mathbb{Z}_m), \sqsubseteq)$ για *οιουσδήποτε* $m \in \mathbb{N}$ θα δοθεί αργότερα στο εδάφιο 3.5.29 (ii).)

3.2.28 Παράδειγμα. Έστω $n \in \mathbb{N}$, $n \geqslant 2$. Το διάγραμμα τού Hasse για το μερικώς διατεταγμένο σύνολο $(\mathfrak{X}, \sqsubseteq)$, όπου

$$\mathfrak{X} := \{\{\mathbf{I}_n\}, \mathrm{SL}_n(\mathbb{Z}), \mathrm{SL}_n(\mathbb{Q}), \mathrm{SL}_n(\mathbb{R}), \mathrm{GL}_n(\mathbb{Q}), \mathrm{GL}_n(\mathbb{R})\} \subsetneqq \mathbf{Subg}(\mathrm{GL}_n(\mathbb{R})),$$

είναι το



3.2.29 Σημείωση. Έστω $(G, \cdot)$ μια ομάδα. Το μερικώς διατεταγμένο σύνολο $(\mathbf{Subg}(G), \subseteq)$ δεν είναι κατ' ανάγκην *υποσύνδεσμος* τού συνδέσμου $(\mathfrak{P}(G), \subseteq)$ (βλ. 1.4.2 (i), 1.4.22, 1.4.23 (i) και 1.4.25), διότι (όπως έχουμε ήδη προαναφέρει στο εδάφιο 3.2.24) η ένωση δυο υποομάδων τής $(G, \cdot)$ δεν είναι κατ' ανάγκην υποομάδα της. Για να καταστήσουμε το σύνολο $\mathbf{Subg}(G)$ σύνδεσμο (βλ. 1.4.22) οφείλουμε να αντικαταστήσουμε τη σχέση εγκλεισμού " $\subseteq$ " με τη σχέση " $\sqsubseteq$ ".

3.2.30 Πρόταση. *Το μερικώς διατεταγμένο σύνολο* $(\mathbf{Subg}(G), \sqsubseteq)$ *είναι σύνδεσμος για κάθε ομάδα* $(G, \cdot)$ (βλ. 1.4.22). *Μάλιστα, για οιεσδήποτε* $H, K \in \mathbf{Subg}(G)$ *έχουμε*

$$H \wedge K = H \cap K, \quad H \vee K = \bigcap \{L \in \mathbf{Subg}(G) \mid H \cup K \subseteq L\}.$$

Απόδειξη. Εάν $H, K \in \mathbf{Subg}(G)$, τότε

$$\left.\begin{array}{r} \text{3.2.23} \Rightarrow H \cap K \in \mathbf{Subg}(G) \\ H \cap K \subseteq H \ \text{ και } \ H \cap K \subseteq K \end{array}\right\} \underset{\text{3.2.20}}{\Longrightarrow} H \cap K \sqsubseteq H \ \text{ και } \ H \cap K \sqsubseteq K.$$

Άρα η $H \cap K \in \mathbf{Subg}(G)$ είναι ένα κάτω φράγμα τού $\{K, H\}$ ως προς την " $\sqsubseteq$ ". Έστω $N \in \mathbf{Subg}(G)$ *τυχόν* κάτω φράγμα τού $\{K, H\}$ ως προς την " $\sqsubseteq$ ". Τότε

$$\left.\begin{array}{r} N \in \mathbf{Subg}(G) \\ N \subseteq H \ \text{ και } \ N \subseteq K \Rightarrow N \cap N = N \subseteq H \cap K \end{array}\right\} \underset{\text{3.2.20}}{\Longrightarrow} N \sqsubseteq H \cap K.$$

Κατά συνέπειαν, η τομή $H \cap K$ είναι το (κατ' ανάγκην μοναδικό, λόγω τής προτάσεως 1.4.15) *μέγιστο κάτω φράγμα* τού $\{K, H\}$ ως προς την " $\sqsubseteq$ ". Επιπροσθέτως, από την πρόταση 3.2.23 έπεται ότι

$$\bigcap \{L \in \mathbf{Subg}(G) \mid H \cup K \subseteq L\} \in \mathbf{Subg}(G).$$

Επειδή τόσον το σύνολο H όσον και το σύνολο K είναι υποσύνολα τού $\bigcap \{L \in \mathbf{Subg}(G) \mid H \cup K \subseteq L\}$ έχουμε (μέσω τού πορίσματος 3.2.20)

$$H \sqsubseteq \bigcap \{L \in \mathbf{Subg}(G) \mid H \cup K \subseteq L\} \text{ και } K \sqsubseteq \bigcap \{L \in \mathbf{Subg}(G) \mid H \cup K \subseteq L\}.$$

Άρα η $\bigcap \{L \in \mathbf{Subg}(G) \mid H \cup K \subseteq L\}$ είναι ένα άνω φράγμα τού $\{K, H\}$ ως προς την " $\sqsubseteq$ ". Έστω $\Xi \in \mathbf{Subg}(G)$ *τυχόν* άνω φράγμα τού $\{K, H\}$ ως προς την " $\sqsubseteq$ ". Τότε $H \subseteq \Xi$ και $K \subseteq \Xi \Rightarrow H \cup K \subseteq \Xi \Rightarrow \bigcap \{L \in \mathbf{Subg}(G) \mid H \cup K \subseteq L\} \subseteq \Xi$, οπότε

$$\left.\begin{array}{r} \Xi \in \mathbf{Subg}(G) \\ \bigcap \{L \in \mathbf{Subg}(G) \mid H \cup K \subseteq L\} \subseteq \Xi \end{array}\right\} \underset{3.2.20}{\Longrightarrow} \bigcap \{L \in \mathbf{Subg}(G) \mid H \cup K \subseteq L\} \sqsubseteq \Xi.$$

Κατά συνέπειαν, η τομή $\bigcap \{L \in \mathbf{Subg}(G) \mid H \cup K \subseteq L\}$ είναι το (κατ' ανάγκην μοναδικό, λόγω τής προτάσεως 1.4.15) *ελάχιστο άνω φράγμα* τού $\{K, H\}$ ως προς την " $\sqsubseteq$ ". □

3.2.31 Σημείωση. Με ανάλογο τρόπο αποδεικνύεται ότι ο $(\mathbf{Subg}(G), \sqsubseteq)$ είναι *πλήρης σύνδεσμος*. (Βλ. εδάφιο 1.4.24 (iii).) Επί παραδείγματι, εάν $(H_j)_{j \in J}$ είναι τυχούσα οικογένεια υποομάδων τής G, τότε

$$\bigwedge_{j \in J} H_j = \bigcap_{j \in J} H_j \text{ και } \bigvee_{j \in J} H_j = \bigcap \left\{ L \in \mathbf{Subg}(G) \;\middle|\; \bigcup_{j \in J} H_j \subseteq L \right\}.$$

3.2.32 Πόρισμα. *Έστω $(G, \cdot)$ μια ομάδα. Εάν $L \sqsubseteq G$ και*

$$\boxed{\mathbf{Subg}(G; L) := \{H \in \mathbf{Subg}(G) \mid L \sqsubseteq H\},}$$

τότε το μερικώς διατεταγμένο σύνολο $(\mathbf{Subg}(G; L), \sqsubseteq)$ είναι ένας υποσύνδεσμος τού $(\mathbf{Subg}(G), \sqsubseteq)$.

Απόδειξη. Για οιεσδήποτε $H, K \in \mathbf{Subg}(G; L)$ έχουμε $H \wedge K \in \mathbf{Subg}(G; L)$ και $H \vee K \in \mathbf{Subg}(G; L)$. □

3.2.33 Σημείωση. Για οιαδήποτε ομάδα $(G, \cdot)$, το $\mathbf{Subg}(G)$ ως προς την " $\sqsubseteq$ " έχει την τετριμμένη υποομάδα $\{e_G\}$ ως *ελάχιστο* και την ίδια την G ως *μέγιστο* στοιχείο του. Γι' αυτόν τον λόγο, η μελέτη ιδιοτήτων διατάξεως υποομάδων εστιάζεται κυρίως στις υπόλοιπες, ήτοι στις μη τετριμμένες, από τη μια μεριά, και στις γνήσιες, από την άλλη.

3.2.34 Ορισμός. Έστω $(G, \cdot)$ μια ομάδα με[20] $|G| \geqslant 2$.

(i) Κάθε υποομάδα της ανήκουσα στο

$$\mathbf{Min\text{-}Subg}(G) := \left\{ H \;\middle|\; \begin{array}{c} H \text{ ελαχιστικό στοιχείο τού } \mathbf{Subg}(G) \setminus \{\{e_G\}\} \\ \text{ως προς την " } \sqsubseteq|_{\mathbf{Subg}(G) \setminus \{\{e_G\}\}} \text{ "} \end{array} \right\}$$

καλείται **ελαχιστική υποομάδα τής** G, ενώ κάθε υποομάδα της ανήκουσα στο

$$\mathbf{Max\text{-}Subg}(G) := \left\{ H \;\middle|\; \begin{array}{c} H \text{ μεγιστικό στοιχείο τού } \mathbf{Subg}(G) \setminus \{G\} \\ \text{ως προς την " } \sqsubseteq|_{\mathbf{Subg}(G) \setminus \{G\}} \text{ "} \end{array} \right\}$$

καλείται **μεγιστική υποομάδα τής** G. (Πρβλ. 1.4.9.)

(ii) Έστω ΙΔ μια (ειδική) ιδιότητα[21] που αφορά σε υποομάδες (ή που χαρακτηρίζει ρητώς κάποιες υποομάδες) τής G. Κάθε υποομάδα τής G ανήκουσα στο

$$\textbf{Min-Subg}(G) \cap \{H \in \textbf{Subg}(G) \mid \text{η } H \text{ έχει την ιδιότητα ΙΔ}\} \tag{3.4}$$

καλείται **ελαχιστική υποομάδα τής** G **με την ιδιότητα** ΙΔ και κάθε υποομάδα τής G ανήκουσα στο

$$\textbf{Max-Subg}(G) \cap \{H \in \textbf{Subg}(G) \mid \text{η } H \text{ έχει την ιδιότητα ΙΔ}\} \tag{3.5}$$

καλείται **μεγιστική υποομάδα τής** G **με την ιδιότητα** ΙΔ. Μια $H \in \textbf{Subg}(G)$ ανήκει στο (3.4) εάν και μόνον εάν ικανοποιείται η εξής συνθήκη: *Για οιαδήποτε υποομάδα* $K \in \textbf{Subg}(G)$, *για την οποία ισχύει* $\{e_G\} \sqsubset K \sqsubseteq H$,

$$\textit{είτε } K = H \textit{ είτε η } K \textit{ δεν έχει την ιδιότητα } \text{ΙΔ}.$$

Κατ' αναλογίαν, μια $H \in \textbf{Subg}(G)$ ανήκει στο (3.5) εάν και μόνον εάν ικανοποιείται η εξής συνθήκη: *Για οιαδήποτε* $L \in \textbf{Subg}(G)$, *για την οποία ισχύει* $H \sqsubseteq L \sqsubset G$,

$$\textit{είτε } L = H \textit{ είτε η } L \textit{ δεν έχει την ιδιότητα } \text{ΙΔ}.$$

(iii) Στην περίπτωση όπου το σύνολο (3.4) (και αντιστοίχως, το σύνολο (3.5)) είναι μονοσύνολο, ήτοι περιέχει μία και μόνον υποομάδα, λέμε ότι η εν λόγω υποομάδα είναι **η ελάχιστη μη τετριμμένη** (και αντιστοίχως, **η μέγιστη γνήσια**) **υποομάδα τής** G **με την ιδιότητα** ΙΔ.

3.2.35 Παραδείγματα. (i) Η $(\mathbb{Z}_{12}, +)$ διαθέτει δύο ελαχιστικές υποομάδες (συγκεκριμένα, τις $\{[0]_{12}, [4]_{12}, [8]_{12}\}$ και $\{[0]_{12}, [6]_{12}\}$) και δύο μεγιστικές υποομάδες (τις

$$\{[0]_{12}, [2]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12}\} \text{ και } \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}).$$

Από την άλλη μεριά, για την $(\mathbb{Z}_4, +)$ έχουμε

$$\textbf{Min-Subg}(\mathbb{Z}_4) = \{[0]_4, [2]_4\} = \textbf{Max-Subg}(\mathbb{Z}_4)$$

και για την $(\mathbb{Z}_2, +)$,

$$\textbf{Min-Subg}(\mathbb{Z}_2) = \mathbb{Z}_2 \text{ και } \textbf{Max-Subg}(\mathbb{Z}_2) = \{[0]_2\}(!)$$

(Πρβλ. 3.5.30 (ii) και 3.2.27.) Τα εν λόγω σύνολα υποομάδων για την $(\mathbb{Z}_m, +)$, όπου m *οιοσδήποτε* φυσικός αριθμός $\geqslant 2$, περιγράφονται στο εδάφιο 3.5.29 (ii).

(ii) Είναι προφανές ότι, για πεπερασμένες ομάδες G, αμφότερα τα **Min-Subg**(G) και **Max-Subg**(G) είναι σύνολα μη κενά. Ωστόσο, υπάρχουν άπειρες ομάδες, όπως, π.χ., η $(\mathbb{Z}, +)$ ή η $(\mathbb{Q}, +)$ (ή οποιαδήποτε άλλη άπειρη ομάδα που «στρεϊται στρέψεως», βλ. 3.4.1 (ii)), οι οποίες, παρά το γεγονός ότι έχουν άπειρου πλήθους υποομάδες, δεν διαθέτουν καμία ελαχιστική υποομάδα. Κατ' αναλογίαν, υπάρχουν άπειρες ομάδες, όπως, π.χ., η p^∞*-ομάδα* $(\mathcal{E}_{p^\infty}, \cdot)$ (όπου p τυχών πρώτος αριθμός, βλ. 3.4.6 (ii)) ή η $(\mathbb{Q}, +)$, οι οποίες, παρά το γεγονός ότι έχουν άπειρου πλήθους υποομάδες, δεν διαθέτουν καμία μεγιστική υποομάδα.

(iii) Έστω $(G, \cdot)$ τυχούσα ομάδα με $\text{card}(G) \geqslant 2$. Εάν για μια $H \in \textbf{Subg}(G)$ ως ΙΔ λάβουμε, π.χ., «το να είναι η H αβελιανή», τότε κάθε υποομάδα τής G ανήκουσα στο (3.5), ήτοι κάθε υποομάδα τής G «που δεν περιέχεται γνησίως σε κάποια αβελιανή υποομάδα τής G» ονομάζεται (εν συντομία) *μεγιστική αβελιανή υποομάδα τής* G.

[20] Κάθε ομάδα με αυτήν την ιδιότητα καλείται **μη τετριμμένη ομάδα** (Βλ. εδάφιο 3.5.27.)

[21] Παραδείγματα τέτοιων ιδιοτήτων: Το να είναι μια υποομάδα *πεπερασμένη*, το να είναι *αβελιανή* (βλ. 3.2.1), το να είναι *πεπερασμένως παραγόμενη* (βλ. 3.3.8), το να είναι *κυκλική* (βλ. 3.3.15), το να είναι *περιοδική* (βλ. 3.4.1), το να είναι *ορθόθετη* (βλ. 5.2.2) κ.ά.

3.2.36 Σημείωση. Ενίοτε, επιβάλλεται η (μερική, αλλά σαφώς υποδηλούμενη) «χαλάρωση» των αξιώσεων τού ορισμού 3.2.34. Έτσι, ο όρος «**ελάχιστη** (και αντιστοίχως, **μέγιστη**) **υποομάδα τής** G **με την ιδιότητα** ΙΔ» (*χωρίς την προσθήκη* τού συνοδευτικού «μη τετριμμένη» και, αντιστοίχως, «γνήσια») θα χρησιμοποιείται για να υποδηλοί (όταν είναι γνωστό ότι αυτό υφίσταται) το *ελάχιστο* (και αντιστοίχως, το *μέγιστο*) στοιχείο τού υποσυνόλου *ολοκλήρου τού* **Subg**(G) ως προς την " $\sqsubseteq$ " το οποίο απαρτίζεται από εκείνες τις υποομάδες τής G που έχουν την ιδιότητα ΙΔ. Επί παραδείγματι, στο αμέσως επόμενο εδάφιο 3.3.1 θα ορίσουμε, για οιοδήποτε υποσύνολο $X \subseteq G$, ως $\langle X\rangle$ την ελάχιστη υποομάδα τής G την παραγόμενη από το X, ήτοι το ελάχιστο στοιχείο τού υποσυνόλου τού **Subg**(G) ως προς την " $\sqsubseteq$ " το οποίο απαρτίζεται από εκείνες τις υποομάδες τής G που έχουν την ιδιότητα τού να περιέχουν το X, *χωρίς να αποκλείουμε το ενδεχόμενο* να ισχύει $\langle X\rangle = \{e_G\}$ ή $\langle X\rangle = G$. (Η πρώτη εξ αυτών των ισοτήτων ισχύει εάν και μόνον εάν $X = \varnothing$.) Αυτή η «λεπτή» διαφοροποίηση θα τηρείται απαρεγκλίτως σε ό,τι θα ακολουθήσει σε κατοπινά εδάφια.

3.3 ΥΠΟΟΜΑΔΕΣ ΠΑΡΑΓΟΜΕΝΕΣ ΑΠΟ ΣΥΝΟΛΑ

Μια μέθοδος παραγωγής υποομάδων μιας δεδομένης ομάδας $(G,\cdot)$ είναι αυτή τής θεωρήσεως τυχόντων υποσυνόλων $X \subseteq G$ και τού σχηματισμού τής *τομής* όλων των υποομάδων που τα περιέχουν.

3.3.1 Ορισμός. Για *τυχόν υποσύνολο* X τού υποκειμένου συνόλου G μιας ομάδας $(G,\cdot)$, χαρακτηρίζουμε την τομή[22]

$$\langle X\rangle := \bigcap \{H \in \mathbf{Subg}(G) \mid X \subseteq H\}, \tag{3.6}$$

η οποία είναι η ελάχιστη υποομάδα τής $(G,\cdot)$ που περιέχει το X, ως **την υποομάδα τής** $(G,\cdot)$ **την παραγόμενη από το** X.

3.3.2 Συμβολισμός. (i) Εάν οι H και K είναι δυο υποομάδες μιας ομάδας $(G,\cdot)$, θα συμβολίζουμε εφεξής ως

$$\langle H,K\rangle := \langle H\cup K\rangle = \bigcap \{L \in \mathbf{Subg}(G) \mid H\cup K \subseteq L\} \ (= H \vee K),$$

την υποομάδα της την παραγόμενη από το σύνολο $X = H\cup K$ (η οποία, σύμφωνα με την πρόταση 3.2.30, αποτελεί το ελάχιστο άνω φράγμα $H \vee K$ τού $\{H,K\}$ ως προς την " $\sqsubseteq$ ").

(ii) Γενικότερα, εάν $(H_j)_{j\in J}$ είναι τυχούσα οικογένεια υποομάδων μιας ομάδας $(G,\cdot)$, θα συμβολίζουμε ως

$$\langle\{H_j \mid j \in J\}\rangle := \left\langle \bigcup_{j\in J} H_j \right\rangle$$

την υποομάδα της την παραγόμενη από την ένωση των μελών της. (Πρόκειται για το ελάχιστο άνω φράγμα $\bigvee_{j\in J} H_j$ των μελών της ως προς την " $\sqsubseteq$ ". Βλ. 3.2.31.)

[22] Εάν το X είναι *πεπερασμένο*, ας πούμε $X = \{x_1,\ldots,x_k\}$, τότε (για λόγους οικονομίας) γράφουμε $\langle x_1,\ldots,x_k\rangle$ αντί τού $\langle\{x_1,\ldots,x_k\}\rangle$.

3.3.3 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Εάν $\varnothing \neq X \subseteq G$, τότε η υποομάδα (3.6), για την οποία λέμε ότι έχει το X ως* ***το σύνολο ή το σύστημα γεννητόρων*** *της (ή ως* ***το παράγον υποσύνολό*** *της), ισούται με*[23]

$$\langle X\rangle = \left\{ x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k} \;\middle|\; (x_1,..,x_k)\in X^k \text{ και } \varepsilon_j\in\mathbb{Z},\ \forall j\in\{1,..,k\}, k\in\mathbb{N}\right\}. \quad (3.7)$$

Απόδειξη. Εξ υποθέσεως, το X είναι μη κενό[24]. Το σύνολο

$$H := \left\{ x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k} \;\middle|\; (x_1,\ldots,x_k)\in X^k \text{ και } \varepsilon_j\in\mathbb{Z},\ \forall j\in\{1,..,k\},\ k\in\mathbb{N}\right\}$$

είναι μια υποομάδα τής G. Πράγματι· το H περιέχει (προφανώς) το ουδέτερο στοιχείο τής G και για κάθε ζεύγος $(x_1^{\varepsilon_1}\, x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}, y_1^{\varrho_1}\, y_2^{\varrho_2} \cdots y_\nu^{\varrho_\nu}) \in H\times H$ έχουμε

$$(x_1^{\varepsilon_1}\, x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k})\,(y_1^{\varrho_1}\, y_2^{\varrho_2} \cdots y_\nu^{\varrho_\nu})^{-1} = x_1^{\varepsilon_1}\, x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}\, y_\nu^{-\varrho_\nu} \cdots y_2^{-\varrho_2} y_1^{-\varrho_1} \in H$$

(πρβλ. 3.2.9 (iii) και 3.2.16 (iii)). Επειδή $x = x^1 \in H$ για *κάθε* $x\in X$, λαμβάνουμε $X\subseteq H$. Αρκεί λοιπόν να αποδειχθεί ότι το H είναι η ελάχιστη υποομάδα τής G που περιέχει το X. Προς τούτο υποθέτουμε ότι η B είναι οιαδήποτε υποομάδα τής G για την οποία ισχύει $X\subseteq B$. Τότε, για κάθε στοιχείο $x_1^{\varepsilon_1}\, x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}$ τής H, έχουμε $[x_j\in B \text{ και } \varepsilon_j\in\mathbb{Z},\ \forall j\in\{1,...,k\}] \Longrightarrow [x_j^{\varepsilon_j}\in B,\ \forall j\in\{1,...,k\}]$, οπότε $x_1^{\varepsilon_1}\, x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}\in B$. Επομένως, $H\sqsubseteq B$ και $\langle X\rangle = H$. □

3.3.4 Παρατήρηση. (i) Με ανάλογο τρόπο αποδεικνύεται ότι

$$\langle X\rangle = \left\{ x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k} \;\middle|\; (x_1,..,x_k)\in X^k \text{ και } \varepsilon_j\in\{\pm 1\}, \forall j\in\{1,..,k\}, k\in\mathbb{N}\right\}. \quad (3.8)$$

Ενίοτε, η παράσταση (3.8) τού $\langle X\rangle$ είναι πιο εύχρηστη από την (3.7).

(ii) Για μια διευκολυντική περιγραφή των στοιχείων δοθείσας ομάδας $(G,\cdot)$ (μέσω τής (3.7)) είναι εμφανώς σημαντική η εύρεση παραγόντων συνόλων *τής ίδιας τής* $(G,\cdot)$ (ήτοι υποσυνόλων $X\subseteq G$ με $\langle X\rangle = G$).

3.3.5 Παραδείγματα. (i) Η $(\mathbb{Z},+)$ παράγεται από το σύνολο $X_1 = \{1\}$, καθώς και από το σύνολο $X_2 = \{-1\}$ ή ακόμη και από ολόκληρο το σύνολο $X_3 = \mathbb{N}$.

(ii) Το σύνολα $\left\{ \frac{1}{n} \middle| n\in\mathbb{N}\right\}$ και $\left\{ \frac{1}{n!} \middle| n\in\mathbb{N}\right\}$ αποτελούν παράγοντα σύνολα[25] τής ομάδας $(\mathbb{Q},+)$.

(iii) Το σύνολο $\{-1\}\cup\{p\,|\,p \text{ πρώτος αριθμός}\}$ είναι ένα σύνολο γεννητόρων τής πολλαπλασιαστικής ομάδας $(\mathbb{Q}\setminus\{0\},\cdot)$. (Βλ. 2.3.11 και 2.3.3).

(iv) Η πολλαπλασιαστική ομάδα $(\mathbb{Q}_{>0},\cdot)$ παράγεται τόσον το σύνολο των πρώτων αριθμών όσον και από το σύνολο[26] $\left\{ \frac{1}{p} \middle| p \text{ πρώτος αριθμός}\right\}$.

---

[23] Δίχως βλάβη τής γενικότητας θα μπορούσαμε στις συνθήκες που δίδονται εντός των αγκυλών να αναγράψουμε επιπλέον "$(x_1,\ldots,x_k)\in X^k$ *με* $x_i\neq x_{i+1}$ *για κάθε* $i\in\{1,\ldots,k-1\}$ *όταν* $k\geqslant 2$" (αφού εάν, για $k\geqslant 2$, υπήρχε κάποιος δείκτης $i_0\in\{1,\ldots,k-1\}$ με $x_{i_0}=x_{i_0+1}$, το $x_1^{\varepsilon_1}\cdots x_{i_0}^{\varepsilon_{i_0}} x_{i_0+1}^{\varepsilon_{i_0+1}}\cdots x_k^{\varepsilon_k}$ θα ήταν ίσο με το $x_1^{\varepsilon_1}\cdots x_{i_0}^{\varepsilon_{i_0}+\varepsilon_{i_0+1}}\cdots x_k^{\varepsilon_k}$ που έχει $k-1$ παράγοντες).

[24] Σημειωτέον ότι, εάν $X=\varnothing$, τότε $\langle\varnothing\rangle = \langle\{e_G\}\rangle = \{e_G\}$ είναι η *τετριμμένη* υποομάδα τής G.

[25] Καθε ρητός αριθμός $\frac{a}{b}\in\mathbb{Q}_{>0}$ ($a\in\mathbb{Z}, b\in\mathbb{Z}\setminus\{0\}$) γράφεται ως $\frac{a}{b} = (\mathrm{sign}(b)a)\,\frac{1}{|b|} = (\mathrm{sign}(b)a(|b|-1)!)\,\frac{1}{|b|!}$.

[26] Έστω τυχόν στοιχείο $\frac{a}{b}\in\mathbb{Q}_{>0}$ ($a\in\mathbb{Z}, b\in\mathbb{Z}\setminus\{0\}, ab>0$). Εάν $a=b$, τότε $\frac{a}{b}=1=\left(\frac{1}{p}\right)^0$ για κάθε πρώτο αριθμό p. Εάν $a\neq b$ και $|a|\geqslant 2$, $|b|\geqslant 2$, τότε θεωρώντας τις κανονικές παραστάσεις (2.19) των θετικών ακεραίων $|a| = p_1^{\alpha_1} p_2^{\alpha_2}\cdots p_\kappa^{\alpha_\kappa}$, $\kappa\in\mathbb{N}$, και $|b| = q_1^{\beta_1} q_2^{\beta_2}\cdots q_\lambda^{\beta_\lambda}$, $\lambda\in\mathbb{N}$, ως γινομένων (δυνάμεων) σαφώς διακεκριμένων πρώτων αριθμών, παρατηρούμε ότι $\frac{a}{b} = \frac{|a|}{|b|} = \left(\prod_{i=1}^{\kappa}\left(\frac{1}{p_i}\right)^{-\alpha_i}\right)\left(\prod_{j=1}^{\lambda}\left(\frac{1}{q_j}\right)^{\beta_j}\right)$. (Στην περίπτωση όπου είτε [$|a|=1$ και $|b|\geqslant 2$] είτε [$|a|\geqslant 2$ και $|b|=1$], χρησιμοποιούμε μόνον μία παράσταση αυτού τού είδους.) Άρα $\mathbb{Q}_{>0}\subseteq\left\langle\left\{ \frac{1}{p} \middle| p \text{ πρώτος αριθμός}\right\}\right\rangle$. Ο αντίστροφος εγκλεισμός είναι προφανής.

3.3.6 Πόρισμα. *Εάν $(H_j)_{j\in J}$ είναι μια οικογένεια υποομάδων μιας ομάδας $(G,\cdot)$, τότε*

$$\langle\{\,H_j\,|\,j\in J\}\rangle=\left\{g\in G\;\middle|\;\begin{array}{c}g=h_{j_1}h_{j_2}\cdots h_{j_k},\text{όπου}\\ h_{j_\rho}\in H_{j_\rho},\ \forall\rho\in\{1,...,k\},\ k\in\mathbb{N}\end{array}\right\}.$$

Απόδειξη. Έστω K το σύνολο τού δεξιού μέλους τής αποδεικτέας ισότητας. Το K αποτελεί μια υποομάδα τής G. Πράγματι· το K περιέχει (προφανώς) το ουδέτερο στοιχείο τής G και για κάθε ζεύγος $\left(h_{j_1}h_{j_2}\cdots h_{j_k},h'_{l_1}h'_{l_2}\cdots h'_{l_\nu}\right)\in K\times K$ (όπου $k,\nu\in\mathbb{N}$) έχουμε

$$\left(h_{j_1}h_{j_2}\cdots h_{j_k}\right)\left(h'_{l_1}h'_{l_2}\cdots h'_{l_\nu}\right)^{-1}=h_{j_1}h_{j_2}\cdots h_{j_k}h'^{-1}_{l_\nu}\cdots h'^{-1}_{l_2}h'^{-1}_{l_1}\in K$$

(πρβλ. 3.2.9 (iii) και 3.2.16 (iii)). Επειδή[27] $h\in K$ για *κάθε* $h\in\bigcup_{j\in J}H_j$, λαμβάνουμε $\bigcup_{j\in J}H_j\subseteq K$. Αρκεί λοιπόν να αποδειχθεί ότι η K είναι η ελάχιστη υποομάδα τής G που περιέχει την ένωση $\bigcup_{j\in J}H_j$. Προς τούτο υποθέτουμε ότι η B είναι οιαδήποτε υποομάδα τής G με $\bigcup_{j\in J}H_j\subseteq B$. Για κάθε στοιχείο $h_{j_1}h_{j_2}\cdots h_{j_k}\in K$, έχουμε

$$[h_{j_\rho}\in H_{j_\rho},\ \forall\rho\in\{1,...,k\}]\Longrightarrow[h_{j_\rho}\in B,\ \forall\rho\in\{1,...,k\}],$$

οπότε $h_{j_1}h_{j_2}\cdots h_{j_k}\in B$. Άρα $K\sqsubseteq B$ και $\langle\{\,H_j\,|\,j\in J\}\rangle=K$. □

3.3.7 Σημείωση. Επειδή μια ομάδα μπορεί να παράγεται από διάφορα υποσύνολα τού υποκειμένου συνόλου της, γίνεται αντιληπτό ότι η περιγραφή (3.7) καθίσταται αρκούντως βοηθητική μόνον όταν κανείς περιορίζεται στη θεώρηση εκείνων που έχουν τον *μικρότερο δυνατό* πληθικό αριθμό[28]. Ωστόσο, θα πρέπει να επισημανθεί ότι τα προβλήματα τα σχετιζόμενα με τον ακριβή προσδιορισμό «μικρών» συνόλων γεννητόρων *τυχούσας* ομάδας (ακόμη και όταν απ' αυτά τα σύνολα απαιτείται να πληρούν ορισμένες επιπρόσθετες συνθήκες) είναι άλλοτε δυσεπίλυτα και άλλοτε (αλγοριθμικώς) μη επιλύσιμα. Από την άλλη μεριά, υφίστανται *ειδικές* ομάδες, με προδιαγεγραμμένο πλήθος γεννητόρων, η μελέτη των οποίων είναι εφικτή μέσω στοιχειωδών τεχνικών εργαλείων.

3.3.8 Ορισμός. Μια ομάδα καλείται **πεπερασμένως παραγόμενη** όταν διαθέτει ένα πεπερασμένο σύνολο γεννητόρων.

3.3.9 Παράδειγμα (Ομάδα των ακεραίων τού Gauss). Θεωρούμε *το σύνολο των ακεραίων τού Gauss*

$$\boxed{\mathbb{Z}[i]:=\{a+bi\,|\,a,b\in\mathbb{Z}\}\subsetneq\mathbb{C},}$$

όπου i η φανταστική μονάδα. Μέσω τού 3.2.16 (iii) αποδεικνύεται εύκολα ότι το $\mathbb{Z}[i]$ (εφοδιασμένο με τη συνήθη *πρόσθεση* μιγαδικών αριθμών) αποτελεί μια άπειρη

[27] Εάν $h\in\bigcup_{j\in J}H_j$, τότε $\exists j\in J:h\in H_j$, οπότε $h\in K$ (λόγω τού ορισμού τού K).

[28] Ακόμη και για μια *πεπερασμένη* ομάδα G (με $|G|\geqslant 2$) τα γνωστά ή πιθανά άνω φράγματα τού αριθμού

$$\min.\mathrm{gen}(G):=\min\{\,\mathrm{card}(X)\,|\,X\in\mathfrak{P}(G)\smallsetminus\{\varnothing\}:\langle X\rangle=G\}$$

εξαρτώνται από την εσώτερη δόμηση τής G και, ως εκ τούτου, από προβλήματα ταξινομήσεων. Επίσης, η απεικόνιση $G\mapsto\min.\mathrm{gen}(G)$ δεν επιδεικνύει «καλή συμπεριφορά» ως προς τις υποομάδες των ομάδων αναφοράς. (Επί παραδείγματι, όπως θα δούμε στο (iii) τού πορίσματος 4.2.13, για τη συμμετρική ομάδα $\mathfrak{S}_n$, $n\geqslant 3$, έχουμε $\min.\mathrm{gen}(\mathfrak{S}_n)=2$. Όμως για την υποομάδα της $H:=\langle[1\ 2],[3\ 4],\ldots,[2i-1\ 2i],\ldots\rangle$ ισχύει $\min.\mathrm{gen}(H)=\left\lfloor\frac{n}{2}\right\rfloor$.) Για διάφορες ιδιότητες τού $\min.\mathrm{gen}(G)$ βλ.

A. Lucchini: *A bound on the number of generators of a finite group*, Arch. Math. **53** (1989) 313-317.

A. Lucchini: *Some questions on the number of generators of a finite group*, Rend. Mat. Un.Padova **83** (1990), 201-222.

A. Lucchini: *A bound on the presentation rank of a finite group*, Bull. London Math. Soc. **29** (1997), 389-394.

F. Menegazzo: *The Number of Generators of a Finite Group*, Irish Math. Soc. Bulletin **50** (2003), 117-128.

γνήσια υποομάδα τής αβελιανής ομάδας $(\mathbb{C},+)$. Η $(\mathbb{Z}[i],+)$ είναι πεπερασμένως παραγόμενη, καθότι $\mathbb{Z}[i]=\langle 1,i\rangle$, και καλείται, ιδιαιτέρως, **ομάδα των ακεραίων τού Gauss**.

3.3.10 Παράδειγμα. Η άπειρη γνήσια υποομάδα

$$H:=\left\{\begin{pmatrix} a & b\\ 0 & 1\end{pmatrix}\middle| a\in\{\pm 1\}, b\in\mathbb{Z}\right\}$$

τής $(\mathrm{SL}_2(\mathbb{Z}),\cdot)$ είναι μη αβελιανή, διότι π.χ.

$$\begin{pmatrix} 1 & 2\\ 0 & 1\end{pmatrix}\begin{pmatrix} -1 & 3\\ 0 & 1\end{pmatrix}=\begin{pmatrix} -1 & 5\\ 0 & 1\end{pmatrix}\neq\begin{pmatrix} -1 & 1\\ 0 & 1\end{pmatrix}=\begin{pmatrix} -1 & 3\\ 0 & 1\end{pmatrix}\begin{pmatrix} 1 & 2\\ 0 & 1\end{pmatrix},$$

και πεπερασμένως παραγόμενη. Πράγματι· κάθε στοιχείο της γράφεται υπό τη μορφή

$$\begin{pmatrix} a & b\\ 0 & 1\end{pmatrix}=\begin{pmatrix} 1 & b\\ 0 & 1\end{pmatrix}\begin{pmatrix} a & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}^b\begin{pmatrix} a & 0\\ 0 & 1\end{pmatrix}$$

και επειδή $a\in\{\pm 1\}$, έχουμε

$$H=\left\langle\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix},\begin{pmatrix} -1 & 0\\ 0 & 1\end{pmatrix}\right\rangle.$$

3.3.11 Παράδειγμα (Ομάδα τετρανίων). Εάν θέσουμε

$$\mathbf{i}:=\begin{pmatrix} 0 & i\\ i & 0\end{pmatrix},\quad \mathbf{j}:=\begin{pmatrix} i & 0\\ 0 & -i\end{pmatrix},\quad \mathbf{k}:=\begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix},$$

όπου i η φανταστική μονάδα, τότε η υποομάδα

$$\boxed{\mathbf{Q}:=\langle\mathbf{j},\mathbf{k}\rangle\sqsubset \mathrm{SU}_2(\mathbb{C}),}$$

η παραγόμενη από τους πίνακες $\mathbf{j}$ και $\mathbf{k}$, καλείται **ομάδα των τετρανίων**. Έστω τυχόν $g\in\mathbf{Q}$. Εάν αυτό γράφεται υπό τη μορφή $g=\mathbf{j}^{\varepsilon_1}\mathbf{k}^{\varepsilon_2}$, για κάποιους $\varepsilon_1,\varepsilon_2\in\mathbb{Z}$, και διαιρέσουμε τους $\varepsilon_1,\varepsilon_2$ διά 4, λαμβάνουμε $\varepsilon_1=4q_1+r_1$, $\varepsilon_2=4q_2+r_2$, για κάποια μονοσημάντως ορισμένα ζεύγη $(q_1,r_1),(q_2,r_2)\in\mathbb{Z}\times\mathbb{Z}$, όπου τα r_1,r_2 είναι στοιχεία τού συνόλου $\{0,1,2,3\}$. (Βλ. 2.1.6). Επειδή $\mathbf{j}^4=\mathbf{k}^4=\mathbf{I}_2\,(=e_{\mathbf{Q}})$ και

$$\mathbf{j}^2=\mathbf{k}^2=\mathbf{i}^2=-\mathbf{I}_2,\ \mathbf{j}^3=-\mathbf{j},\ \mathbf{k}^3=-\mathbf{k},\ \mathbf{jk}=\ \mathbf{i},\ \mathbf{kj}=-\mathbf{jk}=-\mathbf{i},$$

έχουμε $g=\mathbf{j}^{\varepsilon_1}\mathbf{k}^{\varepsilon_2}=((\mathbf{j}^4)^{q_1}\mathbf{j}^{r_1})((\mathbf{k}^4)^{q_2}\mathbf{k}^{r_2})=\mathbf{j}^{r_1}\mathbf{k}^{r_2}$, όπου

g	όταν το (r_1,r_2) είναι το
$\mathbf{I}_2$	$(0,0)$ ή το $(2,2)$
$-\mathbf{I}_2$	$(0,2)$ ή το $(2,0)$
$\mathbf{i}$	$(1,1)$ ή το $(3,3)$
$-\mathbf{i}$	$(1,3)$ ή το $(3,1)$

g	όταν το (r_1,r_2) είναι το
$\mathbf{j}$	$(1,0)$ ή το $(3,2)$
$-\mathbf{j}$	$(1,2)$ ή το $(3,0)$
$\mathbf{k}$	$(0,1)$ ή το $(2,3)$
$-\mathbf{k}$	$(0,3)$ ή το $(2,1)$

Αλλά ακόμη και εάν το στοιχείο g γράφεται υπό τη μορφή $g=\mathbf{k}^{\varepsilon_1}\mathbf{j}^{\varepsilon_2}$, για κάποιους $\varepsilon_1,\varepsilon_2\in\mathbb{Z}$, οφείλει (παρομοίως, λόγω των σχέσεων των γεννητόρων) να συμπεριλαμβάνεται στον κατάλογο των προαναφερθέντων 8 στοιχείων. Επομένως, η

$$\boxed{\mathbf{Q}=\{\mathbf{I}_2,-\mathbf{I}_2,\mathbf{i},-\mathbf{i},\mathbf{j},-\mathbf{j},\mathbf{k},-\mathbf{k}\}}$$

έχει τάξη 8, *δεν είναι αβελιανή* (αφού $\mathbf{kj}\neq\mathbf{jk}$) και ο πολλαπλασιαστικός της κατάλογος (όπου $\mathbf{I}:=\mathbf{I}_2$) είναι ο εξής:

$\cdot$	$\mathbf{I}$	$-\mathbf{I}$	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{j}$	$-\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$
$\mathbf{I}$	$\mathbf{I}$	$-\mathbf{I}$	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{j}$	$-\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$
$-\mathbf{I}$	$-\mathbf{I}$	$\mathbf{I}$	$-\mathbf{i}$	$\mathbf{i}$	$-\mathbf{j}$	$\mathbf{j}$	$-\mathbf{k}$	$\mathbf{k}$
$\mathbf{i}$	$\mathbf{i}$	$-\mathbf{i}$	$-\mathbf{I}$	$\mathbf{I}$	$\mathbf{k}$	$-\mathbf{k}$	$-\mathbf{j}$	$\mathbf{j}$
$-\mathbf{i}$	$-\mathbf{i}$	$\mathbf{i}$	$\mathbf{I}$	$-\mathbf{I}$	$-\mathbf{k}$	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{j}$
$\mathbf{j}$	$\mathbf{j}$	$-\mathbf{j}$	$-\mathbf{k}$	$\mathbf{k}$	$-\mathbf{I}$	$\mathbf{I}$	$\mathbf{i}$	$-\mathbf{i}$
$-\mathbf{j}$	$-\mathbf{j}$	$\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$	$\mathbf{I}$	$-\mathbf{I}$	$-\mathbf{i}$	$\mathbf{i}$
$\mathbf{k}$	$\mathbf{k}$	$-\mathbf{k}$	$\mathbf{j}$	$-\mathbf{j}$	$-\mathbf{i}$	$\mathbf{i}$	$-\mathbf{I}$	$\mathbf{I}$
$-\mathbf{k}$	$-\mathbf{k}$	$\mathbf{k}$	$-\mathbf{j}$	$\mathbf{j}$	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{I}$	$-\mathbf{I}$

(Σημειωτέον ότι $\mathbf{i}^{-1} = -\mathbf{i}$, $\mathbf{j}^{-1} = -\mathbf{j}$, $\mathbf{k}^{-1} = -\mathbf{k}$.)

3.3.12 Σημείωση. (i) Κάθε πεπερασμένη ομάδα είναι προδήλως πεπερασμένως παραγόμενη.

(ii) Το υποκείμενο σύνολο οιασδήποτε πεπερασμένως παραγόμενης ομάδας είναι το πολύ αριθμήσιμο[29]. Κατά συνέπειαν, κάθε ομάδα $(G, \cdot)$ με $|G| > \aleph_0$ (ήτοι με υπεραριθμήσιμο υποκείμενο σύνολο G) είναι *μη πεπερασμένως παραγόμενη*. Αλλά ακόμη και όταν $|G| = \aleph_0$, η $(G, \cdot)$ δεν είναι κατ' ανάγκην πεπερασμένως παραγόμενη, όπως δείχνει το παράδειγμα που ακολουθεί.

3.3.13 Παράδειγμα. Η $(\mathbb{Q}, +)$ *δεν είναι* πεπερασμένως παραγόμενη, καθότι οι υποομάδες οι παραγόμενες από πεπερασμένα υποσύνολα τού $\mathbb{Q}\setminus\{0\}$ είναι *γνήσιες* υποομάδες τής $(\mathbb{Q}, +)$. Πράγματι· εάν υποθέταμε ότι

$$\mathbb{Q} = \langle q_1, ..., q_k\rangle = \{\, n_1q_1 + \cdots + n_kq_k |\, n_1, ..., n_k \in \mathbb{Z}\}\,,\ k \in \mathbb{N},$$

όπου $q_i = \frac{a_i}{b_i}$, $a_i, b_i \in \mathbb{Z}\setminus\{0\}$, για κάθε $i \in \{1, ..., k\}$, τότε κάθε ρητός αριθμός s θα όφειλε να γράφεται υπό τη μορφή

$$s = n_1\tfrac{a_1}{b_1} + \cdots + n_k\tfrac{a_k}{b_k} = \frac{\sum\limits_{i=1}^{k} n_ia_i\left(\prod\limits_{j\in\{1,\ldots,k\}\setminus\{i\}} b_j\right)}{b_1\cdots b_k}$$

για κάποιους $n_1, ..., n_k \in \mathbb{Z}$. Π.χ., θέτοντας

$$c_i := a_i\left(\prod_{j\in\{1,\ldots,k\}\setminus\{i\}} b_j\right)$$

για κάθε $i \in \{1, ..., k\}$, για τον $s := \frac{1}{2b_1\cdots b_k}$ θα ίσχυε

$$\tfrac{1}{2b_1\cdots b_k} = \tfrac{\sum_{i=1}^{k} n_ic_i}{b_1\cdots b_k} \Rightarrow 2\left(\sum_{i=1}^{k} n_ic_i\right) = 1, \tag{3.9}$$

πράγμα άτοπο, καθότι *δεν υφίστανται* $n_1, ..., n_k \in \mathbb{Z}$ ικανοποιούντες την εξίσωση (3.9). (Το αριστερό μέλος τής (3.9) είναι ένας άρτιος και το δεξιό της ένας περιττός ακέραιος αριθμός.)

3.3.14 Σημείωση. Υπάρχουν *υποομάδες* απείρων αλλά πεπερασμένως παραγομένων ομάδων *που δεν είναι πεπερασμένως παραγόμενες*. (Βλ. άσκηση 19 τού φυλλαδίου 6.)

3.3.15 Ορισμός. Μια ομάδα καλείται **κυκλική** (ή **μονογενής**) όταν μπορεί να παραχθεί (υπό την έννοια τού 3.3.1) από ένα *μονοσύνολο*[30]. (Για *κάθε* ομάδα G εισάγουμε τον συμβολισμό $\mathbf{CSubg}(G) := \{\, H \in \mathbf{Subg}(G) |\, H$ κυκλική$\}$.)

3.3.16 Παραδείγματα. (i) Η $(\mathbb{Z}, +)$ (όπως προαναφέραμε στο 3.3.5 (i)) είναι κυκλική. Το ίδιο ισχύει και για την $(n\mathbb{Z}, +)$, για οιονδήποτε $n \in \mathbb{Z}$.

(ii) Η ομάδα $(\mathbb{Z}_m, +)$, $m \in \mathbb{N}$, είναι κυκλική, αφού παράγεται από την κλάση ισοτιμίας $[1]_m$.

(iii) Το σύνολο $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$ *των ακεραίων τού Gauss* (βλ. 3.3.9), εφοδιαζόμενο με τον συνήθη *πολλαπλασιασμό* μιγαδικών αριθμών, καθίσταται αβελιανό μονοειδές. Μέσω τού $(\mathbb{Z}[i], \cdot)$ δημιουργείται η πολλαπλασιαστική ομάδα που

[29] Εάν $(G, \cdot)$ είναι μια ομάδα με $G = \langle X\rangle$, όπου $X = \{g_1, ..., g_n\}$, $n \in \mathbb{N}$, και $X^{-1} := \{g_1^{-1}, ..., g_n^{-1}\}$, $Y := X \cup X^{-1}$, τότε $\mathrm{card}(Y) \leqslant 2n$ και κάθε στοιχείο τής G γράφεται (λόγω τής (3.8)) υπό τη μορφή $y_1y_2\cdots y_k$, όπου $(y_1, ..., y_k) \in Y^k$ για κάποιον $k \in \mathbb{N}$, οπότε $|G| \leqslant \mathrm{card}(\bigcup_{k\in\mathbb{N}} Y^k) \leqslant \aleph_0$, διότι η ένωση μιας αριθμήσιμης οικογενείας πεπερασμένων συνόλων είναι το πολύ αριθμήσιμη.

[30] Όταν από τούδε και στο εξής θα αναφερόμαστε σε κάποιον *γεννήτορα μιας κυκλικής ομάδας* G θα εννοούμε ένα στοιχείο $g \in G$, τέτοιο ώστε να ισχύει $G = \langle g\rangle$.

έχει ως υποκείμενο σύνολό της το $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ (βλ. πρόταση 3.2.6). Η $(\mathbb{Z}[i]^\times, \cdot)$ είναι κυκλική, διότι[31] $\mathbb{Z}[i]^\times = \langle i \rangle = \langle -i \rangle$.

(iv) Η ομάδα $(\mathcal{E}_n, \cdot)$, $n \in \mathbb{N}$, των n-οστών ριζών τής μονάδας (βλ. 3.2.21 (vi)) είναι κυκλική, διότι $\mathcal{E}_n = \langle \zeta_n \rangle$, όπου $\zeta_n := \exp\left(\frac{2\pi i}{n}\right)$. Σημειωτέον ότι $\mathcal{E}_4 = \mathbb{Z}[i]^\times$.

(v) Η $(\mathbb{Q}, +)$ (ως μη πεπερασμένως παραγόμενη, βλ. 3.3.13) δεν είναι κυκλική.

(vi) Η $(\mathbb{R}, +)$ δεν είναι κυκλική. Πράγματι· εάν η $(\mathbb{R}, +)$ παρήγετο από κάποιον $r \in \mathbb{R} \setminus \{0\}$, τότε το $1 \in \mathbb{R}$ θα όφειλε να γράφεται υπό τη μορφή $1 = nr$, για κάποιον $n \in \mathbb{Z} \setminus \{0\}$. Το ίδιο θα ίσχυε και για τον άρρητο αριθμό $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$, δηλαδή θα υπήρχε κάποιος $m \in \mathbb{Z} \setminus \{0\}$ με $\sqrt{2} = mr$, πράγμα άτοπο, καθότι $mr = \frac{m}{n} \in \mathbb{Q}$. (Εναλλακτικώς, η $(\mathbb{R}, +)$ δεν είναι κυκλική, διότι δεν είναι ούτε καν πεπερασμένως παραγόμενη, αφού $|\mathbb{R}| = \mathfrak{c} > \aleph_0$, βλ. 3.3.12 (ii).)

3.3.17 Πρόταση. *Κάθε κυκλική ομάδα είναι αβελιανή.*

Απόδειξη. Έστω $(G, \cdot)$ μια ομάδα. Εάν $G = \langle g \rangle$ (για κάποιο $g \in G$), και εάν $x, y \in G$, τότε $x = g^m$ και $y = g^n$, για κάποιους ακεραίους αριθμούς m και n. Ως εκ τούτου, βάσει τού (i) τής προτάσεως 3.2.11 λαμβάνουμε

$$xy = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = yx,$$

οπότε η G είναι όντως αβελιανή. □

3.3.18 Πρόταση. *Έστω $(G, \cdot)$ μια ομάδα και έστω $g \in G$. Τότε για την κυκλική ομάδα $\langle g \rangle$ που παράγεται από το g υπάρχουν δύο ενδεχόμενα: είτε όλες οι «δυνάμεις» $g^n, n = 0, \pm 1, \pm 2, \ldots$ είναι σαφώς διακεκριμένες, είτε υπάρχουν ακέραιοι n, m, με $n > m$, τέτοιοι ώστε $g^n = g^m$, ήτοι $g^{n-m} = e_G$. Στην πρώτη περίπτωση η $\langle g \rangle$ έχει άπειρη τάξη (και λέγεται **άπειρη κυκλική ομάδα**). Στη δεύτερη περίπτωση,*

$$\langle g \rangle = \left\{ e_G, g, g^2, \ldots, g^{l-1} \right\},$$

όπου $l := \min\{ k \in \mathbb{N} \mid g^k = e_G \}$.

Απόδειξη. Αρκεί να δείξουμε το ότι ο ισχυρισμός στη δεύτερη περίπτωση είναι αληθής. Κατ' αρχάς, επειδή $\exists (n, m) \in \mathbb{Z} \times \mathbb{Z}, n > m$, με $g^{n-m} = e_G$, το σύνολο $\{ k \in \mathbb{N} \mid g^k = e_G \}$ είναι μη κενό. Έστω τώρα g^ν, $\nu \in \mathbb{N}$, ένα τυχόν στοιχείο τής $\langle g \rangle$. Δυνάμει τής ταυτότητας τής ευκλείδειας διαιρέσεως υπάρχουν μοναδικοί ακέραιοι q, r με $0 \leqslant r < l$, τέτοιοι ώστε να ισχύει $\nu = ql + r$ (βλ. 2.1.6). Κατά συνέπειαν, $g^\nu = g^{ql+r} = g^{ql} g^r = g^{lq} g^r = \left(g^l\right)^q g^r = e_G^q g^r = e_G g^r = g^r$. Απομένει λοιπόν να αποδειχθεί ότι τα στοιχεία $e_G, g, g^2, \ldots, g^{l-1}$ είναι σαφώς διακεκριμένα. Εάν υποτεθεί ότι υπάρχουν $\mu, \nu \in \{0, 1, \ldots, l-1\}$, για τους οποίους ισχύει $\mu > \nu$ και $g^\mu = g^\nu$, τότε $g^{\mu-\nu} = e_G$, $1 \leqslant \mu - \nu \leqslant l - 1$, πράγμα που αντίκειται στην επιλογή τού l ως τής ελαχίστης δυνάμεως με αυτήν την ιδιότητα. □

3.3.19 Πρόταση. (i) *Κάθε υποομάδα τής $(\mathbb{Z}, +)$ είναι κυκλική, και μάλιστα τής μορφής $(d\,\mathbb{Z}, +)$, για κάποιον $d \in \mathbb{N}_0$.*

(ii) *Κάθε υποομάδα μιας κυκλικής ομάδας είναι κυκλική.*

Απόδειξη. (i) Έστω H μια υποομάδα τής ομάδας $(\mathbb{Z}, +)$. Εάν η H είναι η τετριμμένη, τότε είναι προφανώς κυκλική. Εάν η H δεν είναι τετριμμένη, τότε περιέχει έναν ακέραιο k διάφορο τού μηδενός και, επειδή η H είναι μια υποομάδα, θα έχουμε και $-k \in H$. Άρα η H περιέχει υποχρεωτικώς έναν θετικό ακέραιο. Έστω d ο

[31] Προφανώς, για κάθε $k \in \mathbb{Z}$ έχουμε $i^{4k} = 1$, $i^{4k+1} = i$, $i^{4k+2} = -1$ και $i^{4k+3} = -i$, οπότε ισχύουν οι ισότητες $\mathbb{Z}[i]^\times = \{ i^n \mid n \in \mathbb{Z} \} = \langle i \rangle$. Παρομοίως αποδεικνύεται ότι $\mathbb{Z}[i]^\times = \langle -i \rangle$.

ελάχιστος θετικός ακέραιος εντός τής H. Ισχυριζόμαστε ότι ο d παράγει την H. Εάν $n \in H$, διαιρούμε τον n διά τού d και λαμβάνουμε $n = qd + r$, όπου οι q και r είναι ακέραιοι και $0 \leqslant r < d$, ήτοι $n \equiv r \pmod d$ (βλ. 2.1.6). Γνωρίζουμε ότι $n \in H$ και $d \in H$. Επειδή η H είναι μια υποομάδα τής $(\mathbb{Z}, +)$, έχουμε $qd \in H$, οπότε $-qd \in H$, απ' όπου συμπεραίνουμε ότι $r = n - qd = n + (-qd) \in H$. Αυτό όμως αντιφάσκει προς την επιλογή τού d, εκτός και εάν ο r ισούται με μηδέν. Κατά συνέπειαν, έχουμε $n = qd$, πράγμα το οποίο μας δείχνει ότι κάθε στοιχείο τής H είναι ένα ακέραιο πολλαπλάσιο τού d, ήτοι ότι $H = \langle d \rangle = d\,\mathbb{Z}$.

(ii) Έστω $(G, \cdot)$ μια κυκλική ομάδα και έστω K μια μη τετριμμένη υποομάδα τής G. Εάν ο g είναι ένας γεννήτορας τής G, τότε κάθε στοιχείο τής G, και επομένως και κάθε στοιχείο τής K, είναι μια δύναμη τού g. Έστω $H := \{n \in \mathbb{Z} \mid g^n \in K\}$. Είναι εύκολο να διαπιστώσουμε ότι το σύνολο H είναι μια υποομάδα τής ομάδας $(\mathbb{Z}, +)$. Κατά το (i) η H είναι κυκλική. Εάν ο d παράγει την H, τότε η δύναμη g^d παράγει την K. Τούτο ολοκληρώνει την απόδειξή μας[32]. □

3.3.20 Πόρισμα. *Εάν $m, n \in \mathbb{N}_0$, τότε για τις υποομάδες $(m\mathbb{Z}, +)$ και $(n\,\mathbb{Z}, +)$ τής $(\mathbb{Z}, +)$ ισχύουν τα εξής:*
(i) $m\mathbb{Z} \sqsupseteq n\mathbb{Z} \iff m \mid n$.
(ii) $m\mathbb{Z} = n\mathbb{Z} \iff m = n$.
(iii) $m\mathbb{Z} \cap n\mathbb{Z} = \text{εκπ}(m, n)\mathbb{Z}$.
(iv) $\langle m\mathbb{Z}, n\mathbb{Z} \rangle = \text{μκδ}(m, n)\mathbb{Z}$.

Απόδειξη. Επειδή τα ανωτέρω είναι προφανή όταν τουλάχιστον ένας εκ των m, n είναι $= 0$, θα υποθέσουμε εφεξής ότι $m, n \in \mathbb{N}$.

(i) Εν πρώτοις θα αποδείξουμε ότι $m\mathbb{Z} \supseteq n\mathbb{Z} \iff m \mid n$. Εάν $m\mathbb{Z} \supseteq n\mathbb{Z}$, τότε $n = n \cdot 1 \in m\mathbb{Z}$, οπότε $\exists s \in \mathbb{Z} : n = ms$. (Μάλιστα, επειδή $m, n \in \mathbb{N}$, έχουμε κατ' ανάγκην $s \in \mathbb{N}$.) Άρα $m \mid n$. Και αντιστρόφως· εάν $m \mid n$, τότε $\exists t \in \mathbb{N} : n = mt$. Έστω x τυχόν στοιχείο τής $n\mathbb{Z}$. Τότε $\exists a \in \mathbb{Z} : x = na = m(ta) \Rightarrow x \in m\mathbb{Z}$. Άρα έχουμε $m\mathbb{Z} \supseteq n\mathbb{Z}$. Εν συνεχεία θα αποδείξουμε ότι $m\mathbb{Z} \sqsupseteq n\mathbb{Z} \iff m \mid n$. Προφανώς ισχύει $m\mathbb{Z} \sqsupseteq n\mathbb{Z} \Rightarrow m\mathbb{Z} \supseteq n\mathbb{Z} \Rightarrow m \mid n$ (από ό,τι προείπαμε). Και αντιστρόφως· εάν $m \mid n$, τότε

$$\left.\begin{array}{r} m\mathbb{Z} \supseteq n\mathbb{Z} \text{ (από ό,τι προείπαμε)} \\ \mathbb{Z} \sqsupseteq m\mathbb{Z} \text{ (βλ. 3.2.21 (iii))} \end{array}\right\} \underset{3.2.20}{\Longrightarrow} m\mathbb{Z} \sqsupseteq n\mathbb{Z}.$$

(ii) Τούτο έπεται από το (i), καθώς έχουμε $m\mathbb{Z} = n\mathbb{Z} \Leftrightarrow m \mid n$ και $n \mid m \Leftrightarrow m = n$.

(iii) Σύμφωνα με το (i) τής προτάσεως 3.3.19 $\exists k \in \mathbb{N} : m\mathbb{Z} \cap n\mathbb{Z} = k\mathbb{Z}$. Επειδή

$$k\mathbb{Z} \sqsubseteq m\mathbb{Z} \text{ και } k\mathbb{Z} \sqsubseteq n\mathbb{Z} \Rightarrow m \mid k \text{ και } n \mid k,$$

ο k είναι κοινό πολλαπλάσιο των m και n. Επιπροσθέτως, για *οιοδήποτε κοινό πολλαπλάσιο* $l \in \mathbb{Z}$ των m και n έχουμε $m \mid |l|$ και $n \mid |l| \Rightarrow |l|\,\mathbb{Z} \sqsubseteq m\mathbb{Z}$ και $|l|\,\mathbb{Z} \sqsubseteq n\mathbb{Z}$, οπότε $|l|\,\mathbb{Z} \sqsubseteq m\mathbb{Z} \cap n\mathbb{Z} = k\mathbb{Z} \Rightarrow k \mid |l| \underset{2.1.5\,\text{(i)}}{\Longrightarrow} k \mid l \underset{2.2.25}{\Longrightarrow} k = \text{εκπ}\,(m, n)$.

(iv) Σύμφωνα με το (i) τής προτάσεως 3.3.19, $\exists \kappa \in \mathbb{N} : \langle m\mathbb{Z}, n\mathbb{Z} \rangle = \kappa\mathbb{Z}$. Επειδή

$$m\mathbb{Z} \sqsubseteq \kappa\mathbb{Z} \text{ και } n\mathbb{Z} \sqsubseteq \kappa\mathbb{Z} \Rightarrow \kappa \mid m \text{ και } \kappa \mid n,$$

ο κ είναι κοινός διαιρέτης των m και n. Επιπροσθέτως, για *οιονδήποτε κοινό διαιρέτη* $\lambda \in \mathbb{Z}$ των m και n έχουμε $|\lambda| \mid m$ και $|\lambda| \mid n \Rightarrow m\mathbb{Z} \sqsubseteq |\lambda|\,\mathbb{Z}$ και $n\mathbb{Z} \sqsubseteq |\lambda|\,\mathbb{Z}$.

[32] Ιδιαιτέρως, $\mathbf{Subg}(G) = \mathbf{CSubg}(G)$ για κάθε κυκλική ομάδα G.

Επειδή η $\langle m\mathbb{Z}, n\mathbb{Z}\rangle$ είναι η ελάχιστη υποομάδα τής $(\mathbb{Z}, +)$ που περιέχει αμφότερες τις $m\mathbb{Z}$ και $n\mathbb{Z}$, λαμβάνουμε

$$\kappa\mathbb{Z} = \langle m\mathbb{Z}, n\mathbb{Z}\rangle \sqsubseteq |\lambda|\,\mathbb{Z} \Rightarrow |\lambda| \mid \kappa \underset{\text{2.1.5 (i)}}{\Longrightarrow} \lambda \mid \kappa \underset{\text{2.2.6}}{\Longrightarrow} \kappa = \mu\kappa\delta\,(m, n)\,,$$

και η απόδειξη λήγει εδώ. □

3.4 ΤΑΞΗ ΣΤΟΙΧΕΙΟΥ ΜΙΑΣ ΟΜΑΔΑΣ

3.4.1 Ορισμός. Έστω $(G, \cdot)$ μια ομάδα. Η **τάξη** $\mathrm{ord}(g) \in \mathbb{N} \cup \{\infty\}$ **ενός στοιχείου** $g \in G$ ορίζεται ως εξής:

$$\mathrm{ord}(g) := \begin{cases} \infty, & \text{όταν } g^k \neq e_G,\ \forall k \in \mathbb{N}, \\ \min\{\, k \in \mathbb{N} \mid\ g^k = e_G\}, & \text{στην αντίθετη περίπτωση.} \end{cases}$$

Όταν $\mathrm{ord}(g) = \infty$, τότε λέμε ότι το g **έχει άπειρη τάξη**. (Ειδάλλως, λέμε ότι έχει **πεπερασμένη τάξη**). Το σύνολο

$$\mathrm{tors}(G) := \big\{ g \in G \,\big|\, g^k = e_G,\ \text{για κάποιον } k \in \mathbb{N} \big\}$$

το αποτελούμενο από όλα τα στοιχεία τής G που έχουν πεπερασμένη τάξη καλείται **σύνολο στρέψεως**[33] τής G. Όταν $\mathrm{tors}(G) = G$, τότε λέμε ότι η G είναι **περιοδική ομάδα** (ή **ομάδα στρέψεως**). Όταν η ίδια η G είναι μια *πεπερασμένη* ομάδα, τότε η G είναι περιοδική. Όταν η G είναι μια *άπειρη* ομάδα, υπάρχουν τρία ενδεχόμενα:

(i) Η G είναι περιοδική.

(ii) $\mathrm{tors}(G) = \{e_G\}$, δηλαδή όλα τα στοιχεία τής G, με εξαίρεση[34] το e_G, έχουν άπειρη τάξη· εν προκειμένω, λέμε ότι η G **δεν διαθέτει στρέψη** ή ότι η G **στερείται στρέψεως**.

(iii) Άλλα στοιχεία τής G έχουν πεπερασμένη και άλλα άπειρη τάξη. (Ήτοι έχουμε $\mathrm{tors}(G) \neq \{e_G\}$ και -ταυτοχρόνως- $G \setminus \mathrm{tors}(G) \neq \{e_G\}$). Εν τοιαύτη περιπτώσει η G καλείται **μικτή ομάδα**.

3.4.2 Παρατήρηση. Εάν $g \in G$, τότε, σύμφωνα με την πρόταση 3.3.18, έχουμε:

$$\mathrm{ord}\,(g) = |\langle g\rangle|\,. \tag{3.10}$$

3.4.3 Παράδειγμα. Στην $(\mathbb{Z}_4, +)$ τα στοιχεία $[0]_4, [1]_4, [2]_4$ και $[3]_4$ έχουν τάξη $1, 4, 2$ και 4, αντιστοίχως.

3.4.4 Παράδειγμα. Στην ομάδα των τετρανίων **Q** (βλ. 3.3.11) καθένα των στοιχείων **j** και **k** έχει τάξη 4.

[33] Το $\mathrm{tors}(G)$ δεν είναι κατ' ανάγκην *υποομάδα* τής G. Ωστόσο, όταν η G είναι *αβελιανή*, το $\mathrm{tors}(G)$ *είναι* υποομάδα τής G και καλείται **υποομάδα στρέψεως** τής G. (Πράγματι· $e_G \in \mathrm{tors}(G)$ και για οιαδήποτε $g_1, g_2 \in \mathrm{tors}(G)$, $\exists (k, l) \in \mathbb{N} \times \mathbb{N} : g_1^k = e_G = g_2^l$. Εάν η G είναι *αβελιανή*, τότε, σύμφωνα με τα προαναφερθέντα στο εδάφιο 3.2.12, $(g_1 g_2^{-1})^{kl} = g_1^{kl}(g_2^{-1})^{kl} = (g_1^k)^l (g_2^l)^{-k} = e_G \cdot e_G = e_G$, οπότε $g_1 g_2^{-1} \in G$ και, ως εκ τούτου, $\mathrm{tors}(G) \sqsubseteq G$ επί τη βάσει τού κριτηρίου 3.2.16 (i)⇔(iii).)

[34] Προφανώς, $\mathrm{ord}(g) = 1 \iff g = e_G$.

3.4.5 Παραδείγματα. Στις $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+),(\mathbb{Q}_{>0},\cdot),\ (\mathbb{R}_{>0},\cdot)$ κάθε στοιχείο διαφορετικό τού ουδετέρου έχει άπειρη τάξη, οπότε αυτές οι ομάδες δεν διαθέτουν στρέψη.

3.4.6 Παραδείγματα. (i) Το (αριθμήσιμο) απειροσύνολο

$$\boxed{\mathcal{E}_\infty := \bigcup_{n\in\mathbb{N}} \mathcal{E}_n = \{z\in\mathbb{C}\,|z^n=1,\ \text{για κάποιον } n\in\mathbb{N}\} \subsetneqq \mathbb{C}\smallsetminus\{0\}}$$

όλων των n-οστών ριζών τής μονάδας (βλ. 3.2.21 (vi)) αποτελεί *περιοδική* υποομάδα[35] τής αβελιανής ομάδας $(\mathbb{C}\smallsetminus\{0\},\cdot)$. Από την άλλη μεριά, η υποομάδα $(\mathbb{S}^1,\cdot)$ τής $(\mathbb{C}\smallsetminus\{0\},\cdot)$ (βλ. 3.2.21 (vi)) είναι μια *μικτή* ομάδα (με το υποκείμενο σύνολό της άπειρο και μη αριθμήσιμο), καθότι τα $\exp(i\theta)\in\mathbb{S}^1$ έχουν πεπερασμένη τάξη εάν και μόνον εάν το θ είναι ένα ρητό πολλαπλάσιο τού 2π (ήτοι $\theta=\frac{2\pi m}{n}$, για κάποιους $m\in\mathbb{Z}$ και $n\in\mathbb{Z}\smallsetminus\{0\}$). Ως εκ τούτου, και η ίδια η $(\mathbb{C}\smallsetminus\{0\},\cdot)$ είναι *μικτή*.

(ii) Άλλη μία ενδιαφέρουσα *περιοδική* ομάδα είναι η λεγόμενη p^∞**-ομάδα**, ήτοι η υποομάδα

$$\boxed{\mathcal{E}_{p^\infty} := \bigcup_{n\in\mathbb{N}_0} \mathcal{E}_{p^n} = \left\{z\in\mathbb{C}\,\middle|z^{p^n}=1,\ \text{για κάποιον } n\in\mathbb{N}_0\right\} \sqsubset \mathcal{E}_\infty \sqsubset \mathbb{S}^1}$$

τής $\mathcal{E}_\infty$ η απαρτιζόμενη από τις p^n-οστές ρίζες τής μονάδας, όπου p *τυχών* πρώτος αριθμός.

3.4.7 Πρόταση. *Έστω $(G,\cdot)$ μια πεπερασμένη ομάδα. Τότε η G είναι κυκλική εάν και μόνον εάν υπάρχει κάποιο $g\in G$ με $\operatorname{ord}(g)=|G|$.*

Απόδειξη. Εάν η G είναι κυκλική, τότε $\exists g\in G: G=\langle g\rangle$, οπότε -βάσει τής (3.10)- έχουμε $\operatorname{ord}(g)=|\langle g\rangle|=|G|$. Και αντιστρόφως· εάν υπάρχει κάποιο $g\in G$ με $\operatorname{ord}(g)=|G|$, τότε ισχύει $|\langle g\rangle|=|G|$ και $\langle g\rangle\subseteq G\Longrightarrow G=\langle g\rangle$, οπότε η G είναι κυκλική. □

3.4.8 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Εάν $g\in G$, $\operatorname{ord}(g)=n\in\mathbb{N}$ και $m\in\mathbb{Z}$, τότε ισχύει η αμφίπλευρη συνεπαγωγή $(g^m=e_G)\Longleftrightarrow n\,|m$.*

Απόδειξη. Εάν $n\,|m$, τότε $\exists q\in\mathbb{Z}: m=nq$. Επομένως,

$$g^m=g^{nq}=(g^n)^q=e_G^q=e_G.$$

Και αντιστρόφως· εάν $g^m=e_G$, για κάποιον $m\in\mathbb{Z}$, τότε υπάρχουν ακέραιοι q,r, τέτοιοι ώστε να ισχύει $m=nq+r$ με $0\leqslant r<n$. Ως εκ τούτου,

$$g^m=g^{nq+r}=(g^n)^q\,g^r=e_G^q g^r=e_G g^r=g^r.$$

Όμως ο n είναι ο ελάχιστος φυσικός αριθμός για τον οποίο ισχύει $g^n=e_G$. Άρα έχουμε $r=0$ και $n\,|m$. □

3.4.9 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Τότε ισχύουν τα ακόλουθα*:

(i) $\operatorname{ord}(g)=\operatorname{ord}\left(g^{-1}\right),\forall g\in G$.

(ii) $\operatorname{ord}\left(g_2g_1g_2^{-1}\right)=\operatorname{ord}(g_1),\forall(g_1,g_2)\in G\times G$.

(iii) $\operatorname{ord}(g_1g_2)=\operatorname{ord}(g_2g_1),\forall(g_1,g_2)\in G\times G$.

(iv) *Εάν κάθε στοιχείο τής G έχει τάξη το πολύ 2, τότε η G είναι αβελιανή.*

[35] Προφανώς, $1\in\mathcal{E}_\infty$. Επιπροσθέτως, εάν $z_1,z_2\in\mathcal{E}_\infty$, τότε $\exists(m,n)\in\mathbb{N}\times\mathbb{N}: z_1^m=1=z_2^n$. Επειδή $(z_1z_2^{-1})^{mn}=z_1^{mn}(z_2^{-1})^{mn}=(z_1^m)^n(z_2^n)^{-m}=1\cdot1=1$, έχουμε $z_1z_2^{-1}\in\mathcal{E}_\infty$. Άρα $\mathcal{E}_\infty\sqsubset\mathbb{C}\smallsetminus\{0\}$. (Βλ. κριτήριο 3.2.16 (i)⇔(iii).)

(v) *Εάν τα* $a, b \in G$ *είναι τέτοια, ώστε* $ab = ba$ *και* $\text{ord}(a) = m$, $\text{ord}(b) = n$, *όπου* $m, n \in \mathbb{N}$ *με* $\text{μκδ}(m, n) = 1$, *τότε* $\text{ord}(ab) = mn$.

ΑΠΟΔΕΙΞΗ. (i) Υποθέτουμε εν πρώτοις ότι $\text{ord}(g) = n \in \mathbb{N}$. Τότε

$$g^n = e_G \Longrightarrow (g^n)^{-1} = e_G^{-1} = e_G \Longrightarrow \left(g^{-1}\right)^n = e_G.$$

Για να αποδείξουμε ότι $\text{ord}\left(g^{-1}\right) = n$ αρκεί να ισχύει $m \geqslant n$, για κάθε $m \in \mathbb{N}$ για το οποίο $\left(g^{-1}\right)^m = e_G$. Όμως

$$\begin{aligned}&\left(g^{-1}\right)^m = e_G \Longrightarrow g^{-m} = e_G \Longrightarrow (g^{-m})^{-1} = e_G^{-1} = e_G\\ &\Longrightarrow g^m = e_G \underset{3.4.8}{\Longrightarrow} n \,|m \Longrightarrow n \leqslant m.\end{aligned}$$

Και αντιστρόφως· εάν $\text{ord}\left(g^{-1}\right) = n \in \mathbb{N}$, τότε, εφαρμόζοντας την ήδη αποδειχθείσα συνεπαγωγή (με εναλλαγή των ρόλων των g και g^{-1}), λαμβάνουμε

$$\text{ord}\left(g^{-1}\right) = n \Longrightarrow \text{ord}\left(\left(g^{-1}\right)^{-1}\right) = \text{ord}\,(g) = n.$$

Εν συνεχεία, υποθέτουμε ότι $\text{ord}(g) = \infty$. Εάν $\text{ord}\left(g^{-1}\right) \neq \infty$, τότε θα υπήρχε ένας φυσικός αριθμός n με $n = \text{ord}\left(g^{-1}\right)$, πράγμα αδύνατο, διότι σε αυτήν την περίπτωση θα είχαμε κατ' ανάγκην και $\text{ord}(g) = n$ (βάσει των όσων προαναφέραμε). Και αντιστρόφως· εάν $\text{ord}\left(g^{-1}\right) = \infty$, τότε, με εκ νέου εφαρμογή τής ήδη αποδειχθείσας συνεπαγωγής (και εναλλαγή των ρόλων των g και g^{-1}), λαμβάνουμε

$$\text{ord}\left(g^{-1}\right) = \infty \Longrightarrow \text{ord}\left(\left(g^{-1}\right)^{-1}\right) = \text{ord}\,(g) = \infty.$$

(ii) Έστω $(g_1, g_2) \in G \times G$ με $\text{ord}(g_1) = n \in \mathbb{N}$. Είναι εύκολο να αποδειχθεί επαγωγικώς ότι ισχύει η ισότητα $\left(g_2 g_1 g_2^{-1}\right)^n = g_2 g_1^n g_2^{-1}$. Επειδή -εξ υποθέσεως- $g_1^n = e_G$, έχουμε $\left(g_2 g_1 g_2^{-1}\right)^n = g_2 e_G g_2^{-1} = g_2 g_2^{-1} = e_G$. Για να αποδείξουμε ότι $\text{ord}\left(g_2 g_1 g_2^{-1}\right) = n$ αρκεί να ισχύει $m \geqslant n$, για κάθε $m \in \mathbb{N}$ για το οποίο $\left(g_2 g_1 g_2^{-1}\right)^m = e_G$. Όμως

$$\left(g_2 g_1 g_2^{-1}\right)^m = g_2 g_1^m g_2^{-1} = e_G \Longrightarrow g_2^{-1} g_2 g_1^m g_2^{-1} g_2 = g_2^{-1} e_G g_2 \Longrightarrow g_1^m = e_G,$$

οπότε $m \geqslant n$. Και αντιστρόφως· εάν $\text{ord}\left(g_2 g_1 g_2^{-1}\right) = n$, τότε, εφαρμόζοντας την ήδη αποδειχθείσα συνεπαγωγή (με εναλλαγή των ρόλων των g_1 και $g_2 g_1 g_2^{-1}$, καθώς και των g_2 και g_2^{-1}), λαμβάνουμε

$$\text{ord}\left(g_2 g_1 g_2^{-1}\right) = n \Longrightarrow \text{ord}\left(g_2^{-1}\left(g_2 g_1 g_2^{-1}\right) g_2\right) = \text{ord}\,(g_1) = n.$$

Εν συνεχεία, υποθέτουμε ότι $\text{ord}(g_1) = \infty$. Εάν $\text{ord}\left(g_2 g_1 g_2^{-1}\right) \neq \infty$, τότε θα υπήρχε ένας φυσικός αριθμός n με $n = \text{ord}\left(g_2 g_1 g_2^{-1}\right)$, πράγμα αδύνατο, διότι εν τοιαύτη περιπτώσει θα είχαμε κατ' ανάγκην και $\text{ord}(g_1) = n$ (βάσει των όσων προαναφέραμε). Και αντιστρόφως· εάν $\text{ord}\left(g_2 g_1 g_2^{-1}\right) = \infty$, τότε, με εκ νέου εφαρμογή τής ήδη αποδειχθείσας συνεπαγωγής (και εναλλαγή των ρόλων των g_1 και $g_2 g_1 g_2^{-1}$, καθώς και των g_2 και g_2^{-1}) λαμβάνουμε

$$\text{ord}\left(g_2 g_1 g_2^{-1}\right) = \infty \Longrightarrow \text{ord}\left(g_2^{-1}\left(g_2 g_1 g_2^{-1}\right) g_2\right) = \text{ord}\,(g_1) = \infty.$$

(iii) Επειδή $g_1 g_2 = g_1 (g_2 g_1) g_1^{-1}$, τα $g_2 g_1$ και $g_1 g_2$ έχουν την ίδια τάξη βάσει τού (ii).
(iv) Εάν $(a, b) \in G \times G$, τότε -εξ υποθέσεως- έχουμε

$$a^2 = b^2 = (ab)^2 = e_G \Longrightarrow a = a^{-1}, b = b^{-1}, (ab)^{-1} = ab,$$

οπότε $ab = (ab)^{-1} = b^{-1} a^{-1} = ba$. Άρα η G είναι αβελιανή.

(v) Επειδή $(ab)^{mn} \underset{3.2.12}{=} a^{mn}b^{mn} = (a^m)^n(b^n)^m = e_G^n e_G^m = e_G$, η τάξη τού στοιχείου ab είναι κατ' ανάγκην πεπερασμένη και $\text{ord}(ab) \leqslant mn$. Έστω $r \in \mathbb{N}$, τέτοιος ώστε $(ab)^r = e_G$. Προφανώς,

$$\left.\begin{array}{l} e_G = (ab)^{rm} \underset{3.2.12}{=} a^{rm}b^{rm} = (a^m)^r b^{rm} = b^{rm} \\ e_G = (ab)^{rn} \underset{3.2.12}{=} a^{rn}b^{rn} = a^{rn}(b^n)^r = a^{rn} \end{array}\right\} \underset{3.4.8}{\Longrightarrow} \left\{\begin{array}{c} n \mid rm \\ \text{και} \\ m \mid rn \end{array}\right\}$$

$$\underset{2.2.9}{\Longrightarrow} \left\{\begin{array}{c} n \mid r \\ \text{και} \\ m \mid r \end{array}\right\} \underset{2.2.10}{\Longrightarrow} mn \mid r \Rightarrow mn \leqslant r \Rightarrow mn \leqslant \text{ord}(ab).$$

Κατά συνέπειαν, $\text{ord}(ab) = mn$. □

3.4.10 Πρόταση. *Έστω $(G, \cdot)$ μια ομάδα με τάξη $|G| = m \in \mathbb{N}$. Εάν η G είναι κυκλική, παραγόμενη από ένα στοιχείο $g \in G$ και $a = g^n$, $n \in \mathbb{N}$, τότε ισχύουν τα εξής:*

(i) *Το a παράγει μια υποομάδα H τής G τάξεως $|H| = \frac{m}{\text{μκδ}(m,n)}$.*

(ii) $H = \left\langle g^{\text{μκδ}(m,n)} \right\rangle$.

Απόδειξη. (i) Κατά την πρόταση 3.3.19 η $H = \langle a \rangle$ είναι μια κυκλική υποομάδα τής G. Αρκεί λοιπόν να προσδιορίσουμε την τάξη της. Σύμφωνα με την πρόταση 3.4.8, εάν $k \in \mathbb{N}$, τότε

$$a^k = e_G \Longleftrightarrow g^{nk} = e_G \Longleftrightarrow m \,|nk\,.$$

Άρα έχουμε $|H| = \min\{\, k \in \mathbb{N} \mid \; m \,|nk\,\}$. Έστω $d := \text{μκδ}(m,n)$. Βάσει τού θεωρήματος 2.2.5 υπάρχουν $\mu, \nu \in \mathbb{Z}$, τέτοιοι ώστε

$$d = \mu m + \nu n \Longrightarrow 1 = \mu\left(\frac{m}{d}\right) + \nu\left(\frac{n}{d}\right). \tag{3.11}$$

Από την τελευταία ισότητα συνάγεται ότι οι $\frac{m}{d}$ και $\frac{n}{d}$ είναι σχετικώς πρώτοι (βλ. πόρισμα 2.2.8). Το ζητούμενο είναι ο προσδιορισμός τού ελαχίστου φυσικού αριθμού k, για τον οποίο

$$\frac{nk}{m} = \frac{k\left(\frac{n}{d}\right)}{\left(\frac{m}{d}\right)} \in \mathbb{Z}.$$

Επειδή $\text{μκδ}(\frac{n}{d}, \frac{m}{d}) = 1$, η ανωτέρω συνθήκη ισοδυναμεί με την: $\frac{m}{d} \big| \, k$ (βλ. πόρισμα 2.2.9). Κατά συνέπειαν, $\min\{k \in \mathbb{N} \;: m \,|nk\,\} = \frac{m}{d} = |H|\,.$

(ii) Επειδή $a = g^n = g^{d\left(\frac{n}{d}\right)} = \left(g^d\right)^{\frac{n}{d}} \Longrightarrow g^n \in \left\langle g^d \right\rangle$, η H είναι μια υποομάδα τής $\left\langle g^d \right\rangle$. Από την άλλη μεριά, λόγω τής (3.11),

$$g^d = g^{\mu m + \nu n} = (g^m)^\mu \, (g^n)^\nu = e_G^\mu \, (g^n)^\nu = e_G \, (g^n)^\nu = (g^n)^\nu \Longrightarrow g^d \in \langle g^n \rangle,$$

οπότε και η $\left\langle g^d \right\rangle$ είναι υποομάδα τής H. □

3.4.11 Πόρισμα. *Έστω $(G, \cdot)$ μια ομάδα και έστω $(m,n) \in \mathbb{N}^2$. Εάν $g \in G$, τότε ισχύει η συνεπαγωγή*

$$\text{ord}\,(g) = m \Longrightarrow \text{ord}\,(g^n) = \frac{m}{\text{μκδ}\,(m,n)}.$$

Απόδειξη. Προφανής βάσει τής προτάσεως 3.4.10 και τού (3.10). □

3.4.12 Πόρισμα. *Έστω $(G,\cdot)$ μια ομάδα και έστω $(m,n)\in\mathbb{N}^2$. Εάν $g\in G$, τότε ισχύει η συνεπαγωγή*

$$[\operatorname{ord}(g)=m \ \textit{και}\ \ n\,|m]\Longrightarrow \operatorname{ord}(g^n)=\frac{m}{n}.$$

3.4.13 Παραδείγματα. (i) Εάν η $(G,\cdot)$ είναι μια ομάδα, $g\in G$ και $\operatorname{ord}(g)=12$, τότε, επί παραδείγματι,

$$\operatorname{ord}\left(g^9\right)=\frac{12}{\text{μκδ}\,(12,9)}=\frac{12}{3}=4,\ \operatorname{ord}\left(g^{10}\right)=\frac{12}{\text{μκδ}\,(12,10)}=\frac{12}{2}=6.$$

(ii) Εντός τής $(\mathbb{Z}_{48},+)$ έχουμε $\operatorname{ord}([4]_{48})=12$, διότι

$$\begin{cases} 2\,[4]_{48}=[8]_{48}\,,\ 3\,[4]_{48}=[12]_{48}\,,\ 4\,[4]_{48}=[16]_{48}\,,\ 5\,[4]_{48}=[20]_{48}\,,\\ 6\,[4]_{48}=[24]_{48}\,,\ 7\,[4]_{48}=[28]_{48}\,,\ 8\,[4]_{48}=[32]_{48}\,,\ 9\,[4]_{48}=[36]_{48}\,,\\ 10\,[4]_{48}=[40]_{48}\,,\ 11\,[4]_{48}=[44]_{48}\,,\ 12\,[4]_{48}=[48]_{48}=[0]_{48}\,. \end{cases}$$

Επομένως, τα $[12]_{48}$ και $[20]_{48}$ έχουν τάξη

$$\operatorname{ord}\left(3\,[4]_{48}\right)=\frac{12}{\text{μκδ}\,(12,3)}=\frac{12}{3}=4,\ \operatorname{ord}\left(5\,[4]_{48}\right)=\frac{12}{\text{μκδ}\,(12,5)}=\frac{12}{1}=12.$$

Γενικότερα, ισχύει το ακόλουθο:

3.4.14 Πόρισμα. *Έστω $m\in\mathbb{N}$. Τότε για κάθε $n\in\mathbb{Z}$ η τάξη τού στοιχείου $[n]_m$ τής ομάδας $(\mathbb{Z}_m,+)$ δίδεται από τον τύπο*:

$$\operatorname{ord}\left([n]_m\right)=\frac{m}{\text{μκδ}\,(m,n)}.$$

Απόδειξη. Επειδή $|\mathbb{Z}_m|=m$, $\mathbb{Z}_m=\langle[1]_m\rangle\Longrightarrow\operatorname{ord}([1]_m)=|\langle[1]_m\rangle|=m$ και $[n]_m=n\,[1]_m$, συνάγεται ότι $\operatorname{ord}([n]_m)=\operatorname{ord}(n\,[1]_m)=\frac{m}{\text{μκδ}(m,n)}$ μέσω εφαρμογής τού πορίσματος 3.4.11. □

3.4.15 Πόρισμα. *Έστω $(G,\cdot)$ μια ομάδα και έστω $g\in G$ με $\operatorname{ord}(g)=\kappa_1\kappa_2$, όπου $\kappa_1,\kappa_2\in\mathbb{N}$ και $\text{μκδ}(\kappa_1,\kappa_2)=1$. Τότε υπάρχουν $g_1,g_2\in\langle g\rangle$, τέτοια ώστε να ισχύει $g=g_1g_2$ με $\operatorname{ord}(g_1)=\kappa_1$ και $\operatorname{ord}(g_2)=\kappa_2$.*

Απόδειξη. Επειδή $\text{μκδ}(\kappa_1,\kappa_2)=1$, υπάρχουν $\lambda_1,\lambda_2\in\mathbb{Z}:\lambda_1\kappa_1+\lambda_2\kappa_2=1$. (Βλ. πόρισμα 2.2.8.) Επομένως, $g=g^1=g^{\lambda_1\kappa_1+\lambda_2\kappa_2}=g^{\lambda_2\kappa_2+\lambda_1\kappa_1}=(g^{\lambda_2\kappa_2})(g^{\lambda_1\kappa_1})$. Θέτοντας $g_1:=g^{\lambda_2\kappa_2}\in\langle g\rangle$ και $g_2:=g^{\lambda_1\kappa_1}\in\langle g\rangle$, παρατηρούμε ότι

$$\text{μκδ}\,(\kappa_1\kappa_2,\lambda_2\kappa_2)=\kappa_2\ \text{μκδ}\,(\kappa_1,\lambda_2)=\kappa_2$$

(βλ. 2.2.14 (i) και 2.2.8), οπότε $\operatorname{ord}(g_1)\underset{3.4.11}{=}\frac{\kappa_1\kappa_2}{\text{μκδ}(\kappa_1\kappa_2,\lambda_2\kappa_2)}=\frac{\kappa_1\kappa_2}{\kappa_2}=\kappa_1$ και, κατ' αναλογίαν, $\operatorname{ord}(g_2)=\frac{\kappa_1\kappa_2}{\kappa_1}=\kappa_2$. □

3.4.16 Πόρισμα. *Έστω ότι η $G=\{e,g,g^2,\ldots,g^{m-1}\}=\langle g\rangle$ (όπου $e=e_G$) είναι μια πεπερασμένη κυκλική ομάδα τάξεως $m\in\mathbb{N}$ και ότι $k,l\in\{0,\ldots,m-1\}$. Τότε*

$$\left\langle g^k\right\rangle=\left\langle g^l\right\rangle\Longleftrightarrow\text{μκδ}\,(k,m)=\text{μκδ}\,(l,m)\,.$$

Απόδειξη. Εάν $\left\langle g^k\right\rangle=\left\langle g^l\right\rangle$, τότε $\left|\left\langle g^k\right\rangle\right|=\left|\left\langle g^l\right\rangle\right|$ και από την πρόταση 3.4.10 (i) έπεται ότι

$$\frac{m}{\text{μκδ}\,(k,m)}=\frac{m}{\text{μκδ}\,(l,m)}\Longrightarrow\text{μκδ}\,(k,m)=\text{μκδ}\,(l,m)\,.$$

Και αντιστρόφως· εάν $\text{μκδ}(k,m)=\text{μκδ}(l,m)=:d$, τότε, βάσει τής 3.4.10 (ii), ισχύουν οι ισότητες $\left\langle g^k\right\rangle=\left\langle g^d\right\rangle=\left\langle g^l\right\rangle$. □

3.4.17 Πόρισμα. *Έστω ότι η* $G = \{e, g, g^2, \dots, g^{m-1}\}$ *(όπου* $e = e_G$*) είναι μια πεπερασμένη κυκλική ομάδα τάξεως* $m \in \mathbb{N}$ *και ότι* $k \in \{0, \dots, m-1\}$*. Τότε η* $\langle g^k \rangle$ *παράγει την* G *εάν και μόνον εάν* $\mu\kappa\delta(k, m) = 1$*. Ως εκ τούτου,*

$$\text{card}\left(\{\text{γεννήτορες τής } G\}\right) = \phi(m),$$

όπου ϕ *η συνάρτηση φι τού Euler (βλ.* 2.4.15*).*

3.4.18 Παράδειγμα. Οι μόνοι γεννήτορες τής (προσθετικής) ομάδας

$$\mathbb{Z}_8 = \{[0]_8, [1]_8, [2]_8, [3]_8, [4]_8, [5]_8, [6]_8, [7]_8\}$$

είναι οι εξής: $\mathbb{Z}_8 = \langle [1]_8 \rangle = \langle [3]_8 \rangle = \langle [5]_8 \rangle = \langle [7]_8 \rangle$.

3.4.19 Πρόταση (Πεπερασμένες ομάδες τάξεως το πολύ 3). *Όλες οι ομάδες τάξεως* $\leqslant 3$ *είναι κυκλικές.*

Απόδειξη. Μια ομάδα με μόνον ένα στοιχείο είναι προφανώς κυκλική. Έστω $(G, \cdot)$ μια ομάδα τάξεως 2. Τότε $G = \{e, g\}$, όπου $e = e_G$ και $g \neq e$. Θεωρούμε το στοιχείο $g^2 \in G$. Αυτό δεν μπορεί να ισούται με το g (λόγω τής συνεπαγωγής $g^2 = g \Rightarrow g = e$ τής απορρέουσας από τον νόμο τής διαγραφής 3.2.9 (i)). Τούτο σημαίνει ότι $g^2 = e$, οπότε $\text{ord}(g) = 2$. Από την πρόταση 3.4.7 έπεται ότι η $(G, \cdot)$ είναι κυκλική έχουσα το g ως (μοναδικό) γεννήτορά της.

Εν συνεχεία, θεωρούμε τυχούσα ομάδα $(G, \cdot)$ τάξεως 3. Τότε $G = \{e, x, y\}$, όπου $e = e_G$, $x \neq y$, $x \neq e$ και $y \neq e$. Παρατηρούμε ότι $xy = e$. (Πράγματι· εάν ίσχυε $xy = x$ ή $xy = y$, τότε θα καταλήγαμε, εκ νέου λόγω τής εφαρμογής τού νόμου τής διαγραφής, σε αντίφαση, διότι θα έπρεπε να ισχύει $y = e$ ή $x = e$.) Χρησιμοποιώντας αυτό συμπεραίνουμε ότι $x^2 = y$. (Πράγματι· εάν ίσχυε $x^2 \neq y$, τότε είτε $x^2 = x$ είτε $x^2 = e$. Η πρώτη ισότητα είναι αδύνατη, διότι θα έπρεπε να έχουμε $x = e$. Η δεύτερη είναι ωσαύτως αδύνατη, διότι εν τοιαύτη περιπτώσει θα καταλήγαμε στο ότι $x^2 y = ey = y$, ήτοι στο ότι $y = x(xy) = x$.) Άρα $G = \{e, x, x^2\}$ με $\text{ord}(x) = 3$ (διότι $x \neq e$, $x^2 \neq e$ και $x^3 = xy = e$). Από την πρόταση 3.4.7 και το πόρισμα 3.4.16 έπεται ότι η $(G, \cdot)$ είναι κυκλική με $G = \langle x \rangle = \langle x^2 \rangle$. □

3.4.20 Σημείωση. Μια ομάδα τάξεως 4 δεν είναι κατ' ανάγκην κυκλική· ωστόσο, οφείλει να είναι *αβελιανή*, όπως θα δούμε στο θεώρημα 4.5.6.

Η εύρεση των υποομάδων μιας δεδομένης ομάδας -*όταν* είναι εφικτή- μας επιφυλάσσει μια ως επί το πλείστον επίπονη διαδικασία. Ωστόσο, στην ειδική περίπτωση κατά την οποία θεωρούμε μόνον *κυκλικές ομάδες*, το θεώρημα 3.4.21 και τα συνακόλουθα πορίσματα 3.4.23 και 3.5.28 μας παρέχουν μια πλήρη (και αρκετά εύκολη) περιγραφή τόσον τού τρόπου σχηματισμού όσον και τού πλήθους των διαθέσιμων υποομάδων.

3.4.21 Θεώρημα. *Έστω* $G = \{e, g, g^2, \dots, g^{m-1}\}$ *μια πεπερασμένη κυκλική ομάδα τάξεως* $m \in \mathbb{N}$ *(όπου* $e = e_G$*). Τότε ισχύουν τα εξής:*

(i) *Για δοθέντα* $n \in \mathbb{N}$*, η* G *διαθέτει μια υποομάδα τάξεως* n *εάν και μόνον εάν* $n \,|m$*.*

(ii) *Εάν* $n \,|m$*, τότε η* G *διαθέτει μία και μόνον υποομάδα τάξεως* n*.*

Απόδειξη. (i) Εάν $n \,|m$, τότε $\frac{m}{n} \,|m$, οπότε -κατά το πόρισμα 3.4.12-

$$\text{ord}(g^{\frac{m}{n}}) = \left|\langle g^{\frac{m}{n}} \rangle\right| = \frac{m}{m/n} = n,$$

δηλαδή η $\left\langle g^{\frac{m}{n}}\right\rangle$ έχει τάξη ίση με n. Και αντιστρόφως· εάν η H είναι μια υποομάδα τής G τάξεως n και $H=\left\langle g^{k}\right\rangle$, για κάποιον $k\in\{0,\ldots,m-1\}$ (πρβλ. 3.3.19 (ii)), τότε (λόγω τής 3.4.10 (i)):

$$|H|=\frac{m}{\text{μκδ}\,(m,k)}\Longrightarrow n=\frac{m}{\text{μκδ}\,(m,k)}\Longrightarrow n\,|m\ .$$

(ii) Ας υποθέσουμε ότι οι H_1 και H_2 είναι δυο υποομάδες τής G τάξεως n και ότι $\exists k_1,k_2\in\{0,\ldots,m-1\}:H_1=\left\langle g^{k_1}\right\rangle,\ \ H_2=\left\langle g^{k_2}\right\rangle$. Τότε

$$|H_1|=\frac{m}{\text{μκδ}\,(m,k_1)}=n=\frac{m}{\text{μκδ}\,(m,k_2)}=|H_2|\Longrightarrow\text{μκδ}\,(m,k_1)=\text{μκδ}\,(m,k_2)\,.$$

Όμως -κατά την πρόταση 3.4.10 (ii)- τούτο σημαίνει ότι $H_1=H_2$. □

3.4.22 Πόρισμα. *Έστω $G=\{e,g,g^2,\ldots,g^{m-1}\}$ μια πεπερασμένη κυκλική ομάδα τάξεως $m\in\mathbb{N}$ (όπου $e=e_G$). Σύμφωνα με το* (ii) *τού θεωρήματος* 3.4.21*, για κάθε θετικό ακέραιο διαιρέτη n τού m υφίσταται μία και μόνον υποομάδα τής G τάξεως n. Αυτή είναι η $\left\langle g^{\frac{m}{n}}\right\rangle=\{\,x\in G|\,x^n=e\}$.*

Απόδειξη. Το ότι η $\left\langle g^{\frac{m}{n}}\right\rangle$ είναι η μοναδική υποομάδα τής G τάξεως n έχει ήδη αποδειχθεί. Προφανώς[36],

$$\left\langle g^{\frac{m}{n}}\right\rangle=\{e,g^{\frac{m}{n}},g^{\frac{2m}{n}},\ldots,g^{\frac{(n-1)m}{n}}\}$$

και $(g^{\frac{im}{n}})^n=(g^m)^i=e^i=e,\forall i\in\{0,1,...,n-1\}$. Άρα $\left\langle g^{\frac{m}{n}}\right\rangle\subseteq\{\,x\in G|\,x^n=e\}$. Και αντιστρόφως· για κάθε $x\in G$ με $x^n=e$ υπάρχει ένας $k\in\{0,1,...,m-1\}$ τέτοιος ώστε να ισχύει $x=g^k$, οπότε

$$g^{kn}=e\underset{3.4.8}{\Longrightarrow}\text{ord}(g)=m\mid kn\Rightarrow[\exists l\in\mathbb{N}:kn=lm].$$

Επειδή

$$0\leqslant k=\frac{lm}{n}\leqslant m-1\Rightarrow 0\leqslant l\leqslant\frac{(m-1)n}{m}\leqslant m-1,$$

έχουμε

$$x=g^k=(g^{\frac{m}{n}})^l\in\left\langle g^{\frac{m}{n}}\right\rangle,$$

οπότε ισχύει και ο αντίστροφος εγκλεισμός $\{\,x\in G|\,x^n=e\}\subseteq\left\langle g^{\frac{m}{n}}\right\rangle$. □

3.4.23 Πόρισμα. *Έστω ότι η $G=\{e,g,g^2,\ldots,g^{m-1}\}$ είναι μια πεπερασμένη κυκλική ομάδα τάξεως $m\in\mathbb{N}$ (όπου $e=e_G$) και ότι οι $d_1,d_2,\ldots,d_\nu$ είναι οι θετικοί ακέραιοι διαιρέτες τού m. Τότε οι $\left\langle g^{d_1}\right\rangle,\left\langle g^{d_2}\right\rangle,\ldots,\left\langle g^{d_\nu}\right\rangle$ είναι όλες οι σαφώς διακεκριμένες (ήτοι οι ανά δύο διαφορετικές) υποομάδες τής G.*

Απόδειξη. Επειδή $d_j|\,m$, για κάθε[37] $j\in\{1,2,\ldots,\nu\}$, έχουμε μκδ$(d_j,m)=d_j$. Εάν λοιπόν για κάποιους $j,j'\in\{1,2,\ldots,\nu\}$ ισχύει

$$\left\langle g^{d_j}\right\rangle=\left\langle g^{d_{j'}}\right\rangle,$$

τότε

$$\left|\left\langle g^{d_j}\right\rangle\right|=\left|\left\langle g^{d_{j'}}\right\rangle\right|\Longrightarrow d_j=\text{μκδ}\,(d_j,m)=\text{μκδ}\,(d_{j'},m)=d_{j'},$$

απ' όπου έπεται ότι $j=j'$. □

[36] Όταν $n\geqslant 2$, τα αναγραφόμενα στοιχεία (εντός των αγκίστρων στο δεξιό μέλος) είναι *σαφώς διακεκριμένα*. Πράγματι· εάν υπήρχαν $i,j\in\{0,1,...,n-1\}$, $i>j$, με $g^{\frac{im}{n}}=g^{\frac{jm}{n}}$, τότε θα είχαμε

$$g^{\frac{im}{n}}g^{-\frac{m}{n}}=g^{\frac{jm}{n}}g^{-\frac{m}{n}}\Rightarrow g^i=g^j\Rightarrow g^{i-j}=e\underset{3.4.8}{\Longrightarrow}\text{ord}(g)=m\mid i-j\Rightarrow m\leqslant i-j,$$

και θα οδηγούμεθα σε κάτι που είναι άτοπο (διότι $m\geqslant n>n-1\geqslant i-j$).

[37] Για τον υπολογισμό τού ν βλ. το (i) τής προτάσεως 2.3.16.

▸ **Ομάδες πεπερασμένου εκθέτη**. Η παρούσα ενότητα κλείνει με τον ορισμό των ομάδων πεπερασμένου εκθέτη και την παράθεση των βασικών ιδιοτήτων τού εκθέτη πεπερασμένων ομάδων.

3.4.24 Ορισμός (Εκθέτης περιοδικής ομάδας). Έστω $(G,\cdot)$ μια περιοδική ομάδα. Εάν το σύνολο

$$\{\, n\in\mathbb{N} |\, g^n = e_G,\ \forall g\in G\} \tag{3.12}$$

δεν είναι κενό, τότε λέμε ότι η G είναι μια **ομάδα πεπερασμένου εκθέτη**. Εν τοιαύτη περιπτώσει ορίζουμε ως **εκθέτη**[38] $\exp(G)$ **τής** G το ελάχιστο στοιχείο αυτού τού συνόλου[39]. Εάν, αντιθέτως, το (3.12) είναι κενό, τότε είθισται να λέμε ότι η G είναι **ομάδα μη φρασσόμενου εκθέτη**[40] (και να γράφουμε $\exp(G)=\infty$).

3.4.25 Πρόταση. *Για κάθε πεπερασμένη ομάδα $(G,\cdot)$ ισχύουν τα ακόλουθα:*
(i) $\exp(G) = \text{εκπ}(\{\,\text{ord}(g) |\, g\in G\})$.
(ii) $\max\{\,\text{ord}(g) |\, g\in G\} \mid \exp(G)$.
(iii) *Εάν* $H\sqsubseteq G$, *τότε* $\exp(H)\mid\exp(G)$.

Απόδειξη. (i) Επειδή, σύμφωνα με την πρόταση 3.4.8, το σύνολο (3.12) ταυτίζεται με το σύνολο των κοινών πολλαπλασίων των τάξεων των στοιχείων τής G, ο εκθέτης $\exp(G)$ τής G είναι (εξ ορισμού) το ελάχιστο κοινό πολλαπλάσιο των τάξεων των στοιχείων της.

(ii) Λόγω τού (i), $\text{ord}(g)\mid\exp(G), \forall g\in G$, οπότε $\max\{\,\text{ord}(g) |\, g\in G\}\mid\exp(G)$.
(iii) Επειδή $\text{ord}(h)\mid\text{εκπ}(\{\,\text{ord}(g) |\, g\in G\}) \underset{\text{(i)}}{=} \exp(G)$ *για κάθε* $h\in H$, έχουμε

$$\exp(H) = \text{εκπ}(\{\,\text{ord}(h) |\, h\in H\}) \mid \exp(G).$$

(Βλ. πρόταση 2.2.25.) □

3.4.26 Πρόταση. *Για κάθε πεπερασμένη αβελιανή ομάδα $(G,\cdot)$ ισχύει η ισότητα*:

$$\exp(G) = \max\{\,\text{ord}(g) |\, g\in G\}\,.$$

(Σημειωτέον ότι υπάρχουν πεπερασμένες μη αβελιανές ομάδες για τις οποίες αυτή η ισότητα δεν ισχύει.[41])

Απόδειξη. Εάν $l := \max\{\,\text{ord}(g) |\, g\in G\}$, τότε, σύμφωνα με το (ii) τής προτάσεως 3.4.25, $l\mid\exp(G)$. Θα αποδείξουμε ότι $\exp(G) = \text{εκπ}(\{\,\text{ord}(g) |\, g\in G\})\mid l$. Προς τούτο αρκεί (λόγω τής προτάσεως 2.2.25) να δείξουμε ότι $\text{ord}(g)\mid l$ *για κάθε* στοιχείο $g\in G$. Θα εργασθούμε με «εις άτοπον απαγωγή». Υποθέτουμε ότι υπάρχει κάποιο $y\in G$ με $\text{ord}(y)\nmid l$. Τότε $\text{ord}(y)\geqslant 2$ και για οιοδήποτε $x\in G$ με $\text{ord}(x)=l$ υπάρχουν (βάσει τού λήμματος 2.3.15) κάποιοι $m,n,j\in\mathbb{N}$, $i\in\mathbb{N}_0$ και κάποιος

[38] Προσοχή! Ορισμένοι συγγραφείς ονομάζουν *κάθε* στοιχείο τού (3.12) εκθέτη τής G και για τον $\exp(G)$ χρησιμοποιούν τον όρο *ελάχιστος εκθέτης*. (Εδώ *δεν* ακολουθείται αυτή η ορολογία.)

[39] Από το (i) τής προτάσεως 3.4.25 έπεται ότι *κάθε πεπερασμένη* ομάδα είναι ομάδα πεπερασμένου εκθέτη. Ωστόσο, υπάρχουν και περιοδικές ομάδες πεπερασμένου εκθέτη που έχουν *άπειρη* τάξη.

[40] Η $\mathcal{E}_\infty$ (βλ. 3.4.6 (i)) αποτελεί παράδειγμα άπειρης (περιοδικής αλλά μη πεπερασμένως παραγόμενης) ομάδας μη φρασσόμενου εκθέτη. (Κάθε στοιχείο της έχει πεπερασμένη τάξη αλλά το σύνολο των τάξεων των στοιχείων της δεν είναι φραγμένο εκ των άνω!) Το πρώτο παράδειγμα άπειρης περιοδικής και (ταυτοχρόνως) *πεπερασμένως παραγόμενης* ομάδας μη φρασσόμενου εκθέτη ανακαλύφθηκε το έτος 1964 από τον E.S. Godol στο άρθρο του υπό τον τίτλο: *On nil-algebras and finitely residual groups*, Izv. Akad. Nauk SSSR. Ser. Mat. **28** (1964), 273-276.

[41] Επί παραδείγματι, η συμμετρική ομάδα $\mathfrak{S}_3$ (βλ. εδ. 4.2.2) έχει ένα στοιχείο τάξεως 1, 3 στοιχεία τάξεως 2 και 2 στοιχεία τάξεως 3. Επομένως, $\exp(\mathfrak{S}_3) = \text{εκπ}(1,2,3) = 6 > 3 = \max\{\,\text{ord}(\sigma) |\, \sigma\in\mathfrak{S}_3\}$.

πρώτος αριθμός p, ούτως ώστε να ισχύει $\text{ord}(x) = l = p^i m$ και $\text{ord}(y) = p^j n$, όπου $p \nmid m,\ p \nmid n$ και $j > i$. Κατά το πόρισμα 3.4.11,

$$\text{ord}(x^{p^i}) = \frac{l}{\text{μκδ}(l, p^i)} = \frac{l}{p^i} = m,\ \text{ord}(y^n) = \frac{p^j n}{\text{μκδ}(p^j n, n)} = \frac{p^j n}{n} = p^j.$$

Επειδή $p \nmid m \Rightarrow \text{μκδ}(m, p) = 1 \underset{2.2.13}{\Longrightarrow} \text{μκδ}(m, p^j) = 1$ και η G είναι αβελιανή, έχουμε

$$\text{ord}(\underbrace{x^{p^i} y^n}_{\in G}) \underset{3.4.9\ (v)}{=} mp^j = lp^{j-i} > l.$$

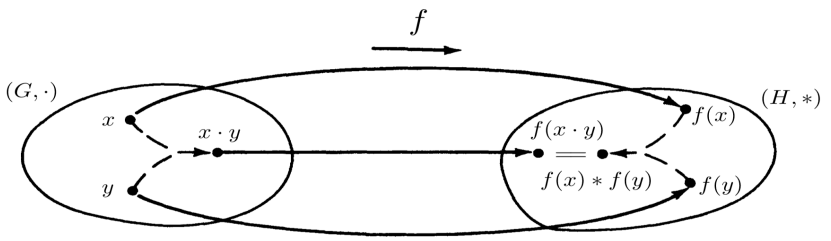
κάτι που αντίκειται στον ορισμό τού l. Άρα $\exp(G) \mid l \Rightarrow \exp(G) = l$. □

3.5 ΟΜΟΜΟΡΦΙΣΜΟΙ, ΙΣΟΜΟΡΦΙΣΜΟΙ ΚΑΙ ΑΥΤΟΜΟΡΦΙΣΜΟΙ ΟΜΑΔΩΝ

3.5.1 Ορισμός. Έστω ότι οι $(G, \cdot)$ και $(H, *)$ είναι δυο ομάδες. Μια απεικόνιση[42] $f : G \longrightarrow H$ καλείται **ομομορφισμός (ομάδων)** όταν για οιαδήποτε $x, y \in G$ ισχύει η ισότητα

$$\boxed{f(x \cdot y) = f(x) * f(y),} \tag{3.13}$$

ήτοι όταν η εικόνα τού «γινομένου» $x \cdot y$ των x και y μέσω τής f συμπίπτει με το «γινόμενο» $f(x) * f(y)$ των εικόνων τους (βλ. σχήμα).



3.5.2 Παραδείγματα. (i) Εάν η $(G, \cdot)$ είναι μια ομάδα και η U μια υποομάδα της, τότε η συνήθης ενθετική απεικόνιση $\iota_U : U \longrightarrow G$ είναι ένας ομομορφισμός, διότι

$$\iota_U(x \cdot y) = x \cdot y = \iota_U(x) \cdot \iota_U(y),\ \ \forall x, y \in G.$$

(ii) Εάν θεωρήσουμε ένα $a \in \mathbb{R}$ και ορίσουμε την απεικόνιση

$$\mu_a : (\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)\,,\quad x \longmapsto ax,$$

τότε η μ_a είναι ένας ομομορφισμός, διότι για όλα τα $x, y \in \mathbb{R}$ ισχύει

$$\mu_a(x + y) = a(x + y) = ax + ay = \mu_a(x) + \mu_a(y).$$

(iii) Η απεικόνιση $(\mathbb{R}, +) \longrightarrow (\mathbb{R} \setminus \{0\}, \cdot)\,,\ \ x \longmapsto \exp(x)$, αποτελεί έναν ομομορφισμό ομάδων.

[42] Όταν επιθυμούμε να τονίσουμε το ποιες είναι οι πράξεις αναφοράς μας, γράφουμε $f : (G, \cdot) \longrightarrow (H, *)$.

3.5.3 Πρόταση. *Εάν η* $f : (G, \cdot) \longrightarrow (H, *)$ *είναι ένας ομομορφισμός ομάδων, τότε ισχύουν τα εξής*:
(i) $f(e_G) = e_H$.
(ii) $f(g)^{-1} = f\left(g^{-1}\right),\ \forall g \in G$.
(iii) $f(g)^n = f(g^n),\ \forall g \in G$ *και* $\forall n \in \mathbb{Z}$.
(iv) *Εάν* $g \in G$ *και* $\operatorname{ord}(g) = n \in \mathbb{N}$, *τότε* $\operatorname{ord}(f(g)) = m \in \mathbb{N}$ *και* $m \mid n$.

Απόδειξη. (i) Επειδή λόγω τής (3.13), $f(e_G) * f(e_G) = f(e_G \cdot e_G) = f(e_G)$, έχουμε

$$f(e_G) * f(e_G) * f(e_G)^{-1} = f(e_G) * f(e_G)^{-1} \Longrightarrow f(e_G) = f(e_G) * f(e_G)^{-1} = e_H.$$

(ii) Για κάθε $g \in G$,

$$f(g) * f\left(g^{-1}\right) = f\left(gg^{-1}\right) = f(e_G) = e_H = f\left(g^{-1}g\right) = f\left(g^{-1}\right) * f(g),$$

οπότε όντως η εικόνα τού συμμετρικού στοιχείου τού g μέσω τής f ισούται με το συμμετρικό στοιχείο τού $f(g)$ εντός τής H.
(iii) Όταν $n = 0$ ο ισχυρισμός είναι αληθής επί τη βάσει τού (i) και όταν $n = 1$ η ισότητα είναι προφανής. Για $n \in \mathbb{N}$ εργαζόμαστε με τη βοήθεια τής κλασικής μαθηματικής επαγωγής. Ας υποθέσουμε ότι η εν λόγω ισότητα ισχύει για κάποιον φυσικό αριθμό $n \geqslant 1$. Τότε

$$f(g)^{n+1} = f(g)^n * f(g) = f(g^n) * f(g) = f(g^n \cdot g) = f(g^{n+1}).$$

Εάν $n \in \mathbb{Z} \smallsetminus \mathbb{N}_0$, τότε $-n > 0$, οπότε εφαρμόζοντας το ανωτέρω αποδειχθέν για τον $-n$, το (ii), καθώς και το (iii) τής προτάσεως 3.2.11, λαμβάνουμε

$$f(g)^n = (f(g)^{-1})^{-n} = f(g^{-1})^{-n} = f((g^{-1})^{-n}) = f(g^n).$$

Τελικώς λοιπόν, $f(g)^n = f(g^n),\ \forall g \in G$ και $\forall n \in \mathbb{Z}$.
(iv) Έστω $g \in G$ τάξεως $\operatorname{ord}(g) = n \in \mathbb{N}$. Τότε $g^n = e_G$, οπότε

$$f(g^n) = f(g)^n = f(e_G) = e_H \underset{3.4.8}{\Longrightarrow} \operatorname{ord}(f(g)) = m \in \mathbb{N} \text{ και } m \mid n,$$

με τις πρώτες ισότητες ισχύουσες λόγω των (i) και (iii). □

3.5.4 Λήμμα. *Εάν η* $f : (G, \cdot) \longrightarrow (H, *)$ *είναι ένας ομομορφισμός ομάδων, τότε ισχύουν τα εξής*:
(i) *Η εικόνα* $\operatorname{Im}(f) = f(G)$ *τής* G *μέσω τής* f *είναι μια υποομάδα τής* H.
(ii) *Το σύνολο*

$$\boxed{\operatorname{Ker}(f) := f^{-1}(\{e_H\}) = \{g \in G \mid f(g) = e_H\}}$$

(*που καλείται, ιδιαιτέρως,* ***πυρήνας*** *τής* f) *είναι μια υποομάδα τής* G.

Απόδειξη. (i) Κατά το 3.5.3 (i), $e_H = f(e_G) \in f(G)$. Εξάλλου, εάν $h, h' \in f(G)$, τότε υπάρχουν στοιχεία $g, g' \in G$ με

$$f(g) = h \text{ και } f(g') = h'.$$

Κατά συνέπειαν,

$$h * h'^{-1} = f(g) * f(g')^{-1} = f(g) * f(g'^{-1}) = f(gg'^{-1}) \in f(G),$$

οπότε η $f\,(G)$ είναι μια υποομάδα τής H δυνάμει τού (iii) τής προτάσεως 3.2.16.

(ii) Επειδή το ουδέτερο στοιχείο e_G τής G απεικονίζεται μέσω τής f στο ουδέτερο στοιχείο e_H τής H, έχουμε $e_G \in \mathrm{Ker}(f)$. Εξάλλου, εάν $g, g' \in \mathrm{Ker}(f)$, τότε

$$f(gg'^{-1}) = f(g) * f(g'^{-1}) = f(g) * f(g')^{-1} = e_H * e_H^{-1} = e_H * e_H = e_H.$$

Συνεπώς $gg'^{-1} \in \mathrm{Ker}(f)$ και αρκεί να εφαρμόσουμε εκ νέου το (iii) τής προτάσεως 3.2.16. □

3.5.5 Σημείωση. Στην ειδική περίπτωση όπου $f(g) = e_H$ για κάθε $g \in G$ (ήτοι $\mathrm{Im}(f) = \{e_H\}$) ο f καλείται **τετριμμένος ομομορφισμός**[43].

3.5.6 Πρόταση. *Έστω $X \neq \varnothing$ ένα σύνολο γεννητόρων μιας ομάδας $(G, \cdot)$* (βλ. ορισμό 3.3.1 και πρόταση 3.3.3)*. Τότε ισχύουν τα εξής:*

(i) *Για κάθε ομομορφισμό ομάδων $f : (G, \cdot) \longrightarrow (H, *)$ έχουμε $f(G) = \langle f(X)\rangle$.*

(ii) *Για δυο ομομορφισμούς ομάδων $f_1, f_2 : (G, \cdot) \longrightarrow (H, *)$ αληθεύει η αμφίπλευρη συνεπαγωγή:*

$$f_1|_X = f_2|_X \iff f_1 = f_2.$$

Απόδειξη. (i) Έστω $h \in f(G)$. Τότε $\exists g \in G : h = f(g)$. Επειδή $G = \langle X\rangle$, η πρόταση 3.3.3 μας πληροφορεί ότι

$$\exists k \in \mathbb{N} : g = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}, \text{ για κάποια } x_j \in X \text{ και κάποια } \varepsilon_j \in \mathbb{Z}, \tag{3.14}$$

$\forall j, 1 \leqslant j \leqslant k$. Κατά συνέπειαν,

$$\begin{aligned} h &= f(x_1^{\varepsilon_1}) * f(x_2^{\varepsilon_2}) * \cdots * f(x_k^{\varepsilon_k}) \\ &= f(x_1)^{\varepsilon_1} * f(x_2)^{\varepsilon_2} * \cdots * f(x_k)^{\varepsilon_k} \in \langle f(X)\rangle \Rightarrow f(G) = \langle f(X)\rangle. \end{aligned}$$

(ii) Η "$\Leftarrow$" είναι προφανής. Για την απόδειξη τής "$\Rightarrow$" θεωρούμε τυχόν στοιχείο $g \in G$. Επειδή $G = \langle X\rangle$, το g γράφεται υπό τη μορφή (3.14). Αυτό σημαίνει ότι

$$f_1(g) = f_1(x_1)^{\varepsilon_1} * \cdots * f_1(x_k)^{\varepsilon_k} = f_2(x_1)^{\varepsilon_1} * \cdots * f_2(x_k)^{\varepsilon_k} = f_2(g),$$

όπου η δεύτερη ισότητα έπεται από την υπόθεσή μας. Άρα τελικώς $f_1 = f_2$. □

3.5.7 Ορισμός. Έστω $f : (G, \cdot) \longrightarrow (H, *)$ ένας ομομορφισμός ομάδων. Ο f καλείται

μονομορφισμός	$\underset{\text{ορσ}}{\iff}$	η απεικόνιση f είναι ενριπτική,
επιμορφισμός	$\underset{\text{ορσ}}{\iff}$	η απεικόνιση f είναι επιριπτική,
ισομορφισμός	$\underset{\text{ορσ}}{\iff}$	η απεικόνιση f είναι αμφιριπτική,
ενδομορφισμός (**τής** G)	$\underset{\text{ορσ}}{\iff}$	$G = H$ και "$\cdot$" = "$*$",
αυτομορφισμός (**τής** G)	$\underset{\text{ορσ}}{\iff}$	η f είναι αμφιριπτικός ενδομορφισμός τής G.

3.5.8 Παραδείγματα. (i) Η απεικόνιση

$$(\mathbb{R}, +) \longrightarrow (\mathbb{R}_{>0}, \cdot), \quad x \longmapsto \exp(x),$$

αποτελεί έναν ισομορφισμό με αντίστροφό του τον $x \longmapsto \ln(x)$ $(:= \log_e(x))$.

(ii) Ο ομομορφισμός $\iota_U : U \longrightarrow G$ ο ορισθείς στο 3.5.2 (i) είναι μονομορφισμός. Οι ομομορφισμοί μ_a οι ορισθέντες στο 3.5.2 (ii) είναι αυτομορφισμοί τής $(\mathbb{R}, +)$ για

[43] Όταν για τις πράξεις των G και H χρησιμοποιείται ο προσθετικός συμβολισμός, είθισται αντί τού όρου *τετριμμένος ομομορφισμός* να χρησιμοποιείται ο όρος **μηδενικός ομομορφισμός**.

κάθε $a \neq 0$ (με τους $\mu_{\frac{1}{a}}$ ως αντιστρόφους τους). Ο μ_0 είναι προφανώς ο *μηδενικός ενδομορφισμός*, ήτοι αυτός ο ενδομορφισμός που στέλνει όλα τα στοιχεία τού $\mathbb{R}$ να απεικονισθούν στο 0.

(iii) Εάν $n \in \mathbb{N}$, τότε η απεικόνιση

$$(\mathbb{Z}, +) \longrightarrow (n\mathbb{Z}, +), \quad m \longmapsto nm,$$

είναι ένας ισομορφισμός μεταξύ τής $(\mathbb{Z}, +)$ και τής $(n\mathbb{Z}, +)$, όπου η $(n\mathbb{Z}, +)$ είναι *γνήσια*(!) υποομάδα τής $(\mathbb{Z}, +)$ όταν $n \geqslant 2$.

(iv) Η ακόλουθη απεικόνιση είναι ένας ισομορφισμός μεταξύ τής $(\mathbb{Z}_4, +)$ και τής $(\mathbb{Z}[i]^\times, \cdot)$ (βλ. 3.3.16 (iii)):

$$[0]_4 \mapsto 1,\ [1]_4 \mapsto i,\ [2]_4 \mapsto -1,\ [3]_4 \mapsto -i.$$

(v) Για κάθε $m \in \mathbb{N}$ υφίσταται ισομορφισμός

$$(\mathbb{Z}_m, +) \longrightarrow (\mathcal{E}_m, \cdot), \quad [k]_m \longmapsto \exp(\tfrac{2\pi i k}{m}).$$

(vi) Η απεικόνιση

$$a + bi \longmapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \ \forall\, (a,b) \in \mathbb{R}^2 \smallsetminus \{(0,0)\},$$

είναι ένας ισομορφισμός μεταξύ τής $(\mathbb{C}\smallsetminus\{0\}, \cdot)$ και τής υποομάδας H τής γενικής γραμμικής ομάδας $\mathrm{GL}_2(\mathbb{R})$ (βλ. 3.2.7 (iv)), όπου

$$H := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \ (a,b) \in \mathbb{R}^2 \smallsetminus \{(0,0)\} \right\}.$$

(vii) Η ακόλουθη απεικόνιση είναι ένας ισομορφισμός μεταξύ τής $(\mathbb{S}^1, \cdot)$ και τής ειδικής ορθογώνιας ομάδας $\mathrm{SO}_2(\mathbb{R})$ (βλ. 3.2.21 (viii)):

$$\mathbb{S}^1 \ni \exp(i\theta) \longmapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \in \mathrm{SO}_2(\mathbb{R}) \quad (0 \leqslant \theta < 2\pi).$$

(viii) Δεν υφίσταται ισομορφισμός μεταξύ των ομάδων $(\mathbb{Q}, +)$ και $(\mathbb{Q}_{>0}, \cdot)$. Πράγματι· εάν υπήρχε ισομορφισμός ομάδων $f : \mathbb{Q} \longrightarrow \mathbb{Q}_{>0}$, τότε, επειδή $2 \in \mathbb{Q}_{>0}$, θα υπήρχε κάποιος $r \in \mathbb{Q}$, τέτοιος ώστε να ισχύει η ισότητα $f(r) = 2$, οπότε θα καταλήγαμε στην ακόλουθη αντίφαση:

$$2 = f(r) = f(\tfrac{r}{2} + \tfrac{r}{2}) = f(\tfrac{r}{2}) f(\tfrac{r}{2}) = f(\tfrac{r}{2})^2 \underset{f(\frac{r}{2}) \in \mathbb{Q}_{>0}}{\Longrightarrow} f(\tfrac{r}{2}) = \sqrt{2} \in \mathbb{R} \smallsetminus \mathbb{Q}_{>0}.$$

3.5.9 Πρόταση. *Εάν $f_1 : (G_1, \cdot_1) \longrightarrow (G_2, \cdot_2)$ και $f_2 : (G_2, \cdot_2) \longrightarrow (G_3, \cdot_3)$ είναι δυο ομομορφισμοί ομάδων, τότε ισχύουν τα ακόλουθα*:

(i) *Η σύνθεση $f_2 \circ f_1 : G_1 \longrightarrow G_3$ είναι ομομορφισμός ομάδων.*

(ii) *Εάν οι f_1 και f_2 είναι μονομορφισμοί (και αντιστοίχως, επιμορφισμοί/ ισομορφισμοί), τότε και η σύνθεσή τους $f_2 \circ f_1 : G_1 \longrightarrow G_3$ είναι μονομορφισμός (και αντιστοίχως, επιμορφισμός/ισομορφισμός).*

Απόδειξη. (i) Για οιαδήποτε $x, y \in G$ έχουμε

$$\begin{aligned} (f_2 \circ f_1)(x \cdot_1 y) &= f_2(f_1(x \cdot_1 y)) = f_2(f_1(x) \cdot_2 f_1(y)) \\ &= f_2(f_1(x)) \cdot_3 f_2(f_1(y)) = (f_2 \circ f_1)(x) \cdot_3 (f_2 \circ f_1)(y). \end{aligned}$$

(ii) Τούτο έπεται άμεσα από το γεγονός ότι η σύνθεση δυο ενρίψεων (και αντιστοίχως, δυο επιρρίψεων/αμφιρρίψεων) είναι ένριψη (και αντιστοίχως, επίρριψη/αμφίρριψη). □

3.5.10 Σημείωση. (i) Το σύνολο $\mathrm{Hom}(G,H) := \{f : G \longrightarrow H \,|\, f \text{ ομομορφισμός}\}$ όλων των ομομορφισμών από μια ομάδα $(G,\cdot)$ σε μια ομάδα $(H,*)$, δεν έχει *πάντοτε* αφ'εαυτού τη δομή ομάδας ως προς κάποια εσωτερική πράξη. (Όταν $G = H$, το σύνολο των ενδομορφισμών και, αντιστοίχως, το σύνολο των αυτομορφισμών *μιας* ομάδας ως προς την εσωτερική πράξη τής συνθέσεως απεικονίσεων (βλ. 3.5.9 (i)) καθίσταται *μονοειδές* και, αντιστοίχως, *ομάδα*. Βλ. πρόταση 3.5.32.)

(ii) Στην περίπτωση όπου η $(H,*)$ είναι *αβελιανή*, το $\mathrm{Hom}(G,H)$, εφοδιαζόμενο με μια (άλλη, συνήθως εν είδει «προσθέσεως» συμβολιζόμενη) εσωτερική πράξη:

$$+ : \mathrm{Hom}(G,H) \times \mathrm{Hom}(G,H) \longrightarrow \mathrm{Hom}(G,H),\ (f_1,f_2) \longmapsto f_1 + f_2,$$
$$(f_1 + f_2)(x) := f_1(x) * f_2(x),\ \forall x \in G,$$

καθίσταται *αβελιανή ομάδα*. (Αυτή η αβελιανή ομάδα είναι ωσαύτως χρήσιμη για τον χειρισμό κάποιων θεωρητικών προβλημάτων.)

3.5.11 Ορισμός. Έστω ότι οι $(G,\cdot)$ και $(H,*)$ είναι δυο ομάδες. Λέμε ότι η G είναι **εμφυτεύσιμη στην** H ή ότι η G **εμφυτεύεται στην** H όταν υπάρχει κάποιος μονομορφισμός ομάδων $f : G \longrightarrow H$.

3.5.12 Πρόταση. *Ένας ομομορφισμός ομάδων $f : (G,\cdot) \longrightarrow (H,*)$ αποτελεί μονομορφισμό εάν και μόνον εάν ο πυρήνας του είναι η τετριμμένη υποομάδα τής G (ήτοι συνίσταται μόνον από το ουδέτερο στοιχείο e_G τής G).*

Απόδειξη. Εάν ο f είναι ένας μονομορφισμός, τότε για κάθε $g \in \mathrm{Ker}(f)$ έχουμε

$$f(g) = e_H = f(e_G) \underset{f \text{ ένριψη}}{\Longrightarrow} g = e_G.$$

Επομένως, $\mathrm{Ker}(f) = \{e_G\}$. Και αντιστρόφως· εάν υποθέσουμε ότι $\mathrm{Ker}(f) = \{e_G\}$ και ότι $f(g_1) = f(g_2)$ για δυο στοιχεία g_1, g_2 τής G, τότε

$$f\left(g_2^{-1} g_1\right) = (f(g_2))^{-1} * f(g_1) = (f(g_2))^{-1} * f(g_2) = e_H,$$

οπότε $g_2^{-1} \cdot g_1 = e_G \Longrightarrow g_1 = g_2$. Άρα ο ομομορφισμός f είναι όντως ένας μονομορφισμός. □

3.5.13 Ορισμός. Λέμε ότι δυο ομάδες $(G,\cdot)$ και $(H,*)$ είναι (μεταξύ τους) **ισόμορφες** ή ότι η G είναι **ισόμορφη με την** H ή, απλούστερα, ότι η G **είναι ισόμορφη τής** H (και σημειώνουμε: $(G,\cdot) \cong (H,*)$ ή απλώς[44] $G \cong H$) όταν υπάρχει κάποιος ισομορφισμός[45] ομάδων $f : G \longrightarrow H$.

3.5.14 Πρόταση. *Μια ομάδα $(G,\cdot)$ είναι εμφυτεύσιμη σε μια ομάδα $(H,*)$ εάν και μόνον εάν η G είναι ισόμορφη με μια υποομάδα τής H.*

Απόδειξη. Εάν μια ομάδα $(G,\cdot)$ είναι εμφυτεύσιμη σε μια ομάδα $(H,*)$, τότε υφίσταται κάποιος μονομορφισμός $f : G \longrightarrow H$. Θέτοντας $K := f(G)$, γνωρίζουμε ότι $K \sqsubseteq H$ (βλ. 3.5.4 (i)). Περιορίζοντας το πεδίο τιμών τής f στην εικόνα της λαμβάνουμε τον ισομορφισμό $G \ni g \longmapsto f(g) \in K$. Και αντιστρόφως· εάν η G είναι ισόμορφη με μια υποομάδα L τής H, τότε υφίσταται κάποιος ισομορφισμός $f : G \longrightarrow L$. Θεωρώντας (κατόπιν επεκτάσεως) ως πεδίο τιμών τής f το υποκείμενο σύνολο H τής $(H,*)$ λαμβάνουμε τον μονομορφισμό $G \ni g \longmapsto f(g) \in H$. □

[44] Κατ' αναλογίαν, ο συμβολισμός $G \ncong H$ θα δηλοί ότι η G δεν είναι ισόμορφη με την H.

[45] Ενίοτε, για να τονίσουμε ιδιαιτέρως (π.χ., σε μεταθετικά διαγράμματα και αλλού) ότι ένας ομομορφισμός ομάδων $f : G \longrightarrow H$ είναι *ισομορφισμός*, γράφουμε $f : G \xrightarrow{\cong} H$.

3.5.15 Παράδειγμα. Όπως είδαμε στο εδάφιο 3.5.8 (vi), η $(\mathbb{C}\setminus\{0\},\cdot)$ εμφυτεύεται στη γενική γραμμική ομάδα $\mathrm{GL}_2(\mathbb{R})$.

▸ **Μελέτη συμπεριφοράς υποομάδων μέσω ομομορφισμών ομάδων**. Ξεκινούμε με δύο θεμελιώδεις προτάσεις.

3.5.16 Πρόταση. *Έστω $f:(G,\cdot)\longrightarrow(H,*)$ ένας ομομορφισμός ομάδων. Εάν υποθέσουμε ότι $K\sqsubseteq G$ και $L\sqsubseteq H$, τότε ισχύουν τα ακόλουθα:*
(i) $f(K\cap f^{-1}(L))=f(K)\cap L$.
(ii) $f(f^{-1}(L))=\mathrm{Im}(f)\cap L$.

Απόδειξη. (i) Σύμφωνα με το (iii) της προτάσεως 1.2.4,

$$f\left(f^{-1}\left(L\right)\right)\subseteq L.$$

Επειδή οι σχέσεις εγκλεισμού παραμένουν εν ισχύ κατόπιν εφαρμογής της απεικονίσεως f, έχουμε

$$\left.\begin{array}{r} f\left(K\cap f^{-1}\left(L\right)\right)\subseteq f(K)\\ f\left(K\cap f^{-1}\left(L\right)\right)\subseteq f\left(f^{-1}\left(L\right)\right)\end{array}\right\}\Longrightarrow f\left(K\cap f^{-1}\left(L\right)\right)\subseteq f(K)\cap L.$$

Έστω τώρα τυχόν $h\in f(K)\cap L$. Προφανώς, $h\in L$ και $h=f(g)$ για κάποιο στοιχείο $g\in K$. Επειδή $f(g)\in L\Rightarrow g\in f^{-1}(L)$, έχουμε $h\in f\left(K\cap f^{-1}\left(L\right)\right)$, οπότε ισχύει και ο αντίστροφος εγκλεισμός $f(K)\cap L\subseteq f\left(K\cap f^{-1}\left(L\right)\right)$.
(ii) Αρκεί να εφαρμοσθεί το (i) στην ειδική περίπτωση όπου $K=G$. □

3.5.17 Πρόταση. *Εάν η $f:(G,\cdot)\longrightarrow(H,*)$ είναι ένας ομομορφισμός ομάδων, τότε ισχύουν τα ακόλουθα*:
(i) *Εάν $K\sqsubseteq G$, τότε η εικόνα της $f\left(K\right)$ μέσω της f είναι μια υποομάδα της $f\left(G\right)$.*
(ii) *Εάν $L\sqsubseteq H$, τότε η αντίστροφη εικόνα της $f^{-1}\left(L\right)=\{g\in G\mid f(g)\in L\}$ μέσω της f είναι μια υποομάδα της G έχουσα τον πυρήνα $\mathrm{Ker}(f)$ της f ως υποομάδα της.*

Απόδειξη. (i) Κατά το (i) τού λήμματος 3.5.4 η εικόνα $f\left(G\right)$ της G μέσω της f αποτελεί μια υποομάδα της H. Επειδή το ουδέτερο στοιχείο e_G της G απεικονίζεται μέσω της f στο ουδέτερο στοιχείο της H (που ταυτίζεται με το ουδέτερο στοιχείο της $f\left(G\right)$), έχουμε $e_H\in f\left(K\right)$. Εξάλλου, εάν $u,v\in f\left(K\right)$, τότε υπάρχουν στοιχεία $x,y\in K$ με $f(x)=u$ και $f(y)=v$. Κατά συνέπειαν,

$$u*v^{-1}=f(x)*f(y)^{-1}=f(x)*f(y^{-1})=f(xy^{-1})\in f(K),$$

οπότε η $f\left(K\right)$ είναι μια υποομάδα της H δυνάμει τού (iii) της προτάσεως 3.2.16.
(ii) Επειδή το ουδέτερο στοιχείο e_G της G απεικονίζεται μέσω της f στο ουδέτερο στοιχείο της $\mathrm{Im}(f)$ (που ταυτίζεται με το ουδέτερο στοιχείο της ομάδας L), έχουμε $e_G\in f^{-1}\left(L\right)$. Εξάλλου, εάν $x,y\in f^{-1}\left(L\right)$, τότε ισχύει

$$f(xy^{-1})=f(x)*f(y^{-1})=f(x)*f(y)^{-1}\in L,$$

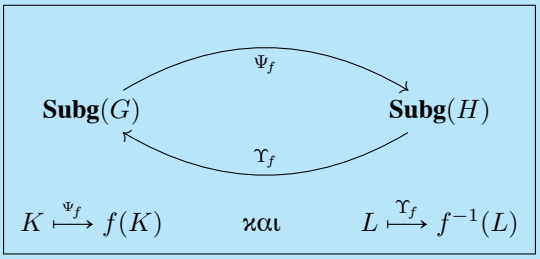
διότι η L είναι υποομάδα της H. Συνεπώς $xy^{-1}\in f^{-1}\left(L\right)$ και αρκεί να εφαρμόσουμε εκ νέου το (iii) της προτάσεως 3.2.16. Τέλος, επειδή

$$\{e_H\}\subseteq L\Rightarrow\mathrm{Ker}(f)=f^{-1}(\{e_H\})\subseteq f^{-1}\left(L\right),$$

έχουμε $\mathrm{Ker}(f)\sqsubseteq G$, $\mathrm{Ker}(f)\subseteq f^{-1}\left(L\right)\underset{3.2.20}{\Longrightarrow}\mathrm{Ker}(f)\sqsubseteq f^{-1}\left(L\right)$. □

Μέσω οιουδήποτε ομομορφισμού ομάδων κατασκευάζονται ισότονες απεικονίσεις μεταξύ των αντιστοίχων συνδέσμων υποομάδων, έχουσες ενδιαφέρουσες ιδιότητες (που αποτυπώνονται στα πορίσματα 3.5.18 και 3.5.20).

3.5.18 Πόρισμα (1ο θεώρημα αντιστοιχίσεως υποομάδων μέσω ομομορφισμών). *Εάν* $f : (G, \cdot) \longrightarrow (H, *)$ *είναι ένας ομομορφισμός ομάδων, τότε μεταξύ των (υποκειμένων συνόλων των) συνδέσμων* $(\mathbf{Subg}(G), \sqsubseteq)$ *και* $(\mathbf{Subg}(H), \sqsubseteq)$ *ορίζονται απεικονίσεις*



οι οποίες έχουν τις εξής ιδιότητες:

(i) $H\ \Psi_f$ *είναι ισότονη και* $\Psi_f(K) \sqsubseteq \mathrm{Im}(f)$ *για κάθε* $K \in \mathbf{Subg}(G)$.

(ii) $H\ \Upsilon_f$ *είναι ισότονη και* $\mathrm{Ker}(f) \sqsubseteq \Upsilon_f(L)$ *για κάθε* $L \in \mathbf{Subg}(H)$.

(iii) *Για κάθε* $K \in \mathbf{Subg}(G)$ *έχουμε*

$$(\Upsilon_f \circ \Psi_f)(K) = K \vee \mathrm{Ker}(f) = \langle K, \mathrm{Ker}(f) \rangle . \tag{3.15}$$

(iv) *Για κάθε* $L \in \mathbf{Subg}(H)$ *έχουμε*

$$(\Psi_f \circ \Upsilon_f)(L) = L \wedge \mathrm{Im}(f) = L \cap \mathrm{Im}(f). \tag{3.16}$$

(v) $\Psi_f(K_1 \cap K_2) \sqsubseteq \Psi_f(K_1) \cap \Psi_f(K_2)$, $\forall (K_1, K_2) \in \mathbf{Subg}(G) \times \mathbf{Subg}(G)$, *ισχύουσα ως ισότητα όταν η* Ψ_f *είναι ένριψη.*

(vi) $\Psi_f(\langle K_1, K_2 \rangle) = \langle \Psi_f(K_1), \Psi_f(K_2) \rangle$, $\forall (K_1, K_2) \in \mathbf{Subg}(G) \times \mathbf{Subg}(G)$.

(vii) $\Upsilon_f(L_1 \cap L_2) = \Upsilon_f(L_1) \cap \Upsilon_f(L_2)$, $\forall (L_1, L_2) \in \mathbf{Subg}(H) \times \mathbf{Subg}(H)$.

(viii) $\langle \Upsilon_f(L_1), \Upsilon_f(L_2) \rangle \sqsubseteq \Upsilon_f(\langle L_1, L_2 \rangle)$, $\forall (L_1, L_2) \in \mathbf{Subg}(H) \times \mathbf{Subg}(H)$, *ισχύουσα ως ισότητα όταν ο* f *είναι επιμορφισμός.*

(ix) *Ο* f *είναι μονομορφισμός* $\Leftrightarrow$ *η* Ψ_f *είναι ένριψη* $\Leftrightarrow$ *η* Υ_f *είναι επίρριψη.*

(x) *Ο* f *είναι επιμορφισμός* $\Leftrightarrow$ *η* Ψ_f *είναι επίρριψη* $\Leftrightarrow$ *η* Υ_f *είναι ένριψη.*

(xi) *Ο* f *είναι ισομορφισμός* $\Leftrightarrow$ *η* Ψ_f *είναι αμφίρριψη* $\Leftrightarrow$ *η* Υ_f *είναι αμφίρριψη.*

Απόδειξη. (i) Από το (i) της προτάσεως 3.5.17 έχουμε $\Psi_f(K) \sqsubseteq \mathrm{Im}(f)$ για κάθε $K \in \mathbf{Subg}(G)$ και για κάθε ζεύγος $(K_1, K_2) \in \mathbf{Subg}(G) \times \mathbf{Subg}(G)$ με $K_1 \sqsubseteq K_2$,

$$\left.\begin{array}{c} K_1 \subseteq K_2 \Rightarrow f(K_1) = \Psi_f(K_1) \subseteq \Psi_f(K_2) = f(K_2) \\ K_2 \sqsubseteq G \Rightarrow \Psi_f(K_2) = f(K_2) \sqsubseteq \mathrm{Im}(f) \end{array}\right\} \underset{3.2.20}{\Longrightarrow} \Psi_f(K_1) \sqsubseteq \Psi_f(K_2).$$

(ii) Από το (ii) της προτάσεως 3.5.17 έχουμε $\mathrm{Ker}(f) \sqsubseteq \Upsilon_f(L)$ για κάθε $L \in \mathbf{Subg}(H)$ και για κάθε ζεύγος $(L_1, L_2) \in \mathbf{Subg}(H) \times \mathbf{Subg}(H)$ με $L_1 \sqsubseteq L_2$,

$$\left.\begin{array}{c} L_1 \subseteq L_2 \Rightarrow f^{-1}(L_1) = \Upsilon_f(L_1) \subseteq \Upsilon_f(L_2) = f^{-1}(L_2) \\ L_2 \sqsubseteq H \Rightarrow \Upsilon_f(L_2) = f^{-1}(L_2) \sqsubseteq G \end{array}\right\} \underset{3.2.20}{\Longrightarrow} \Upsilon_f(L_1) \sqsubseteq \Upsilon_f(L_2).$$

(iii) Για κάθε $K \in \mathbf{Subg}(G)$ έχουμε (από γνωστό εγκλεισμό από τη Θεωρία Συνόλων)

$$(\Upsilon_f \circ \Psi_f)(K) = \Upsilon_f(\Psi_f(K)) = f^{-1}(f(K)) \supseteq K.$$

Από την άλλη μεριά (επειδή $f(K) \sqsubseteq H$) η $f^{-1}(f(K))$ είναι μια υποομάδα τής G περιέχουσα τον πυρήνα $\mathrm{Ker}(f)$ τού ομομορφισμού f. (Βλ. 3.5.17 (ii).) Επομένως, $\langle K,\ \mathrm{Ker}(f) \rangle \sqsubseteq \Upsilon_f(\Psi_f(K))$. Και αντιστρόφως· εάν θεωρήσουμε τυχόν στοιχείο

$y \in \Upsilon_f(\Psi_f(K)) = f^{-1}(f(K))$, τότε $f(y) \in f(K)$, οπότε υπάρχει κάποιο $x \in K$ με

$$f(y) = f(x) \Rightarrow f(x^{-1}y) = e_H \Rightarrow x^{-1}y = z \in \mathrm{Ker}(f) \Rightarrow y = xz \in \langle K,\ \mathrm{Ker}(f)\rangle,$$

κάτι που σημαίνει ότι $\Upsilon_f(\Psi_f(K)) \subseteq \langle K,\ \mathrm{Ker}(f)\rangle$. Άρα η (3.15) είναι αληθής.
(iv) Για κάθε $L \in \mathbf{Subg}(H)$ η (3.16) είναι ωσαύτως αληθής, διότι από το (ii) τής προτάσεως 3.5.16 έπεται ότι

$$(\Psi_f \circ \Upsilon_f)(L) = \Psi_f(\Upsilon_f(L)) = f(f^{-1}(L)) = L \cap \mathrm{Im}(f).$$

(v) Για κάθε ζεύγος $(K_1, K_2) \in \mathbf{Subg}(G) \times \mathbf{Subg}(G)$ λαμβάνουμε (λόγω τού (i))

$$\left.\begin{array}{l} K_1 \cap K_2 \sqsubseteq K_1 \\ K_1 \cap K_2 \sqsubseteq K_2 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \Psi_f(K_1 \cap K_2) \sqsubseteq \Psi_f(K_1) \\ \Psi_f(K_1 \cap K_2) \sqsubseteq \Psi_f(K_1) \end{array}\right\} \Rightarrow \Psi_f(K_1 \cap K_2) \sqsubseteq \Psi_f(K_1) \cap \Psi_f(K_2).$$

Ως γνωστόν, όταν η Ψ_f είναι ένριψη ισχύει $\Psi_f(K_1 \cap K_2) = \Psi_f(K_1) \cap \Psi_f(K_2)$.
(vi) Για κάθε ζεύγος $(K_1, K_2) \in \mathbf{Subg}(G) \times \mathbf{Subg}(G)$ λαμβάνουμε (λόγω τού (i))

$$\left.\begin{array}{l} K_1 \sqsubseteq \langle K_1, K_2\rangle \\ K_2 \sqsubseteq \langle K_1, K_2\rangle \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \Psi_f(K_1) \sqsubseteq \Psi_f(\langle K_1, K_2\rangle) \\ \Psi_f(K_2) \sqsubseteq \Psi_f(\langle K_1, K_2\rangle) \end{array}\right\} \Rightarrow \langle \Psi_f(K_1), \Psi_f(K_2)\rangle \sqsubseteq \Psi_f(\langle K_1, K_2\rangle). \tag{3.17}$$

Επιπροσθέτως (λόγω τού (ii) και τής ισότητας (3.15))

$$\begin{aligned} &\Psi_f(K_1) = f(K_1) \sqsubseteq \langle \Psi_f(K_1), \Psi_f(K_2)\rangle \\ \Rightarrow\ &K_1 \sqsubseteq \langle K_1,\ \mathrm{Ker}(f)\rangle = (\Upsilon_f \circ \Psi_f)(K_1) \sqsubseteq \Upsilon_f(\langle \Psi_f(K_1), \Psi_f(K_2)\rangle) \end{aligned}$$

και, κατ' αναλογίαν, $K_2 \sqsubseteq \Upsilon_f(\langle \Psi_f(K_1), \Psi_f(K_2)\rangle)$, οπότε (από το εδ. 3.3.2,το (i) και την ισότητα (3.16))

$$\begin{aligned} &\langle K_1, K_2\rangle \sqsubseteq \Upsilon_f(\langle \Psi_f(K_1), \Psi_f(K_2)\rangle) \\ \Rightarrow\ &\Psi_f(\langle K_1, K_2\rangle) \sqsubseteq (\Psi_f \circ \Upsilon_f)(\langle \Psi_f(K_1), \Psi_f(K_2)\rangle) = \langle \Psi_f(K_1), \Psi_f(K_2)\rangle \cap \mathrm{Im}(f). \end{aligned}$$

Επειδή $\langle \Psi_f(K_1), \Psi_f(K_2)\rangle = \langle f(K_1), f(K_2)\rangle \sqsubseteq \mathrm{Im}(f)$, η τελευταία σχέση δίδει

$$\Psi_f(\langle K_1, K_2\rangle) \sqsubseteq \langle \Psi_f(K_1), \Psi_f(K_2)\rangle. \tag{3.18}$$

Εκ των (3.17) και (3.18) έπεται η ισότητα $\Psi_f(\langle K_1, K_2\rangle) = \langle \Psi_f(K_1), \Psi_f(K_2)\rangle$.
(vii) Τούτο είναι προφανές (για αμιγώς συνολοθεωρητικούς λόγους).
(viii) Για κάθε ζεύγος $(L_1, L_2) \in \mathbf{Subg}(H) \times \mathbf{Subg}(H)$ λαμβάνουμε (λόγω τού (ii))

$$\left.\begin{array}{l} L_1 \sqsubseteq \langle L_1, L_2\rangle \\ L_2 \sqsubseteq \langle L_1, L_2\rangle \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \Upsilon_f(L_1) \sqsubseteq \Upsilon_f(\langle L_1, L_2\rangle) \\ \Upsilon_f(L_2) \sqsubseteq \Upsilon_f(\langle L_1, L_2\rangle) \end{array}\right\} \Rightarrow \langle \Upsilon_f(L_1), \Upsilon_f(L_2)\rangle \sqsubseteq \Upsilon_f(\langle L_1, L_2\rangle).$$

Όταν ο f είναι *επιμορφισμός*, έχουμε για $j \in \{1, 2\}$

$$(\Psi_f \circ \Upsilon_f)(L_j) = L_j \cap \mathrm{Im}(f) = L_j \ \text{ και } \ \mathrm{Ker}(f) \sqsubseteq \Upsilon_f(L_j),$$

οπότε

$$\begin{aligned} &\Upsilon_f(\langle L_1, L_2\rangle) = \Upsilon_f(\langle (\Psi_f \circ \Upsilon_f)(L_1), (\Psi_f \circ \Upsilon_f)(L_2)\rangle) \\ &\underset{\text{(vi)}}{=} (\Upsilon_f \circ \Psi_f)(\langle \Upsilon_f(L_1), \Upsilon_f(L_2)\rangle) \underset{(3.15)}{=} \langle\langle \Upsilon_f(L_1), \Upsilon_f(L_2)\rangle, \mathrm{Ker}(f)\rangle \\ &= \langle \Upsilon_f(L_1), \Upsilon_f(L_2)\rangle, \end{aligned}$$

διότι $\mathrm{Ker}(f) \sqsubseteq \Upsilon_f(L_j) \sqsubseteq \langle \Upsilon_f(L_1), \Upsilon_f(L_2)\rangle$.
(ix) Εάν ο f είναι μονομορφισμός, τότε $\mathrm{Ker}(f) = \{e_G\}$ (βλ. 3.5.12) και

$$[(\Upsilon_f \circ \Psi_f)(K) = \langle K, \mathrm{Ker}(f)\rangle = K,\ \forall K \in \mathbf{Subg}(G)] \Rightarrow \Upsilon_f \circ \Psi_f = \mathrm{id}_{\mathbf{Subg}(G)},$$

απ' όπου έπεται ότι η Ψ_f είναι ένριψη και η Υ_f είναι επίριψη. Εάν υποτεθεί ότι η Ψ_f είναι ένριψη, τότε

$$\Psi_f(\mathrm{Ker}(f)) = f(\mathrm{Ker}(f)) = \{e_H\} = f(\{e_G\}) = \Psi_f(\{e_G\}),$$

οπότε $\mathrm{Ker}(f) = \{e_G\} \underset{3.5.12}{\Longrightarrow} f$ μονομορφισμός. Τέλος, εάν υποτεθεί ότι η Υ_f είναι επίριψη, τότε

$$\left.\begin{array}{r} \{e_G\} \in \mathbf{Subg}(G) \Rightarrow [\exists L \in \mathbf{Subg}(H) : \Upsilon_f(L) = \{e_G\}] \\ \mathrm{Ker}(f) \sqsubseteq \Upsilon_f(L) \end{array}\right\} \Rightarrow \mathrm{Ker}(f) = \{e_G\},$$

οπότε ο f είναι κατ' ανάγκην μονομορφισμός.

(x) Εάν ο f είναι επιμορφισμός, τότε $\mathrm{Im}(f) = H$ και

$$[(\Psi_f \circ \Upsilon_f)(L) = L \cap \mathrm{Im}(f) = L,\ \forall L \in \mathbf{Subg}(H)] \Rightarrow \Psi_f \circ \Upsilon_f = \mathrm{id}_{\mathbf{Subg}(H)},$$

απ' όπου έπεται ότι η Υ_f είναι ένριψη και η Ψ_f είναι επίριψη. Εάν υποτεθεί ότι η Ψ_f είναι επίριψη, τότε για κάθε $y \in H$ έχουμε

$$\langle y\rangle \in \mathbf{Subg}(H) \Rightarrow [\exists K \in \mathbf{Subg}(K) : \Psi_f(K) = f(K) = \langle y\rangle] \Rightarrow y \in f(K) \subseteq \mathrm{Im}(f),$$

οπότε $\mathrm{Im}(f) = H \Longrightarrow f$ επιμορφισμός. Τέλος, εάν υποτεθεί ότι η Υ_f είναι ένριψη, τότε για κάθε $y \in H$ έχουμε

$$\Upsilon_f(\langle y\rangle) = \{x \in G \,|\, f(x) \in \langle y\rangle\} = \{x \in G \,|\, f(x) \in \langle y\rangle \cap \mathrm{Im}(f)\} = \Upsilon_f(\langle y\rangle \cap \mathrm{Im}(f)),$$

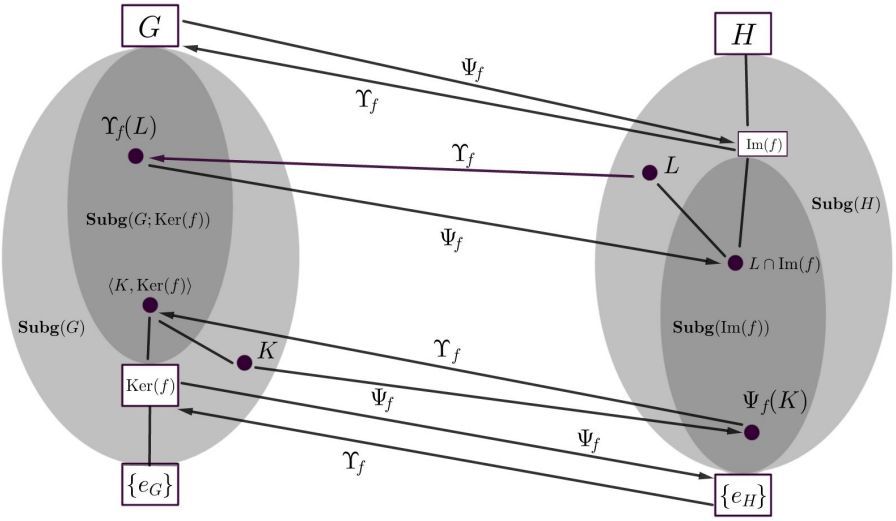
οπότε

$$\langle y\rangle = \langle y\rangle \cap \mathrm{Im}(f) \Rightarrow \langle y\rangle \subseteq \mathrm{Im}(f) \Rightarrow y \in \mathrm{Im}(f).$$

Αυτό όμως σημαίνει ότι $\mathrm{Im}(f) = H \Longrightarrow f$ επιμορφισμός.

(xi) Τούτο έπεται άμεσα από τα (ix) και (x). □

3.5.19 Σημείωση. Το τι συμβαίνει ύστερα από εφαρμογή των Ψ_f και Υ_f εικονογραφείται ως ακολούθως:



Επισημαίνεται ότι όταν ο f είναι μονομορφισμός, τότε -σε επίπεδο συνδέσμων- η επαγόμενη απεικόνιση $\Psi_f : \mathbf{Subg}(G) \longrightarrow \mathbf{Subg}(H)$ είναι ισότονη και ενριπτική, έχουσα εικόνα $\mathrm{Im}(\Psi_f) = \mathbf{Subg}(\mathrm{Im}(f))$. Και αντιστοίχως, όταν ο f είναι επιμορφισμός, η επαγόμενη απεικόνιση $\Upsilon_f : \mathbf{Subg}(H) \longrightarrow \mathbf{Subg}(G)$ είναι ωσαύτως ισότονη

και ενριπτική, έχουσα εικόνα $\mathrm{Im}(\Upsilon_f) = \mathbf{Subg}(G;\mathrm{Ker}(f))$. Το πόρισμα 3.5.20 αποσαφηνίζει και -ταυτοχρόνως- γενικεύει αυτές τις ιδιότητες για *τυχόντες ομομορφισμούς* (μέσω των οποίων επάγονται ισομορφισμοί μεταξύ των υποσυνδέσμων των παριστώμενων με σκούρο γκρι χρώμα στο ανωτέρω σχήμα).

3.5.20 Πόρισμα (2ο θεώρημα αντιστοιχίσεως υποομάδων μέσω ομομορφισμών). *Εάν $f : (G,\cdot) \longrightarrow (H,*)$ είναι ένας ομομορφισμός ομάδων, τότε ορίζεται η απεικόνιση*

$$\boxed{\mathbf{Subg}(G;\mathrm{Ker}(f)) \ni K \overset{\bar{\Psi}_f}{\longmapsto} f(K) \in \mathbf{Subg}(\mathrm{Im}(f))}$$

από το σύνολο $\mathbf{Subg}(G;\mathrm{Ker}(f))$ των υποομάδων της G που περιέχουν τον πυρήνα της f στο σύνολο $\mathbf{Subg}(\mathrm{Im}(f))$ των υποομάδων της εικόνας $\mathrm{Im}(f)$ της f. Η $\bar{\Psi}_f$ είναι αμφιρριπτική έχουσα την

$$\boxed{\mathbf{Subg}(\mathrm{Im}(f)) \ni L \overset{\bar{\Upsilon}_f}{\longmapsto} f^{-1}(L) \in \mathbf{Subg}(G;\mathrm{Ker}(f))}$$

ως αντίστροφό της. (Ειδικότερα, κάθε υποομάδα της $\mathrm{Im}(f)$ οφείλει να είναι της μορφής $f(K)$, όπου K μια υποομάδα της G που περιέχει τον πυρήνα της f.) Επιπροσθέτως, ισχύουν τα ακόλουθα:

(i) *Για $K_1, K_2 \in \mathbf{Subg}(G;\mathrm{Ker}(f))$ αληθεύει η κάτωθι αμφίπλευρη συνεπαγωγή*

$$K_1 \sqsubseteq K_2 \Longleftrightarrow \bar{\Psi}_f(K_1) \sqsubseteq \bar{\Psi}_f(K_2).$$

(ii) *Η $\bar{\Psi}_f$ καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων*

$$(\mathbf{Subg}(G;\mathrm{Ker}(f)),\sqsubseteq) \quad \textit{και} \quad (\mathbf{Subg}(\mathrm{Im}(f)),\sqsubseteq)$$

(βλ. 3.2.30, 3.2.32, και 1.4.26).

(iii) $\bar{\Psi}_f(K_1 \cap K_2) = \bar{\Psi}_f(K_1) \cap \bar{\Psi}_f(K_2),\ \forall (K_1,K_2) \in \mathbf{Subg}(G;\mathrm{Ker}(f))^2$.

(iv) $\bar{\Psi}_f(\langle K_1,K_2\rangle) = \langle \bar{\Psi}_f(K_1), \bar{\Psi}_f(K_2)\rangle,\ \forall (K_1,K_2) \in \mathbf{Subg}(G;\mathrm{Ker}(f))^2$.

(v) *Για $L_1, L_2 \in \mathbf{Subg}(\mathrm{Im}(f))$ αληθεύει η κάτωθι αμφίπλευρη συνεπαγωγή*

$$L_1 \sqsubseteq L_2 \Longleftrightarrow \bar{\Upsilon}_f(L_1) \sqsubseteq \bar{\Upsilon}_f(L_2).$$

(vi) *Η $\bar{\Psi}_f$ καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων*

$$(\mathbf{Subg}(\mathrm{Im}(f)),\sqsubseteq) \quad \textit{και} \quad (\mathbf{Subg}(G;\mathrm{Ker}(f)),\sqsubseteq).$$

(vii) $\bar{\Upsilon}_f(L_1 \cap L_2) = \bar{\Upsilon}_f(L_1) \cap \bar{\Upsilon}_f(L_2),\ \forall (L_1,L_2) \in \mathbf{Subg}(\mathrm{Im}(f))^2$.

(viii) $\bar{\Upsilon}_f(\langle L_1,L_2\rangle) = \langle \bar{\Upsilon}_f(L_1), \bar{\Upsilon}_f(L_2)\rangle,\ \forall (L_1,L_2) \in \mathbf{Subg}(\mathrm{Im}(f))^2$.

Απόδειξη. Το ότι οι περιορισμοί[46]

$$\bar{\Psi}_f : \mathbf{Subg}(G;\mathrm{Ker}(f)) \longrightarrow \mathbf{Subg}(\mathrm{Im}(f)) \ \text{ και } \ \bar{\Upsilon}_f : \mathbf{Subg}(\mathrm{Im}(f)) \longrightarrow \mathbf{Subg}(G;\mathrm{Ker}(f))$$

είναι «καλώς ορισμένοι» έπεται από την πρόταση 3.5.17. Ας θεωρήσουμε τυχούσα $K \in \mathbf{Subg}(G;\mathrm{Ker}(f))$. Προφανώς,

$$\left(\bar{\Upsilon}_f \circ \bar{\Psi}_f\right)(K) = \left(\Upsilon_f \circ \Psi_f\right)(K) = \Upsilon_f(\Psi_f(K)) = \langle K, \mathrm{Ker}(f)\rangle = K,$$

οπότε $\bar{\Upsilon}_f \circ \bar{\Psi}_f = \mathrm{id}_{\mathbf{Subg}(G;\mathrm{Ker}(f))}$. Έστω τώρα τυχούσα $L \in \mathbf{Subg}(\mathrm{Im}(f))$. Προφανώς,

$$\left.\begin{array}{r} \left(\bar{\Psi}_f \circ \bar{\Upsilon}_f\right)(L) = \left(\Psi_f \circ \Upsilon_f\right)(L) = L \cap \mathrm{Im}(f) \\ L \sqsubseteq \mathrm{Im}(f) \Rightarrow L \cap \mathrm{Im}(f) = L \end{array}\right\} \Rightarrow \left(\bar{\Psi}_f \circ \bar{\Upsilon}_f\right)(L) = L,$$

[46] Προφανώς, $\bar{\Psi}_f := \Psi_f|_{(\mathbf{Subg}(G;\mathrm{Ker}(f)),\mathbf{Subg}(\mathrm{Im}(f)))}$ και $\bar{\Upsilon}_f := \Upsilon_f|_{(\mathbf{Subg}(\mathrm{Im}(f)),\mathbf{Subg}(G;\mathrm{Ker}(f)))}$. (Βλ. 1.2.6.)

οπότε $\bar{\Psi}_f \circ \bar{\Upsilon}_f = \mathrm{id}_{\mathbf{Subg}(\mathrm{Im}(f))}$. Εκ των ανωτέρω συνάγεται ότι η $\bar{\Psi}_f$ είναι αμφιριπτική έχουσα την $\bar{\Upsilon}_f$ ως αντίστροφό της.

(i) Για οιαδήποτε ζεύγη $(K_1, K_2) \in \mathbf{Subg}(G; \mathrm{Ker}(f))^2$ με $K_1 \sqsubseteq K_2$ έχουμε

$$\bar{\Psi}_f(K_1) = \Psi_f(K_1) \underset{3.5.18\,\text{(i)}}{\sqsubseteq} \Psi_f(K_2) = \bar{\Psi}_f(K_2).$$

Επίσης, για οιαδήποτε $(K_1, K_2) \in \mathbf{Subg}(G; \mathrm{Ker}(f))^2$ με $\bar{\Psi}_f(K_1) \sqsubseteq \bar{\Psi}_f(K_2)$ έχουμε

$$\bar{\Upsilon}_f\left(\bar{\Psi}_f(K_1)\right) = K_1 \sqsubseteq K_2 = \bar{\Upsilon}_f\left(\bar{\Psi}_f(K_2)\right).$$

(ii) Λόγω τού (i) αμφότερες οι $\bar{\Psi}_f$ και $\bar{\Upsilon}_f$ είναι ισότονες, οπότε η $\bar{\Psi}_f$ καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων $(\mathbf{Subg}(G; \mathrm{Ker}(f)), \sqsubseteq)$ και $(\mathbf{Subg}(\mathrm{Im}(f)), \sqsubseteq)$ (βλ. 1.4.26). Άπαξ και έχουμε αποδείξει ότι το (ii) αληθεύει, αληθεύουν και τα (iii) και (iv), διότι καθένα εξ αυτών είναι ισοδύναμο με το (ii) επί τη βάσει τής προτάσεως 1.4.27. Τα (v)-(viii) αποδεικνύονται παρομοίως (ύστερα από εναλλαγή των ρόλων των $\bar{\Psi}_f$ και $\bar{\Upsilon}_f$). □

3.5.21 Παρατήρηση. Έστω $f : (G, \cdot) \longrightarrow (H, *)$ ένας ομομορφισμός ομάδων. Σύμφωνα με το (xi) τού πορίσματος 3.5.18, ο f είναι ισομορφισμός ομάδων εάν και μόνον εάν οι Ψ_f και Υ_f είναι ισομορφισμοί συνδέσμων μεταξύ των $(\mathbf{Subg}(G), \sqsubseteq)$ και $(\mathbf{Subg}(H), \sqsubseteq)$. Όμως ακόμη και όταν ο f *δεν* είναι ισομορφισμός, οι *περιορισμοί* $\bar{\Psi}_f$ και $\bar{\Upsilon}_f$ καθορίζουν, βάσει τού (ii) τού πορίσματος 3.5.20, ισομορφισμούς συνδέσμων μεταξύ των $(\mathbf{Subg}(G; \mathrm{Ker}(f)), \sqsubseteq)$ και $(\mathbf{Subg}(\mathrm{Im}(f)), \sqsubseteq)$.

▸ **Ιδιότητες ομάδων που διατηρούνται μέσω ισομορφισμών**. Οι πρώτες εξ αυτών παρατίθενται στην ακόλουθη:

3.5.22 Πρόταση. *Έστω $f : (G, \cdot) \longrightarrow (H, *)$ ένας ισομορφισμός ομάδων. Τότε ισχύουν τα ακόλουθα*:

(i) $|G| = |H|$.

(ii) *Η G είναι αβελιανή εάν και μόνον εάν η H είναι αβελιανή.*

(iii) *Η G είναι κυκλική εάν και μόνον εάν η H είναι κυκλική.*

(iv) $\mathrm{ord}(g) = \mathrm{ord}(f(g)), \forall g \in G$.

(v) *Εάν η G είναι περιοδική (δηλαδή εάν κάθε στοιχείο τής G έχει πεπερασμένη τάξη, βλ. 3.4.1 (i)), τότε και η H είναι περιοδική (και τανάπαλιν).*

Απόδειξη. (i) Τούτο είναι προφανές λόγω τής αμφιρριπτικότητας τής f.

(ii) Εάν η G είναι αβελιανή και $h, h' \in H$, τότε υπάρχουν $g, g' \in G$, τέτοια ώστε $h = f(g)$ και $h' = f(g')$. Επομένως,

$$h * h' = f(g) * f(g') = f(gg') = f(g'g) = f(g') * f(g) = h' * h,$$

και η H είναι, ως εκ τούτου, αβελιανή. Το αντίστροφο αποδεικνύεται παρομοίως.

(iii) Εάν $\exists g \in G : G = \langle g \rangle$, τότε, λόγω τής επιρριπτικότητας τής f, για *κάθε* $h \in H$ υπάρχει $\nu \in \mathbb{Z}$ με $h = f(g^\nu)$, οπότε από το (iii) τής προτάσεως 3.5.3 συμπεραίνουμε ότι

$$\left.\begin{array}{l} h = f(g)^\nu \Rightarrow H \subseteq \langle f(g) \rangle \\ f(g) \in H \Rightarrow \langle f(g) \rangle \subseteq H \end{array}\right\} \Longrightarrow H = \langle f(g) \rangle.$$

Το αντίστροφο αποδεικνύεται παρομοίως.

(iv) Έστω $g \in G$ τάξεως $\mathrm{ord}(g) = n \in \mathbb{N}$. Τότε $\mathrm{ord}(f(g)) = m \in \mathbb{N}$ και $m \mid n$. (Βλ. 3.5.3 (iv).) Επειδή

$$f(g)^m = f(g^m) = e_H \underset{3.4.8}{\Longrightarrow} g^m \in \mathrm{Ker}(f) = \{e_G\} \Rightarrow g^m = e_G \Rightarrow n \mid m,$$

έχουμε τελικώς $m = n$. Εάν $\mathrm{ord}(g) = \infty$, τότε $g^\nu \neq e_G$ για κάθε $\nu \in \mathbb{N}$, οπότε η ενριπτικότητα τής f μας οδηγεί στο συμπέρασμα ότι $(f(g))^\nu \neq e_H$ για κάθε $\nu \in \mathbb{N}$, απ' όπου έπεται ότι $\mathrm{ord}(f(g)) = \infty$.

(v) Εάν κάθε στοιχείο g τής G έχει πεπερασμένη τάξη, τότε $\exists n_g \in \mathbb{N} : g^{n_g} = e_G$. Για οιοδήποτε στοιχείο $h \in H$ υπάρχει $x \in G : h = f(x)$, οπότε μέσω των (i) και (iii) τής προτάσεως 3.5.3 συνάγεται ότι

$$h^{n_x} = f(x)^{n_x} = f(x^{n_x}) = f(e_G) = e_H \Rightarrow \mathrm{ord}(h) < \infty.$$

Το αντίστροφο αποδεικνύεται παρομοίως. □

3.5.23 Παραδείγματα. (i) Είναι αδύνατον να υφίσταται ισομορφισμός μεταξύ των ομάδων $(\mathbb{Z}, +)$ και $(\mathbb{Q}, +)$, διότι η πρώτη εξ αυτών είναι κυκλική και η δεύτερη μη κυκλική (βλ. 3.3.16 (i) και (v)).

(ii) Αμφότερες οι ομάδες $(\mathbb{Z}_8^\times, \cdot)$ και $(\mathbb{Z}_{10}^\times, \cdot)$ έχουν τάξη 4. (Βλ. 3.2.7 (ii).) Ωστόσο, $\mathbb{Z}_{10}^\times \ncong \mathbb{Z}_8^\times$. Πράγματι· εάν υπήρχε ισομορφισμός

$$\{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\} = \mathbb{Z}_{10}^\times \xrightarrow{f} \mathbb{Z}_8^\times = \{[1]_8, [3]_8, [5]_8, [7]_8\},$$

τότε, λαμβάνοντας υπ' όψιν ότι $\mathrm{ord}([3]_{10}) = 4$ (διότι $[3]_{10}^2 = [9]_{10}$, $[3]_{10}^3 = [7]_{10}$, και $[3]_{10}^4 = [1]_{10}$), θα έπρεπε (λόγω τού 3.5.22 (iv)) να ισχύει $\mathrm{ord}(f([3]_{10})) = 4$, κάτι αδύνατον, καθόσον $\mathrm{ord}([1]_8) = 1$, $\mathrm{ord}([3]_8) = \mathrm{ord}([5]_8) = \mathrm{ord}([7]_8) = 2$. (Ένας εναλλακτικός τρόπος αποδείξεως τού ανωτέρω ισχυρισμού είναι ο εξής: Διαπιστώνουμε άμεσα ότι $\mathbb{Z}_{10}^\times = \langle [3]_{10} \rangle = \langle [7]_{10} \rangle$. Η $\mathbb{Z}_8^\times$ *δεν είναι κυκλική* ομάδα, διότι

$$\langle [1]_8 \rangle = \{[1]_8\},\ \langle [3]_8 \rangle = \{[1]_8, [3]_8\},\ \langle [5]_8 \rangle = \{[1]_8, [5]_8\},\ \langle [7]_8 \rangle = \{[1]_8, [7]_8\},$$

οπότε καταλήγουμε σε άτοπο μέσω τού (iii) τής προτάσεως 3.5.22.)

(iii) Η ομάδα $(\mathbb{C}\setminus\{0\}, \cdot)$ δεν είναι ισόμορφη τής $(\mathbb{R}\setminus\{0\}, \cdot)$. Πράγματι· εάν υπήρχε ισομορφισμός $f : \mathbb{C}\setminus\{0\} \longrightarrow \mathbb{R}\setminus\{0\}$, τότε, λαμβάνοντας υπ' όψιν ότι $\mathrm{ord}(i) = 4$ (όπου i η φανταστική μονάδα), θα έπρεπε (λόγω τού (iv) τής προτάσεως 3.5.22) να ισχύει $\mathrm{ord}(f(i)) = 4$, κάτι αδύνατον, καθόσον η εξίσωση $x^4 = 1$ έχει μόνον τις λύσεις ± 1 εντός τού $\mathbb{R}$ (με $\mathrm{ord}(1) = 1$, $\mathrm{ord}(-1) = 2$ στην $(\mathbb{R}\setminus\{0\}, \cdot)$).

3.5.24 Πρόταση. *Για οιεσδήποτε ομάδες* $(G_1, \cdot_1), (G_2, \cdot_2), (G_3, \cdot_3)$ *ισχύουν τα εξής*:
(i) $G_1 \cong G_1$,
(ii) $G_1 \cong G_2 \Rightarrow G_2 \cong G_1$,
(iii) $[G_1 \cong G_2$ *και* $G_2 \cong G_3] \Rightarrow G_1 \cong G_3$.

Απόδειξη. (i) Η ταυτοτική απεικόνιση $\mathrm{id}_{G_1} : G_1 \longrightarrow G_1$ είναι προφανώς ένας ισομορφισμός ομάδων.

(ii) Εάν ο $f : G_1 \longrightarrow G_2$ είναι ένας ισομορφισμός ομάδων, τότε, ως αμφιρριπτική απεικόνιση, διαθέτει μια (μονοσημάντως ορισμένη, αμφιρριπτική) αντίστροφο f^{-1}. Αρκεί λοιπόν να αποδειχθεί ότι η f^{-1} είναι ομομορφισμός ομάδων. Εάν $x, y \in G_2$, τότε υπάρχουν $a, b \in G_1$ με $x = f(a)$ και $y = f(b)$. Επομένως,

$$f^{-1}(x \cdot_2 y) = f^{-1}(f(a) \cdot_2 f(b)) = f^{-1}(f(a \cdot_1 b)) = a \cdot_1 b = f^{-1}(x) \cdot_1 f^{-1}(y),$$

(αφού οι f, f^{-1} είναι αμφιρριπτικές) και η f^{-1} αποτελεί ομομορφισμό ομάδων.

(iii) Εάν οι $f : G_1 \longrightarrow G_2$ και $g : G_2 \longrightarrow G_3$ είναι δυο ισομορφισμοί ομάδων, τότε, σύμφωνα με το (ii) τής προτάσεως 3.5.9, *και* η σύνθεσή τους $g \circ f$ είναι ένας ισομορφισμός ομάδων. □

3.5.25 Σημείωση. Σύμφωνα με την πρόταση 3.5.24, η διμελής σχέση "$\cong$" ορίζει μια σχέση ισοδυναμίας επί οιουδήποτε συνόλου απαρτιζομένου από ομάδες (ή επί τής NBG-«κλάσεως» *όλων* των ομάδων). Οι κλάσεις ισοδυναμίας ως προς την "$\cong$" ονομάζονται **κλάσεις ισομορφίας**. Δυο ομάδες λογίζονται ως (ομαδοθεωρητικώς) *ταυτιζόμενες* όταν είναι μεταξύ τους ισόμορφες, ήτοι όταν ανήκουν στην ίδια κλάση ισομορφίας. Ως εκ τούτου, ο ομαδοθεωρητικός προσδιορισμός μιας οικογενείας ομάδων, τα μέλη τής οποίας έχουν μια *ειδική* ιδιότητα, ισοδυναμεί με την *ταξινόμηση* των μελών της *μέχρις ισομορφισμού*[47].

‣ **Ταξινόμηση των κυκλικών ομάδων και των υποομάδων αυτών**. Το ακόλουθο θεώρημα μας παρέχει τη δυνατότητα πλήρους *ταξινομήσεως* των κυκλικών ομάδων *μέχρις ισομορφισμού*.

3.5.26 Θεώρημα (Ταξινόμηση κυκλικών ομάδων). *Έστω $(G,\cdot)$ μια κυκλική ομάδα. Τότε ισχύουν τα εξής*:

(i) *Εάν η $(G,\cdot)$ είναι άπειρη ομάδα, τότε είναι ισόμορφη με την $(\mathbb{Z},+)$.*

(ii) *Εάν η $(G,\cdot)$ είναι πεπερασμένη ομάδα τάξεως $m\in\mathbb{N}$, τότε $(G,\cdot)\cong(\mathbb{Z}_m,+)$.*

Απόδειξη. Έστω ότι η $(G,\cdot)$ έχει κάποιο $g\in G$ ως γεννήτορά της.

(i) Εάν η $(G,\cdot)$ είναι άπειρη κυκλική, τότε η επιρριπτική απεικόνιση

$$(\mathbb{Z},+)\longrightarrow(G,\cdot),\ \ n\longmapsto g^n,$$

είναι ένας ισομορφισμός ομάδων. Πράγματι· η απεικόνιση αυτή είναι *ενριπτική*, διότι εάν υπήρχαν $n,n'\in\mathbb{Z}$ με $n\neq n'$ και $g^n=g^{n'}$, τότε θα προέκυπτε η ισότητα

$$g^{\max\{n,n'\}-\min\{n,n'\}}=e_G,$$

απ' όπου θα συνήγετο ότι η G είναι πεπερασμένη ομάδα (βλ. πρόταση 3.3.18), κάτι που θα αντέφασκε προς την υπόθεσή μας. Επιπροσθέτως, η εν λόγω απεικόνιση είναι και *ομομορφισμός ομάδων*, διότι (σύμφωνα με το 3.2.11 (i)) έχουμε

$$g^{n+n'}=g^ng^{n'},\ \forall(n,n')\in\mathbb{Z}\times\mathbb{Z}.$$

(ii) Εάν η $(G,\cdot)$ είναι πεπερασμένη ομάδα τάξεως m, τότε $G=\{e,g,g^2,...,g^{m-1}\}$ (όπου $e=e_G$). Η

$$(\mathbb{Z}_m,+)\longrightarrow(G,\cdot),\ \ [n]_m\longmapsto g^n,\ \forall n\in\{0,1,...,m-1\},$$

είναι μια *καλώς ορισμένη* απεικόνιση, διότι θεωρώντας

$$n,n'\in\{0,1,...,m-1\}:[n]_m=\left[n'\right]_m,$$

υπάρχει $k\in\mathbb{Z}:n-n'=km$, οπότε $g^{n-n'}=(g^k)^m=e\Rightarrow g^n=g^{n'}$. Η εν λόγω (προφανώς επιρριπτική) απεικόνιση είναι ένας ισομορφισμός ομάδων. Πράγματι· επειδή η εικόνα τού $[n]_m+[n']_m=[n'']_m$ (όπου $n''\in\{0,1,...,m-1\}$ το υπόλοιπο που αφήνει το $n+n'$ διαιρούμενο διά τού m) είναι το

$$g^{n''}=g^{n+n'}=g^ng^{n'},\ \forall(n,n')\in\{0,1,...,m-1\}\times\{0,1,...,m-1\}$$

(βλ. 3.2.11 (i)), αυτή είναι *ομομορφισμός ομάδων*· επιπροσθέτως, είναι και *μονομορφισμός ομάδων*, διότι ο πυρήνας της είναι (προφανώς) η τετριμμένη υποομάδα $\{[0]_m\}$ τής $(\mathbb{Z}_m,+)$ (βλ. πρόταση 3.5.12). □

[47] Η φράση «ταξινόμηση μέχρις ισομορφισμού» ή «με ακρίβεια ισομορφισμού» (up to isomorphism) δηλοί τη «διάκριση (ομάδων) με μόνο κριτήριο ταυτίσεως τη διαμεσολάβηση κάποιου ισομορφισμού».

3.5.27 Παρατήρηση (Η «τετριμμένη ομάδα»). Έστω $(G,\cdot)$ τυχούσα ομάδα τάξεως $|G|=1$. Τότε το υποκείμενο σύνολό της G αποτελείται από ένα και μόνον στοιχείο, το οποίο είναι κατ' ανάγκην το αντίστροφο τού εαυτού του και, ταυτοχρόνως, το ουδέτερο στοιχείο τής $(G,\cdot)$. Ως εκ τούτου, η $(G,\cdot)$ είναι κυκλική και (βάσει τού (ii) τού θεωρήματος 3.5.26) ισόμορφη με την $(\{[0]_1\},+)$. Κατ' αυτόν τον τρόπο ταξινομούνται *ομαδοθεωρητικώς όλες οι ομάδες τάξεως* 1 (πρβλ. σημείωση 8.1.10). Η *μέχρις ισομορφισμού μονοσημάντως ορισμένη* ομάδα τάξεως 1 ονομάζεται **τετριμμένη ομάδα**. Ο αναγνώστης καλείται, εν προκειμένω, να διακρίνει τη λεπτή διαφορά μεταξύ τής «τετριμμένης ομάδας», όπως εισήχθη εδώ, και τής «τετριμμένης υποομάδας δοθείσας ομάδας», όπως είχε εισαχθεί στο 3.2.21 (i). Η πρώτη εκφράζει μια *απόλυτη* έννοια (*μέχρις ισομορφισμού*), ενώ η δεύτερη εκφράζει μια *σχετική* έννοια (παρότι είναι *συνολοθεωρητικώς* μονοσημάντως ορισμένη), αφού είναι -εκ παραλλήλου- απαραίτητη η αναφορά τής ομάδας εντός τής οποίας περιέχεται (ως το μονοσύνολο το περιέχον ως στοιχείο του το ουδέτερο στοιχείο αυτής τής ομάδας).

3.5.28 Πόρισμα (Υποομάδες κυκλικών ομάδων). *Έστω $(G,\cdot)$ μια κυκλική ομάδα. Τότε ισχύουν τα εξής*:

(i) *Εάν η G είναι άπειρη ομάδα και $G=\langle g\rangle$, για κάποιο $g\in G$, τότε, σύμφωνα με τα* 3.5.26 (i) *και* 3.3.19 (i), *οι υποομάδες της είναι ακριβώς οι κυκλικές ομάδες $\langle g^d\rangle$, όπου $d\in\mathbb{N}_0$.*

(ii) *Εάν η G είναι πεπερασμένη ομάδα τάξεως $m\in\mathbb{N}$, τότε οι υποομάδες της είναι ακριβώς αυτές που περιεγράφησαν στο πόρισμα* 3.4.23.

(Σημειωτέον ότι η $\mathbb{N}_0\ni d\longmapsto\langle g^d\rangle$ είναι μια *αμφίρριψη*.[48])

Κάνοντας χρήση τού θεωρήματος 3.5.26, σε συνδυασμό με το 2ο θεώρημα αντιστοιχίσεως υποομάδων 3.5.20, καταλήγουμε σε μια *συστηματικότερη ταξινόμηση* των υποομάδων των κυκλικών ομάδων, ύστερα από αναγωγή τού προβλήματος στον στοιχειώδη αριθμοθεωρητικό χαρακτηρισμό των υποομάδων των $(\mathbb{Z},+)$ και $(\mathbb{Z}_m,+)$. Συγκεκριμένα, το πόρισμα 3.5.28 ισχυροποιείται ως ακολούθως:

3.5.29 Πόρισμα (Ταξινόμηση υποομάδων κυκλικών ομάδων). *Έστω $(G,\cdot)$ μια κυκλική ομάδα. Τότε ισχύουν τα εξής*:

(i) *Εάν η $(G,\cdot)$ είναι άπειρη ομάδα και $G=\langle g\rangle$, για κάποιο $g\in G$, τότε υφίστανται δύο αμφιρρίψεις*

$$\boxed{\mathbb{N}_0\longrightarrow\mathbf{Subg}(\mathbb{Z})\longrightarrow\mathbf{Subg}(G),\ d\longmapsto d\,\mathbb{Z}\longmapsto\langle g^d\rangle.}$$

Η πρώτη εξ αυτών καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων $(\mathbb{N}_0,|)$ και $(\mathbf{Subg}(\mathbb{Z}),\supseteq)$ (ήτοι τον ανάστροφο σύνδεσμο τού $(\mathbf{Subg}(\mathbb{Z}),\sqsubseteq)$, βλ. 3.2.26, 1.4.23 (iii), και 1.4.26). *Η δεύτερη καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων $(\mathbf{Subg}(\mathbb{Z}),\supseteq)$ και $(\mathbf{Subg}(G),\supseteq)$, και στέλνει κάθε υποομάδα τής $(\mathbb{Z},+)$ να απεικονισθεί σε ακριβώς μία υποομάδα τής $(G,\cdot)$ που είναι (ομαδοθεωρητικώς) ισόμορφη με αυτήν. Επιπροσθέτως,*

$$\mathbf{Min\text{-}Subg}(G)=\varnothing\ \text{ και }\ \mathbf{Max\text{-}Subg}(G)=\{\langle g^p\rangle\,|\,p\text{ πρώτος αριθμός}\}.$$

(ii) *Εάν η $(G,\cdot)$ είναι πεπερασμένη ομάδα τάξεως $m\in\mathbb{N}$, $\mathfrak{D}_m$ το σύνολο των θετικών ακεραίων διαιρετών τού m* (βλ. 2.2.34), *και $G=\langle g\rangle$, για κάποιο στοιχείο $g\in G$,*

[48] Πράγματι· εάν $d\neq d'$, τότε έχουμε $\langle g^d\rangle\neq\langle g^{d'}\rangle$, απ' όπου έπεται η ενριπτικότητά της, διότι από την ισότητα $\langle g^d\rangle=\langle g^{d'}\rangle$ θα καταλήγαμε στο ότι η G είναι πεπερασμένη, πράγμα άτοπο. Η επιριπτικότητα είναι σαφής επί τη βάσει των προηγηθέντων επιχειρημάτων. Βλ. απόδειξη τής προτάσεως 3.3.18.)

τότε υφίστανται δύο αμφιρρίψεις

$$\boxed{\mathfrak{D}_m \longrightarrow \mathbf{Subg}(\mathbb{Z}_m) \longrightarrow \mathbf{Subg}(G),\ d \longmapsto \left\langle \left[\tfrac{m}{d}\right]_m \right\rangle \longmapsto \left\langle g^{\frac{m}{d}} \right\rangle .}$$

Η πρώτη εξ αυτών καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων

$$(\mathfrak{D}_m, |) \ \textit{και}\ \ (\mathbf{Subg}(\mathbb{Z}_m), \sqsubseteq) .$$

Η δεύτερη καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων

$$(\mathbf{Subg}(\mathbb{Z}_m), \sqsubseteq)\ \ \textit{και}\ \ (\mathbf{Subg}(G), \sqsubseteq) ,$$

και στέλνει κάθε υποομάδα τής $(\mathbb{Z}_m, +)$ να απεικονισθεί σε ακριβώς μία υποομάδα τής $(G, \cdot)$ που είναι (ομαδοθεωρητικώς) ισόμορφη με αυτήν. Επιπροσθέτως, εάν $m \geqslant 2$ και $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ είναι η κανονική παράσταση (2.19) τού m ως γινομένου πρώτων αριθμών, τότε η G διαθέτει k ελαχιστικές και k μεγιστικές υποομάδες. Συγκεκριμένα,

$$\mathbf{Min\text{-}Subg}(G) = \left\{ \left\langle g^{(p_1^{\alpha_1 - 1} p_2^{\alpha_2} \cdots p_k^{\alpha_k})} \right\rangle, \left\langle g^{(p_1^{\alpha_1} p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k})} \right\rangle, \ldots, \left\langle g^{(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k - 1})} \right\rangle \right\}$$

και $\mathbf{Max\text{-}Subg}(G) = \{\langle g^{p_1} \rangle, \langle g^{p_2} \rangle, \ldots, \langle g^{p_k} \rangle\}$.

Απόδειξη. (i) Το ότι η πρώτη απεικόνιση είναι αμφίρριψη και ότι καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων $(\mathbb{N}_0, |)$ και $(\mathbf{Subg}(\mathbb{Z}), \supseteq)$ έπεται από το (i) τής προτάσεως 3.3.19 και το (i) τού πορίσματος 3.3.20. Το ότι η δεύτερη απεικόνιση είναι αμφίρριψη και ότι καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων

$$(\mathbf{Subg}(\mathbb{Z}), \supseteq)\ \ \text{και}\ \ (\mathbf{Subg}(G), \supseteq) ,$$

(στέλνοντας κάθε υποομάδα τής $(\mathbb{Z}, +)$ να απεικονισθεί σε ακριβώς μία υποομάδα τής $(G, \cdot)$ που είναι ισόμορφη με αυτήν) έπεται ύστερα από την εφαρμογή τού 2ου θεωρήματος αντιστοιχίσεως υποομάδων 3.5.20 για τον ισομορφισμό

$$(\mathbb{Z}, +) \longrightarrow (G, \cdot),\ \ n \longmapsto g^n,$$

τον θεσπισθέντα στο (i) τού θεωρήματος 3.5.26. Σημειωτέον ότι η $(\mathbb{Z}, +)$ (και, κατ' επέκταση, και η $(G, \cdot)$) δεν διαθέτει καμία ελαχιστική υποομάδα. (Εάν K ήταν κάποια ελαχιστική υποομάδα της, τότε η K δεν θα διέθετε καμία μη τετριμμένη γνήσια υποομάδα. Αυτό, όπως θα δούμε στο πόρισμα 5.1.34, θα σήμαινε ότι η K είναι *πεπερασμένη* και κυκλική, έχουσα ως τάξη της έναν πρώτο αριθμό. Άτοπο, καθόσον η K είναι κατ' ανάγκην *άπειρη* ομάδα!). Επιπροσθέτως,

$$\mathbf{Max\text{-}Subg}(\mathbb{Z}) = \{p\mathbb{Z} \,|\, p \text{ πρώτος αριθμός}\} .$$

Πράγματι· εάν p είναι ένας πρώτος αριθμός και $p\mathbb{Z} \sqsubseteq H \sqsubset \mathbb{Z}$, τότε $H = \langle d \rangle = d\mathbb{Z}$ για κάποιον $d \in \mathbb{N}$, $d \geqslant 2$, και $d \mid p$. (Βλ. 3.3.19 (i) και 3.3.20 (i)). Άρα $d = p$ και η $\langle p \rangle = p\mathbb{Z}$ είναι μια μεγιστική υποομάδα τής $(\mathbb{Z}, +)$. Αλλά και κάθε μεγιστική υποομάδα K τής $(\mathbb{Z}, +)$ είναι αυτής τής μορφής, διότι $K = m\mathbb{Z}$ για κάποιον $m \in \mathbb{N}$, $m \geqslant 2$ (βλ. 3.3.19 (i)). Εάν υποθέταμε ότι ο m δεν είναι πρώτος, τότε θα υπήρχε κάποιος πρώτος διαιρέτης p αυτού με $K \sqsubset p\mathbb{Z} \sqsubset \mathbb{Z}$ (βλ. 2.3.2 και 3.3.20 (i)), οπότε η K δεν θα ήταν μεγιστική υποομάδα τής $(\mathbb{Z}, +)$.

(ii) Το ότι η πρώτη απεικόνιση είναι αμφίρριψη και ότι καθορίζει έναν ισομορφισμό μεταξύ των $(\mathfrak{D}_m, |)$ και $(\mathbf{Subg}(\mathbb{Z}_m), \sqsubseteq)$ έπεται από το θεώρημα[49] 3.4.21 και το

[49] Σημειωτέον ότι για οιουσδήποτε $d_1, d_2 \in \mathfrak{D}_m$ έχουμε $d_1 \mid d_2 \Leftrightarrow \frac{m}{d_2} \mid \frac{m}{d_1} \Leftrightarrow \left\langle \left[\frac{m}{d_1}\right]_m \right\rangle \sqsubseteq \left\langle \left[\frac{m}{d_2}\right]_m \right\rangle$.

πόρισμα 3.4.23 (πρβλ. 3.4.14). Το ότι η δεύτερη απεικόνιση είναι αμφίρριψη και ότι καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων

$$(\mathbf{Subg}(\mathbb{Z}_m), \sqsubseteq) \quad \text{και} \quad (\mathbf{Subg}(G), \sqsubseteq)\,,$$

(στέλνοντας κάθε υποομάδα τής $(\mathbb{Z}_m, +)$ να απεικονισθεί σε ακριβώς μία υποομάδα τής $(G, \cdot)$ που είναι ισόμορφη με αυτήν) έπεται ύστερα από την εφαρμογή τού 2ου θεωρήματος αντιστοιχίσεως υποομάδων 3.5.20 για τον ισομορφισμό

$$(\mathbb{Z}_m, +) \longrightarrow (G, \cdot), \;\; [n]_m \longmapsto g^n, \;\; \forall n \in \{0, 1, ..., m-1\},$$

τον θεσπισθέντα στο (ii) τού θεωρήματος 3.5.26. Επιπροσθέτως, εάν $m \geqslant 2$ και $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ είναι η κανονική παράσταση (2.19) τού m ως γινομένου πρώτων αριθμών (με $\alpha_1, ..., \alpha_k \in \mathbb{N}$), τότε οι φυσικοί αριθμοί

$$p_1^{\alpha_1 - 1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \; p_1^{\alpha_1} p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k}, \; \ldots, \; p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k - 1}$$

αποτελούν τα *μεγιστικά στοιχεία* τού $(\mathfrak{D}_m \smallsetminus \{m\}, |)$ και οι πρώτοι αριθμοί $p_1, p_2, \ldots, p_k$ τα *ελαχιστικά στοιχεία* τού $(\mathfrak{D}_m \smallsetminus \{1\}, |)$ (βλ. 1.4.9 και 2.3.15), οπότε

$$\mathbf{Min\text{-}Subg}(\mathbb{Z}_m) = \left\{ \left\langle \left[p_1^{\alpha_1 - 1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\right]_m \right\rangle, ..., \left\langle \left[p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k - 1}\right]_m \right\rangle \right\}$$

και $\mathbf{Max\text{-}Subg}(\mathbb{Z}_m) = \{\langle [p_1]_m \rangle, \langle [p_2]_m \rangle, ..., \langle [p_k]_m \rangle\}$. □

3.5.30 Παραδείγματα. (i) Οι υποομάδες τής (προσθετικής) ομάδας

$$\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$$

είναι η τετριμμένη $\{[0]_6\}$, ολόκληρη η $\mathbb{Z}_6$, καθώς και οι

$$\langle [3]_6 \rangle = \{[0]_6, [3]_6\}, \quad \langle [2]_6 \rangle = \{[0]_6, [2]_6, [4]_6\}.$$

Η αμφίρριψη $\mathfrak{D}_6 \longrightarrow \mathbf{Subg}(\mathbb{Z}_6)$ είναι η εξής:

$$1 \longmapsto \{[0]_6\}, \; 2 \longmapsto \langle [3]_6 \rangle, \; 3 \longmapsto \langle [2]_6 \rangle, \; 6 \longmapsto \mathbb{Z}_6 = \langle [1]_6 \rangle$$

(ii) Κατ' αναλογίαν, οι υποομάδες τής (προσθετικής) ομάδας

$$\mathbb{Z}_{12} = \{[0]_{12}, [1]_{12}, [2]_{12}, [3]_{12}, [4]_{12}, [5]_{12}, [6]_{12}, [7]_{12}, [8]_{12}, [9]_{12}, [10]_{12}, [11]_{12}\}$$

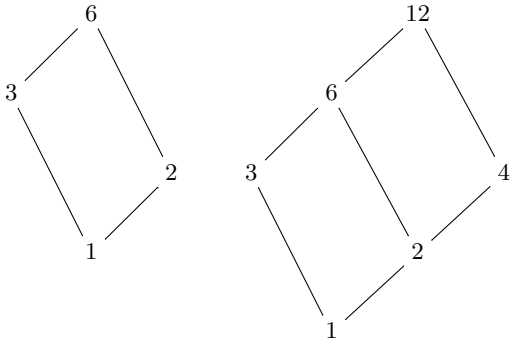
είναι η τετριμμένη $\{[0]_{12}\}$, ολόκληρη η $\mathbb{Z}_{12}$, καθώς και οι

$$\begin{gathered}
\langle [6]_{12} \rangle = \{[0]_{12}, [6]_{12}\}, \\
\langle [4]_{12} \rangle = \{[0]_{12}, [4]_{12}, [8]_{12}\}, \\
\langle [3]_{12} \rangle = \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}, \\
\langle [2]_{12} \rangle = \{[0]_{12}, [2]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12}\}.
\end{gathered}$$

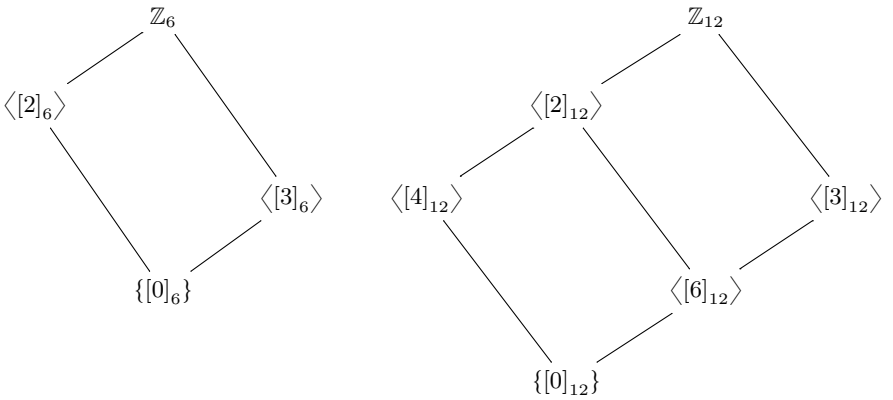
Η αμφίρριψη $\mathfrak{D}_{12} \longrightarrow \mathbf{Subg}(\mathbb{Z}_{12})$ είναι η εξής:

$$\begin{gathered}
1 \longmapsto \langle [0]_{12} \rangle, \quad 2 \longmapsto \langle [6]_{12} \rangle, \quad 3 \longmapsto \langle [4]_{12} \rangle, \\
4 \longmapsto \langle [3]_{12} \rangle, \quad 6 \longmapsto \langle [2]_{12} \rangle, \quad 12 \longmapsto \mathbb{Z}_{12}.
\end{gathered}$$

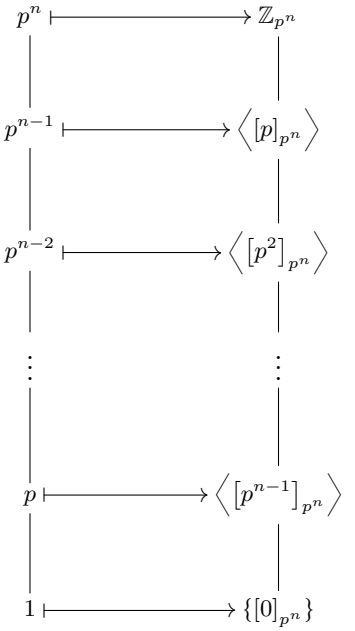
Τα διαγράμματα τού Hasse για τους συνδέσμους των διαιρετών στα (i) και (ii) είναι τα



ενώ τα αντίστοιχα διαγράμματα για τους συνδέσμους των υποομάδων είναι τα



3.5.31 Παράδειγμα. Εάν ο p είναι ένας πρώτος αριθμός και $n \in \mathbb{N}$, τότε το διάγραμμα τού Hasse και η αμφίρριψη $\mathfrak{D}_{p^n} \longrightarrow \mathbf{Subg}(\mathbb{Z}_{p^n})$ για την $(\mathbb{Z}_{p^n}, +)$ εκφράζονται ως ακολούθως:



‣ **Ενδομορφισμοί και αυτομορφισμοί ομάδων**. Έστω $(G, \cdot)$ μια ομάδα. Το σύνολο $\mathrm{Hom}(G, G)$ όλων των ενδομορφισμών (και αντιστοίχως, το σύνολο όλων των αυτομορφισμών) τής G σημειώνεται ως $\mathrm{End}(G)$ (και αντιστοίχως, ως $\mathrm{Aut}(G)$).

3.5.32 Πρόταση. *Το ζεύγος* $(\mathrm{End}(G),\circ)$ *(και αντιστοίχως, το ζεύγος* $(\mathrm{Aut}(G),\circ)$*) αποτελεί ένα μονοειδές (και αντιστοίχως, μια ομάδα).*

ΑΠΟΔΕΙΞΗ. Προφανής επί τη βάσει των προτάσεων 3.5.9 και 3.5.24. (Το ουδέτερο στοιχείο αυτών είναι η ταυτοτική απεικόνιση id_G.) □

3.5.33 Σημείωση. (i) Προφανώς, $\mathrm{End}(G)^\times = \mathrm{Aut}(G)$. (Βλ. 3.2.5.)

(ii) Όταν η ομάδα G είναι *αβελιανή*, το ζεύγος $(\mathrm{End}(G),+)$ (όπου "+" η πράξη η εισαχθείσα στο εδάφιο 3.5.10 (ii)) καθίσταται *αβελιανή ομάδα*.

3.5.34 Πρόταση. *Εάν* $X \neq \varnothing$ *είναι ένα σύνολο γεννητόρων μιας ομάδας* $(G,\cdot)$*, τότε* $\langle \vartheta(X)\rangle = G$ *για κάθε* $\vartheta \in \mathrm{Aut}(G)$.

ΑΠΟΔΕΙΞΗ. Προφανώς, $G = \vartheta(G) = \vartheta(\langle X\rangle) = \langle \vartheta(X)\rangle$ για κάθε αυτομορφισμό ϑ τής G (βλ. 3.5.6 (i)). □

Για ορισμένες ειδικές ομάδες $(G,\cdot)$ είναι δυνατός ένας λεπτομερής χαρακτηρισμός τής $(\mathrm{Aut}(G),\circ)$. Επί παραδείγματι, τα θεωρήματα 3.5.35 και 3.5.36 μας παρέχουν την ταξινόμηση των ομάδων αυτομορφισμών των κυκλικών ομάδων και τής (αβελιανής, μη κυκλικής) ομάδας $(\mathbb{Q},+)$, αντιστοίχως, *μέχρις ισομορφισμού*[50].

3.5.35 Θεώρημα (Ομάδα αυτομορφισμών κυκλικών ομάδων). *Έστω* $(G,\cdot)$ *μια κυκλική ομάδα. Τότε ισχύουν τα εξής:*

(i) *Εάν η* $(G,\cdot)$ *είναι άπειρη ομάδα, τότε η ομάδα* $(\mathrm{Aut}(G),\circ)$ *των αυτομορφισμών της είναι ισόμορφη με την* $(\mathbb{Z}_2,+)$.

(ii) *Εάν η* $(G,\cdot)$ *είναι πεπερασμένη ομάδα τάξεως* $m \in \mathbb{N}$*, τότε η* $(\mathrm{Aut}(G),\circ)$ *είναι ισόμορφη με την* $(\mathbb{Z}_m^\times,\cdot)$ (βλ. 3.2.7 (iii)).

ΑΠΟΔΕΙΞΗ. (i) Έστω G μια άπειρη κυκλική ομάδα και έστω g κάποιος γεννήτοράς της. Από το (i) τού θεωρήματος 3.5.26 γνωρίζουμε ότι η απεικόνιση

$$\lambda : (\mathbb{Z},+) \longrightarrow (G,\cdot),\ \ n \longmapsto \lambda(g) := g^n,$$

είναι ισομορφισμός ομάδων. Ως εκ τούτου, επάγεται ένας ισομορφισμός

$$\mathrm{Aut}(\mathbb{Z}) \ni \vartheta \longmapsto \lambda \circ \vartheta \circ \lambda^{-1} \in \mathrm{Aut}(G)$$

μεταξύ των ομάδων $(\mathrm{Aut}(G),\circ)$ και $(\mathrm{Aut}(\mathbb{Z}),\circ)$. Αρκεί λοιπόν να δείξουμε ότι υφίσταται ισομορφισμός μεταξύ των $(\mathrm{Aut}(\mathbb{Z}),\circ)$ και $(\mathbb{Z}_2,+)$. Έστω $\vartheta \in \mathrm{End}(\mathbb{Z})$. Τότε $\vartheta(n) = n\cdot\vartheta(1)$ για κάθε $n \in \mathbb{Z}$. Πράγματι·

$$\vartheta(n) = \begin{cases} \vartheta(\underbrace{1+\cdots+1}_{n\ \text{φορές}}) = \underbrace{\vartheta(1)+\cdots+\vartheta(1)}_{n\ \text{φορές}} = n\cdot\vartheta(1), & \text{όταν } n>0,\\ \vartheta(0) = 0\cdot\vartheta(1), & \text{όταν } n=0,\\ \vartheta(\underbrace{(-1)+\cdots+(-1)}_{-n\ \text{φορές}}) = (-n)\cdot\vartheta(-1) = n\cdot\vartheta(1), & \text{όταν } n<0. \end{cases}$$

Κατά συνέπειαν[51], $\mathrm{End}(\mathbb{Z}) = \{\vartheta_\kappa \mid \kappa\in\mathbb{Z}\}$, όπου

$$\vartheta_\kappa : \mathbb{Z} \longrightarrow \mathbb{Z},\ n \longmapsto \vartheta_\kappa(n) := \kappa n.$$

[50] Σημειωτέον ότι, συν τοις άλλοις, κατά την αποδεικτική πορεία των θεωρημάτων 3.5.35 και 3.5.36 *περιγράφονται διεξοδικώς* οι εν λόγω αυτομορφισμοί.

[51] Εν προκειμένω, ως δακτύλιος (βλ. 3.5.33 (ii)), ο $\mathrm{End}(\mathbb{Z})$ είναι ισόμορφος τού δακτυλίου των ακεραίων αριθμών.

Σημειωτέον ότι οι ϑ_κ είναι ενριπτικές για κάθε $\kappa \in \mathbb{Z}\smallsetminus\{0\}$. Έστω $\kappa \in \mathbb{Z}\smallsetminus\{0\}$, τέτοιος ώστε $\vartheta_\kappa \in \mathrm{Aut}(\mathbb{Z})$. Τότε η ϑ_κ είναι *και* επιρριπτική, και επειδή $1 \in \mathbb{Z}$, υπάρχει κάποιος $n \in \mathbb{Z}$, τέτοιος ώστε $\vartheta_\kappa(n) = \kappa n = 1$. Τούτο σημαίνει ότι

$$(\kappa, n) \in \{(1,1), (-1,-1)\}.$$

Άρα $\mathrm{Aut}(\mathbb{Z}) = \{\vartheta_{-1}, \vartheta_1\}$ και (προφανώς) η ακόλουθη απεικόνιση είναι ισομορφισμός ομάδων:

$$f : (\mathbb{Z}_2, +) \longrightarrow (\mathrm{Aut}(\mathbb{Z}), \circ), \;\; [0]_2 \mapsto f([0]_2) := \vartheta_1, \;\; [1]_2 \mapsto f([1]_2) := \vartheta_{-1}.$$

(ii) Έστω G μια πεπερασμένη κυκλική ομάδα τάξεως m έχουσα το $g \in G$ ως (κάποιον) γεννήτορά της και έστω $\vartheta \in \mathrm{Aut}(G)$. Λόγω των (3.10) και 3.5.22 (iv) έχουμε

$$m = |G| = |\langle g\rangle| = \mathrm{ord}(g) = \mathrm{ord}(\vartheta(g)).$$

Επιπροσθέτως, επειδή $\vartheta(g) \in G = \langle g\rangle$, υπάρχει κάποιος $k \in \mathbb{Z} : \vartheta(g) = g^k$. Επομένως,

$$\langle g\rangle = G = \vartheta(G) = \vartheta\left(\langle g\rangle\right) = \langle\vartheta(g)\rangle = \left\langle g^k\right\rangle,$$

όπου η δεύτερη ισότητα έπεται από την επιρριπτικότητα τής ϑ και η τρίτη από την πρόταση 3.5.6. Λαμβάνοντας υπ' όψιν το πόρισμα 3.4.17 συμπεραίνουμε ότι

$$\langle g\rangle = G = \left\langle g^k\right\rangle \Longrightarrow \mu\kappa\delta(k,m) = 1,$$

οπότε υφίστανται το πολύ $\phi(m)$ αυτομορφισμοί τής G, όπου ϕ η συνάρτηση τού Euler (βλ. (3.3)). Άρα

$$|\mathrm{Aut}(G)| \leqslant \phi(m) = \left|\mathbb{Z}_m^\times\right|. \tag{3.19}$$

Από τη άλλη μεριά, *για κάθε* $k \in \mathbb{N}$ *με* $k \leqslant m$ *και* $\mu\kappa\delta(k,m) = 1$ οι απεικονίσεις

$$\vartheta_k : G \longrightarrow G, \;\; x \longmapsto \vartheta_k(x) := x^k,$$

είναι ενδομορφισμοί τής G, διότι $\vartheta_k(x_1x_2) = (x_1x_2)^k = x_1^k x_2^k$, για οιαδήποτε στοιχεία $x_1, x_2 \in G$. (Η τελευταία ισότητα ισχύει, διότι η G -ως κυκλική- είναι αβελιανή, βλ. πρόταση 3.3.17 και παρατήρηση 3.2.12). Επειδή $G = \left\langle g^k\right\rangle$ (και πάλι λόγω τού πορίσματος 3.4.17) έχουμε

$$G = \left\langle g^k\right\rangle = \{\left(g^k\right)^l \;\Big|\; l \in \mathbb{Z}\} = \{\left(g^l\right)^k \;\Big|\; l \in \mathbb{Z}\} = \vartheta_k(G),$$

οπότε οι ενδομορφισμοί ϑ_k είναι επιρριπτικοί. Επειδή κάθε επιρριπτική απεικόνιση από ένα πεπερασμένο σύνολο επί τού εαυτού του είναι κατ' ανάγκην ενριπτική (και, ως εκ τούτου, αμφιρριπτική), συνάγεται ότι $\vartheta_k \in \mathrm{Aut}(G)$ και

$$|\mathrm{Aut}(G)| \geqslant \phi(m) \underset{(3.19)}{\Longrightarrow} |\mathrm{Aut}(G)| = \phi(m)$$

$$\Longrightarrow \mathrm{Aut}(G) = \{\vartheta_k \mid k \in \mathbb{N} \text{ με } k \leqslant m \text{ και } \mu\kappa\delta(k,m) = 1\}.$$

Εν συνεχεία, παρατηρούμε ότι η

$$f : \mathbb{Z}_m^\times \longrightarrow \mathrm{Aut}(G), \;\; [k]_m \longmapsto f([k]_m) := \vartheta_k,$$

είναι αφ' ενός μεν μια καλώς ορισμένη απεικόνιση ($[k]_m = [k']_m \Rightarrow \vartheta_k = \vartheta_{k'}$), αφ' ετέρου δε ένας ομομορφισμός ομάδων (καθόσον $\vartheta_{kk'} = \vartheta_k \circ \vartheta_{k'}$). Εκ κατασκευής, η f είναι επιρριπτική. Επειδή κάθε επιρριπτική απεικόνιση από ένα πεπερασμένο σύνολο επί ενός συνόλου που έχει τον ίδιο πληθικό αριθμό είναι κατ' ανάγκην ενριπτική (και, ως εκ τούτου, αμφιρριπτική), συνάγεται τελικώς η f είναι ένας ισομορφισμός ομάδων. □

3.5.36 Θεώρημα (Ομάδα αυτομορφισμών τής $(\mathbb{Q},+)$). *Η ομάδα $(\mathrm{Aut}(\mathbb{Q}),\circ)$ των αυτομορφισμών τής $(\mathbb{Q},+)$ είναι ισόμορφη με την (πολλαπλασιαστική) ομάδα $(\mathbb{Q}\smallsetminus\{0\},\cdot)$.*

Απόδειξη. Έστω $\vartheta\in\mathrm{End}(\mathbb{Q})$. Τότε $\vartheta(q)=q\cdot\vartheta(1)$ για κάθε $q\in\mathbb{Q}$. Πράγματι· επειδή κάθε $q\in\mathbb{Q}$ γράφεται υπό τη μορφή $q=\frac{m}{n}$, όπου $m\in\mathbb{Z}$, $n\in\mathbb{N}$, λαμβάνουμε

$$\vartheta(q)=\begin{cases}\vartheta(\underbrace{\frac{1}{n}+\cdots+\frac{1}{n}}_{m\text{ φορές}})=\underbrace{\vartheta\left(\frac{1}{n}\right)+\cdots+\vartheta\left(\frac{1}{n}\right)}_{m\text{ φορές}}=q\cdot\vartheta(1), & \text{όταν } m>0,\\ \vartheta(0)=0\cdot\vartheta(1), & \text{όταν } m=0,\\ \vartheta(\underbrace{(-\frac{1}{n})+\cdots+(-\frac{1}{n})}_{-m\text{ φορές}})=(-q)\vartheta(-1)=q\cdot\vartheta(1), & \text{όταν } m<0,\end{cases}$$

διότι

$$n\cdot\vartheta\left(\tfrac{1}{n}\right)=\underbrace{\vartheta\left(\tfrac{1}{n}\right)+\cdots+\vartheta\left(\tfrac{1}{n}\right)}_{n\text{ φορές}}=\vartheta(\underbrace{\tfrac{1}{n}+\cdots+\tfrac{1}{n}}_{n\text{ φορές}})=\vartheta(1)\Rightarrow\vartheta\left(\tfrac{1}{n}\right)=\tfrac{1}{n}\vartheta(1).$$

Κατά συνέπειαν, $\mathrm{End}(\mathbb{Q})=\{\vartheta_\ell\mid\ell\in\mathbb{Q}\}$, όπου

$$\vartheta_\ell:\mathbb{Q}\longrightarrow\mathbb{Q},\ q\longmapsto\vartheta_\ell(q):=\ell q.$$

Σημειωτέον ότι οι ϑ_ℓ είναι αμφιριπτικές για κάθε $\ell\in\mathbb{Q}\smallsetminus\{0\}$. Άρα

$$\mathrm{Aut}(\mathbb{Q})=\{\vartheta_\ell\mid\ell\in\mathbb{Q}\smallsetminus\{0\}\}$$

και η

$$f:(\mathbb{Q}\smallsetminus\{0\},\cdot)\longrightarrow(\mathrm{Aut}(\mathbb{Q}),\circ),\ \ \ell\longmapsto f(\ell):=\vartheta_\ell,$$

είναι ισομορφισμός ομάδων. □

3.5.37 Σημείωση (Περί τής Aut (G)). Η ομάδα αυτομορφισμών $\mathrm{Aut}(G)$ δοθείσας ομάδας G εξαρτάται κατά κανόνα από τα ιδιαίτερα γνωρίσματα και τις «εσώτερες» ιδιότητες τής G. Ως εκ τούτου, οι *γενικής φύσεως* πληροφορίες για την $\mathrm{Aut}(G)$ είναι περιορισμένες:

(i) Εάν η ομάδα αναφοράς G είναι πεπερασμένη, τότε και η $\mathrm{Aut}(G)$ είναι πεπερασμένη (τάξεως[52] $|\mathrm{Aut}(G)|\leqslant(|G|-1)!$). Αντιθέτως, εάν η G είναι άπειρη ομάδα, τότε άλλοτε η ομάδα αυτομορφισμών της είναι άπειρη (όπως, π.χ., είδαμε στο θεώρημα 3.5.36 για την ομάδα των αυτομορφισμών τής $(\mathbb{Q},+)$) και άλλοτε πεπερασμένη[53] (όπως, π.χ., είδαμε στα 3.5.26 (i) και 3.5.35 (i) για την ομάδα των αυτομορφισμών τής $(\mathbb{Z},+)$). Εξάλλου, είναι γνωστό ότι κάθε ομάδα που έχει πεπερασμένη ομάδα αυτομορφισμών και δεν διαθέτει στρέψη (βλ. 3.4.1 (ii)) είναι κατ' ανάγκην άπειρη αβελιανή.

(ii) Στην περίπτωση όπου η G είναι αβελιανή μη κυκλική ομάδα, η $\mathrm{Aut}(G)$ δεν είναι αβελιανή όταν $|G|<\infty$, ενώ μπορεί να είναι αβελιανή μόνον σε ειδικές περιπτώσεις[54] όταν $|G|=\infty$. Επίσης, δεν υπάρχει καμία άπειρη μη αβελιανή

[52] Η $(\mathrm{Aut}(G),\circ)$ είναι υποομάδα τής λεγομένης *συμμετρικής ομάδας* $(\mathfrak{S}_G,\circ)$ *επί τής* G τής απαρτιζόμενης από όλες τις αμφιρρίψεις $f:G\longrightarrow G$ που έχει τάξη $|\mathfrak{S}_G|=|G|!$ (Βλ. εδάφια 4.1.1 και 4.1.3.) Επειδή $\vartheta(e_G)=e_G$, για κάθε $\vartheta\in\mathrm{Aut}(G)$, έχουμε $|\mathrm{Aut}(G)|\leqslant(|G|-1)!$.

[53] Για περαιτέρω παραδείγματα άπειρων ομάδων με πεπερασμένη ομάδα αυτομορφισμών βλ. F. Fournelle: *Finite groups of automorhisms of infinite groups I*, Journal of Algebra **70** (1981), 16-22.

[54] Όπως αποδεικνύεται στο άρθρο τού F. Fournelle: *Finite groups of automorhisms of infinite groups II,* Journal of Algebra **80** (1983), 106-112, μια άπειρη αβελιανή ομάδα G έχει πεπερασμένη ομάδα αυτομορφισμών εάν και μόνον εάν η $\mathrm{Aut}(G)$ έχει άρτια τάξη και είναι ισόμορφη με το ευθύ άθροισμα πεπερασμένου πλήθους «αντιτύπων» των $\mathbb{Z}_2$, $\mathbb{Z}_3$ και $\mathbb{Z}_4$, έχουσα ένα στοιχείο τάξεως 12 και ένα στοιχείο τάξεως 2 το οποίο δεν αποτελεί την έκτη δύναμη άλλου.

ομάδα έχουσα κυκλική ομάδα αυτομορφισμών. Από την άλλη μεριά, η ομάδα αυτομορφισμών $\mathrm{Aut}(G)$ μιας μη αβελιανής πεπερασμένης ομάδας G είναι, κατά περίπτωση, άλλοτε αβελιανή και άλλοτε μη αβελιανή.

(iii) Ιδιαίτερο ενδιαφέρον παρουσιάζει το εξής πρόβλημα: Δοθείσας μιας ομάδας H, ποιες (και πόσες, μέχρις ισομορφισμού) ομάδες G υπάρχουν, ούτως ώστε να ισχύει $\mathrm{Aut}(G) \cong H$; Μερικές λύσεις του (και εκτεταμένοι κατάλογοι καλύπτοντες ειδικές περιπτώσεις) συναντώνται σε αρκετά άρθρα[55]. Όταν η H είναι πεπερασμένη, τότε υφίστανται μόνον *πεπερασμένου πλήθους* (μη ισόμορφες) *πεπερασμένες* ομάδες G με[56] $\mathrm{Aut}(G) \cong H$. Τούτο παύει να ισχύει όταν στην G επιτραπεί να είναι άπειρη: Π.χ., ο D.J.S. Robinson[57] έχει κατασκευάσει για τη συμμετρική ομάδα $H = \mathfrak{S}_4$ (τάξεως 24, βλ. 4.1.3) μια *υπεραριθμήσιμη* οικογένεια άπειρων μη αβελιανών (ανά δύο μη ισόμορφων) ομάδων (G_j) με $\mathrm{Aut}(G_j) \cong \mathfrak{S}_4$.

(iv) Υπάρχουν ζεύγη ομάδων (G_1, G_2), τέτοια ώστε $\mathrm{Aut}(G_1) \cong \mathrm{Aut}(G_2)$ αλλά (ταυτοχρόνως) $G_1 \ncong G_2$.

(v) Υπάρχουν *γνήσιες* υποομάδες H πεπερασμένων ομάδων G, τέτοιες ώστε να ισχύει $|\mathrm{Aut}(H)| > |\mathrm{Aut}(G)|$.

(vi) Τέλος, είναι αξιοπρόσεκτο το ότι υπάρχουν και κάποιες ειδικές ομάδες G για τις οποίες ισχύει $|\mathrm{Aut}(G)| = |G|$ ή ακόμη και $\mathrm{Aut}(G) \cong G$.

3.6 ΕΥΘΕΑ ΓΙΝΟΜΕΝΑ

Το καρτεσιανό γινόμενο δύο ομάδων καθίσταται *κατά τρόπο φυσικό* (ήτοι μέσω «πολλαπλασιασμού κατά συντεταγμένες») *ομάδα*.

3.6.1 Ορισμός. (i) Έστω ότι οι $(G_1, \circledast)$ και $(G_2, \circledcirc)$ είναι τυχούσες ομάδες. Εφοδιάζοντας το καρτεσιανό γινόμενο $G_1 \times G_2$ των υποκειμένων συνόλων τους με την εσωτερική πράξη

$$\boxed{\begin{array}{c}(G_1 \times G_2) \times (G_1 \times G_2) \longrightarrow G_1 \times G_2 \\ ((x_1, x_2), (y_1, y_2)) \longmapsto (x_1, x_2) \boxdot (y_1, y_2) := (x_1 \circledast y_1, x_2 \circledcirc y_2),\end{array}} \tag{3.20}$$

παρατηρούμε ότι το ζεύγος $(G_1 \times G_2, \boxdot)$ αποτελεί ομάδα έχουσα (ως προς την ορισθείσα πράξη "$\boxdot$") το (e_{G_1}, e_{G_2}) ως ουδέτερο στοιχείο της και το (x_1^{-1}, x_2^{-1}) ως αντίστροφο (= συμμετρικό) στοιχείο οιουδήποτε $(x_1, x_2) \in G_1 \times G_2$, όπου x_1^{-1} το αντίστροφο στοιχείο τού $x_1 \in G_1$ ως προς την "$\circledast$" και x_2^{-1} το αντίστροφο στοιχείο τού $x_2 \in G_2$ ως προς την "$\circledcirc$" (βλ. πρόταση 1.5.16). Η $(G_1 \times G_2, \boxdot)$ καλείται **(εξωτερικό) ευθύ γινόμενο των** $(G_1, \circledast)$ **και** $(G_2, \circledcirc)$.

[55] G.A. Miller: *Groups with the same group of isomorphisms*, Trans. A.M.S. **1** (1900), 395-401.

H. de Vries & A.B. de Miranda: *Groups with a small number of automorphisms*, Math. Zeitschrift **68** (1958), 450-464.

J.L. Alperin: *Groups with finitely many automorphisms*, Pacific Jour. Math. **12** (1962), 1-5.

J.T Hallett & K.A. Hirsch: *Die Konstruktion von Gruppen mit vorgeschriebenen Automorphismen-Gruppen*, Jour. reine und ang. Math. **238/240** (1970), 32-46.

D.J.S. Robinson: *A contribution to the theory of groups with finitely many automorphisms*, Proc. London Math. Soc. **35** (1977), 34-54.

H.K. Iyer: *On solving the equation* $\mathrm{Aut}(X) = G$, Rocky Mountain Jour. Math. **9** (1979), 653-670.

J. Flynn & D. MacHale: *Determining all finite groups whose automorphism group is a p-group*. Math. Proc. of the Royal Irish Academy **91** (1991), 259-264.

D. MacHale & R. Sheehy: *Finite groups with odd order automorphism groups*, Math. Proc. of the Royal Irish Academy **95** (1995), 113-116.

D. MacHale & R. Sheehy: *Finite groups with few automorphisms*, Math. Proc. of the Royal Irish Academy **104** (2004), 231-238.

[56] Βλ. H.K. Iyer, ό.π., Thm. 3.1, σελ. 657-658.

[57] D.J.S. Robinson: *Groups with prescribed automorphism group*, Proc. Edinburgh Math. Soc. (2) **25** (1982), 217-227.

(ii) Η επίρριψη

$$\mathrm{pr}_1 : G_1 \times G_2 \to G_1,\ (x_1, x_2) \mapsto x_1, \quad (\text{και αντ., η } \mathrm{pr}_2 : G_1 \times G_2 \to G_2,\ (x_1, x_2) \mapsto x_2)$$

καλείται **πρώτη** (και αντιστοίχως, **δεύτερη**) **φυσική προβολή τής** $G_1 \times G_2$ **επί τής** G_1 (και αντιστοίχως, **επί τής** G_2). Επίσης, η ένριψη

$$\iota_1 : G_1 \to G_1 \times G_2,\ x \mapsto (x, e_{G_2}), \quad (\text{και αντ., η } \iota_2 : G_2 \to G_1 \times G_2,\ y \mapsto (e_{G_1}, y))$$

καλείται **φυσική εμφύτευση τής** G_1 **εντός τής** $G_1 \times G_2$ (και αντιστοίχως, **τής** G_2 **εντός τής** $G_1 \times G_2$).

(iii) Θεωρώντας τό ευθύ γινόμενο των $(G_2, \circledcirc)$ και $(G_1, \circledast)$ (ήτοι *εναλλάσσοντας* τους ρόλους των δοθεισών ομάδων), παρατηρούμε ότι η απεικόνιση

$$G_1 \times G_2 \ni (x_1, x_2) \longmapsto (x_2, x_1) \in G_2 \times G_1$$

αποτελεί ισομορφισμό. Ως εκ τούτου, ο ανωτέρω ορισμός τού ευθέος γινομένου είναι *μέχρις ισομορφισμού ανεξάρτητος* τού ποιον εκ δύο «παραγόντων» αναφέρουμε ως πρώτο και ποιον ως δεύτερο.

(iv) Εάν μια ομάδα είναι *ισόμορφη* με την $(G_1 \times G_2, \boxdot)$, τότε είθισται να λέμε ότι οι $(G_1, \circledast)$ και $(G_2, \circledcirc)$ είναι **ευθείς παράγοντές της**.

3.6.2 Πρόταση. *Οι* pr_1 *και* pr_2 *είναι επιμορφισμοί ομάδων έχοντες ως πυρήνες τους τις υποομάδες* $\mathrm{Ker}(\mathrm{pr}_1) = \{e_{G_1}\} \times G_2$, $\mathrm{Ker}(\mathrm{pr}_2) = G_1 \times \{e_{G_2}\}$.

Απόδειξη. Για οιαδήποτε στοιχεία $(x_1, x_2), (y_1, y_2) \in G_1 \times G_2$ έχουμε

$$\begin{aligned} \mathrm{pr}_1((x_1, x_2) \boxdot (y_1, y_2)) &= \mathrm{pr}_1 (x_1 \circledast y_1, x_2 \circledcirc y_2) = x_1 \circledast y_1 \\ &= \mathrm{pr}_1 (x_1, x_2) \circledast \mathrm{pr}_1 (y_1, y_2) \end{aligned}$$

και, κατ' αναλογίαν,

$$\begin{aligned} \mathrm{pr}_2((x_1, x_2) \boxdot (y_1, y_2)) &= \mathrm{pr}_2 (x_1 \circledast y_1, x_2 \circledcirc y_2) = x_2 \circledcirc y_2 \\ &= \mathrm{pr}_2 (x_1, x_2) \circledcirc \mathrm{pr}_2 (y_1, y_2) . \end{aligned}$$

Άρα οι pr_1 και pr_2 είναι επιμορφισμοί ομάδων. Επιπροσθέτως,

$$\mathrm{Ker}\,(\mathrm{pr}_1) = \{(x_1, x_2) \in G_1 \times G_2 \,|\mathrm{pr}_1((x_1, x_2) = e_{G_1}\} = \{e_{G_1}\} \times G_2$$

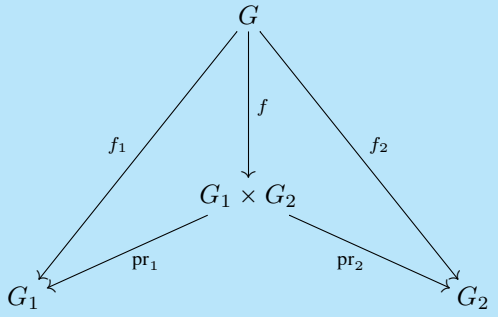
και, κατ' αναλογίαν, $\mathrm{Ker}(\mathrm{pr}_2) = G_1 \times \{e_{G_2}\}$. □

3.6.3 Πρόταση («Καθολική ιδιότητα» ευθέος γινομένου).
Έστω $(G, *)$ *μια ομάδα. Εάν οι* $f_1 : G \longrightarrow G_1$ *και* $f_2 : G \longrightarrow G_2$ *είναι ομομορφισμοί ομάδων, τότε υφίσταται ένας και μόνον ομομορφισμός ομάδων*

$$f : (G, *) \longrightarrow (G_1 \times G_2, \boxdot),$$

τέτοιος ώστε να ισχύει $\mathrm{pr}_1 \circ f = f_1$ *και* $\mathrm{pr}_2 \circ f = f_2$, *δηλαδή τέτοιος ώστε το*

διάγραμμα



να καθίσταται μεταθετικό.

ΑΠΟΔΕΙΞΗ. Ορίζουμε την απεικόνιση

$$f : G \longrightarrow G_1 \times G_2, g \longmapsto f(g) := (f_1(g), f_2(g)).$$

Για κάθε $g \in G$ έχουμε

$$(\mathrm{pr}_1 \circ f)\,(g) = \mathrm{pr}_1(f_1(g), f_2(g)) = f_1(g)$$

και, κατ' αναλογίαν, $(\mathrm{pr}_2 \circ f)\,(g) = f_2(g)$. Εάν η $h : G \longrightarrow G_1 \times G_2$ είναι *τυχούσα* απεικόνιση με $\mathrm{pr}_1 \circ h = f_1$ και $\mathrm{pr}_2 \circ h = f_2$, τότε για κάθε $g \in G$ έχουμε

$$h(g) = (\mathrm{pr}_1(h(g)), \mathrm{pr}_2(h(g))) = (f_1(g), f_2(g)) = f(g),$$

οπότε $h = f$. Επιπροσθέτως, για οιαδήποτε στοιχεία $x, y \in G$ ισχύουν τα εξής:

$$\begin{aligned} &f(x * y) = (\mathrm{pr}_1(f(x * y)), \mathrm{pr}_2(f(x * y))) = ((\mathrm{pr}_1 \circ f)\,(x * y), (\mathrm{pr}_2 \circ f)\,(x * y)) \\ &= (f_1(x * y), f_2(x * y)) = (f_1(x) \circledast f_1(y), f_2(x) \circledcirc f_2(y)) = (f_1(x), f_2(x)) \boxdot (f_1(y), f_2(y)) \\ &= ((\mathrm{pr}_1 \circ f)\,(x), (\mathrm{pr}_2 \circ f)\,(x)) \boxdot ((\mathrm{pr}_1 \circ f)\,(y), (\mathrm{pr}_2 \circ f)\,(y)) = f(x) \boxdot f(y). \end{aligned}$$

Άρα η f είναι ομομορφισμός ομάδων. □

3.6.4 Πρόταση. *Ας συμβολίσουμε ως*

$$\overline{G}_1 := \mathrm{Im}(\iota_1) \ \textit{και} \ \ \overline{G}_2 := \mathrm{Im}(\iota_2)$$

τις εικόνες των φυσικών εμφυτεύσεων

$$\iota_1 : G_1 \longrightarrow G_1 \times G_2 \ \textit{και} \ \ \iota_2 : G_2 \longrightarrow G_1 \times G_2$$

των G_1, G_2 εντός τής $G_1 \times G_2$. Τότε ισχύουν τα ακόλουθα:
(i) *Οι ι_1 και ι_2 είναι μονομορφισμοί ομάδων και, ως εκ τούτου,*

$$G_1 \cong \iota_1(G_1) =: \overline{G}_1, \ \ G_2 \cong \iota_2(G_2) =: \overline{G}_2.$$

(ii) $\overline{G}_1 = \mathrm{Ker}(\mathrm{pr}_2)$ *και* $\overline{G}_2 = \mathrm{Ker}(\mathrm{pr}_1)$.
(iii) $\overline{G}_1 \cap \overline{G}_2 = \{e_{G_1 \times G_2}\}$.
(iv) $\overline{G}_1 \boxdot \overline{G}_2 = G_1 \times G_2$.

ΑΠΟΔΕΙΞΗ. (i) Για οιαδήποτε στοιχεία $x_1, y_1 \in G_1, x_2, y_2 \in G_2$ έχουμε

$$\iota_1(x_1 \circledast y_1) = (x_1 \circledast y_1, e_{G_2}) = \iota_1(x_1) \boxdot \iota_1(y_1)$$

και, κατ' αναλογίαν, $\iota_2(x_2 \circledast y_2) = \iota_2(x_2) \boxdot \iota_2(y_2)$, οπότε οι ι_1 και ι_2 είναι μονομορφισμοί ομάδων.

(ii) Λόγω τής προτάσεως 3.6.2,

$$\overline{G}_1 := \mathrm{Im}(\iota_1) = \{\iota_1(x_1)\,|x_1 \in G_1\} = \{(x_1, e_{G_2})\,|x_1 \in G_1\} = G_1 \times \{e_{G_2}\} = \mathrm{Ker}\,(\mathrm{pr}_2)$$

και, κατ' αναλογίαν, $\overline{G}_2 = \mathrm{Ker}(\mathrm{pr}_1)$.
(iii) Προφανώς,

$$\overline{G}_1 \cap \overline{G}_2 = \big\{(x_1,x_2) \in G_1 \times G_2 \,\big|(x_1,x_2) \in \overline{G}_1 \ \text{ και } \ (x_1,x_2) \in \overline{G}_2\big\}$$
$$\underset{\text{(ii)}}{=} \{(x_1,x_2) \in G_1 \times G_2\,|x_1 = e_{G_1} \ \text{ και } x_2 = e_{G_2}\} = \{(e_{G_1}, e_{G_2})\} = \{e_{G_1\times G_2}\}.$$

(iv) Προφανώς,

$$\overline{G}_1 \boxdot \overline{G}_2 := \big\{(x_1,x_2) \boxdot (y_1,y_2) \,\big|(x_1,x_2) \in \overline{G}_1 \ \text{ και } \ (x_1,x_2) \in \overline{G}_2\big\} \subseteq G_1 \times G_2.$$

Από την άλλη μεριά, για οιοδήποτε στοιχείο $(x_1, x_2) \in G_1 \times G_2$ έχουμε

$$(x_1,x_2) = (x_1, e_{G_2}) \boxdot (e_{G_1}, x_2) \in \overline{G}_1 \boxdot \overline{G}_2,$$

οπότε ισχύει και ο αντίστροφος εγκλεισμός $G_1 \times G_2 \subseteq \overline{G}_1 \boxdot \overline{G}_2$. □

3.6.5 Σημείωση (Απλούστευση συμβολισμού). Στον ορισμό 3.6.1 και στις προτάσεις 3.6.2, 3.6.3 και 3.6.4 χρησιμοποιήσαμε τα σύμβολα "$\circledast$", "$\circledcirc$", "$\boxdot$" για τη σήμανση των εσωτερικών πράξεων επί των G_1, G_2 και $G_1 \times G_2$, αντιστοίχως, προκειμένου να περιγράψουμε επακριβώς τους μεταξύ τους υφιστάμενους συσχετισμούς και τη συμπεριφορά τους ύστερα από εφαρμογή των φυσικών προβολών, των εμφυτεύσεων κ.ά. Ωστόσο, η περαιτέρω διατήρηση ενός τόσο δυσκίνητου συμβολισμού θα μας ήταν κάτι το πολύ φορτικό. Γι' αυτόν τον λόγο θα μεταβούμε, από εδώ και στο εξής, στον *απλουστευμένο πολλαπλασιαστικό* συμβολισμό των πράξεων *και των τριών* ομάδων G_1, G_2 και $G_1 \times G_2$ (μέσω τού συνήθους dot[58] "$\cdot$"), χωρίς επιπρόσθετη συμβολιστική επιβάρυνση[59]. Εξαίρεση θα αποτελέσει μόνον η περίπτωση κατά την οποία θα χρησιμοποιούμε τον *προσθετικό συμβολισμό* για τις πράξεις *αμφοτέρων* των G_1 και G_2, οπότε και θα γράφουμε (ιδιαιτέρως) $G_1 \oplus G_2$ αντί τού $G_1 \times G_2$.

▸ **Ευθύ γινόμενο με πεπερασμένο πλήθος παραγόντων.** Ο ορισμός 3.6.1 γενικεύεται για s τυχούσες ομάδες (όπου $s \in \mathbb{N}$, $s \geqslant 2$) ως ακολούθως:

3.6.6 Ορισμός. Έστω ότι $s \in \mathbb{N}$, $s \geqslant 2$, και ότι οι

$$(G_1, \circledast_1), (G_2, \circledast_2), \ldots, (G_{s-1}, \circledast_{s-1}), (G_s, \circledast_s)$$

είναι s τυχούσες ομάδες. Εφοδιάζοντας το καρτεσιανό γινόμενο

$$\prod_{j=1}^{s} G_j := G_1 \times G_2 \times \cdots \times G_{s-1} \times G_s,$$

των υποκειμένων συνόλων τους με την εσωτερική πράξη

$$\prod_{j=1}^{s} G_j \times \prod_{j=1}^{s} G_j \longrightarrow \prod_{j=1}^{s} G_j$$
$$((x_1,..,x_s),(y_1,..,y_s)) \longmapsto (x_1,..,x_s) \boxdot (y_1,..,y_s) := (x_1 \circledast_1 y_1,..,x_s \circledast_s y_s),$$

παρατηρούμε ότι το ζεύγος $(\prod_{j=1}^{s} G_j, \boxdot)$ αποτελεί ομάδα έχουσα (ως προς την ορισθείσα πράξη " $\boxdot$ ") το $(e_{G_1}, \ldots, e_{G_s})$ ως ουδέτερο στοιχείο της και

[58] Είναι βεβαίως αυτονόητο ότι σε ορισμένες εφαρμογές και σε ορισμένα παραδείγματα, στα οποία μία εκ των υπεισερχομένων ομάδων έχει ως πράξη της τη σύνθεση ή τη (συνήθη) πρόσθεση, το dot υποκαθίσταται αυτομάτως από τα " $\circ$ " και " $+$ ".

[59] Γράφοντας, από εδώ και στο εξής, $G_1 \times G_2$ (χωρίς άλλα σχόλια), θα εννοούμε ότι το εν λόγω καρτεσιανό γινόμενο είναι εφοδιασμένο με την πράξη (3.20). (Ως γνωστόν, ένα τέτοιο καρτεσιανό γινόμενο ομάδων θα μπορούσε να καταστεί ομάδα και με κάποια πράξη *διαφορετική* τής (3.20). Πρβλ. άσκηση 20 τού 6ου φυλλαδίου.)

το $(x_1^{-1}, \ldots, x_s^{-1})$ ως αντίστροφο στοιχείο οιουδήποτε $(x_1, \ldots, x_s) \in \prod_{j=1}^{s} G_j$, όπου x_j^{-1} το αντίστροφο στοιχείο τού $x_j \in G_j$ ως προς την " $\circledast_j$ " για κάθε $j \in \{1, \ldots, s\}$. Η ομάδα $(\prod_{j=1}^{s} G_j, \boxdot)$ καλείται **(εξωτερικό) ευθύ γινόμενο των** $(G_1, \circledast_1), \ldots, (G_s, \circledast_s)$. Έστω $i \in \{1, \ldots, s\}$. Η επίριψη

$$\mathrm{pr}_i : \prod_{j=1}^{s} G_j \longrightarrow G_i,\ (x_1, \ldots, x_s) \mapsto x_i,$$

καλείται (i-οστή) **φυσική προβολή τής** $\prod_{j=1}^{s} G_j$ **επί τής** G_i. Επίσης, η ένριψη

$$\iota_i : G_i \longrightarrow \prod_{j=1}^{s} G_j,\ x \mapsto (e_{G_1}, \ldots, e_{G_{i-1}}, x, e_{G_{i+1}} \ldots, , e_{G_s}),$$

καλείται (i-οστή) **φυσική εμφύτευση τής** G_i **εντός τής** $\prod_{j=1}^{s} G_j$.

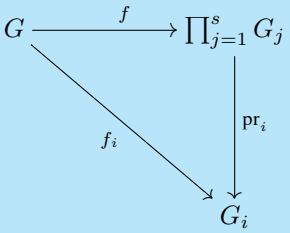
Οι προτάσεις 3.6.7, 3.6.8 και 3.6.9 μπορούν να θεωρηθούν ως άμεσες γενικεύσεις των προτάσεων 3.6.2, 3.6.3 και 3.6.4. Γι' αυτόν τον λόγο οι αποδείξεις τους αφήνονται ως ασκήσεις για τον αναγνώστη.

3.6.7 Πρόταση. *Οι* pr_i *είναι επιμορφισμοί ομάδων έχοντες ως πυρήνες τους τις υποομάδες*

$$\mathrm{Ker}(\mathrm{pr}_i) = G_1 \times \cdots \times G_{i-1} \times \{e_{G_i}\} \times G_{i+1} \times \cdots \times G_s,$$

για κάθε $i \in \{1, \ldots, s\}$.

3.6.8 Πρόταση («Καθολική ιδιότητα» ευθέος γινομένου).
Έστω $(G, *)$ *μια ομάδα. Εάν οι* $f_i : G \longrightarrow G_i$ *είναι ομομορφισμοί ομάδων, τότε υφίσταται ένας και μόνον ομομορφισμός ομάδων* $f : (G, *) \longrightarrow (\prod_{j=1}^{s} G_j, \boxdot)$, *τέτοιος ώστε να ισχύει* $\mathrm{pr}_i \circ f = f_i$, *δηλαδή τέτοιος ώστε το διάγραμμα*



να καθίσταται μεταθετικό για κάθε $i \in \{1, \ldots, s\}$.

3.6.9 Πρόταση. *Για* $i \in \{1, \ldots, s\}$ *ας συμβολίσουμε ως* $\overline{G}_i := \mathrm{Im}(\iota_i)$ *την εικόνα τής φυσικής εμφυτεύσεως*

$$\iota_i : G_i \longrightarrow \prod_{j=1}^{s} G_j,\ x \mapsto (e_{G_1}, \ldots, e_{G_{i-1}}, x, e_{G_{i+1}} \ldots, , e_{G_s}).$$

Τότε για κάθε $i \in \{1, \ldots, s\}$ *ισχύουν τα ακόλουθα*:
(i) *Η* ι_i *είναι μονομορφισμός ομάδων και, ως εκ τούτου,* $G_i \cong \overline{G}_i$.
(ii) $\overline{G}_i = \{e_{G_1}\} \times \cdots \times \{e_{G_{i-1}}\} \times G_i \times \{e_{G_{i+1}}\} \times \cdots \times \{e_{G_s}\}$.
(iii) $\overline{G}_i \cap \left(\overline{G}_1 \boxdot \overline{G}_2 \boxdot \cdots \boxdot \overline{G}_{i-1} \boxdot \overline{G}_{i+1} \boxdot \cdots \boxdot \overline{G}_s\right) = \{(e_{G_1}, \ldots, e_{G_s})\}$.

(iv) $\overline{G}_1 \boxdot \overline{G}_2 \boxdot \cdots \boxdot \overline{G}_s = \prod_{j=1}^{s} G_j$.

3.6.10 Σημείωση (Απλούστευση συμβολισμού). (i) Όπως συνέβη και στην περίπτωση κατά την οποία $s = 2$ (βλ. σημείωση 3.6.5), θα μεταβούμε, από εδώ και στο εξής, στον *απλουστευμένο πολλαπλασιαστικό* συμβολισμό των πράξεων των ομάδων $G_1, \ldots, G_s$ και $\prod_{j=1}^{s} G_j$ (μέσω τού συνήθους dot " $\cdot$ "), με μόνη εξαίρεση τις (κατά τα ειωθότα θεωρούμενες ως) *προσθετικές* ομάδες (για τις οποίες γράφουμε $\bigoplus_{j=1}^{s} G_j$ αντί τού $\prod_{j=1}^{s} G_j$).

(ii) Εάν $G_1 = \cdots = G_s =: G$, τότε αντί τού $\prod_{j=1}^{s} G_j$ γράφουμε απλώς G^s. (Σύμβαση: Ο συμβολισμός αυτός επεκτείνεται προδήλως και για $s = 1$ και $s = 0$. Όταν $s = 0$, τότε ως G^0 νοείται η τετριμμένη ομάδα.)

3.6.11 Πρόταση. *Έστω ότι $s \in \mathbb{N}$, $s \geqslant 2$, και ότι οι $G_1, \ldots, G_s$ είναι s τυχούσες ομάδες. Τότε ισχύουν τα εξής*:

(i) $\left|\prod_{j=1}^{s} G_j\right| = \prod_{j=1}^{s} |G_j|$. *Ως εκ τούτου, το ευθύ γινόμενο $\prod_{j=1}^{s} G_j$ των $G_1, \ldots, G_s$ είναι πεπερασμένη (και αντιστοίχως, άπειρη) ομάδα εάν και μόνον εάν όλες οι ομάδες $G_1, \ldots, G_s$ είναι πεπερασμένες (και αντιστοίχως, εάν και μόνον εάν μία τουλάχιστον εκ των $G_1, \ldots, G_s$ είναι άπειρη).*

(ii) *Για κάθε αμφίριψη $\sigma : \{1, ..., s\} \to \{1, ..., s\}$ υφίσταται ισομορφισμός ομάδων*

$$\boxed{\prod_{j=1}^{s} G_j \cong \prod_{j=1}^{s} G_{\sigma(j)}.}$$

(iii) *Εάν $r \in \mathbb{N}$, $r + 1 \leqslant s$, και $\kappa_1, .., \kappa_r \in \mathbb{N}$ με $1 \leqslant \kappa_1 < \kappa_2 < ... < \kappa_r < s$, τότε*

$$\boxed{\prod_{j=1}^{s} G_j \cong (G_1 \times \cdots \times G_{\kappa_1}) \times (G_{\kappa_1+1} \times \cdots \times G_{\kappa_2}) \times \cdots \times (G_{\kappa_r+1} \times \cdots \times G_s)\,.}$$

(iv) *Εάν υπάρχει δείκτης $i \in \{1, \ldots, s\}$, τέτοιος ώστε η G_i να είναι τετριμμένη, τότε*

$$\boxed{\prod_{j=1}^{s} G_j \cong \prod_{j \in \{1,\ldots,s\} \smallsetminus \{i\}} G_j.}$$

(v) *Εάν οι $H_1, \ldots, H_s$ είναι s ομάδες, τέτοιες ώστε να ισχύει $G_j \cong H_j$ για κάθε δείκτη $j \in \{1, \ldots, s\}$, τότε*

$$\boxed{\prod_{j=1}^{s} G_j \cong \prod_{j=1}^{s} H_j.}$$

Απόδειξη. (i) Τούτο έπεται άμεσα από τις ιδιότητες των πληθικών αριθμών που είναι γνωστές από τη Θεωρία Συνόλων.

(ii) Είναι άμεσος ο έλεγχος τού ότι η απεικόνιση

$$\prod_{j=1}^{s} G_j \ni (g_1, \ldots, g_s) \longmapsto (g_{\sigma(1)}, \ldots, g_{\sigma(s)}) \in \prod_{j=1}^{s} G_{\sigma(j)}$$

αποτελεί ισομορφισμό ομάδων.

(iii) Παρομοίως, διαπιστώνουμε ότι η απεικόνιση

$$\begin{aligned} \prod_{j=1}^{s} G_j &\longrightarrow (G_1 \times \cdots \times G_{\kappa_1}) \times \cdots \times (G_{\kappa_r+1} \times \cdots \times G_s) \\ (g_1, \ldots, g_s) &\longmapsto ((g_1, \ldots, g_{\kappa_1}), \ldots, (g_{\kappa_r+1}, \ldots, g_s)) \end{aligned}$$

είναι ισομορφισμός ομάδων.

(iv) Η απεικόνιση

$$\prod_{j=1}^{s} G_j \longrightarrow \prod_{j\in\{1,\ldots,s\}\smallsetminus\{i\}} G_j,\ (g_1,..,g_{i-1},e_{G_i},g_{i+1},..,g_s)\mapsto(g_1,..,g_{i-1},g_{i+1},..,g_s),$$

είναι προδήλως ένας ισομορφισμός ομάδων.

(v) Έστω ότι οι $f_j : G_j \longrightarrow H_j$ είναι ισομορφισμοί για κάθε $j \in \{1,\ldots,s\}$. Τότε και η απεικόνιση

$$\prod_{j=1}^{s} G_j \ni (g_1,\ldots,g_s) \longmapsto (f_1(g_1),\ldots,f_s(g_s)) \in \prod_{j=1}^{s} H_j$$

είναι ισομορφισμός ομάδων. □

3.6.12 Πόρισμα. *Για οιεσδήποτε ομάδες G_1, G_2, G_3 υφίστανται ισομορφισμοί*

$$G_1 \times G_2 \cong G_2 \times G_1$$

και $(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3)$.

3.6.13 Πρόταση. *Έστω ότι $s \in \mathbb{N}$, $s \geqslant 2$, και ότι οι $G_1,\ldots,G_s$ είναι s τυχούσες ομάδες. Η τάξη οιουδήποτε στοιχείου $(g_1,\ldots,g_s) \in \prod_{j=1}^{s} G_j$ υπολογίζεται ως ακολούθως*:

(i) *Εάν η τάξη* $\mathrm{ord}(g_j)$ *τού στοιχείου g_j εντός τής ομάδας G_j είναι πεπερασμένη για κάθε $j \in \{1,\ldots,s\}$, τότε* $\mathrm{ord}((g_1,\ldots,g_s)) = \mathrm{εκπ}(\mathrm{ord}(g_1),\ldots,\mathrm{ord}(g_s))$.

(ii) *Εάν υπάρχει δείκτης $i_0 \in \{1,\ldots,s\}$, τέτοιος ώστε η τάξη* $\mathrm{ord}(g_{i_0})$ *τού g_{i_0} εντός τής G_{i_0} να είναι άπειρη, τότε* $\mathrm{ord}((g_1,\ldots,g_s)) = \infty$.

Απόδειξη. (i) Εάν η τάξη $\mathrm{ord}(g_j)$ τού g_j εντός τής G_j είναι πεπερασμένη για κάθε $j \in \{1,\ldots,s\}$ και $k \in \mathbb{N}$, τέτοιος ώστε να ισχύει

$$(g_1^k,\ldots,g_s^k) = (g_1,\ldots,g_s)^k = (e_{G_1},\ldots,e_{G_s}),$$

τότε $g_j^k = e_{G_j} \underset{3.4.8}{\Longrightarrow} \mathrm{ord}(g_j) \mid k$ για κάθε $j \in \{1,\ldots,s\}$, οπότε ο k είναι κάποιο *κοινό* πολλαπλάσιο των $\mathrm{ord}(g_1),\ldots,\mathrm{ord}(g_s)$. Κατά συνέπειαν, το *ελάχιστο* κοινό πολλαπλάσιο των $\mathrm{ord}(g_1),\ldots,\mathrm{ord}(g_s)$ είναι ο ελάχιστος φυσικός αριθμός που πληροί την ανωτέρω συνθήκη.

(ii) Εάν $i_0 \in \{1,\ldots,s\}$ με $\mathrm{ord}(g_{i_0}) = \infty$, τότε $g_{i_0}^k \neq e_{G_{i_0}}$ για κάθε $k \in \mathbb{N}$, οπότε

$$(g_1,\ldots,g_{i_0},\ldots,g_s)^k = (g_1^k,\ldots,g_{i_0}^k,\ldots,g_s^k) \neq (e_{G_1},\ldots,e_{G_{i_0}},\ldots,e_{G_s}),$$

για κάθε $k \in \mathbb{N}$. Αυτό σημαίνει ότι $\mathrm{ord}((g_1,\ldots,g_s)) = \infty$. □

3.6.14 Παράδειγμα. Εάν $s \in \mathbb{N}$, $s \geqslant 2$, και εάν οι $m_1,\ldots,m_s$ είναι s φυσικοί αριθμοί, τότε δυνάμει τού πορίσματος 3.4.14 η τάξη οιουδήποτε στοιχείου

$$([a_1]_{m_1},\ldots,[a_s]_{m_s}) \in \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s}$$

ισούται με $\mathrm{ord}(([a_1]_{m_1},\ldots,[a_s]_{m_s})) = \mathrm{εκπ}\left(\frac{m_1}{\mathrm{μκδ}(m_1,a_1)},\ldots,\frac{m_s}{\mathrm{μκδ}(m_s,a_s)}\right)$.

3.6.15 Θεώρημα. *Έστω ότι $s \in \mathbb{N}$, $s \geqslant 2$, και ότι οι $G_1, \ldots, G_s$ είναι s πεπερασμένες ομάδες. Τότε*

$$\exp(\prod_{j=1}^{s} G_j) = \text{εκπ}(\exp(G_1), ..., \exp(G_s)). \tag{3.21}$$

Απόδειξη. Θέτουμε $r_j := \exp(G_j),\ \forall j \in \{1, ..., s\}$. Εάν $s = 2$, τότε

$$G_1 \cong G_1 \times \{e_{G_2}\} \sqsubseteq G_1 \times G_2,\ \ G_2 \cong \{e_{G_1}\} \times G_2 \sqsubseteq G_1 \times G_2$$

και $\text{εκπ}(r_1, r_2) = r_1 t_1 = r_2 t_2$ για κάποιους $t_1, t_2 \in \mathbb{N}$. Το 3.4.25 (iii) δίδει

$$\left.\begin{array}{l} r_1 = \exp(G_1 \times \{e_{G_2}\}) \mid \exp(G_1 \times G_2) \\ r_2 = \exp(\{e_{G_1}\} \times G_2) \mid \exp(G_1 \times G_2) \end{array}\right\} \underset{2.2.25}{\Longrightarrow} \text{εκπ}(r_1, r_2) \mid \exp(G_1 \times G_2),$$

οπότε $\text{εκπ}(r_1, r_2) \leqslant \exp(G_1 \times G_2)$. Εξάλλου, για *οιοδήποτε* $(g_1, g_2) \in G_1 \times G_2$ λαμβάνουμε

$$(g_1, g_2)^{\text{εκπ}(r_1, r_2)} = ((g_1^{r_1})^{t_1}, (g_2^{r_2})^{t_2}) = (e_{G_1}^{t_1}, e_{G_2}^{t_2}) = (e_{G_1}, e_{G_2}) = e_{G_1 \times G_2}$$

και από τον ορισμό 3.4.24 τού εκθέτη έπεται ότι $\exp(G_1 \times G_2) \leqslant \text{εκπ}(r_1, r_2)$. Κατά συνέπειαν, $\exp(G_1 \times G_2) = \text{εκπ}(r_1, r_2)$. Εάν $s \geqslant 3$, τότε χρησιμοποιούμε μαθηματική επαγωγή ως προς το s. Υποθέτουμε ότι η ισότητα (3.21) είναι αληθής για το ευθύ γινόμενο $s - 1$ πεπερασμένων ομάδων. Προφανώς,

$$\begin{aligned} &\exp(\prod_{j=1}^{s} G_j) = \exp(G_1 \times (\prod_{j=2}^{s} G_j)) = \text{εκπ}(r_1, \exp(\prod_{j=2}^{s} G_j)) \\ &= \text{εκπ}(r_1, \text{εκπ}(r_2, ..., r_s)) = \text{εκπ}(r_1, r_2, ..., r_s), \end{aligned}$$

όπου η δεύτερη ισότητα προκύπτει από ό,τι είχαμε αποδείξει στην περίπτωση δύο παραγόντων, η τρίτη από την επαγωγική μας υπόθεση και η τέταρτη από την πρόταση 2.2.27. Άρα η (3.21) είναι αληθής και για s παράγοντες, για *κάθε* $s \geqslant 2$. □

Το *κέντρο* μιας ομάδας αποτελεί το «αβελιανό μέρος» αυτής.

3.6.16 Ορισμός. Έστω $(G, \cdot)$ μια ομάδα. Το σύνολο

$$\boxed{Z(G) := \{\, g \in G \mid\ gx = xg,\ \forall x \in G\}}$$

όλων των στοιχείων τής G που μετατίθενται αμοιβαίως με κάθε στοιχείο τής G καλείται **κέντρο τής** G.

3.6.17 Πρόταση. *Έστω $(G, \cdot)$ μια ομάδα. Τότε το $Z(G)$ αποτελεί μια υποομάδα τής G και*

$$G = Z(G) \iff \textit{η } G \textit{ είναι αβελιανή.}$$

Απόδειξη. Αφήνεται ως άσκηση. □

3.6.18 Πρόταση. *Έστω ότι $s \in \mathbb{N}$, $s \geqslant 2$, και ότι οι $G_1, \ldots, G_s$ είναι s τυχούσες ομάδες. Τότε ισχύουν τα εξής:*

(i) *Το κέντρο τής ομάδας $\prod_{j=1}^{s} G_j$ ισούται με*

$$\boxed{Z(\prod_{j=1}^{s} G_j) = \prod_{j=1}^{s} Z(G_j).}$$

(ii) *$H \prod_{j=1}^{s} G_j$ είναι αβελιανή $\Longleftrightarrow$ η G_j είναι αβελιανή για κάθε $j \in \{1, \ldots, s\}$.*

Απόδειξη. (i) Προφανώς, $(a_1, \ldots, a_s) \in Z(\prod_{j=1}^{s} G_j)$ εάν και μόνον εάν

$$(a_1, \ldots, a_s)(b_1, \ldots, b_s) = (b_1, \ldots, b_s)(a_1, \ldots, a_s),\ \forall (b_1, \ldots, b_s) \in \prod_{j=1}^{s} G_j,$$

$$\Leftrightarrow (a_1 b_1, \ldots, a_s b_s) = (b_1 a_1, \ldots, b_s a_s),\ \forall (b_1, \ldots, b_s) \in \prod_{j=1}^{s} G_j,$$

$$\Leftrightarrow [a_j b_j = b_j a_j,\ \forall b_j \in G_j \ \text{ και } \ \forall j \in \{1, \ldots, s\}] \Leftrightarrow [a_j \in Z(G_j),\ \forall j \in \{1, \ldots, s\}].$$

(ii) Τούτο έπεται από το (i) και την πρόταση 3.6.17. □

▸ **Περί τής «κυκλικότητας» τής $\prod_{j=1}^{s} G_j$.** Βάσει τής προτάσεως 3.6.18 (ii) η $\prod_{j=1}^{s} G_j$ είναι αβελιανή *εάν και μόνον εάν* η G_j είναι αβελιανή για κάθε δείκτη $j \in \{1, ..., s\}$. Κατ' αναλογίαν, εάν η $\prod_{j=1}^{s} G_j$ είναι κυκλική, τότε και η G_j είναι κυκλική ομάδα για κάθε $j \in \{1, ..., s\}$. Ωστόσο, εάν οι G_j, $j \in \{1, ..., s\}$, είναι κυκλικές ομάδες, τότε η $\prod_{j=1}^{s} G_j$ *δεν είναι κατ' ανάγκην κυκλική*, εκτός κι αν πληρούνται κάποιες *επιπρόσθετες συνθήκες* (βλ. τα θεωρήματα 3.6.21 και 3.6.25, και το πόρισμα 3.6.26).

3.6.19 Θεώρημα. *Εάν $s \in \mathbb{N}$, $s \geqslant 2$, και εάν οι $m_1, m_2, \ldots, m_s$ είναι s σχετικώς πρώτοι ανά δύο φυσικοί αριθμοί, τότε*

$$\boxed{\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s},}$$

όπου $m := m_1 m_2 \cdots m_s$.

Απόδειξη. Θεωρούμε την

$$f : \mathbb{Z}_m \longrightarrow \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s},\ [a]_m \longmapsto f([a]_m) := ([a]_{m_1}, [a]_{m_2}, \ldots, [a]_{m_s}).$$

Προφανώς, για οιουσδήποτε $a, b \in \mathbb{Z}$ ισχύουν οι αμφίπλευρες συνεπαγωγές

$$[a]_m = [b]_m \Leftrightarrow a \equiv b (\mathrm{mod}\, m) \Leftrightarrow m \mid a - b \underset{2.4.9}{\Longleftrightarrow} (m_j \mid a - b,\ \ \forall j \in \{1, \ldots, s\})$$

$$\Leftrightarrow \left([a]_{m_j} = [b]_{m_j},\ \ \forall j \in \{1, \ldots, s\}\right) \Leftrightarrow f([a]_m) = f([b]_m).$$

Ακολουθώντας αυτές προς τη (δεξιά) κατεύθυνση "⇒" διαπιστώνουμε ότι η θεωρηθείσα f είναι μια καλώς ορισμένη απεικόνιση. Ακολουθώντας τες προς την (αριστερή) κατεύθυνση "⇐" συμπεραίνουμε ότι η f είναι ενριπτική απεικόνιση. Επειδή $|\mathbb{Z}_m| = m = m_1 m_2 \cdots m_s = |\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s}|$, η f, ως ενριπτική απεικόνιση μεταξύ ισοπληθικών πεπερασμένων συνόλων, είναι επιριπτική και, κατ' επέκταση, αμφιριπτική. Επιπροσθέτως, επειδή για οιουσδήποτε $a, b \in \mathbb{Z}$ έχουμε

$$\begin{aligned} &f([a]_m + [b]_m) = f([a+b]_m) = ([a+b]_{m_1}, [a+b]_{m_2}, \ldots, [a+b]_{m_s}) \\ &= ([a]_{m_1} + [b]_{m_1}, [a]_{m_2} + [b]_{m_2}, \ldots, [a]_{m_s} + [b]_{m_s}) \\ &= ([a]_{m_1}, [a]_{m_2}, \ldots, [a]_{m_s}) + ([b]_{m_1}, [b]_{m_2}, \ldots, [b]_{m_s}) = f([a]_m) + f([b]_m), \end{aligned}$$

η f είναι ομομορφισμός (προσθετικών) ομάδων και, βάσει των προαναφερθέντων, ισομορφισμός. □

3.6.20 Πόρισμα. *Έστω* $n = p_1^{\nu_1} p_2^{\nu_2} \cdots p_\kappa^{\nu_\kappa}$, $\kappa \in \mathbb{N}$, *η κανονική παράσταση* (2.19) *ενός φυσικού αριθμού* $n \geqslant 2$ *ως γινομένου (δυνάμεων) πρώτων αριθμών* $p_1, \ldots, p_\kappa$ *με* $p_1 < \cdots < p_\kappa$ *(όταν* $\kappa \geqslant 2$*) και* $\nu_1, \ldots, \nu_\kappa \in \mathbb{N}$. *Τότε*

$$\boxed{\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\nu_1}} \oplus \mathbb{Z}_{p_2^{\nu_2}} \oplus \cdots \oplus \mathbb{Z}_{p_\kappa^{\nu_\kappa}}.}$$

3.6.21 Θεώρημα. *Εάν* $s \in \mathbb{N}$, $s \geqslant 2$, *και εάν οι* $G_1, G_2, \ldots, G_s$ *είναι* s *πεπερασμένες κυκλικές ομάδες, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Η ομάδα* $G := G_1 \times G_2 \times \cdots \times G_s$ *είναι κυκλική.*

(ii) $\text{μκδ}\left(|G_i|, |G_j|\right) = 1$ *για οιουσδήποτε* $i, j \in \{1, ..., s\}, i \neq j$.

Απόδειξη. Έστω ότι $|G_j| =: m_j \in \mathbb{N}$ για κάθε $j \in \{1, ..., s\}$.

(ii)⇒(i) Εάν $\text{μκδ}(m_i, m_j) = 1$ για οιουσδήποτε $i, j \in \{1, ..., s\}$, $i \neq j$, τότε το (ii) τού θεωρήματος 3.5.26, το (v) τής προτάσεως 3.6.11 και το θεώρημα 3.6.19 μας πληροφορούν ότι $G := G_1 \times G_2 \times \cdots \times G_s \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s} \cong \mathbb{Z}_m$, όπου $m := m_1 m_2 \cdots m_s$, ήτοι ότι η G είναι κυκλική τάξεως m.

(i)⇒(ii) Εάν η ομάδα G είναι κυκλική και εάν υποθέσουμε ότι $\exists i, j \in \{1, ..., s\}, i \neq j$, με $d := \text{μκδ}(m_i, m_j) > 1$, τότε, σύμφωνα με το (ii) τού θεωρήματος 3.4.21, υπάρχει ακριβώς μία μη τετριμμένη υποομάδα H τής G_i και ακριβώς μία μη τετριμμένη υποομάδα K τής G_j με $|H| = d = |K|$. Οι υποομάδες

$$\begin{aligned} \overline{H} &:= \left\{ \left(e_{G_1}, \ldots, e_{G_{i-1}}, x, e_{G_{i+1}}, \ldots, e_{G_s}\right) \middle| \, x \in H \right\}, \\ \overline{K} &:= \left\{ \left(e_{G_1}, \ldots, e_{G_{j-1}}, y, e_{G_{j+1}}, \ldots, e_{G_s}\right) \middle| \, y \in K \right\}, \end{aligned}$$

τής G έχουν τάξη d και $\overline{H} \neq \overline{K}$. Άρα η G δεν είναι κυκλική (εκ νέου λόγω τού (ii) τού θεωρήματος 3.4.21). Άτοπο! Ως εκ τούτου, οι τάξεις $m_1, ..., m_s$ των $G_1, \ldots, G_s$ είναι κατ' ανάγκην σχετικώς πρώτες ανά δύο. □

3.6.22 Πόρισμα. *Εάν* $s \in \mathbb{N}$, $s \geqslant 2$, *και εάν οι* $G_1, \ldots, G_s$ *είναι* s *πεπερασμένες κυκλικές ομάδες, τέτοιες ώστε η* $\prod_{j=1}^{s} G_j$ *να είναι ωσαύτως κυκλική, τότε για ένα στοιχείο* $(g_1, \ldots, g_s) \in \prod_{j=1}^{s} G_j$ *ισχύει η αμφίπλευρη συνεπαγωγή*:

$$\prod_{j=1}^{s} G_j = \langle (g_1, \ldots, g_s) \rangle \iff [G_j = \langle g_j \rangle, \ \forall j \in \{1, ..., s\}].$$

Απόδειξη. Εάν υποθέσουμε ότι $\prod_{j=1}^{s} G_j = \langle (g_1, \ldots, g_s) \rangle$ και εάν θεωρήσουμε τυχόντα στοιχεία $x_1 \in G_1, \ldots, x_s \in G_s$, τότε υπάρχουν $k_1, \ldots, k_s \in \mathbb{Z}$, τέτοιοι ώστε να ισχύουν οι ισότητες

$$(g_1, \ldots, g_s)^{k_j} = (e_{G_1}, \ldots, e_{G_{j-1}}, x_j, e_{G_{j+1}}, \ldots, e_{G_s}), \ \forall j \in \{1, ..., s\},$$

οπότε $[x_j = g_j^{k_j}, \ \forall j \in \{1, ..., s\}] \Longrightarrow [x_j \in \langle g_j \rangle, \ \forall j \in \{1, ..., s\}]$ και, ως εκ τούτου, $G_j = \langle g_j \rangle, \ \forall j \in \{1, ..., s\}$. Και αντιστρόφως· εάν έχουμε $G_j = \langle g_j \rangle, \ \forall j \in \{1, ..., s\}$, τότε από την υπόθεσή μας και το θεώρημα 3.6.21 έπεται ότι $\text{μκδ}(|G_i|, |G_j|) = 1$ για οιουσδήποτε $i, j \in \{1, ..., s\}, i \neq j$. Εξ αυτού συμπεραίνουμε (μέσω τού πορίσματος 2.3.20) ότι

$$\text{εκπ}(|G_1|, \ldots, |G_s|) = \prod_{j=1}^{s} |G_j| = \left| \prod_{j=1}^{s} G_j \right|. \tag{3.22}$$

Επιπροσθέτως, μέσω τού 3.6.13 (i) λαμβάνουμε

$$\text{ord}(g_1, \ldots, g_s) = \text{εκπ}(\text{ord}\,(g_1), \ldots, \text{ord}\,(g_2)) = \text{εκπ}(|G_1|, \ldots, |G_s|), \tag{3.23}$$

όπου η δεύτερη ισότητα προκύπτει από την πρόταση 3.4.7. Οι (3.22) και (3.23) δίδουν $\mathrm{ord}(g_1,\dots,g_s) = \left|\prod_{j=1}^{s} G_j\right|$, οπότε εκ νέου εφαρμογή τής προτάσεως 3.4.7 μας οδηγεί στο ότι ισχύει η ισότητα $\prod_{j=1}^{s} G_j = \langle (g_1,\dots,g_s)\rangle$. □

3.6.23 Πόρισμα. *Εάν οι G_1 και G_2 είναι δυο πεπερασμένες κυκλικές ομάδες, τότε ισχύουν τα εξής*:
(i) *Η $G_1 \times G_2$ είναι κυκλική εάν και μόνον εάν* μκδ$(|G_1|, |G_2|) = 1$.
(ii) *Εάν η $G_1 \times G_2$ είναι κυκλική και $g_1 \in G_1$, $g_2 \in G_2$, τότε*

$$G_1 \times G_2 = \langle (g_1, g_2)\rangle \iff [G_1 = \langle g_1\rangle \ \text{ και } \ G_2 = \langle g_2\rangle].$$

3.6.24 Λήμμα. *Εάν η $(H,\cdot)$ είναι μια μη τετριμμένη ομάδα, τότε η $H \times \mathbb{Z}$ είναι μη κυκλική.*

Απόδειξη. Ας υποθέσουμε ότι η $H \times \mathbb{Z}$ είναι κυκλική. Τότε υπάρχουν στοιχεία $a \in H \setminus \{e_H\}$ και $b \in \mathbb{Z}\setminus\{0\}$, τέτοια ώστε να ισχύει $H \times \mathbb{Z} = \langle (a,b)\rangle$. Επειδή έχουμε $(a,0) \in H \times \mathbb{Z}$, θα πρέπει να υπάρχει κάποιος $k \in \mathbb{Z}$ με

$$(a,b)^k = (a^k, kb) = (a,0) \Rightarrow k = 0 \ \text{ και } \ a = a^0 = e_H.$$

Άτοπο (αφού εξ υποθέσεως $a \neq e_H$)! Άρα η $H \times \mathbb{Z}$ είναι όντως μη κυκλική. □

3.6.25 Θεώρημα. *Έστω ότι $s \in \mathbb{N}$, $s \geqslant 2$, και ότι οι $G_1, G_2, \dots, G_s$ είναι s ομάδες. Εάν η $G := G_1 \times \cdots \times G_s$ είναι κυκλική, τότε ισχύουν τα ακόλουθα*:
(i) *Η G_j είναι κυκλική ομάδα για κάθε $j \in \{1,...,s\}$.*
(ii) *Εάν η G είναι πεπερασμένη, τότε* μκδ $(|G_i|, |G_j|) = 1$ *για οιουσδήποτε δείκτες $i, j \in \{1,...,s\}, i \neq j$.*
(iii) *Εάν η G είναι πεπερασμένη και $G = \langle (g_1,\dots,g_s)\rangle$, τότε $G_j = \langle g_j\rangle$ για κάθε δείκτη $j \in \{1,...,s\}$.*
(iv) *Εάν η G είναι άπειρη, τότε $\exists i_0 \in \{1,...,s\} : G_{i_0} \cong \mathbb{Z}$ και η G_j είναι τετριμμένη για κάθε $j \in \{1,...,s\}\setminus\{i_0\}$.*

Απόδειξη. (i) Κατά τα 3.6.9 (i)-(ii), $G_j \cong \overline{G}_j \sqsubseteq G$, οπότε G_j είναι κυκλική ομάδα για κάθε $j \in \{1,...,s\}$ (βλ. 3.3.19 (ii) και 3.5.22 (iii)).

(ii) Τούτο έπεται από το θεώρημα 3.6.21.

(iii) Η απόδειξη είναι πανομοιότυπη εκείνης τής " ⇒ " τού πορίσματος 3.6.22.

(iv) Εάν η G είναι άπειρη, τότε $\exists i_0 \in \{1,...,s\}$, τέτοιος ώστε η G_{i_0} να είναι άπειρη (βλ. 3.6.11 (i)) και (λόγω τού (i)) κυκλική. Άρα $G_{i_0} \cong \mathbb{Z}$ (βλ. 3.5.26 (i)). Ας υποθέσουμε ότι $\nu := \mathrm{card}(\{j \in \{1,...,s\}\setminus\{i_0\} \mid G_j \text{ μη τετριμμένη}\})$. Προφανώς (λόγω των 3.6.11 (ii) και (iv)) $G \cong H \times \mathbb{Z}$, για κάποια ομάδα $H \cong \mathbb{Z}^\nu$. Θα αποδείξουμε ότι $\nu = 0$. Εάν $\nu \geqslant 1$, τότε η G δεν θα ήταν κυκλική βάσει τού λήμματος 3.6.24. □

3.6.26 Πόρισμα. *Έστω ότι $s \in \mathbb{N}$, $s \geqslant 2$, και ότι οι $G_1, G_2, \dots, G_s$ είναι s κυκλικές ομάδες. Εάν η $G := G_1 \times \cdots \times G_s$ είναι άπειρη και το πλήθος των μη τετριμμένων παραγόντων της είναι $\geqslant 2$, τότε η G είναι αβελιανή μη κυκλική.*

Απόδειξη. Εάν η G ήταν κυκλική, τότε (σύμφωνα με το 3.6.25 (iv)) θα όφειλε να διαθέτει μόνον έναν μη τετριμμένο παράγοντα. □

ΚΕΦΑΛΑΙΟ 4

Ομάδες μετατάξεων

Η αναδιευθέτηση ή μετάταξη των στοιχείων ενός συνόλου είναι μια οικεία έννοια· επί παραδείγματι, εναλλάσσοντας τα 1 και 3, και αφήνοντας το 2 αμετάβλητο, λαμβάνουμε μια μετάταξη τού συνόλου $\{1,2,3\}$. Στο παρόν κεφάλαιο εξηγείται το πώς *κάθε* ομάδα είναι δυνατόν να εκληφθεί (μέχρις ισομορφισμού) ως μια *ομάδα μετατάξεων*. Επίσης, παρατίθενται ποικίλα *παραδείγματα* ομάδων μετατάξεων, η χρησιμότητα των οποίων θα αναφανεί ήδη στο αμέσως επόμενο κεφάλαιο.

4.1 Η ΣΥΜΜΕΤΡΙΚΗ ΟΜΑΔΑ

4.1.1 Ορισμός. (i) Έστω A ένα μη κενό σύνολο και

$$\mathfrak{S}_A := \mathbf{Bij}\,(A,A) := \left\{ \sigma : A \longrightarrow A \;\middle|\; \begin{array}{c} \sigma \text{ αμφιριπτική απεικόνιση} \\ \text{από το } A \text{ επί τού } A \end{array} \right\}.$$

Τότε το ζεύγος $(\mathfrak{S}_A, \circ)$, όπου "$\circ$" η πράξη τής συνθέσεως απεικονίσεων, αποτελεί μια ομάδα, τη λεγομένη **συμμετρική ομάδα** επί τού συνόλου A (με την ταυτοτική απεικόνιση id_A ως ουδέτερό της στοιχείο). Από «ομαδοθεωρητική» άποψη, η ομάδα $\mathfrak{S}_A$ δεν εξαρτάται από το ίδιο το σύνολο A, αλλά μόνον από τον πληθικό του αριθμό $\mathrm{card}(A)$. (Πράγματι· εάν το B είναι ένα άλλο σύνολο που έχει τον ίδιο πληθικό αριθμό με το A, τότε υπάρχει μια αμφίρριψη $f : A \longrightarrow B$, οπότε η απεικόνιση

$$\mathfrak{S}_A \longrightarrow \mathfrak{S}_B, \;\; \sigma \longmapsto f \circ \sigma \circ f^{-1},$$

είναι ένας *ισομορφισμός ομάδων*). Τα στοιχεία τής ομάδας $\mathfrak{S}_A$ ονομάζονται **μετατάξεις**[1]. Όταν $\sigma \in \mathfrak{S}_A \setminus \{\mathrm{id}_A\}$, η σ «μετατάσσει» *κυριολεκτικώς* τουλάχιστον ένα εκ των στοιχείων τού A, δηλαδή το απεικονίζει σε ένα άλλο (διαφορετικό) στοιχείο τού A. Εάν το θεωρούμενο A είναι ένα *πεπερασμένο* σύνολο και $n = \mathrm{card}(A)$, τότε μπορούμε δίχως βλάβη τής γενικότητας να υποθέσουμε ότι $A = \{1, ..., n\}$. Εν τοιαύτη περιπτώσει η $\mathfrak{S}_A$ συμβολίζεται ως $\mathfrak{S}_n$ και καλείται **συμμετρική ομάδα σε n σύμβολα**.

(ii) Συνήθως γράφουμε τις μετατάξεις $\sigma \in \mathfrak{S}_n$ υπό τη μορφή

$$\begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{bmatrix} \text{ ή } \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ \sigma(x_1) & \sigma(x_2) & \cdots & \sigma(x_n) \end{bmatrix}$$

στην περίπτωση όπου τα $x_1, \ldots, x_n$ αποτελούν μια αναδιάταξη των αριθμών $1, 2, \ldots, n$. Αυτός ο τρόπος γραφής μάς διευκολύνει κατά τον υπολογισμό τής συνθέσεως δύο μετατάξεων. Π.χ.,

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{bmatrix}.$$

Θα πρέπει να επισημανθεί ότι κατά την εκτέλεση τής συνθέσεως *προηγείται* η εφαρμογή τής δεξιάς απεικονίσεως και *ακολουθεί* η εφαρμογή τής αριστεράς. Γενικότερα, για τυχούσες μετατάξεις τ και $\sigma \in \mathfrak{S}_n$ έχουμε

$$\begin{bmatrix} 1 & \cdots & n \\ \tau(\sigma(1)) & \cdots & \tau(\sigma(n)) \end{bmatrix} = \begin{bmatrix} 1 & \cdots & n \\ \tau(1) & \cdots & \tau(n) \end{bmatrix} \circ \begin{bmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{bmatrix}.$$

4.1.2 Σημείωση. (i) Η αντίστροφος σ^{-1} μιας μετατάξεως $\sigma \in \mathfrak{S}_n$ (που είναι ταυτόσημη με το ομαδοθεωρητικό αντίστροφο στοιχείο τής σ εντός τής $\mathfrak{S}_n$) έχει πολύ απλή μορφή. Εάν γράψουμε την σ ως

$$\begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{bmatrix},$$

τότε η σ^{-1} είναι η

$$\begin{bmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{bmatrix}.$$

(ii) Για λόγους συντομίας, θα συμβολίζουμε το ουδέτερο στοιχείο $\mathrm{id}_{\{1,\ldots,n\}}$ τής $\mathfrak{S}_n$ απλώς ως id.

(iii) Όταν $n \geqslant 3$, η $\mathfrak{S}_n$ *δεν* είναι αβελιανή. Πράγματι· ορίζοντας τις $\sigma, \tau \in \mathfrak{S}_n$ ως ακολούθως:

$$\sigma(1) = 1, \quad \sigma(2) = 3, \quad \sigma(3) = 2, \quad \sigma(j) = j, \quad \forall j \in \{4, ..., n\},$$
$$\tau(1) = 2, \quad \tau(2) = 1, \quad \tau(3) = 3, \quad \tau(j) = j, \quad \forall j \in \{4, ..., n\},$$

λαμβάνουμε $(\tau \circ \sigma)(1) = 2 \neq 3 = (\sigma \circ \tau)(1)$. Επομένως, $\tau \circ \sigma \neq \sigma \circ \tau$.

4.1.3 Πρόταση. *Η τάξη τής ομάδας $\mathfrak{S}_n$ ισούται με*

$$\boxed{|\mathfrak{S}_n| = n!}$$

Απόδειξη. Με τη βοήθεια τής (κλασικής) μαθηματικής επαγωγής θα αποδείξουμε -γενικότερα- ότι αληθεύει ο ακόλουθος ισχυρισμός:

Ισχυρισμός: *Εάν τα $A = \{x_1, \ldots, x_n\}$ και $B = \{y_1, \ldots, y_n\}$ είναι δυο σύνολα που περιέχουν (ακριβώς) n στοιχεία, τότε το σύνολο*

$$\mathbf{Bij}(A, B) := \{f : A \longrightarrow B \mid f \text{ αμφιρριπτική απεικόνιση}\}$$

έχει ακριβώς $n!$ στοιχεία.

Για $n = 1$ ο ισχυρισμός είναι αληθής. Ας υποθέσουμε ότι για κάποιον $n > 1$ ισχύει $\mathrm{card}(\mathbf{Bij}(A', B')) = (n-1)!$ για οιαδήποτε σύνολα A', B' που διαθέτουν (ακριβώς) $n-1$ στοιχεία. Έστω τώρα ότι τα $A = \{x_1, \ldots, x_n\}$ και $B = \{y_1, \ldots, y_n\}$ είναι δυο σύνολα που περιέχουν (ακριβώς) n στοιχεία. Για κάθε $j \in \{1, \ldots, n\}$ ορίζουμε το

$$\mathbf{Bij}(A, B)_j := \{f \in \mathbf{Bij}(A, B) \mid f(x_1) = y_j\}.$$

[1] Χρησιμοποιείται το προσήκον ουσιαστικό *μετάταξη* αντί τού *μετάθεση* για τη μετάφραση τού όρου permutation, καθότι η επιλογή τού δευτέρου θα οδηγούσε σε ατυχή ομοειδή απόδοση των ρημάτων commute και permute. (Σημειωτέον ότι όλες οι permutation groups $\mathfrak{S}_n$, $n \geqslant 3$, είναι μη μεταθετικές ομάδες! Εξάλλου, το ουσιαστικό *αντιμετάθεση* δεσμεύεται για την απόδοση τού όρου transposition.)

Προφανώς η απεικόνιση

$$\mathbf{Bij}\,(A,B)_j \longrightarrow \mathbf{Bij}\,(A\smallsetminus\{x_1\}, B\smallsetminus\{y_j\})\,, \quad f \longmapsto f|_{A\smallsetminus\{x_1\}}\,,$$

είναι αμφιρριπτική. Επομένως, κατά την επαγωγική μας υπόθεση,

$$\text{card}\left(\mathbf{Bij}\,(A,B)_j\right) = (n-1)!.$$

Επιπροσθέτως, $\mathbf{Bij}\,(A,B) = \coprod_{j=1}^{n} \mathbf{Bij}\,(A,B)_j$. Εξ αυτού συνάγεται ότι

$$\text{card}\,(\mathbf{Bij}\,(A,B)) = \sum_{j=1}^{n} \text{card}\left(\mathbf{Bij}\,(A,B)_j\right) = n\cdot(n-1)! = n!.$$

Άρα $|\mathfrak{S}_n| = n!$. □

4.1.4 Ορισμός. (i) Εάν $\sigma \in \mathfrak{S}_n$, τότε το σύνολο

$$\text{supp}(\sigma) := \{j \in \{1,...,n\} \mid \sigma(j) \neq j\ \}$$

εκείνων των στοιχείων τού $\{1,...,n\}$ που «μετατάσσονται» *κυριολεκτικώς* (δηλαδή δεν παραμένουν αμετάβλητα) μέσω τής σ καλείται **φορέας τής** σ.

(ii) Λέμε ότι δυο μετατάξεις $\sigma, \tau \in \mathfrak{S}_n$ είναι **ξένες μεταξύ τους** όταν για οιουσδήποτε φυσικούς αριθμούς $j,k \in \{1,\ldots,n\}$ ισχύουν (ταυτοχρόνως) οι συνεπαγωγές

$$\sigma\,(j) \neq j \Rightarrow \tau(j) = j \quad \text{και} \quad \tau\,(k) \neq k \Rightarrow \sigma(k) = k.$$

4.1.5 Πρόταση. *Δυο μετατάξεις $\sigma, \tau \in \mathfrak{S}_n$ είναι ξένες μεταξύ τους εάν και μόνον εάν* $\text{supp}(\sigma)\cap\ \text{supp}(\tau) = \varnothing$.

Απόδειξη. Εάν οι $\sigma, \tau \in \mathfrak{S}_n$ είναι ξένες μεταξύ τους και $j \in \text{supp}(\sigma)$, τότε

$$\sigma(j) \neq j \Rightarrow \tau(j) = j \Rightarrow j \notin \text{supp}(\tau).$$

Άρα $\text{supp}(\sigma)\cap\ \text{supp}(\tau) = \varnothing$. Και αντιστρόφως· εάν υποθέσουμε ότι οι φορείς των σ και τ δεν διαθέτουν κανένα κοινό στοιχείο και θεωρήσουμε οιονδήποτε $j \in \{1,...,n\}$ για τον οποίο ισχύει $\sigma(j) \neq j$, τότε $j \in \text{supp}(\sigma)$. Εξ υποθέσεως, $j \notin \text{supp}(\tau) \Rightarrow \tau(j) = j$. Κατ' αναλογίαν, εάν $k \in \{1,...,n\}$ με $\tau\,(k) \neq k$, τότε

$$k \in \text{supp}(\tau) \Rightarrow k \notin \text{supp}(\sigma) \Rightarrow \sigma(k) = k.$$

Ως εκ τούτου, οι σ, τ είναι ξένες μεταξύ τους. □

4.1.6 Παράδειγμα. Εντός τής $\mathfrak{S}_4$ οι μετατάξεις

$$\sigma := \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{bmatrix}, \quad \tau := \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{bmatrix}$$

είναι ξένες μεταξύ τους, διότι οι φυσικοί 2 και 3 μετατάσσονται μέσω τής σ και μένουν αμετάβλητοι μέσω τής τ, ενώ οι φυσικοί 1 και 4 μετατάσσονται μέσω τής τ και μένουν αμετάβλητοι μέσω τής σ.

4.1.7 Πρόταση. *Εάν δυο μετατάξεις $\sigma, \tau \in \mathfrak{S}_n$ είναι ξένες μεταξύ τους, τότε μετατίθενται αμοιβαίως, δηλαδή $\sigma \circ \tau = \tau \circ \sigma$.*

Αποδειξη. Εάν οι μετατάξεις σ, τ είναι ξένες μεταξύ τους, αρκεί θα δείξουμε ότι

$$(\sigma \circ \tau)(j) = (\tau \circ \sigma)(j), \quad \forall j \in \{1, ..., n\}. \tag{4.1}$$

Για κάθε $j \in \{1, ..., n\} \setminus (\text{supp}(\sigma) \cup \text{supp}(\tau))$ έχουμε

$$j \notin \text{supp}(\sigma) \text{ και } j \notin \text{supp}(\tau) \Rightarrow \sigma(j) = j = \tau(j),$$

οπότε $(\sigma \circ \tau)(j) = \sigma(\tau(j)) = \sigma(j) = j$ και $(\tau \circ \sigma)(j) = \tau(\sigma(j)) = \tau(j) = j$. Απομένει να αποδειχθεί ότι ισχύει η (4.1) για όλους τους φυσικούς τους ανήκοντες στην ένωση των φορέων των σ και τ. Έστω τυχών $j \in (\text{supp}(\sigma) \cup \text{supp}(\tau))$. Τότε είτε $j \in \text{supp}(\sigma)$ είτε $j \in \text{supp}(\tau)$. Εάν $j \in \text{supp}(\sigma)$, λαμβάνοντας υπ' όψιν ότι οι σ, τ είναι ξένες μεταξύ τους συμπεραίνουμε ότι

$$j \in \text{supp}(\sigma) \setminus \text{supp}(\tau) \Rightarrow \tau(j) = j \neq \sigma(j) \Rightarrow (\sigma \circ \tau)(j) = \sigma(\tau(j)) = \sigma(j) \neq j.$$

Από την τελευταία σχέση έπεται ότι $\sigma(\sigma(j)) \neq \sigma(j)$ (καθότι η σ είναι ενριπτική). Αυτό σημαίνει ότι $\sigma(j) \notin \text{supp}(\tau) \Rightarrow \tau(\sigma(j)) = \sigma(j)$, οπότε

$$(\sigma \circ \tau)(j) = \sigma(\tau(j)) = \sigma(j) = \tau(\sigma(j)) = (\tau \circ \sigma)(j), \quad \forall j \in \text{supp}(\sigma).$$

Με ανάλογη επιχειρηματολογία (ύστερα από εναλλαγή των ρόλων των σ και τ) αποδεικνύεται ότι η (4.1) είναι αληθής ακόμη και για τους φυσικούς j τους ανήκοντες στον φορέα τής τ. □

4.1.8 Παρατήρηση. Το αντίστροφο τής προτάσεως 4.1.7 δεν είναι αληθές. Επί παραδείγματι, εντός τής $\mathfrak{S}_4$ οι μετατάξεις

$$\sigma := \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}, \quad \tau := \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix}$$

είναι αμοιβαίως μετατιθέμενες με

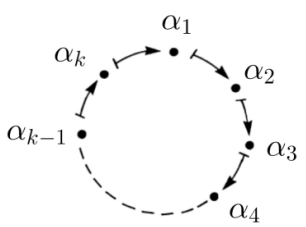
$$\sigma \circ \tau = \tau \circ \sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix},$$

αλλά δεν είναι ξένες μεταξύ τους, διότι $\text{supp}(\sigma) \cap \text{supp}(\tau) = \{1, 2, 3, 4\} \neq \varnothing$.

4.2 ΚΥΚΛΟΙ

4.2.1 Ορισμός. Μια μετάταξη $\sigma \in \mathfrak{S}_n$ λέγεται **κύκλος μήκους** k (όπου $k \in \mathbb{N}$) ή k-**κύκλος**[2] και γράφεται ως $[\alpha_1\ \alpha_2\ \ldots\ \alpha_k]$ όταν υπάρχουν k σαφώς διακεκριμένοι αριθμοί $\alpha_1, \alpha_2, \ldots, \alpha_k$ από το σύνολο $\{1, \ldots, n\}$ $(k \leqslant n)$, ούτως ώστε να ισχύει

$$\begin{cases} \sigma(\alpha_1) = \alpha_2, \sigma(\alpha_2) = \alpha_3, \ldots, \sigma(\alpha_{k-1}) = \alpha_k, \sigma(\alpha_k) = \alpha_1 \text{ (για } k \geqslant 2) \\ (\sigma(\alpha_1) = \alpha_1, \text{ για } k = 1) \text{ και } \sigma(\beta) = \beta, \ \forall \beta \in \{1, .., n\} \setminus \{\alpha_1, .., \alpha_k\}. \end{cases}$$



(Προφανώς, $\mathrm{supp}([\alpha_1\ \alpha_2\ \ldots\ \alpha_k]) = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ όταν $k \geqslant 2$ και κάθε 1-κύκλος ισούται με την id.) Ο συμβολισμός για το «γινόμενο» (= σύνθεση) δυο κύκλων ακολουθεί τη συλλογιστική εκείνου που προαναφέραμε για τις μετατάξεις. Έτσι π.χ. εντός τής $\mathfrak{S}_n$, $n \geqslant 3$, έχουμε $[2\ 3] \circ [1\ 2] = [1\ 3\ 2]$, και εντός τής $\mathfrak{S}_n$, $n \geqslant 8$,

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 6 & 7 & 3 & 5 & 4 & 2 \end{bmatrix} = [1\ 8\ 2] \circ [3\ 6\ 5] \circ [4\ 7]\,.$$

Οι 2-κύκλοι ονομάζονται, ιδιαιτέρως, **αντιμεταθέσεις**.

4.2.2 Παράδειγμα. Τα στοιχεία τής $\mathfrak{S}_3$ είναι τα

$$\mathrm{id},\ [1\,2]\,,\ [1\,3]\,,\ [2\,3]\,,\ [1\,2\,3]\,,\ [1\,3\,2]\,,$$

με $[1\,2\,3] = [1\,3] \circ [1\,2]$ και $[1\,3\,2] = [2\,3] \circ [1\,2]$, ενώ ο κατάλογος τής πράξεως "$\circ$" τής $\mathfrak{S}_3$ είναι ο εξής:

$\circ$	id	$[1\,2]$	$[1\,3]$	$[2\,3]$	$[1\,2\,3]$	$[1\,3\,2]$
id	id	$[1\,2]$	$[1\,3]$	$[2\,3]$	$[1\,2\,3]$	$[1\,3\,2]$
$[1\,2]$	$[1\,2]$	id	$[1\,3\,2]$	$[1\,2\,3]$	$[2\,3]$	$[1\,3]$
$[1\,3]$	$[1\,3]$	$[1\,2\,3]$	id	$[1\,3\,2]$	$[1\,2]$	$[2\,3]$
$[2\,3]$	$[2\,3]$	$[1\,3\,2]$	$[1\,2\,3]$	id	$[1\,3]$	$[1\,2]$
$[1\,2\,3]$	$[1\,2\,3]$	$[1\,3]$	$[2\,3]$	$[1\,2]$	$[1\,3\,2]$	id
$[1\,3\,2]$	$[1\,3\,2]$	$[2\,3]$	$[1\,2]$	$[1\,3]$	id	$[1\,2\,3]$

Η εκτέλεση πράξεων με κύκλους διευκολύνεται αισθητά εάν κανείς λάβει υπ' όψιν ορισμένες χαρακτηριστικές ιδιότητες τους που δίδονται στην επόμενη πρόταση.

4.2.3 Πρόταση (Ιδιότητες κύκλων). *Για τους k-κύκλους (εντός τής $\mathfrak{S}_n$) ισχύουν τα εξής*:

(i) $[\alpha_1\ \alpha_2\ \ldots\ \alpha_k] = [\alpha_2\ \alpha_3\ \ldots\ \alpha_k\ \alpha_1] = \cdots = [\alpha_k\ \alpha_1\ \ldots\ \alpha_{k-1}]$, *ήτοι όλες οι «κυκλικές εναλλαγές» των k στοιχείων ενός k-κύκλου είναι ίσες μεταξύ τους.*

(ii) *Εάν $k \geqslant 3$, τότε $[\alpha_1\ \alpha_2\ \ldots\ \alpha_k] = [\alpha_1\ \ldots\ \alpha_j] \circ [\alpha_j\ \alpha_{j+1}\ \ldots\ \alpha_k]$, για κάθε $j \in \{2, .., k-1\}$.*

(iii) *Εάν $k \geqslant 3$, τότε*

$$[\alpha_1\ \alpha_2\ \ldots\ \alpha_k] = [\alpha_1\ \alpha_2]\ \circ [\alpha_2\ \alpha_3] \circ \cdots \circ [\alpha_{k-1}\ \alpha_k] \tag{4.2}$$

και

$$[\alpha_1\ \alpha_2\ \ldots\ \alpha_k] = [\alpha_1\ \alpha_k]\ \circ [\alpha_1\ \alpha_{k-1}] \circ \cdots \circ [\alpha_1\ \alpha_2]. \tag{4.3}$$

(iv) *Για κάθε $m \in \mathbb{N}$ ισχύει η ισότητα*

$$[\alpha_1\ \alpha_2\ \ldots\ \alpha_k]^m = \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_{m+1} & a_{m+2} & \cdots & a_{m+k} \end{bmatrix},$$

όπου οι (υπο)δείκτες τής κάτω γραμμής οφείλουν να «διαβάζονται κατά μόδιο k», ήτοι $a_{k+1} = a_1$, $a_{k+2} = a_2, \ldots\ldots, a_{k+t} = a_l$, όπου $t \equiv l (\mathrm{mod}\, k)$ $(t, l \in \mathbb{N})$.

(v) $\mathrm{ord}([\alpha_1\ \alpha_2\ \ldots\ \alpha_k]) = k$.

(vi) $[\alpha_1\ \alpha_2\ \ldots\ \alpha_k]^{-1} = [\alpha_k\ \alpha_{k-1}\ \ldots\ \alpha_1]$.

[2] Πρόκειται κατ' ουσίαν για έναν *προσανατολισμένο κύκλο* ως προς κάποιον *προεπιλεγμένο* προσανατολισμό.

(vii) *Για κάθε $\sigma \in \mathfrak{S}_n$ ισχύει η ισότητα*

$$\boxed{\sigma \circ [\alpha_1\ \alpha_2\ \ldots\ \alpha_k] \circ \sigma^{-1} = [\sigma(\alpha_1)\ \sigma(\alpha_2)\ \ldots\ \sigma(\alpha_k)].} \tag{4.4}$$

Απόδειξη. Το (i) είναι εξ ορισμού προφανές. Το (ii) είναι άμεση συνέπεια τού υπολογισμού τού γινομένου (= συνθέσεως).

(iii) Η ισότητα (4.2) έπεται από το (ii) (για $j = 2$) και εφαρμογή τής πρώτης μορφής τής μαθηματικής επαγωγής ως προς τον k, εκκινώντας από τον $k = 3$. Η (4.3) ισχύει για $k = 3$, διότι το $[\alpha_1\ \alpha_3] \circ [\alpha_1\ \alpha_2]$ ισούται με

$$\begin{bmatrix} a_1 & \cdots & a_2 & \cdots & a_3 \\ a_3 & \cdots & a_2 & \cdots & a_1 \end{bmatrix} \circ \begin{bmatrix} a_1 & \cdots & a_2 & \cdots & a_3 \\ a_2 & \cdots & a_1 & \cdots & a_3 \end{bmatrix} = [\alpha_1\ \alpha_2\ \alpha_3].$$

Για $k \geqslant 4$ αρκεί να εφαρμόσουμε εκ νέου την πρώτη μορφή τής μαθηματική επαγωγής ως προς τον k.

(iv) Εδώ εφαρμόζεται κλασική μαθηματική επαγωγή ως προς τον m. Για $m = 1$ ο ισχυρισμός είναι προφανώς αληθής. Εάν υποθέσουμε ότι είναι αληθής για κάποιον $m \geqslant 1$, τότε

$$\begin{aligned} [\alpha_1\ \alpha_2\ \ldots\ \alpha_k]^{m+1} &= [\alpha_1\ \alpha_2\ \ldots\ \alpha_k]^m \circ [\alpha_1\ \alpha_2\ \ldots\ \alpha_k] \\ &= \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_{m+1} & a_{m+2} & \cdots & a_{m+k} \end{bmatrix} \circ \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_2 & a_3 & \cdots & a_1 \end{bmatrix} \\ &= \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_{m+2} & a_{m+3} & \cdots & a_{m+1+k} \end{bmatrix}, \end{aligned}$$

όπου η δεύτερη ισότητα έπεται από την επαγωγική μας υπόθεση.

(v) Εάν $\sigma := [\alpha_1\ \alpha_2\ \ldots\ \alpha_k]$, τότε από το (iv) λαμβάνουμε

$$\begin{aligned} \sigma^k &= [\alpha_1\ \alpha_2\ \ldots\ \alpha_k]^k \\ &= \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_{k+1} & a_{k+2} & \cdots & a_{k+k} \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_1 & a_2 & \cdots & a_k \end{bmatrix} = \mathrm{id}. \end{aligned}$$

Εάν $\varrho \in \{1, ..., k-1\}$, τότε $\sigma^\varrho(a_j) = a_{j+\varrho}$, $\forall j \in \{1, ..., k\}$, οπότε

$$j + \varrho \not\equiv j (\mathrm{mod}\, k), \forall j \in \{1, ..., k\} \Longrightarrow \sigma^\varrho \neq \mathrm{id} \Longrightarrow \mathrm{ord}\,([\alpha_1\ \alpha_2\ \ldots\ \alpha_k]) = k.$$

(vi) Για $k = 1$ τούτο είναι προφανές. Για $k \geqslant 2$ έχουμε

$$\begin{aligned} [\alpha_1\ \alpha_2\ \ldots\ \alpha_k]^{-1} &= [\alpha_1\ \alpha_2\ \ldots\ \alpha_k]^{k-1} = \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_k & a_{k+1} & \cdots & a_{2k-1} \end{bmatrix} \\ &= \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_k & a_1 & \cdots & a_{k-1} \end{bmatrix} = [\alpha_k\ \alpha_{k-1}\ \ldots\ \alpha_1] \end{aligned}$$

όπου η πρώτη ισότητα έπεται από το (v), και η δεύτερη και η τρίτη από το (iv), καθόσον το $2k - 1$ γράφεται ως $(k - 1) + k$.

(vii) Όταν έχουμε $k = 1$ η ισότητα (4.4) είναι προφανής. Για οιαδήποτε αντιμετάθεση (= 2-κύκλο) $[\alpha_1\ \alpha_2]$ (εντός τής $\mathfrak{S}_n$) και $\sigma \in \mathfrak{S}_n$ η εικόνα ενός $j \in \{1, ..., n\}$ μέσω τής συνθέσεως $\sigma \circ [\alpha_1\ \alpha_2] \circ \sigma^{-1}$ ισούται με

$$(\sigma \circ [\alpha_1\ \alpha_2] \circ \sigma^{-1})(j) = \begin{cases} j, & \text{όταν } \sigma^{-1}(j) \in \{1, ..., n\} \setminus \{\alpha_1, \alpha_2\}, \\ \sigma(\alpha_1), & \text{όταν } \sigma^{-1}(j) = \alpha_2\ (\Leftrightarrow j = \sigma(\alpha_2)), \\ \sigma(\alpha_2), & \text{όταν } \sigma^{-1}(j) = \alpha_1\ (\Leftrightarrow j = \sigma(\alpha_1)), \end{cases}$$

απ' όπου έπεται ότι $\sigma \circ [\alpha_1\ \alpha_2] \circ \sigma^{-1} = [\sigma(\alpha_1)\ \sigma(\alpha_2)]$, οπότε η ισότητα (4.4) είναι αληθής και *για κάθε* αντιμετάθεση (εντός τής $\mathfrak{S}_n$). Στην περίπτωση θεωρήσεως k-κύκλων $[\alpha_1\ \alpha_2\ \ldots\ \alpha_k]$, όπου $k \geqslant 3$, χρησιμοποιούμε το (iii): Για κάθε $\sigma \in \mathfrak{S}_n$ έχουμε

$$\sigma \circ [\alpha_1\ \alpha_2\ \ldots\ \alpha_k] \circ \sigma^{-1} = \sigma \circ [\alpha_1\ \alpha_2] \circ [\alpha_2\ \alpha_3] \circ \cdots \circ [\alpha_{k-1}\ \alpha_k] \circ \sigma^{-1}$$

$$= \left(\sigma \circ [\alpha_1\ \alpha_2] \circ \sigma^{-1}\right) \circ \left(\sigma \circ [\alpha_2\ \alpha_3] \circ \sigma^{-1}\right) \circ \cdots \circ \left(\sigma \circ [\alpha_{k-1}\ \alpha_k] \circ \sigma^{-1}\right)$$

$$= [\sigma(\alpha_1)\ \sigma(\alpha_2)] \circ [\sigma(\alpha_2)\ \sigma(\alpha_3)] \circ \cdots \circ [\sigma(\alpha_{k-1})\ \sigma(\alpha_k)] = [\sigma(\alpha_1)\ \sigma(\alpha_2)\ \ldots\ \sigma(\alpha_k)],$$

όπου η προτελευταία ισότητα έπεται από ό,τι είχαμε αποδείξει προηγουμένως για τις αντιμεταθέσεις. Ως εκ τούτου, η ισότητα (4.4) είναι αληθής για *οιουσδήποτε* k-κύκλους (εντός τής $\mathfrak{S}_n$). □

4.2.4 Λήμμα. *Εάν δυο κύκλοι $\sigma, \tau \in \mathfrak{S}_n$ είναι ξένοι μεταξύ τους, τότε μετατίθενται αμοιβαίως, δηλαδή $\sigma \circ \tau = \tau \circ \sigma$.*

Απόδειξη. Έπεται άμεσα από την πρόταση 4.1.7. □

4.2.5 Λήμμα. *Εάν μια μετάταξη $\sigma \in \mathfrak{S}_n$ γράφεται υπό τη μορφή*

$$\sigma = c_1 \circ c_2 \circ \cdots \circ c_\nu \quad (\nu \in \mathbb{N})$$

επαλλήλων συνθέσεων ανά δύο ξένων μεταξύ τους κύκλων $c_1, c_2, \ldots, c_\nu \in \mathfrak{S}_n$, και εάν υπάρχει $j \in \{1, ..., n\}$ με $j \in \operatorname{supp}(c_s)$ για κάποιον $s \in \{1, ..., \nu\}$, τότε

$$\sigma^\kappa(j) = c_s^\kappa(j), \quad \forall \kappa \in \mathbb{N}.$$

Απόδειξη. Επειδή οι $c_1, c_2, \ldots, c_\nu$ είναι ανά δύο ξένοι μεταξύ τους κύκλοι, το λήμμα 4.2.4 μας επιτρέπει να γράψουμε την σ ως εξής:

$$\sigma = \check{\sigma} \circ c_s, \quad \text{όπου} \quad \check{\sigma} := c_1 \circ \cdots \circ c_{s-1} \circ c_{s+1} \circ \cdots \circ c_\nu.$$

Προφανώς, οι $\check{\sigma}, c_s$ είναι μεταξύ τους ξένες μετατάξεις. Κατά συνέπειαν, $\check{\sigma}(j) = j$ (πρβλ. πρόταση 4.1.5) και

$$\check{\sigma} \circ c_s = c_s \circ \check{\sigma} \tag{4.5}$$

(και πάλι λόγω τού λήμματος 4.2.4). Κάνοντας χρήση τής κλασικής μαθηματικής επαγωγής ως προς τον κ και τής ισότητας (4.5) αποδεικνύουμε ότι

$$(\check{\sigma} \circ c_s)^\kappa = (c_s \circ \check{\sigma})^\kappa = c_s^\kappa \circ \check{\sigma}^\kappa, \ \forall \kappa \in \mathbb{N}.$$

Επομένως, $\sigma^\kappa(j) = (c_s \circ \check{\sigma})^\kappa(j) = c_s^\kappa(\check{\sigma}^\kappa(j)) = c_s^\kappa(\check{\sigma}^{k-1}(j)) = \cdots = c_s^\kappa(j)$ για κάθε $\kappa \in \mathbb{N}$. □

4.2.6 Λήμμα. *Εάν οι $\sigma, \tau \in \mathfrak{S}_n$ είναι κύκλοι και εάν υπάρχει $j \in \{1, ..., n\}$, ούτως ώστε $j \in \operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau)$, τότε ισχύει η ακόλουθη συνεπαγωγή:*

$$[\sigma^\kappa(j) = \tau^\kappa(j),\ \forall \kappa \in \mathbb{N}] \Longrightarrow \sigma = \tau.$$

Απόδειξη. Λόγω τού (i) τής προτάσεως 4.2.3 μπορούμε δίχως βλάβη τής γενικότητας να υποθέσουμε ότι

$$\sigma = [\alpha_1\ \alpha_2\ \ldots\ \alpha_\nu],\ \tau = [\beta_1\ \beta_2\ \ldots\ \beta_\xi], \quad \text{όπου} \quad \alpha_1 = \beta_1 = j.$$

Κατά το 4.2.3 (iv), $\alpha_{\kappa+1} = \sigma^\kappa(j)$ για κάθε κ, $1 \leqslant \kappa < \nu$, και $\beta_{\kappa+1} = \tau^\kappa(j)$ για κάθε κ, $1 \leqslant \kappa < \xi$. Δίχως βλάβη τής γενικότητας υποθέτουμε ότι $\nu \leqslant \xi$. Προφανώς,

$$[\sigma^\kappa(j) = \tau^\kappa(j),\ \forall \kappa \in \mathbb{N}] \Longrightarrow \alpha_2 = \beta_2, ...,\ \alpha_\nu = \beta_\nu$$

και (ταυτοχρόνως) $\beta_{\nu+1} = \tau^{\nu}(j) = \sigma^{\nu}(j) = j = \beta_1$ (διότι $\sigma^{\nu} = \mathrm{id}$, λόγω τού 4.2.3 (v)), οπότε έχουμε κατ' ανάγκην $\xi = \nu$ και $\sigma = \tau$. □

4.2.7 Θεώρημα. *Κάθε μη ταυτοτική μετάταξη ανήκουσα στην $\mathfrak{S}_n$, $n \geqslant 2$, είτε είναι αφ' εαυτής ένας κύκλος είτε μπορεί να γραφεί υπό τη μορφή επαλλήλων συνθέσεων (πεπερασμένου πλήθους) ανά δύο ξένων μεταξύ τους κύκλων μήκους $\geqslant 2$. Επιπροσθέτως, μια τέτοια έκφραση είναι μονοσημάντως ορισμένη (ενδεχομένως ύστερα από κάποια αναδιάταξη των μετεχόντων κύκλων).*

Απόδειξη. 1) Επαλήθευση πρώτου ισχυρισμού. Επειδή $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{id}\}$, έχουμε προφανώς $\varnothing \neq \mathrm{supp}(\sigma) \subseteq \{1, 2, ..., n\}$. Θέτουμε[3]

$$j_1 := \min(\mathrm{supp}(\sigma)) \ \text{ και } \ k_1 := \min\{\xi \in \mathbb{N} \,|\sigma^{\xi}(j_1) = j_1\},$$

και ορίζουμε τον k_1-κύκλο $\tau_1 := [j_1\ \sigma(j_1)\ \sigma^2(j_1)\ \ldots\ \sigma^{k_1-1}(j_1)]$, όπου $k_1 \geqslant 2$. Εάν $\mathrm{supp}(\sigma) = \mathrm{supp}(\tau_1)$, τότε $\sigma = \tau_1$. Ειδάλλως, $\mathrm{supp}(\tau_1) \subsetneqq \mathrm{supp}(\sigma)$, θέτουμε

$$j_2 := \min(\mathrm{supp}(\sigma) \setminus \mathrm{supp}(\tau_1)) \ \text{ και } \ k_2 := \min\{\xi \in \mathbb{N} \,|\sigma^{\xi}(j_2) = j_2\},$$

και ορίζουμε τον k_2-κύκλο $\tau_2 := [j_2\ \sigma(j_2)\ \sigma^2(j_2)\ \ldots\ \sigma^{k_2-1}(j_2)]$, όπου $k_2 \geqslant 2$. Εάν $\mathrm{supp}(\sigma) = \mathrm{supp}(\tau_1) \cup \mathrm{supp}(\tau_2)$, τότε η σ ισούται με τον κύκλο $\tau_1 \circ \tau_2$. Ειδάλλως, $\mathrm{supp}(\tau_1) \cup \mathrm{supp}(\tau_2) \subsetneqq \mathrm{supp}(\sigma)$, θέτουμε

$$j_3 := \min(\mathrm{supp}(\sigma) \setminus (\mathrm{supp}(\tau_1) \cup \mathrm{supp}(\tau_2))) \ \text{ και } \ k_3 := \min\{\xi \in \mathbb{N} \,|\sigma^{\xi}(j_3) = j_3\},$$

ορίζουμε τον k_3-κύκλο $\tau_3 := [j_3\ \sigma(j_3)\ \sigma^2(j_3)\ \ldots\ \sigma^{k_3-1}(j_3)]$, όπου $k_3 \geqslant 2$, και συνεχίζουμε την κατασκευή διαδοχικών κύκλων κατ' αυτόν τον τρόπο. Επειδή το σύνολο $\{1, 2, ..., n\}$ είναι πεπερασμένο, η εν λόγω διαδικασία περατούται ύστερα από $\lfloor \frac{n}{2} \rfloor$ βήματα· συγκεκριμένα, όταν

$$\mathrm{supp}(\sigma) = \bigcup_{s=1}^{\nu} \mathrm{supp}(\tau_s) \Longrightarrow \sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_{\nu}.$$

Απομένει να αποδειχθεί ότι οι ανωτέρω κύκλοι είναι ανά δύο ξένοι μεταξύ τους. Κατ' αρχάς παρατηρούμε ότι

$$\sigma^m(j_s) = \tau_s^m(j_s), \ \forall s \in \{1, ..., \nu\} \ \text{ και } \ \forall m \in \mathbb{Z}. \tag{4.6}$$

Πράγματι· εάν $s \in \{1, ..., \nu\}$, τότε κάθε $m \in \mathbb{Z}$ γράφεται υπό τη μορφή $m = q_s k_s + r_s$ για κάποιο μονοσημάντως ορισμένο ζεύγος $(q_s, r_s) \in \mathbb{Z} \times \mathbb{Z}$, όπου $0 \leqslant r_s \leqslant k_s - 1$. (Βλ. θεώρημα 2.1.6.) Επειδή $\mathrm{ord}(\tau_s) = k_s$, έχουμε $\tau_s^m = \tau_s^{r_s}$ και

$$\left.\begin{array}{c} \tau_s^{r_s}(j_s) = \sigma^{1+r_s-1}(j_s) = \sigma^{r_s}(j_s) \ \ (\text{από το 4.2.3 (iv)}) \\ \sigma^m(j_s) = \sigma^{q_s k_s + r_s}(j_s) \\ = \sigma^{r_s}(\underbrace{\sigma^{\mathrm{sign}(q_s)k_s} \circ \cdots \circ \sigma^{\mathrm{sign}(q_s)k_s}}_{|q_s| \ \text{φορές}}(j_s)) = \sigma^{r_s}(j_s) \\ \big(\text{καθότι} \ \ \sigma^{k_s}(j_s) = j_s\big) \end{array}\right\} \Rightarrow \sigma^m(j_s) = \tau_s^m(j_s).$$

Ας υποθέσουμε ότι υπάρχουν $s, s' \in \{1, ..., \nu\}$, $s < s'$, με $\mathrm{supp}(\tau_s) \cap \mathrm{supp}(\tau_{s'}) \neq \varnothing$. Έστω τυχόν στοιχείο $j \in \mathrm{supp}(\tau_s) \cap \mathrm{supp}(\tau_{s'})$. Προφανώς,

$$\exists\, (m, m') \in \mathbb{N}_0 \times \mathbb{N}_0 : j = \sigma^m(j_s) = \sigma^{m'}(j_{s'}).$$

[3] Για οιονδήποτε $j \in \mathrm{supp}(\sigma)$ το σύνολο $\{\sigma^{\xi}(j) \,|\xi \in \mathbb{N}\}$ είναι προδήλως πεπερασμένο. Κατά συνέπειαν, υπάρχουν $\xi, \xi' \in \mathbb{N}$, $\xi > \xi'$, ούτως ώστε να ισχύει $\sigma^{\xi}(j) = \sigma^{\xi'}(j)$, απ' όπου έπεται ότι $\sigma^{\xi-\xi'}(j) = j$. Αυτό σημαίνει ότι το $\{\xi \in \mathbb{N} \,|\sigma^{\xi}(j) = j\}$ είναι ένα μη κενό υποσύνολο τού $\mathbb{N}$ περιέχον (σύμφωνα με την αρχή τής καλής διατάξεως τού $\mathbb{N}$) ελάχιστο στοιχείο.

Η (4.6) δίδει $j_{s'} = \sigma^{-m'}(\sigma^m(j_s)) = \sigma^{m-m'}(j_s) = \tau_s^{m-m'}(j_s) \Rightarrow j_{s'} \in \mathrm{supp}(\tau_s)$. Από την άλλη μεριά, επειδή

$$j_{s'} := \min(\mathrm{supp}(\sigma) \setminus (\mathrm{supp}(\tau_1) \cup \cdots \cup \mathrm{supp}(\tau_s) \cup \cdots \cup \mathrm{supp}(\tau_{s'-1}))),$$

έχουμε $j_{s'} \notin \mathrm{supp}(\tau_s)$. Άρα οι $\tau_1, ..., \tau_\nu$ είναι όντως ανά δύο ξένοι μεταξύ τους.

2) Επαληθευση δευτερου ισχυρισμου. Έστω $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{id}\}$. Υποθέτουμε ότι η σ γράφεται υπό τη μορφή $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_\nu = \varrho_1 \circ \varrho_2 \circ \cdots \circ \varrho_{\nu'}$, $\nu, \nu' \in \mathbb{N}$, όπου οι $\tau_1, \tau_2, \ldots, \tau_\nu$ (και, αντιστοίχως, οι $\varrho_1, \varrho_2, \ldots, \varrho_{\nu'}$) είναι κύκλοι ανά δύο ξένοι μεταξύ τους μήκους $\geqslant 2$. Θα εφαρμόσουμε τη δεύτερη μορφή τής μαθηματικής επαγωγής ως προς τον $\ell := \max\{\nu, \nu'\}$. Όταν $\ell = 1$, τότε $\nu = \nu' = 1$ και ο ισχυρισμός είναι προφανώς αληθής. Υποθέτοντας ότι αυτός είναι αληθής για όλους τους φυσικούς αριθμούς που είναι μικρότεροι ενός $\ell \geqslant 2$, αρκεί να αποδείξουμε την ορθότητά του και για τον ίδιον τον ℓ. Επειδή $\sigma \neq \mathrm{id}$, $\exists j \in \{1, ..., n\} : \sigma(j) \neq j$ και $\exists s \in \{1, ..., \nu\}$, $s' \in \{1, ..., \nu'\} : j \in \mathrm{supp}(\tau_s) \cap \mathrm{supp}(\varrho_{s'})$. Κατά το λήμμα 4.2.5,

$$\sigma^\kappa(j) = \tau_s^\kappa(j) = \varrho_{s'}^\kappa(j), \quad \forall \kappa \in \mathbb{N},$$

οπότε το λήμμα 4.2.6 μας πληροφορεί ότι $\tau_s = \varrho_{s'}$. Εξάλλου, δυνάμει τού λήμματος 4.2.4 και τού νόμου τής διαγραφής 3.2.9 (i) συνάγεται ότι

$$\begin{aligned}
&\tau_1 \circ \cdots \circ \tau_{s-1} \circ \tau_s \circ \tau_{s+1} \circ \cdots \circ \tau_\nu = \varrho_1 \circ \cdots \circ \varrho_{s'-1} \circ \varrho_{s'} \circ \varrho_{s'+1} \circ \cdots \circ \varrho_{\nu'} \\
&\Rightarrow (\tau_1 \circ \cdots \circ \tau_{s-1} \circ \tau_{s+1} \circ \cdots \circ \tau_\nu) \circ \tau_s = (\varrho_1 \circ \cdots \circ \varrho_{s'-1} \circ \varrho_{s'+1} \circ \cdots \circ \varrho_{\nu'}) \circ \varrho_{s'} \\
&\Rightarrow \tau_1 \circ \cdots \circ \tau_{s-1} \circ \tau_{s+1} \circ \cdots \circ \tau_\nu = \varrho_1 \circ \cdots \circ \varrho_{s'-1} \circ \varrho_{s'+1} \circ \cdots \circ \varrho_{\nu'}
\end{aligned}$$

Στο αριστερό μέλος τής τελευταίας ισότητας εμφανίζονται $\nu - 1$ κύκλοι και στο δεξιό μέλος $\nu' - 1$ κύκλοι, οπότε $\max\{\nu - 1, \nu' - 1\} < \ell$. Κατά την επαγωγική μας υπόθεση, $\nu - 1 = \nu' - 1$ (οπότε $\nu = \nu'$) και υπάρχει κάποια αμφίρριψη (ήτοι κάποια αναδιάταξη δεικτών)

$$\psi : \{1, ..., s-1, s+1, ..., \nu\} \longrightarrow \{1, ..., s'-1, s'+1, ..., \nu\}$$

με $\tau_x = \varrho_{\psi(x)}$, για κάθε $x \in \{1, ..., s-1, s+1, ..., \nu\}$. Επειδή $\tau_s = \varrho_{s'}$, ορίζεται η αμφίρριψη $\vartheta : \{1, ..., \nu\} \longrightarrow \{1, ..., \nu\}$ μέσω τού τύπου

$$\vartheta(x) := \begin{cases} \psi(x), & \text{όταν } x \in \{1, ..., s-1, s+1, ..., \nu\}, \\ s', & \text{όταν } x = s. \end{cases}$$

Προφανώς, $\tau_x = \varrho_{\vartheta(x)}$, για κάθε $x \in \{1, ..., \nu\}$, και η απόδειξη λήγει εδώ. □

4.2.8 Παράδειγμα. Για τη μετάταξη

$$\sigma := \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 \end{bmatrix} \in \mathfrak{S}_9$$

λαμβάνουμε $\mathrm{supp}(\sigma) = \{1, 2, 3, 4, 6, 7, 8, 9\}$, $j_1 = 1$, $k_1 = 2$, $\tau_1 = [1\ 6]$ και

$$\begin{aligned}
&\mathrm{supp}(\sigma) \setminus \mathrm{supp}(\tau_1) = \{2, 3, 4, 7, 8, 9\}, \quad j_2 = 2, \quad k_2 = 2, \quad \tau_2 = [2\ 4], \\
&\mathrm{supp}(\sigma) \setminus \bigcup_{s=1}^{2} \mathrm{supp}(\tau_s) = \{3, 7, 8, 9\}, \quad j_3 = 3, \quad k_3 = 4, \quad \tau_3 = [3\ 7\ 8\ 9],
\end{aligned}$$

οπότε $\sigma = \tau_1 \circ \tau_2 \circ \tau_3$. (Το 5 δεν εμφανίζεται διότι μένει αμετάβλητο μέσω τής σ.)

4.2.9 Σημείωση. Ο λογισμός με τους κύκλους και τις μετατάξεις αναπτύχθηκε πλήρως από τον Γάλλο μαθηματικό Augustin-Louis Cauchy (1789-1857) περί το[4] 1815. Αυτός είχε κατ' ουσίαν αποδείξει *και* το θεώρημα 4.2.7, αν και πολλά συναφή λήμματα και αποτελέσματα (όπως είναι το πόρισμα 4.2.10) ήταν ήδη γνωστά (τουλάχιστον σε υπολογιστικό επίπεδο) ήδη από τα τέλη τού 18ου αιώνα.

[4] Βλ. Mémoire sur le nombre des valeurs qu'une fonction peut acqu'erir lorsqu'on y permute de toutes les manieères possibles les quantités qu'elle renferme, J. de l' École Polyt. **XVII**^{e} Cahier, Tome **X** (1815). 1-28.

4.2.10 Πόρισμα (P. Ruffini, 1799). *Εάν μια μετάταξη $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{id}\}$, $n \geqslant 2$, γραφεί υπό τη μορφή επαλλήλων συνθέσεων $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_\nu$ -ανά δύο ξένων μεταξύ τους- κύκλων $\tau_1, \ldots, \tau_\nu$ με μήκη $k_1, \ldots, k_\nu \geqslant 2$, αντιστοίχως, τότε*

$$\boxed{\mathrm{ord}\,(\sigma) = \text{εκπ}(k_1, \ldots, k_\nu).}$$

(Στην ειδική περίπτωση όπου $\nu = 1$, λαμβάνουμε $\mathrm{ord}(\sigma) = k_1$. Βλ. 4.2.3 (v).)

Απόδειξη. Από το (v) της προτάσεως 4.2.3 γνωρίζουμε ότι $k_i = \mathrm{ord}(\tau_i)$ για κάθε $i \in \{1, \ldots, \nu\}$. Θέτουμε[5] $k := \text{εκπ}(k_1, \ldots, k_\nu)$. Επειδή οι $\tau_1, \ldots, \tau_\nu$ είναι ανά δύο ξένοι μεταξύ τους, μετατίθενται αμοιβαίως ανά δύο (βλ. λήμμα 4.2.4). Επομένως,

$$\begin{aligned} \sigma^k &= (\tau_1 \circ \tau_2 \circ \cdots \circ \tau_\nu)^k = {\tau_1}^k \circ {\tau_2}^k \circ \cdots \circ {\tau_\nu}^k \\ &= ({\tau_1}^{k_1})^{\frac{k}{k_1}} \circ ({\tau_2}^{k_2})^{\frac{k}{k_2}} \circ \cdots \circ ({\tau_\nu}^{k_\nu})^{\frac{k}{k_\nu}} = \mathrm{id} \circ \mathrm{id} \circ \cdots \circ \mathrm{id} = \mathrm{id}, \end{aligned}$$

και, ως εκ τούτου,

$$k \geqslant \mathrm{ord}(\sigma). \tag{4.7}$$

Έστω τώρα *τυχών* $m \in \mathbb{N}$ με $\sigma^m = \mathrm{id}$. Επειδή οι $\tau_1, \ldots, \tau_\nu$ μετατίθενται αμοιβαίως ανά δύο, έχουμε

$$\mathrm{id} = \sigma^m = (\tau_1 \circ \tau_2 \circ \cdots \circ \tau_\nu)^m = {\tau_1}^m \circ {\tau_2}^m \circ \cdots \circ {\tau_\nu}^m.$$

Ας υποθέσουμε ότι $\exists i_0 \in \{1, \ldots, \nu\}$, τέτοιος ώστε να ισχύει ${\tau_{i_0}}^m \neq \mathrm{id}$. Τότε ${\tau_{i_0}}^m(x) \neq x$ για κάποιο $x \in \{1, \ldots, n\}$. Επειδή η ${\tau_{i_0}}^m$ «μετακινεί» (ήτοι μετατάσσει *κυριολεκτικώς*) το x, θα το μετακινεί και η τ_{i_0} (διότι αλλιώς, $\tau_{i_0}(x) = x \Rightarrow {\tau_{i_0}}^m(x) = x$). Κι επειδή οι $\tau_1, \ldots, \tau_\nu$ είναι ανά δύο ξένοι μεταξύ τους, θα έχουμε

$$\tau_j(x) = x,\ \forall j \in \{1, \ldots, \nu\} \setminus \{i_0\} \Longrightarrow {\tau_j}^m(x) = x,\ \forall j \in \{1, \ldots, \nu\} \setminus \{i_0\},$$

οπότε

$$({\tau_1}^m \circ {\tau_2}^m \circ \cdots \circ {\tau_\nu}^m)(x) \neq x \Longrightarrow {\tau_1}^m \circ {\tau_2}^m \circ \cdots \circ {\tau_\nu}^m \neq \mathrm{id}.$$

Άτοπο! Κατά συνέπειαν,

$${\tau_1}^m = {\tau_2}^m = \cdots = {\tau_\nu}^m = \mathrm{id}.$$

Δυνάμει της προτάσεως 3.4.8, $k_i \mid m$ για κάθε $i \in \{1, \ldots, \nu\}$, οπότε (λόγω της προτάσεως 2.2.25)

$$k \mid m \Longrightarrow k \leqslant m \Longrightarrow k \leqslant \mathrm{ord}(\sigma). \tag{4.8}$$

Από τις (4.7) και (4.8) έπεται ότι $k = \mathrm{ord}(\sigma)$. □

4.2.11 Πόρισμα. *Κάθε μετάταξη εντός της $\mathfrak{S}_n$, $n \geqslant 2$, μπορεί να γραφεί υπό τη μορφή επαλλήλων συνθέσεων (πεπερασμένου πλήθους) αντιμεταθέσεων.*

Απόδειξη. Εάν $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{id}\}$, τότε αυτό έπεται άμεσα από τον συνδυασμό τού θεωρήματος 4.2.7 με την ισότητα (4.2) (ή, εναλλακτικώς, την ισότητα (4.3)) τού (iii) της προτάσεως 4.2.3. Εξάλλου, για την id έχουμε

$$\mathrm{id} = [1\ 2\ \ldots\ n]^n = ([1\ 2] \circ [2\ 3] \circ \cdots \circ [n-1\ n])^n,$$

λόγω των (v) και (iii) της προτάσεως 4.2.3. □

[5] Εάν $\nu = 1$, τότε θέτουμε απλώς $k := k_1$.

4.2.12 Πόρισμα. *Όταν $n \in \mathbb{N}$, $n \geqslant 2$, τότε η συμμετρική ομάδα $\mathfrak{S}_n$ παράγεται από το σύνολο των αντιμεταθέσεών της.*

4.2.13 Πόρισμα. *Έστω $n \in \mathbb{N}$, $n \geqslant 2$. Τότε ισχύουν τα ακόλουθα:*

(i) $\mathfrak{S}_n = \langle \{[1\ i] \mid i \in \{2, ..., n\}\} \rangle$.

(ii) $\mathfrak{S}_n = \langle \{[j\ j+1] \mid j \in \{1, ..., n-1\}\} \rangle$.

(iii) $\mathfrak{S}_n = \langle [1\ 2], [1\ 2\ \ldots\ n] \rangle$, *όταν $n \geqslant 3$.*

Αποδειξη. (i) Λόγω τού πορίσματος 4.2.12 αρκεί να δειχθεί ότι κάθε αντιμετάθεση ανήκουσα στην $\mathfrak{S}_n$ μπορεί να γραφεί ως σύνθεση (πεπερασμένου πλήθους) αντιμεταθέσεων τής μορφής $[1\ i]$ (όπου $i \in \{2, ..., n\}$). Έστω τυχούσα αντιμετάθεση

$$[\alpha_1\ \alpha_2] \in \mathfrak{S}_n.$$

Εάν ένας εκ των α_1, α_2 ισούται με 1, τότε η $[\alpha_1\ \alpha_2]$ είναι αυτής τής μορφής (πρβλ. 4.2.3 (i)). Εάν $\alpha_1 \neq 1$ και $\alpha_2 \neq 1$, τότε αρκεί να παρατηρήσουμε ότι

$$[\alpha_1\ \alpha_2] = [1\ \alpha_1] \circ [1\ \alpha_2] \circ [1\ \alpha_1].$$

(ii) Λόγω τού (i) είναι αρκετό να δειχθεί ότι κάθε αντιμετάθεση τής μορφής $[1\ i]$ (όπου $i \in \{2, ..., n\}$) μπορεί να γραφεί ως σύνθεση (πεπερασμένου πλήθους) αντιμεταθέσεων τής μορφής $[j\ j+1]$ (όπου $j \in \{1, ..., n-1\}$). Προς τούτο αρκεί να παρατηρήσουμε ότι

$$\begin{aligned}
[1\ i] &= [1\ i-1] \circ [i-1\ i] \circ [1\ i-1] \\
&= [1\ i-2] \circ [i-2\ i-1] \circ [1\ i-2] \circ [i-1\ i] \circ [1\ i-2] \circ [i-2\ i-1] \circ [1\ i-2] \\
&= [1\ i-2] \circ [i-2\ i-1] \circ [i-1\ i] \circ [1\ i-2]^2 \circ [i-2\ i-1] \circ [1\ i-2] \\
&= [1\ i-2] \circ [i-2\ i-1] \circ [i-1\ i] \circ [i-2\ i-1] \circ [1\ i-2] \\
&= \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}$$

$$= [1\ 2] \circ [2\ 3] \circ [3\ 4] \circ \cdots \circ [i-2\ i-1] \circ [i-1\ i] \circ [i-2\ i-1] \circ \cdots \circ [3\ 4] \circ [2\ 3] \circ [1\ 2]\,.$$

(iii) Λόγω τού (ii) αρκεί να δειχθεί ότι κάθε αντιμετάθεση τής μορφής $[j\ j+1]$ (όπου $j \in \{1, ..., n-1\}$) ανήκει στην υποομάδα τής $\mathfrak{S}_n$ που παράγεται από τους κύκλους

$$\tau := [1\ 2] \ \text{ και } \ \sigma := [1\ 2\ \ldots\ n].$$

Εφαρμόζοντας την (4.4) για τη μετάταξη $\sigma^{j-1} \in \mathfrak{S}_n$ λαμβάνουμε

$$\sigma^{j-1} \circ \tau \circ (\sigma^{j-1})^{-1} = \sigma^{j-1} \circ [1\ 2] \circ (\sigma^{j-1})^{-1} = [\sigma^{j-1}(1)\ \ \sigma^{j-1}(2)] = [j\ \ j+1],$$

αποκτώντας κατ' αυτόν τον τρόπο την επιθυμητή έκφραση τής $[j\ j+1]$. □

4.3 ΑΡΤΙΕΣ ΚΑΙ ΠΕΡΙΤΤΕΣ ΜΕΤΑΤΑΞΕΙΣ

Έστω τυχούσα μετάταξη $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{id}\}$ (όπου $n \geqslant 2$). Αυτή, σύμφωνα με το θεώρημα 4.2.7, μπορεί να γραφεί *μονοσημάντως* υπό τη μορφή επαλλήλων συνθέσεων (πεπερασμένου πλήθους) ανά δύο ξένων μεταξύ τους κύκλων μήκους $\geqslant 2$ (ενδεχομένως ύστερα από κάποια αναδιάταξη των μετεχόντων κύκλων). Όμως η έκφρασή της υπό τη μορφή επαλλήλων συνθέσεων (πεπερασμένου πλήθους) αντιμεταθέσεων (βλ. πόρισμα 4.2.11) *δεν είναι* κατ' ανάγκην μονοσημάντως ορισμένη· επί παραδείγματι, για $n = 6$,

$$\begin{bmatrix} 1\,2\,3\,4\,5\,6 \\ 5\,4\,3\,6\,1\,2 \end{bmatrix} = [1\,5] \circ [2\,4\,6] = [1\,5] \circ [2\,6] \circ [2\,4]\,.$$

Επειδή $[2\,4\,6] = [6\,2\,4]$, μπορούμε ισοδυνάμως να γράψουμε αυτό το στοιχείο τής $\mathfrak{S}_6$ και ως

$$\begin{bmatrix} 1\,2\,3\,4\,5\,6 \\ 5\,4\,3\,6\,1\,2 \end{bmatrix} = [1\,5] \circ [6\,2\,4] = [1\,5] \circ [6\,4] \circ [6\,2] = [1\,5] \circ [4\,6] \circ [2\,6]\,.$$

Για την άντληση ακόμη πιο απλών παραδειγμάτων αυτού τού είδους, αρκεί κανείς να θεωρήσει *οιονδήποτε* κύκλο $[\alpha_1\ \alpha_2\ \ldots\ \alpha_k]$ μήκους $k \geqslant 3$ εντός τής $\mathfrak{S}_n$ $(k \leqslant n)$ και να εφαρμόσει την (4.2):

$$[\alpha_1\ \alpha_2\ \ldots\ \alpha_k] = [\alpha_1\ \alpha_2] \circ [\alpha_2\ \alpha_3] \circ [\alpha_3\ \alpha_4] \circ \cdots \circ [\alpha_{k-1}\ \alpha_k]. \tag{4.9}$$

Επειδή $[\alpha_1\ \alpha_2] \circ [\alpha_2\ \alpha_3] = [\alpha_1\ \alpha_2\ \alpha_3] = [\alpha_1\ \alpha_3] \circ [\alpha_1\ \alpha_2]$ (με την πρώτη ισότητα ισχύουσα λόγω τής (4.2) και τη δεύτερη λόγω τής (4.3) για $k = 3$) έχουμε

$$[\alpha_1\ \alpha_2\ \ldots\ \alpha_k] = ([\alpha_1\ \alpha_3] \circ [\alpha_1\ \alpha_2]) \circ [\alpha_3\ \alpha_4] \circ \cdots \circ [\alpha_{k-1}\ \alpha_k], \tag{4.10}$$

με τις (4.9) και (4.10) περιέχουσες διαφορετικές αντιμεταθέσεις! Ωστόσο, αξίζει να επισημανθεί ότι σε *οιεσδήποτε* θεωρούμενες εκφράσεις μιας $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{id}\}$, $n \geqslant 2$, υπό τη μορφή επαλλήλων συνθέσεων αντιμεταθέσεων περισώζεται μια λίαν σημαντική ιδιότητα: *το πλήθος των εμφανιζομένων αντιμεταθέσεων είναι ή πάντοτε ένας άρτιος ή πάντοτε ένας περιττός φυσικός αριθμός* (βλ. 4.3.5 (iv)).

4.3.1 Ορισμός. (i) Έστω $n \in \mathbb{N}$ και έστω $\sigma \in \mathfrak{S}_n$. Ορίζουμε ως **παραβατικό ζεύγος**[6] (για την σ) κάθε διατεταγμένο ζεύγος $(i, j) \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ για το οποίο ισχύει η συνεπαγωγή: $i < j \Longrightarrow \sigma(i) > \sigma(j)$.

(ii) Ως **απεικόνιση προσημάνσεως** (των στοιχείων τής $\mathfrak{S}_n$) ορίζουμε την απεικόνιση

$$\mathrm{sgn} : (\mathfrak{S}_n, \circ) \longrightarrow (\{1, -1\}, \cdot) \tag{4.11}$$

μέσω τού τύπου[7]:

$$\mathrm{sgn}(\sigma) := \begin{cases} 1, & \text{όταν η } \sigma \text{ διαθέτει έναν άρτιο αριθμό παραβατικών ζευγών,} \\ -1, & \text{όταν η } \sigma \text{ διαθέτει έναν περιττό αριθμό παραβατικών ζευγών,} \end{cases}$$

για κάθε[8] $\sigma \in \mathfrak{S}_n$.

(iii) Μια μετάταξη $\sigma \in \mathfrak{S}_n$ ονομάζεται **άρτια** (και αντιστοίχως, **περιττή**) όταν $\mathrm{sgn}(\sigma) = 1$ (και αντιστοίχως, όταν $\mathrm{sgn}(\sigma) = -1$).

[6] Σε αυτά τα στοιχεία η σ υποπίπτει στην «παράβαση» τής αντιστροφής των κατευθύνσεων των ανισοτήτων (στις εικόνες τους). Γι' αυτό και πολλές φορές στη βιβλιογραφία συναντούμε αντί τού *παραβατικού ζεύγους* τον όρο *αντιστροφή* (ο οποίος όμως εντάσσεται στην κατηγορία των overused terms).

[7] Η τιμή $\mathrm{sgn}(\sigma)$ ονομάζεται **προσημασμένος άσος** (ή -πιο σύντομα, αλλά όχι ακριβολογημένα- **πρόσημο**) τής σ.

[8] Σημειωτέον ότι $\mathrm{sgn}(\mathrm{id}) = 1$ (διότι το πλήθος των παραβατικών ζευγών τής id ισούται με το 0).

4.3.2 Παράδειγμα. Τα παραβατικά ζεύγη τής μετατάξεως

$$\begin{bmatrix} 1\,2\,3\,4 \\ 2\,1\,4\,3 \end{bmatrix}$$

είναι τα $(1,2)$ και $(3,4)$.

4.3.3 Λήμμα. *Κάθε αντιμετάθεση $\tau \in \mathfrak{S}_n$, $n \geqslant 2$, είναι περιττή μετάταξη, δηλαδή*

$$\boxed{\operatorname{sgn}(\tau) = -1.}$$

Απόδειξη. Έστω $\tau = [i\ j]$, όπου $1 \leqslant i < j \leqslant n$. Αρκεί να καταμετρήσουμε το πλήθος των παραβατικών ζευγών της. Γράφοντάς την «σε πλήρη έκταση», λαμβάνουμε

$$\begin{bmatrix} 1 & \dots & i-1 & \boxed{i} & i+1 & \dots & j-1 & \boxed{j} & j+1 & \dots & n \\ 1 & \dots & i-1 & \boxed{j} & i+1 & \dots & j-1 & \boxed{i} & j+1 & \dots & n \end{bmatrix}.$$

Προφανώς, τα παραβατικά ζεύγη -πέραν τού ιδίου τού (i,j)- ανήκουν στην ένωση δύο συνόλων:

$$\{(i,k) \mid i+1 \leqslant k \leqslant j-1\} \cup \{(l,j) \mid i+1 \leqslant l \leqslant j-1\}.$$

Επειδή καθένα εξ αυτών έχει πληθικό αριθμό ίσον με $j-i-1$, η τ διαθέτει εν συνόλω $2(j-i-1)+1 = 2(j-i)-1$ παραβατικά ζεύγη. Άρα $\operatorname{sgn}(\tau) = -1$. □

4.3.4 Λήμμα. *Η τιμή που λαμβάνει οιαδήποτε μετάταξη $\sigma \in \mathfrak{S}_n$, $n \geqslant 1$, μέσω τής απεικονίσεως προσημάνσεως μπορεί να εκφρασθεί με τη βοήθεια τού ακολούθου «κλειστού» τύπου*:

$$\boxed{\operatorname{sgn}(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j-i}.}$$

Απόδειξη. Κατ' αρχάς πρέπει να τονισθεί ότι το γινόμενο τού δεξιού μέλους μπορεί να ιδωθεί ως ένα μακρύ κλάσμα στο οποίο τόσον ο αριθμητής όσον και ο παρονομαστής περιέχουν τις *ίδιες* διαφορές· εντούτοις, στον αριθμητή αυτές βρίσκονται (εν γένει) *σε άλλες θέσεις* και μάλιστα -στην περίπτωση εμφανίσεως παραβατικών ζευγών- *με αρνητικό πρόσημο*. Έστω s ο αριθμός των παραβατικών ζευγών (για την σ). Τότε

$$\begin{aligned} &\prod_{1 \leqslant i < j \leqslant n} (\sigma(j) - \sigma(i)) \\ &\qquad = \left(\prod_{\substack{1 \leqslant i < j \leqslant n \\ \sigma(i) < \sigma(j)}} \sigma(j) - \sigma(i) \right) \cdot (-1)^s \prod_{\substack{1 \leqslant i < j \leqslant n \\ \sigma(i) > \sigma(j)}} |\sigma(j) - \sigma(i)| \\ &\qquad = (-1)^s \prod_{1 \leqslant i < j \leqslant n} |\sigma(j) - \sigma(i)| = (-1)^s \prod_{1 \leqslant i < j \leqslant n} (j-i). \end{aligned}$$

Σημειωτέον ότι στην τελευταία ισότητα χρησιμοποιήσαμε το γεγονός τού ότι αμφότερα τα γινόμενα περιέχουν *τους ίδιους παράγοντες* (έστω κι αν αυτοί τύχει να είναι παρατεταγμένοι κατά διαφορετικό τρόπο). Τούτο έπεται από την αμφιρριπτικότητα τής σ. □

4.3.5 Θεώρημα. (i) *Για τυχούσες* $\sigma, \tau \in \mathfrak{S}_n$ (*όπου* $n \geqslant 1$) *έχουμε*

$$\boxed{\operatorname{sgn}(\tau \circ \sigma) = \operatorname{sgn}(\tau) \cdot \operatorname{sgn}(\sigma).}$$

οπότε η απεικόνιση προσημάνσεως (4.11) *είναι ένας ομομορφισμός ομάδων.*
(ii) *Για κάθε* $\sigma \in \mathfrak{S}_n$ (*όπου* $n \geqslant 1$) *έχουμε*

$$\boxed{\operatorname{sgn}(\sigma) = \operatorname{sgn}\left(\sigma^{-1}\right).}$$

(iii) *Εάν μια μετάταξη*

$$\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k \in \mathfrak{S}_n, \quad n \geqslant 2,$$

συντίθεται από k *αντιμεταθέσεις* $\tau_1, \tau_2, \ldots, \tau_k$, *τότε*

$$\boxed{\operatorname{sgn}(\sigma) = (-1)^k.}$$

Ιδιαιτέρως, τούτο ισχύει για κάθε $(k+1)$*-κύκλο* $\sigma \in \mathfrak{S}_n$ $(0 \leqslant k \leqslant n-1)$.
(iv) *Εάν μια μετάταξη* $\sigma \in \mathfrak{S}_n$, $n \geqslant 2$, *γράφεται υπό τη μορφή επαλλήλων συνθέσεων*

$$\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k = \tau'_1 \circ \tau'_2 \circ \cdots \circ \tau'_l$$

k *αντιμεταθέσεων* $\tau_1, \ldots, \tau_k$ *και -ταυτοχρόνως-* l *αντιμεταθέσεων* $\tau'_1, \ldots, \tau'_l$, *όπου* $k, l \in \mathbb{N}$, *τότε τόσον ο* k *όσον και ο* l *είναι ή πάντοτε ένας άρτιος ή πάντοτε ένας περιττός φυσικός αριθμός.*

Απόδειξη. (i) Σύμφωνα με το λήμμα 4.3.4 έχουμε

$$\begin{aligned}
\operatorname{sgn}(\tau \circ \sigma) &= \prod_{1 \leqslant i < j \leqslant n} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{j - i} \\
&= \prod_{1 \leqslant i < j \leqslant n} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)} \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}.
\end{aligned}$$

Επειδή λοιπόν το δεύτερο γινόμενο ισούται με $\operatorname{sgn}(\sigma)$, αρκεί να δείξουμε ότι το πρώτο ισούται με το $\operatorname{sgn}(\tau)$. Όμως το γινόμενο

$$\prod_{1 \leqslant i < j \leqslant n} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)}$$

γράφεται ως ακολούθως:

$$\begin{aligned}
&\prod_{\substack{1 \leqslant i < j \leqslant n \\ \sigma(i) < \sigma(j)}} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)} \prod_{\substack{1 \leqslant i < j \leqslant n \\ \sigma(i) > \sigma(j)}} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)} \\
= &\prod_{\substack{1 \leqslant i < j \leqslant n \\ \sigma(i) < \sigma(j)}} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)} \prod_{\substack{1 \leqslant j < i \leqslant n \\ \sigma(i) < \sigma(j)}} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)} \\
= &\prod_{\sigma(i) < \sigma(j)} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)}.
\end{aligned}$$

Επειδή η σ είναι αμφιρριπτική, θα υπάρχουν *μοναδικοί* $l, m \in \{1, \ldots, n\}$ για *κάθε* i, j, τέτοιοι ώστε $\sigma(j) = l$, $\sigma(i) = m$ (και *τανάπαλιν*). Επομένως, το τελευταίο αυτό

γινόμενο περιέχει (ενδεχομένως παρατεταγμένους κατά έναν διαφορετικό τρόπο, πράγμα ουσιαστικώς αδιάφορο) *τους ίδιους παράγοντες* με το γινόμενο

$$\prod_{\lambda<\mu} \frac{\tau(\lambda)-\tau(\mu)}{\lambda-\mu} = \operatorname{sgn}(\tau)\,.$$

(ii) Άμεσο επί τη βάσει τού (i), καθόσον ισχύει: $\sigma\circ\sigma^{-1}=\mathrm{id}$ και $\operatorname{sgn}(\mathrm{id})=1$.

(iii) Τούτο έπεται από το (i), το λήμμα 4.3.3 και το (iii) τής προτάσεως 4.2.3. Ένας k-κύκλος εντός τής $\mathfrak{S}_n$ $(1\leqslant k\leqslant n)$ είναι άρτια (και αντιστοίχως, περιττή) μετάταξη εάν και μόνον εάν ο k είναι περιττός (και αντιστοίχως, άρτιος) φυσικός αριθμός.

(iv) Προφανώς,

$$\begin{aligned}
&\tau_1\circ\tau_2\circ\cdots\circ\tau_k=\tau_1'\circ\tau_2'\circ\cdots\circ\tau_l'\\
&\Longrightarrow (\tau_1\circ\tau_2\circ\cdots\circ\tau_k)\circ(\tau_1'\circ\tau_2'\circ\cdots\circ\tau_l')^{-1}=\mathrm{id}\\
&\underset{\text{(ii)}}{\overset{\text{(i)}}{\Longrightarrow}} \operatorname{sgn}(\tau_1\circ\tau_2\circ\cdots\circ\tau_k)\cdot\operatorname{sgn}(\tau_1'\circ\tau_2'\circ\cdots\circ\tau_l')=1\\
&\underset{\text{(iii)}}{\Longrightarrow} (-1)^k\cdot(-1)^l=1\Longrightarrow(-1)^{k+l}=1,
\end{aligned}$$

οπότε το άθροισμα $k+l$ οφείλει να είναι ένας άρτιος φυσικός αριθμός. □

4.3.6 Πόρισμα. *Για οιεσδήποτε μετατάξεις $\sigma,\tau\in\mathfrak{S}_n$ (όπου $n\geqslant 2$) ισχύουν τα ακόλουθα:*

(i) *Εάν η σ είναι άρτια, τότε και η σ^{-1} είναι άρτια.*

(ii) *Εάν η σ είναι περιττή, τότε και η σ^{-1} είναι περιττή.*

(iii) *Εάν αμφότερες οι σ,τ είναι άρτιες, τότε και η $\tau\circ\sigma$ είναι άρτια.*

(iv) *Εάν αμφότερες οι σ,τ είναι περιττές, τότε η $\tau\circ\sigma$ είναι άρτια.*

(v) *Η σ^2 είναι πάντοτε άρτια.*

(vi) *Εάν η μία εκ των σ,τ είναι άρτια και η άλλη περιττή, τότε η $\tau\circ\sigma$ είναι περιττή.*

(vii) *Εάν η $\tau\circ\sigma$ είναι άρτια, τότε και η $\sigma\circ\tau$ είναι άρτια.*

(viii) *Εάν η $\tau\circ\sigma$ είναι περιττή, τότε και η $\sigma\circ\tau$ είναι περιττή.*

Απόδειξη. Τα (i) και (ii) έπονται άμεσα από το 4.3.5 (ii), και τα (iii), (iv), (v), (vi) από το 4.3.5 (i).

(vii) Εάν η $\tau\circ\sigma$ είναι άρτια, τότε (βάσει των (iii), (iv) και (vi)) υπάρχουν δύο ενδεχόμενα: *Είτε αμφότερες* οι σ,τ είναι άρτιες *είτε αμφότερες* οι σ,τ είναι περιττές. Άρα η $\sigma\circ\tau$ οφείλει να είναι άρτια λόγω των (iii) και (iv) (κατόπιν εναλλαγής των ρόλων των σ και τ).

(viii) Εάν η $\tau\circ\sigma$ είναι περιττή, τότε (βάσει των (iii), (iv) και (vi)) η μία εκ των σ,τ είναι άρτια και η άλλη περιττή, οπότε και η $\sigma\circ\tau$ οφείλει να είναι περιττή λόγω τού (vi) (κατόπιν εναλλαγής των ρόλων των σ και τ). □

4.3.7 Πόρισμα. *Έστω $n\in\mathbb{N}$, $n\geqslant 2$, και έστω $\sigma\in\mathfrak{S}_n\setminus\{\mathrm{id}\}$. Γράφοντας την σ (κατ' ουσίαν μονοσημάντως) υπό τη μορφή*

$$\sigma=\tau_1\circ\tau_2\circ\cdots\circ\tau_\nu,$$

όπου $\nu\in\mathbb{N}$ και τ_j κύκλος μήκους $k_j\geqslant 2$ για κάθε $j\in\{1,\ldots,\nu\}$ (όπως στο θεώρημα 4.2.7), συμπεραίνουμε ότι η σ είναι άρτια εάν και μόνον εάν ο αριθμός εκείνων των

κύκλων που έχουν άρτιο μήκος είναι άρτιος.

ΑΠΟΔΕΙΞΗ. Θέτοντας $\xi := \mathrm{card}(\mathcal{A})$, όπου

$$\mathcal{A} := \{\, j \in \{1, ..., \nu\} \,|\, k_j \equiv 0 (\mathrm{mod}\, 2)\} \,,$$

τα (i) και (iii) τού θεωρήματος 4.3.5 δίδουν

$$\begin{aligned} \mathrm{sgn}\,(\sigma) &= \mathrm{sgn}\,(\tau_1 \circ \tau_2 \circ \cdots \circ \tau_\nu) = \prod_{j=1}^{\nu} \mathrm{sgn}\,(\tau_j) \\ &= \prod_{j=1}^{\nu} (-1)^{k_j - 1} = \prod_{j \in \mathcal{A}} (-1)^{k_j - 1} = (-1)^{\xi} \,, \end{aligned}$$

οπότε η σ είναι άρτια εάν και μόνον εάν $\xi \equiv 0 (\mathrm{mod}\, 2)$. □

4.3.8 Ορισμός. Έστω n ένας φυσικός αριθμός $\geqslant 2$. Ο πυρήνας

$$\boxed{\mathfrak{A}_n := \mathrm{Ker}\,(\mathrm{sgn}) = \{\, \sigma \in \mathfrak{S}_n \mid \mathrm{sgn}\,(\sigma) = 1\}}$$

τού ομομορφισμού (4.11) είναι μια υποομάδα τής συμμετρικής ομάδας $\mathfrak{S}_n$ (κατά το (ii) τού λήμματος 3.5.4), απαρτίζεται από όλες τις άρτιες μετατάξεις τής $\mathfrak{S}_n$ και καλείται **εναλλάσσουσα ομάδα** (σε n σύμβολα). Σημειωτέον ότι το σύνολο $\{\, \sigma \in \mathfrak{S}_n \mid \mathrm{sgn}\,(\sigma) = -1\}$ *δεν* είναι υποομάδα τής $\mathfrak{S}_n$, διότι δεν περιέχει το ουδέτερο στοιχείο id τής $\mathfrak{S}_n$.

4.3.9 Πρόταση. *Η τάξη τής $\mathfrak{A}_n$, $n \geqslant 2$, ισούται με*

$$\boxed{|\mathfrak{A}_n| = \frac{n!}{2}.}$$

ΑΠΟΔΕΙΞΗ. Έστω μια μετάταξη $\tau \in \mathfrak{S}_n$ και έστω $\mathfrak{A}_n \circ \tau := \{\, \sigma \circ \tau \mid \sigma \in \mathfrak{A}_n\}$. Εάν $\mathrm{sgn}(\tau) = 1$, τότε $\mathfrak{A}_n \circ \tau = \mathfrak{A}_n$. Ας παγιώσουμε τώρα μια $\tau \in \mathfrak{S}_n$ για την οποία ισχύει $\mathrm{sgn}(\tau) = -1$. Για κάθε $\sigma \in \mathfrak{S}_n$ με $\mathrm{sgn}(\sigma) = -1$ έχουμε $\mathrm{sgn}\big(\sigma \circ \tau^{-1}\big) = 1$ (βάσει τού (i) τού θεωρήματος 4.3.5), οπότε $\sigma \in \mathfrak{A}_n \circ \tau$, διότι $\sigma = \big(\sigma \circ \tau^{-1}\big) \circ \tau$. Τούτο σημαίνει ότι $\{\, \sigma \in \mathfrak{S}_n \mid \mathrm{sgn}\,(\sigma) = -1\} \subseteq \mathfrak{A}_n \circ \tau$, οπότε τελικώς

$$\{\, \sigma \in \mathfrak{S}_n \mid \mathrm{sgn}\,(\sigma) = -1\} = \mathfrak{A}_n \circ \tau$$

(διότι ο αντίστροφος εγκλεισμός είναι προφανής) και $(\mathfrak{A}_n \circ \tau) \cap \mathfrak{A}_n = \varnothing$. Επειδή η απεικόνιση $\mathfrak{A}_n \longrightarrow \mathfrak{A}_n \circ \tau$, $\sigma \longmapsto \sigma \circ \tau$, είναι αμφιρριπτική, λαμβάνουμε (βάσει τής προτάσεως 4.1.3)

$$\mathfrak{S}_n = \mathfrak{A}_n \coprod (\mathfrak{A}_n \circ \tau) \Rightarrow n! = |\mathfrak{S}_n| = |\mathfrak{A}_n| + \mathrm{card}(\mathfrak{A}_n \circ \tau) = 2\,|\mathfrak{A}_n| \,,$$

οπότε $|\mathfrak{A}_n| = \frac{n!}{2}$. □

4.3.10 Παρατήρηση. Από το (i) τού θεωρήματος 4.3.5 και την απόδειξη τής προτάσεως 4.3.9 έπεται άμεσα ότι για $n \geqslant 2$ η απεικόνιση προσημάνσεως (4.11) είναι *επιμορφισμός* ομάδων.

4.3.11 Παραδείγματα. Προφανώς,

$$\mathfrak{A}_2 = \{\mathrm{id}\}, \quad \mathfrak{A}_3 = \{\mathrm{id}, [1\ 2\ 3], [1\ 3\ 2]\} = \langle [1\ 2\ 3] \rangle \,.$$

Για την εύρεση των στοιχείων τής $\mathfrak{A}_4$ επιχειρηματολογούμε ως εξής: Κατά το θεώρημα 4.2.7 κάθε μη ταυτοτική μετάταξη ανήκουσα στην $\mathfrak{S}_4$ μπορεί να γραφεί υπό

τη μορφή επαλλήλων συνθέσεων (πεπερασμένου πλήθους) ανά δύο ξένων μεταξύ τους κύκλων μήκους $\geqslant 2$. Επιπροσθέτως, μια τέτοια έκφραση είναι *μονοσημάντως ορισμένη* (ενδεχομένως ύστερα από κάποια αναδιάταξη των μετεχόντων κύκλων). Η εναλλάσσουσα ομάδα $\mathfrak{A}_4$ έχει τάξη $\frac{4!}{2} = 12$ (βλ. πρόταση 4.3.9) και αποτελείται από όλες τις άρτιες μετατάξεις τής $\mathfrak{S}_4$. Εάν γράψουμε μια $\sigma \in \mathfrak{A}_4 \setminus \{\mathrm{id}\}$ ως σύνθεση $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_\nu$ τέτοιων κύκλων, τότε (επειδή διαθέτουμε μόνον 4 σύμβολα)

$$2\nu \leqslant \sum_{\kappa=1}^{\nu} (\text{μήκος τού } \tau_\kappa) \leqslant 4 \Longrightarrow \nu \leqslant 2.$$

Λαμβάνοντας υπ' όψιν ότι οι 2-κύκλοι (= αντιμεταθέσεις) είναι περιττές μετατάξεις (βλ. λήμμα 4.3.3), συμπεραίνουμε (από το (iii) τού θεωρήματος 4.3.5) ότι η σ θα είναι είτε ένας 3-κύκλος είτε η σύνθεση δύο ξένων μεταξύ τους 2-κύκλων (= αντιμεταθέσεων). Στη δεύτερη περίπτωση, η σ θα είναι τής μορφής $[i\ j] \circ [k\ l]$, όπου $1 \leqslant i < j \leqslant 4$, $1 \leqslant k < l \leqslant 4$ και $\{i, j\} \cap \{k, l\} = \varnothing$. Επειδή, εν προκειμένω, ισχύει $[i\ j] \circ [k\ l] = [k\ l] \circ [i\ j]$ (βλ. λήμμα 4.2.4), συνάγεται ότι

$$\sigma \in \{[1\ 2] \circ [3\ 4], [1\ 3] \circ [2\ 4], [1\ 4] \circ [2\ 3]\}.$$

Στην περίπτωση όπου η σ είναι ένας 3-κύκλος $[i\ j\ k]$, έχουμε $[i\ j\ k] = [i\ j] \circ [j\ k]$. Οι 3-κύκλοι τής μορφής $[i\ j\ k]$, $1 \leqslant i < j < k \leqslant 4$ εντός τής $\mathfrak{A}_4$ είναι οι εξής:

$$[1\ 2\ 3],\ [1\ 2\ 4],\ [1\ 3\ 4],\ [2\ 3\ 4].$$

Τα αντίστροφά τους (που δεν έχουν τάξη 2, αλλά 3, οπότε δεν ταυτίζονται με τους ιδίους) οφείλουν να ανήκουν στην $\mathfrak{A}_4$. Επειδή $3 + 4 + 4 = 11 = \mathrm{card}(\mathfrak{A}_4 \setminus \{\mathrm{Id}\})$, έχουμε τελικώς (λόγω των (vi) και (i) τής προτάσεως 4.2.3)

$$\mathfrak{A}_4 = \left\{ \begin{array}{cccc} \mathrm{id}, & [1\ 2] \circ [3\ 4], & [1\ 3] \circ [2\ 4], & [1\ 4] \circ [2\ 3], \\ [1\ 2\ 3], & [1\ 2\ 4], & [1\ 3\ 4], & [2\ 3\ 4], \\ [1\ 3\ 2], & [1\ 4\ 2], & [1\ 4\ 3], & [2\ 4\ 3] \end{array} \right\}.$$

4.3.12 Σημείωση. Η εναλλάσσουσα ομάδα $\mathfrak{A}_n$ *δεν είναι αβελιανή για* $n \geqslant 4$. Πράγματι· ορίζοντας τις $\sigma, \tau \in \mathfrak{A}_n$ ως ακολούθως:

$$\begin{array}{llll} \sigma(1) = 2, & \sigma(2) = 3, & \sigma(3) = 1, & \sigma(j) = j, \quad \forall j \in \{4, ..., n\}, \\ \tau(1) = 2, & \tau(2) = 4, & \tau(4) = 1, & \tau(j) = j, \quad \forall j \in \{3, 5, 6, ..., n\}, \end{array}$$

$(\sigma = [1\ 2\ 3], \tau = [1\ 2\ 4])$ λαμβάνουμε $(\tau \circ \sigma)(1) = 4 \neq 3 = (\sigma \circ \tau)(1)$. Επομένως, $\tau \circ \sigma \neq \sigma \circ \tau$.

4.3.13 Πρόταση. *Έστω* $n \in \mathbb{N}$, $n \geqslant 3$. *Τότε ισχύουν τα ακόλουθα:*

(i) $\mathfrak{A}_n = \langle \{[i\ j] \circ [k\ l] \mid 1 \leqslant i < j \leqslant n,\ 1 \leqslant k < l \leqslant n\} \rangle$.

(ii) *Η* $\mathfrak{A}_n$ *παράγεται από το σύνολο των 3-κύκλων.*

(iii) $\mathfrak{A}_n = \langle \{[\alpha\ \beta\ i] \mid i \in \{1, \ldots, n\} \setminus \{\alpha, \beta\}\} \rangle$, *όπου τα* α, β *είναι δύο παγιωμένα στοιχεία τού* $\{1, \ldots, n\}$ *και* $\alpha \neq \beta$.

(iv) $\mathfrak{A}_n = \langle \{[1\ 2\ i] \mid 3 \leqslant i \leqslant n\} \rangle$.

Απόδειξη. (i) Επειδή η $\mathfrak{A}_n$ απαρτίζεται από όλες τις άρτιες μετατάξεις τής $\mathfrak{S}_n$, κάθε μη ταυτοτικό στοιχείο τής $\mathfrak{A}_n$ μπορεί να γραφεί ως υπό τη μορφή επαλλήλων συνθέσεων *αρτίου πλήθους* αντιμεταθέσεων (βλ. 4.2.11 και 4.3.5 (iv)). Άρα το $\{[i\ j] \circ [k\ l] \mid 1 \leqslant i < j \leqslant n,\ 1 \leqslant k < l \leqslant n\}$ είναι όντως ένα σύνολο γεννητόρων τής $\mathfrak{A}_n$.

(ii) Λόγω τού (i) αρκεί να δειχθεί ότι η σύνθεση δυο αντιμεταθέσεων μπορεί να γραφεί ως σύνθεση (πεπερασμένου πλήθους) κύκλων μήκους 3. Θεωρούμε λοιπόν τυχούσα σύνθεση αντιμεταθέσεων τής μορφής

$$[i\ j] \circ [k\ l] \in \mathfrak{A}_n,\ \ 1 \leqslant i < j \leqslant n,\ 1 \leqslant k < l \leqslant n,$$

και εξετάζουμε τέσσερεις περιπτώσεις χωριστά.
Περίπτωση πρώτη. Εάν $i = k$ και $j = l$, τότε, σύμφωνα με το 4.2.3 (v), έχουμε

$$[i\ j] \circ [k\ l] = [i\ j]^2 = \mathrm{id} = [1\ 2\ 3]^3.$$

Περίπτωση δεύτερη. Εάν $i = k$ και $j \neq l$, τότε, σύμφωνα με τα (i) και (ii) τής προτάσεως 4.2.3, έχουμε $[i\ j] \circ [k\ l] = [i\ j] \circ [i\ l] = [j\ i] \circ [i\ l] = [j\ i\ l]$.
Περίπτωση τρίτη. Εάν $j = k$, τότε $i < l$ και -κατ' αναλογίαν- λαμβάνουμε

$$[i\ j] \circ [k\ l] = [i\ j] \circ [j\ l] = [i\ j\ l].$$

Περίπτωση τέταρτη. Εάν $i \neq k$ και $j \neq l$, τότε βάσει των (ii) και (v) τής προτάσεως 4.2.3 και τής γενικευμένης προσεταιριστικής ιδιότητας (βλ. πρόταση 1.6.40) συμπεραίνουμε ότι

$$\begin{aligned} [i\ j] \circ [k\ l] &= [i\ j] \circ \mathrm{id} \circ [k\ l] = [i\ j] \circ [j\ k]^2 \circ [k\ l] \\ &= ([i\ j] \circ [j\ k]) \circ ([j\ k] \circ [k\ l]) = [i\ j\ k] \circ [j\ k\ l]. \end{aligned}$$

(iii) Κατ' αρχάς, κατά το (iii) τού θεωρήματος 4.3.5 κάθε 3-κύκλος είναι άρτια μετάταξη, οπότε ανήκει στην $\mathfrak{A}_n$. Λόγω τού (ii) αρκεί να δειχθεί ότι κάθε κύκλος $[i\ j\ k] \in \mathfrak{A}_n$ μήκους 3 μπορεί να γραφεί ως σύνθεση (πεπερασμένου πλήθους) στοιχείων τού συνόλου $\langle \{[\alpha\ \beta\ i] \mid i \in \{1, \ldots, n\} \smallsetminus \{\alpha, \beta\}\} \rangle$. Επειδή

$$[i\ j\ k] = [\alpha\ \beta\ i]^2 \circ [\alpha\ \beta\ k] \circ [\alpha\ \beta\ j]^2 \circ [\alpha\ \beta\ i],$$

τούτο είναι πρόδηλο. Τέλος, το (iv) έπεται από το (iii) θέτοντας $\alpha = 1, \beta = 2$. □

4.4 ΠΑΡΑΔΕΙΓΜΑΤΑ ΟΜΑΔΩΝ ΜΕΤΑΤΑΞΕΩΝ

4.4.1 Ορισμός. Κάθε υποομάδα τής $\mathfrak{S}_n$ (όπου $n \in \mathbb{N}$) ή, γενικότερα, τής $\mathfrak{S}_A$ (όπου A ένα μη κενό σύνολο) καλείται **ομάδα μετατάξεων**.

4.4.2 Παραδείγματα. (i) Η εναλλάσσουσα ομάδα $\mathfrak{A}_n$ είναι μια ομάδα μετατάξεων.
(ii) Έστω **V** το ακόλουθο υποσύνολο τής $\mathfrak{A}_4$:

$$\mathbf{V} := \{\mathrm{id}, [1\,2] \circ [3\,4]\,, [1\,3] \circ [2\,4]\,, [1\,4] \circ [2\,3]\}\,.$$

Είναι άμεσος ο έλεγχος τού ότι το **V** είναι κλειστό ως προς την πράξη τής συνθέσεως και τού ότι αποτελεί μια *αβελιανή* υποομάδα τής $\mathfrak{A}_4$ (και, κατ' επέκταση, και τής $\mathfrak{S}_4$), έχουσα ως πολλαπλασιαστικό κατάλογό της τον

$\circ$	id	$[1\,2] \circ [3\,4]$	$[1\,3] \circ [2\,4]$	$[1\,4] \circ [2\,3]$
id	id	$[1\,2] \circ [3\,4]$	$[1\,3] \circ [2\,4]$	$[1\,4] \circ [2\,3]$
$[1\,2] \circ [3\,4]$	$[1\,2] \circ [3\,4]$	id	$[1\,4] \circ [2\,3]$	$[1\,3] \circ [2\,4]$
$[1\,3] \circ [2\,4]$	$[1\,3] \circ [2\,4]$	$[1\,4] \circ [2\,3]$	id	$[1\,2] \circ [3\,4]$
$[1\,4] \circ [2\,3]$	$[1\,4] \circ [2\,3]$	$[1\,3] \circ [2\,4]$	$[1\,2] \circ [3\,4]$	id

Η ομάδα μετατάξεων[9] $(\mathbf{V}, \circ)$ καλείται **ομάδα των τεσσάρων στοιχείων τού Klein**. Η $(\mathbf{V}, \circ)$ *δεν είναι κυκλική*, διότι

$$\mathrm{ord}(\mathrm{id}) = 1,\ \mathrm{ord}([1\,2] \circ [3\,4]) = \mathrm{ord}([1\,3] \circ [2\,4]) = \mathrm{ord}([1\,4] \circ [2\,3]) = 2,$$

οπότε $\mathbf{V} \ncong \mathbb{Z}_4$. (Βλ. 3.4.7.)

(iii) Έστω $n \in \mathbb{N}$, $n \geqslant 3$. Ορίζουμε τις ακόλουθες μετατάξεις $\sigma, \tau \in \mathfrak{S}_n$:

$$\sigma := \begin{bmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{bmatrix},\ \tau := [1\,2\ \ldots\ n]. \tag{4.12}$$

Σημειωτέον ότι

$$\sigma^2 = \mathrm{id} = \tau^n,\quad \tau \circ \sigma = \sigma \circ \tau^{-1}\ \left(= \sigma \circ \tau^{n-1}\right). \tag{4.13}$$

Η τρίτη ισότητα έπεται από τα (vi) και (vii) τής προτάσεως 4.2.3, διότι

$$\tau^{-1} = [n\ n-1\ \ldots\ 3\,2\,1] = [\sigma(1)\,\sigma(2)\ \ldots\ \sigma(n)] = \sigma \circ \tau \circ \sigma^{-1},$$

οπότε $\tau^{-1} = \sigma \circ \tau \circ \sigma^{-1} \underset{(\sigma^{-1}=\sigma)}{\Longrightarrow} \tau^{-1} = \sigma \circ \tau \circ \sigma \Rightarrow \sigma \circ \tau^{-1} = \sigma^{-1} \circ \tau^{-1} = \tau \circ \sigma$. Η υποομάδα

$$\boxed{\bar{\mathbf{D}}_n := \langle \sigma, \tau \rangle} \tag{4.14}$$

τής $\mathfrak{S}_n$ η παραγόμενη από τις σ και τ είναι μια (μη αβελιανή[10]) ομάδα μετατάξεων. Επειδή $\mathrm{ord}(\sigma) = 2$ (καθότι $\sigma \neq \mathrm{id}$, $\sigma^2 = \mathrm{id}$) και $\mathrm{ord}(\tau) = n$ (βλ. 4.2.3 (v)), μέσω των ισοτήτων (4.13) διαπιστώνουμε εύκολα ότι

$$\bar{\mathbf{D}}_n = \left\{\sigma^j \circ \tau^k \,|\, j \in \{0,1\}\ ,\ k \in \{0,1,...,n-1\}\right\}.$$

Τα αναγραφόμενα $2n$ στοιχεία είναι σαφώς διακεκριμένα. Πράγματι· εάν

$$j_1, j_2 \in \{0,1\},\ k_1, k_2 \in \{0,1,...,n-1\} : \sigma^{j_1} \circ \tau^{k_1} = \sigma^{j_2} \circ \tau^{k_2},$$

τότε $\tau^{k_2} = \sigma^{-j_2} \circ \sigma^{j_2} \circ \tau^{k_2} = \sigma^{-j_2} \circ \sigma^{j_1} \circ \tau^{k_1} = \sigma^{j_1 - j_2} \circ \tau^{k_1} \Rightarrow \sigma^{j_1 - j_2} = \tau^{k_2 - k_1}$, οπότε $\tau^{k_2-k_1} \in \{\mathrm{id}, \sigma\}$. Στην περίπτωση κατά την οποία $\tau^{k_2-k_1} = \mathrm{id}$, έχουμε

$$\left.\begin{array}{r} \mathrm{ord}(\tau) = n \underset{(\text{βλ. } 3.4.8)}{\Longrightarrow} n \mid k_2 - k_1 \\ |k_2 - k_1| < n \end{array}\right\} \Rightarrow k_2 - k_1 = 0 \Rightarrow k_1 = k_2$$

και $\sigma^{j_1 - j_2} = \mathrm{id} \underset{(\mathrm{ord}(\sigma)=2)}{\Longrightarrow} j_1 - j_2 = 0 \Rightarrow j_1 = j_2$. Από την άλλη μεριά, υποτιθεμένου ότι $\tau^{k_2-k_1} = \sigma$, θα έπρεπε να ισχύει

$$\tau^{k_2-k_1+1} = \tau \circ \sigma = \sigma \circ \tau^{-1} = \tau^{k_2-k_1-1} \Rightarrow \tau^2 = \mathrm{id},$$

ήτοι κάτι που είναι αδύνατο, καθόσον $\mathrm{ord}(\tau) = n > 2$. Άρα τελικώς

$$\sigma^{j_1} \circ \tau^{k_1} = \sigma^{j_2} \circ \tau^{k_2} \Longleftrightarrow [j_1 = j_2 \ \text{ και } \ k_1 = k_2],$$

και $\left|\bar{\mathbf{D}}_n\right| = 2n$. Στο εδάφιο 4.4.4 θα ορισθεί άλλη μία σημαντική ομάδα μετατάξεων, η οποία, όπως θα δούμε, είναι ισόμορφη με την $\bar{\mathbf{D}}_n$ και διαθέτει στοιχεία που επιδέχονται μια ειδική *γεωμετρική ερμηνεία*.

4.4.3 Σημείωση. Όταν $n = 3$, τότε $\bar{\mathbf{D}}_3 = \mathfrak{S}_3$ (πρβλ. 4.2.2).

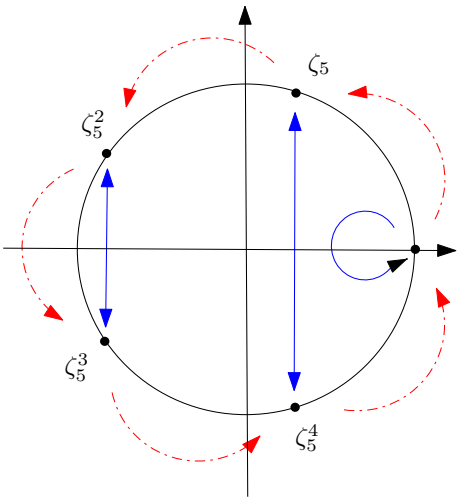
[9] Το γράμμα **V** επελέγη για να θυμίζει τη λέξη Vierergruppe που χρησιμοποιήθηκε για πρώτη φορά από τον Felix Klein (1849-1925) για την ονομασία τής εν λόγω ομάδας (ή, για να ακριβολογούμε, μιας ομάδας που είναι ισόμορφη με αυτή). Βλ. σελ. 13 τού συγγράμματός του: *Vorlesungen über das Ikosaeder*, Teubner, 1884.

[10] Προφανώς, $\tau \circ \sigma = \sigma \circ \tau^{-1} \neq \sigma \circ \tau$.

4.4.4 Παράδειγμα (Διεδρική ομάδα). Έστω $n \in \mathbb{N}$, $n \geqslant 3$, και έστω $(\mathcal{E}_n, \cdot)$ η ομάδα των n-οστών ριζών τής μονάδας (βλ. 3.2.21 (vi)). Ως γνωστόν, η $(\mathcal{E}_n, \cdot)$ είναι κυκλική, διότι γράφεται π.χ. ως $\mathcal{E}_n = \langle \zeta_n \rangle \sqsubset \mathbb{S}^1$, όπου $\zeta_n := \exp\left(\frac{2\pi i}{n}\right)$. (Βλ. το (iv) τού εδ. 3.3.16.) Θεωρούμε τα στοιχεία α και β τής $\mathfrak{S}_{\mathcal{E}_n}$ τα οριζόμενα μέσω των τύπων

$$\alpha(z) := z^{-1} = \frac{\overline{z}}{z\overline{z}} = \frac{\overline{z}}{|z|^2} = \overline{z}, \quad \beta(z) := \zeta_n z, \quad \forall z \in \mathcal{E}_n. \tag{4.15}$$

Αυτά επιδέχονται την εξής γεωμετρική ερμηνεία: Το α δηλοί τον *κατοπτρισμό* ως προς τον άξονα των (αμιγώς) πραγματικών αριθμών (στο μιγαδικό επίπεδο $\mathbb{C}$) και το β τη *στροφή* κατά $\frac{2\pi}{n}$ ακτίνια περί το $0 \in \mathbb{C}$ κατά τη φορά την αντίθετη τής κινήσεως των δεικτών τού ρολογιού (αντιωρολογιακή φορά). Μέσω τού κάτωθι σχήματος περιγράφονται οι εικόνες των α και β όταν $n = 5$.



Επίσης, παρατηρούμε ότι μεταξύ των α και β υφίστανται οι εξής σχέσεις:

$$\alpha^2 = \beta^n = \mathrm{id}_{\mathcal{E}_n}, \quad \beta \circ \alpha = \alpha \circ \beta^{-1} \left(= \alpha \circ \beta^{n-1}\right). \tag{4.16}$$

Η υποομάδα

$$\boxed{\mathbf{D}_n := \langle \alpha, \beta \rangle}$$

τής $\mathfrak{S}_{\mathcal{E}_n}$ η παραγόμενη από τα α και β είναι μια (μη αβελιανή) ομάδα μετατάξεων. Χρησιμοποιώντας επιχειρήματα ανάλογα εκείνων που χρησιμοποιήθηκαν στο (iii) τού εδαφίου 4.4.2 διαπιστώνουμε μέσω των ισοτήτων (4.16) ότι

$$\mathbf{D}_n = \left\{\alpha^j \circ \beta^k \,|j \in \{0,1\}\ ,\ k \in \{0,1,...,n-1\}\right\}$$

(με τα αναγραφόμενα στοιχεία σαφώς διακεκριμένα). Άρα[11] $|\mathbf{D}_n| = 2n$. Επιπροσθέτως, η απεικόνιση

$$\mathbf{D}_n \ni \alpha^j \circ \beta^k \longmapsto \sigma^j \circ \tau^k \in \bar{\mathbf{D}}_n, \quad j \in \{0,1\},\ k \in \{0,1,...,n-1\},$$

(όπου σ, τ όπως στην (4.12)) είναι ισομορφισμός ομάδων, οπότε

$$\boxed{\mathbf{D}_n \cong \bar{\mathbf{D}}_n.} \tag{4.17}$$

Η $(\mathbf{D}_n, \circ)$ καλείται n-**οστή διεδρική ομάδα**. Στην ειδική περίπτωση όπου $n = 3$ έχουμε[12] (λόγω των (4.17) και 4.4.3)

$$\boxed{\mathbf{D}_3 \cong \mathfrak{S}_3.}$$

[11] Προσοχή! Ορισμένοι συγγραφείς χρησιμοποιούν το σύμβολο $\mathbf{D}_{2n}$ αντί τού $\mathbf{D}_n$, επιθυμώντας να δηλούν μέσω τού (υπο)δείκτη *την τάξη* τής εν λόγω ομάδας (αντί τού πλήθους των αντιστοίχων ριζών τής μονάδας).

[12] Όταν $n > 3$, τότε $|\mathbf{D}_n| = 2n < n! = |\mathfrak{S}_n|$, οπότε $\mathbf{D}_n \ncong \mathfrak{S}_n$ (βλ. 4.1.3 και 3.5.22 (i)).

4.4.5 Σημείωση. Στην πραγματικότητα, η χρήση τής ονομασίας «διεδρική ομάδα» για την $\mathbf{D}_n$ οφείλεται σε μια ελαφρά παραλλαγή τής ανωτέρω γεωμετρικής ερμηνείας των γεννητόρων της, η οποία εκκινεί από το κανονικό n-γωνο P_n που έχει τα στοιχεία τής $\mathcal{E}_n \subsetneqq \mathbb{C}$ ως κορυφές του (βλ. 3.2.21 (vi)): Χρησιμοποιώντας τις ταυτίσεις

$$\mathbb{C} \ni x+yi \longleftrightarrow (x,y) \in \mathbb{R}^2, \quad \mathbb{R}^2 \ni (x,y) \longleftrightarrow \begin{pmatrix} x \\ y \end{pmatrix} \in \mathrm{Mat}_{2\times 1}(\mathbb{R}),$$

θεωρούμε το $\{\mathbf{v}_0, \mathbf{v}_1, ..., \mathbf{v}_{n-1}\}$, με $\mathbf{v}_j := \begin{pmatrix} \cos\left(\frac{2j\pi}{n}\right) \\ \sin\left(\frac{2j\pi}{n}\right) \end{pmatrix}$, $\forall j \in \{0,1,...,n-1\}$, ως το σύνολο των κορυφών τού P_n. Θέτοντας

$$\mathbf{M}P_n := \left\{ \mathbf{M}\begin{pmatrix} x \\ y \end{pmatrix} \middle| \begin{pmatrix} x \\ y \end{pmatrix} \in P_n \right\}, \ \forall \mathbf{M} \in \mathrm{Mat}_{2\times 2}(\mathbb{R}),$$

και ορίζοντας ως **ομάδα των (πλήρων, επιπέδων) συμμετριών τού** P_n την

$$\boxed{\Sigma\upsilon\mu\mu(P_n) := \{\mathbf{M} \in \mathrm{O}_2(\mathbb{R}) | \, \mathbf{M}P_n = P_n\} \sqsubset \mathrm{O}_2(\mathbb{R}),}$$

ήτοι την ομάδα την απαρτιζόμενη από τους ορθογώνιους πίνακες που στέλνουν το P_n να απεικονισθεί στο εαυτό του, αποδεικνύεται ότι

$$\begin{aligned} \Sigma\upsilon\mu\mu(P_n) = \langle \mathbf{A}, \mathbf{B} \rangle &= \left\{ \mathbf{A}^j\mathbf{B}^k \, | j \in \{0,1\} \ , \ k \in \{0,1,...,n-1\} \right\} \\ &= \left\{ \mathbf{I}_2, \mathbf{B}, \mathbf{B}^2, \ldots, \mathbf{B}^{n-1}, \mathbf{A}, \mathbf{AB}, \mathbf{AB}^2, \ldots, \mathbf{AB}^{n-1} \right\}, \end{aligned}$$

όπου

$$\mathbf{A} := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \ \mathbf{B} := \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}, \tag{4.18}$$

με

$$\mathbf{A}^2 = \mathbf{B}^n = \mathbf{I}_2, \quad \mathbf{BA} = \mathbf{AB}^{-1} \ \left(= \mathbf{AB}^{n-1}\right). \tag{4.19}$$

Επιπροσθέτως, $|\Sigma\upsilon\mu\mu(P_n)| = 2n$. Για κάθε $k \in \{0,1,...,n-1\}$ ο ορθογώνιος μετασχηματισμός

$$\mathbb{R}^2 \ni \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \mathbf{B}^k \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2, \ \text{με} \ \mathbf{B}^k = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) & -\sin\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) & \cos\left(\frac{2k\pi}{n}\right) \end{pmatrix},$$

παριστά γεωμετρικώς τη *στροφή*[13] κάθε σημείου τού $\mathbb{R}^2$ κατά $\frac{2\pi k}{n}$ ακτίνια περί το βαρύκεντρο $\binom{0}{0}$ τού P_n κατά τη θετική φορά (= αντιωρολογιακή φορά) και

$$\mathbf{B}^k\mathbf{v}_j = \mathbf{v}_{j+k}, \ \ \forall j \in \{0,1,...,n-1\},$$

όπου, εν προκειμένω, οι (υπο)δείκτες «διαβάζονται κατά μόδιο n». Από την άλλη μεριά, ο ορθογώνιος μετασχηματισμός

$$\mathbb{R}^2 \ni \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \mathbf{A}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ -y \end{pmatrix} \in \mathbb{R}^2$$

παριστά γεωμετρικώς τον *κατοπτρισμό* τού $\mathbb{R}^2$ ως προς τον άξονα των x. Γενικότερα, ο ορθογώνιος μετασχηματισμός

$$\mathbb{R}^2 \ni \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \mathbf{AB}^k \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2, \ \ k \in \{0,1,...,n-1\},$$

[13] Πρβλ. Σ.Α. Ανδρεαδάκη: *Αναλυτική Γεωμετρία*, Εκδόσεις Συμμετρία, Αθήνα, 1993, κεφάλαιο 16, ενότητα 8 (υπό τον τίτλο: *Ταξινόμηση των ισομετριών τού επιπέδου*), σελ. 322-326.

με

$$\mathbf{AB}^k = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) & -\sin\left(\frac{2k\pi}{n}\right) \\ -\sin\left(\frac{2k\pi}{n}\right) & -\cos\left(\frac{2k\pi}{n}\right) \end{pmatrix} = \begin{pmatrix} \cos(\frac{2(n-k)\pi}{n}) & \sin(\frac{2(n-k)\pi}{n}) \\ \sin(\frac{2(n-k)\pi}{n}) & -\cos(\frac{2(n-k)\pi}{n}) \end{pmatrix},$$

παριστά τον *κατοπτρισμό*[14] ως προς την ευθεία που διέρχεται από το $\binom{0}{0}$, σχηματίζει γωνία $\frac{(n-k)\pi}{n}$ ακτινίων με τον θετικό ημιάξονα των x και τέμνει (κατ' ανάγκην) το σύνορο τού P_n σε *ακριβώς δύο* σημεία, η θέση των οποίων εξαρτάται από το κατά πόσον ο n είναι άρτιος ή περιττός.

• Συγκεκριμένα, εάν $n = 2m+1$, για κάποιον φυσικό αριθμό $m \geqslant 1$, τότε αυτή η ευθεία καθορίζεται (κατά περίπτωση)

(I) από την κορυφή $\mathbf{v}_0$ και το μεσοσημείο $\frac{1}{2}(\mathbf{v}_m + \mathbf{v}_{m+1})$ τής αντικείμενης πλευράς $\overline{\mathbf{v}_m\mathbf{v}_{m+1}}$ τού P_n όταν $k = 0$,

(II) από την κορυφή $\mathbf{v}_{m-\frac{k}{2}}$ και το μεσοσημείο $\frac{1}{2}(\mathbf{v}_{m-\frac{k}{2}} + \mathbf{v}_{m-\frac{k}{2}+1})$ τής αντικείμενης πλευράς $\overline{\mathbf{v}_{m-\frac{k}{2}}\mathbf{v}_{m-\frac{k}{2}+1}}$ τού P_n όταν $k \in \{2, 4, \ldots, 2m-2, 2m\}$, και

(III) από την κορυφή $\mathbf{v}_{m-\frac{k-1}{2}}$ και το μεσοσημείο $\frac{1}{2}(\mathbf{v}_{n-\frac{k-3}{2}} + \mathbf{v}_{n-\frac{k-1}{2}})$ τής αντικείμενης πλευράς $\overline{\mathbf{v}_{n-\frac{k-3}{2}}\mathbf{v}_{n-\frac{k-1}{2}}}$ τού P_n όταν $k \in \{1, 3, 5, \ldots, 2m-3, 2m-1\}$.

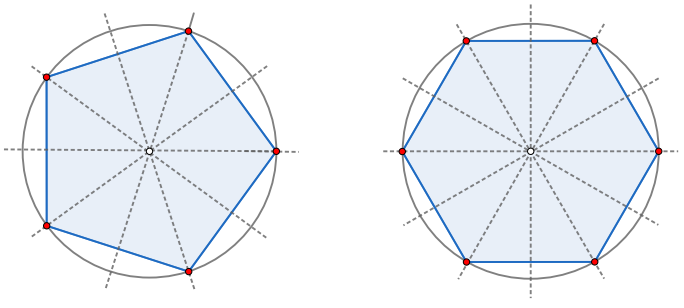
• Εάν $n = 2m$, για κάποιον φυσικό αριθμό $m \geqslant 2$, τότε η εν λόγω ευθεία η καθορίζεται (κατά περίπτωση)

(I) από τις κορυφές $\mathbf{v}_0$ και $\mathbf{v}_m$ όταν $k = 0$,

(II) από τις κορυφές $\mathbf{v}_k$ και $\mathbf{v}_{n-\frac{k}{2}}$ όταν $k \in \{2, 4, \ldots, 2m-4, 2m-2\}$, και

(III) από το μεσοσημείο $\frac{1}{2}(\mathbf{v}_{m-\frac{k+1}{2}} + \mathbf{v}_{m-\frac{k-1}{2}})$ τής πλευράς $\overline{\mathbf{v}_{m-\frac{k+1}{2}} + \mathbf{v}_{m-\frac{k-1}{2}}}$ και το μεσοσημείο $\frac{1}{2}(\mathbf{v}_{n-\frac{k+1}{2}} + \mathbf{v}_{n-\frac{k-1}{2}})$ τής αντικείμενης πλευράς της $\overline{\mathbf{v}_{n-\frac{k+1}{2}}\mathbf{v}_{n-\frac{k-1}{2}}}$ όταν $k \in \{1, 3, 5, \ldots, 2m-3, 2m-1\}$.

Οι κατ' αυτόν τον τρόπο περιγραφόμενες ευθείες, ως προς τις οποίες εκτελούνται οι n κατοπτρισμοί, δείχνονται στο ακόλουθο σχήμα για $n = 5$ και $n = 6$:



Η απεικόνιση

$$\mathbf{D}_n \ni \alpha^j \circ \beta^k \longmapsto \mathbf{A}^j\mathbf{B}^k \in \Sigma\upsilon\mu\mu(P_n), \;\; j \in \{0,1\}, \; k \in \{0,1,...,n-1\},$$

(όπου α, β όπως στην (4.15)) είναι ισομορφισμός ομάδων, οπότε

$$\boxed{\mathbf{D}_n \cong \Sigma\upsilon\mu\mu(P_n).}$$

[14] Ενας ορθογώνιος μετασχηματισμός τού επιπέδου $\binom{x}{y} \longmapsto \mathbf{M}\binom{x}{y}$, $\mathbf{M} \in \mathrm{O}_2(\mathbb{R})$, παριστά *κατοπτρισμό* εάν και μόνον εάν $\mathbf{M} = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}$, για κάποιον $\theta \in [0, 2\pi)$. (Εν προκειμένω, $\det(\mathbf{M}) = -1$ και ο *άξονας* τού κατοπτρισμού είναι η ευθεία που διέρχεται από το $\binom{0}{0}$ και σχηματίζει γωνία $\frac{\theta}{2}$ με τον θετικό ημιάξονα των x.)

Εν συνεχεία, παρατηρούμε ότι *όλοι* οι γραμμικοί μετασχηματισμοί οι επαγόμενοι από τα στοιχεία τού $\Sigma\upsilon\mu\mu(P_n)\setminus\{\mathbf{I}_2\}$ μπορούν να μετατραπούν καταλλήλως σε *περιστροφές τού τριδιάστατου χώρου* $\mathbb{R}^3$. Προς τούτο, χρησιμοποιούμε τις ταυτίσεις

$$\mathrm{Mat}_{2\times 1}(\mathbb{R}) \longleftrightarrow \mathbb{R}^2 \longleftrightarrow \left\{ (x,y,z) \in \mathbb{R}^3 \middle| \, z=0 \right\},$$

$$\mathbb{R}^3 \ni (x,y,z) \longleftrightarrow \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathrm{Mat}_{3\times 1}(\mathbb{R}),$$

και την εικόνα $\widehat{P}_n$ τού n-γώνου P_n μέσω αυτών. Το $\widehat{P}_n$ είναι ένα n-γωνο κείμενο επί τού xy-επιπέδου *εντός τού* $\mathbb{R}^3$ με το βαρύκεντρό του τοποθετημένο στην αρχή των (τριων) αξόνων των συντεταγμένων. (Κάθε σημείο τού n-γώνου $\widehat{P}_n$ έχει κατηγμένη $z=0$). Ενορατικώς, θα μπορούσαμε για διευκόλυνσή μας να το εκλάβουμε ως μια *n-γωνική πλάκα* απειροελάχιστου πάχους *εντός τού* $\mathbb{R}^3$ έχουσα *δύο έδρες* (εξ ου και το επίθετο *δίεδρος*). Ορίζοντας ως **ομάδα των περιστροφικών συμμετριών τού (δίεδρου n-γώνου)** $\widehat{P}_n$ την

$$\boxed{\Pi\varepsilon\rho.\Sigma\upsilon\mu\mu(\widehat{P}_n) := \left\{ \mathbf{M} \in \mathrm{SO}_3(\mathbb{R}) \middle| \, \mathbf{M}\widehat{P}_n = \widehat{P}_n \right\} \sqsubset \mathrm{SO}_3(\mathbb{R}),}$$

ήτοι την ομάδα την απαρτιζόμενη από τους ορθογώνιους πίνακες *με ορίζουσα ίση με* 1 που στέλνουν το $\widehat{P}_n$ να απεικονισθεί στο εαυτό του, αποδεικνύεται ότι

$$\begin{aligned} \Pi\varepsilon\rho.\Sigma\upsilon\mu\mu(\widehat{P}_n) &= \left\langle \widehat{\mathbf{A}}, \widehat{\mathbf{B}} \right\rangle = \left\{ \widehat{\mathbf{A}}^j \widehat{\mathbf{B}}^k \,|\, j \in \{0,1\} \ , \ k \in \{0,1,...,n-1\} \right\} \\ &= \left\{ \mathbf{I}_3, \widehat{\mathbf{B}}, \widehat{\mathbf{B}}^2, \ldots, \widehat{\mathbf{B}}^{n-1}, \widehat{\mathbf{A}}, \widehat{\mathbf{A}}\widehat{\mathbf{B}}, \widehat{\mathbf{A}}\widehat{\mathbf{B}}^2, \ldots, \widehat{\mathbf{A}}\widehat{\mathbf{B}}^{n-1} \right\}, \end{aligned}$$

όπου

$$\widehat{\mathbf{A}} := \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \ \widehat{\mathbf{B}} := \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) & 0 \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

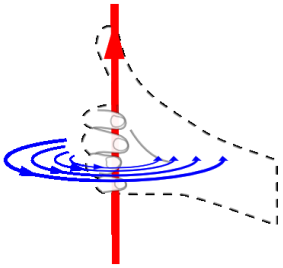
με

$$\widehat{\mathbf{A}}^2 = \widehat{\mathbf{B}}^n = \mathbf{I}_3, \quad \widehat{\mathbf{B}}\widehat{\mathbf{A}} = \widehat{\mathbf{A}}\widehat{\mathbf{B}}^{-1} \ (= \widehat{\mathbf{A}}\widehat{\mathbf{B}}^{n-1}). \tag{4.20}$$

Επιπροσθέτως, $\left|\Pi\varepsilon\rho.\Sigma\upsilon\mu\mu(\widehat{P}_n)\right| = 2n$. Για κάθε $k \in \{0,1,...,n-1\}$ ο ορθογώνιος μετασχηματισμός

$$\mathbb{R}^3 \ni \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \widehat{\mathbf{B}}^k \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3,$$

παριστά γεωμετρικώς τη *στροφή* κάθε σημείου τού $\mathbb{R}^3$ κατά $\frac{2\pi k}{n}$ ακτίνια περί τον άξονα των z και μάλιστα κατά τη *θετική φορά* ως προς το διάνυσμα που έχει ως απαρχή του την αρχή των αξόνων $\mathbf{0} \in \mathbb{R}^3$ και ως πέρας του το $\mathbf{v} := (0,0,1)$. [*Υπενθύμιση*: Η φορά μιας στροφής τού $\mathbb{R}^3$ περί έναν άξονα διερχόμενον από $\mathbf{0} \in \mathbb{R}^3$ καθορίζεται από ένα παγιωμένο διάνυσμα $\overrightarrow{\mathbf{0v}}$, όπου $\mathbf{v} \in \mathbb{R}^3$ ένα σημείο ανήκον σε αυτόν, μέσω τού κλασικού *κανόνα τής δεξιάς χειρός* (ή *κανόνα τής κοχλιώσεως*): Τοποθετώντας τόν αντίχειρα τής δεξιάς χειρός κατά τέτοιον τρόπο, ώστε αυτός να είναι ομόρροπος προς το διάνυσμα $\overrightarrow{\mathbf{0v}}$, λέμε ότι η στροφή τού $\mathbb{R}^3$ περί την ευθεία επί τής οποίας κείται το $\overrightarrow{\mathbf{0v}}$ εκτελείται κατά τη *θετική φορά* όταν εκτελείται κατά τη φορά την εξυπονοούμενη μέσω τής κάμψεως των λοιπών δακτύλων.]



Από την άλλη μεριά, ο ορθογώνιος μετασχηματισμός

$$\mathbb{R}^3 \ni \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \widehat{\mathbf{A}} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ -y \\ -z \end{pmatrix} \in \mathbb{R}^3$$

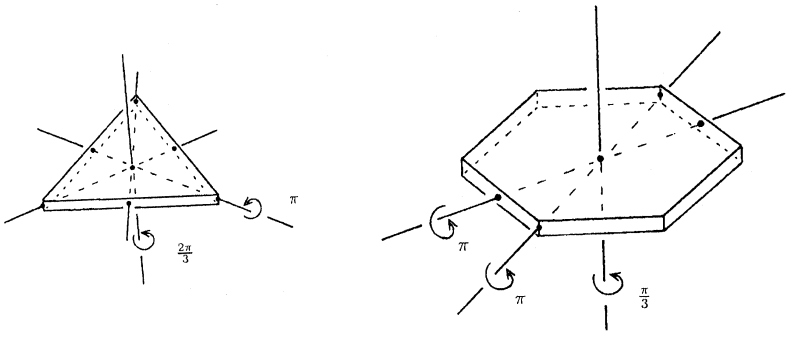
παριστά τη *στροφή* κάθε σημείου τού $\mathbb{R}^3$ κατά π ακτίνια περί τον άξονα των τετμημένων x (κατά τη θετική φορά ως προς το διάνυσμα $\overrightarrow{\mathbf{0v}}$, όπου $\mathbf{v} := (1,0,0)$). Γενικότερα, οι ορθογώνιοι μετασχηματισμοί

$$\mathbb{R}^3 \ni \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \widehat{\mathbf{A}}\,\widehat{\mathbf{B}}^k \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3, \quad k \in \{0,1,...,n-1\},$$

όπου

$$\widehat{\mathbf{A}}\,\widehat{\mathbf{B}}^k = \begin{pmatrix} \cos(\frac{2(n-k)\pi}{n}) & \sin(\frac{2(n-k)\pi}{n}) & 0 \\ \sin(\frac{2(n-k)\pi}{n}) & -\cos(\frac{2(n-k)\pi}{n}) & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

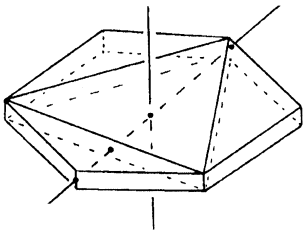
παριστούν *στροφές* τού $\mathbb{R}^3$ κατά π ακτίνια περί τις ευθείες, ως προς τις οποίες εκτελούνται οι n κατοπτρισμοί τού P_n (και τις οποίες έχουμε ήδη περιγράψει διεξοδικώς σε ό,τι προηγήθηκε). Στο κάτωθι σχήμα υποδηλούνται οι στροφές τού $\mathbb{R}^3$ οι επαγόμενες μέσω των πινάκων $\widehat{\mathbf{A}}$, $\widehat{\mathbf{B}}$ και $\widehat{\mathbf{A}}$, $\widehat{\mathbf{B}}$, $\widehat{\mathbf{A}}\,\widehat{\mathbf{B}}$, αντιστοίχως, και σχεδιάζονται οι άξονες περιστροφής, όταν $n = 3$ και $n = 6$, ύστερα από κατάλληλη επιλογή συντεταγμένων.



Παρεμπιπτόντως, αναφέρουμε ότι τα ανωτέρω είναι δυνατόν να «συνδυασθούν» προκειμένου να δοθεί μια *γεωμετρική* απόδειξη για το ότι[15]

$$\text{Περ.Συμμ}(\widehat{P}_3) \sqsubset \text{Περ.Συμμ}(\widehat{P}_6).$$

[15] Γενικότερα, $\text{Περ.Συμμ}(\widehat{P}_n) \sqsubset \text{Περ.Συμμ}(\widehat{P}_{2n})$ *για κάθε* $n \geqslant 3$.



Η απεικόνιση

$$\text{Συμμ}(P_n) \ni \mathbf{A}^j\mathbf{B}^k \longmapsto \widehat{\mathbf{A}}^j\widehat{\mathbf{B}}^k \in \text{Περ.Συμμ}(\widehat{P}_n),\ \ j \in \{0,1\},\ k \in \{0,1,...,n-1\},$$

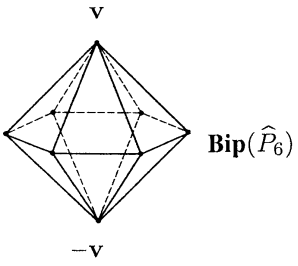
(όπου $\mathbf{A}, \mathbf{B}$ όπως στην (4.18)) είναι ισομορφισμός ομάδων, οπότε

$$\boxed{\mathbf{D}_n \cong \text{Συμμ}(P_n) \cong \text{Περ.Συμμ}(\widehat{P}_n).}$$

Τέλος, εάν κανείς επιθυμεί να αποκτήσει ένα «καθαρόαιμο» πολύεδρο, οι περιστροφικές συμμετρίες τού οποίου δομούν μια ομάδα ισόμορφη με την $\mathbf{D}_n$, αρκεί να θεωρήσει τη *διπλή πυραμίδα* $\textbf{Bip}(\widehat{P}_n)$ που σχηματίζεται ενώνοντας ένα σημείο $\mathbf{v} = (0,0,\lambda)$, $\lambda \in \mathbb{R}_{>0}\setminus\{1\}$, καθώς και το αντίθετό του $-\mathbf{v}$, με τις κορυφές τού $\widehat{P}_n$, διότι τότε

$$\boxed{\text{Περ.Συμμ}(\widehat{P}_n) \cong \text{Περ.Συμμ}(\textbf{Bip}(\widehat{P}_n)).}$$

Η διπλή πυραμίδα $\textbf{Bip}(\widehat{P}_6)$ δείχνεται στο σχήμα που ακολουθεί. [Αξίζει να επισημανθεί ότι, κατ' ουσίαν, ο περιορισμός $\lambda \neq 1$ απαιτείται μόνον όταν $n = 4$. Στην περίπτωση όπου $\lambda = 1$ και $n = 4$, η διπλή πυραμίδα $\textbf{Bip}(\widehat{P}_4)$ είναι ένα *κανονικό οκτάεδρο*, η ομάδα περιστροφικών συμμετριών τού οποίου είναι ισόμορφη με την ομάδα $\mathfrak{S}_4 \ncong \mathbf{D}_4$.]



4.4.6 Παρατήρηση. Η πρόταση 4.4.7 και το πόρισμα 4.4.8 μας πληροφορούν ότι η κλάση ισομορφίας τής $\mathbf{D}_n$ *καθορίζεται πλήρως* μόνον από τις υφιστάμενες σχέσεις μεταξύ των γεννητόρων. Ως εκ τούτου, κάθε επιπρόσθετη συνδυαστική (και αντιστοίχως, γεωμετρική) «υλοποίησή τους», όπως π.χ. μέσω των σ, τ (και αντιστοίχως, μέσω των $\mathbf{A}, \mathbf{B}$, των $\widehat{\mathbf{A}}, \widehat{\mathbf{B}}$ κ.ά.) δεν έχει ιδιαίτερη αξία για την «αφηρημένη συνιστώσα» τής Θεωρίας Ομάδων. Ωστόσο, ο ρόλος που διαδραματίζουν αυτές οι «υλοποιήσεις» σε διάφορα προβλήματα εντασσόμενα στη Γεωμετρία, στην Τοπολογία και σε άλλους μαθηματικούς κλάδους, στους οποίους απαιτείται η χρήση εποπτικών επιχειρημάτων, είναι σημαίνων και -ορισμένες φορές- λυτρωτικός.

4.4.7 Πρόταση. *Έστω $(G,\cdot)$ μια πεπερασμένη μη αβελιανή ομάδα η οποία μπορεί να παραχθεί από το σύνολο $\{s,t\}$ δύο στοιχείων της s και t. Εάν αυτοί οι γεννήτορες τής $(G,\cdot)$ υπόκεινται στις σχέσεις*

$$\boxed{s^2 = e_G,\ \ ts = st^{-1},}$$

και $n := \mathrm{ord}(t)$, *τότε* $n \geqslant 3$ *και* $(G,\cdot) \cong (\mathbf{D}_n, \circ)$.

Απόδειξη. Επειδή η $G = \langle s,t\rangle$ είναι εξ υποθέσεως μη αβελιανή, έχουμε κατ' ανάγκην $s \neq e_G$, $t \neq e_G$ και $s \neq t$. (Αλλιώς η G θα ήταν κυκλική και, ως εκ τούτου, αβελιανή, βλ. 3.3.17.) Σύμφωνα με την πρόταση 3.3.3,

$$G = \{x_1^{\varepsilon_1} \cdots x_\nu^{\varepsilon_\nu} \mid (x_1,..,x_\nu) \in \{s,t\}^\nu \text{ και } \varepsilon_\varrho \in \mathbb{Z},\ \forall \varrho \in \{1,..,\nu\}, \nu \in \mathbb{N}\}\,.$$

Πρώτος ισχυρισμός: $t^k s = st^{-k}$ *για κάθε* $k \in \mathbb{Z}$. Για $k = 1$ τούτο είναι εξ υποθέσεως αληθές. Ας υποθέσουμε ότι ο ισχυρισμός είναι αληθής και για κάποιον φυσικό αριθμό $k \geqslant 1$. Θα εφαρμόσουμε μαθηματική επαγωγή ως προς τον k. Προφανώς, $t^{k+1}s = t(t^k s) = t(st^{-k}) = (ts)t^{-k} = (st^{-1})t^{-k} = st^{-(k+1)}$. Κατ' αναλογίαν, για τους αρνητικούς ακεραίους k η ισότητα αποδεικνύεται χρησιμοποιώντας μαθηματική επαγωγή ως προς τον $-k$. Χρησιμοποιώντας τήν ισότητα $t^k s = st^{-k}$, καθώς και το ότι το s έχει τάξη 2, συνάγεται ότι $G = \left\{t^k \mid k \in \mathbb{Z}\right\} \cup \left\{st^k \mid k \in \mathbb{Z}\right\}$. Επειδή για κάθε $k \in \mathbb{Z}$ υπάρχει ζεύγος $(q,r) \in \mathbb{Z}^2 : k = nq + r$, $0 \leqslant r < n$ (βλ. θεώρημα 2.1.6), έχουμε $t^k = t^{nq+r} = (t^n)^q\, t^r = (e_G^n)^q\, t^r = e_G^q t^r = e_G t^r = t^r$, οπότε

$$G = \left\{s^j t^k \mid j \in \{0,1\}\ ,\ k \in \{0,1,...,n-1\}\right\}. \tag{4.21}$$

Δεύτερος ισχυρισμός: $n \geqslant 3$. Εάν ίσχυε $n = 1$, θα είχαμε $G = \{e_G, s\}$, ενώ εάν ίσχυε $n = 2$, θα είχαμε $G = \{e_G, s, t, st\}$. Αμφότερες οι περιπτώσεις αποκλείονται, διότι έχουμε υποθέσει ότι η G είναι μη αβελιανή.

Τρίτος ισχυρισμός: Τα αναγραφόμενα $2n$ στοιχεία στο (4.21) *είναι σαφώς διακεκριμένα*. Πράγματι· εάν $j_1, j_2 \in \{0,1\}$, $k_1, k_2 \in \{0,1,...,n-1\} : s^{j_1}t^{k_1} = s^{j_2}t^{k_2}$, τότε λαμβάνουμε

$$t^{k_2} = s^{-j_2}s^{j_2}t^{k_2} = s^{-j_2}s^{j_1}t^{k_1} \Rightarrow s^{j_1-j_2} = t^{k_2-k_1} \Rightarrow t^{k_2-k_1} \in \{e_G, s\}.$$

Στην περίπτωση κατά την οποία $t^{k_2-k_1} = e_G$, έχουμε

$$\left.\begin{array}{r} \mathrm{ord}(t) = n \underset{3.4.8}{\Longrightarrow} n \mid k_2 - k_1 \\ |k_2 - k_1| < n \end{array}\right\} \Rightarrow k_2 - k_1 = 0 \Rightarrow k_1 = k_2$$

και $s^{j_1-j_2} = e_G \underset{(\mathrm{ord}(s)=2)}{\Longrightarrow} j_1 - j_2 = 0 \Rightarrow j_1 = j_2$. Από την άλλη μεριά, υποτιθεμένου ότι $t^{k_2-k_1} = s$, θα έπρεπε να ισχύει $t^{k_2-k_1+1} = ts = st^{-1} = t^{k_2-k_1-1} \Rightarrow t^2 = e_G$, ήτοι κάτι που είναι αδύνατο, καθόσον $\mathrm{ord}(t) = n > 2$. Άρα

$$s^{j_1}t^{k_1} = s^{j_2}t^{k_2} \Longleftrightarrow [j_1 = j_2 \text{ και } k_1 = k_2],$$

και $|G| = 2n$. Η απεικόνιση

$$G \ni s^j t^k \longmapsto \alpha^j \circ \beta^k \in \mathbf{D}_n,\ \ j \in \{0,1\},\ k \in \{0,1,...,n-1\},$$

είναι εξ ορισμού αμφιρριπτική· επιπροσθέτως, είναι και ομομορφισμός ομάδων, καθότι για οιουσδήποτε $j_1, j_2 \in \{0,1\}$, $k_1, k_2 \in \{0,1,...,n-1\}$, έχουμε

$$(s^{j_1}t^{k_1})(s^{j_2}t^{k_2}) = \begin{cases} t^{k_1+k_2}, & \text{όταν } \ j_1 = j_2 = 0, \\ st^{k_1+k_2}, & \text{όταν } \ j_1 = 1,\ j_2 = 0, \\ t^{k_1}st^{k_2} = st^{k_2-k_1}, & \text{όταν } \ j_1 = 0,\ j_2 = 1, \\ s\left(t^{k_1}s\right)t^{k_2} = t^{k_2-k_1}, & \text{όταν } \ j_1 = j_2 = 1, \end{cases}$$

οπότε η εικόνα τού γινομένου δυο στοιχείων τής G μέσω αυτής ισούται με τη σύνθεση των εικόνων τους. Κατά συνέπειαν, $(G,\cdot) \cong (\mathbf{D}_n, \circ)$. □

4.4.8 Πόρισμα. *Έστω $(G,\cdot)$ μια πεπερασμένη, μη αβελιανή ομάδα η οποία μπορεί να παραχθεί από το σύνολο $\{s,u\}$ δύο στοιχείων της s και u. Εάν αυτοί οι γεννήτορες τής $(G,\cdot)$ υπόκεινται στις σχέσεις*

$$\boxed{s^2 = u^2 = e_G,}$$

και $n := \mathrm{ord}(su)$, τότε $n \geqslant 3$ και $(G,\cdot) \cong (\mathbf{D}_n, \circ)$.

Απόδειξη. Επειδή η $G = \langle s,u\rangle$ είναι εξ υποθέσεως μη αβελιανή, έχουμε κατ' ανάγκην $s \neq e_G$, $u \neq e_G$ και $s \neq u$. (Αλλιώς η G θα ήταν κυκλική και, ως εκ τούτου, αβελιανή, βλ. 3.3.17.) Θέτοντας $t := su$ παρατηρούμε ότι

$$s = tu \Rightarrow u = t^{-1}s \Rightarrow s,u \in \langle s,t\rangle \Rightarrow G = \langle s,t\rangle$$

με $ts = s(us) = s(u^{-1}s^{-1}) = s(su)^{-1} = st^{-1}$. Επομένως, για την αποπεράτωση τής αποδείξεως αρκεί η εφαρμογή τής προτάσεως 4.4.7 για τους γεννήτορες s,t τής ομάδας G. □

‣ **Από την πεπερασμένη στην άπειρη διεδρική ομάδα.** Αντικαθιστώντας τόν γεννήτορα t που παρατίθεται στην πρόταση 4.4.7 με έναν άλλον *απείρου τάξεως* και διατηρώντας -εκ παραλλήλου- τις υφιστάμενες σχέσεις μεταξύ των δύο γεννητόρων έχουμε τη δυνατότητα μεταβάσεως σε (ισόμορφες) μη αβελιανές *άπειρες ομάδες* (ομοιάζουσες με την $\mathbf{D}_n$). Το υποκείμενο σύνολο $\mathbf{D}_\infty$ τής ομάδας $(\mathbf{D}_\infty,\circ)$ που θεωρείται «πρότυπος εκπρόσωπος» τής κλάσεως ισομορφίας αυτών των ομάδων αποτελείται από τις *ισομετρίες* τού $\mathbb{R}$ που απεικονίζουν το σύνολο $\mathbb{Z}$ των ακεραίων επί τού εαυτού του.

4.4.9 Ορισμός (Ισομετρίες τού $\mathbb{R}$.). Το σύνολο

$$\boxed{\mathrm{Isom}(\mathbb{R}) := \{\,\sigma \in \mathfrak{S}_{\mathbb{R}} \mid\ |\sigma(x) - \sigma(y)| = |x-y|\,,\ \forall (x,y) \in \mathbb{R}\times\mathbb{R}\},}$$

καλείται **σύνολο ισομετριών** (και τα στοιχεία του **ισομετρίες**) **τού** $\mathbb{R}$. Επειδή (προφανώς) $\mathrm{id}_{\mathbb{R}} \in \mathrm{Isom}(\mathbb{R})$ και επειδή για οιεσδήποτε $\sigma_1,\sigma_2 \in \mathrm{Isom}(\mathbb{R})$ και για οιαδήποτε $(x,y) \in \mathbb{R}\times\mathbb{R}$ ισχύουν οι ισότητες

$$\begin{aligned}\left|(\sigma_1\circ\sigma_2^{-1})(x) - (\sigma_1\circ\sigma_2^{-1})(y)\right| &= \left|(\sigma_1(\sigma_2^{-1}(x)) - (\sigma_1(\sigma_2^{-1}(y))\right| \\ &= \left|\sigma_2^{-1}(x) - \sigma_2^{-1}(y)\right| = |x-y|\,,\end{aligned}$$

έχουμε $\sigma_1\circ\sigma_2^{-1} \in \mathrm{Isom}(\mathbb{R})$, οπότε $\mathrm{Isom}(\mathbb{R}) \sqsubset \mathfrak{S}_{\mathbb{R}}$. (Βλ. 3.2.16 (iii).)

4.4.10 Ορισμός. Για κάθε $a \in \mathbb{R}$ ορίζουμε ως **μεταφορά τού** $\mathbb{R}$ **κατά** a την αμφιριπτική απεικόνιση $T_a \in \mathfrak{S}_{\mathbb{R}}$ με $T_a(x) := x+a, \forall x \in \mathbb{R}$. Προφανώς, $T_a \in \mathrm{Isom}(\mathbb{R})$ για κάθε $a \in \mathbb{R}$.

4.4.11 Λήμμα. *Το σύνολο*

$$\boxed{\mathrm{Trans}(\mathbb{R}) := \{T_a \mid a \in \mathbb{R}\} \subseteq \mathrm{Isom}(\mathbb{R}),}$$

όλων των μεταφορών τού $\mathbb{R}$ συγκροτεί μια άπειρη αβελιανή υποομάδα τής $\mathrm{Isom}(\mathbb{R})$. *Επιπροσθέτως,* $(\mathrm{Trans}(\mathbb{R}),\circ) \cong (\mathbb{R},+)$.

Απόδειξη. Επειδή $T_0 = e_{\mathrm{Isom}(\mathbb{R})} = \mathrm{id}_{\mathbb{R}}$ και επειδή για οιουσδήποτε πραγματικούς αριθμούς a,b έχουμε $T_a^{-1} = T_{-a}$, $T_{a+b} = T_a\circ T_b = T_b\circ T_a = T_{b+a}$, ο πρώτος

ισχυρισμός είναι προφανής. Επιπροσθέτως, η $\mathbb{R} \ni a \mapsto T_a \in \mathrm{Trans}(\mathbb{R})$ αποτελεί ισομορφισμό ομάδων. □

4.4.12 Συμβολισμός. Με το γράμμα S θα συμβολίσουμε τον *κατοπτρισμό*

$$S : \mathbb{R} \longrightarrow \mathbb{R}, \quad x \longmapsto S(x) := -x,$$

τού $\mathbb{R}$ ως προς το 0.

4.4.13 Πρόταση (Περιγραφή των ισομετριών τού $\mathbb{R}$.). *Κάθε ισομετρία*

$$\sigma \in \mathrm{Isom}(\mathbb{R}) \setminus \mathrm{Trans}(\mathbb{R})$$

γράφεται υπό τη μορφή $\sigma = T_a \circ S = S \circ T_a^{-1} = S \circ T_{-a}$ για κάποιον $a \in \mathbb{R}$. Κατά συνέπειαν,

$$\begin{aligned} \mathrm{Isom}(\mathbb{R}) &= \mathrm{Trans}(\mathbb{R}) \cup \{T_a \circ S \,|a \in \mathbb{R}\} = \{T_a \,|a \in \mathbb{R} \cup \{T_a \circ S \,|a \in \mathbb{R}\} \\ &= \{\sigma \in \mathfrak{S}_{\mathbb{R}} | \, \exists a \in \mathbb{R} \text{ και } \exists \varepsilon \in \{\pm 1\} : \sigma(x) = \varepsilon x + a, \forall x \in \mathbb{R}\} \\ &= \{S^j \circ T_a \big| \, a \in \mathbb{R} \text{ και } j \in \{0,1\}\}. \end{aligned}$$

Απόδειξη. Έστω τυχούσα $\sigma \in \mathrm{Isom}(\mathbb{R})$ και έστω $a := \sigma(0)$. Τότε

$$\left(T_a^{-1} \circ \sigma\right)(0) = (T_{-a} \circ \sigma)(0) = 0$$

και $|(T_{-a} \circ \sigma)(x)| = |(T_{-a} \circ \sigma)(x) - (T_{-a} \circ \sigma)(0)| = |x - 0| = |x|$ για κάθε στοιχείο $x \in \mathbb{R} \setminus \{0\}$. Τούτο σημαίνει ότι

$$(T_{-a} \circ \sigma)(x) = \varepsilon x, \ \forall x \in \mathbb{R},$$

όπου $\varepsilon \in \{\pm 1\}$. Εν συνεχεία εξετάζουμε τα δύο ενδεχόμενα χωριστά.

Περίπτωση πρώτη. Εάν $\varepsilon = 1$, τότε $T_{-a} \circ \sigma = \mathrm{id}_{\mathbb{R}}$, οπότε $\sigma = T_a \in \mathrm{Trans}(\mathbb{R})$.

Περίπτωση δεύτερη. Εάν $\varepsilon = -1$, τότε $\sigma \in \mathrm{Isom}(\mathbb{R}) \setminus \mathrm{Trans}(\mathbb{R})$ και

$$T_{-a} \circ \sigma = S \Rightarrow \sigma = T_a \circ S = S \circ T_a^{-1} = S \circ T_{-a}.$$

Κατ' αυτόν τον τρόπο περιεγράφη διεξοδικώς *κάθε* ισομετρία τού $\mathbb{R}$. □

4.4.14 Παράδειγμα (Άπειρη διεδρική ομάδα). Η υποομάδα

$$\boxed{\mathbf{D}_\infty := \{\sigma \in \mathrm{Isom}(\mathbb{R}) | \, \sigma(\mathbb{Z}) = \mathbb{Z}\},}$$

τής $\mathrm{Isom}(\mathbb{R})$, η απαρτιζόμενη από εκείνες τις ισομετρίες τού $\mathbb{R}$ που απεικονίζουν το σύνολο $\mathbb{Z}$ των ακεραίων επί τού εαυτού του, καλείται **άπειρη διεδρική ομάδα**. Όπως θα δούμε στην πρόταση 4.4.15, η χρήση αυτής τής ονομασίας για την $\mathbf{D}_\infty$ οφείλεται στο ότι η $\mathbf{D}_\infty$ διαθέτει δύο γεννήτορες υποκειμένους σε σχέσεις πανομοιότυπες εκείνων στις οποίες υπόκεινται οι γεννήτορες α και β τής $\mathbf{D}_n$. (Ο πρώτος εξ αυτών έχει τάξη 2. Η μόνη διαφορά έγκειται στη φύση τού δευτέρου: Εν προκειμένω, η περιστροφή τάξεως n αντικαθίσταται με μια μεταφορά άπειρης τάξεως.)

4.4.15 Πρόταση. *Η $(\mathbf{D}_\infty, \circ)$ είναι μια άπειρη μη αβελιανή ομάδα με*

$$\boxed{\mathbf{D}_\infty = \langle S, T_{-1} \rangle = \left\{S^j \circ T_{-1}^k \,|j \in \{0,1\} \ , \ k \in \mathbb{Z}\right\},}$$

όπου $T_{-1} \circ S = S \circ {T_{-1}}^{-1}$ $(= S \circ T_1)$.

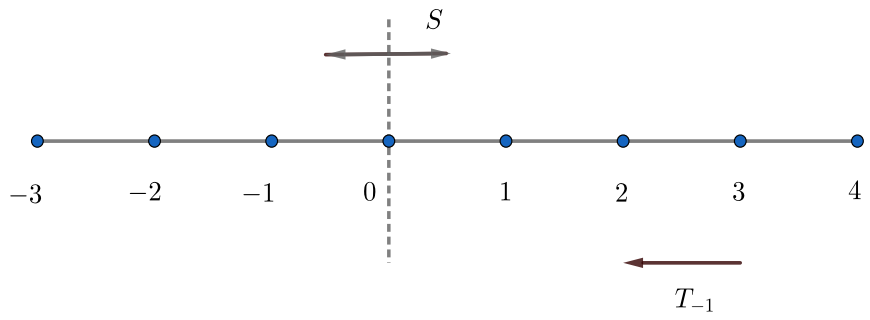
Απόδειξη. Έστω τυχούσα ισομετρία $\sigma \in \mathbf{D}_\infty$. Προφανώς, $\sigma(0) =: k \in \mathbb{Z}$. Κατά την πρόταση 4.4.13, $\exists j \in \{0,1\} : \sigma = S^j \circ T_{-k}$, όπου

$$T_{-k} = \begin{cases} {T_{-1}}^k, & \text{όταν} \quad k \geqslant 0, \\ {T_1}^{-k}, & \text{όταν} \quad k < 0. \end{cases}$$

Στηριζόμενοι στις ισότητες $T_{-1} \circ S = S \circ {T_{-1}}^{-1}$ $(= S \circ T_1)$ αποδεικνύουμε επαγωγικώς ότι

$$T_{-1}^k \circ S = S \circ {T_{-1}}^{-k} = S \circ T_1^k, \ \forall k \in \mathbb{Z}.$$

Εξ αυτού έπεται ότι $\langle S, T_{-1} \rangle = \left\{ S^j \circ T_{-1}^k \,|\, j \in \{0,1\} \ , \ k \in \mathbb{Z} \right\} = \mathbf{D}_\infty$ και η απόδειξη λήγει εδώ. □



4.4.16 Παρατήρηση. Κάθε στοιχείο τής $\mathbf{D}_\infty$, διάφορο τού ταυτοτικού, είναι *ή* μια (προς τα αριστερά ή προς τα δεξιά) μεταφορά κατά μία ακεραία απόσταση (ήτοι ένα εκ των στοιχείων τού συνόλου $\left\{ T_{-1}^k \,|\, k \in \mathbb{Z} \smallsetminus \{0\} \right\}$) *ή* ένας κατοπτρισμός[16], ο οποίος εκτελείται *είτε* ως προς ένα ακέραιο σημείο (όταν αυτός ανήκει στο $\left\{ S \circ T_{-1}^k \,|\, k \in \mathbb{Z}, k \equiv 0 \bmod 2 \right\}$) *είτε* ως προς ένα σημείο που βρίσκεται στο μέσον τού τμήματος τού καθοριζομένου από δύο ακέραια σημεία (όταν αυτός ανήκει στο $\left\{ S \circ T_{-1}^k \,|\, k \in \mathbb{Z}, k \equiv 1 \bmod 2 \right\}$).

Η κλάση ισομορφίας τής $\mathbf{D}_\infty$ (όπως συμβαίνει και με εκείνην τής $\mathbf{D}_n$) *καθορίζεται πλήρως* μόνον από τις υφιστάμενες σχέσεις μεταξύ των γεννητόρων. Συγκεκριμένα, ισχύει η ακόλουθη πρόταση:

4.4.17 Πρόταση. *Έστω $(G, \cdot)$ μια άπειρη μη αβελιανή ομάδα η οποία μπορεί να παραχθεί από το σύνολο $\{s, t\}$ δύο στοιχείων της s και t. Εάν αυτοί οι γεννήτορες τής $(G, \cdot)$ υπόκεινται στις σχέσεις*

$$\boxed{s^2 = e_G, \ \ ts = st^{-1},}$$

τότε $(G, \cdot) \cong (\mathbf{D}_\infty, \circ)$.

Απόδειξη. Επειδή η $G = \langle s, t \rangle$ είναι εξ υποθέσεως μη αβελιανή, έχουμε κατ' ανάγκην $s \neq e_G$, $t \neq e_G$ και $s \neq t$. (Αλλιώς η G θα ήταν κυκλική και, ως εκ τούτου, αβελιανή, βλ. 3.3.17.) Σύμφωνα με την πρόταση 3.3.3,

$$G = \{ x_1^{\varepsilon_1} \cdots x_\nu^{\varepsilon_\nu} \ | \ (x_1, .., x_\nu) \in \{s,t\}^\nu \text{ και } \varepsilon_\varrho \in \mathbb{Z}, \ \forall \varrho \in \{1, .., \nu\}, \nu \in \mathbb{N} \} .$$

Στηριζόμενοι στην ισότητα $ts = st^{-1}$ αποδεικνύουμε επαγωγικώς ότι $t^k s = st^{-k}$, για κάθε $k \in \mathbb{Z}$. Επειδή $s \neq e_G, s^2 = e_G \Rightarrow \mathrm{ord}(s) = 2$, συμπεραίνουμε τελικώς ότι

[16] Για κάθε $k \in \mathbb{Z}$ η ισομετρία $S \circ T_{-1}^k$ είναι ένας κατοπτρισμός ως προς το σημείο $\frac{k}{2}$, διότι έχουμε προφανώς $S(T_{-1}^k(x)) = x \Leftrightarrow x = \frac{k}{2}$.

$G = \left\{t^k \ | k \in \mathbb{Z}\right\} \cup \left\{st^k \,| k \in \mathbb{Z}\right\}$. (Η άπειρη κυκλική ομάδα $\langle t\rangle$ είναι υποομάδα τής G). Είναι εύκολο να ελεγχθεί ότι η $G \ni s^j t^k \longmapsto S^j \circ T_{-1}^k \in \mathbf{D}_\infty,\ j \in \{0,1\},\ k \in \mathbb{Z}$, αποτελεί ισομορφισμό ομάδων. □

4.5 ΤΟ ΘΕΩΡΗΜΑ ΤΟΥ CAYLEY

Η σημασία των ομάδων μετατάξεων στη Θεωρία Ομάδων παρεμφαίνεται στο ακόλουθο:

4.5.1 Θεώρημα (Cayley, 1878). *Κάθε ομάδα $(G,\cdot)$ εμφυτεύεται στην ομάδα $(\mathfrak{S}_G,\circ)$, ήτοι είναι ισόμορφη με μια ομάδα μετατάξεων $L(G)$ που αποτελεί υποομάδα τής $(\mathfrak{S}_G,\circ)$* (βλ. 3.5.11 και 8.1.18).

Απόδειξη. Έστω $(G,\cdot)$ τυχούσα ομάδα. Σε κάθε στοιχείο g τής G αντιστοιχούμε μια μετάταξη L_g οριζόμενη ως εξής:

$$L_g : G \longrightarrow G, \quad x \longmapsto L_g(x) := gx.$$

(Η απεικόνιση L_g είναι ενριπτική, διότι

$$L_g(x) = L_g(y) \Rightarrow gx = gy \Rightarrow g^{-1}gx = g^{-1}gy \Rightarrow e_G x = e_G y \Rightarrow x = y,$$

αλλά *και* επιριπτική, διότι εάν $z \in G$, τότε $L_g\left(g^{-1}z\right) = gg^{-1}z = e_G z = z$). Η L_g ονομάζεται **εξ αριστερών μεταφορά μέσω τού** g. Έστω τώρα

$$\boxed{L(G) := \{\, L_g \mid g \in G\} \subseteq \mathfrak{S}_G.}$$

Η πράξη με την οποία είναι εφοδιασμένη η $\mathfrak{S}_G$ είναι η σύνθεση απεικονίσεων. Προφανώς, $(L_g \circ L_h)(x) = L_g(L_h(x)) = L_g(hx) = ghx = L_{gh}(x), \forall x \in G$. Κατά συνέπειαν, η σύνθεση δυο τυχόντων στοιχείων τού $L(G)$ ανήκει στο $L(G)$. Το ταυτοτικό στοιχείο id_G τής $\mathfrak{S}_G$ ανήκει στο $L(G)$ διότι ισούται με την L_{e_G}, ενώ το αντίστροφο τής L_g εντός τής $\mathfrak{S}_G$ ισούται με την $L_{g^{-1}}$ και ανήκει και αυτό στο $L(G)$. Άρα $L(G) \sqsubseteq \mathfrak{S}_G$ δυνάμει τού (ii) τής προτάσεως 3.2.16. Η απεικόνιση

$$G \longrightarrow L(G), \quad g \longmapsto L_g,$$

είναι προφανώς επιριπτική και μεταφέρει τον πολλαπλασιασμό τής G στη σύνθεση απεικονίσεων τής $L(G)$ ($gh \longmapsto L_{gh} = L_g \circ L_h$). Εξάλλου, η εν λόγω απεικόνιση είναι και ενριπτική, αφού από την $L_g = L_h$ έπεται ότι

$$g = L_g(e_G) = L_h(e_G) = h.$$

Κατ' αυτόν τον τρόπο κατασκευάσαμε έναν ισομορφισμό μεταξύ τής G και τής υποομάδας $L(G)$ τής ομάδας $\mathfrak{S}_G$. □

4.5.2 Σημείωση. Η ανωτέρω κατασκευασθείσα ομάδα μετατάξεων $L(G)$ καλείται **εξ αριστερών κανονική αναπαράσταση τής G εντός τής $\mathfrak{S}_G$**. Βεβαίως, κατ' αναλογίαν, θα μπορούσε κανείς να εργασθεί και με την **εκ δεξιών κανονική αναπαράσταση**

$$\boxed{R(G) := \{\, R_g \mid g \in G\} \sqsubseteq \mathfrak{S}_G.}$$

τής G εντός τής $\mathfrak{S}_G$, όπου $R_g : G \longrightarrow G,\ x \longmapsto R_g(x) := xg$, η **εκ δεξιών μεταφορά μέσω τού** g. Προφανώς,

$$\boxed{L(G) \cong G \cong R(G).}$$

4.5.3 Πόρισμα. *Εάν η G είναι μια πεπερασμένη ομάδα τάξεως n, τότε η G είναι εμφυτεύσιμη στη συμμετρική ομάδα $\mathfrak{S}_n$.*

ΑΠΟΔΕΙΞΗ. Εάν, κατά κάποιον τρόπο, αριθμήσουμε τα στοιχεία τής ομάδας G ως $1, 2, \ldots, n$, δηλαδή εάν ορίσουμε μια αμφίρριψη $f : G \longrightarrow \{1, 2, \ldots, n\}$, τότε κάθε μετάταξη τής G επάγει μια μετάταξη των $1, 2, \ldots, n$ και, ως εκ τούτου, δημιουργείται ένας ισομορφισμός

$$\boxed{\Phi_f : \mathfrak{S}_G \longrightarrow \mathfrak{S}_n, \;\; \sigma \longmapsto \Phi_f(\sigma) := f \circ \sigma \circ f^{-1},}$$

μεταξύ τής $\mathfrak{S}_G$ και τής $\mathfrak{S}_n$. Επομένως, η υποομάδα $L(G)$ τής $\mathfrak{S}_G$ είναι ισόμορφη με την υποομάδα $\Phi_f(L(G))$ τής $\mathfrak{S}_n$. Επειδή η G είναι ισόμορφη με την $L(G)$ και επειδή η σύνθεση δύο ισομορφισμών είναι ένας ισομορφισμός (βλ. 3.5.9 (ii)), η G είναι ισόμορφη με την $\Phi_f(L(G))$. □

4.5.4 Παράδειγμα (Κυκλική ομάδα τάξεως 4). Έστω G μια κυκλική ομάδα τάξεως 4 και έστω g ένας γεννήτοράς της. Τότε $G = \{e, g, g^2, g^3\}$ (όπου $e := e_G$), ο δε πολλαπλασιαστικός κατάλογός της είναι ο εξής:

$\cdot$	e	g	g^2	g^3
e	e	g	g^2	g^3
g	g	g^2	g^3	e
g^2	g^2	g^3	e	g
g^3	g^3	e	g	g^2

Σύμφωνα με το θεώρημα 4.5.1 τού Cayley, $G \cong L(G)$, όπου

$$L(G) = \{L_e, L_g, L_{g^2}, L_{g^3}\} \sqsubset \mathfrak{S}_G.$$

Σημειωτέον ότι $L_e = \mathrm{id}_G$ και ότι οι εικόνες των τεσσάρων στοιχείων τής G μέσω των L_g, L_{g^2}, L_{g^3} είναι οι ακόλουθες:

x	$L_g(x)$
e	g
g	g^2
g^2	g^3
g^3	e

x	$L_{g^2}(x)$
e	g^2
g	g^3
g^2	e
g^3	g

x	$L_{g^3}(x)$
e	g^3
g	e
g^2	g
g^3	g^2

Έστω $f : G \longrightarrow \{1, 2, 3, 4\}$ η αμφίρριψη με $f(e) := 1$, $f(g) := 2$, $f(g^2) := 3$ και $f(g^3) := 4$. Τότε η απεικόνιση

$$\Phi_f : \mathfrak{S}_G \longrightarrow \mathfrak{S}_4, \;\; \sigma \longmapsto \Phi_f(\sigma) := f \circ \sigma \circ f^{-1},$$

αποτελεί έναν ισομορφισμό ομάδων. Άρα έχουμε $L(G) \cong \Phi_f(L(G))$. Προφανώς, $\Phi_f(L_e) = \mathrm{id}$ και

$$\Phi_f(L_g) = f \circ L_g \circ f^{-1},$$

οπότε

$$\begin{aligned}
\Phi_f(L_g)(1) &= f(L_g(f^{-1}(1))) = f(L_g(e)) = f(g) = 2,\\
\Phi_f(L_g)(2) &= f(L_g(f^{-1}(2))) = f(L_g(g)) = f(g^2) = 3,\\
\Phi_f(L_g)(3) &= f(L_g(f^{-1}(3))) = f(L_g(g^2)) = f(g^3) = 4,\\
\Phi_f(L_g)(4) &= f(L_g(f^{-1}(4))) = f(L_g(g^3)) = f(e) = 1,
\end{aligned}$$

και, ως εκ τούτου,

$$\Phi_f\left(L_g\right) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} = [1\,2\,3\,4].$$

Κατ' αναλογίαν,

$$\Phi_f\left(L_{g^2}\right) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} = [1\,3] \circ [2\,4]\,,\ \Phi_f\left(L_{g^3}\right) = [1\,4\,3\,2].$$

Άρα η G είναι ισόμορφη με την υποομάδα

$$\Phi_f(L(G)) = \{\mathrm{id}, [1\,2\,3\,4], [1\,3] \circ [2\,4]\,, [1\,4\,3\,2]\}$$

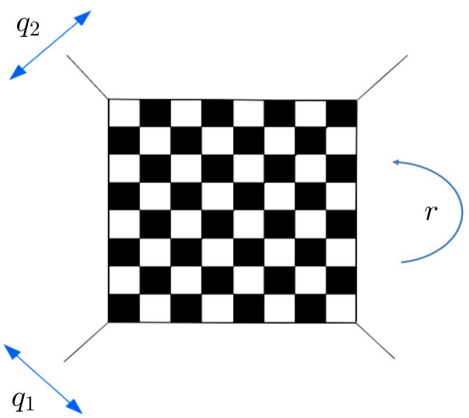
της $\mathfrak{S}_4$ (και φυσικά και με την ομάδα $(\mathbb{Z}_4, +)$ επί τη βάσει τού (ii) τού θεωρήματος 3.5.26). Τέλος, αξίζει να επισημανθεί ότι, ορίζοντας ως f μια *άλλη* αμφίριψη μεταξύ της G και τού $\{1, 2, 3, 4\}$, λαμβάνουμε μια *άλλη* εμφύτευση της G εντός της $\mathfrak{S}_4$. Επί παραδείγματι, εάν ορισθεί ως

$$f : G \longrightarrow \{1, 2, 3, 4\}$$

η αμφίριψη με $f(e) := 1$, $f(g) := 3$, $f(g^2) := 2$ και $f(g^3) := 4$, τότε

$$\Phi_f(L(G)) = \{\mathrm{id}, [1\,3\,2\,4], [1\,2] \circ [3\,4]\,, [1\,4\,3\,2]\}.$$

4.5.5 Παράδειγμα (Επίπεδες συμμετρίες μιας σκακιέρας). Μια σκακιέρα διαθέτει τέσσερεις επίπεδες συμμετρίες[17]: την ταυτοτική e ($:= \mathrm{id}_{\mathbb{R}^2}$), τη στροφή r περί το κέντρο της κατά π ακτίνια και τους κατοπτρισμούς q_1 και q_2 ως προς τις διαγωνίους της.



Αυτές οι συμμετρίες συγκροτούν μια ομάδα $G = \{e, r, q_1, q_2\}$ με πράξη της τη σύνθεση απεικονίσεων. Ο κατάλογος τής πράξεως "$\circ$" τής G είναι ο εξής:

$\circ$	e	r	q_1	q_2
e	e	r	q_1	q_2
r	r	e	q_2	q_1
q_1	q_1	q_2	e	r
q_2	q_2	q_1	r	e

[17] Ως *επίπεδες συμμετρίες* τής σκακιέρας ορίζονται εκείνα τα στοιχεία τής $\mathfrak{S}_{\mathbb{R}^2}$ που διατηρούν τις αποστάσεις και στέλνουν τη σκακιέρα να απεικονίζεται στον εαυτό της, διατηρώντας τό κέντρο της σταθερό. Προσοχή! Η ομάδα G που συγκροτούν οι εν λόγω συμμετρίες *δεν είναι* η ομάδα των συμμετριών ενός τετραγώνου (ήτοι ισόμορφη με την $\mathbf{D}_4$ τάξεως 8), διότι τα στοιχεία τής G οφείλουν, συν τοις άλλοις, να στέλνουν κάθε μαύρο (μικρό) τετραγωνάκι τής σκακιέρας να απεικονίζεται σε ένα μαύρο τετραγωνάκι (και κάθε άσπρο σε ένα άσπρο). Επί παραδείγματι, η στροφή περί το κέντρο τής σκακιέρας κατά $\frac{\pi}{2}$ (ή κατά $\frac{3\pi}{2}$) ακτίνια *δεν πληροί* αυτήν τη συνθήκη.

Σύμφωνα με το θεώρημα 4.5.1 τού Cayley, $G \cong L(G)$, όπου

$$L(G) = \{L_e, L_r, L_{q_1}, L_{q_2}\} \sqsubset \mathfrak{S}_G.$$

Σημειωτέον ότι $L_e = \mathrm{id}_G$ και ότι οι εικόνες των τεσσάρων στοιχείων τής G μέσω των L_r, L_{q_1}, L_{q_2} είναι οι ακόλουθες:

x	$L_r(x)$
e	r
r	e
q_1	q_2
q_2	q_1

x	$L_{q_1}(x)$
e	q_1
r	q_2
q_1	e
q_2	r

x	$L_{q_2}(x)$
e	q_2
r	q_1
q_1	r
q_2	e

Έστω $f : G \longrightarrow \{1,2,3,4\}$ η αμφίρριψη με $f(e) := 1$, $f(r) := 2$, $f(q_1) := 3$ και $f(q_2) := 4$. Τότε η απεικόνιση $\Phi_f : \mathfrak{S}_G \longrightarrow \mathfrak{S}_4$, $\sigma \longmapsto \Phi_f(\sigma) := f \circ \sigma \circ f^{-1}$, αποτελεί έναν ισομορφισμό ομάδων. Άρα έχουμε $L(G) \cong \Phi_f(L(G))$. Προφανώς, $\Phi_f(L_e) = \mathrm{id}$ και $\Phi_f(L_r) = f \circ L_r \circ f^{-1}$, οπότε

$$\begin{aligned}
\Phi_f(L_r)(1) &= f(L_r(f^{-1}(1))) = f(L_r(e)) = f(r) = 2,\\
\Phi_f(L_r)(2) &= f(L_r(f^{-1}(2))) = f(L_r(r)) = f(e) = 1,\\
\Phi_f(L_r)(3) &= f(L_r(f^{-1}(3))) = f(L_r(q_1)) = f(q_2) = 4,\\
\Phi_f(L_r)(4) &= f(L_r(f^{-1}(4))) = f(L_r(q_2)) = f(q_1) = 3,
\end{aligned}$$

και, ως εκ τούτου, $\Phi_f(L_r) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} = [1\,2] \circ [3\,4]$. Κατ' αναλογίαν,

$$\Phi_f(L_{q_1}) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} = [1\,3] \circ [2\,4]$$

και

$$\Phi_f(L_{q_2}) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix} = [1\,4] \circ [2\,3].$$

Κατά συνέπειαν, $\Phi_f(L(G)) = \mathbf{V}$, όπου η $\mathbf{V}$ είναι η ομάδα 4.4.2 (ii) των τεσσάρων στοιχείων τού Klein και $G \cong \mathbf{V}$.

Το θεώρημα 4.5.6 μας πληροφορεί ότι *κάθε* ομάδα *τάξεως* 4 οφείλει να είναι ισόμορφη με μία εκ των ομάδων μετατάξεων που παρουσιάσθηκαν στα παραδείγματα 4.5.4 και 4.5.5.

4.5.6 Θεώρημα (Ταξινόμηση ομάδων τάξεως 4). *Έστω $(G,\cdot)$ τυχούσα ομάδα τάξεως 4. Τότε ισχύουν τα ακόλουθα*:

(i) *H $(G,\cdot)$ είναι αβελιανή.*

(ii) *Εάν η $(G,\cdot)$ είναι κυκλική, τότε $(G,\cdot) \cong (\mathbb{Z}_4, +)$.*

(iii) *Εάν η $(G,\cdot)$ δεν είναι κυκλική, τότε είναι ισόμορφη με την ομάδα $(\mathbf{V},\circ)$ των τεσσάρων στοιχείων τού Klein.*

Απόδειξη. (i) Εάν η $(G,\cdot)$ είναι τυχούσα ομάδα τάξεως 4, τότε αυτή είναι αβελιανή. Πράγματι·

(α) Εάν η G διαθέτει κάποιο στοιχείο τάξεως 4, τότε η G είναι κυκλική και, ως εκ τούτου, αβελιανή (βλ. προτάσεις 3.4.7 και 3.3.17).

(β) Εάν η G έχει δεν έχει κανένα στοιχείο τάξεως 4, τότε η G δεν είναι κυκλική (βλ. πρόταση 3.4.7). Θεωρούμε τυχόντα $a, b \in G$. Θα αποδείξουμε ότι $ab = ba$.

(β_1) Εάν (τουλάχιστον) ένα εκ των a, b ισούται με το e $(:= e_G)$, τότε προφανώς $ab = ba$.

(β_2) Εάν $a = b$, τότε είναι και πάλι προφανές ότι $ab = ba$.

(β_3) Εάν $a \neq b$, $a \neq e$ και $b \neq e$, τότε $G = \{e, a, b, c\}$, όπου c το «τέταρτο» στοιχείο τής ομάδας G ($\{c\} \cap \{e, a, b\} = \varnothing$). Θεωρούμε το στοιχείο $ab \in G$. Αυτό αποκλείεται να ισούται με το a ή με το b, διότι, βάσει τού νόμου τής διαγραφής 3.2.9 (i), θα έπρεπε το a (ή, αντιστοίχως, το b) να ισούται με το e, κάτι που θα αντέκειτο στην υπόθεσή μας. Άρα $ab \in \{e, c\}$. Προτού προβούμε στην περαιτέρω εξέταση των δύο ενδεχομένων τιμών τού γινομένου ab, θα προσδιορίσουμε τις τάξεις των a και b.

Ισχυρισμός. $\mathrm{ord}(a) = \mathrm{ord}(b) = 2$.

Απόδειξη ισχυρισμού. Θεωρούμε την $\langle a \rangle \sqsubset G$. Προφανώς, $|\langle a \rangle| = \mathrm{ord}(a) \in \{2, 3\}$ (αφού $a \neq e$ και η G δεν είναι κυκλική). Εάν $|\langle a \rangle| = 3$, τότε $a \neq a^2$ και

$$\langle a \rangle = \{e, a, a^2\} \subsetneqq \{e, a, b, c\} = G \Rightarrow \text{είτε } \ b = a^2 \ \text{ είτε } \ c = a^2.$$

Εάν $b = a^2$, τότε $b = a^{-1}$ και $ac \in \{e, a, b, c\}$, κάτι που αποκλείεται λόγω των συνεπαγωγών

$$ac = e \Rightarrow c = a^{-1} = b,\ ac = a \Rightarrow c = e,\ ac = b = a^2 \Rightarrow c = a,\ ac = c \Rightarrow a = e.$$

Εάν $c = a^2$, τότε $c = a^{-1}$ και $ab \in \{e, a, b, c\}$, κάτι που αποκλείεται λόγω των συνεπαγωγών

$$ab = e \Rightarrow b = a^{-1} = c,\ ab = a \Rightarrow b = e,\ ab = b \Rightarrow a = e,\ ab = c = a^2 \Rightarrow b = a.$$

Κατά συνέπειαν, $\mathrm{ord}(a) = 2$. Εναλλάσσοντας τώρα τους ρόλους των a και b, και επιχειρηματολογώντας αναλόγως, αποδεικνύουμε την ισότητα $\mathrm{ord}(b) = 2$.

Εξέταση τού γινομένου ab. Είτε $ab = e$ είτε $ab = c$. Εάν $ab = e$, τότε $b = a^{-1} = a$ (αφού $\mathrm{ord}(a) = 2$, κατά τα προαναφερθέντα), κάτι που αντίκειται στην υπόθεσή μας. Άρα έχουμε κατ' ανάγκην $ab = c$. Εν συνεχεία, θεωρώντας τό στοιχείο $ba \in G$ και επαναλαμβάνοντας τα ως άνω επιχειρήματα τού (β_3) γι' αυτό (κατόπιν εναλλαγής των ρόλων των a και b), καταλήγουμε στο ότι $ba = c$. Άρα τελικώς $ab = c = ba$.

(ii) Τούτο έπεται άμεσα από το (ii) τού θεωρήματος 3.5.26.

(iii) Εάν η ομάδα $(G, \cdot)$ δεν είναι κυκλική, τότε (βασιζόμενοι σε ό,τι έχει προαναφερθεί στο (i)) μπορούμε να υποθέσουμε ότι το υποκείμενο σύνολό της είναι τής μορφής $G = \{e, a, b, c\}$ με τα e, a, b, c σαφώς διακεκριμένα και $c = ab$. Ο πολλαπλασιαστικός κατάλογος τής $(G, \cdot)$ είναι ο εξής:

$\cdot$	e	a	b	ab
e	e	a	b	ab
a	a	a^2	ab	a^2b
b	b	ab	b^2	ab^2
ab	ab	a^2b	ab^2	a^2b^2

Λαμβάνοντας υπ' όψιν ότι $\mathrm{ord}(a) = \mathrm{ord}(b) = 2$ (ή, εναλλακτικώς, ότι η G είναι αβελιανή και ότι κάθε στοιχείο της εμφανίζεται σε κάθε γραμμή και κάθε στήλη του μόνον μία φορά), αυτός γράφεται ως ακολούθως[18]:

$\cdot$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Υπάρχουν δύο τρόποι αποπερατώσεως τής αποδείξεως: Είτε επαναλαμβάνουμε κατά γράμμα τη διαδικασία που ακολουθήσαμε στο εδάφιο 4.5.5 (με τα a, b, ab στη θέση των r, q_1 και q_2, αντιστοίχως) είτε ορίζουμε απευθείας την απεικόνιση

$$e \longmapsto \mathrm{id},\ \ a \longmapsto [1\,2] \circ [3\,4]\,,\ \ b \longmapsto [1\,3] \circ [2\,4]\,,\ \ ab \longmapsto [1\,4] \circ [2\,3]$$

και διαπιστώνουμε ότι είναι ισομορφισμός ομάδων. □

[18] Εξ αυτού έπεται, ιδιαιτέρως, ότι $G = \langle a, b \rangle = \langle a, ab \rangle = \langle b, ab \rangle$.

4.5.7 Παρατήρηση. Προφανώς, $(\mathbf{V},\circ) \ncong (\mathbb{Z}_4,+)$. (Βλ. 3.5.22 (iii).) Επιπροσθέτως, η $\mathbf{V}$ γράφεται ως ένωση των τριών μη τετριμμένων γνησίων υποομάδων της.[19]

4.5.8 Πόρισμα (Ομάδα αυτομορφισμών ομάδων τάξεως 4).
Έστω $(G,\cdot)$ *τυχούσα ομάδα τάξεως* 4. *Τότε ισχύουν τα ακόλουθα*:
(i) *Εάν η* $(G,\cdot)$ *είναι κυκλική, τότε* $(\mathrm{Aut}(G),\circ) \cong (\mathbb{Z}_4^\times,\cdot) \cong (\mathbb{Z}_2,+)$.
(ii) *Εάν η* $(G,\cdot)$ *δεν είναι κυκλική, τότε* $(\mathrm{Aut}(G),\circ) \cong (\mathfrak{S}_3,\circ)$.

Απόδειξη. (i) Η ύπαρξη τού πρώτου ισομορφισμού διασφαλίζεται μέσω τού (ii) τού θεωρήματος 3.5.35. Για την απόδειξη τού ότι $(\mathbb{Z}_4^\times,\cdot) \cong (\mathbb{Z}_2,+)$ αρκεί να ληφθεί υπ' όψιν ότι $\mathbb{Z}_4^\times = \{[1]_4, [3]_4\} = \langle [3]_4 \rangle$ και να εφαρμοσθεί το 3.5.26 (ii).
(ii) Εάν η ομάδα $(G,\cdot)$ δεν είναι κυκλική, τότε $(G,\cdot) \cong (\mathbf{V},\circ)$ (σύμφωνα με το θεώρημα 4.5.6), όπου $\mathbf{V} := \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3\}$ με

$$\sigma_1 := [1\,2]\circ[3\,4]\,,\quad \sigma_2 := [1\,3]\circ[2\,4]\,,\quad \sigma_3 := [1\,4]\circ[2\,3]\,.$$

Έστω $f : G \longrightarrow \mathbf{V}$ ένας ισομορφισμός. Μέσω αυτού επάγεται ένας ισομορφισμός

$$\mathrm{Aut}(G) \ni \gamma \longmapsto f\circ\gamma\circ f^{-1} \in \mathrm{Aut}(\mathbf{V})$$

μεταξύ των ομάδων $(\mathrm{Aut}(G),\circ)$ και $(\mathrm{Aut}(\mathbf{V}),\circ)$. Αρκεί λοιπόν να δείξουμε ότι υφίσταται ισομορφισμός μεταξύ των $(\mathrm{Aut}(\mathbf{V}),\circ)$ και $(\mathfrak{S}_3,\circ)$. Για κάθε $\vartheta \in \mathrm{Aut}(\mathbf{V})$ ισχύει $\vartheta(\mathrm{id}) = \mathrm{id}$ (βλ. 3.5.3 (i)) και, ως εκ τούτου,

$$\{\vartheta(\sigma_1), \vartheta(\sigma_2), \vartheta(\sigma_3)\} = \{\sigma_1,\sigma_2,\sigma_3\}$$

με

$$\vartheta(\sigma_j\circ\sigma_k) = \vartheta(\sigma_j)\circ\vartheta(\sigma_k)\,,\ \forall (j,k)\in\{1,2,3\}\times\{1,2,3\}. \tag{4.22}$$

Παρατηρούμε ότι, στην πραγματικότητα, η μόνη δεσμευτική συνθήκη για τις εικόνες και τις αντίστροφες εικόνες των $\mathrm{id}, \sigma_1, \sigma_2, \sigma_3$ μέσω οιουδήποτε $\vartheta \in \mathrm{Aut}(\mathbf{V})$ είναι η $\vartheta(\mathrm{id}) = \mathrm{id}$, αφού η (4.22) πληρούται *αυτομάτως* για οιαδήποτε διατεταγμένα ζεύγη $(j,k) \in \{1,2,3\}\times\{1,2,3\}$. Τούτο είναι πρόδηλο στην περίπτωση κατά την οποία $j = k$ και έπεται από το γεγονός ότι

$$\sigma_{\varrho(j,k)} = \sigma_j\circ\sigma_k$$

στην περίπτωση κατά την οποία $j \neq k$, όπου $\{\varrho(j,k)\} = \{1,2,3\}\setminus\{j,k\}$. Κατά συνέπειαν,

$$[\vartheta(\mathrm{id}) = \mathrm{id} \text{ και } \vartheta|_{\{\sigma_1,\sigma_2,\sigma_3\}} \in \mathfrak{S}_{\{\sigma_1,\sigma_2,\sigma_3\}} \cong \mathfrak{S}_3,\ \forall\vartheta\in\mathrm{Aut}(\mathbf{V})] \Rightarrow \mathrm{Aut}(\mathbf{V}) \cong \mathfrak{S}_3.$$

Συγκεκριμένα,

$$\mathrm{Aut}(\mathbf{V}) = \{\vartheta_0,\vartheta_1,\vartheta_2,\vartheta_3,\vartheta_4,\vartheta_5\},$$

όπου $\vartheta_0 := e_{\mathrm{Aut}(\mathbf{V})}$, $\vartheta_j(\mathrm{id}) = \mathrm{id}$, για κάθε $j \in \{1,2,3,4,5\}$,

$$\begin{aligned}
&\vartheta_1(\sigma_1) := \sigma_1,\ \vartheta_1(\sigma_2) := \sigma_3,\ \vartheta_1(\sigma_3) := \sigma_2,\\
&\vartheta_2(\sigma_1) := \sigma_2,\ \vartheta_2(\sigma_2) := \sigma_1,\ \vartheta_2(\sigma_3) := \sigma_3,\\
&\vartheta_3(\sigma_1) := \sigma_2,\ \vartheta_3(\sigma_2) := \sigma_3,\ \vartheta_3(\sigma_3) := \sigma_1,\\
&\vartheta_4(\sigma_1) := \sigma_3,\ \vartheta_4(\sigma_2) := \sigma_1,\ \vartheta_4(\sigma_3) := \sigma_2
\end{aligned}$$

και $\vartheta_5(\sigma_1) := \sigma_3,\ \vartheta_5(\sigma_2) := \sigma_2,\ \vartheta_5(\sigma_3) := \sigma_1$. □

[19] Απαντήσεις στο ερώτημα τού πότε μια πεπερασμένη ομάδα G γράφεται ως ένωση n μη τετριμμένων γνησίων υποομάδων της, αλλά όχι ως ένωση τετριμμένων γνησίων υποομάδων της, το πλήθος των οποίων είναι $< n$, έχουν δοθεί για $3 \leqslant n \leqslant 7$ από τους Scorza, Cohn και Tomkinson. Βλ., σχετικώς, M. Bhargava: *Groups as unions of proper subgroups*, The American Mathematical Monthly **116** (2009), no 5, 413–422.

ΚΕΦΑΛΑΙΟ 5

Δείκτες, πηλικοομάδες και θεωρήματα ισομορφισμών

Σε αυτό το κεφάλαιο αποδεικνύεται εν πρώτοις ένα από τα σημαντικότερα θεωρήματα που αφορούν στις πεπερασμένες ομάδες, το λεγόμενο *θεώρημα τού Lagrange* 5.1.22, μέσω ενός γενικότερου θεωρήματος που συνδέει την τάξη *οιασδήποτε* ομάδας με την τάξη μιας υποομάδας της (βλ. θεώρημα 5.1.20). Προς τούτο προαπαιτείται η παράθεση των ορισμών των *πλευρικών κλάσεων* και τού *δείκτη* υποομάδων. Εν συνεχεία, αποδεικνύεται η *απλότητα* τής $\mathfrak{A}_n$ για $n \geqslant 5$, ορίζονται *πηλικοομάδες* και αποδεικνύονται τα τρία χαρακτηριστικά *θεωρήματα ισομορφισμών ομάδων*, καθώς και το *θεώρημα τής αντιστοιχίσεως ορθόθετων υποομάδων*.

5.1 ΠΛΕΥΡΙΚΕΣ ΚΛΑΣΕΙΣ ΚΑΙ ΔΕΙΚΤΕΣ ΥΠΟΟΜΑΔΩΝ

5.1.1 Ορισμός. Έστω $(G, \cdot)$ μια ομάδα. Εάν $\varnothing \neq A \subseteq G$ και $\varnothing \neq B \subseteq G$, τότε ορίζουμε ως $A \cdot B$ ή, απλούστερα (παραλείποντας το dot "$\cdot$", όταν δεν υφίσταται κίνδυνος συγχύσεως), ως AB το σύνολο[1]

$$\boxed{AB := \{xy \mid x \in A \quad \text{και} \quad y \in B\}.} \tag{5.1}$$

όλων των «γινομένων» ζευγών στοιχείων τού υποκειμένου συνόλου G τής ομάδας αναφοράς, με το *πρώτο* εξ αυτών (των στοιχείων) ειλημμένο από το A και το *δεύτερο* ειλημμένο από το B. (Προσοχή! Όταν η G δεν είναι αβελιανή, ενδέχεται το AB να μην είναι ίσο με το BA.)

5.1.2 Πρόταση. *Έστω $(G, \cdot)$ μια ομάδα. Εάν τα A, B, C είναι τρία μη κενά υποσύνολα τού υποκειμένου συνόλου G αυτής, τότε ισχύουν τα ακόλουθα*:

(i) $A(B \cup C) = AB \cup AC$.

(ii) $A(B \cap C) \subseteq AB \cap AC$. *Μάλιστα, στην περίπτωση κατά την οποία το A είναι ένα μονοσύνολο, αυτή η σχέση ισχύει ως ισότητα.*

[1] Όταν χρησιμοποιείται *προσθετικός συμβολισμός* για την ομάδα G, τότε αντί τού συνόλου AB θεωρούμε το σύνολο $A + B := \{x + y \mid x \in A \quad \text{και} \quad y \in B\}$.

(iii) $A\,(BC) = (AB)\,C$.

ΑΠΟΔΕΙΞΗ. (i) Τούτο έπεται από τις εξής αμφίπλευρες συνεπαγωγές:

$$\begin{aligned} & g \in A\,(B \cup C) = \{\,xy \mid x \in A \ \text{και} \ y \in B \cup C\} \subseteq G \\ \Leftrightarrow\ & g \in \{\,xy \mid x \in A \ \text{και} \ y \in B \ \text{ή} \ \ y \in C\} \\ \Leftrightarrow\ & g \in \{\,xy \mid x \in A \ \text{και} \ y \in B\} \ \text{ ή } \ g \in \{\,xy \mid x \in A \ \text{και} \ y \in C\} \\ \Leftrightarrow\ & g \in \{\,xy \mid x \in A \ \text{και} \ y \in B\} \cup \{\,xy \mid x \in A \ \text{και} \ y \in C\} \\ \Leftrightarrow\ & g \in AB \cup AC. \end{aligned}$$

(ii) Έστω τυχόν $g \in A\,(B \cap C)$. Τότε $g = xy$ για κάποια $x \in A$ και $y \in B \cap C$, οπότε

$$x \in A,\ y \in B \ \text{ και } \ x \in A,\ y \in C \Rightarrow g \in AB \cap AC.$$

Επομένως, $A\,(B \cap C) \subseteq AB \cap AC$. Στην περίπτωση κατά την οποία υπάρχει κάποιο στοιχείο $x \in G : A = \{x\}$, θεωρούμε τυχόν στοιχείο $g \in AB \cap AC$. Προφανώς,

$$\exists y \in B \ \text{ και } \ \exists z \in C : g = xy = xz \underset{\text{3.2.9 (i)}}{\Longrightarrow} y = z \in B \cap C,$$

οπότε $g \in A\,(B \cap C)$. Αυτό σημαίνει ότι $A\,(B \cap C) \supseteq AB \cap AC$.

(iii) Τούτο είναι άμεσο από τον ορισμό 5.1.1 και την προσεταιριστικότητα τής πράξεως "$\cdot$". □

5.1.3 Σημείωση. Το σύνολο $\mathfrak{P}\,(G) \setminus \{\varnothing\}$ των μη κενών υποσυνόλων τού υποκειμένου συνόλου G μιας ομάδας $(G, \cdot)$, εφοδιαζόμενο με την εσωτερική πράξη

$$(\mathfrak{P}\,(G) \setminus \{\varnothing\}) \times (\mathfrak{P}\,(G) \setminus \{\varnothing\}) \ni (A, B) \longmapsto AB \in \mathfrak{P}\,(G) \setminus \{\varnothing\}$$

την ορισθείσα στην (5.1), καθίσταται μονοειδές έχον το μονοσύνολο $\{e_G\}$ ως ουδέτερό του στοιχείο.

5.1.4 Πρόταση. *Έστω ότι τα H και K είναι δυο υποομάδες μιας ομάδας $(G, \cdot)$. Τότε*

$$\boxed{HK \sqsubseteq G \Longleftrightarrow HK = KH.}$$

(Προσοχή! Η ισότητα $HK = KH$ δεν σημαίνει ότι κάθε στοιχείο τής H μετατίθεται κατ' ανάγκην αμοιβαίως με κάθε στοιχείο τής K. Σημαίνει ότι για οιαδήποτε $a \in H$ και $b \in K$ υπάρχουν $a' \in H$ και $b' \in K$ με $ab = b'a'$ (και τανάπαλιν).)

ΑΠΟΔΕΙΞΗ. "$\Rightarrow$": Έστω τυχόν $x \in HK$. Τότε $x = ab$ για κάποια $a \in H$ και $b \in K$. Επειδή $HK \sqsubseteq G$, έχουμε $x^{-1} \in HK$ (βλ. το (ii) (c) τής προτάσεως 3.2.16). Άρα $x^{-1} = a'b'$ για κάποια $a' \in H$ και $b' \in K$, και

$$\left.\begin{aligned} x = \left(x^{-1}\right)^{-1} \Rightarrow x = (a'b')^{-1} = (b')^{-1}(a')^{-1} \\ b' \in K \Rightarrow (b')^{-1} \in K \ \ \text{και} \ \ a' \in H \Rightarrow (a')^{-1} \in H \end{aligned}\right\} \Rightarrow x = (b')^{-1}(a')^{-1} \in KH.$$

Τούτο σημαίνει ότι $HK \subseteq KH$. Για την απόδειξη τού αντιστρόφου εγκλεισμού θεωρούμε τυχόν $y \in KH$. Προφανώς, $y = ba$ για κάποια $b \in K$ και $a \in H$, και

$$\left.\begin{aligned} a \in H \Rightarrow a^{-1} \in H \ \ \text{και} \ \ b \in K \Rightarrow b^{-1} \in K \\ y^{-1} = (ba)^{-1} = a^{-1}b^{-1} \end{aligned}\right\} \Rightarrow y^{-1} \in HK.$$

Επειδή το HK υπετέθη ότι είναι υποομάδα τής G, έχουμε $\left(y^{-1}\right)^{-1} = y \in HK$. Άρα ισχύει και αντίστροφος εγκλεισμός $HK \supseteq KH$.

"$\Leftarrow$": Επειδή $H, K \sqsubseteq G$, έχουμε $e_G \in H$ και $e_G \in K$, οπότε $e_G e_G = e_G \in HK$. Εν συνεχεία θεωρούμε τυχόντα στοιχεία $x_1, x_2 \in HK$. Εξ ορισμού υπάρχουν στοιχεία $a_1, a_2 \in H$ και $b_1, b_2 \in K$, τέτοια ώστε $x_1 = a_1 b_1$ και $x_2 = a_2 b_2$. Επιπροσθέτως,

$$b_1 a_2 \in KH = HK \Rightarrow \exists a_3 \in H \text{ και } \exists b_3 \in K : b_1 a_2 = a_3 b_3.$$

Κατά συνέπειαν,

$$\begin{aligned} x_1 x_2 &= (a_1 b_1)(a_2 b_2) \underset{1.6.40}{=} a_1 (b_1 a_2) b_2 \\ &= a_1 (a_3 b_3) b_2 \underset{1.6.40}{=} (\underbrace{a_1 a_3}_{\in H})(\underbrace{b_3 b_2}_{\in K}) \in HK. \end{aligned}$$

Τέλος, για οιοδήποτε $x \in HK$ υπάρχουν $a \in H$ και $b \in K$, τέτοια ώστε να ισχύει η ισότητα $x = ab$, οπότε $x^{-1} = (ab)^{-1} = b^{-1}a^{-1} \in KH = HK$. Σύμφωνα με το (ii) τής προτάσεως 3.2.16, $HK \sqsubseteq G$. □

5.1.5 Παράδειγμα. Εάν $G := \mathfrak{S}_3$ και $H := \langle [1\,2] \rangle$, $K := \langle [2\,3] \rangle$, τότε

$$\{\mathrm{id},\ [1\,2]\,,\ [2\,3]\,,\ [1\,2\,3]\} = H \circ K \neq K \circ H = \{\mathrm{id},\ [1\,2]\,,\ [2\,3]\,,\ [1\,3\,2]\}\,,$$

οπότε κανένα εκ των συνόλων $H \circ K, K \circ H$ δεν είναι υποομάδα τής $\mathfrak{S}_3$.

5.1.6 Πρόταση. *Έστω $f : (G, \cdot) \longrightarrow (H, *)$ ένας ομομορφισμός ομάδων. Εάν υποθέσουμε ότι $K \sqsubseteq G$ και $L \sqsubseteq H$, τότε ισχύουν τα ακόλουθα:*
(i) $f^{-1}(f(K) * L) = Kf^{-1}(L)$.
(ii) $f^{-1}(L * f(K)) = f^{-1}(L)K$.
(iii) $f^{-1}(f(K)) = K(\mathrm{Ker}(f)) = (\mathrm{Ker}(f))K$, *οπότε* $K(\mathrm{Ker}(f)) \sqsubseteq G$.

Απόδειξη. (i) Από το (ii) τής προτάσεως 3.5.16 γνωρίζουμε ότι

$$f(f^{-1}(L)) = \mathrm{Im}(f) \cap L. \tag{5.2}$$

Επειδή η απεικόνιση f είναι εξ υποθέσεως ομομορφισμός, ισχύει η ισότητα

$$f(Kf^{-1}(L)) = f(K) * f(f^{-1}(L)). \tag{5.3}$$

Ως εκ τούτου,

$$\begin{aligned} Kf^{-1}(L) \subseteq f^{-1}\left(f(Kf^{-1}(L))\right) &\underset{(5.3)}{=} f^{-1}\left(f(K) * f(f^{-1}(L))\right) \\ &\underset{(5.2)}{=} f^{-1}\left(f(K) * (\mathrm{Im}(f) \cap L)\right). \end{aligned} \tag{5.4}$$

Επιπροσθέτως,

$$f(K) * (\mathrm{Im}(f) \cap L) \underset{5.1.2\,\text{(ii)}}{\subseteq} (f(K) * \mathrm{Im}(f)) \cap (f(K) * L) \subseteq f(K) * L, \tag{5.5}$$

οπότε από τις (5.4) και (5.5) προκύπτει ότι

$$Kf^{-1}(L) \subseteq f^{-1}\left(f(K) * (\mathrm{Im}(f) \cap L)\right) \subseteq f^{-1}(f(K) * L).$$

Έστω τώρα τυχόν $g \in f^{-1}(f(K) * L)$. Επειδή $f(g) \in f(K) * L$, υπάρχουν $g' \in K$ και $h \in L$, τέτοια ώστε να ισχύει $f(g) = f(g') * h$. Κατά συνέπειαν,

$$\begin{aligned} &f((g')^{-1}g) = f(g')^{-1} * f(g) = h \in L \Rightarrow (g')^{-1}g \in f^{-1}(\{h\}) \subseteq f^{-1}(L) \\ &\Rightarrow g = g'\left((g')^{-1}g\right) \in Kf^{-1}(L), \end{aligned}$$

οπότε ισχύει και ο αντίστροφος εγκλεισμός $f^{-1}(f(K) * L) \subseteq Kf^{-1}(L)$.

(ii) Αποδεικνύεται όπως το (i) (με εναλλαγή θέσεων των $f(K)$ και L).

(iii) Αρκεί να εφαρμοσθούν τα (i) και (ii) στην ειδική περίπτωση όπου $L = \{e_H\}$. Το ότι $K(\mathrm{Ker}(f)) \sqsubseteq G$ έπεται από την πρόταση 5.1.4. □

5.1.7 Ορισμός. Εάν η H είναι μια υποομάδα μιας ομάδας $(G,\cdot)$, τότε κάθε σύνολο τής μορφής

$$\boxed{Hg := H\{g\} = \{\, hg \mid h \in H\}}$$

(και αντιστοίχως, κάθε σύνολο τής μορφής

$$\boxed{gH := \{g\}H = \{\, gh \mid h \in H\}}\ )$$

όπου $g \in G$, καλείται **δεξιά** (και αντιστοίχως, **αριστερή**) **πλευρική κλάση**[2] **τής** H **εντός τής** G.

5.1.8 Ορισμός. Έστω ότι η $(G,\cdot)$ είναι μια ομάδα και η H μια υποομάδα της. Επί τού συνόλου G ορίζουμε τις διμελείς σχέσεις $\mathcal{R}_H, {}_H\mathcal{R} \subseteq G \times G$ μέσω των

$$\boxed{(x,y) \in \mathcal{R}_H \underset{\text{ορσ}}{\iff} xy^{-1} \in H} \tag{5.6}$$

και

$$\boxed{(x,y) \in {}_H\mathcal{R} \underset{\text{ορσ}}{\iff} x^{-1}y \in H.} \tag{5.7}$$

5.1.9 Πρόταση. *Οι* (5.6) *και* (5.7) *αποτελούν σχέσεις ισοδυναμίας επί τού* G.

Απόδειξη. Η (5.6) είναι *αυτοπαθής*, διότι

$$(e_G = xx^{-1} \in H \Longrightarrow (x,x) \in \mathcal{R}_H), \quad \forall x \in G,$$

συμμετρική, διότι εάν $(x,y) \in \mathcal{R}_H$, τότε

$$xy^{-1} \in H \Longrightarrow \left(xy^{-1}\right)^{-1} = yx^{-1} \in H \Longrightarrow (y,x) \in \mathcal{R}_H,$$

και, τέλος, *μεταβατική*, διότι εάν $(x,y) \in \mathcal{R}_H$ και $(y,z) \in \mathcal{R}_H$, τότε

$$\left(xy^{-1} \in H \ \text{ και } \ yz^{-1} \in H\right) \Longrightarrow \left(xy^{-1}\right)\left(yz^{-1}\right) = xz^{-1} \in H \Longrightarrow (x,z) \in \mathcal{R}_H.$$

Κατά συνέπειαν, η "$\mathcal{R}_H$" είναι μια σχέση ισοδυναμίας επί τού συνόλου G. Παρομοίως αποδεικνύεται ότι το ίδιο ισχύει και για την (5.7). □

5.1.10 Πρόταση. *Έστω* H *μια υποομάδα μιας ομάδας* $(G,\cdot)$. *Τότε ισχύουν τα εξής:*
(i) H *κλάση ισοδυναμίας* $[g]_{\mathcal{R}_H} := \{\, y \in G \mid (y,g) \in \mathcal{R}_H\}$ *οιουδήποτε στοιχείου* $g \in G$ *(ως προς τη σχέση ισοδυναμίας* (5.6)*) ισούται με τη δεξιά πλευρική κλάση* Hg *τής* H *εντός τής* G *την οριζόμενη μέσω τού* g.
(ii) H *κλάση ισοδυναμίας* $[g]_{{}_H\mathcal{R}} := \{\, y \in G \mid (y,g) \in {}_H\mathcal{R}\}$ *οιουδήποτε στοιχείου* $g \in G$ *(ως προς τη σχέση ισοδυναμίας* (5.7)*) ισούται με την αριστερή πλευρική κλάση* gH *τής* H *εντός τής* G *την οριζόμενη μέσω τού* g.

[2] Εδώ προτιμάται η απόδοση τού *coset* ως *πλευρική κλάση* κατά τον αντίστοιχο γερμανικό όρο **Nebenklasse**. Λέξεις όπως *συσσύνολο* ή *ομοσύνολο* είναι εν γένει αδόκιμες, ενώ η αντ' αυτών χρήση τής λέξεως *σύμπλοκο* είναι προβληματική. Το «σύμπλοκο» ή «σύμπλεγμα» χρησιμοποιείται (ορθώς) για τη μετάφραση τής λέξεως complex, αλλά βεβαίως αναφέρεται στη σύγχρονη εννοιολόγησή της στα πλαίσια τής Ομολογικής Άλγεβρας και τής Αλγεβρικής Τοπολογίας! Ως εκ τούτου, η εμμονή σε πεπαλαιωμένη ορολογία (βλ. παραδόσεις τού R. Dedekind κατά το χειμερινό εξάμηνο τού 1855/56 στο πανεπιστήμιο τού Göttingen) σαφώς βλάπτει. Ο ίδιος ο van der Waerden (ενδεχομένως και άθελά του) ήταν αυτός που έδωσε τέλος στη χαοτική πολυσημία των αρχών τού εικοστού αιώνα, διότι χρησιμοποίησε *και* τον όρο Nebenklasse, ο οποίος τελικώς και επεβλήθη έναντι όλων των άλλων που ήταν τότε διαθέσιμοι (βλ. *Algebra* I, Springer, 1936, σελ. 25).

ΑΠΟΔΕΙΞΗ. (i) Η $[g]_{\mathcal{R}_H}$ ισούται πράγματι με

$$\{y \in G \mid (y,g) \in \mathcal{R}_H\} = \{y \in G \mid yg^{-1} \in H\} = \{y \in G \mid yg^{-1} = h \in H\}$$

$$= \{y \in G \mid y = hg,\ h \in H\} = \{hg \mid h \in H\}$$

ήτοι με τη δεξιά πλευρική κλάση Hg τής H εντός τής G την οριζόμενη μέσω τού στοιχείου g. Η απόδειξη τού (ii) είναι παρόμοια. □

5.1.11 Πόρισμα. *Εάν η H είναι μια υποομάδα μιας ομάδας $(G,\cdot)$, τότε*

$$\boxed{G = \bigcup_{Hg \in (G/\mathcal{R}_H)} Hg = \bigcup_{gH \in (G/_H\mathcal{R})} gH} \tag{5.8}$$

και ισχύουν οι αμφίπλευρες συνεπαγωγές

$$Hg_1 \cap Hg_2 \neq \varnothing \Leftrightarrow Hg_1 = Hg_2 \Leftrightarrow g_1 \in Hg_2 \Leftrightarrow g_1 g_2^{-1} \in H,\ \ \forall\, (g_1,g_2) \in G \times G,$$

καθώς και οι

$$g_1 H \cap g_2 H \neq \varnothing \Leftrightarrow g_1 H = g_2 H \Leftrightarrow g_1 \in g_2 H \Leftrightarrow g_1^{-1} g_2 \in H,\ \ \forall\, (g_1,g_2) \in G \times G.$$

Ιδιαιτέρως δε, για ένα $g \in G$, $g \in H \Leftrightarrow Hg = H \Leftrightarrow H = gH$.

ΑΠΟΔΕΙΞΗ. Αυτή έπεται από το γεγονός ότι τα σύνολα $G/\mathcal{R}_H = \{Hg \mid g \in G\}$ και $G/_H\mathcal{R} = \{gH \mid g \in G\}$ των κλάσεων ισοδυναμίας ως προς τις "$\mathcal{R}_H$" και "$_H\mathcal{R}$" είναι διαμελισμοί τού υποκειμένου συνόλου G τής ομάδας $(G,\cdot)$. Οι αμφίπλευρες συνεπαγωγές

$$Hg_1 = Hg_2 \Leftrightarrow g_1 \in Hg_2 \Leftrightarrow g_1 g_2^{-1} \in H$$

αποδεικνύονται στοιχειωδώς: Εάν $Hg_1 = Hg_2$, τότε προφανώς $g_1 \in Hg_1 = Hg_2$. Εάν $g_1 \in Hg_2$, τότε $\exists h \in H : g_1 = hg_2$, οπότε $g_1 g_2^{-1} = h \in H$. Τέλος, εάν υποθέσουμε ότι $g_1 g_2^{-1} \in H$, τότε $g_1 g_2^{-1} = h$ για κάποιο $h \in H$, οπότε

$$g_1 = hg_2 \Rightarrow Hg_1 = H\,(hg_2) = (Hh)g_2 = Hg_2.$$

Οι λοιπές αμφίπλευρες συνεπαγωγές αποδεικνύονται παρομοίως. □

5.1.12 Πρόταση. *Εάν η H είναι μια υποομάδα μιας ομάδας $(G,\cdot)$, τότε για κάθε στοιχείο $g \in G$ οι απεικονίσεις*

$$\left\{ \begin{array}{c} \theta_g^{[\delta]} : H \longrightarrow Hg \\ h \longmapsto hg \end{array} \right\},\ \left\{ \begin{array}{c} \theta_g^{[\alpha]} : H \longrightarrow gH \\ h \longmapsto gh \end{array} \right\}$$

είναι αμφιρριπτικές. Ως εκ τούτου,

$$|H| = \mathrm{card}\,(Hg) = \mathrm{card}\,(gH),\ \ \forall g \in G. \tag{5.9}$$

ΑΠΟΔΕΙΞΗ. Θεωρούμε την απεικόνιση

$$\psi_g^{[\delta]} : Hg \longrightarrow H,\ \ \psi_g^{[\delta]}(x) := xg^{-1},\ \forall x \in Hg.$$

Είναι εύκολο να διαπιστωθεί ότι $\theta_g^{[\delta]} \circ \psi_g^{[\delta]} = \mathrm{id}_{Hg}$ και $\psi_g^{[\delta]} \circ \theta_g^{[\delta]} = \mathrm{id}_H$. Άρα η $\theta_g^{[\delta]}$ είναι αμφιρριπτική απεικόνιση έχουσα την $\psi_g^{[\delta]}$ ως αντίστροφό της. Παρομοίως αποδεικνύεται ότι η $\theta_g^{[\alpha]}$ είναι ωσαύτως αμφιρριπτική έχουσα την

$$\psi_g^{[\alpha]} : gH \longrightarrow H,\ \ \psi_g^{[\alpha]}(x) := g^{-1}x,\ \forall x \in gH.$$

ως αντίστροφό της. □

5.1.13 Πόρισμα. *Εάν η* $f : (G, \cdot) \longrightarrow (H, *)$ *είναι ένας ομομορφισμός ομάδων, τότε ισχύουν τα ακόλουθα*:

(i) *Εάν* $g \in G$ *και* $y = f(g) \in \mathrm{Im}(f)$, *τότε*

$$f^{-1}(\{y\}) = g(\mathrm{Ker}(f)).$$

(ii) *Εάν* $L \sqsubseteq \mathrm{Im}(f)$ *και* $|\mathrm{Ker}(f)| < \infty, |L| < \infty$, *τότε η* $f^{-1}(L) \sqsubseteq G$ *έχει τάξη*

$$\left|f^{-1}(L)\right| = |\mathrm{Ker}(f)|\,|L|\,. \tag{5.10}$$

Απόδειξη. (i) Έστω τυχόν $x \in f^{-1}(\{y\})$ $(= \{x \in G \,|\, f(x) = y\})$. Τότε

$$f(x) = y = f(g) \Rightarrow f(g)^{-1} * f(x) = f(g^{-1}) * f(x) = f(g^{-1} \cdot x) \Rightarrow g^{-1} \cdot x \in \mathrm{Ker}(f),$$

οπότε $x \in g\mathrm{Ker}(f)$ και, ως εκ τούτου, $f^{-1}(\{y\}) \subseteq g\mathrm{Ker}(f)$. Και αντιστρόφως· εάν $x \in \mathrm{Ker}(f)$, τότε

$$f(g \cdot x) = f(g) * f(x) = e_H * y = y \Rightarrow g\mathrm{Ker}(f) \subseteq f^{-1}(\{y\})\,.$$

(ii) Επειδή $f^{-1}(L) = f^{-1}(\bigcup_{y\in L}\{y\}) = \bigcup_{y\in L} f^{-1}(\{y\})$, έχουμε (λόγω τού (i)) $f^{-1}(L) = \bigcup_{y\in L} g_y\mathrm{Ker}(f)$, για κάποιο στοιχείο $g_y \in f^{-1}(\{y\})$. Εάν $y_1, y_2 \in L$ με $y_1 \neq y_2$, τότε (βάσει τού πορίσματος 5.1.11) $g_{y_1}\mathrm{Ker}(f) \cap g_{y_2}\mathrm{Ker}(f) = \varnothing$. Τούτο σημαίνει ότι

$$f^{-1}(L) = \coprod_{y\in L} g_y\mathrm{Ker}(f) \Rightarrow |f^{-1}(L)| = \sum_{y\in L} \mathrm{card}(g_y\mathrm{Ker}(f)).$$

Κατά την (5.9), $\mathrm{card}(g_y\mathrm{Ker}(f)) = |\mathrm{Ker}(f)|$ για κάθε $g_y \in G$ και $y \in L$, οπότε η (5.10) είναι αληθής. □

5.1.14 Ορισμός. Εάν η H είναι μια υποομάδα μιας ομάδας $(G, \cdot)$, τότε κάθε πλήρες σύστημα εκπροσώπων τού συνόλου G ως προς την "$\mathcal{R}_H$", ήτοι κάθε $\Delta \subseteq G$, τέτοιο ώστε[3] για οιαδήποτε $x, y \in \Delta$ να ισχύει η συνεπαγωγή

$$x \neq y \Longrightarrow Hx \neq Hy \tag{5.11}$$

καλείται **σύστημα δεξιών εκπροσώπων τής** H **εντός τής** G. (Σημειωτέον ότι δυο τέτοια συστήματα εκπροσώπων έχουν πάντοτε *τον ίδιο πληθικό αριθμό*, καθότι καθένα εξ αυτών απαρτίζεται από μονοσημάντως επιλεγμένους εκπροσώπους των σαφώς διακεκριμένων δεξιών πλευρικών κλάσεων τής H εντός τής G.) Προφανώς,

$$\boxed{G = \coprod_{g\in\Delta} [g]_{\mathcal{R}_H} = \coprod_{g\in\Delta} Hg.}$$

Κατ' αναλογίαν, κάθε πλήρες σύστημα εκπροσώπων τού συνόλου G ως προς την "${}_H\mathcal{R}$" καλείται **σύστημα αριστερών εκπροσώπων τής** H **εντός τής** G.

5.1.15 Σημείωση. Επειδή $e_G = e_H \in H$, υπάρχει πάντοτε κάποιο $g_0 \in \Delta$, τέτοιο ώστε να ισχύει $e_G \in Hg_0$, οπότε $g_0 \in H$. Εν προκειμένω, το $Hg_0 = He_G = H$ είναι η μοναδική δεξιά πλευρική κλάση που περιέχει το e_G. Γι' αυτόν τον λόγο, όταν εργαζόμαστε με *συγκεκριμένα παραδείγματα* συστημάτων Δ δεξιών εκπροσώπων τής H εντός τής G, μπορούμε δίχως βλάβη τής γενικότητας να επιλέγουμε εξαρχής ως g_0 το ίδιο το e_G. (Αντίστοιχη σύμβαση υιοθετούμε και για συστήματα αριστερών εκπροσώπων.)

[3] Προφανώς, η συνθήκη (5.11) ισοδυναμεί με την: $\mathrm{card}(\Delta \cap Hg) = 1, \forall g \in G$.

5.1.16 Πρόταση. *Έστω H μια υποομάδα μιας ομάδας $(G,\cdot)$. Εάν το Δ είναι ένα σύστημα δεξιών και το A ένα σύστημα αριστερών εκπροσώπων τής H εντός τής G, τότε*

$$\operatorname{card}(\{Hg \,|g\in\Delta\}) = \operatorname{card}(\Delta) = \operatorname{card}(\mathrm{A}) = \operatorname{card}(\{gH \,|g\in\mathrm{A}\}). \tag{5.12}$$

Απόδειξη. Θεωρούμε την $f : \{Hg \,|g\in\Delta\} \longrightarrow \{gH \,|g\in\mathrm{A}\}$ με τύπο

$$f(Hg) := g^{-1}H, \ \ \forall g\in\Delta.$$

Λόγω τής ισχύος των αμφιπλεύρων συνεπαγωγών

$$Hg_1 = Hg_2 \Leftrightarrow g_1g_2^{-1}\in H \Leftrightarrow \left(g_1^{-1}\right)^{-1}g_2^{-1}\in H \Leftrightarrow g_1^{-1}H = g_2^{-1}H,$$

για κάθε $(g_1,g_2)\in G\times G$, η f είναι καλώς ορισμένη και ενριπτική απεικόνιση. Εάν το gH είναι τυχούσα αριστερή πλευρική κλάση τής H εντός τής G με $g\in\mathrm{A}$, τότε $f(Hg^{-1}) = (g^{-1})^{-1}H = gH$, οπότε η f είναι και επιριπτική. □

5.1.17 Ορισμός. Εάν η H είναι μια υποομάδα μιας ομάδας $(G,\cdot)$, τότε ο πληθικός αριθμός (5.12) τού συνόλου των σαφώς διακεκριμένων δεξιών (ή -ισοδυνάμως- αριστερών) πλευρικών κλάσεων τής H εντός τής G ονομάζεται **δείκτης τής** H **εντός τής** G και συμβολίζεται ως $|G:H|$. Όταν το εν λόγω σύνολο είναι πεπερασμένο (και, αντιστοίχως, άπειρο), τότε γράφουμε $|G:H|<\infty$ (και, αντιστοίχως, $|G:H|=\infty$).

5.1.18 Παραδείγματα. (i) Προφανώς, $|G:\{e_G\}| = |G|$, $|G:G| = 1$, όπου $\{e_G\}$ η τετριμμένη υποομάδα τής G, για οιαδήποτε ομάδα G. Εξάλλου, για οιαδήποτε $H\sqsubseteq G$ για την οποία ισχύει $|G:H| = 1$, έχουμε $H = G$ (διότι η μόνη αριστερή πλευρική κλάση τής H εντός τής G είναι η $\{e_G\}H = H$).

(ii) Εάν ως G θεωρήσουμε την προσθετική (άπειρη) ομάδα $\mathbb{Z}$ των ακεραίων και ως H την (άπειρη) υποομάδα της $n\,\mathbb{Z}$, για κάποιον $n\in\mathbb{N}$, τότε $|\mathbb{Z}:n\,\mathbb{Z}| = n$, διότι το σύνολο $\mathrm{A} := \{0,1,...,n-1\}$ αποτελεί ένα σύστημα αριστερών εκπροσώπων τής H εντός τής $\mathbb{Z}$, καθόσον $\mathbb{Z} = \coprod_{j=0}^{n-1}(j+H)$.

(iii) Η υποομάδα $(\mathbb{Z},+)$ τής $(\mathbb{Q},+)$ έχει δείκτη $|\mathbb{Q}:\mathbb{Z}| = \aleph_0$ εντός αυτής. (Βλ. εδ. 5.4.7.)

5.1.19 Παρατήρηση. Έστω H μια υποομάδα μιας ομάδας $(G,\cdot)$. Το ότι ο πληθικός αριθμός ενός συστήματος δεξιών εκπροσώπων τής H εντός τής G ισούται με τον πληθικό αριθμό ενός συστήματος αριστερών εκπροσώπων τής H εντός τής G *δεν σημαίνει* ότι οι πλευρικές κλάσεις οι απαρτίζουσες τους αντιστοίχους διαμελισμούς τής G θα ταυτίζονται κατ' ανάγκην ανά δύο και συνολοθεωρητικώς (ήτοι *στοιχείο προς στοιχείο*). Επί παραδείγματι, για τις

$$G := \mathfrak{S}_3 = \{\mathrm{id},\ [1\,2]\,,\ [1\,3]\,,\ [2\,3]\,,\ [1\,2\,3]\,,\ [1\,3\,2]\}$$

και $H := \langle[1\,2]\rangle = \{\mathrm{id},\ [1\,2]\}$ έχουμε

$$H\circ\mathrm{id} = H, \qquad H\circ[1\,2] = H,$$
$$H\circ[1\,3] = \{[1\,3]\,,[1\,3\,2]\}\,, \qquad H\circ[2\,3] = \{[2\,3]\,,[1\,2\,3]\}\,,$$
$$H\circ[1\,2\,3] = \{[2\,3]\,,[1\,2\,3]\}\,, \qquad H\circ[1\,3\,2] = \{[1\,3]\,,[1\,3\,2]\}\,,$$

και

$$\mathrm{id}\circ H = H, \qquad [1\,2]\circ H = H,$$
$$[1\,3]\circ H = \{[1\,3]\,,[1\,2\,3]\}\,, \qquad [2\,3]\circ H = \{[2\,3]\,,[1\,3\,2]\}\,,$$
$$[1\,2\,3]\circ H = \{[1\,3]\,,[1\,2\,3]\}\,, \qquad [1\,3\,2]\circ H = \{[2\,3]\,,[1\,3\,2]\}.$$

Το σύνολο $\{g_1, g_2, g_3\}$, όπου $g_1 := \mathrm{id}$, $g_2 := [1\,3]$, $g_3 := [2\,3]$, μπορεί να εκληφθεί τόσον ως σύστημα δεξιών όσον και ως σύστημα αριστερών εκπροσώπων τής H εντός τής G, οπότε

$$G = (H \circ g_1) \coprod (H \circ g_2) \coprod (H \circ g_3)$$
$$= (g_1 \circ H) \coprod (g_2 \circ H) \coprod (g_3 \circ H) \Rightarrow |G : H| = 3.$$

Ωστόσο, συνολοθεωρητικώς, $H \circ g_2 \neq g_2 \circ H$ και $H \circ g_3 \neq g_3 \circ H$. Θα πρέπει, βεβαίως, εκ παραλλήλου να τονισθεί ότι υπάρχουν πάντοτε υποομάδες *οιασδήποτε* θεωρούμενης ομάδας (μεταξύ των οποίων συγκαταλέγονται τουλάχιστον η τετριμμένη υποομάδα και η ίδια η ομάδα), κάθε δεξιά πλευρική κλάση των οποίων είναι και αριστερή πλευρική κλάση (ως προς το ίδιο στοιχείο αναφοράς τής ομάδας) και τανάπαλιν. (Οι εν λόγω υποομάδες καλούνται, ιδιαιτέρως, *ορθόθετες υποομάδες* και θα μελετηθούν στην επομένη ενότητα[4].)

5.1.20 Θεώρημα. *Εάν η H είναι μια υποομάδα μιας ομάδας $(G, \cdot)$, τότε*

$$\boxed{|G| = |G : H|\,|H|\,.} \tag{5.13}$$

Απόδειξη. Έστω Δ ένα σύστημα δεξιών εκπροσώπων τής H εντός τής G. Τότε

$$|G| := \mathrm{card}(G) = \mathrm{card}(\coprod_{g\in\Delta} Hg). \tag{5.14}$$

Η απεικόνιση

$$f : H \times \Delta \longrightarrow \coprod_{g\in\Delta} Hg, \quad f(h, g) := hg \in Hg,\ \forall (h, g) \in H \times \Delta, \tag{5.15}$$

είναι αμφίρριψη. Ως εκ τούτου, μέσω των (5.14) και (5.15) ή, εναλλακτικώς, μέσω των (5.14) και (5.9) συνάγεται ότι

$$|G| = \mathrm{card}\,(H \times \Delta) = |H| \cdot \mathrm{card}(\Delta) = \mathrm{card}(\Delta) \cdot |H| = |G : H|\,|H|\,,$$

οπότε η (5.13) είναι αληθής. □

5.1.21 Σημείωση. Εάν δύο εκ των πληθικών αριθμών $|G|\,, |H|\,, |G : H|$ είναι πεπερασμένοι, τότε και ο τρίτος είναι πεπερασμένος.

5.1.22 Πόρισμα (Θεώρημα τού Lagrange, 1770). *Εάν $(G, \cdot)$ είναι μια πεπερασμένη ομάδα, τότε η τάξη της $|G|$ διαιρείται διά τής τάξεως $|H|$ οιασδήποτε υποομάδας της H και $|G : H| = \frac{|G|}{|H|}$.*

Απόδειξη[5]. Εάν η G είναι μια πεπερασμένη ομάδα τάξεως $|G| = n \in \mathbb{N}$ και η H τυχούσα υποομάδα της τάξεως $|H| = m \leqslant n$, τότε $|G : H| < \infty$ και δυνάμει τής (5.13) έχουμε $m\,|n$ και $|G : H| = \frac{n}{m}$. □

[4] Κάθε υποομάδα μιας *αβελιανής* ομάδας είναι ορθόθετη (βλ. 5.2.6). Ως εκ τούτου, δεν θα πρέπει να μας εκπλήσσει το ότι για την αναζήτηση ενός παραδείγματος ομάδας περιέχουσας (κάποιες) μη ορθόθετες υποομάδες είμαστε υποχρεωμένοι να καταφύγουμε σε ομάδες όπως η $\mathfrak{S}_3$. Στην πραγματικότητα, μεταξύ των πεπερασμένων μη αβελιανών ομάδων, η $\mathfrak{S}_3$ είναι εκείνη η (-μέχρις ισομορφισμού- μονοσημάντως ορισμένη) ομάδα, η οποία διαθέτει *τη μικρότερη δυνατή τάξη* (βλ. 5.1.36, 5.1.37).

[5] Ο Joseph-Louis Lagrange (1736-1813) ήταν ο πρώτος που διετύπωσε ένα θεώρημα ισοδύναμο τού 5.1.22 το 1770 για μια *ειδική υποομάδα τής* $\mathfrak{S}_n$, η πρώτη ολοκληρωμένη απόδειξη τού οποίου εδόθη το 1803 από τον Pietro Abbatti (1768-1842). Πιθανολογείται ότι η πρώτη απόδειξη τού θεωρήματος 5.1.22 για *οιεσδήποτε πεπερασμένες ομάδες* οφείλεται στον Evariste Galois (1811-1832).

5.1.23 Παράδειγμα. Έστω H η κυκλική υποομάδα τής $(\mathbb{Z}_{12},+)$ παραγόμενη από το στοιχείο $[4]_{12}$. Τότε $H=\{[0]_{12},[4]_{12},[8]_{12}\}$ και οι δεξιές πλευρικές κλάσεις τής H εντός τής $\mathbb{Z}_{12}$ είναι οι

$$\begin{aligned}
H+[0]_{12}&=H+[4]_{12}=H+[8]_{12}=\{[0]_{12},[4]_{12},[8]_{12}\},\\
H+[1]_{12}&=H+[5]_{12}=H+[9]_{12}=\{[1]_{12},[5]_{12},[9]_{12}\},\\
H+[2]_{12}&=H+[6]_{12}=H+[10]_{12}=\{[2]_{12},[6]_{12},[10]_{12}\},\\
H+[3]_{12}&=H+[7]_{12}=H+[11]_{12}=\{[3]_{12},[7]_{12},[11]_{12}\}.
\end{aligned}$$

Κατά συνέπειαν, $|\mathbb{Z}_{12}:H|=4=\frac{12}{3}=\frac{|\mathbb{Z}_{12}|}{|H|}$.

▸ **Συνέπειες τού θεωρήματος τού Lagrange**. Το θεώρημα 5.1.22, όσο απλό κι αν φαντάζει, συγκαταλέγεται σε εκείνα τα τεχνικά μέσα τα οποία μας διευκολύνουν τόσο στις αποδείξεις πληθώρας σημαντικών αποτελεσμάτων (τής Θεωρίας Αριθμών και τής Θεωρίας Πεπερασμένων Ομάδων) όσον και στη μελέτη των υποομάδων συγκεκριμένων ομάδων σχετικώς μικρής τάξεως.

5.1.24 Πόρισμα. *Εάν $(G,\cdot)$ είναι μια πεπερασμένη ομάδα και H μια γνήσια υποομάδα της, τότε $|H|\leqslant\frac{1}{2}|G|$.*

Απόδειξη. $H\sqsubset G\underset{5.1.18\,\text{(i)}}{\Longrightarrow}|G:H|\geqslant 2\underset{5.1.22}{\Longrightarrow}\frac{|G|}{|H|}\geqslant 2\Rightarrow|H|\leqslant\frac{1}{2}|G|$. □

5.1.25 Πόρισμα. *Εάν οι H,K είναι δυο υποομάδες μιας πεπερασμένης ομάδας $(G,\cdot)$, τότε ισχύουν τα εξής:*

(i) $|H\cap K|\,|\,|H|,|H\cap K|\,|\,|K|$ *και* $|H\cap K|\,|\,\text{μκδ}(|H|,|K|)$.

(ii) *Εάν* $\text{μκδ}(|H|,|K|)=1$, *τότε* $H\cap K=\{e_G\}$.

(iii) *Εάν ισχύει* $|H|=|K|=p$ (*όπου p ένας πρώτος αριθμός*), *τότε είτε* $H=K$ *είτε* $H\cap K=\{e_G\}$.

Απόδειξη. (i) Επειδή $H\cap K\sqsubseteq H$ και $H\cap K\sqsubseteq K$, οι δύο πρώτες σχέσεις διαιρετότητας έπονται άμεσα από το θεώρημα 5.1.22 τού Lagrange. Προφανώς (λόγω τού πορίσματος 2.2.6) η τάξη $|H\cap K|$ τής τομής $H\cap K$ οφείλει να διαιρεί *και* τον μέγιστο κοινό διαιρέτη των $|H|$ και $|K|$.

(ii) $|H\cap K|\,|\,\text{μκδ}(|H|,|K|)=1\Rightarrow|H\cap K|=1\Rightarrow H\cap K=\{e_G\}$.

(iii) Εάν $|H|=|K|=p$, όπου p πρώτος αριθμός, τότε $\text{μκδ}(|H|,|K|)=p$, οπότε (λόγω τής τρίτης σχέσεως διαιρετότητας στο (i)) είτε $|H\cap K|=1$ είτε $|H\cap K|=p$. Στην πρώτη περίπτωση έχουμε $H\cap K=\{e_G\}$. Στη δεύτερη περίπτωση έχουμε $|H|=|H\cap K|=|K|=p$, οπότε $H=H\cap K=K$. □

5.1.26 Πόρισμα. *Έστω $(G,\cdot)$ μια πεπερασμένη ομάδα και έστω p ένας πρώτος αριθμός. Τότε υπάρχουν ακριβώς $(p-1)k$ στοιχεία τής G τάξεως p, όπου*

$$k:=\text{card}(\{H\in\mathbf{Subg}(G)\mid H\text{ κυκλική τάξεως }|H|=p\}).$$

Απόδειξη. Εάν ένα στοιχείο $x\in G$ έχει τάξη p, τότε $|\langle x\rangle|=p$ (βλ. (3.10)) και η πρόταση 3.4.10 μας πληροφορεί ότι *κάθε* στοιχείο $g\in\langle x\rangle\smallsetminus\{e_G\}$ έχει τάξη p και, ως εκ τούτου, $\langle g\rangle=\langle x\rangle$ (λόγω τού πορίσματος 3.4.17). Δυνάμει τού (iii) τού πορίσματος 5.1.25 δύο τυχούσες *διαφορετικές* κυκλικές υποομάδες τής G έχουν την τετριμμένη υποομάδα ως τομή τους. Επομένως το $\{g\in G\,|\text{ord}(g)=p\}$ είναι το σύνολο όλων των στοιχείων τού $G\smallsetminus\{e_G\}$ που ανήκουν σε όλες τις κυκλικές υποομάδες τής G τάξεως p. Καθεμιά εξ αυτών των υποομάδων διαθέτει ακριβώς $p-1$ στοιχεία τάξεως p (κανένα εκ των οποίων δεν ανήκει σε κάποια άλλη υποομάδα τής G τάξεως p). Εξ αυτού έπεται ότι $\text{card}(\{g\in G\,|\text{ord}(g)=p\})=(p-1)k$. □

5.1.27 Πόρισμα. *Εάν $(G,\cdot)$ είναι μια πεπερασμένη ομάδα, τότε η τάξη οιουδήποτε στοιχείου της είναι διαιρέτης τής $|G|$. (Ιδιαιτέρως,* $\exp(G) \mid |G|$.)

Απόδειξη. Εάν $g \in G$, τότε $\operatorname{ord}(g) = |\langle g\rangle|$ (βλ. (3.10)), οπότε η τάξη $\operatorname{ord}(g)$ τού g είναι διαιρέτης τής $|G|$ επί τη βάσει τού θεωρήματος 5.1.22 τού Lagrange. Σημειωτέον ότι $[\operatorname{ord}(g) \mid |G|\,,\ \forall g \in G] \Longrightarrow \exp(G) = \text{εκπ}(\{\operatorname{ord}(g) | \, g \in G\}) \mid |G|$. (Βλ. το (i) τής προτάσεως 3.4.25 και την πρόταση 2.2.25.) □

5.1.28 Πόρισμα. *Εάν $(G,\cdot)$ είναι μια πεπερασμένη ομάδα, τότε*

$$\boxed{g^{|G|} = e_G, \quad \forall g \in G.} \tag{5.16}$$

Απόδειξη. Έστω τυχόν $g \in G$. Εάν $m := \operatorname{ord}(g)$, τότε $g^m = e_G$ και, σύμφωνα με το πόρισμα 5.1.27, η τάξη $\operatorname{ord}(g)$ τού g είναι διαιρέτης τής $|G|$, οπότε

$$g^{|G|} = g^{m\left(\frac{|G|}{m}\right)} = (g^m)^{\frac{|G|}{m}} = e_G^{\frac{|G|}{m}} = e_G,$$

και η (5.16) είναι αληθής. □

5.1.29 Πόρισμα. *Εάν $(G,\cdot)$ είναι μια πεπερασμένη κυκλική ομάδα, τότε ισχύει η ισότητα* $\exp(G) = |G|$.

Απόδειξη. Σύμφωνα με την πρόταση 3.4.7, $\exists x \in G$: $\operatorname{ord}(x) = |G|$, οπότε

$$\operatorname{ord}(x) = |G| \mid \text{εκπ}(\{\operatorname{ord}(g) | \, g \in G\}) = \exp(G) \Rightarrow |G| \leqslant \exp(G).$$

Από την άλλη μεριά, από την (5.16) και από τον ορισμό 3.4.24 τού εκθέτη λαμβάνουμε $\exp(G) \leqslant |G|$. Επομένως, $\exp(G) = |G|$. □

5.1.30 Πόρισμα (Θεώρημα τού Euler περί ισοτιμιών, 1760). *Έστω m ένας φυσικός αριθμός $\geqslant 2$ και έστω a ένας ακέραιος με* $\text{μκδ}(a,m) = 1$. *Τότε*

$$\boxed{a^{\phi(m)} \equiv 1 (\operatorname{mod} m),} \tag{5.17}$$

όπου ϕ η συνάρτηση φι τού Euler. (Βλ. 2.4.15 και 3.2.7 (iii)).

Απόδειξη. Θεωρούμε την πολλαπλασιαστική ομάδα $(\mathbb{Z}_m^\times, \cdot)$,

$$\mathbb{Z}_m^\times = \{[k]_m \in \mathbb{Z}_m \mid k \in \mathbb{N},\ \ k \leqslant m,\ \ \text{μκδ}\,(k,m) = 1\}\,,$$

η τάξη τής οποίας ισούται με $|\mathbb{Z}_m^\times| = \phi\,(m)$. Ας υποθέσουμε ότι ο a διαιρούμενος διά τού m αφήνει υπόλοιπο r. Προφανώς, $[a]_m = [r]_m$ με $r \in \{1, ..., m-1\}$ και $\text{μκδ}(r,m) = 1$. Από το πόρισμα 5.1.28 συνάγεται ότι

$$[r]_m \in \mathbb{Z}_m^\times \Rightarrow [a^{\phi(m)}]_m = ([a]_m)^{\phi(m)} = ([r]_m)^{\phi(m)} = [1]_m\,,$$

οπότε καταλήγουμε σε μια (ομαδοθεωρητική) απόδειξη τής (5.17). □

5.1.31 Πόρισμα («Μικρό» Θεώρημα τού Fermat, 1640). *Εάν ο p είναι ένας πρώτος αριθμός και ο a ένας ακέραιος, τέτοιος ώστε $p \nmid a$, τότε*[6]

$$\boxed{a^{p-1} \equiv 1 (\operatorname{mod} p).} \tag{5.18}$$

Απόδειξη. Άμεση από το πόρισμα 5.1.30 και το γεγονός ότι $\phi(p) = p - 1$. (Βλ. λήμμα 2.4.18.) □

[6] Από τη συνθήκη $p \nmid a$, έπεται, ιδιαιτέρως, ότι $a \neq 0$.

5.1.32 Πόρισμα. *Εάν p είναι ένας πρώτος αριθμός, τότε*

$$\boxed{a^p \equiv a (\mathrm{mod}\, p), \quad \forall a \in \mathbb{Z}.} \tag{5.19}$$

Απόδειξη. Έστω a τυχών ακέραιος αριθμός. Εάν $p \nmid a$, τότε η (5.19) έπεται άμεσα από την (5.18). Εάν $\exists l \in \mathbb{Z} : a = lp$, τότε

$$a^p - a = (lp)^p - lp = p(l^p p^{p-1} - l) \equiv 0 (\mathrm{mod}\, p) \Rightarrow a^p \equiv a (\mathrm{mod}\, p),$$

οπότε και σε αυτήν την περίπτωση η (5.19) είναι αληθής. □

5.1.33 Πόρισμα. *Εάν μια ομάδα $(G, \cdot)$ έχει ως τάξη της έναν πρώτο αριθμό p, τότε αυτή είναι κυκλική.*

Απόδειξη. Επειδή $p = |G| \geqslant 2$, υπάρχει κάποιο $g \in G$ με $g \neq e_G$. Συνεπώς, $\mathrm{ord}(g) \geqslant 2$ και $\mathrm{ord}(g) \,|p$ (δυνάμει τού πορίσματος 5.1.27). Και επειδή ο p είναι εξ υποθέσεως πρώτος, έχουμε $\mathrm{ord}(g) = p$. Αυτό όμως σημαίνει ότι η G είναι κυκλική δυνάμει τής προτάσεως 3.4.7. □

5.1.34 Πόρισμα. *Για οιαδήποτε μη τετριμμένη ομάδα $(G, \cdot)$ οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Εάν $H \sqsubseteq G$, τότε είτε $H = G$ είτε $H = \{e_G\}$.*

(ii) *$G = \langle g \rangle$ για κάθε $g \in G \setminus \{e_G\}$.*

(iii) *$|G| = p$, όπου p πρώτος αριθμός.*

Απόδειξη. (i)⇒(ii) Εάν ισχύει η συνθήκη (i) και $g \in G \setminus \{e_G\}$, τότε η κυκλική ομάδα $\langle g \rangle$ είναι μια μη τετριμμένη υποομάδα τής G, οπότε κατ' ανάγκην $G = \langle g \rangle$.

(ii)⇒(iii) Υποθέτουμε ότι $G = \langle g \rangle$ για κάθε $g \in G \setminus \{e_G\}$. Εάν η G είχε άπειρη τάξη, τότε $G = \langle x \rangle$, για κάποιο $x \in G$ με $x^2 \neq e_G$ (διότι αλλιώς θα ήταν πεπερασμένη, βλ. πρόταση 3.3.18). Άρα $G = \langle x^2 \rangle$. Εν τοιαύτη περιπτώσει, *κάθε* στοιχείο τής G θα ήταν ίσο με κάποια (ακεραία) δύναμη τού x^2 (βλ. πρόταση 3.3.18), οπότε και το ίδιο το στοιχείο x θα εγράφετο ως $x = (x^2)^k$, για κάποιον $k \in \mathbb{Z} \setminus \{0\}$. Τούτο όμως θα σήμαινε ότι

$$e_G = x^{2k-1} \Rightarrow \mathrm{ord}(x) < \infty,$$

κάτι που προδήλως θα αντέκειτο προς την υπόθεσή μας (και πάλι λόγω τής προτάσεως 3.3.18). Κατά συνέπειαν, η G είναι *πεπερασμένη* και *κυκλική* με $|G| > 1$. Κατά το πόρισμα 3.4.17, $\mathrm{card}(\{\text{γεννήτορες τής } G\}) = \phi(|G|)$, όπου ϕ η συνάρτηση φι τού Euler (βλ. 2.4.15). Εξ υποθέσεως, η G διαθέτει ακριβώς $|G| - 1$ γεννήτορες. Κατά συνέπειαν, $\phi(|G|) = |G| - 1$. Εάν η τάξη $|G|$ τής ομάδας G ήταν σύνθετος αριθμός, τότε θα εγράφετο ως γινόμενο $|G| = mn$, όπου $m, n \in \mathbb{N}$, $1 < m, n < |G|$, κι επειδή $\mu\kappa\delta(m, |G|) = m > 1$ και $\mu\kappa\delta(n, |G|) = n > 1$, θα είχαμε

$$\phi(|G|) = \mathrm{card}\,\{k \in \mathbb{N} \mid \ k \leqslant |G| \ \text{και}\ \mu\kappa\delta(k, |G|) = 1\} < |G| - 2.$$

Άτοπο! Άρα η τάξη $|G|$ τής G είναι όντως ένας πρώτος αριθμός.

(iii)⇒(i) Υποθέτουμε ότι $|G| = p$, όπου p πρώτος αριθμός. Έστω H τυχούσα υποομάδα τής G. Βάσει τού θεωρήματος 5.1.22 τού Lagrange, η τάξη $|H|$ τής H θα διαιρεί τον p. Επειδή ο p είναι πρώτος, *είτε* $|H| = 1$, οπότε η H είναι τετριμμένη, *είτε* $|H| = p$, οπότε $|H| = |G| \Rightarrow H = G$. □

5.1.35 Πόρισμα. *Εάν μια ομάδα δεν διαθέτει άλλες υποομάδες πέραν τής τετριμμένης και τού εαυτού της, τότε είναι είτε πεπερασμένη κυκλική έχουσα ως τάξη της έναν πρώτο αριθμό είτε τετριμμένη.*

5.1.36 Πόρισμα. *Κάθε πεπερασμένη ομάδα τάξεως* $\leqslant 5$ *είναι αβελιανή. Από την άλλη μεριά, η διεδρική ομάδα* $\mathbf{D}_3$ $(\cong \mathfrak{S}_3)$ *είναι μια μη αβελιανή ομάδα τάξεως* 6 (πρβλ. 4.1.2, 4.4.4).

Απόδειξη. Κάθε ομάδα τάξεως $1, 2, 3$ ή 5 είναι κυκλική και, ως εκ τούτου, αβελιανή (βλ. 3.5.27, 3.4.19, 5.1.33 και 3.3.17). Επίσης, σύμφωνα με το (i) τού θεωρήματος 4.5.6 κάθε ομάδα τάξεως 4 είναι αβελιανή. □

5.1.37 Θεώρημα (Ταξινόμηση ομάδων τάξεως 6). *Κάθε ομάδα τάξεως* 6 *είναι ισόμορφη είτε με την* $(\mathbb{Z}_6, +)$ *είτε με την* $(\mathbf{D}_3, \circ)$ *(που είναι ισόμορφη τής* $(\mathfrak{S}_3, \circ)$*).*

Απόδειξη. Έστω $(G, \cdot)$ μια ομάδα με ακριβώς 6 στοιχεία. Εξετάζουμε δύο ενδεχόμενα χωριστά:

Περίπτωση πρώτη. Εάν υπάρχει κάποιο στοιχείο τής G τάξεως 6, τότε έχουμε $(G, \cdot) \cong (\mathbb{Z}_6, +)$ (βλ. 3.4.7 και 3.5.26 (ii)).

Περίπτωση δεύτερη. Εάν οι τάξεις *όλων* των στοιχείων τής G είναι < 6, τότε έχουμε $(G, \cdot) \cong (\mathbf{D}_3, \circ)$. Πράγματι· σύμφωνα με το πόρισμα 5.1.27 κάθε στοιχείο διαφορετικό τού ουδετέρου οφείλει να έχει τάξη είτε 2 είτε 3. Εάν όλα τα $g \in G \smallsetminus \{e_G\}$ είχαν τάξη 2, τότε η G θα ήταν αβελιανή (βλ. 3.4.9 (iv)). Εν τοιαύτη περιπτώσει, για οιαδήποτε $a, b \in G \smallsetminus \{e_G\}$, $a \neq b$, το σύνολο $\{e_G, a, b, ab\}$ θα ήταν κλειστό ως προς την πράξη τής ομάδας G, οπότε (σύμφωνα με την πρόταση 3.2.19) θα αποτελούσε *υποομάδα* τής G τάξεως 4, πράγμα που θα μας οδηγούσε σε άτοπο λόγω τού θεωρήματος 5.1.22 τού Lagrange (καθότι $4 \nmid 6$). *Άρα η* G *διαθέτει κατ' ανάγκην κάποιο στοιχείο*, ας πούμε x, *τάξεως* 3. Έστω τυχόν στοιχείο $y \in G \smallsetminus \langle x \rangle$. Επειδή

$$y\langle x\rangle \neq \langle x\rangle \neq \langle x\rangle y$$

και $|G : \langle x\rangle| = 2$, έχουμε $G = \langle x\rangle \coprod y\langle x\rangle = \{e_G, x, x^2\} \coprod \{y, yx, yx^2\}$ και ταυτοχρόνως

$$G = \langle x\rangle \coprod \langle x\rangle y = \{e_G, x, x^2\} \coprod \{y, xy, x^2y\},$$

οπότε $y\langle x\rangle = \langle x\rangle y$. Επειδή οι $\langle x\rangle$ και $y\langle x\rangle$ είναι οι μόνες (ξένες) αριστερές πλευρικές κλάσεις τής $\langle x\rangle$ εντός τής G, για την $y^2\langle x\rangle$ ισχύει είτε $y^2\langle x\rangle = y\langle x\rangle$ είτε $y^2\langle x\rangle = \langle x\rangle$. Στην πρώτη περίπτωση, $y^2\langle x\rangle = y\langle x\rangle \Rightarrow y\langle x\rangle = \langle x\rangle$, ήτοι κάτι εξ υποθέσεως αποκλεισθέν. Στη δεύτερη περίπτωση, $y^2\langle x\rangle = \langle x\rangle$, οπότε

$$y^2 \in \langle x\rangle \underset{5.1.27}{\Longrightarrow} \operatorname{ord}(y^2) \mid |\langle x\rangle| \Rightarrow \text{ είτε } \operatorname{ord}(y^2) = 1 \text{ είτε } \operatorname{ord}(y^2) = 3.$$

Εάν ίσχυε $\operatorname{ord}(y^2) = \left|\left\langle y^2\right\rangle\right| = 3$, τότε θα είχαμε

$$\{e_G, y^2, y^4\} = \left\langle y^2\right\rangle = \langle x\rangle = \{e_G, x, x^2\},$$

οπότε είτε $[y^2 = x$ και $y^4 = x^2]$ είτε $[y^2 = x^2$ και $y^4 = x]$. Άρα τα στοιχεία τής G θα ήταν είτε τα

$$e_G,\ x = y^2,\ x^2 = y^4,\ y,\ yx = y^3,\ yx^2 = y^5$$

είτε τα $e_G,\ x = y^4,\ x^2 = y^2,\ y,\ yx = y^5,\ yx^2 = y^3$, κάτι που θα σήμαινε ότι $G = \langle y\rangle$ και $\operatorname{ord}(y) = 6$ (βλ. 3.4.7). Άτοπο! Κατ' ανάγκην, λοιπόν,

$$\operatorname{ord}(y^2) = 1 \Rightarrow y^2 = e_G \underset{y \neq e_G}{\Longrightarrow} \operatorname{ord}(y) = 2.$$

Ως εκ τούτου, *κάθε στοιχείο* $y \in G \smallsetminus \langle x \rangle$ *έχει τάξη* 2. Για οιοδήποτε $y \in G \smallsetminus \langle x \rangle$ έχουμε $xy \notin \langle x \rangle$, οπότε μέσω τού ανωτέρω επιχειρήματος (αλλά αυτήν τη φορά με το xy στη θέση τού y) συνάγεται ότι

$$\mathrm{ord}(xy) = 2 \Rightarrow xyxy = e_G \Rightarrow xy = y^{-1}x^{-1} = yx^{-1}.$$

Αυτές οι σχέσεις καθορίζουν πλήρως τον πολλαπλασιαστικό κατάλογο τής ομάδας G. Η G είναι μη αβελιανή (αφού[7] $xy \neq yx$) και

$$\left.\begin{array}{r} \langle x \rangle \sqsubset \langle x, y \rangle \sqsubseteq G \Rightarrow 3 = |\langle x \rangle| < |\langle x, y \rangle| \leqslant |G| = 6 \\ \text{5.1.22} \Longrightarrow |\langle x \rangle| \mid |\langle x, y \rangle| \Rightarrow |\langle x, y \rangle| = 6 \end{array}\right\} \Rightarrow G = \langle x, y \rangle .$$

Εφαρμόζοντας την πρόταση 4.4.7 (ή ελέγχοντας απευθείας ότι η απεικόνιση

$$G \ni y^j x^k \longmapsto \alpha^j \circ \beta^k \in \mathbf{D}_3, \quad j \in \{0, 1\},\ k \in \{0, 1, 2\},$$

είναι ισομορφισμός) συμπεραίνουμε ότι $(G, \cdot) \cong (\mathbf{D}_3, \circ)$. □

5.1.38 Θεώρημα (Ταξινόμηση ομάδων τάξεως $\leqslant 7$). *Η ταξινόμηση των ομάδων G με $|G| \leqslant 7$ μέχρις ισομορφισμού είναι αυτή που καταχωρίζεται στον ακόλουθο κατάλογο*:

τάξη	G
1	τετριμμένη
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4$, $\mathbf{V}$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6$, $\mathbf{D}_3$ ($\cong \mathfrak{S}_3$)
7	$\mathbb{Z}_7$

Απόδειξη. Αυτή έπεται ύστερα από συνδυασμό τού (ii) τού θεωρήματος 3.5.26, τού θεωρήματος 3.4.19, τού θεωρήματος 4.5.6, τού πορίσματος 5.1.33 και τού θεωρήματος 5.1.37. □

5.1.39 Θεώρημα. *Κάθε μη αβελιανή ομάδα τάξεως 8 είναι ισόμορφη είτε με την $(\mathbf{Q}, \cdot)$ είτε με την $(\mathbf{D}_4, \circ)$.*

Απόδειξη. Έστω $(G, \cdot)$ μια μη αβελιανή ομάδα τάξεως 8 και έστω $g \in G$. Από το πόρισμα 5.1.27 έπεται ότι $\mathrm{ord}(g) = |\langle g \rangle| \in \{1, 2, 4, 8\}$. Το ενδεχόμενο να ισχύει $\mathrm{ord}(g) = 8$ αποκλείεται (διότι τότε η $G = \langle g \rangle$, ως κυκλική, θα ήταν αβελιανή, βλ. προτάσεις 3.4.7 και 3.3.17). Άρα οι τάξεις *όλων* των στοιχείων τής G είναι $\leqslant 4$. Από την άλλη μεριά, αποκλείεται ωσαύτως το να έχουν *όλα* τα στοιχεία τής G τάξεις $\leqslant 2$ (διότι εν τοιαύτη περιπτώσει η G θα ήταν αβελιανή επί τη βάσει τού (iv) τής προτάσεως 3.4.9). Επομένως υπάρχει τουλάχιστον ένα στοιχείο, ας πούμε το x, τής G με $\mathrm{ord}(x) = 4$. Κατά το θεώρημα 5.1.22 τού Lagrange ο δείκτης τής κυκλικής ομάδας $\langle x \rangle = \{e_G, x, x^2, x^3\}$ εντός τής G είναι ίσος με 2. Επιλέγουμε τυχόν στοιχείο $y \in G \smallsetminus \langle x \rangle$. Προφανώς,

$$G = \langle x \rangle \coprod \langle x \rangle y = \{e_G, x, x^2, x^3\} \coprod \{y, xy, x^2y, x^3y\},$$

[7] Εάν ίσχυε η ισότητα $xy = yx$, τότε θα είχαμε $yx = yx^{-1} \Rightarrow x = x^{-1} \Rightarrow x^2 = e_G$, κάτι που θα σήμαινε ότι $\mathrm{ord}(x) < 3$.

και -ταυτοχρόνως- $G = \langle x\rangle \coprod y\langle x\rangle = \{e_G, x, x^2, x^3\} \coprod \{y, yx, yx^2, yx^3\}$, οπότε $y\langle x\rangle = \langle x\rangle y$. Ιδιαιτέρως, $yx \in \langle x\rangle y \Rightarrow yxy^{-1} \in \langle x\rangle = \{e_G, x, x^2, x^3\}$ με $\mathrm{ord}(yxy^{-1}) = \mathrm{ord}(x) = 4$ (βλ. 3.4.9 (ii)). Επειδή $\mathrm{ord}(e_G) = 1$, $\mathrm{ord}(x^2) = 2$ και $\mathrm{ord}(x^3) = 4$ (βλ. 3.4.10 (i)), συμπεραίνουμε ότι $yxy^{-1} \in \{x, x^3\}$. Το ενδεχόμενο να ισχύει $yxy^{-1} = x$ (ή, ισοδυνάμως, $xy = yx$) αποκλείεται (διότι αλλιώς θα είχαμε $x^iy^j = y^jx^i$ για οιουσδήποτε $i, j \in \mathbb{Z}$ και η G θα ήταν αβελιανή). Κατά συνέπειαν,

$$yxy^{-1} = x^3 = x^{-1} \Rightarrow yx^{-1}y^{-1} = (yxy^{-1})^{-1} = x \Rightarrow xy = yx^{-1}.$$

Επειδή οι $\langle x\rangle$ και $y\langle x\rangle$ είναι οι μόνες (ξένες) πλευρικές κλάσεις τής $\langle x\rangle$ εντός τής G, για την πλευρική κλάση $y^2\langle x\rangle$ έχουμε είτε $y^2\langle x\rangle = y\langle x\rangle$ είτε $y^2\langle x\rangle = \langle x\rangle$. Στην πρώτη περίπτωση, $y^2\langle x\rangle = y\langle x\rangle \Rightarrow y\langle x\rangle = \langle x\rangle$, ήτοι κάτι εξ υποθέσεως αποκλεισθέν. Στη δεύτερη περίπτωση, $y^2\langle x\rangle = \langle x\rangle$, οπότε

$$\left.\begin{array}{r} y^2 \in \langle x\rangle = \{e_G, x, x^2, x^3\} \\ \mathrm{ord}(y) \in \{2,4\} \underset{\text{3.4.10 (i)}}{\Longrightarrow} \mathrm{ord}(y^2) \in \{1,2\} \end{array}\right\} \Rightarrow y^2 \in \{e_G, x^2\}.$$

Επιπροσθέτως,

$$\left.\begin{array}{r} \langle x\rangle \sqsubset \langle x, y\rangle \sqsubseteq G \Rightarrow 4 = |\langle x\rangle| < |\langle x, y\rangle| \leqslant |G| = 8 \\ \text{5.1.22} \Longrightarrow |\langle x\rangle| \mid |\langle x, y\rangle| \Rightarrow |\langle x, y\rangle| = 8 \end{array}\right\} \Rightarrow G = \langle x, y\rangle.$$

Εν κατακλείδι, υπάρχουν μόνον δύο ενδεχόμενα:

(i) $G = \langle x, y\rangle$, *όπου* $y^2 = e_G$ *και* $xy = yx^{-1}$. Εφαρμόζοντας την πρόταση 4.4.7 (ή ελέγχοντας απευθείας ότι η απεικόνιση

$$G \ni y^jx^k \longmapsto \alpha^j \circ \beta^k \in \mathbf{D}_4, \quad j \in \{0,1\},\ k \in \{0,1,2,3\},$$

είναι ισομορφισμός) συνάγεται ότι $(G, \cdot) \cong (\mathbf{D}_4, \circ)$.

(ii) $G = \langle x, y\rangle$, *όπου* $y^2 = x^2$ *και* $xy = yx^{-1} = yx^3$. Λαμβάνοντας υπ' όψιν τον πολλαπλασιαστικό κατάλογο τόσον τής ομάδας G

$\cdot$	e_G	x	x^2	x^3	y	yx	yx^2	yx^3
e_G	e_G	x	x^2	x^3	y	yx	yx^2	yx^3
x	x	x^2	x^3	e_G	yx^3	y	yx	yx^2
x^2	x^2	x^3	e_G	x	yx^2	yx^3	y	yx
x^3	x^3	e_G	x	x^2	yx	yx^2	yx^3	y
y	y	yx	yx^2	yx^3	x^2	x^3	e_G	x
yx	yx	yx^2	yx^3	y	x	x^2	x^3	e_G
yx^2	yx^2	yx^3	y	yx	e_G	x	x^2	x^3
yx^3	yx^3	y	yx	yx^2	x^3	e_G	x	x^2

όσον και τής ομάδας των τετρανίων (βλ. 3.3.11) παρατηρούμε ότι η απεικόνιση[8]

$$G \ni y^\mu x^\nu \longmapsto \mathbf{k}^\mu\mathbf{i}^\nu = \mathbf{k}^\mu(\mathbf{jk})^\nu \in \mathbf{Q}, \quad \mu \in \{0,1\},\ \nu \in \{0,1,2,3\},$$

είναι ισομορφισμός, οπότε $(G, \cdot) \cong (\mathbf{Q}, \cdot)$. □

5.1.40 Παρατήρηση. Η $\mathbf{Q}$ διαθέτει μόνον ένα στοιχείο τάξεως 2 (συγκεκριμένα, το $-\mathbf{I}_2$), ενώ η $\mathbf{D}_4 = \langle \alpha, \beta\rangle$ (βλ. 4.4.4) έχει εν συνόλω πέντε στοιχεία τάξεως 2 (συγκεκριμένα, τα $\beta^2, \alpha, \alpha\circ\beta, \alpha\circ\beta^2, \alpha\circ\beta^3$). Άρα $\mathbf{D}_4 \ncong \mathbf{Q}$ (βλ. 3.5.22 (iv)).

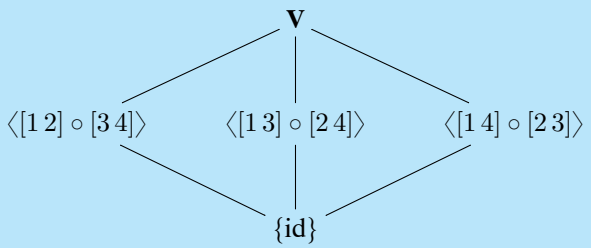
[8] Σημειωτέον ότι $\mathbf{i}^0 = \mathbf{I}_2$, $\mathbf{i}^1 = \mathbf{i}$, $\mathbf{i}^2 = -\mathbf{I}_2$, $\mathbf{i}^3 = -\mathbf{i}$, $\mathbf{ki}^0 = \mathbf{k}$, $\mathbf{ki} = \mathbf{j}$, $\mathbf{ki}^2 = -\mathbf{k}$, $\mathbf{ki}^3 = -\mathbf{j}$.

‣ **Εφαρμογές τού θεωρήματος τού Lagrange κατά τον προσδιορισμό υποομάδων.** Δοθείσας μιας πεπερασμένης ομάδας G *σχετικώς μικρής τάξεως* $m := |G|$, το θεώρημα 5.1.22 τού Lagrange περιορίζει την αναζήτηση των τάξεων των πιθανών υποομάδων τής G στους διαιρέτες τού m, διευκολύνοντάς μας, ως εκ τούτου, κατά την πορεία που οφείλουμε να ακολουθήσουμε για την εύρεση αυτών των υποομάδων. Επειδή το πρόβλημα τού προσδιορισμού των υποομάδων οιασδήποτε πεπερασμένης *κυκλικής ομάδας* έχει επιλυθεί (σε πλήρη γενικότητα) μέσω τού πορίσματος 3.5.29, θα επικεντρωθούμε εν πρώτοις στον προσδιορισμό των υποομάδων (και στον σχεδιασμό των διαγραμμάτων τού Hasse για τον αντίστοιχο σύνδεσμο) τής $\mathbf{V}$ (τής μοναδικής -μέχρις ισομορφισμού- μη κυκλικής ομάδας τάξεως 4), τής $\mathfrak{S}_3$ (τής μοναδικής -μέχρις ισομορφισμού- μη αβελιανής ομάδας τάξεως 6) και των (μοναδικών -μέχρις ισομορφισμού- μη αβελιανών) ομάδων $\mathbf{Q}$ και $\mathbf{D}_4$ τάξεως 8.

5.1.41 Εφαρμογή. *Το σύνολο των υποομάδων τής ομάδας* $\mathbf{V}$ *των τεσσάρων στοιχείων τού Klein (βλ.* 4.4.2 (ii)*) είναι το*

$$\boxed{\mathbf{Subg}(\mathbf{V}) = \{\{\mathrm{id}\}, \langle [1\,2]\circ[3\,4]\rangle, \langle [1\,3]\circ[2\,4]\rangle, \langle [1\,4]\circ[2\,3]\rangle, \mathbf{V}\}}$$

και το διάγραμμα τού Hasse για τον σύνδεσμο $(\mathbf{Subg}(\mathbf{V}), \sqsubseteq)$ *το*



Απόδειξη. Έστω H μια υποομάδα τής $\mathbf{V}$. Κατά το θεώρημα 5.1.22, $|H| \in \{1, 2, 4\}$. Εάν $|H| = 1$, τότε $H = \{\mathrm{id}\}$. Εάν $|H| = 4$, τότε $H = \mathbf{V}$. Εάν $|H| = 2$, τότε η H είναι κυκλική (βλ. 3.4.19). Επειδή

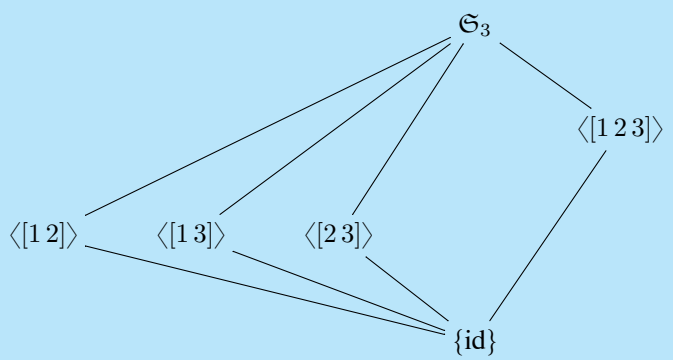
$$\mathrm{ord}([1\,2]\circ[3\,4]) = \mathrm{ord}([1\,3]\circ[2\,4]) = \mathrm{ord}([1\,4]\circ[2\,3]) = 2,$$

έχουμε κατ' ανάγκην $H \in \{\langle [1\,2]\circ[3\,4]\rangle, \langle [1\,3]\circ[2\,4]\rangle, \langle [1\,4]\circ[2\,3]\rangle\}$. □

5.1.42 Εφαρμογή. *Το σύνολο των υποομάδων τής ομάδας* $\mathfrak{S}_3$ $(\cong \mathbf{D}_3)$ *είναι το*

$$\boxed{\mathbf{Subg}(\mathfrak{S}_3) = \{\{\mathrm{id}\}, \langle [1\,2]\rangle, \langle [1\,3]\rangle, \langle [2\,3]\rangle, \langle [1\,2\,3]\rangle, \mathfrak{S}_3\}}$$

και το διάγραμμα τού Hasse για τον σύνδεσμο $(\mathbf{Subg}(\mathfrak{S}_3), \sqsubseteq)$ *το*



Απόδειξη. Έστω ότι $H \sqsubseteq \mathfrak{S}_3$. Κατά το θεώρημα 5.1.22, $|H| \in \{1,2,3,6\}$. Εάν $|H| = 1$, τότε $H = \{\mathrm{id}\}$. Εάν $|H| = 6$, τότε $H = \mathfrak{S}_3$. Εάν $|H| \in \{2,3\}$, τότε η H είναι κυκλική (βλ. 3.4.19). Επειδή

$$\mathrm{ord}([1\,2]) = \mathrm{ord}([1\,3]) = \mathrm{ord}([2\,3]) = 2,\ \mathrm{ord}([1\,2\,3]) = 3,$$

(βλ. 4.2.2) και $[1\,2\,3] = [1\,3\,2]^{-1}$, έχουμε $H \in \{\langle[1\,2]\rangle, \langle[1\,3]\rangle, \langle[2\,3]\rangle, \langle[1\,2\,3]\rangle\}$. □

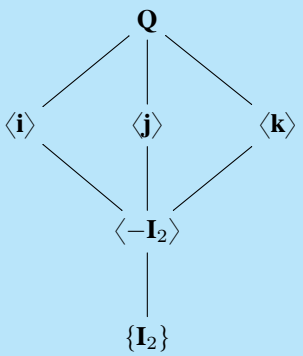
5.1.43 Εφαρμογή. *Το σύνολο των υποομάδων τής ομάδας*

$$\mathbf{Q} := \langle \mathbf{j}, \mathbf{k} \rangle$$

των τετρανίων (τής ορισθείσας στο εδάφιο 3.3.11) είναι το

$$\boxed{\mathbf{Subg}(\mathbf{Q}) = \{\{\mathbf{I}_2\}, \langle -\mathbf{I}_2\rangle, \langle \mathbf{i}\rangle, \langle \mathbf{j}\rangle, \langle \mathbf{k}\rangle, \mathbf{Q}\}}$$

και το διάγραμμα τού Hasse για τον σύνδεσμο $(\mathbf{Subg}(\mathbf{Q}), \sqsubseteq)$ *το*



Απόδειξη. Έστω H μια υποομάδα τής

$$\mathbf{Q} = \{\pm\mathbf{I}_2, \pm\mathbf{i} \pm \mathbf{j}, \pm\mathbf{k}\}.$$

Σύμφωνα με το θεώρημα 5.1.22, $|H| \in \{1,2,4,8\}$. Εάν $|H| = 1$, τότε $H = \{\mathbf{I}_2\}$. Εάν $|H| = 8$, τότε $H = \mathbf{Q}$. Απομένει να εξετάσουμε την περίπτωση κατά την οποία $|H| \in \{2,4\}$. Προς τούτο σχηματίζουμε τον κατάλογο

g	$\mathbf{I}_2$	$-\mathbf{I}_2$	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{j}$	$-\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$
g^{-1}	$\mathbf{I}_2$	$-\mathbf{I}_2$	$-\mathbf{i}$	$\mathbf{i}$	$-\mathbf{j}$	$\mathbf{j}$	$-\mathbf{k}$	$\mathbf{k}$
$\mathrm{ord}(g)$	1	2	4	4	4	4	4	4

στον οποίο καταχωρίζουμε τα 8 στοιχεία τής $\mathbf{Q}$ στην πρώτη του γραμμή, τα αντίστροφά τους στη δεύτερη και τις τάξεις τους στην τρίτη (πρβλ. 3.4.9 (i)). Εάν $|H| = 2$, τότε η H είναι κυκλική (βλ. 3.4.19), οπότε $H = \langle -\mathbf{I}_2\rangle$. Εάν $|H| = 4$, τότε η H είναι *είτε* κυκλική *είτε* αβελιανή, μη κυκλική και ισόμορφη με την ομάδα $\mathbf{V}$ των τεσσάρων στοιχείων τού Klein (βλ. θεώρημα 4.5.6). Επειδή η $\mathbf{V}$ περιέχει *τρία* στοιχεία τάξεως 2, συμπεραίνουμε ότι $H \not\cong \mathbf{V}$ (διότι η $\mathbf{Q}$ περιέχει *μόνον ένα* στοιχείο τάξεως 2, πρβλ. 3.5.22 (iv)). Άρα

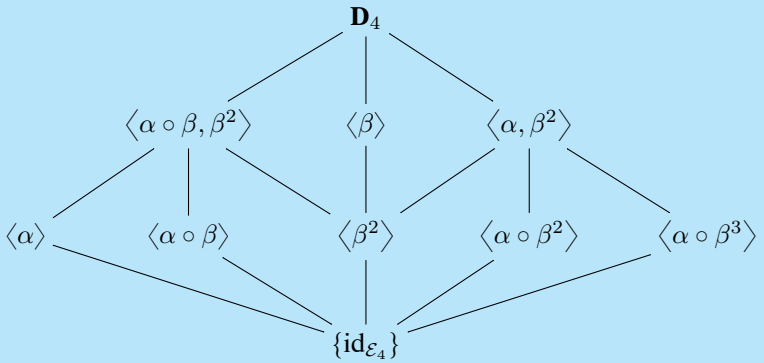
$$|H| = 4 \Rightarrow H \in \{\langle \mathbf{i}\rangle, \langle \mathbf{j}\rangle, \langle \mathbf{k}\rangle\},$$

αφού $\langle \mathbf{i}\rangle = \langle -\mathbf{i}\rangle, \langle \mathbf{j}\rangle = \langle -\mathbf{j}\rangle$ και $\langle \mathbf{k}\rangle = \langle -\mathbf{k}\rangle$. □

5.1.44 Εφαρμογή. *Το σύνολο των υποομάδων τής διεδρικής* $\mathbf{D}_4 := \langle \alpha, \beta \rangle$ *(τής ορισθείσας στο εδάφιο 4.4.4) είναι το*

$$\mathbf{Subg}(\mathbf{D}_4) = \left\{ \begin{array}{c} \{\mathrm{id}_{\mathcal{E}_4}\}, \langle\alpha\rangle, \langle\beta\rangle, \langle\beta^2\rangle, \langle\alpha\circ\beta\rangle, \langle\alpha\circ\beta^2\rangle, \\ \langle\alpha\circ\beta^3\rangle, \langle\alpha, \beta^2\rangle, \langle\alpha\circ\beta, \beta^2\rangle, \mathbf{D}_4 \end{array} \right\}$$

και το διάγραμμα τού Hasse για τον σύνδεσμο $(\mathbf{Subg}(\mathbf{D}_4), \sqsubseteq)$ *το*



Απόδειξη. Η $\mathbf{D}_4$ παράγεται από τις αμφιρρίψεις

$$\mathcal{E}_4 \ni z \overset{\alpha}{\longmapsto} \overline{z} \in \mathcal{E}_4, \quad \mathcal{E}_4 \ni z \overset{\beta}{\longmapsto} \zeta_4 z = iz \in \mathcal{E}_4,$$

τις υποκείμενες στις σχέσεις $\alpha^2 = \beta^4 = \mathrm{id}_{\mathcal{E}_4}$, $\beta\circ\alpha = \alpha\circ\beta^{-1}$ $\left(= \alpha\circ\beta^3\right)$, (βλ. 4.4.4), έχουσα ως πολλαπλασιαστικό της κατάλογο τον ακόλουθο:

$\circ$	$\mathrm{id}_{\mathcal{E}_4}$	β	β^2	β^3	α	$\alpha\circ\beta$	$\alpha\circ\beta^2$	$\alpha\circ\beta^3$
$\mathrm{id}_{\mathcal{E}_4}$	$\mathrm{id}_{\mathcal{E}_4}$	β	β^2	β^3	α	$\alpha\circ\beta$	$\alpha\circ\beta^2$	$\alpha\circ\beta^3$
β	β	β^2	β^3	$\mathrm{id}_{\mathcal{E}_4}$	$\alpha\circ\beta^3$	α	$\alpha\circ\beta$	$\alpha\circ\beta^2$
β^2	β^2	β^3	$\mathrm{id}_{\mathcal{E}_4}$	β	$\alpha\circ\beta^2$	$\alpha\circ\beta^3$	α	$\alpha\circ\beta$
β^3	β^3	$\mathrm{id}_{\mathcal{E}_4}$	β	β^2	$\alpha\circ\beta$	$\alpha\circ\beta^2$	$\alpha\circ\beta^3$	α
α	α	$\alpha\circ\beta$	$\alpha\circ\beta^2$	$\alpha\circ\beta^3$	$\mathrm{id}_{\mathcal{E}_4}$	β	β^2	β^3
$\alpha\circ\beta$	$\alpha\circ\beta$	$\alpha\circ\beta^2$	$\alpha\circ\beta^3$	α	β^3	$\mathrm{id}_{\mathcal{E}_4}$	β	β^2
$\alpha\circ\beta^2$	$\alpha\circ\beta^2$	$\alpha\circ\beta^3$	α	$\alpha\circ\beta$	β^2	β^3	$\mathrm{id}_{\mathcal{E}_4}$	β
$\alpha\circ\beta^3$	$\alpha\circ\beta^3$	α	$\alpha\circ\beta$	$\alpha\circ\beta^2$	β	β^2	β^3	$\mathrm{id}_{\mathcal{E}_4}$

Έστω H μια υποομάδα τής $\mathbf{D}_4$. Κατά το θεώρημα 5.1.22, $|H| \in \{1, 2, 4, 8\}$. Εάν $|H| = 1$, τότε $H = \{\mathrm{id}_{\mathcal{E}_4}\}$. Εάν $|H| = 8$, τότε $H = \mathbf{D}_4$. Απομένει να εξετάσουμε την περίπτωση κατά την οποία $|H| \in \{2, 4\}$. Προς τούτο σχηματίζουμε τον κατάλογο

g	$\mathrm{id}_{\mathcal{E}_4}$	β	β^2	β^3	α	$\alpha\circ\beta$	$\alpha\circ\beta^2$	$\alpha\circ\beta^3$
g^{-1}	$\mathrm{id}_{\mathcal{E}_4}$	β^3	β^2	β	α	$\alpha\circ\beta$	$\alpha\circ\beta^2$	$\alpha\circ\beta^3$
$\mathrm{ord}(g)$	1	4	2	4	2	2	2	2

στον οποίο καταχωρίζουμε τα 8 στοιχεία τής $\mathbf{D}_4$ στην πρώτη του γραμμή, τα αντίστροφά τους στη δεύτερη και τις τάξεις τους στην τρίτη (πρβλ. 3.4.9 (i)). Εάν $|H| = 2$, τότε η H είναι κυκλική (βλ. 3.4.19), οπότε

$$H \in \left\{\langle\alpha\rangle, \langle\beta^2\rangle, \langle\alpha\circ\beta\rangle, \langle\alpha\circ\beta^2\rangle, \langle\alpha\circ\beta^3\rangle\right\}.$$

Εάν $|H| = 4$, τότε η H είναι *είτε* κυκλική *είτε* αβελιανή, μη κυκλική και ισόμορφη με την ομάδα $\mathbf{V}$ των τεσσάρων στοιχείων τού Klein (βλ. θεώρημα 4.5.6). Εάν η H

είναι κυκλική, τότε (προφανώς) $H = \langle\beta\rangle = \langle\beta^3\rangle = \{\mathrm{id}_{\mathcal{E}_4}, \beta, \beta^2, \beta^3\}$. Εάν η H είναι αβελιανή μη κυκλική, τότε είναι τής μορφής $H = \{\mathrm{id}_{\mathcal{E}_4}, x, y, z\}$,

$$x \neq y,\ x \neq z,\ y \neq z,\ \{x, y, z\} \subsetneq \{\alpha, \beta^2, \alpha\circ\beta, \alpha\circ\beta^2, \alpha\circ\beta^3\},$$

με την επιπρόσθετη ιδιότητα $xy = z$. Ύστερα από $\binom{5}{3} = 10$ δοκιμές (για την εξεύρεση των τριάδων x, y, z που ικανοποιούν τα προαναφερθέντα) διαπιστώνουμε ότι το σύνολο $\{x, y, z\}$ ισούται με ένα εκ των ακολούθων:

$$\{\alpha, \beta^2, \alpha\circ\beta^2\},\ \{\beta^2, \alpha\circ\beta, \alpha\circ\beta^3\}.$$

Ως εκ τούτου, $H \in \left\{\langle\alpha, \beta^2\rangle, \langle\alpha\circ\beta, \beta^2\rangle\right\}$. □

5.1.45 Παρατήρηση. Κάθε *γνήσια* υποομάδα των ομάδων **V**, $\mathfrak{S}_3$ και **Q** είναι *κυκλική*. Αντιθέτως, η $\mathbf{D}_4$, πέραν των επτά κυκλικών, διαθέτει και δύο αβελιανές μη κυκλικές γνήσιες υποομάδες.

▸ **Το «αντίστροφο» τού θεωρήματος τού Lagrange δεν είναι πάντοτε ορθό.** Σύμφωνα με το θεώρημα 5.1.22 τού Lagrange, $|H| \mid |G|$, για οιαδήποτε υποομάδα H μιας πεπερασμένης ομάδας G. Ευλόγως τίθεται το ερώτημα τού κατά πόσον ισχύει και το *αντίστροφο*: Δοθείσας μιας πεπερασμένης ομάδας G τάξεως $m := |G|$ και δοθέντος ενός $k \in \mathbb{N}$ που διαιρεί τον m, υφίσταται πάντοτε μια υποομάδα H τής G με $k = |H|$; Παρότι τούτο είναι ορθό για τις πεπερασμένες κυκλικές ομάδες (βλ. 3.4.21 (i)) και, γενικότερα, για τις πεπερασμένες αβελιανές ομάδες (βλ. 5.4.22), για τις προηγουμένως εξετασθείσες (μη αβελιανές) ομάδες $\mathfrak{S}_3$, **Q** και $\mathbf{D}_4$, καθώς και για τις ομάδες τάξεως p^ν (p πρώτος, $\nu \in \mathbb{N}$), η απάντηση είναι *εν γένει αρνητική*. Η ομάδα με τη μικρότερη δυνατή τάξη, η οποία μπορεί, όπως θα δούμε στην πρόταση 5.1.47, να μας παράσχει *αντιπαράδειγμα*, είναι η εναλλάσσουσα ομάδα $\mathfrak{A}_4$ (με $|\mathfrak{A}_4| = 12$). Ωστόσο, θα πρέπει -εκ παραλλήλου- να τονισθεί ότι υπάρχουν θεωρήματα τα οποία είναι δυνατόν να ιδωθούν ως *μερικά αντίστροφα* τού θεωρήματος 5.1.22 τού Lagrange, καθότι διασφαλίζουν *την ύπαρξη υποομάδων* δοθείσας πεπερασμένης ομάδας G που έχουν ως τάξη τους κάποιους *ειδικής φύσεως διαιρέτες* τής τάξεως $|G|$ τής G. Η απόδειξη τής προτάσεως 5.1.47 στηρίζεται στο ακόλουθο:

5.1.46 Λήμμα. *Έστω H μια υποομάδα μιας ομάδας $(G, \cdot)$ με $|G : H| = 2$. Τότε*

$$g^2 \in H,\ \ \forall g \in G.$$

Απόδειξη. Επειδή $|G : H| = 2$, έχουμε $G = H \coprod aH$, για κάποιο $a \notin H$. Επομένως, $aH = G \setminus H$. Έστω τυχόν $g \in G$.

Περίπτωση πρώτη. Εάν $g \in H$, τότε $g^2 \in H$ (λόγω τής κλειστότητας τής πράξεως).

Περίπτωση δεύτερη. Εάν $g \in G \setminus H$, τότε $g = ah$, για κάποιο $h \in H$. Ας υποθέσουμε ότι $g^2 \notin H$. Τότε $g^2 = ah'$, για κάποιο $h' \in H$. Τούτο σημαίνει ότι

$$g = g^{-1}g^2 = h^{-1}a^{-1}ah' = h^{-1}h' \in H,$$

πράγμα που αντιφάσκει προς την αρχική υπόθεσή μας (ότι $g \in G \setminus H$). Άρα όντως (και σε αυτήν την περίπτωση) $g^2 \in H$. □

5.1.47 Πρόταση. *Η εναλλάσσουσα ομάδα $\mathfrak{A}_4$ δεν διαθέτει υποομάδες τάξεως 6.*

Απόδειξη. Ας υποθέσουμε ότι υπάρχει υποομάδα H τής $\mathfrak{A}_4$ τάξεως 6. Τότε από το θεώρημα 5.1.22 προκύπτει ότι $|\mathfrak{A}_4 : H| = \frac{12}{6} = 2$. Έστω $\sigma \in \mathfrak{A}_4$ *οιοσδήποτε* 3-κύκλος. Επειδή, κατά το (v) τής προτάσεως 4.2.3, ισχύει $\mathrm{ord}(\sigma) = 3$, έχουμε

$$\left.\begin{array}{r} \sigma = \sigma^3 \circ \sigma = \sigma^4 = (\sigma^2)^2 \\ \sigma^2 \in \mathfrak{A}_4 \underset{5.1.46}{\Longrightarrow} (\sigma^2)^2 \in H \end{array}\right\} \Longrightarrow \sigma \in H.$$

Κατά συνέπειαν, *όλοι* οι 3-κύκλοι που ανήκουν στην $\mathfrak{A}_4$ οφείλουν να ανήκουν στην H. Όμως εντός τής $\mathfrak{A}_4$ υπάρχουν ακριβώς 8 (σαφώς διακεκριμένοι) 3-κύκλοι (βλ. εδάφιο 4.3.11), ενώ $|H| = 6$. Άτοπο! Άρα η εναλλάσσουσα ομάδα $\mathfrak{A}_4$ δεν διαθέτει υποομάδες τάξεως 6. □

5.1.48 Σημείωση. Μια διαφορετική απόδειξη τής προτάσεως 5.1.47 (που δεν χρησιμοποιεί το λήμμα 5.1.46) είναι η εξής: Ας υποθέσουμε εκ νέου ότι υπάρχει υποομάδα H τής $\mathfrak{A}_4$ τάξεως 6. Τότε, σύμφωνα με το θεώρημα 5.1.37, η H είναι ισόμορφη είτε με την $(\mathbb{Z}_6, +)$ είτε με την $(\mathfrak{S}_3, \circ)$. Στην πρώτη περίπτωση θα υπάρχει κάποιος ισομορφισμός $f : \mathbb{Z}_6 \xrightarrow{\cong} H$ απεικονίζων το στοιχείο $[1]_6$ (τάξεως 6) στο στοιχείο $f([1]_6)$ (ωσαύτως τάξεως 6, βλ. 3.5.22 (iv)). Όμως τούτο είναι αδύνατο, καθόσον η $\mathfrak{A}_4$ δεν περιέχει κανένα στοιχείο τάξεως 6. Επομένως η H οφείλει να είναι ισόμορφη με την $\mathfrak{S}_3$. Σημειωτέον ότι η $\mathfrak{S}_3$ περιέχει ακριβώς τρία στοιχεία τάξεως 2, ήτοι τα $u_1 := [1\ 2], u_2 := [1\ 3]$ και $u_3 := [2\ 3]$. Από την άλλη μεριά, τα μόνα στοιχεία τής $\mathfrak{A}_4$ τάξεως 2 είναι τα $v_1 := [1\ 2] \circ [3\ 4],\ v_2 := [1\ 3] \circ [2\ 4],\ v_3 := [1\ 4] \circ [2\ 3]$. Κάθε ισομορφισμός $f : \mathfrak{S}_3 \xrightarrow{\cong} H$ απεικονίζει καθένα εκ των u_1, u_2, u_3 σε *ακριβώς ένα* εκ των v_1, v_2, v_3 (λόγω τού (iv) τής προτάσεως 3.5.22 και τής αμφιρριπτικότητας τής απεικονίσεως f). Συγκεκριμένα, $\exists \tau \in \mathfrak{S}_3 : f(u_j) = v_{\tau(j)},\ \forall j \in \{1, 2, 3\}$. Επειδή λοιπόν έχουμε αφ' ενός μεν

$$v_1 \circ v_2 = v_3 = v_2 \circ v_1,\ v_1 \circ v_3 = v_2 = v_3 \circ v_1,\ v_2 \circ v_3 = v_1 = v_3 \circ v_2,$$

αφ' ετέρου δε $u_1 \circ u_2 = [1\ 3\ 2] \neq [1\ 2\ 3] = u_2 \circ u_1$,

$$u_1 \circ u_3 = [1\ 2\ 3] \neq [1\ 3\ 2] = u_3 \circ u_1, \quad u_2 \circ u_3 = [1\ 3\ 2] \neq [1\ 2\ 3] = u_3 \circ u_2,$$

για οιαδήποτε $j, k \in \{1, 2, 3\}$ με $j \neq k$, συμπεραίνουμε ότι

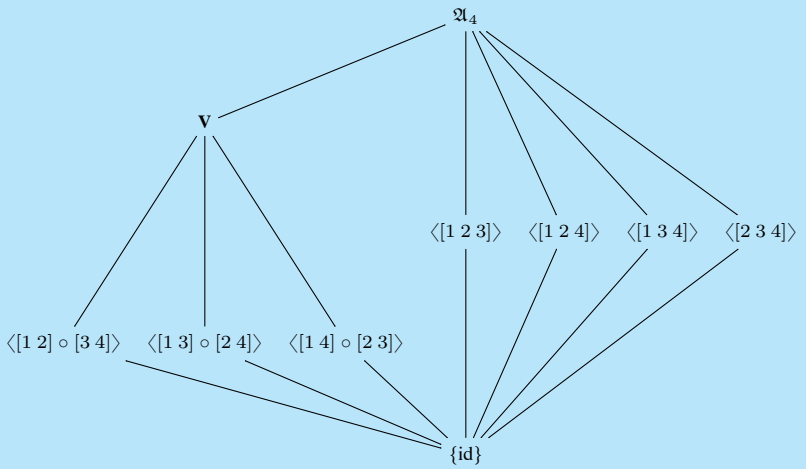
$$u_j \circ u_k \neq u_k \circ u_j \underset{f \text{ ένριψη}}{\Longrightarrow} f(u_j) \circ f(u_k) = f(u_j \circ u_k) \neq f(u_k \circ u_j) = f(u_k) \circ f(u_j),$$

όπου $f(u_j) \circ f(u_k) = v_{\tau(j)} \circ v_{\tau(k)} = v_{\tau(k)} \circ v_{\tau(j)} = f(u_k) \circ f(u_j)$. Άτοπο! Άρα η εναλλάσσουσα ομάδα $\mathfrak{A}_4$ δεν διαθέτει υποομάδες τάξεως 6.

5.1.49 Πόρισμα. *Το σύνολο των υποομάδων τής εναλλάσσουσας ομάδας $\mathfrak{A}_4$ είναι το*

$$\mathbf{Subg}(\mathfrak{A}_4) = \left\{ \begin{array}{l} \{\mathrm{id}\}, \langle [1\ 2] \circ [3\ 4] \rangle, \langle [1\ 3] \circ [2\ 4] \rangle, \langle [1\ 4] \circ [2\ 3] \rangle \\ \langle [1\ 2\ 3] \rangle,\ \langle [1\ 2\ 4] \rangle,\ \langle [1\ 3\ 4] \rangle,\ \langle [2\ 3\ 4] \rangle,\ \mathbf{V},\ \mathfrak{A}_4 \end{array} \right\}$$

και το διάγραμμα τού Hasse για τον σύνδεσμο $(\mathbf{Subg}(\mathfrak{A}_4), \sqsubseteq)$ είναι το ακόλουθο:



Απόδειξη. Έστω H μια υποομάδα τής $\mathfrak{A}_4$. Σύμφωνα με το θεώρημα 5.1.22 και την πρόταση 5.1.47 έχουμε $|H| \in \{1,2,3,4,12\}$. Εάν $|H| = 1$, τότε $H = \{\mathrm{id}\}$. Εάν $|H| = 12$, τότε $H = \mathfrak{A}_4$. Απομένει να εξετάσουμε την περίπτωση κατά την οποία έχουμε $|H| \in \{2,3,4\}$. Προς τούτο σχηματίζουμε τους καταλόγους

g	id	$[1\,2]\circ[3\,4]$	$[1\,3]\circ[2\,4]$	$[1\,4]\circ[2\,3]$
g^{-1}	id	$[1\,2]\circ[3\,4]$	$[1\,3]\circ[2\,4]$	$[1\,4]\circ[2\,3]$
$\mathrm{ord}(g)$	1	2	2	2

g	$[1\,2\,3]$	$[1\,2\,4]$	$[1\,3\,4]$	$[2\,3\,4]$	$[1\,3\,2]$	$[1\,4\,2]$	$[1\,4\,3]$	$[2\,4\,3]$
g^{-1}	$[1\,3\,2]$	$[1\,4\,2]$	$[1\,4\,3]$	$[2\,4\,3]$	$[1\,2\,3]$	$[1\,2\,4]$	$[1\,3\,4]$	$[2\,3\,4]$
$\mathrm{ord}(g)$	3	3	3	3	3	3	3	3

Εάν $|H| = 2$, τότε η H είναι κυκλική (βλ. 3.4.19), οπότε

$$H \in \{\langle[1\,2]\circ[3\,4]\rangle, \langle[1\,3]\circ[2\,4]\rangle, \langle[1\,4]\circ[2\,3]\rangle\}.$$

Εάν $|H| = 3$, τότε η H είναι κυκλική (βλ. 3.4.19), οπότε

$$H \in \{\langle[1\,2\,3]\rangle, \langle[1\,2\,4]\rangle, \langle[1\,3\,4]\rangle, \langle[2\,3\,4]\rangle\},$$

δεδομένου ότι

$$\langle[1\,2\,3]\rangle = \langle[1\,3\,2]\rangle, \quad \langle[1\,2\,4]\rangle = \langle[1\,4\,2]\rangle,$$
$$\langle[1\,3\,4]\rangle = \langle[1\,4\,3]\rangle, \quad \langle[2\,3\,4]\rangle = \langle[2\,4\,3]\rangle.$$

Τέλος, στην περίπτωση κατά την οποία $|H| = 4$, έχουμε κατ' ανάγκην[9] $H = \mathbf{V}$. □

▸ **Βασικές ιδιότητες υποομάδων πεπερασμένου δείκτη.** Το θεώρημα 5.1.20 γενικεύεται ως ακολούθως:

5.1.50 Θεώρημα. *Έστω $(G,\cdot)$ μια ομάδα. Εάν οι H και K είναι δυο υποομάδες της με $K \sqsubseteq H$, τότε*

$$\boxed{|G:K| = |G:H|\,|H:K|} \tag{5.20}$$

Ιδιαιτέρως, ισχύει η συνεπαγωγή: $K \sqsubset H \Longrightarrow |G:H| < |G:K|$.

Απόδειξη. Έστω A ένα σύστημα αριστερών εκπροσώπων *τής H εντός τής G* και έστω A′ ένα σύστημα αριστερών εκπροσώπων *τής K εντός τής H*. Τότε

$$\mathrm{card}(\mathrm{A}) = |G:H| \quad \text{και} \quad \mathrm{card}(\mathrm{A}') = |H:K|. \tag{5.21}$$

Θα αποδείξουμε ότι το $\mathrm{AA}' \subseteq G$ αποτελεί ένα σύστημα αριστερών εκπροσώπων *τής K εντός τής G*. Κατ' αρχάς,

$$G = \bigcup_{g\in\mathrm{A}} gH = \bigcup_{g\in\mathrm{A}} g\left(\bigcup_{h\in\mathrm{A}'} hK\right) = \bigcup_{g\in\mathrm{A},\,h\in\mathrm{A}'} (gh)\,K,$$

όπου η τελευταία ισότητα έπεται από το (i) τής προτάσεως 5.1.2. Η τελευταία ένωση είναι *αποσυνδετή*. Πράγματι· εάν $g_1, g_2 \in \mathrm{A}$ και $h_1, h_2 \in \mathrm{A}'$, τέτοια ώστε να ισχύει η ισότητα $(g_1h_1)\,K = (g_2h_2)\,K$, τότε

$$\left.\begin{aligned}(g_1h_1)\,KH &= (g_2h_2)\,KH\\ K\subseteq H &\Rightarrow KH = H\end{aligned}\right\} \Rightarrow \left.\begin{aligned}g_1h_1H &= g_2h_2H\\ h_j\in H &\Rightarrow h_jH = H, \forall j\in\{1,2\}\end{aligned}\right\} \Rightarrow g_1H = g_2H,$$

[9] Υπό την προϋπόθεση ότι $|H| = 4$, η H θα πρέπει να είναι ισόμορφη είτε με την $(\mathbb{Z}_4,+)$ με την είτε με την $(\mathbf{V},\circ)$ (βλ. θεώρημα 4.5.6). Το πρώτο ενδεχόμενο αποκλείεται, διότι μια υποομάδα τής $\mathfrak{A}_4$ είναι κυκλική εάν και μόνον εάν η τάξη της είναι ίση με 2 ή 3 (βάσει των προαναφερθέντων).

οπότε $g_1 = g_2$ (διότι το A είναι εξ υποθέσεως ένα σύστημα αριστερών εκπροσώπων τής H εντός τής G). Τούτο σημαίνει ότι το σύνολο AA' είναι όντως (εκ κατασκευής) ένα σύστημα αριστερών εκπροσώπων τής K εντός τής G. Άρα $\mathrm{card}(\mathrm{AA}') = |G : K|$. Εν συνεχεία, παρατηρούμε ότι για οιαδήποτε $g_1, g_2 \in \mathrm{A}$ και $h_1, h_2 \in \mathrm{A}'$, για τα οποία $g_1 h_1 = g_2 h_2$, ισχύουν οι συνεπαγωγές

$$g_1 h_1 = g_2 h_2 \Rightarrow (g_1 h_1)\, KH = (g_2 h_2)\, KH \Rightarrow g_1 = g_2 \Rightarrow h_1 = h_2,$$

όπου η πρώτη είναι προφανής, η δεύτερη απόρροια των όσων έχουμε ήδη προαναφέρει και η τρίτη έπεται από τον νόμο τής διαγραφής 3.2.9 (i). Από το γεγονός τού ότι τελικώς ισχύει $g_1 h_1 = g_2 h_2 \Rightarrow [g_1 = g_2 \quad \text{και} \quad h_1 = h_2]$ συμπεραίνουμε ότι

$$|G : K| = \mathrm{card}(\mathrm{AA}') = \mathrm{card}(\mathrm{A} \times \mathrm{A}') = \mathrm{card}(\mathrm{A}) \cdot \mathrm{card}(\mathrm{A}'). \tag{5.22}$$

Ο συνδυασμός των (5.21) και (5.22) δίδει την (5.20). □

5.1.51 Παρατήρηση. Η ισότητα (5.13) έπεται άμεσα από την (5.20) εάν ως K θεωρήσουμε την τετριμμένη υποομάδα τής G (βλ. 5.1.18 (i)).

5.1.52 Παράδειγμα. Λαμβάνοντας υπ' όψιν την τοποθέτηση των υποομάδων $\langle -\mathbf{I}_2 \rangle$ και $\langle \mathbf{i} \rangle$ τής ομάδας $\mathbf{Q} = \{\pm\mathbf{I}_2, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ των τετρανίων εντός τού διαγράμματος τού Hasse για τον σύνδεσμο $(\mathbf{Subg}(\mathbf{Q}), \sqsubseteq)$ (βλ. 3.3.11 και 5.1.43), η (5.20) είναι άμεσα επαληθεύσιμη, καθόσον $|\mathbf{Q} : \langle -\mathbf{I}_2 \rangle| = 4 = 2 \cdot 2 = |\mathbf{Q} : \langle \mathbf{i} \rangle|\, |\langle \mathbf{i} \rangle : \langle -\mathbf{I}_2 \rangle|$.

5.1.53 Ορισμός. Κάθε υποομάδα H μιας ομάδας $(G, \cdot)$ με $|G : H| < \infty$ καλείται **υποομάδα πεπερασμένου δείκτη** (εντός τής G).

5.1.54 Θεώρημα (H. Poincaré). *Εάν H και K είναι δυο υποομάδες μιας ομάδας $(G, \cdot)$, τότε ισχύουν τα ακόλουθα*:

(i) *Ο δείκτης τής $H \cap K$ εντός τής G έχει ως άνω φράγμα το γινόμενο των δεικτών των H και K*:

$$\boxed{|G : H \cap K| \leqslant |G : H|\, |G : K|.} \tag{5.23}$$

Ως εκ τούτου, εάν αμφότερες οι H και K είναι υποομάδες πεπερασμένου δείκτη, τότε και η $H \cap K$ είναι υποομάδα πεπερασμένου δείκτη.

(ii) *Εάν αμφότερες οι H και K είναι υποομάδες πεπερασμένου δείκτη, τότε ο δείκτης τής $H \cap K$ εντός τής G έχει ως κάτω φράγμα το ελάχιστο κοινό πολλαπλάσιο των δεικτών των H και K*:

$$\boxed{\text{εκπ}\,(|G : H|, |G : K|) \leqslant |G : H \cap K|} \tag{5.24}$$

και ισχύει, ιδιαιτέρως, η συνεπαγωγή

$$\text{μκδ}\,(|G : H|, |G : K|) = 1 \Longrightarrow |G : H \cap K| = |G : H|\, |G : K|.$$

Πρωτη αποδειξη του (i). Κατ' αρχάς, εάν $x, y \in G$, τότε το σύνολο $(xH) \cap (yK)$ είναι είτε το κενό σύνολο είτε μια αριστερή πλευρική κλάση τής $H \cap K$ εντός τής G. Πράγματι· εάν $g \in (xH) \cap (yK)$, τότε

$$g \in xH \text{ και } g \in yK \Rightarrow gH = xH \text{ και } gK = yK$$

(βλ. πρόταση 5.1.11). Από το (ii) τής προτάσεως 5.1.2 συνάγεται ότι

$$(xH) \cap (yK) = (gH) \cap (gK) = g(H \cap K).$$

Έστω A ένα σύστημα αριστερών εκπροσώπων *τής* H *εντός τής* G και έστω A′ ένα σύστημα αριστερών εκπροσώπων *τής* K *εντός τής* G. Επειδή

$$G = G \cap G = \left(\bigcup_{x \in \mathrm{A}} xH \right) \cap \left(\bigcup_{y \in \mathrm{A}'} yK \right) = \bigcup_{x \in \mathrm{A},\, y \in \mathrm{A}'} ((xH) \cap (yK)),$$

λαμβάνοντας υπ' όψιν ότι

$$\begin{aligned} \operatorname{card}\left(\left\{ (xH) \cap (yK) \,\middle|\, x \in \mathrm{A},\ y \in \mathrm{A}' \right\} \right) &= \operatorname{card}(\mathrm{A}) \cdot \operatorname{card}(\mathrm{A}') \\ &= |G : H|\, |G : K| \end{aligned}$$

και ότι (βάσει των προαναφερθέντων) κάθε σύνολο τής μορφής $(xH) \cap (yK)$ που είναι διάφορο τού κενού οφείλει να είναι μια αριστερή πλευρική κλάση τής $H \cap K$ εντός τής G, καταλήγουμε στην ανισοϊσότητα (5.23).

Δευτερη αποδειξη του (i). Εφαρμόζοντας το θεώρημα 5.1.50 (με την $H \cap K$ στη θέση τής εκεί παρατεθείσας K) λαμβάνουμε $|G : H \cap K| = |G : H|\, |H : H \cap K|$. Αρκεί λοιπόν να δειχθεί η ανισοϊσότητα $|H : H \cap K| \leqslant |G : K|$. Έστω A ένα σύστημα αριστερών εκπροσώπων *τής* $H \cap K$ *εντός τής* H και έστω A′ ένα σύστημα αριστερών εκπροσώπων *τής* K *εντός τής* G. Επειδή για οιαδήποτε $h_1, h_2 \in H$ ισχύουν οι αμφίπλευρες συνεπαγωγές

$$h_1 (H \cap K) = h_2 (H \cap K) \Leftrightarrow h_1^{-1} h_2 \in H \cap K \underset{h_1, h_2 \in H}{\Longleftrightarrow} h_1^{-1} h_2 \in K \Leftrightarrow h_1 K = h_2 K,$$

η $f : \{ h (H \cap K) \,|\, h \in \mathrm{A} \} \longrightarrow \left\{ gK \,\middle|\, g \in \mathrm{A}' \right\}$ με τύπο

$$f(h (H \cap K)) := hK$$

είναι μια καλώς ορισμένη *ενριπτική* απεικόνιση, πράγμα που σημαίνει ότι

$$|H : H \cap K| = \operatorname{card}(\mathrm{A}) \leqslant \operatorname{card}(\mathrm{A}') = |G : K|.$$

Αποδειξη του (ii). Θέτοντας $m := |G : H|$ και $n := |G : K|$, η (5.23) μας πληροφορεί ότι

$$|G : H \cap K| \leqslant mn < \infty. \tag{5.25}$$

Θέτοντας $k := |G : H \cap K|$, διπλή εφαρμογή τού θεωρήματος 5.1.50 μας δίδει[10]

$$[k = m \,|H : H \cap K| \Rightarrow m \mid k] \text{ και } [k = n \,|K : H \cap K| \Longrightarrow n \mid k].$$

Άρα εκπ$(m, n) \mid k$ (βλ. 2.2.25), οπότε εκπ$(m, n) \leqslant k$. Στην ειδική περίπτωση όπου μκδ$(m, n) = 1$ συμπεραίνουμε (μέσω τής προτάσεως 2.2.29) ότι εκπ$(m, n) = mn$, οπότε από τις (5.24) και (5.25) προκύπτει ότι $k = mn$. □

5.1.55 Πόρισμα. *Εάν* $H_1, \ldots, H_k$ *είναι υποομάδες μιας ομάδας* $(G, \cdot)$ *(όπου* k *κάποιος φυσικός αριθμός* $\geqslant 2$*), τότε*

$$|G : \bigcap_{j=1}^{k} H_j| \leqslant \prod_{j=1}^{k} |G : H_j|.$$

Ως εκ τούτου, εάν $H_1, \ldots, H_k$ *είναι υποομάδες πεπερασμένου δείκτη, τότε και η τομή* $\bigcap_{j=1}^{k} H_j$ *είναι υποομάδα πεπερασμένου δείκτη. Εν τοιαύτη περιπτώσει,*

$$\text{εκπ}\left(|G : H_1|, \ldots, |G : H_k| \right) \leqslant |G : \bigcap_{j=1}^{k} H_j|$$

[10] Από την υπόθεσή μας και από το θεώρημα 5.1.50 έπεται ότι $|H : H \cap K| < \infty$ και $|K : H \cap K| < \infty$.

και ισχύει, ιδιαιτέρως, η συνεπαγωγή:

$$\left[\begin{array}{c}\text{μκδ}\left(|G:H_i|,|G:H_j|\right)=1\\ \text{για οιουσδήποτε } i,j\in\{1,....k\},\ i\neq j\end{array}\right]\Longrightarrow |G:\bigcap_{j=1}^{k}H_j|=\prod_{j=1}^{k}|G:H_j|\,.$$

ΑΠΟΔΕΙΞΗ. Έπεται μέσω μαθηματικής επαγωγής ως προς το πλήθος k των υποομάδων, κατόπιν εφαρμογής τού θεωρήματος 5.1.54, τής προτάσεως 2.2.27 και τού πορίσματος 2.3.20. □

5.1.56 Πρόταση. *Εάν $(G,\cdot)$ είναι μια πεπερασμένως παραγόμενη ομάδα, τότε κάθε υποομάδα πεπερασμένου δείκτη (εντός τής G) είναι αφ' εαυτής πεπερασμένως παραγόμενη.*

ΑΠΟΔΕΙΞΗ. Έστω $\varnothing\neq X\subseteq G$ ένα πεπερασμένο σύνολο γεννητόρων τής G και έστω $H\sqsubseteq G$ με $|G:H|<\infty$. Επιλέγουμε ένα σύστημα δεξιών εκπροσώπων Δ τής H εντός τής G. (Προφανώς, $\text{card}(\Delta)=|G:H|$. Επίσης, δίχως βλάβη τής γενικότητας υποθέτουμε ότι $e_G\in\Delta$. Βλ. εδ. 5.1.15.) Θα δείξουμε ότι ο ισχυρισμός είναι αληθής αποδεικνύοντας ότι $H=\left\langle \Delta X\Delta^{-1}\cap H\right\rangle$, όπου $\Delta X\Delta^{-1}:=\left\{yxz^{-1}\middle|\, x\in X,\ y,z\in\Delta\right\}$. Προφανώς, $\left\langle \Delta X\Delta^{-1}\cap H\right\rangle\subseteq H$. Έστω τώρα τυχόν $h\in H$. Εξ υποθέσεως, το h γράφεται υπό τη μορφή $h=x_1^{\varepsilon_1}\cdots x_k^{\varepsilon_k}$, όπου $(x_1,..,x_k)\in X^k$ και $\varepsilon_j\in\{\pm1\}$ για κάθε $j\in\{1,..,k\}$, για κάποιον $k\in\mathbb{N}$. (Βλ. (3.8).) Επειδή $G=\coprod_{g\in\Delta}Hg$, υπάρχει κάποιο $g_1\in\Delta$, τέτοιο ώστε να ισχύει $x_1^{\varepsilon_1}\in Hg_1$. Άρα $\exists h_1\in H: x_1^{\varepsilon_1}=h_1g_1$. Ως εκ τούτου,

$$h_1=x_1^{\varepsilon_1}g_1^{-1}=\begin{cases}e_Gx_1g_1^{-1}, & \text{όταν } \varepsilon_1=1,\\ \left(g_1x_1e_G^{-1}\right)^{-1}, & \text{όταν } \varepsilon_1=-1.\end{cases}$$

Στην πρώτη περίπτωση, $h_1\in\Delta X\Delta^{-1}\cap H$. Στη δεύτερη περίπτωση, το h_1 ισούται με το αντίστροφο ενός στοιχείου τού $\Delta X\Delta^{-1}\cap H$, οπότε ανήκει στην υποομάδα την παραγόμενη από αυτό. Εάν $k\geqslant 2$, τότε συνεχίζουμε ως εξής: Προφανώς, υπάρχει κάποιο $g_2\in\Delta$, τέτοιο ώστε να ισχύει $g_1x_2^{\varepsilon_2}\in Hg_2$. Άρα $\exists h_2\in H: g_1x_2^{\varepsilon_2}=h_2g_2$. Ως εκ τούτου,

$$h_2=g_1x_2^{\varepsilon_2}g_2^{-1}=\begin{cases}g_1x_2g_2^{-1}, & \text{όταν } \varepsilon_2=1,\\ \left(g_2x_2g_1^{-1}\right)^{-1}, & \text{όταν } \varepsilon_2=-1.\end{cases}$$

Σε αμφότερες τις περιπτώσεις, $h_2\in\left\langle \Delta X\Delta^{-1}\cap H\right\rangle$. Επαναλαμβάνοντας την ίδια διαδικασία και για τους υπολοίπους δείκτες (όταν $k\geqslant 4$), ορίζουμε αναλόγως στοιχεία $h_3,...,h_{k-1}$ καταλήγουμε στις ισότητες

$$\begin{aligned}h&=x_1^{\varepsilon_1}\cdots x_k^{\varepsilon_k}=x_1^{\varepsilon_1}\left(g_1^{-1}g_1\right)x_2^{\varepsilon_2}\left(g_2^{-1}g_2\right)x_3^{\varepsilon_3}\cdots x_{k-1}^{\varepsilon_{k-1}}\left(g_{k-1}^{-1}g_{k-1}\right)x_k^{\varepsilon_k}\\ &=\left(x_1^{\varepsilon_1}\,g_1^{-1}\right)\left(g_1x_2^{\varepsilon_2}g_2^{-1}\right)\left(g_2x_3^{\varepsilon_3}g_3^{-1}\right)\cdots\left(g_{k-2}x_{k-1}^{\varepsilon_{k-1}}\,g_{k-1}^{-1}\right)g_{k-1}x_k^{\varepsilon_k}\\ &=h_1h_2\cdots h_{k-1}g_{k-1}x_k^{\varepsilon_k},\end{aligned}$$

όπου $h_j\in\left\langle \Delta X\Delta^{-1}\cap H\right\rangle,\forall j\in\{1,...,k-1\}$, και $g_{k-1}x_k^{\varepsilon_k}=(h_1\cdots h_{k-1})^{-1}h\in H$. Επειδή

$$g_{k-1}x_k^{\varepsilon_k}=\begin{cases}g_{k-1}x_ke_G^{-1}, & \text{όταν } \varepsilon_k=1,\\ \left(e_Gx_kg_{k-1}^{-1}\right)^{-1}, & \text{όταν } \varepsilon_k=-1,\end{cases}$$

έχουμε και εδώ $g_{k-1}x_k^{\varepsilon_k}\in\left\langle \Delta X\Delta^{-1}\cap H\right\rangle$. Τελικώς λοιπόν, $h\in\left\langle \Delta X\Delta^{-1}\cap H\right\rangle$ και ισχύει και ο αντίστροφος εγκλεισμός. □

‣ **Αντιστοίχιση πλευρικών κλάσεων και διατήρηση δεικτών.** Εάν η

$$f:(G,\cdot)\longrightarrow(H,*)$$

είναι ένας ομομορφισμός ομάδων, τότε, σύμφωνα με το 2ο θεώρημα αντιστοιχίσεως υποομάδων 3.5.20, ορίζεται η αμφίρριψη

$$\mathbf{Subg}(G;\mathrm{Ker}(f)) \ni K \overset{\bar{\Psi}_f}{\longmapsto} f(K) \in \mathbf{Subg}(\mathrm{Im}(f))$$

που καθορίζει έναν ισομορφισμό μεταξύ των αντιστοίχων συνδέσμων. Λόγω τής «ισοτονίας» τής $\bar{\Psi}_f$ έχουμε για οιεσδήποτε $K_1, K_2 \in \mathbf{Subg}(G;\,\mathrm{Ker}(f))$,

$$K_1 \sqsubseteq K_2 \Longleftrightarrow \bar{\Psi}_f\,(K_1) \sqsubseteq \bar{\Psi}_f\,(K_2)\,.$$

Φυσικό ερώτημα: Πώς σχετίζονται οι *δείκτες* $|K_2 : K_1|$ και $|\bar{\Psi}_f\,(K_2) : \bar{\Psi}_f\,(K_1)\,|$; Βάσει τής ακόλουθης προτάσεως, αυτοί οφείλουν να είναι ίσοι. Ως εκ τούτου, πέραν τής μερικής διατάξεως " $\sqsubseteq$ ", τού μεγίστου κάτω φράγματος $K_1 \cap K_2$ και τού ελαχίστου άνω φράγματος $\langle K_1, K_2\rangle$ των K_1 και K_2, η $\bar{\Psi}_f$ *διατηρεί και τους δείκτες*.

5.1.57 Πρόταση (Θεώρημα αντιστοιχίσεως πλευρικών κλάσεων).
Εάν η $f : (G,\cdot) \longrightarrow (H,*)$ *είναι ομομορφισμός ομάδων, τότε για οιεσδήποτε* $K_1, K_2 \in \mathbf{Subg}(G;\mathrm{Ker}(f))$ *με* $K_1 \sqsubseteq K_2$ *ισχύει η ισότητα*

$$|K_2 : K_1| = |\bar{\Psi}_f\,(K_2) : \bar{\Psi}_f\,(K_1)\,|\;(= |f\,(K_2) : f\,(K_1)\,|).$$

Απόδειξη. Έστω A ένα σύστημα αριστερών εκπροσώπων τής K_1 εντός τής K_2. Τότε $K_2 = \coprod\limits_{x\in \mathrm{A}} xK_1$ και $\mathrm{card}(\mathrm{A}) = |K_2 : K_1|$. Παρατηρούμε ότι

$$(\bar{\Psi}_f\,(K_2) =)\; f(K_2) = \bigcup_{x\in \mathrm{A}} f(x) * f(K_1). \tag{5.26}$$

Πράγματι· εάν $z \in f(K_2)$, τότε $\exists u \in K_2 : z = f(u)$. Το u γράφεται υπό τη μορφή $u = xy$, για κάποιο (μονοσημάντως ορισμένο) $x \in \mathrm{A}$ και κάποιο $y \in K_1$, οπότε

$$z = f(u) = f(xy) = f(x) * f(y) \in \bigcup_{x\in \mathrm{A}} f(x) * f(K_1) \Rightarrow f(K_2) \subseteq \bigcup_{x\in \mathrm{A}} f(x) * f(K_1).$$

Και αντιστρόφως· εάν $z \in \bigcup\limits_{x\in \mathrm{A}} f(x) * f(K_1)$, τότε

$$\exists x \in \mathrm{A} \;\text{ και }\; \exists y \in K_1 : z = f(x) * f(y) = f(xy).$$

Επειδή $K_1 \sqsubseteq K_2$, έχουμε $y \in K_2$, οπότε $xy \in K_2 \Rightarrow z \in f(K_2)$ και, ως εκ τούτου, ισχύει και ο αντίστροφος εγκλεισμός

$$\bigcup_{x\in\, \mathrm{A}} f(x) * f(K_1) \subseteq f(K_2).$$

Άρα η ισότητα (5.26) είναι αληθής. Θα αποδείξουμε ότι το $f(\mathrm{A}) = \{f(x)\,|x \in \mathrm{A}\}$ είναι ένα σύστημα αριστερών εκπροσώπων τής υποομάδας $\bar{\Psi}_f\,(K_1) = f(K_1)$ εντός τής $\bar{\Psi}_f\,(K_2) = f(K_2)$. Προς τούτο αρκεί να αποδειχθεί ότι η ένωση στο δεξιό μέλος τής (5.26) είναι *αποσυνδετή*. Ας υποθέσουμε τα $z, w \in f(\mathrm{A})$ είναι τέτοια, ώστε να ισχύει η ισότητα $z * f(K_1) = w * f(K_1)$. Τότε

$$\exists x_1, x_2 \in \mathrm{A} : f(x_1) = z, f(x_2) = w \Rightarrow f(K_1) \ni z^{-1} * w = f(x_1^{-1}) * f(x_2) = f(x_1^{-1}x_2),$$

απ' όπου έπεται ότι

$$x_1^{-1}x_2 \in f^{-1}(f(K_1)) = \bar{\Upsilon}_f\left(\bar{\Psi}_f\,(K_1)\right) = \mathrm{id}_{\mathbf{Subg}(G;\mathrm{Ker}(f))}(K_1) = K_1,$$

(όπου $\bar{\Upsilon}_f$ η αντίστροφος τής $\bar{\Psi}_f$, βλ. 3.5.20) και, κατ' επέκταση, ότι $x_1K_1 = x_2K_1$. Επειδή $x_1, x_2 \in \mathrm{A}$, έχουμε κατ' ανάγκην $x_1 = x_2$. Συνεπώς,

$$\mathrm{card}(f(\mathrm{A})) = |f\,(K_2) : f\,(K_1)\,|\;(= |\bar{\Psi}_f\,(K_2) : \bar{\Psi}_f\,(K_1)\,|).$$

Εν συνεχεία, ορίζουμε την επιρριπτική απεικόνιση

$$\mathfrak{y} : \{xK_1 \,|x \in \mathrm{A}\} \longrightarrow \{z * f(K_1) \,|z \in f(\mathrm{A})\}\,, \;\; \mathfrak{y}(xK_1) := f(x) * f(K_1), \forall x \in \mathrm{A}.$$

Αυτή είναι *και ενριπτική*, διότι για $z, w \in f(\mathrm{A})$ με $z * f(K_1) = w * f(K_1)$, υπάρχουν $x_1, x_2 \in \mathrm{A}$: $f(x_1) = z, f(x_2) = w$, τα οποία (όπως έχουμε ήδη προαναφέρει) οφείλουν να είναι ίσα. Η ισότητα $\mathrm{card}(\mathrm{A}) = \mathrm{card}(f(\mathrm{A}))$ έπεται άμεσα από την αμφιρριπτικότητα τής απεικονίσεως $\mathfrak{y}$. □

5.1.58 Πόρισμα. *Εάν η $f : (G, \cdot) \longrightarrow (H, *)$ είναι ένας ομομορφισμός ομάδων, τότε για οιεσδήποτε $L_1, L_2 \in$ **Subg**$(\mathrm{Im}(f))$ με $L_1 \sqsubseteq L_2$ ισχύει η ισότητα*

$$\boxed{|L_2 : L_1| = |\bar{\Upsilon}_f\,(L_2) : \bar{\Upsilon}_f\,(L_1)\,|\,(= |f^{-1}\,(L_2) : f^{-1}\,(L_1)\,|).}$$

Απόδειξη. Αρκεί κανείς να επαναλάβει κατά γράμμα την επιχειρηματολογία που χρησιμοποιήθηκε προηγουμένως στην απόδειξη τής προτάσεως 5.1.57 με την $\bar{\Upsilon}_f$ στη θέση τής $\bar{\Psi}_f$. □

5.2 ΟΡΘΟΘΕΤΕΣ ΥΠΟΟΜΑΔΕΣ

Μεταξύ των υποομάδων μιας ομάδας συγκαταλέγονται πάντοτε κάποιες οι οποίες είναι «ορθώς τιθέμενες» (= *ορθόθετες*), υπό την έννοια ότι κάθε αριστερή πλευρική τους κλάση είναι και δεξιά (ως προς το ίδιο στοιχείο αναφοράς τής ομάδας) και τανάπαλιν.

5.2.1 Πρόταση. *Έστω $(G, \cdot)$ μια ομάδα και έστω H μια υποομάδα της. Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Οι σχέσεις ισοδυναμίας "$\mathcal{R}_H$" και "${}_H\mathcal{R}$" οι οριζόμενες επί τού υποκειμένου συνόλου G τής δοθείσας ομάδας είναι ίσες.*

(ii) *Κάθε αριστερή πλευρική κλάση τής H εντός τής G είναι και δεξιά πλευρική κλάση της και τανάπαλιν.*

(iii) $gH = Hg,\ \forall g \in G.$

(iv) $gHg^{-1} = H,\ \forall g \in G$ (όπου $gHg^{-1} := \{g\}H\{g^{-1}\} = \{ghg^{-1}\,|h \in H\}$).

(v) $gHg^{-1} \subseteq H,\ \forall g \in G.$

(vi) *Αμφότερες οι "$\mathcal{R}_H$" και "${}_H\mathcal{R}$" είναι συμβατές με την πράξη "$\cdot$".* (Αυτό σημαίνει ότι για οιαδήποτε στοιχεία $g_1, g_2, g_1', g_2' \in G$ με $(g_1, g_2) \in \mathcal{R}_H$ και $(g_1', g_2') \in \mathcal{R}_H$ έχουμε $(g_1g_1', g_2g_2') \in \mathcal{R}_H$ (και παρομοίως για την "${}_H\mathcal{R}$").)

Απόδειξη. Οι συνεπαγωγές (i)⇔(iii)⇒(ii) και (iv)⇒(v) είναι προφανείς.

(ii)⇒(iii). Έστω gH τυχούσα αριστερή πλευρική κλάση τής H εντός τής G. Εξ υποθέσεως, $gH = Hg'$, για κάποιο $g' \in G$. Επειδή $g \in gH$ έχουμε $g \in Hg'$, οπότε $g(g')^{-1} \in H$ ή, ισοδυνάμως, $Hg' = Hg$ (βλ. 5.1.11). Άρα $gH = Hg,\ \forall g \in G$.

(iii)⇔(iv). Προφανώς, $gH = Hg \Leftrightarrow gHg^{-1} = Hgg^{-1} = He_G = H,\ \forall g \in G$.

(v)⇒(iv). Εξ υποθέσεως, $gHg^{-1} \subseteq H,\ \forall g \in G$. Κατά συνέπειαν, για το αντίστροφο g^{-1} *οιουδήποτε* στοιχείου $g \in G$, έχουμε $g^{-1}H\left(g^{-1}\right)^{-1} = g^{-1}Hg \subseteq H$. Για κάθε $g \in G$, ύστερα από «πολλαπλασιασμό» τού $g^{-1}Hg$ με το g εξ αριστερών και με το g^{-1} εκ δεξιών λαμβάνουμε $g\left(g^{-1}Hg\right)g^{-1} \subseteq gHg^{-1} \subseteq H$, οπότε

$$H = e_GHe_G = (gg^{-1})H(gg^{-1}) = g\left(g^{-1}Hg\right)g^{-1} \subseteq gHg^{-1},$$

απ' όπου έπεται ότι $gHg^{-1} = H,\ \forall g \in G$.

(v)⇒(vi). Ας υποθέσουμε ότι $g_1, g_2, g_1', g_2' \in G$ με $(g_1, g_2) \in \mathcal{R}_H$ και $(g_1', g_2') \in \mathcal{R}_H$. Τότε $g_1 g_2^{-1} \in H$ και $g_1' g_2'^{-1} \in H$, και (εξ υποθέσεως) $g_2(g_1' g_2'^{-1}) g_2^{-1} \in H$. Άρα

$$\left.\begin{array}{r} g_1 g_2^{-1} \in H \\ g_2(g_1' g_2'^{-1}) g_2^{-1} \in H \end{array}\right\} \Rightarrow \left(g_1 g_2^{-1}\right)\left(g_2(g_1' g_2'^{-1}) g_2^{-1}\right) = (g_1 g_1')(g_2'^{-1} g_2^{-1}) \in H,$$

οπότε $(g_1 g_1')(g_2'^{-1} g_2^{-1}) = (g_1 g_1')(g_2 g_2')^{-1} \in H \Rightarrow (g_1 g_1', g_2 g_2') \in \mathcal{R}_H$. Η απόδειξη τής συμβατότητας τής "$_H\mathcal{R}$" με την "$\cdot$" είναι παρόμοια.

(vi)⇒(v). Για κάθε $h \in H$ και κάθε $g \in G$ έχουμε

$$\left.\begin{array}{r} (g, g) \in \mathcal{R}_H \\ (h, e_G) \in \mathcal{R}_H \end{array}\right\} \Longrightarrow (gh, ge_G) \in \mathcal{R}_H \Rightarrow (gh, g) \in \mathcal{R}_H,$$

οπότε

$$\left.\begin{array}{r} (gh, g) \in \mathcal{R}_H \\ (g^{-1}, g^{-1}) \in \mathcal{R}_H \end{array}\right\} \Rightarrow \left(ghg^{-1}, gg^{-1}\right) \in \mathcal{R}_H \underset{\text{ορσ}}{\Longleftrightarrow} ghg^{-1}e_G^{-1}\ (= ghg^{-1}) \in H.$$

Άρα $gHg^{-1} \subseteq H$, $\forall g \in G$. (Τούτο αποδεικνύεται παρομοίως εάν εργασθούμε με την "$_H\mathcal{R}$" στη θέση τής "$\mathcal{R}_H$".) □

5.2.2 Ορισμός. Έστω $(G, \cdot)$ μια ομάδα. Μια υποομάδα H τής G ονομάζεται **ορθόθετη**[11] (σημειούμενη συνήθως ως[12] $H \trianglelefteq G$) όταν πληρούται μία (και, κατ' επέκταση, και οιαδήποτε άλλη) εκ των συνθηκών (i)-(vi) τής προτάσεως 5.2.1. (Όταν επιθυμούμε να δώσουμε *έμφαση* στο ότι μια υποομάδα H τής G είναι *γνήσια* ορθόθετη υποομάδα της, γράφουμε "$H \triangleleft G$".)

5.2.3 Παρατήρηση. Θα πρέπει να δοθεί ιδιαίτερη προσοχή στο ότι οι συνθήκες (iv) και (v) τής προτάσεως 5.2.1 είναι ισοδύναμες μόνον όταν ισχύουν *για κάθε* $g \in G$. Θεωρώντας, επί παραδείγματι, την υποομάδα

$$H := \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \middle| \, n \in \mathbb{Z} \right\}$$

τής ομάδας $G := \mathrm{GL}_2(\mathbb{Q})$ και το $g := \left(\begin{smallmatrix} 5 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in G$, διαπιστώνουμε ότι

$$g \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} g^{-1} = \begin{pmatrix} 1 & 5n \\ 0 & 1 \end{pmatrix} \in H, \ \forall n \in \mathbb{Z},$$

ήτοι ότι $gHg^{-1} \subsetneqq H$ (!) Εν προκειμένω, το *συγκεκριμένο στοιχείο* g ναι μεν ικανοποιεί την $gHg^{-1} \subseteq H$ αλλά *δεν ικανοποιεί* τη συνθήκη $gHg^{-1} = H$. (Κατόπιν τούτου συμπεραίνουμε ότι $H \ntriangleleft G$ -κάνοντας χρήση *τού συγκεκριμένου* g- *μόνον μέσω τής* (iv)!)

5.2.4 Παράδειγμα. Στο εδάφιο 5.1.19 έχουμε δείξει ότι η υποομάδα $\langle [1\,2] \rangle$ τής συμμετρικής ομάδας $\mathfrak{S}_3$ δεν είναι ορθόθετη. Κατ' αναλογίαν, $\langle [1\,3] \rangle \ntriangleleft \mathfrak{S}_3$ και $\langle [2\,3] \rangle \ntriangleleft \mathfrak{S}_3$. Εντούτοις, οι $\{\mathrm{id}\}$, $\langle [1\,2\,3] \rangle$ και $\mathfrak{S}_3$ *είναι* ορθόθετες υποομάδες τής $\mathfrak{S}_3$.

5.2.5 Πρόταση. *Η τετριμμένη υποομάδα μιας ομάδας G και η ίδια η G αποτελούν πάντοτε ορθόθετες υποομάδες τής G.*

Απόδειξη. Προφανώς, $G \trianglelefteq G$. Εξάλλου, $\forall g \in G$ έχουμε $ge_G = g = e_G g$, οπότε $\{e_G\} \trianglelefteq G$. □

[11] Στην ελληνική βιβλιογραφία συναντάται και ως *κανονική υποομάδα*. Η παρούσα αποστασιοποίηση από τη χρήση αυτού τού όρου σχετίζεται τόσο με την επιζήμια *πολυσημία* του όσο και με θέματα ετυμολογίας.

[12] Κατ' αντιστοιχίαν, ο συμβολισμός "$H \ntriangleleft G$" θα σημαίνει ότι η H *δεν είναι ορθόθετη υποομάδα* τής ομάδας G.

5.2.6 Πρόταση. *Κάθε υποομάδα μιας αβελιανής ομάδας είναι ορθόθετη.*

Απόδειξη. Έστω H μια υποομάδα μιας αβελιανής ομάδας $(G,\cdot)$. Τότε για κάθε στοιχείο $g \in G$ έχουμε $gHg^{-1} = \{ghg^{-1}\,|h \in H\} = \{gg^{-1}h\,|h \in H\} = H$, οπότε $H \trianglelefteq G$. □

5.2.7 Παραδείγματα. (i) Κάθε υποομάδα μιας κυκλικής ομάδας είναι ορθόθετη.
(ii) Κάθε υποομάδα τής ομάδας **V** των τεσσάρων στοιχείων τού Klein είναι ορθόθετη (βλ. 4.4.2 (ii) και 5.1.41).

5.2.8 Πρόταση. *Η τομή των μελών οιασδήποτε οικογενείας ορθόθετων υποομάδων $(H_j)_{j\in J}$ μιας ομάδας $(G,\cdot)$ αποτελεί μια ορθόθετη υποομάδα τής $(G,\cdot)$.*

Απόδειξη. Σύμφωνα με την πρόταση 3.2.23 η τομή $\bigcap\limits_{j\in J} H_j$ των μελών οιασδήποτε οικογενείας υποομάδων $(H_j)_{j\in J}$ μιας ομάδας $(G,\cdot)$ αποτελεί μια υποομάδα τής G. Εάν υποθέσουμε ότι $H_j \trianglelefteq G$ για κάθε $j \in J$ και εάν θεωρήσουμε τυχόντα στοιχεία $g \in G$ και $h \in \bigcap\limits_{j\in J} H_j$, τότε

$$[h \in H_j,\ \forall j \in J] \Rightarrow \left[ghg^{-1} \in H_j,\ \forall j \in J\right] \Rightarrow ghg^{-1} \in \bigcap_{j\in J} H_j.$$

Κατά συνέπειαν, $g(\bigcap\limits_{j\in J} H_j)g^{-1} \subseteq \bigcap\limits_{j\in J} H_j \Rightarrow \bigcap\limits_{j\in J} H_j \trianglelefteq G$. □

5.2.9 Πρόταση. *Εάν $(H_j)_{j\in J}$ είναι μια οικογένεια ορθόθετων υποομάδων μιας ομάδας $(G,\cdot)$, τότε $\langle\{H_j|\, j \in J\}\rangle \trianglelefteq G$.*

Απόδειξη. Έστω τυχόν $h \in \langle\{H_j|\, j \in J\}\rangle$. Σύμφωνα με το πόρισμα 3.3.6, το h γράφεται υπό τη μορφή $h = h_{j_1}h_{j_2}\cdots h_{j_k}$, όπου $h_{j_\rho} \in H_{j_\rho}$, $\forall \rho \in \{1,...,k\}$, $k \in \mathbb{N}$. Για οιοδήποτε $g \in G$ έχουμε $gh_{j_\rho}g^{-1} \in H_{j_\rho}$ (διότι -εξ υποθέσεως- $H_{j_\rho} \trianglelefteq G$) για κάθε $\rho \in \{1,...,k\}$. Θέτοντας $h'_{j_\rho} := gh_{j_\rho}g^{-1}$ παρατηρούμε ότι

$$ghg^{-1} = g(h_{j_1}h_{j_2}\cdots h_{j_k})g^{-1} = \prod_{\rho=1}^{k}\left(gh_{j_\rho}g^{-1}\right) = h'_{j_1}h'_{j_2}\cdots h'_{j_k},$$

απ' όπου έπεται ότι $ghg^{-1} \in \langle\{H_j|\, j \in J\}\rangle$. Επομένως, $\langle\{H_j|\, j \in J\}\rangle \trianglelefteq G$. □

5.2.10 Ορισμός. Για *οιοδήποτε υποσύνολο* X τού υποκειμένου συνόλου G μιας ομάδας $(G,\cdot)$, χαρακτηρίζουμε την τομή

$$\boxed{\mathrm{NCL}_G(X) := \bigcap \{K \in \mathbf{Subg}(G)\ |\ K \trianglelefteq G \text{ και } \ X \subseteq K\},} \qquad (5.27)$$

η οποία είναι η ελάχιστη ορθόθετη υποομάδα τής $(G,\cdot)$ που περιέχει το X, ως **την ορθόθετη θήκη τού** X **εντός τής** $(G,\cdot)$ (πρβλ. 3.3.1).

5.2.11 Πρόταση. *Έστω H μια υποομάδα μιας ομάδας $(G,\cdot)$. Τότε ισχύει η αμφίπλευρη συνεπαγωγή*

$$\mathrm{NCL}_G(H) = H \iff H \trianglelefteq G.$$

Απόδειξη. Επειδή $\mathrm{NCL}_G(H) \trianglelefteq G$, η συνεπαγωγή " $\Rightarrow$ " είναι προφανής. Εάν υποθέσουμε ότι $H \trianglelefteq G$, τότε έχουμε $\mathrm{NCL}_G(H) \trianglelefteq G$ από τον ορισμό (5.27), διότι η H είναι η ελάχιστη ορθόθετη υποομάδα τής G που περιέχει τον εαυτό της, οπότε η " $\Leftarrow$ " είναι ωσαύτως αληθής. □

5.2.12 Πρόταση. *Για οιοδήποτε μη κενό υποσύνολο X τού υποκειμένου συνόλου G μιας ομάδας $(G,\cdot)$ έχουμε*

$$\mathrm{NCL}_G(X) = \left\langle \left\{ gxg^{-1} \mid g \in G \ \text{ και } \ x \in X \right\} \right\rangle .$$

(Εάν $X = \varnothing$, τότε $\mathrm{NCL}_G(X) = \{e_G\}$.)

Απόδειξη. Έστω $H := \left\langle \left\{ gxg^{-1} \mid g \in G \ \text{ και } \ x \in X \right\} \right\rangle$ και έστω τυχόν $h \in H$. Τότε, σύμφωνα με την πρόταση 3.3.3, υπάρχουν $k \in \mathbb{N}$ και

$$(g_1, \ldots, g_k) \in G^k,\ (x_1, \ldots, x_k) \in X^k,\ (\varepsilon_1, \ldots, \varepsilon_k) \in \mathbb{Z}^k,$$

ούτως ώστε να ισχύει

$$h = \left(g_1 x_1 g_1^{-1}\right)^{\varepsilon_1} \cdots \left(g_k x_k g_k^{-1}\right)^{\varepsilon_k} = \left(g_1 x_1^{\varepsilon_1} g_1^{-1}\right) \cdots \left(g_k x_k^{\varepsilon_k} g_k^{-1}\right). \tag{5.28}$$

Για κάθε $g \in G$ έχουμε

$$ghg^{-1} = \left((gg_1)x_1^{\varepsilon_1}(gg_1)^{-1}\right)\left((gg_2)x_2^{\varepsilon_2}(gg_2)^{-1}\right) \cdots \left((gg_k)x_k^{\varepsilon_k}(gg_k)^{-1}\right) \in H,$$

οπότε $H \trianglelefteqslant G$. Επειδή $x = e_G x e_G^{-1} \in H$ για *κάθε* $x \in X$, λαμβάνουμε $X \subseteq H$. Αρκεί λοιπόν να αποδειχθεί ότι το H είναι η ελάχιστη ορθόθετη υποομάδα τής G που περιέχει το X. Προς τούτο υποθέτουμε ότι η B είναι οιαδήποτε ορθόθετη υποομάδα τής G, για την οποία ισχύει $X \subseteq B$. Τότε, για κάθε στοιχείο (5.28) τής H έχουμε για κάθε $j \in \{1, ..., k\}$, $x_j \in B$ και $\varepsilon_j \in \mathbb{Z} \Rightarrow x_j^{\varepsilon_j} \in B$, και

$$\left.\begin{array}{r} g_j \in G \\ x_j^{\varepsilon_j} \in B \trianglelefteqslant G \end{array}\right\} \Rightarrow g_j x_j^{\varepsilon_j} g_j^{-1} \in B,$$

οπότε $\left(g_1 x_1^{\varepsilon_1} g_1^{-1}\right) \cdots \left(g_k x_k^{\varepsilon_k} g_k^{-1}\right) \in B$. Εξ αυτού συνάγεται ότι $H \sqsubseteq B$, ήτοι ότι $\mathrm{NCL}_G(X) = H$. □

5.2.13 Πρόταση. *Έστω H μια υποομάδα μιας ομάδας $(G,\cdot)$. Εάν ο δείκτης τής H εντός τής G είναι $|G : H| = 2$, τότε $H \lhd G$.*

Απόδειξη. Εξ υποθέσεως,

$$\exists g_1 \in G \smallsetminus H : G = H \coprod g_1 H \ \text{ και } \ \exists g_2 \in G \smallsetminus H : G = H \coprod H g_2.$$

Αυτό σημαίνει ότι $g_1 H = H g_2 = G \smallsetminus H$. Έστω τώρα *τυχόν* στοιχείο $x \in G$. Αρκεί να αποδειχθεί ότι $xH = Hx$. Διακρίνουμε δύο περιπτώσεις:

Περίπτωση πρώτη. Εάν $x \in H$, τότε προφανώς $xH = H = Hx$.

Περίπτωση δεύτερη. Εάν $x \in G \smallsetminus H = g_1 H = H g_2$, τότε υπάρχουν $h_1, h_2 \in H$, τέτοια ώστε να ισχύει $x = g_1 h_1 = h_2 g_2$, οπότε

$$xH = (g_1 h_1)H = g_1 H = H g_2 = H(h_2 g_2) = Hx.$$

Επομένως, $H \lhd G$. □

5.2.14 Παράδειγμα. Έστω n ένας φυσικός αριθμός $\geqslant 2$. Επειδή, σύμφωνα με τις προτάσεις 4.1.3 και 4.3.9, $|\mathfrak{S}_n| = n!$ και $|\mathfrak{A}_n| = \frac{n!}{2}$, το θεώρημα 5.1.22 τού Lagrange μας πληροφορεί ότι $|\mathfrak{S}_n : \mathfrak{A}_n| = \frac{|\mathfrak{S}_n|}{|\mathfrak{A}_n|} = 2$. Άρα $\mathfrak{A}_n \lhd \mathfrak{S}_n$.

5.2.15 Παράδειγμα. Έστω n ένας φυσικός αριθμός $\geqslant 3$ και έστω $\mathbf{D}_n = \langle \alpha, \beta \rangle$ η n-οστή διεδρική ομάδα (βλ. 4.4.4). Η κυκλική ομάδα $\langle \beta \rangle$ έχει τάξη n, οπότε από το θεώρημα 5.1.22 τού Lagrange συνάγεται ότι $|\mathbf{D}_n : \langle \beta \rangle| = 2$. Άρα $\langle \beta \rangle \lhd \mathbf{D}_n$. Από την άλλη μεριά, η $\langle \alpha \rangle = \{\mathrm{id}_{\mathcal{E}_n}, \alpha\}$ δεν είναι ορθόθετη υποομάδα τής ομάδας $\mathbf{D}_n$, διότι $\beta \circ \alpha \circ \beta^{-1} = \alpha \circ \beta^{n-2} \notin \langle \alpha \rangle$. (Όπως θα δούμε στο εδάφιο 5.2.18, υπάρχουν και *μη αβελιανές* ομάδες, *κάθε* υποομάδα των οποίων είναι ορθόθετη.)

5.2.16 Λήμμα. *Έστω H μια υποομάδα μιας ομάδας $(G,\cdot)$ και έστω $g\in G$. Τότε το σύνολο gHg^{-1} αποτελεί μια υποομάδα τής G τάξεως $\left|gHg^{-1}\right| = |H|$.*

Απόδειξη. Επειδή $e_G\in H$, έχουμε $ge_Gg^{-1} = e_G \in gHg^{-1}$. Εν συνεχεία θεωρούμε τυχόντα στοιχεία gh_1g^{-1} και gh_2g^{-1} τού gHg^{-1}. Προφανώς,

$$\left(gh_1g^{-1}\right)\left(gh_2g^{-1}\right)^{-1} = \left(gh_1g^{-1}\right)\left(gh_2^{-1}g^{-1}\right) = g(\underbrace{h_1h_2^{-1}}_{\in H})g^{-1} \in gHg^{-1},$$

οπότε το gHg^{-1} είναι πράγματι μια υποομάδα τής G δυνάμει τού (iii) τής προτάσεως 3.2.16. Επιπροσθέτως, η απεικόνιση $H\ni h\longmapsto ghg^{-1}\in gHg^{-1}$ είναι αμφιρριπτική. Άρα $\left|gHg^{-1}\right| = |H|$. □

5.2.17 Πρόταση. *Έστω H μια πεπερασμένη υποομάδα μιας ομάδας $(G,\cdot)$ τάξεως $|H| = m\in\mathbb{N}$. Εάν η H είναι η μόνη υποομάδα τής $(G,\cdot)$ τάξεως m, τότε $H\trianglelefteq G$.*

Απόδειξη. Έστω τυχόν στοιχείο $g\in G$. Σύμφωνα με το λήμμα 5.2.16 το σύνολο gHg^{-1} αποτελεί μια υποομάδα τής G τάξεως $\left|gHg^{-1}\right| = |H| = m$. Εξ υποθέσεως, $gHg^{-1} = H \Rightarrow H\trianglelefteq G$. □

5.2.18 Παράδειγμα. Ως παράδειγμα μιας οικείας μας μη αβελιανής ομάδας, κάθε υποομάδα τής οποίας είναι ορθόθετη, αναφέρουμε την ομάδα $\mathbf{Q}$ των τετρανίων (βλ. 3.3.11 και 5.1.43). Οι υποομάδες της $\{\mathbf{I}_2\}$ και $\mathbf{Q}$ είναι ορθόθετες λόγω τής προτάσεως 5.2.5, οι υποομάδες $\langle\mathbf{i}\rangle, \langle\mathbf{j}\rangle$ και $\langle\mathbf{k}\rangle$ είναι ορθόθετες λόγω τής προτάσεως 5.2.13 (αφού ο δείκτης τους εντός τής $\mathbf{Q}$ ισούται με 2), και η υποομάδα $\langle-\mathbf{I}_2\rangle$ είναι ορθόθετη λόγω τής προτάσεως 5.2.17 (αφού η $\langle-\mathbf{I}_2\rangle$ είναι η μόνη υποομάδα τής $\mathbf{Q}$ τάξεως 2). Μια εναλλακτική απόδειξη για το ότι $\langle-\mathbf{I}_2\rangle\lhd\mathbf{Q}$ προκύπτει από το ότι

$$\langle-\mathbf{I}_2\rangle = \langle\mathbf{i}\rangle\cap\langle\mathbf{j}\rangle = \langle\mathbf{i}\rangle\cap\langle\mathbf{k}\rangle = \langle\mathbf{j}\rangle\cap\langle\mathbf{k}\rangle,$$

καθόσον οι $\langle\mathbf{i}\rangle, \langle\mathbf{j}\rangle$ και $\langle\mathbf{k}\rangle$ είναι ορθόθετες υποομάδες τής $\mathbf{Q}$ (βλ. 5.2.8).

5.2.19 Πρόταση. *Εάν H και K είναι δυο υποομάδες μιας ομάδας $(G,\cdot)$, τέτοιες ώστε $K\sqsubseteq H$ και $K\trianglelefteq G$, τότε $K\trianglelefteq H$.*

Απόδειξη. Θεωρούμε τυχόντα στοιχεία $x\in H$ και $y\in K$. Προφανώς,

$$x\in G,\ K\trianglelefteq G \Rightarrow xyx^{-1}\in K,$$

οπότε $xKx^{-1}\subseteq K \Rightarrow K\trianglelefteq H$. □

5.2.20 Παρατήρηση. Με τα δεδομένα τής προτάσεως 5.2.19 δεν μπορούμε να συμπεράνουμε ότι θα ισχύει κατ' ανάγκην $H\trianglelefteq G$. Επί παραδείγματι, θέτοντας $G := \mathfrak{S}_3$, $H := \langle[1\,2]\rangle = \{\mathrm{id},\ [1\,2]\}$ και $K := \{\mathrm{id}\}$ έχουμε $H\not\trianglelefteq G$ (βλ. 5.1.19).

5.2.21 Παράδειγμα. Η ομάδα $\mathbf{V}$ των τεσσάρων στοιχείων τού Klein (βλ. 4.4.2 (ii)) είναι ορθόθετη υποομάδα τής $\mathfrak{S}_4$. Πράγματι· για οιαδήποτε μετάταξη $\sigma\in\mathfrak{S}_4$ έχουμε (λόγω τού (vii) τής προτάσεως 4.2.3)

$$\begin{aligned}\sigma\circ([1\,2]\circ[3\,4])\circ\sigma^{-1} &= \left(\sigma\circ[1\,2]\circ\sigma^{-1}\right)\circ\left(\sigma\circ[3\,4]\circ\sigma^{-1}\right)\\ &= [\sigma(1)\,\sigma(2)]\circ[\sigma(3)\,\sigma(4)]\end{aligned}$$

και $\{\sigma(1),\sigma(2),\sigma(3),\sigma(4)\} = \{1,2,3,4\}$, οπότε $\sigma\circ([1\,2]\circ[3\,4])\circ\sigma^{-1}\in\mathbf{V}$. Κατ' αναλογίαν, $\sigma\circ([1\,3]\circ[2\,4])\circ\sigma^{-1}\in\mathbf{V}$ και $\sigma\circ([1\,4]\circ[2\,3])\circ\sigma^{-1}\in\mathbf{V}$. Άρα $\mathbf{V}\lhd\mathfrak{S}_4$. Επειδή $\mathbf{V}\sqsubset\mathfrak{A}_4\lhd\mathfrak{S}_4$ (βλ. 5.1.49 και 5.2.14), η πρόταση 5.2.19 μας πληροφορεί ότι $\mathbf{V}\lhd\mathfrak{A}_4$.

5.2.22 Πρόταση. *Εάν H και K είναι δυο υποομάδες μιας ομάδας $(G,\cdot)$, τότε ισχύει η συνεπαγωγή:* $K \trianglelefteq G \Longrightarrow K \cap H \trianglelefteq H$.

Απόδειξη. Έστω $h \in H$ και έστω $x \in K \cap H$. Τότε

$$\left.\begin{array}{r} x \in K \\ h \in H \Rightarrow h \in G \end{array}\right\} \underset{K\trianglelefteq G}{\Longrightarrow} hxh^{-1} \in K$$

και

$$\left.\begin{array}{r} h \in H,\ x \in H \underset{H\sqsubseteq G}{\Longrightarrow} hx \in H \\ h \in H \underset{H\sqsubseteq G}{\Longrightarrow} h^{-1} \in H \end{array}\right\} \underset{H\sqsubseteq G}{\Longrightarrow} hxh^{-1} \in H,$$

οπότε $hxh^{-1} \in K \cap H$ και, ως εκ τούτου, $K \cap H \trianglelefteq H$. □

5.2.23 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Υποθέτουμε ότι $H, K \in$ **Subg**(G). Εάν $H \cap K \trianglelefteq H$ και $H \cap K \trianglelefteq K$, τότε $H \cap K \trianglelefteq \langle H, K\rangle$.*

Απόδειξη. Έστω $g \in \langle H, K\rangle$. Σύμφωνα με το πόρισμα 3.3.6, το g γράφεται υπό τη μορφή $g = h_1k_1h_2k_2\cdots h_\nu k_\nu$, όπου $\nu \in \mathbb{N}$ και $h_i \in H$, $k_i \in K$ για κάθε $i \in \{1,..,\nu\}$. Άρα για κάθε $y \in H \cap K$ λαμβάνουμε

$$gyg^{-1} = h_1(k_1(\cdots(h_\nu(k_\nu y k_\nu^{-1})h_\nu^{-1})\cdots)k_1^{-1})h_1^{-1} \in H \cap K,$$

διότι $H \cap K \trianglelefteq H$ και $H \cap K \trianglelefteq K$. Επομένως, $H \cap K \trianglelefteq \langle H, K\rangle$. □

5.2.24 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Υποθέτουμε ότι $H, K \in$ **Subg**(G). Εάν τουλάχιστον μία εκ των H, K είναι ορθόθετη υποομάδα τής G, τότε $HK \sqsubseteq G$ και $HK = \langle H, K\rangle = KH$. Επιπροσθέτως, εάν $H \trianglelefteq G$ και $K \trianglelefteq G$, τότε $HK \trianglelefteq G$.*

Απόδειξη. Ας υποθέσουμε ότι $K \trianglelefteq G$. Προφανώς, $e_G \in HK$. Θεωρούμε τυχόντα στοιχεία $x_1, x_2 \in H$ και $y_1, y_2 \in K$. Επειδή

$$H \sqsubseteq G \Rightarrow x_1x_2^{-1} \in H,\ \ K \sqsubseteq G \Rightarrow y_1y_2^{-1} \in K,\ \ K \trianglelefteq G,$$

έχουμε $(x_1y_1)(x_2y_2)^{-1} = x_1y_1y_2^{-1}x_2^{-1} = \left(x_1x_2^{-1}\right)\left(x_2\left(y_1y_2^{-1}\right)x_2^{-1}\right) \in HK$, οπότε $HK \sqsubseteq G$ (βλ. 3.2.16 (iii)) και $HK = KH$ (βλ. πρόταση 5.1.4). (Παρομοίως αποδεικνύεται ότι $HK = KH \sqsubseteq G$ εάν $H \trianglelefteq G$.) Προφανώς, η υποομάδα $HK = KH$ τής G περιέχεται στην υποομάδα $\langle H, K\rangle$. Επειδή η $\langle H, K\rangle$ είναι η *ελάχιστη* υποομάδα τής G η οποία περιέχει την ένωση $H \cup K \subseteq HK$, ισχύει και ο αντίστροφος εγκλεισμός $\langle H, K\rangle \subseteq HK$, οπότε $HK = \langle H, K\rangle$. Εν συνεχεία, υποθέτοντας ότι *αμφότερες* οι H και K είναι ορθόθετες και θεωρώντας οιαδήποτε $x \in H$, $y \in K$ και $g \in G$ διαπιστώνουμε ότι

$$g(xy)g^{-1} = (\underbrace{gxg^{-1}}_{\in H})(\underbrace{gyg^{-1}}_{\in K}) \in HK,$$

απ' όπου συμπεραίνουμε ότι $HK \trianglelefteq G$. □

5.2.25 Συμβολισμός. Έστω $(G,\cdot)$ μια ομάδα. Ως

$$\boxed{\textbf{NSubg}(G) := \{H \in \textbf{Subg}(G) \mid H \trianglelefteq G\}}$$

συμβολίζουμε το σύνολο όλων των ορθόθετων υποομάδων της. Το $(\textbf{NSubg}(G), \sqsubseteq)$ αποτελεί ένα μερικώς διατεταγμένο σύνολο (ως προς τη μερική διάταξη "$\sqsubseteq$" -ή, ακριβέστερα, ως προς την "$\sqsubseteq|_{\textbf{NSubg}(G)\times\textbf{NSubg}(G)}$"- την επαγομένη επ' αυτού.) Επίσης, θέτουμε

$$\textbf{Min-NSubg}(G) := \textbf{Min-Subg}(G) \cap \textbf{NSubg}(G) \tag{5.29}$$

και

$$\textbf{Max-NSubg}(G) := \textbf{Max-Subg}(G) \cap \textbf{NSubg}(G) \tag{5.30}$$

καλώντας τά στοιχεία τού (5.29) (και αντιστοίχως, τού (5.30)) **ελαχιστικές** (και αντιστοίχως, **μεγιστικές**) **ορθόθετες υποομάδες τής** G. (Πρβλ. (3.4) και (3.5). Εν προκειμένω, θεωρούνται υποομάδες με την ιδιότητα ΙΔ «τού να είναι ορθόθετες».)

5.2.26 Πρόταση. *Το μερικώς διατεταγμένο σύνολο* $(\textbf{NSubg}(G), \sqsubseteq)$ *αποτελεί έναν υποσύνδεσμο τού συνδέσμου* $(\textbf{Subg}(G), \sqsubseteq)$. (Βλ. 1.4.25 και 3.2.30.)

Απόδειξη. Θεωρούμε τυχούσες $H, K \in \textbf{NSubg}(G)$. Από την πρόταση 5.2.8 λαμβάνουμε $H \wedge K = H \cap K \in \textbf{NSubg}(G)$. Εξάλλου, σύμφωνα με την πρόταση 5.2.24 έχουμε

$$H \vee K = \langle H, K\rangle = HK \trianglelefteqslant G \Rightarrow H \vee K \in \textbf{NSubg}(G).$$

Άρα το μερικώς διατεταγμένο σύνολο $(\textbf{NSubg}(G), \sqsubseteq)$ είναι όντως υποσύνδεσμος τού $(\textbf{Subg}(G), \sqsubseteq)$. □

5.2.27 Σημείωση (Η " $\trianglelefteqslant$ " δεν είναι μεταβατική επί τού Subg(G).). Εν αντιθέσει προς την " $\sqsubseteq$ ", η διμελής σχέση " $\trianglelefteqslant$ " *δεν είναι* μερική διάταξη επί τού συνόλου **Subg**(G) διότι ναι μεν είναι (προφανώς) αυτοπαθής και αντισυμμετρική αλλά *δεν είναι* μεταβατική: Εάν $K \trianglelefteqslant H$ και $H \trianglelefteqslant G$, τότε ενδέχεται να έχουμε $K \ntrianglelefteqslant G$. Επί παραδείγματι, θέτοντας $G := \mathfrak{A}_4$, $H := \mathbf{V}$ (την ομάδα των τεσσάρων στοιχείων τού Klein) και $K := \langle [1\,2] \circ [3\,4]\rangle$, γνωρίζουμε ότι ισχύει $K \lhd \mathbf{V}$ (επί τη βάσει τής προτάσεως 5.2.6) και $\mathbf{V} \lhd \mathfrak{A}_4$. (Βλ. παράδειγμα 5.2.21.) Μολαταύτα, χρησιμοποιώντας τόν 3-κύκλο $\sigma := [1\,2\,3] \in \mathfrak{A}_4$ συμπεραίνουμε ότι $K \ntrianglelefteqslant \mathfrak{A}_4$, καθόσον

$$\begin{aligned}\sigma \circ ([1\,2] \circ [3\,4]) \circ \sigma^{-1} &= \big(\sigma \circ [1\,2] \circ \sigma^{-1}\big) \circ \big(\sigma \circ [3\,4] \circ \sigma^{-1}\big)\\ &= [\sigma(1)\,\sigma(2)] \circ [\sigma(3)\,\sigma(4)] = [2\,3] \circ [1\,4] = [1\,4] \circ [2\,3] \notin K.\end{aligned}$$

5.2.28 Πρόταση. *Έστω* $(G, \cdot)$ *μια ομάδα. Η "*$\trianglelefteqslant$*" είναι μεταβατική (και, ως εκ τούτου, μερική διάταξη) επί τού συνόλου* **NSubg**(G)*. Επιπροσθέτως, το ζεύγος* $(\textbf{NSubg}(G), \trianglelefteqslant)$ *είναι σύνδεσμος. Μάλιστα, εν προκειμένω, για τυχούσες ομάδες* $H, K \in \textbf{NSubg}(G)$ *έχουμε*

$$H \wedge K = H \cap K, \quad H \vee K = \mathrm{NCL}_G(H, K) := \mathrm{NCL}_G(H \cup K).$$

Απόδειξη. Εάν $H_1, H_2, H_3 \in \textbf{NSubg}(G)$ με $H_1 \trianglelefteqslant H_2$ και $H_2 \trianglelefteqslant H_3$, τότε

$$\left.\begin{array}{r} H_1 \sqsubseteq H_2,\ H_2 \sqsubseteq H_3 \Rightarrow H_1 \sqsubseteq H_3 \\ H_1 \trianglelefteqslant G \end{array}\right\} \underset{5.2.19}{\Longrightarrow} H_1 \trianglelefteqslant H_3.$$

Οι λοιποί ισχυρισμοί είναι προδήλως αληθείς. □

5.2.29 Πόρισμα. *Έστω* $(G, \cdot)$ *μια ομάδα. Εάν* $L \sqsubseteq G$ *και*

$$\boxed{\textbf{NSubg}(G; L) := \{H \in \textbf{NSubg}(G) \mid L \sqsubseteq H\} = \textbf{NSubg}(G) \cap \textbf{Subg}(G; L)}$$

(βλ. 3.2.32), *τότε το μερικώς διατεταγμένο σύνολο* $(\textbf{NSubg}(G; L), \trianglelefteqslant)$ *είναι υποσύνδεσμος τού* $(\textbf{NSubg}(G), \trianglelefteqslant)$.

Απόδειξη. Για οιεσδήποτε $H, K \in \textbf{NSubg}(G; L)$, έχουμε

$$H \cap K \in \textbf{NSubg}(G; L) \ \text{ και } \ \mathrm{NCL}_G(H, K) \in \textbf{NSubg}(G; L),$$

οπότε το $(\textbf{NSubg}(G; L), \trianglelefteqslant)$ είναι όντως υποσύνδεσμος τού $(\textbf{NSubg}(G), \trianglelefteqslant)$. □

5.2.30 Πρόταση. *Εάν η $f : (G, \cdot) \longrightarrow (H, *)$ είναι ένας ομομορφισμός ομάδων, τότε ισχύουν τα ακόλουθα*:

(i) *Εάν $K \in \mathbf{NSubg}(G)$, τότε $f(K) \in \mathbf{NSubg}(\mathrm{Im}(f))$.*

(ii) *Εάν $L \in \mathbf{NSubg}(\mathrm{Im}(f))$, τότε*

$$f^{-1}(L) = \{ g \in G \mid f(g) \in L \} \in \mathbf{NSubg}(G; \mathrm{Ker}(f)).$$

Απόδειξη. (i) Κατά το 3.5.17 (i) η εικόνα $f(K)$ οιασδήποτε υποομάδας K τής G μέσω τής f είναι μια υποομάδα τής $f(G)$. Εάν υποθέσουμε ότι $K \trianglelefteq G$, τότε θεωρώντας τυχόντα στοιχεία $h \in f(G)$ και $v \in f(K)$ και λαμβάνοντας υπ' όψιν ότι υπάρχουν $g \in G, u \in K$, τέτοια ώστε $h = f(g)$ και $v = f(u)$, συμπεραίνουμε ότι

$$\left.\begin{array}{r} h * v * h^{-1} = f(g) * f(u) * f(g)^{-1} = f(gug^{-1}) \\ u \in K,\ K \trianglelefteq G \Rightarrow gug^{-1} \in K \end{array}\right\} \Rightarrow h * v * h^{-1} \in f(K).$$

Κατά συνέπειαν, $f(K) \trianglelefteq f(G)$.

(ii) Κατά το 3.5.17 (ii) η αντίστροφη εικόνα $f^{-1}(L)$ οιασδήποτε υποομάδας L τής $\mathrm{Im}(f)$ είναι μια υποομάδα τής G έχουσα τον πυρήνα $\mathrm{Ker}(f)$ τής f ως υποομάδα της. Εάν υποθέσουμε ότι $L \trianglelefteq \mathrm{Im}(f)$, τότε θεωρώντας τυχόντα στοιχεία $g \in G$ και $u \in f^{-1}(L)$ συμπεραίνουμε ότι

$$\left.\begin{array}{r} f(gug^{-1}) = f(g) * f(u) * f(g)^{-1} \\ u \in f^{-1}(L) \Rightarrow f(u) \in L \end{array}\right\} \Rightarrow f(gug^{-1}) \in L \Rightarrow gug^{-1} \in f^{-1}(L).$$

Κατά συνέπειαν, $f^{-1}(L) \trianglelefteq G$. □

5.2.31 Πόρισμα. *Ο πυρήνας οιουδήποτε ομομορφισμού $f : (G, \cdot) \to (H, *)$ είναι μια ορθόθετη υποομάδα τής G.*

Απόδειξη. Άμεση από τα 3.5.4 (ii), 5.2.5 και 5.2.30 (ii), καθόσον ο πυρήνας $\mathrm{Ker}(f)$ είναι εξ ορισμού η αντίστροφη εικόνα τής τετριμμένης υποομάδας τής H μέσω τής απεικονίσεως f. □

5.2.32 Παραδείγματα. (i) Έστω $n \in \mathbb{N}$, $n \geqslant 2$. Εξ ορισμού, $\mathfrak{A}_n := \mathrm{Ker}(\mathrm{sgn})$, όπου $\mathrm{sgn}: (\mathfrak{S}_n, \circ) \longrightarrow (\{1, -1\}, \cdot)$ η απεικόνιση προσημάνσεως (4.11). Κατά το (i) τού θεωρήματος 4.3.5 και την παρατήρηση 4.3.10 η sgn είναι ένας επιμορφισμός ομάδων. Εάν εφαρμόσουμε το πόρισμα 5.2.31, τότε διαπιστώνουμε εκ νέου ότι $\mathfrak{A}_n \lhd \mathfrak{S}_n$ (πρβλ. 5.2.14).

(ii) Έστω $(R, \cdot)$ το αβελιανό μονοειδές με $R \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, όπου "$\cdot$" ο συνήθης πολλαπλασιασμός. Τότε ο ομομορφισμός ομάδων

$$\mathrm{GL}_n(R) \longrightarrow R^\times,\ \mathbf{A} \longmapsto \det(\mathbf{A}),$$

είναι επιμορφισμός, διότι

$$\det \begin{pmatrix} x & 0_R & \cdots & 0_R \\ 0_R & 1_R & & \vdots \\ \vdots & & \ddots & 0_R \\ 0_R & \cdots & 0_R & 1_R \end{pmatrix} = x,\ \ \forall x \in R^\times,$$

και έχει ως πυρήνα του την $\mathrm{SL}_n(R)$, οπότε $\mathrm{SL}_n(R) \trianglelefteq \mathrm{GL}_n(R)$ (βλ. 3.2.21 (vii)).

(iii) Ο επιμορφισμός ομάδων

$$\mathrm{O}_n(\mathbb{R}) \longrightarrow \{1, -1\},\ \mathbf{A} \longmapsto \det(\mathbf{A}),$$

έχει ως πυρήνα του την $\mathrm{SO}_n(\mathbb{R})$, οπότε $\mathrm{SO}_n(\mathbb{R}) \lhd \mathrm{O}_n(\mathbb{R})$.

(iv) Κατ' αναλογίαν, ο επιμορφισμός ομάδων

$$\mathrm{U}_n(\mathbb{C}) \longrightarrow \mathbb{S}^1,\ \mathbf{A} \longmapsto \det(\mathbf{A}),$$

έχει ως πυρήνα του την $\mathrm{SU}_n(\mathbb{C})$, οπότε $\mathrm{SU}_n(\mathbb{C}) \lhd \mathrm{U}_n(\mathbb{C})$.

5.3 ΑΠΛΕΣ ΟΜΑΔΕΣ

Ένα σημαντικό τμήμα τής Θεωρίας Ομάδων συναρτάται με τη μελέτη εκείνων των ομάδων που διαθέτουν *τον ελάχιστο δυνατό αριθμό* ορθόθετων υποομάδων.

5.3.1 Ορισμός. Μια μη τετριμμένη ομάδα καλείται **απλή ομάδα** όταν διαθέτει ως ορθόθετες υποομάδες της μόνον την τετριμμένη και τον εαυτό της.

Λόγω τής επομένης προτάσεως, η μελέτη των απλών ομάδων (πεπερασμένης ή άπειρης τάξεως) επικεντρώνεται στην εξέταση τής δομήσεως των *μη αβελιανών*.

5.3.2 Πρόταση. *Κάθε αβελιανή απλή ομάδα είναι κυκλική και έχει ως τάξη της έναν πρώτο αριθμό.*

Απόδειξη. Έστω G μια αβελιανή ομάδα. Εάν η G είναι απλή, τότε, σύμφωνα με την πρόταση 5.2.6, οι μόνες υποομάδες της είναι η τετριμμένη και ο εαυτός της. Αρκεί λοιπόν η εφαρμογή τού πορίσματος 5.1.35. □

5.3.3 Σημείωση (Περί τής ταξινομήσεως των πεπερασμένων απλών ομάδων). Η *ταξινόμηση των μη αβελιανών απλών πεπερασμένων ομάδων μέχρις ισομορφισμού* υπήρξε ένα από τα δυσκολότερα προβλήματα των Σύγχρονων Μαθηματικών. Για την ολοκλήρωσή της (κατά τις αρχές τής δεκαετίας τού 1980) απαιτήθηκαν σκληρές (και, εν πολλοίς, συντονισμένες) προσπάθειες εκατοντάδων μαθηματικών επί περίπου μία τεσσαρακονταετία. Στην τελική «απόδειξη» υπεισέρχονται αποτελέσματα, τα οποία συναντούμε σε περισσότερα από 500 άρθρα δημοσιευθέντα σε μαθηματικά περιοδικά, και τα οποία καλύπτουν το εύρος 10-15 χιλιάδων τυπωμένων σελίδων. Ο πλήρης κατάλογος των μη αβελιανών απλών πεπερασμένων ομάδων υποδιαιρείται σε τρεις κλάσεις ομάδων. Αυτές είναι οι εξής:

(i) Οι *εναλλάσσουσες ομάδες* $\mathfrak{A}_n$, $n \geqslant 5$ (βλ. θεώρημα 5.3.6).

(ii) 16 απειροπληθείς οικογένειες ομάδων *τύπου Lie*.

(iii) Οι *σποραδικές ομάδες*, ήτοι 26 ειδικές απλές ομάδες που δεν εντάσσονται στις (i)-(ii).

▸ **Απλότητα των $\mathfrak{A}_n$, $n \geqslant 5$, και άμεσες συνέπειες αυτής.** Η εναλλάσσουσα ομάδα $\mathfrak{A}_3$ είναι κυκλική τάξεως 3 και κατ' επέκταση απλή, ενώ η $\mathfrak{A}_4$ δεν είναι απλή, διότι περιέχει την ομάδα $\mathbf{V}$ των τεσσάρων στοιχείων τού Klein ως ορθόθετη υποομάδα της (βλ. 5.2.21). Για να αποδείξουμε την απλότητα τής $\mathfrak{A}_n$ όταν $n \geqslant 5$ θα προτάξουμε δύο βοηθητικά λήμματα.

5.3.4 Λήμμα. *Έστω $n \in \mathbb{N}$, $n \geqslant 5$. Εάν η H είναι μια ορθόθετη υποομάδα τής $\mathfrak{A}_n$ περιέχουσα (τουλάχιστον) έναν 3-κύκλο, τότε $H = \mathfrak{A}_n$.*

Απόδειξη. Ας υποθέσουμε ότι $H \leqslant \mathfrak{A}_n$ και ότι η H περιέχει τον 3-κύκλο $[\alpha\ \beta\ \gamma]$. Θεωρούμε *τυχόν* στοιχείο $i \in \{1,\dots,n\}\smallsetminus\{\alpha,\beta,\gamma\}$. Τότε

$$\begin{aligned}
[\alpha\ \beta\ i] &= [i\,\alpha\,\beta] = [i\ \alpha] \circ [\alpha\ \beta] = [\alpha\ \beta] \circ [\alpha\ i\ \beta] \circ [\alpha\ \beta] \\
&= [\alpha\ \beta] \circ [i\ \gamma\ \alpha\ \beta] \circ [\alpha\ \beta\ \gamma\ i] \circ [\alpha\ \beta] \\
&= [\alpha\ \beta] \circ [i\ \gamma] \circ [\gamma\ \alpha\ \beta] \circ [\alpha\ \beta\ \gamma\ i] \circ [\alpha\ \beta] \\
&= [\alpha\ \beta] \circ [\gamma\ i] \circ [\alpha\ \beta\ \gamma]^2 \circ [\gamma\ i] \circ [\alpha\ \beta] \\
&= \underbrace{([\alpha\ \beta] \circ [\gamma\ i])}_{\in\mathfrak{A}_n} \circ \underbrace{[\alpha\ \beta\ \gamma]^2}_{\in H} \circ \underbrace{([\alpha\ \beta] \circ [\gamma\ i])^{-1}}_{\in\mathfrak{A}_n},
\end{aligned}$$

οπότε $[\alpha\ \beta\ i] \in H$. Κατά συνέπειαν,

$$\{[\alpha\ \beta\ i] \mid i \in \{1,\dots,n\}\smallsetminus\{\alpha,\beta\}\} \subseteq H.$$

Όμως αυτό το υποσύνολο παράγει την εναλλάσσουσα ομάδα $\mathfrak{A}_n$ (επί τη βάσει τού (iii) τής προτάσεως 4.3.13). Ως εκ τούτου, $H = \mathfrak{A}_n$. □

5.3.5 Λήμμα. *Έστω $n \in \mathbb{N}$, $n \geqslant 5$. Εάν η H είναι μια ορθόθετη υποομάδα τής $\mathfrak{A}_n$ περιέχουσα τη σύνθεση δύο ξένων μεταξύ τους αντιμεταθέσεων, τότε $H = \mathfrak{A}_n$.*

Απόδειξη. Έστω ότι οι $[\alpha_1\ \alpha_2]$ και $[\alpha_3\ \alpha_4]$ είναι οι αντιμεταθέσεις τής υποθέσεώς μας. Θέτοντας

$$\tau := [\alpha_1\ \alpha_2] \circ [\alpha_3\ \alpha_4] \in H,\ \ \sigma := [\alpha_1\ \alpha_2\ \beta] \in \mathfrak{A}_n,$$

όπου $\beta \in \{1,\dots,n\}\smallsetminus\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$, παρατηρούμε ότι

$$\tau^{-1} \in H,\ \sigma \circ \tau \circ \sigma^{-1} \in H \Rightarrow \left(\sigma \circ \tau \circ \sigma^{-1}\right) \circ \tau^{-1} \in H.$$

Επειδή (κατά το 4.2.3 (vii))

$$\begin{aligned}
\sigma \circ \tau \circ \sigma^{-1} &= \sigma \circ ([\alpha_1\ \alpha_2] \circ [\alpha_3\ \alpha_4]) \circ \sigma^{-1} \\
&= (\sigma \circ [\alpha_1\ \alpha_2] \circ \sigma^{-1}) \circ (\sigma \circ [\alpha_3\ \alpha_4] \circ \sigma^{-1}) \\
&= [\sigma(\alpha_1)\ \sigma(\alpha_2)] \circ [\sigma(\alpha_3)\ \sigma(\alpha_4)] = [\alpha_2\ \beta] \circ [\alpha_3\ \alpha_4],
\end{aligned}$$

συνάγεται ότι

$$\begin{aligned}
\left(\sigma \circ \tau \circ \sigma^{-1}\right) \circ \tau^{-1} &= ([\alpha_2\ \beta] \circ [\alpha_3\ \alpha_4]) \circ [\alpha_3\ \alpha_4]^{-1} \circ [\alpha_1\ \alpha_2]^{-1} \\
&= [\beta\ \alpha_2] \circ [\alpha_2\ \alpha_1] = [\beta\ \alpha_2\ \alpha_1] \in H.
\end{aligned}$$

Επειδή η H περιέχει τον 3-κύκλο $[\beta\ \alpha_2\ \alpha_1]$, από το λήμμα 5.3.4 συμπεραίνουμε ότι $H = \mathfrak{A}_n$. □

5.3.6 Θεώρημα. *Οι εναλλάσσουσες ομάδες $\mathfrak{A}_n$ είναι απλές για κάθε $n \geqslant 5$.*

Απόδειξη[13]. Έστω H μια μη τετριμμένη ορθόθετη υποομάδα τής $\mathfrak{A}_n$, $n \geqslant 5$, και έστω $\sigma \in H\smallsetminus\{\mathrm{id}\}$. Σύμφωνα με το θεμελιώδες θεώρημα 4.2.7 η μετάταξη σ μπορεί να γραφεί υπό τη μορφή επαλλήλων συνθέσεων $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_\nu$ *ανά δύο ξένων* μεταξύ τους κύκλων μήκους $\geqslant 2$. Επιπροσθέτως, μια τέτοια έκφραση είναι *μονοσημάντως ορισμένη* (ενδεχομένως ύστερα από κάποια αναδιάταξη των μετεχόντων κύκλων). Μπορούμε λοιπόν δίχως βλάβη τής γενικότητας να υποθέσουμε ότι

$$(\text{μήκος τού } \tau_j) \geqslant (\text{μήκος τού } \tau_{j+1}),\ \forall j \in \{1,2,\dots,\nu-1\}$$

[13] Η πρώτη ολοκληρωμένη απόδειξη αυτού τού θεωρήματος εδόθη από τον C. Jordan (1838-1922) το έτος 1870 στο σύγγραμμά του *Traité des substitutions et des équations algebriques* (σελ. 66).

(όταν $\nu \geqslant 2$) και ότι $\tau_1 = [\alpha_1\ \alpha_2\ \ldots\ \alpha_k]$. Εξετάζουμε τα πέντε ενδεχόμενα χωριστά:

Περίπτωση πρώτη. Υποθέτουμε ότι $k \geqslant 4$, $\nu \geqslant 1$. Θέτοντας $c := [\alpha_1\ \alpha_2\ \alpha_3] \in \mathfrak{A}_n$ παρατηρούμε ότι

$$c \in \mathfrak{A}_n,\ \sigma \in H \Rightarrow c \circ \sigma \circ c^{-1} \in H,$$

οπότε $\sigma^{-1} \in H \Rightarrow \left(c \circ \sigma \circ c^{-1}\right) \circ \sigma^{-1} \in H$. Επειδή (κατά το 4.2.3 (vii))

$$\begin{aligned} c \circ \sigma \circ c^{-1} &= c \circ (\tau_1 \circ \cdots \circ \tau_\nu) \circ c^{-1} \\ &= (c \circ \tau_1 \circ c^{-1}) \circ (c \circ \tau_2 \circ c^{-1}) \circ \cdots \circ (c \circ \tau_\nu \circ c^{-1}) \\ &= (c \circ \tau_1 \circ c^{-1}) \circ (\tau_2 \circ \cdots \circ \tau_\nu) \\ &= [c(\alpha_1)\ c(\alpha_2)\ \ldots\ c(\alpha_k)] \circ (\tau_2 \circ \cdots \circ \tau_\nu) \\ &= [\alpha_2\ \alpha_3\ \alpha_1\ \alpha_4\ \ldots\ \alpha_k] \circ (\tau_2 \circ \cdots \circ \tau_\nu), \end{aligned}$$

έχουμε

$$\begin{aligned} \left(c \circ \sigma \circ c^{-1}\right) \circ \sigma^{-1} &= [\alpha_2\ \alpha_3\ \alpha_1\ \alpha_4\ \ldots\ \alpha_k] \circ (\tau_2 \circ \cdots \circ \tau_\nu) \circ (\tau_\nu^{-1} \circ \cdots \circ \tau_1^{-1}) \\ &= [\alpha_2\ \alpha_3\ \alpha_1\ \alpha_4\ \ldots\ \alpha_k] \circ \tau_1^{-1} \\ &= [\alpha_2\ \alpha_3\ \alpha_1\ \alpha_4\ \ldots\ \alpha_k] \circ [\alpha_k\ \alpha_{k-1}\ \ldots\ \alpha_1] = [\alpha_1\ \alpha_2\ \alpha_4] \in H. \end{aligned}$$

Επειδή η H περιέχει τον 3-κύκλο $[\alpha_1\ \alpha_2\ \alpha_4]$, $H = \mathfrak{A}_n$ δυνάμει τού λήμματος 5.3.4.

Περίπτωση δεύτερη. Εάν $k = 3, \nu = 1$, τότε $H = \mathfrak{A}_n$ (με απευθείας εφαρμογή τού λήμματος 5.3.4).

Περίπτωση τρίτη. Υποθέτουμε ότι $k = 3$, $\nu \geqslant 2$, και ότι ο τ_2 είναι ωσαύτως ένας 3-κύκλος, ας πούμε ο $\tau_2 = [\beta_1\ \beta_2\ \beta_3]$. Θέτοντας $c := [\alpha_2\ \alpha_3\ \beta_1] \in \mathfrak{A}_n$ παρατηρούμε ότι

$$c \in \mathfrak{A}_n,\ \sigma \in H \Rightarrow c \circ \sigma \circ c^{-1} \in H,$$

οπότε $\sigma^{-1} \in H \Rightarrow \left(c \circ \sigma \circ c^{-1}\right) \circ \sigma^{-1} \in H$. Επειδή (κατά το 4.2.3 (vii))

$$\begin{aligned} c \circ \sigma \circ c^{-1} &= c \circ (\tau_1 \circ \cdots \circ \tau_\nu) \circ c^{-1} \\ &= (c \circ \tau_1 \circ c^{-1}) \circ (c \circ \tau_2 \circ c^{-1}) \circ \cdots \circ (c \circ \tau_\nu \circ c^{-1}) \\ &= (c \circ \tau_1 \circ c^{-1}) \circ (c \circ \tau_2 \circ c^{-1}) \circ (\tau_3 \circ \cdots \circ \tau_\nu) \\ &= [c(\alpha_1)\ c(\alpha_2)\ c(\alpha_3)] \circ [c(\beta_1)\ c(\beta_2)\ c(\beta_3)] \circ (\tau_3 \circ \cdots \circ \tau_\nu) \\ &= [\alpha_1\ \alpha_3\ \beta_1] \circ [\alpha_2\ \beta_2\ \beta_3] \circ (\tau_3 \circ \cdots \circ \tau_\nu), \end{aligned}$$

η σύνθεση $\left(c \circ \sigma \circ c^{-1}\right) \circ \sigma^{-1}$ ισούται με

$$\begin{aligned} & [\alpha_1\ \alpha_3\ \beta_1] \circ [\alpha_2\ \beta_2\ \beta_3] \circ (\tau_3 \circ \cdots \circ \tau_\nu) \circ (\tau_\nu^{-1} \circ \cdots \circ \tau_2^{-1} \circ \tau_1^{-1}) \\ = \ & [\alpha_1\ \alpha_3\ \beta_1] \circ [\alpha_2\ \beta_2\ \beta_3] \circ \tau_2^{-1} \circ \tau_1^{-1} \\ = \ & [\alpha_1\ \alpha_3\ \beta_1] \circ [\alpha_2\ \beta_2\ \beta_3] \circ [\beta_3\ \beta_2\ \beta_1] \circ [\alpha_3\ \alpha_2\ \alpha_1] \\ = \ & [\beta_1\ \alpha_1\ \alpha_3] \circ [\beta_2\ \beta_3\ \alpha_2] \circ [\alpha_2\ \alpha_1\ \alpha_3] \circ [\beta_3\ \beta_2\ \beta_1] \\ = \ & [\beta_1\ \alpha_1\ \alpha_3] \circ [\beta_2\ \beta_3\ \alpha_2\ \alpha_1\ \alpha_3] \circ [\beta_3\ \beta_2\ \beta_1] \\ = \ & [\beta_1\ \alpha_1\ \alpha_3] \circ [\beta_2\ \beta_1\ \alpha_2\ \alpha_1\ \alpha_3] = [\alpha_1\ \beta_1\ \alpha_2\ \alpha_3\ \beta_2] \in H \end{aligned}$$

(βλ. 4.2.3 (i), (vi)). Επειδή η H περιέχει τον 5-κύκλο $[\alpha_1\ \beta_1\ \alpha_2\ \alpha_3\ \beta_2]$, μπορούμε να εργασθούμε με αυτόν (στη θέση τής αρχικώς θεωρηθείσας μετατάξεως σ), να εφαρμόσουμε ό,τι προαναφέρθηκε στην πρώτη περίπτωση και να συμπεράνουμε ότι $H = \mathfrak{A}_n$.

Περίπτωση τέταρτη. Υποθέτουμε ότι $k = 3$, $\nu \geqslant 2$, και ότι όλοι οι κύκλοι $\tau_2, \ldots, \tau_\nu$ είναι αντιμεταθέσεις. Τότε

$$\begin{aligned} \sigma^2 &= [\alpha_1\ \alpha_2\ \alpha_3] \circ (\tau_2 \circ \cdots \circ \tau_\nu) \circ [\alpha_1\ \alpha_2\ \alpha_3] \circ (\tau_2 \circ \cdots \circ \tau_\nu) \\ &= [\alpha_1\ \alpha_2\ \alpha_3]^2 \circ (\tau_2^2 \circ \cdots \circ \tau_\nu^2) = [\alpha_1\ \alpha_2\ \alpha_3]^2 \circ (\mathrm{id} \circ \cdots \circ \mathrm{id}) \\ &= [\alpha_1\ \alpha_2\ \alpha_3]^2 = [\alpha_1\ \alpha_3\ \alpha_2] \in H. \end{aligned}$$

(βλ. 4.2.3 (iv), (v), και 4.2.4). Επειδή η H περιέχει τον 3-κύκλο $[\alpha_1\ \alpha_3\ \alpha_2]$, $H = \mathfrak{A}_n$ δυνάμει τού λήμματος 5.3.4.

Περίπτωση πέμπτη. Υποθέτουμε ότι $k = 2$, $\nu \geqslant 2$, και ότι όλοι οι κύκλοι $\tau_1, \ldots, \tau_\nu$ είναι αντιμεταθέσεις, με τον φυσικό αριθμό ν κατ' ανάγκην *άρτιο* (αφού $\sigma \in \mathfrak{A}_n$). Εάν έχουμε $\tau_2 = [\beta_1\ \beta_2]$, τότε θέτοντας $c := [\alpha_2\ \beta_1\ \beta_2] \in \mathfrak{A}_n$ παρατηρούμε ότι $c \in \mathfrak{A}_n, \sigma \in H \Rightarrow c \circ \sigma \circ c^{-1} \in H$, οπότε $\sigma^{-1} \in H \Rightarrow \left(c \circ \sigma \circ c^{-1}\right) \circ \sigma^{-1} \in H$. Επειδή (κατά το 4.2.3 (vii))

$$\begin{aligned} c \circ \sigma \circ c^{-1} &= c \circ (\tau_1 \circ \cdots \circ \tau_\nu) \circ c^{-1} \\ &= (c \circ \tau_1 \circ c^{-1}) \circ (c \circ \tau_2 \circ c^{-1}) \circ \cdots \circ (c \circ \tau_\nu \circ c^{-1}) \\ &= (c \circ \tau_1 \circ c^{-1}) \circ (c \circ \tau_2 \circ c^{-1}) \circ (\tau_3 \circ \cdots \circ \tau_\nu) \\ &= [c(\alpha_1)\ c(\alpha_2)] \circ [c(\beta_1)\ c(\beta_2)] \circ (\tau_3 \circ \cdots \circ \tau_\nu) \\ &= [\alpha_1\ \beta_1] \circ [\beta_2\ \alpha_2] \circ (\tau_3 \circ \cdots \circ \tau_\nu), \end{aligned}$$

η σύνθεση $\left(c \circ \sigma \circ c^{-1}\right) \circ \sigma^{-1}$ ισούται με

$$\begin{aligned} & [\alpha_1\ \beta_1] \circ [\beta_2\ \alpha_2] \circ (\tau_3 \circ \cdots \circ \tau_\nu) \circ (\tau_\nu^{-1} \circ \cdots \circ \tau_2^{-1} \circ \tau_1^{-1}) \\ = \ & [\alpha_1\ \beta_1] \circ [\beta_2\ \alpha_2] \circ \tau_2^{-1} \circ \tau_1^{-1} \\ = \ & [\alpha_1\ \beta_1] \circ [\beta_2\ \alpha_2] \circ [\beta_2\ \beta_1] \circ [\alpha_2\ \alpha_1] \\ = \ & [\alpha_1\ \beta_1] \circ [\alpha_2\ \beta_2] \circ [\beta_2\ \beta_1] \circ [\alpha_2\ \alpha_1] \\ = \ & [\alpha_1\ \beta_1] \circ [\alpha_2\ \beta_2\ \beta_1] \circ [\alpha_2\ \alpha_1] \\ = \ & [\alpha_1\ \beta_1] \circ [\beta_2\ \beta_1\ \alpha_2] \circ [\alpha_2\ \alpha_1] \\ = \ & [\alpha_1\ \beta_1] \circ [\beta_2\ \beta_1\ \alpha_2\ \alpha_1] = [\alpha_1\ \beta_2] \circ [\alpha_2\ \beta_1] \in H \end{aligned}$$

(βλ. 4.2.3 (i)-(iii)). Κι επειδή η H περιέχει τη σύνθεση $[\alpha_1\ \beta_2] \circ [\alpha_2\ \beta_1]$ δύο ξένων μεταξύ τους αντιμεταθέσεων, έχουμε $H = \mathfrak{A}_n$ επί τη βάσει τού λήμματος 5.3.5. □

5.3.7 Σημείωση (Άπειρη εναλλάσσουσα ομάδα επί τού $\mathbb{N}$). Η άπειρη υποομάδα

$$\mathfrak{A}_\infty := \langle \{[i\ j\ k] \mid i, j, k \in \mathbb{N},\ i < j < k\} \rangle$$

τής συμμετρικής ομάδας $\mathfrak{S}_\mathbb{N}$ (επί *ολοκλήρου* τού συνόλου των φυσικών αριθμών), η οποία παράγεται από τους όλους τους κύκλους[14] μήκους 3, καλείται **άπειρη εναλλάσσουσα ομάδα επί τού** $\mathbb{N}$ (και αποτελεί άμεση γενίκευση τής $\mathfrak{A}_n$, πρβλ. 4.3.13 (ii)). Ακολουθώντας κατά γράμμα την αποδεικτική μέθοδο που εφαρμόσθηκε στο θεώρημα 5.3.6 καταλήγουμε στη διαπίστωση τού ότι η $\mathfrak{A}_\infty$ είναι ωσαύτως απλή. Ως εκ τούτου, η $\mathfrak{A}_\infty$ αποτελεί *παράδειγμα άπειρης απλής ομάδας*.

5.3.8 Θεώρημα. *Κάθε πεπερασμένη ομάδα εμφυτεύεται σε μια πεπερασμένη απλή ομάδα* (βλ. 3.5.11 και 8.1.18).

Απόδειξη. Έστω G τυχούσα πεπερασμένη ομάδα τάξεως $n = |G| \geqslant 1$. Εάν $n = 1$, τότε η G είναι ισόμορφη με την τετριμμένη υποομάδα οιασδήποτε πεπερασμένης απλής ομάδας. Εάν $n \in \{2, 3\}$, τότε η G είναι κυκλική έχουσα ως τάξη της έναν πρώτο αριθμό και, ως εκ τούτου, αφ' εαυτής απλή. Εάν $n \geqslant 4$, τότε (σύμφωνα με το πόρισμα 4.5.3) η G εμφυτεύεται εντός τής συμμετρικής ομάδας $\mathfrak{S}_n$ σε n σύμβολα. Από την άλλη μεριά, η $\mathfrak{S}_n$ εμφυτεύεται στην εναλλάσσουσα ομάδα $\mathfrak{A}_{2n}$ σε $2n$ σύμβολα μέσω ενός μονομορφισμού $f : \mathfrak{S}_n \longrightarrow \mathfrak{A}_{2n}$ τον οποίο ορίζουμε ως εξής: Σε κάθε k-κύκλο $\tau = [a_1\ a_2\ \cdots\ a_k] \in \mathfrak{S}_n$ μήκους $k \in \{2, \ldots, n\}$ αντιστοιχίζουμε τον

[14] Εν προκειμένω, ένας k-**κύκλος** $\sigma = [a_1\ a_2\ \cdots\ a_k]$ ορίζεται όπως και ο k-κύκλος εντός τής $\mathfrak{S}_n$ (βλ. 4.2.1), με μόνη διαφορά ότι $\sigma\,(\beta) = \beta$ *για κάθε* $\beta \in \mathbb{N} \setminus \{a_1, a_2, \ldots, a_k\}$.

k-κύκλο $\widetilde{\tau} = [n + a_1\ n + a_2\ \cdots\ n + a_k] \in \mathfrak{S}_{2n}$. Σημειωτέον ότι $\tau \circ \widetilde{\tau} \in \mathfrak{A}_{2n}$ (εάν ο τ ιδωθεί ως k-κύκλος *εντός τής* $\mathfrak{S}_{2n}$), διότι

$$\operatorname{sgn}(\tau \circ \widetilde{\tau}) = \operatorname{sgn}(\tau) \cdot \operatorname{sgn}(\widetilde{\tau}) = (-1)^{k-1} \cdot (-1)^{k-1} = (-1)^{2k-2} = 1$$

(βάσει τού (iii) τού θεωρήματος 4.3.5). Εκφράζοντας κάθε μετάταξη $\sigma \in \mathfrak{S}_n \smallsetminus \{\mathrm{id}\}$ υπό τη μορφή επαλλήλων συνθέσεων (πεπερασμένου πλήθους) ανά δύο ξένων μεταξύ τους κύκλων μήκους $\geqslant 2$, ας πούμε $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_\nu$, κατά το θεμελιώδες θεώρημα 4.2.7, ορίζοντας ως εικόνα τής σ μέσω τής f το στοιχείο

$$f(\sigma) := \tau_1 \circ \widetilde{\tau}_1 \circ \tau_2 \circ \widetilde{\tau}_2 \circ \cdots \circ \tau_\nu \circ \widetilde{\tau}_\nu \in \mathfrak{A}_{2n},$$

και θέτοντας $f(\mathrm{id}) := \mathrm{id}$, διαπιστώνουμε άμεσα ότι η απεικόνιση f είναι ομομορφισμός ομάδων. Η ενριπτικότητα τής f έπεται από το γεγονός ότι οι συντιθέμενοι κύκλοι είναι μεταξύ τους ξένοι και οι χρησιμοποιούμενες εκφράσεις μονοσημάντως ορισμένες (ενδεχομένως ύστερα από κάποια αναδιάταξη των μετεχόντων κύκλων, κάτι που είναι ουσιαστικώς αδιάφορο, αφού ισχύει η μεταθετικότητα λόγω τού λήμματος 4.2.4). Κατά συνέπειαν, η ίδια η G είναι εμφυτεύσιμη εντός τής $\mathfrak{A}_{2n}$ (βάσει τού (ii) τής προτάσεως 3.5.9). Όμως η $\mathfrak{A}_{2n}$ είναι *απλή ομάδα*, αφού εξ υποθέσεως $2n \geqslant 8$ (βλ. θεώρημα 5.3.6). □

▸ **Ορθόθετες υποομάδες τής** $\mathfrak{S}_n$, $n \geqslant 5$. Το θεώρημα 5.3.10 μας πληροφορεί ότι για φυσικούς αριθμούς $n \geqslant 5$ ακόμη και η ίδια η συμμετρική ομάδα $\mathfrak{S}_n$ δεν διαθέτει άλλες ορθόθετες υποομάδες πέραν των (τριών) προφανών. Για την απόδειξή του θα χρησιμοποιήσουμε το ακόλουθο:

5.3.9 Λήμμα. *Εάν $n \in \mathbb{N}$, $n \geqslant 3$, τότε δεν υφίσταται στοιχείο $\sigma \in \mathfrak{S}_n \smallsetminus \{\mathrm{id}\}$, τέτοιο ώστε να ισχύει $\sigma \circ \varrho \circ \sigma^{-1} = \varrho$* (ή, ισοδυνάμως, $\sigma \circ \varrho = \varrho \circ \sigma$), $\forall \varrho \in \mathfrak{S}_n$.

Απόδειξη. Εργαζόμαστε με «εις άτοπον απαγωγή». Υποθέτουμε ότι υπάρχει κάποιο στοιχείο $\sigma \in \mathfrak{S}_n \smallsetminus \{\mathrm{id}\}$, τέτοιο ώστε να ισχύει $\sigma \circ \varrho \circ \sigma^{-1} = \varrho$, *για κάθε* $\varrho \in \mathfrak{S}_n$. Το σ (σύμφωνα με το θεμελιώδες θεώρημα 4.2.7) γράφεται υπό τη μορφή επαλλήλων συνθέσεων (πεπερασμένου πλήθους) ανά δύο ξένων μεταξύ τους κύκλων μήκους $\geqslant 2$, ας πούμε $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_\nu$. Έστω ότι $\tau_1 = [a_1\ a_2\ \cdots\ a_k]$, για κάποιον $k \in \mathbb{N}$, $2 \leqslant k \leqslant n$. Εξετάζουμε δύο περιπτώσεις χωριστά:

Περίπτωση πρώτη. Εάν $k \geqslant 3$, τότε θεωρώντας ως ϱ τον 2-κύκλο $[a_1\ a_2]$ καταλήγουμε σε άτοπο, καθόσον (κατά το 4.2.3 (vii))

$$\sigma \circ \varrho \circ \sigma^{-1} = \sigma \circ [a_1\ a_2] \circ \sigma^{-1} = [\sigma(a_1)\ \sigma(a_2)] = [a_2\ a_3] \neq [a_1\ a_2] = \varrho.$$

Περίπτωση δεύτερη. Εάν $k = 2$, τότε θεωρώντας ως ϱ τον 3-κύκλο $[a_1\ a_2\ a_3]$, όπου $a_3 \in \{1, \ldots, n\} \smallsetminus \{a_1, a_2\}$, καταλήγουμε εκ νέου σε άτοπο, καθόσον (κατά το 4.2.3 (vii))

$$\sigma \circ \varrho \circ \sigma^{-1} = \sigma \circ [a_1\ a_2\ a_3] \circ \sigma^{-1} = [\sigma(a_1)\ \sigma(a_2)\ \sigma(a_3)] = [a_2\ a_1\ \sigma(a_3)],$$

όπου $\sigma(a_3) \notin \{a_1, a_2\}$ και $\left(\sigma \circ \varrho \circ \sigma^{-1}\right)(a_2) = a_1 \neq a_3 = \varrho(a_2)$. □

5.3.10 Θεώρημα. *Εάν $n \in \mathbb{N}$, $n \geqslant 5$, τότε οι $\{\mathrm{id}\}$, $\mathfrak{A}_n$ και $\mathfrak{S}_n$ είναι οι μόνες ορθόθετες υποομάδες τής*[15] $\mathfrak{S}_n$.

[15] Λόγω τής προτάσεως 5.2.13, *η μόνη υποομάδα τής $\mathfrak{S}_n$ που έχει δείκτη* 2 εντός αυτής είναι η $\mathfrak{A}_n$. (Τούτο εξακολουθεί να ισχύει ακόμη και όταν $n \in \{2, 3, 4\}$.)

Απόδειξη. Έστω H τυχούσα ορθόθετη υποομάδα τής $\mathfrak{S}_n$. Τότε

$$\left.\begin{array}{r} H \trianglelefteqslant \mathfrak{S}_n \text{ (εξ υποθέσεως)} \\ \mathfrak{A}_n \lhd \mathfrak{S}_n \ \text{(βλ. 5.2.14)} \end{array}\right\} \underset{\text{(βλ. 5.2.8)}}{\Longrightarrow} H \cap \mathfrak{A}_n \lhd \mathfrak{S}_n$$

και

$$\left.\begin{array}{r} H \sqsubseteq \mathfrak{S}_n,\ \mathfrak{A}_n \sqsubseteq \mathfrak{S}_n \underset{3.2.23}{\Longrightarrow} H \cap \mathfrak{A}_n \sqsubseteq \mathfrak{S}_n \\ H \cap \mathfrak{A}_n \subseteq \mathfrak{A}_n \sqsubseteq \mathfrak{S}_n \underset{3.2.20}{\Longrightarrow} H \cap \mathfrak{A}_n \sqsubseteq \mathfrak{A}_n \\ H \cap \mathfrak{A}_n \lhd \mathfrak{S}_n \text{ (λόγω των προαναφερθέντων)} \end{array}\right\} \underset{5.2.19}{\Longrightarrow} H \cap \mathfrak{A}_n \trianglelefteqslant \mathfrak{A}_n$$

$$\underset{5.3.6}{\Longrightarrow} H \cap \mathfrak{A}_n \in \{\{\mathrm{id}\}, \mathfrak{A}_n\}.$$

Περίπτωση πρώτη. Εάν $H \cap \mathfrak{A}_n = \mathfrak{A}_n$, τότε

$$\mathfrak{A}_n \sqsubseteq H \sqsubseteq \mathfrak{S}_n$$

και (κατά το θεώρημα 5.1.50) έχουμε

$$2 = |\mathfrak{S}_n : \mathfrak{A}_n| = |\mathfrak{S}_n : H|\ |H : \mathfrak{A}_n|\,,$$

οπότε

$$(|\mathfrak{S}_n : H|\,, |H : \mathfrak{A}_n|) \in \{(2,1),(1,2)\} \Longrightarrow H \in \{\mathfrak{A}_n, \mathfrak{S}_n\}.$$

Περίπτωση δεύτερη. Εάν $H \cap \mathfrak{A}_n = \{\mathrm{id}\}$, θα δείξουμε (εργαζόμενοι με εις άτοπον απαγωγή) ότι $H = \{\mathrm{id}\}$. Ας υποθέσουμε ότι $H \neq \{\mathrm{id}\}$ κι ας επιλέξουμε κάποια μετάταξη $\sigma \in H \smallsetminus \{\mathrm{id}\}$. Το τετράγωνό της σ^2 (σύμφωνα με το (v) τού πορίσματος 4.3.6) είναι μια *άρτια* μετάταξη ανήκουσα στην υποομάδα H. Αυτό σημαίνει ότι

$$\sigma^2 \in H \cap \mathfrak{A}_n = \mathrm{id} \Rightarrow \sigma^2 = \mathrm{id}.$$

Από την άλλη μεριά, θεωρώντας *οιοδήποτε* στοιχείο $\tau \in H \smallsetminus \{\mathrm{id}\}$ παρατηρούμε ότι η σύνθεση $\tau \circ \sigma$ είναι μια *άρτια* μετάταξη ανήκουσα στην H (αφού *αμφότερες* οι μετατάξεις σ και τ είναι εξ υποθέσεως *περιττές*, βλ. 4.3.6 (iv)). Αυτό σημαίνει ότι

$$\tau \circ \sigma \in H \cap \mathfrak{A}_n = \{\mathrm{id}\} \Rightarrow \tau \circ \sigma = \mathrm{id} \Rightarrow \tau = \sigma^{-1} = \sigma \Rightarrow H = \{\mathrm{id}, \sigma\}.$$

Επειδή

$$\{\sigma\} = H \smallsetminus \{\mathrm{id}\} \subseteq \mathfrak{S}_n \smallsetminus \{\mathrm{id}\},$$

υφίσταται, κατά το λήμμα 5.3.9, κάποιο στοιχείο $\varrho \in \mathfrak{S}_n$, τέτοιο ώστε να ισχύει

$$\sigma \circ \varrho \circ \sigma^{-1} \neq \varrho.$$

Ως εκ τούτου,

$$\left.\begin{array}{r} H \trianglelefteqslant \mathfrak{S}_n \Rightarrow \varrho \circ \sigma \circ \varrho^{-1} \in \{\mathrm{id}, \sigma\} = H \\ \sigma \circ \varrho \circ \sigma^{-1} \neq \varrho \Rightarrow \varrho \circ \sigma \circ \varrho^{-1} \neq \sigma \end{array}\right\} \Rightarrow \varrho \circ \sigma \circ \varrho^{-1} = \mathrm{id} \Rightarrow \varrho \circ \sigma = \varrho \Rightarrow \sigma = \mathrm{id}.$$

Άτοπο! Επομένως, $H = \{\mathrm{id}\}$. □

5.4 ΚΑΤΑΣΚΕΥΗ ΚΑΙ ΙΔΙΟΤΗΤΕΣ ΠΗΛΙΚΟΟΜΑΔΩΝ

Μέσω των ορθόθετων υποομάδων δοθείσας ομάδας δημιουργούνται νέες ομάδες, οι λεγόμενες *πηλικοομάδες*, ύστερα από «μεταφορά» τού «πολλαπλασιασμού» τής ομάδας σε κατάλληλο «πολλαπλασιασμό» μεταξύ των διαθέσιμων πλευρικών κλάσεων.

5.4.1 Ορισμός. Εάν η H είναι μια ορθόθετη υποομάδα μιας ομάδας $(G,\cdot)$, τότε συμβολίζουμε ως

$$\boxed{G/H := G/_H\mathcal{R}\,(= G/\mathcal{R}_H)}$$

το αντίστοιχο σύνολο των κλάσεων ισοδυναμίας και ως $\pi_H^G : G \longrightarrow G/H$ τη φυσική επίριψη (δηλαδή $\pi_H^G(g) := gH, \forall g \in G$).

5.4.2 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω H μια ορθόθετη υποομάδα της. Μέσω τού τύπου*

$$\boxed{g_1H \odot g_2H := (g_1 \cdot g_2)\,H,\ \ \forall\,(g_1,g_2) \in G \times G,}$$

ορίζουμε μια απεικόνιση

$$(G/H) \times (G/H) \longrightarrow G/H,\ \ (gH, g'H) \longmapsto gH \odot g'H,$$

(ήτοι μια εσωτερική πράξη "$\odot$" επί τού G/H), η οποία καθιστά το διάγραμμα

$$\begin{array}{ccc} G \times G & \xrightarrow{\ \cdot\ } & G \\ \Big\downarrow{\scriptstyle \pi_H^G \times \pi_H^G} & & \Big\downarrow{\scriptstyle \pi_H^G} \\ (G/H) \times (G/H) & \xrightarrow[\ \odot\ ]{} & G/H \end{array}$$

μεταθετικό. Το ζεύγος $(G/H, \odot)$ αποτελεί μια ομάδα τάξεως $|G/H| = |G : H|$ έχουσα το $e_GH\ (= H)$ ως ουδέτερο στοιχείο της. Επιπροσθέτως, ισχύουν τα ακόλουθα:

(i) *Το συμμετρικό (= αντίστροφο) στοιχείο οιουδήποτε $gH \in G/H$ είναι το $g^{-1}H$.*

(ii) *Εάν η G είναι αβελιανή, τότε και η G/H είναι αβελιανή.*

(iii) *Εάν η G είναι πεπερασμένη, τότε $|G/H| = \frac{|G|}{|H|}$.*

Απόδειξη. Επειδή η ${}_H\mathcal{R}$ είναι συμβατή με την "$\cdot$" (βλ. 5.2.1), η εσωτερική πράξη "$\odot$" είναι (σύμφωνα με το (a) τού θεωρήματος 1.5.20) η μόνη που καθιστά το ανωτέρω διάγραμμα μεταθετικό και είναι προσεταιριστική λόγω τής προσεταιριστικότητας τής "$\cdot$". Επιπροσθέτως, το $e_GH\ (= H)$ αποτελεί ουδέτερο στοιχείο τού G/H ως προς την "$\odot$" και κάθε gH έχει το $g^{-1}H$ ως συμμετρικό (= αντίστροφο) στοιχείο του ως προς την "$\odot$". (Αρκεί να εφαρμοσθούν τα (b), (d) και (e) τού θεωρήματος 1.5.20, με τα ${}_H\mathcal{R}, G/H$ και gH στη θέση των εκεί παρατεθέντων $\mathcal{R}, A/\mathcal{R}$ και $[x]_{\mathcal{R}}$, αντιστοίχως.) Άρα το ζεύγος $(G/H, \odot)$ αποτελεί μια ομάδα τάξεως $|G/H| = |G : H|$ με $e_{G/H} = e_GH = H$, η οποία είναι αβελιανή στην περίπτωση κατά την οποία η $(G,\cdot)$ είναι αβελιανή. (Βλ. 1.5.20 (c).) Τα (i) και (ii) είναι, ως εκ τούτου, αληθή. Το (iii) έπεται άμεσα από το θεώρημα 5.1.22 τού Lagrange. □

5.4.3 Ορισμός. Η ομάδα $(G/H, \odot)$ η ορισθείσα μέσω τής προτάσεως 5.4.2 καλείται **πηλικοομάδα** (ή **ομάδα πηλίκων**) τής ομάδας G ως προς την H. (Επειδή έχουμε $(x,y) \in {}_H\mathcal{R} \underset{\text{ορσ}}{\iff} x^{-1}y \in H$, είναι σαφής ο λόγος για τον οποίο εκλαμβάνουμε τα στοιχεία τής G/H -συνεκδοχικώς- ως *πηλίκα* στοιχείων τής G ανήκοντα στην H και ομιλούμε ενίοτε -εκφραζόμενοι αφαιρετικώς- για *διαίρεση* «τής G διά τής H».)

5.4.4 Σημείωση (Απλούστευση συμβολισμού). Επιθυμώντας να τηρήσουμε την εξαπλούστευση και «ελάφρυνση» των χρησιμοποιούμενων συμβολισμών που διέπει το μεγαλύτερο μέρος τού κειμένου θα γράφουμε εφεξής, χωρίς να διατρέχουμε τον κίνδυνο παρερμηνείας, $(gH)\cdot(g'H)$ ή απλώς[16] $(gH)\,(g'H)$ αντί τού $gH \odot g'H$, έχοντας πάντοτε κατά νου ότι κατά τον «πολλαπλασιασμό» πλευρικών κλάσεων θα εννοούμε την εφαρμογή τού "$\odot$" που προκύπτει από την πρόταση 5.4.2 (και που απλώς *επάγεται* μέσω τού «πολλαπλασιασμού» τού ορισμένου επί τού G).

5.4.5 Παραδείγματα. Έστω $(G,\cdot)$ τυχούσα ομάδα. Τότε $\{e_G\} \trianglelefteqslant G$ και $G \trianglelefteqslant G$ (βλ. 5.2.5). Προφανώς, $G/\{e_G\} = \{\,g\{e_G\} \,|\, g \in G\} \cong G$ και $G/G \cong \{e_G\}$, διότι οι απεικονίσεις

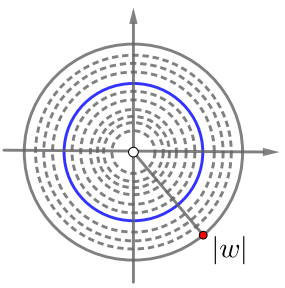
$$G/\{e_G\} \ni g\{e_G\} \longmapsto g \in G \quad \text{και} \quad G/G \ni gG \longmapsto e_G \in \{e_G\}$$

είναι ισομορφισμοί ομάδων.

5.4.6 Παράδειγμα. Η ομάδα $(\mathbb{S}^1,\cdot)$ είναι ορθόθετη υποομάδα τής πολλαπλασιαστικής ομάδας $(\mathbb{C}\smallsetminus\{0\},\cdot)$ (βλ. 3.2.21 (vi) και 5.2.5). Τα στοιχεία τής πηλικοομάδας $(\mathbb{C}\smallsetminus\{0\})/\mathbb{S}^1$ είναι οι πλευρικές κλάσεις $w\mathbb{S}^1$, $w \in \mathbb{C}\smallsetminus\{0\}$. Συγκεκριμένα, για οιονδήποτε μιγαδικό αριθμό $w \in \mathbb{C}\smallsetminus\{0\}$ η πλευρική κλάση

$$\begin{aligned} w\mathbb{S}^1 &= [w]_{\mathbb{S}^1\mathcal{R}} = \{\,z \in \mathbb{C}\smallsetminus\{0\} \mid (z,w) \in {}_{\mathbb{S}^1}\mathcal{R}\} = \left\{\,z \in \mathbb{C}\smallsetminus\{0\} \mid z^{-1}w \in \mathbb{S}^1\right\} \\ &= \left\{\,z \in \mathbb{C}\smallsetminus\{0\} \mid |z^{-1}w| = 1\right\} = \{\,z \in \mathbb{C}\smallsetminus\{0\} \mid |z| = |w|\} \end{aligned}$$

είναι η περιφέρεια κύκλου κέντρου $0 \in \mathbb{C}$ και ακτίνας $|w|$. (Βλ. κάτωθι σχήμα όταν $|w| > 1$, όπου ο εσωτερικός -εντόνως σημειούμενος- κύκλος είναι ο $\mathbb{S}^1$.)



Επομένως, τα στοιχεία τής $(\mathbb{C}\smallsetminus\{0\})/\mathbb{S}^1$ είναι οι ομόκεντροι κύκλοι κέντρου $0 \in \mathbb{C}$ και θετικής ακτίνας, και η ίδια είναι ισόμορφη[17] τής $(\mathbb{R}_{>0},\cdot)$.

5.4.7 Παράδειγμα. Η ομάδα $(\mathbb{Z},+)$ είναι ορθόθετη υποομάδα τής ομάδας $(\mathbb{Q},+)$ (βλ. 5.2.6). Το υποκείμενο σύνολο τής πηλικοομάδας $(\mathbb{Q}/\mathbb{Z},+)$ γράφεται ως εξής:

$$\mathbb{Q}/\mathbb{Z} = \coprod \{\,\lambda + \mathbb{Z} \mid \lambda \in \mathbb{Q} \cap [0,1)\}\,,$$

[16] Όταν χρησιμοποιούμε *προσθετικό συμβολισμό*, γράφουμε αντ' αυτού $(g+H)+(g'+H)$.

[17] Η απεικόνιση $\mathbb{C}\smallsetminus\{0\}/\mathbb{S}^1 \ni w\mathbb{S}^1 \longmapsto |w| \in \mathbb{R}_{>0}$ είναι ισομορφισμός ομάδων.

οπότε το $\mathbb{Q}\cap[0,1)$ αποτελεί ένα σύστημα αριστερών εκπροσώπων τής $\mathbb{Z}$ εντός τής $\mathbb{Q}$ (και, ως εκ τούτου, $|\mathbb{Q}/\mathbb{Z}| = \mathrm{card}(\mathbb{Q}\cap[0,1)) = \aleph_0$). Πράγματι· για οιονδήποτε $\xi\in\mathbb{Q}$ υπάρχουν $a,b\in\mathbb{Z}$, $b>0$, τέτοιοι ώστε να ισχύει η ισότητα $\xi=\frac{a}{b}$, καθώς και $q,r\in\mathbb{Z}$ με $0\leqslant r<b$, τέτοιοι ώστε να ισχύει η ισότητα $a=bq+r$. Θέτοντας $\lambda:=\frac{r}{b}\in\mathbb{Q}\cap[0,1)$ διαπιστώνουμε ότι

$$\xi=\frac{a}{b}=q+\lambda\Rightarrow\xi-\lambda=q\in\mathbb{Z}\Rightarrow\xi+\mathbb{Z}=\lambda+\mathbb{Z}.$$

Επιπροσθέτως, εάν $\lambda_1,\lambda_2\in\mathbb{Q}\cap[0,1)$ με $\lambda_1\neq\lambda_2$, τότε $\lambda_1+\mathbb{Z}\neq\lambda_2+\mathbb{Z}$, διότι αλλιώς καταλήγουμε σε άτοπο, αφού η ισότητα

$$\lambda_1+\mathbb{Z}=\lambda_2+\mathbb{Z}\Rightarrow\exists c\in\mathbb{Z}\smallsetminus\{0\}:\lambda_1-\lambda_2=c$$

σημαίνει ότι $|\lambda_1-\lambda_2|=|c|\geqslant 1$ (πράγμα αδύνατο, καθόσον $0\leqslant\lambda_1,\lambda_2<1$).

5.4.8 Παράδειγμα. Έστω n ένας φυσικός αριθμός $\geqslant 3$ και έστω $\mathbf{D}_n=\langle\alpha,\beta\rangle$ η n-οστή διεδρική ομάδα (βλ. 4.4.4). Ως γνωστόν, $\langle\beta\rangle\lhd\mathbf{D}_n$ (βλ. 5.2.15). Η πηλικοομάδα $\mathbf{D}_n/\langle\beta\rangle$ έχει τάξη

$$|\mathbf{D}_n/\langle\beta\rangle|=\frac{|\mathbf{D}_n|}{|\langle\beta\rangle|}=\frac{2n}{n}=2,$$

οπότε είναι κυκλική (και, κατ' επέκταση, αβελιανή, βλ. 3.3.17). Κατά συνέπειαν, το αντίστροφο τού (ii) τής προτάσεως 5.4.2 δεν είναι πάντοτε ορθό (διότι η ίδια η $\mathbf{D}_n$ δεν είναι αβελιανή).

5.4.9 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H\trianglelefteqslant G$. Τότε για τις δυνάμεις των στοιχείων τής πηλικοομάδας G/H ισχύει η ισότητα*

$$(gH)^n=g^nH,\ \forall g\in G\ \textit{και}\ \ \forall n\in\mathbb{Z}.$$

Απόδειξη. Όταν $n=0$ ή $n=1$ η ισότητα είναι προφανής. Για $n\in\mathbb{N}$ εργαζόμαστε με τη βοήθεια τής κλασικής μαθηματικής επαγωγής. Ας υποθέσουμε ότι η εν λόγω ισότητα ισχύει για κάποιον φυσικό αριθμό $n\geqslant 1$. Τότε

$$(gH)^{n+1}=\ (gH)^n(gH)=(g^nH)(gH)=(g^ngH)=g^{n+1}H.$$

Εάν $n\in\mathbb{Z}\smallsetminus\mathbb{N}_0$, τότε $-n>0$, οπότε εφαρμόζοντας το ανωτέρω αποδειχθέν για τον $-n$, το (i) τής προτάσεως 5.4.2, καθώς και το (iii) τής προτάσεως 3.2.11, λαμβάνουμε

$$(gH)^n=\ ((gH)^{-1})^{-n}=(g^{-1}H)^{-n}=(g^{-1})^{-n}H=g^nH.$$

Τελικώς λοιπόν, $(gH)^n=g^nH,\ \forall g\in G$ και $\forall n\in\mathbb{Z}$. □

5.4.10 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H\trianglelefteqslant G$. Για οιοδήποτε $g\in G$ η τάξη τού στοιχείου gH τής G/H ισούται με*

$$\mathrm{ord}(gH)=\begin{cases}\infty, & \text{όταν } g^k\notin H,\ \forall k\in\mathbb{N},\\ \min\{k\in\mathbb{N}\mid g^k\in H\}, & \text{στην αντίθετη περίπτωση.}\end{cases}$$

Απόδειξη. Έστω τυχόν στοιχείο $g\in G$. Εάν $g^k\notin H$ για κάθε $k\in\mathbb{N}$, τότε έχουμε $g^kH=(gH)^k\neq H,\ \forall k\in\mathbb{N}$, οπότε $\mathrm{ord}(gH)=\infty$. Εάν $\{k\in\mathbb{N}\mid g^k\in H\}\neq\varnothing$ και

$$m:=\min\{k\in\mathbb{N}\mid g^k\in H\},$$

τότε $m=\min\{k\in\mathbb{N}\mid (gH)^k=H\}=\mathrm{ord}(gH)$. □

5.4.11 Παράδειγμα. Η πηλικοομάδα $(\mathbb{Q}/\mathbb{Z},+)$ (βλ. 5.4.7) είναι περιοδική. Πράγματι· για οιονδήποτε $\xi\in\mathbb{Q}$ υπάρχουν $a,b\in\mathbb{Z}$, $b>0$, τέτοιοι ώστε να ισχύει η ισότητα $\xi=\frac{a}{b}$. Από τις προτάσεις 5.4.9 και 5.4.10 έπεται ότι

$$b(\xi+\mathbb{Z})=b\xi+\mathbb{Z}=a+\mathbb{Z}=\mathbb{Z}\Rightarrow b\xi\in\mathbb{Z}\Rightarrow\ \mathrm{ord}(\xi+\mathbb{Z})\leqslant b<\infty.$$

5.4.12 Πρόταση. *Εάν $(G,\cdot)$ είναι μια πεπερασμένη ομάδα, τότε*

$$\exp(G/H) \mid \exp(G),\ \forall H \in \mathbf{NSubg}(G).$$

Απόδειξη. Εάν $H \trianglelefteq G$ και $g \in H$, τότε για την πλευρική κλάση gH έχουμε

$$(gH)^{\mathrm{ord}(g)} = g^{\mathrm{ord}(g)}H = e_G H = H = e_{G/H} \Longrightarrow \mathrm{ord}(gH) \mid \mathrm{ord}(g).$$

Εξ αυτού έπεται ότι

$$\exp(G/H) = \text{εκπ}(\{\,\mathrm{ord}(gH) \,|\, g \in G\}) \mid \text{εκπ}(\{\,\mathrm{ord}(g) \,|\, g \in G\}) = \exp(G).$$

(Βλ. το (i) τής προτάσεως 3.4.25.) □

▸ **Ιδιότητες τού φυσικού επιμορφισμού.** Τα στοιχεία δοθείσας πηλικοομάδας G/H είναι οι εικόνες των στοιχείων τής G μέσω τού επιμορφισμού (5.31). Η μελέτη των ιδιοτήτων του είναι, ως εκ τούτου, απαραίτητη για την ομαδοθεωρητική περιγραφή τής ίδιας τής G/H.

5.4.13 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \trianglelefteq G$. Η φυσική επίρριψη*

$$\boxed{\pi_H^G : G \longrightarrow G/H,\ \ g \longmapsto \pi_H^G(g) := gH,} \tag{5.31}$$

(βλ. 5.4.1) *είναι ένας επιμορφισμός ομάδων έχων την H ως πυρήνα του και (γι' αυτόν τον λόγο) καλείται, ιδιαιτέρως,* **φυσικός επιμορφισμός** *τής G επί τής G/H.*

Απόδειξη. Αρκεί να αποδείξουμε ότι η π_H^G είναι ομομορφισμός ομάδων και ότι $\mathrm{Ker}(\pi_H^G) = H$. Για οιαδήποτε στοιχεία $g, g' \in G$ έχουμε

$$\pi_H^G(gg') = (gg')H = (gH)\,(g'H) = \pi_H^G(g)\pi_H^G(g').$$

Εξάλλου, $\mathrm{Ker}(\pi_H^G) = \{g \in G \,|\, \pi_H^G(g) = H\} = \{g \in G \,|\, gH = H\} = H$. □

5.4.14 Πόρισμα. *Έστω υποομάδα H μιας ομάδας $(G,\cdot)$. Τότε $H \trianglelefteq G$ εάν και μόνον εάν η H αποτελεί τον πυρήνα ενός ομομορφισμού $f : (G,\cdot) \longrightarrow (K,*)$.*

Απόδειξη. Έπεται άμεσα από την πρόταση 5.4.13 και το πόρισμα 5.2.31. □

5.4.15 Πόρισμα (Θεώρημα αντιστοιχίσεως υποομάδων μέσω τού π_H^G). *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \trianglelefteq G$. Τότε ορίζεται η αμφιρριπτική απεικόνιση*

$$\boxed{\mathbf{Subg}(G;H) \ni K \overset{\bar{\Psi}_{\pi_H^G}}{\longmapsto} \pi_H^G(K) \in \mathbf{Subg}(G/H)}$$

από το σύνολο $\mathbf{Subg}(G;H)$ των υποομάδων τής G που περιέχουν την H επί τού συνόλου $\mathbf{Subg}(G/H)$ των υποομάδων τής πηλικοομάδας G/H. Ως εκ τούτου, κάθε υποομάδα τής πηλικοομάδας G/H οφείλει να είναι τής μορφής $\pi_H^G(K) = K/H$, όπου K μια υποομάδα τής G που περιέχει την H. Επιπροσθέτως, ισχύουν τα ακόλουθα:

(i) *Για $K_1, K_2 \in \mathbf{Subg}(G;H)$ αληθεύει η κάτωθι αμφίπλευρη συνεπαγωγή*

$$K_1 \sqsubseteq K_2 \Longleftrightarrow K_1/H \sqsubseteq K_2/H.$$

(ii) *Η $\bar{\Psi}_{\pi_H^G}$ καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων*

$$(\mathbf{Subg}(G;H), \sqsubseteq) \quad \textit{και} \quad (\mathbf{Subg}(G/H), \sqsubseteq)$$

(βλ. 3.2.30, 3.2.32, και 1.4.26).

(iii) $(K_1 \cap K_2)/H = (K_1/H) \cap (K_2/H)\,,\ \forall\,(K_1,K_2) \in \mathbf{Subg}(G;H)^2$.

(iv) $\langle K_1, K_2\rangle/H = \langle K_1/H, K_2/H\rangle\,,\ \forall\,(K_1,K_2) \in \mathbf{Subg}(G;H)^2$.

(v) *Για* $K_1, K_2 \in \mathbf{Subg}(G;H)$ *με* $K_1 \sqsubseteq K_2$ *ισχύει η ισότητα*

$$|K_2 : K_1| = |K_2/H : K_1/H|.$$

(vi) *Για* $L_1, L_2 \in \mathbf{Subg}(G/H)$ *με* $L_1 \sqsubseteq L_2$ *ισχύει η ισότητα*

$$|L_2 : L_1| = |(\pi_H^G)^{-1}(L_2) : (\pi_H^G)^{-1}(L_1)|.$$

Απόδειξη. Για κάθε υποομάδα K τής G που περιέχει την H έχουμε $H \trianglelefteq K$ (λόγω τής προτάσεως 5.2.19, ύστερα από εναλλαγή των ρόλων των σε αυτήν παρατεθειμένων υποομάδων H και K), οπότε η εικόνα $\pi_H^G(K)$ τής K μέσω τού φυσικού επιμορφισμού (5.31) είναι αφ' εαυτής *πηλικοομάδα*. Το πόρισμα έπεται άμεσα ύστερα από εφαρμογή τού 2ου θεωρήματος αντιστοιχίας υποομάδων 3.5.20, τής προτάσεως 5.1.57 και τού πορίσματος 5.1.58 για τον φυσικό επιμορφισμό (5.31). □

5.4.16 Πρόταση. *Έστω* $(G,\cdot)$ *μια ομάδα και έστω* $H \trianglelefteq G$. *Εάν ένα στοιχείο* $g \in G$ *έχει τάξη* $\mathrm{ord}(g) = n \in \mathbb{N}$, *τότε* $\mathrm{ord}(gH) = m \in \mathbb{N}$ *και* $m \mid n$.

Απόδειξη. Αρκεί να εφαρμοσθεί το (iv) τής προτάσεως 3.5.3 για τον φυσικό επιμορφισμό (5.31). □

5.4.17 Παράδειγμα. Εάν θεωρήσουμε την υποομάδα $H := \langle \mathbf{i}\rangle$ τής ομάδας $\mathbf{Q}$ των τετρανίων (βλ. 3.3.11), τότε είναι προφανές ότι $H \lhd \mathbf{Q}$, $\mathbf{Q}/H = \{H, \mathbf{j}H\}$ και ότι η πλευρική κλάση

$$\mathbf{j}H = \{\mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\}$$

(ως στοιχείο τής $\mathbf{Q}/H$) έχει τάξη 2, ενώ το $\mathbf{j}$ (εντός τής $\mathbf{Q}$) έχει τάξη 4.

5.4.18 Πρόταση. *Έστω* X *ένα σύστημα γεννητόρων μιας ομάδας* $(G,\cdot)$ *και έστω* $H \trianglelefteq G$. *Τότε*

$$\boxed{G/H = \langle \{\, xH \mid x \in X\}\rangle\,.}$$

Απόδειξη. Σύμφωνα με το 3.5.6 (i),

$$G/H = \pi_H^G(G) = \pi_H^G(\langle X\rangle) = \left\langle \pi_H^G(X)\right\rangle,$$

όπου $\pi_H^G(X) = \left\{\, \pi_H^G(x) \;\middle|\; x \in X\right\} = \{\, xH \mid x \in X\}$. □

5.4.19 Πόρισμα. *Έστω* H *μια υποομάδα μιας κυκλικής ομάδας* $(G,\cdot)$. *Τότε η πηλικοομάδα* G/H *είναι κυκλική. Ειδικότερα, για κάθε γεννήτορα* g *τής* G *έχουμε* $G/H = \langle gH\rangle$.

Απόδειξη. Η G ως κυκλική είναι αβελιανή (βλ. 3.3.17), οπότε η H είναι ορθόθετη (βλ. 5.2.6). Ως εκ τούτου, ορίζεται η πηλικομάδα G/H. Αρκεί λοιπόν να εφαρμοσθεί η πρόταση 5.4.18 για το $X = \{g\}$, όπου g οιοσδήποτε γεννήτορας τής G. □

5.4.20 Παρατήρηση. Εάν η H είναι μια ορθόθετη κυκλική υποομάδα μιας ομάδας $(G,\cdot)$, τότε η πηλικοομάδα G/H *δεν είναι κατ' ανάγκην κυκλική*. Επί παραδείγματι, θεωρώντας τή διεδρική ομάδα $\mathbf{D}_4 = \langle \alpha, \beta\rangle$ και την $\left\langle \beta^2\right\rangle \lhd \mathbf{D}_4$, παρατηρούμε ότι

$$\begin{aligned} \mathbf{D}_4/\left\langle \beta^2\right\rangle &= \left\langle \left\{\, x\left\langle \beta^2\right\rangle \;\middle|\; x \in \{\alpha,\beta\}\right\}\right\rangle \\ &= \left\{\left\langle \beta^2\right\rangle, \alpha\circ\left\langle \beta^2\right\rangle, \beta\circ\left\langle \beta^2\right\rangle, (\alpha\circ\beta)\circ\left\langle \beta^2\right\rangle\right\} \end{aligned}$$

και ότι

$$\left(\alpha\circ\left\langle\beta^2\right\rangle\right)^2=\alpha^2\circ\left\langle\beta^2\right\rangle=\ \mathrm{id}_{\mathcal{E}_4}\circ\left\langle\beta^2\right\rangle=\left\langle\beta^2\right\rangle,\left(\beta\circ\left\langle\beta^2\right\rangle\right)^2=\beta^2\circ\left\langle\beta^2\right\rangle=\left\langle\beta^2\right\rangle$$

και

$$\begin{aligned}\left((\alpha\circ\beta)\circ\left\langle\beta^2\right\rangle\right)^2 &= (\alpha\circ\beta)^2\circ\left\langle\beta^2\right\rangle=(\alpha\circ(\beta\circ\alpha)\circ\beta)\circ\left\langle\beta^2\right\rangle\\ &= \left(\alpha\circ(\alpha\circ\beta^{-1})\circ\beta\right)\circ\left\langle\beta^2\right\rangle=\alpha^2\circ\left\langle\beta^2\right\rangle=\left\langle\beta^2\right\rangle.\end{aligned}$$

Άρα καθένα εκ των στοιχείων

$$\alpha\circ\left\langle\beta^2\right\rangle,\beta\circ\left\langle\beta^2\right\rangle,(\alpha\circ\beta)\circ\left\langle\beta^2\right\rangle$$

έχει τάξη 2. Αυτό σημαίνει ότι η πηλικοομάδα $\mathbf{D}_4/\left\langle\beta^2\right\rangle$ είναι αβελιανή *μη κυκλική* (και κατ' ανάγκην ισόμορφη με την ομάδα $\mathbf{V}$ των τεσσάρων στοιχείων τού Klein, βλ. 4.5.6).

‣ **Το «αντίστροφο» τού θεωρήματος τού Lagrange για αβελιανές ομάδες**. Εάν η $(G,\cdot)$ είναι οιαδήποτε πεπερασμένη αβελιανή ομάδα, τότε τα (ii) και (iii) τής προτάσεως 5.4.2, σε συνδυασμό με το θεώρημα 5.4.21, μας δίδουν τη δυνατότητα επαγωγικής αποδείξεως τής υπάρξεως μιας υποομάδας H τής G τάξεως $|H|=k$ *για κάθε* διαιρέτη k τής $|G|$.

5.4.21 Θεώρημα («Θεώρημα τού Cauchy για αβελιανές ομάδες»). *Έστω $(G,\cdot)$ μια πεπερασμένη αβελιανή ομάδα. Εάν $p\mid|G|$, όπου p κάποιος πρώτος αριθμός, τότε*

$$\exists g\in G\smallsetminus\{e_G\}:\mathrm{ord}(g)=p,$$

ήτοι η κυκλική ομάδα $\langle g\rangle$ είναι μια υποομάδα τής G τάξεως p (βλ. (3.10)).

Απόδειξη. Εξ υποθέσεως, $p\mid|G|$, οπότε

$$\exists n\in\mathbb{N}:|G|=pn.$$

Θα εφαρμόσουμε τη δεύτερη μορφή τής μαθηματικής επαγωγής ως προς τον n. Εάν $n=1$, τότε $|G|=p$ και $\mathrm{ord}(g)\mid p$ για κάθε $g\in G$ (βλ. 5.1.27), οπότε $\mathrm{ord}(g)=p$ για κάθε $g\in G\smallsetminus\{e_G\}$. Για $n>1$ υποθέτουμε ότι *κάθε αβελιανή ομάδα* H με $|H|=pk$, όπου $k\in\mathbb{N}$, $k<n$, διαθέτει κάποιο στοιχείο τάξεως p. Επειδή $n>1$, η G διαθέτει μη τετριμμένες γνήσιες υποομάδες (βλ. 5.1.35). Διακρίνουμε δύο περιπτώσεις:

Περίπτωση πρώτη. Η τάξη κάποιας εξ αυτών των υποομάδων, ας την πούμε K, διαιρείται διά τού p. Τότε

$$\exists k\in\mathbb{N},\ k<n:|K|=pk.$$

Κατά την επαγωγική μας υπόθεση, η K διαθέτει κάποιο στοιχείο g τάξεως p. Επειδή $g\in G$, ο ισχυρισμός είναι αληθής σε αυτήν την περίπτωση.

Περίπτωση δεύτερη. Ο p *δεν διαιρεί την τάξη καμίας* μη τετριμμένης γνήσιας υποομάδας τής G. Τότε για *οιαδήποτε* μη τετριμμένη γνήσια υποομάδα L τής G έχουμε

$$\left.\begin{aligned}|G|=pn=|G:L|\cdot|L|\\ p\nmid|L|\underset{2.3.17}{\Longrightarrow}\mu\kappa\delta(p,|L|)=1\end{aligned}\right\}\underset{2.2.9}{\Longrightarrow}p\mid|G:L|\Rightarrow\exists k\in\mathbb{N}:|G:L|=pk.$$

Επειδή η G είναι αβελιανή, $L\lhd G$ (βλ. 5.2.6). Επομένως ορίζεται η πηλικοομάδα G/L, η δε τάξη της ισούται με

$$|G/L|=|G:L|=pk$$

(βλ. 5.4.2), όπου $k < n$, διότι (εξ υποθέσεως) $|L| > 1$. Σύμφωνα με το (ii) τής προτάσεως 5.4.2 η πηλικοομάδα G/L είναι *αβελιανή*. Εφαρμόζοντας την επαγωγική μας υπόθεση γι' αυτήν, κατοχυρώνουμε την ύπαρξη ενός στοιχείου $gL \in G/L$ (για κάποιο $g \in G$) τάξεως p (εντός τής G/L!). Αυτό σημαίνει ότι

$$g^p L = (gL)^p = e_{G/L} = L \Rightarrow g^p \in L \underset{5.1.28}{\Longrightarrow} (g^p)^{|L|} = e_G = (g^{|L|})^p \underset{3.4.8}{\Longrightarrow} \mathrm{ord}(g^{|L|}) \mid p,$$

σχέση από την οποία έπεται ότι

$$\mathrm{ord}(g^{|L|}) \in \{1, p\}.$$

Το ενδεχόμενο να ισχύει η ισότητα

$$\mathrm{ord}(g^{|L|}) = 1 \ (\Leftrightarrow g^{|L|} = e_G)$$

αποκλείεται, διότι εν τοιαύτη περιπτώσει θα καταλήγαμε στην ακόλουθη αντίφαση:

$$(gL)^{|L|} = g^{|L|}L = e_G L = L = e_{G/L} \underset{5.1.27}{\Longrightarrow} p \mid |L|\,.$$

Επομένως, $g^{|L|} \in G$ με $\mathrm{ord}(g^{|L|}) = p$. □

5.4.22 Θεώρημα («Το αντίστροφο τού θεωρήματος τού Lagrange για αβελιανές ομάδες»). *Έστω $(G, \cdot)$ μια αβελιανή ομάδα τάξεως $|G| = m \in \mathbb{N}$. Τότε για κάθε $k \in \mathbb{N}$ με $k \mid m$ υπάρχει μια υποομάδα H τής G τάξεως $|H| = k$.*

Απόδειξη. Θα εφαρμόσουμε τη δεύτερη μορφή τής μαθηματικής επαγωγής ως προς τον m. Για $m = 1$ ο ισχυρισμός είναι προφανώς αληθής. Για $m > 1$ υποθέτουμε ότι αυτός είναι αληθής για *κάθε αβελιανή ομάδα τάξεως* $< m$. Εάν $k = 1$, τότε λαμβάνουμε ως H την τετριμμένη υποομάδα τής G. Εάν $k > 1$, τότε υπάρχει κάποιος πρώτος αριθμός p που διαιρεί τον k. Κατά το θεώρημα 5.4.21,

$$\exists g \in G \setminus \{e_G\} : \mathrm{ord}(g) = |\langle g \rangle| = p.$$

Επειδή η G είναι αβελιανή, $\langle g \rangle \trianglelefteq G$ (βλ. 5.2.6). Επομένως ορίζεται η πηλικοομάδα $G/\langle g \rangle$, η δε τάξη της ισούται με

$$|G/\langle g \rangle| = \frac{m}{p}$$

(βλ. 5.4.2 (iii)). Σύμφωνα με το (ii) τής προτάσεως 5.4.2 η πηλικοομάδα $G/\langle g \rangle$ είναι *αβελιανή*. Εφαρμόζοντας την επαγωγική μας υπόθεση γι' αυτήν, κατοχυρώνουμε την ύπαρξη μιας υποομάδας K τής $G/\langle g \rangle$ τάξεως $|K| = \frac{k}{p}$ (αφού $\frac{k}{p} \mid \frac{m}{p}$). Κατά το (ii) τής προτάσεως 3.5.17,

$$(\pi^G_{\langle g \rangle})^{-1}(K) \sqsubseteq G,$$

όπου $\pi^G_{\langle g \rangle} : G \longrightarrow G/\langle g \rangle$ ο φυσικός επιμορφισμός τής G επί τής $G/\langle g \rangle$. Από το (ii) τού πορίσματος 5.1.13 συνάγεται ότι

$$\left|(\pi^G_{\langle g \rangle})^{-1}(K)\right| = \left|\mathrm{Ker}(\pi^G_{\langle g \rangle})\right| \cdot |K| = |\langle g \rangle| \cdot |K| = p \cdot \frac{k}{p} = k.$$

Αυτό σημαίνει ότι ο ισχυρισμός είναι και σε αυτήν την περίπτωση αληθής (καθόσον είναι αρκετό να επιλέξουμε ως H την $(\pi^G_{\langle g \rangle})^{-1}(K)$). □

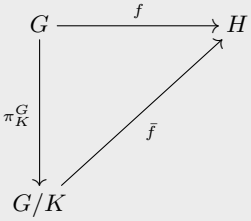
5.5 ΘΕΩΡΗΜΑΤΑ ΙΣΟΜΟΡΦΙΣΜΩΝ ΟΜΑΔΩΝ

Αυτά είναι ορισμένα χαρακτηριστικά θεωρήματα που περιγράφουν τον τρόπο διασυνδέσεως των ομομορφισμών ομάδων, των ορθόθετων υποομάδων και των πηλικοομάδων.

5.5.1 Θεώρημα (Θεμελιώδες θεώρημα περί πηλικοομάδων). *Έστω*

$$f : (G, \cdot) \longrightarrow (H, *)$$

ένας ομομορφισμός ομάδων και έστω $K \trianglelefteq G$. Τότε υφίσταται ένας και μόνον ομομορφισμός $\bar{f} : G/K \longrightarrow H$, τέτοιος ώστε να ισχύει $f = \bar{f} \circ \pi_K^G$, δηλαδή τέτοιος ώστε το διάγραμμα



(5.32)

να καθίσταται μεταθετικό, εάν και μόνον εάν $K \subseteq \mathrm{Ker}(f)$. Ο εν λόγω ομομορφισμός ορίζεται μέσω τού τύπου

$$\boxed{\bar{f}(gK) := f(g), \ \ \forall g \in G.} \tag{5.33}$$

Επιπροσθέτως, όταν $K \subseteq \mathrm{Ker}(f)$ ισχύουν τα ακόλουθα:

(i) $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f)$. (*Ως εκ τούτου, ο $\bar{f}$ είναι επιμορφισμός εάν και μόνον εάν ο f είναι επιμορφισμός.*)

(ii) $\mathrm{Ker}(\bar{f}) = \mathrm{Ker}(f)/K$.

(iii) *Ο $\bar{f}$ είναι μονομορφισμός εάν και μόνον εάν $K = \mathrm{Ker}(f)$.*

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς υποθέτουμε ότι ισχύει ο εγκλεισμός $K \subseteq \mathrm{Ker}(f)$ και ορίζουμε την $\bar{f} : G/K \longrightarrow H$ μέσω τού τύπου (5.33). Επειδή το σύνολο $[g]_{K\mathcal{R}} = gK$ δεν είναι μονοσημάντως ορισμένο από το g, οφείλουμε εν πρώτοις να αποδείξουμε ότι η $\bar{f}$ είναι *καλώς ορισμένη* απεικόνιση, ήτοι ότι για κάθε $g_1, g_2 \in G$ ισχύει η συνεπαγωγή $g_1K = g_2K \Rightarrow \bar{f}(g_1K) = \bar{f}(g_2K)$. Ας υποθέσουμε λοιπόν ότι $g_1, g_2 \in G$ με $g_1K = g_2K$. Τότε

$$g_1^{-1}g_2 \in K \subseteq \mathrm{Ker}(f) \Rightarrow f(g_1^{-1}g_2) = f(g_1)^{-1} * f(g_2) = e_H.$$

Κατόπιν «πολλαπλασιασμού» αμφοτέρων των μελών τής τελευταίας ισότητας εξ αριστερών με το $f(g_1)$ λαμβάνουμε $f(g_1) = f(g_2)$, απ' όπου έπεται η ζητούμενη ισότητα $\bar{f}(g_1K) = \bar{f}(g_2K)$ είναι ομομορφισμός ομάδων, διότι για οιαδήποτε στοιχεία $g_1, g_2 \in G$ έχουμε

$$\bar{f}(g_1K) * \bar{f}(g_2K) = f(g_1) * f(g_2) = f(g_1g_2) = \bar{f}((g_1g_2)\,K) = \bar{f}((g_1K)(g_2K)).$$

Εξάλλου,

$$(\bar{f} \circ \pi_K^G)(g) = \bar{f}(\pi_K^G(g)) = \bar{f}(gK) = f(g), \ \forall g \in G \Rightarrow f = \bar{f} \circ \pi_K^G.$$

Έστω τώρα $f' : G/K \longrightarrow H$ οιοσδήποτε ομομορφισμός ομάδων για τον οποίο ισχύει $f = f' \circ \pi_K^G$. Είναι πρόδηλο ότι

$$f'(gK) = f'(\pi_K^G(g)) = f(g) = \bar{f}(\pi_K^G(g)) = \bar{f}(gK), \ \forall g \in G \Rightarrow f' = \bar{f}.$$

Άρα ο $\bar{f}$ είναι ο μοναδικός ομομορφισμός που καθιστά το διάγραμμα (5.32) μεταθετικό. Και αντιστρόφως· εάν ο $\bar{f} : G/K \longrightarrow H$ είναι ο μόνος ομομορφισμός που καθιστά το διάγραμμα (5.32) μεταθετικό, τότε για οιοδήποτε $x \in K$ έχουμε

$$f(x) = (\bar{f} \circ \pi_K^G)(x) = \bar{f}(xK) = \bar{f}(K) = \bar{f}(e_{G/K}) = e_H \Rightarrow x \in \mathrm{Ker}(f),$$

οπότε $K \subseteq \mathrm{Ker}(f)$. Επιπροσθέτως, όταν $K \subseteq \mathrm{Ker}(f)$ ισχύουν τα ακόλουθα:

(i) Εκ κατασκευής, $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f)$.

(ii) Κατ' αρχάς παρατηρούμε ότι

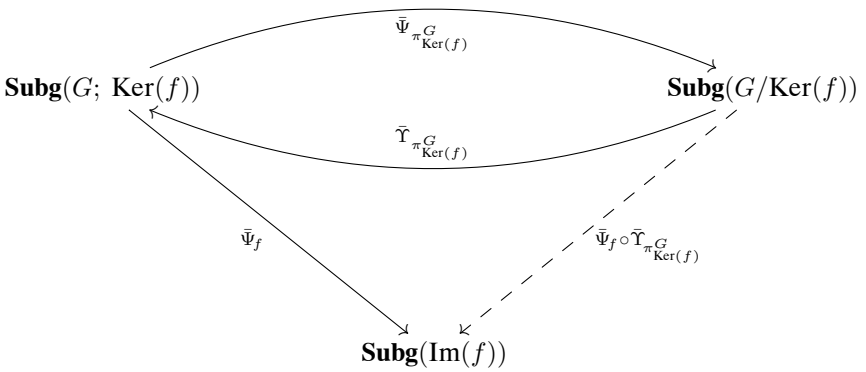
$$\left.\begin{array}{l} \mathrm{Ker}(f) \sqsubseteq G \\ K \subseteq \mathrm{Ker}(f) \end{array}\right\} \underset{3.2.20}{\Longrightarrow} K \sqsubseteq \mathrm{Ker}(f).$$

Επειδή εξ υποθέσεως $K \trianglelefteq G$ και $K \sqsubseteq \mathrm{Ker}(f)$, η πρόταση 5.2.19 μας πληροφορεί ότι $K \trianglelefteq \mathrm{Ker}(f)$. Κατά συνέπειαν, ορίζεται η πηλικομάδα $\mathrm{Ker}(f)/K$. Προφανώς,

$$\begin{aligned} \mathrm{Ker}(f)/K &= \{gK \,|g \in \mathrm{Ker}(f)\} = \{gK \,|f(g) = e_H\} \\ &= \left\{gK \,|\bar{f}(\pi_K^G(g)) = e_H\right\} = \left\{gK \,|\bar{f}(gK) = e_H\right\} = \mathrm{Ker}(\bar{f}). \end{aligned}$$

(iii) Το ότι ο $\bar{f}$ είναι μονομορφισμός $\Leftrightarrow K = \mathrm{Ker}(f)$ είναι άμεση συνέπεια τού (ii) και τής προτάσεως 3.5.12. □

5.5.2 Παρατήρηση. Σε επίπεδο υποομάδων τα πορίσματα 3.5.20 και 5.4.15 και το θεώρημα 5.5.1 δίδουν τους εξής ισομορφισμούς συνδέσμων:



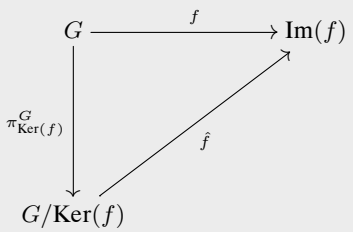
όπου για κάθε $K \in$ **Subg**$(G; \mathrm{Ker}(f))$ έχουμε

$$\textbf{Subg}(G/\mathrm{Ker}(f)) \ni G/K \longmapsto (\bar{\Psi}_f \circ \bar{\Upsilon}_{\pi^G_{\mathrm{Ker}(f)}})(G/K) = \bar{\Psi}_f(K) = f(K) \in \textbf{Subg}(\mathrm{Im}(f)).$$

5.5.3 Πρώτο Θεώρημα Ισομορφισμών. *Εάν $f : (G, \cdot) \longrightarrow (H, *)$ είναι ένας ομομορφισμός ομάδων, τότε υφίσταται μία και μόνον απεικόνιση*

$$\hat{f} : G/\mathrm{Ker}(f) \longrightarrow \mathrm{Im}\,(f)\,,$$

τέτοια ώστε το διάγραμμα



να καθίσταται μεταθετικό. Η απεικόνιση αυτή ορίζεται μέσω τού τύπου

$$\boxed{\hat{f}(g\mathrm{Ker}(f)) := f(g),\ \ \forall g \in G,}$$

και αποτελεί ισομορφισμό ομάδων. Ως εκ τούτου,

$$\boxed{G/\mathrm{Ker}(f) \cong \mathrm{Im}\,(f)\,.}$$

Απόδειξη. Εφαρμόζοντας το θεώρημα 5.5.1 στην περίπτωση όπου $K = \mathrm{Ker}(f)$ αποκτούμε τον μονομορφισμό ομάδων

$$\bar{f} : G/\mathrm{Ker}(f) \longrightarrow H,\ \ g\mathrm{Ker}(f) \longmapsto \bar{f}(g\mathrm{Ker}(f)) := f(x),$$

με $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f)$. Αρκεί λοιπόν να ορίσουμε τον $\hat{f}$ ως τον $\bar{f}$ *ύστερα από περιορισμό τού πεδίου τιμών του H στο σύνολο* $\mathrm{Im}(f) \subseteq H$. □

5.5.4 Παραδείγματα. (i) Η απεικόνιση $(\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_n, +),\ \ k \longmapsto [k]_n$, όπου $n \in \mathbb{N}$, είναι ένας επιμορφισμός με πυρήνα του την $n\mathbb{Z}$ (βλ. 3.2.21 (iii)). Συνεπώς,

$$\boxed{\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.}$$

Γενικότερα, εάν $m, n \in \mathbb{N}$ και $m \mid n$, τότε $n\mathbb{Z} \trianglelefteq m\mathbb{Z}$ (βλ. 3.3.20 (i) και 5.2.6) και ορίζεται η πηλικοομάδα $m\mathbb{Z}/n\mathbb{Z}$. Η

$$(m\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_{\frac{n}{m}}, +),\ mk \longmapsto [k]_{\frac{n}{m}},$$

είναι ένας επιμορφισμός ομάδων με πυρήνα του την υποομάδα

$$\{\, mk |\, k \in \mathbb{Z} : [k]_{\frac{n}{m}} = [0]_{\frac{n}{m}}\} = \{\, mk |\, k \in \mathbb{Z} :\ \tfrac{n}{m} \mid k\} = \{\, mk |\, k \in \tfrac{n}{m}\mathbb{Z}\} = n\mathbb{Z}$$

τής ομάδας $m\mathbb{Z}$. Συνεπώς,

$$\boxed{m\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_{\frac{n}{m}}.} \tag{5.34}$$

(ii) Η απεικόνιση

$$(\mathbb{R}, +) \longrightarrow (\mathbb{S}^1, \cdot),\ \ x \longmapsto \exp(2\pi i x),$$

είναι ένας επιμορφισμός ομάδων με πυρήνα του την ομάδα $(\mathbb{Z}, +)$, οπότε

$$\boxed{\mathbb{R}/\mathbb{Z} \cong \mathbb{S}^1.}$$

(iii) Ο επιμορφισμός πολλαπλασιαστικών ομάδων

$$(\mathbb{C}\smallsetminus\{0\}, \cdot) \longrightarrow (\mathbb{S}^1, \cdot),\ \ z \longmapsto \frac{z}{|z|},$$

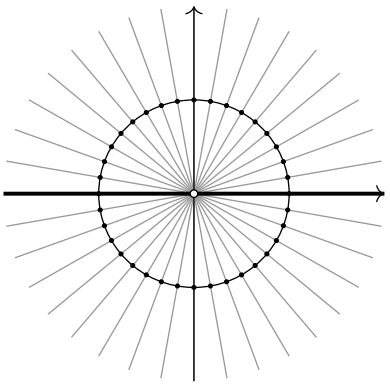
γνωστός και ως *ακτινική προβολή*, έχει ως πυρήνα του την $(\mathbb{R}_{>0}, \cdot)$. Άρα

$$\boxed{(\mathbb{C}\smallsetminus\{0\})/\mathbb{R}_{>0} \cong \mathbb{S}^1.} \tag{5.35}$$

Τα στοιχεία τής πηλικοομάδας $(\mathbb{C}\smallsetminus\{0\})/\mathbb{R}_{>0}$ είναι οι πλευρικές κλάσεις $\mathbb{R}_{>0}w$, $w \in \mathbb{C}\smallsetminus\{0\}$. Συγκεκριμένα, για οιονδήποτε μιγαδικό αριθμό $w \in \mathbb{C}\smallsetminus\{0\}$ η πλευρική κλάση

$$\begin{aligned}\mathbb{R}_{>0}w &= [w]_{\mathcal{R}_{\mathbb{R}_{>0}}} := \{\, z \in \mathbb{C}\smallsetminus\{0\} |\, (z, w) \in \mathcal{R}_{\mathbb{R}_{>0}}\} = \{\, z \in \mathbb{C}\smallsetminus\{0\} |\, zw^{-1} \in \mathbb{R}_{>0}\} \\ &= \{\, z \in \mathbb{C}\smallsetminus\{0\} |\, \exists r \in \mathbb{R}_{>0} : zw^{-1} = r\} = \{\, z \in \mathbb{C}\smallsetminus\{0\} |\, \exists r \in \mathbb{R}_{>0} : z = rw\}\end{aligned}$$

είναι η ημιευθεία που ξεκινά από το $0 \in \mathbb{C}$ και διέρχεται από τον w. Μέσω τού ισομορφισμού (5.35) επέρχεται ταύτιση καθεμιάς εξ αυτών των ημιευθειών με το σημείο τομής της με τον μοναδιαίο κύκλο $\mathbb{S}^1$, όπως στο σχήμα:



(iv) Η πηλικοομάδα μιας *άπειρης* ομάδας ως προς μια μη τετριμμένη υποομάδα της ενδέχεται να είναι ισόμορφη με την ίδια την ομάδα αναφοράς! Επί παραδείγματι, ο επιμορφισμός $(\mathbb{S}^1, \cdot) \longrightarrow (\mathbb{S}^1, \cdot)$, $z \longmapsto z^2$, μας οδηγεί σε ισομορφισμό

$$\boxed{\mathbb{S}^1/\{\pm 1\} \xrightarrow{\cong} \mathbb{S}^1.}$$

(v) Μέσω τού επιμορφισμού 5.2.32 (i) κατασκευάζεται ισομορφισμός

$$\boxed{\mathfrak{S}_n/\mathfrak{A}_n \xrightarrow{\cong} \{\pm 1\}.}$$

(vi) Μέσω τού επιμορφισμού 5.2.32 (ii) κατασκευάζεται ισομορφισμός

$$\boxed{\mathrm{GL}_n(R)/\mathrm{SL}_n(R) \xrightarrow{\cong} R^\times.}$$

(vii) Μέσω τού επιμορφισμού 5.2.32 (iii) κατασκευάζεται ισομορφισμός

$$\boxed{\mathrm{O}_n(\mathbb{R})/\mathrm{SO}_n(\mathbb{R}) \xrightarrow{\cong} \{\pm 1\}.}$$

(viii) Μέσω τού επιμορφισμού 5.2.32 (iv) κατασκευάζεται ισομορφισμός

$$\boxed{\mathrm{U}_n(\mathbb{C})/\mathrm{SU}_n(\mathbb{C}) \xrightarrow{\cong} \mathbb{S}^1.}$$

5.5.5 Πόρισμα. *Έστω $f : (G, \cdot) \longrightarrow (H, *)$ ένας ομομορφισμός πεπερασμένων ομάδων. Εάν $K \sqsubseteq G$, τότε ισχύουν τα ακόλουθα*:
(i) $|K| = |f(K)|\,|\mathrm{Ker}(f|_K)|$.
(ii) $|G| = |\mathrm{Im}(f)|\,|\mathrm{Ker}(f)|$.
(iii) $|G : K| = |\mathrm{Im}(f) : f(K)|\,|\mathrm{Ker}(f) : \mathrm{Ker}(f|_K)|$.

Απόδειξη. (i) Ύστερα από περιορισμό τού πεδίου τιμών τής απεικονίσεως $f|_K$ στο $f(K)$ προκύπτει ένας επιμορφισμός ομάδων

$$(f|_K)^\wedge : K \longrightarrow f(K),\ x \longmapsto (f|_K)^\wedge(x) := f|_K(x) = f(x).$$

(Σημειωτέον ότι $\mathrm{Ker}(f|_K)^\wedge = \mathrm{Ker}(f|_K)$.) Κατά το θεώρημα 5.5.3,

$$K/\mathrm{Ker}(f|_K) = K/\mathrm{Ker}\,(f|_K)^\wedge \cong \mathrm{Im}\,(f|_K)^\wedge = f(K),$$

όπου $\mathrm{Ker}(f|_K) = \mathrm{Ker}(f) \cap K$, οπότε ο ισχυρισμός είναι αληθής επί τη βάσει τού θεωρήματος 5.1.22 τού Lagrange.

(ii) Δυνάμει τού (i) (στην ειδική περίπτωση όπου $K = G$) ισχύει η ισότητα

$$|G| = |f(G)|\,|\mathrm{Ker}(f)|\,.$$

(iii) Από τα (i) και (ii) έπεται ότι

$$\left.\begin{aligned} |G| &= |f(G)|\,|\mathrm{Ker}(f)| \\ |K| &= |f(K)|\,|\mathrm{Ker}(f|_K)| \end{aligned}\right\} \Rightarrow |G:K| = |f(G):f(K)|\,\left|\mathrm{Ker}(f):\mathrm{Ker}(f|_K)\right|,$$

κατόπιν εφαρμογής τού θεωρήματος 5.1.22 τού Lagrange. □

5.5.6 Θεώρημα (Μεταφορά ομομορφισμού σε «επίπεδο πηλικοομάδων»). *Έστω $f : (G_1, \cdot) \longrightarrow (G_2, *)$ ένας ομομορφισμός ομάδων. Εάν $K_1 \trianglelefteq G_1$, $K_2 \trianglelefteq G_2$, τότε οι εξής συνθήκες είναι ισοδύναμες*:

(i) *Υφίσταται ένας και μόνον ομομορφισμός $f^{\pi\eta\lambda.} : G_1/K_1 \longrightarrow G_2/K_2$ ο οποίος καθιστά το διάγραμμα*

$$\begin{array}{ccc} G_1 & \xrightarrow{\ f\ } & G_2 \\ {\scriptstyle \pi^{G_1}_{K_1}}\downarrow & \circlearrowleft & \downarrow{\scriptstyle \pi^{G_2}_{K_2}} \\ G_1/K_1 & \xrightarrow[f^{\pi\eta\lambda.}]{} & G_2/K_2 \end{array}$$

μεταθετικό, ήτοι ο «κανονιστικός» ομομορφισμός ο επαγόμενος από τον f που ορίζεται από τον τύπο

$$\boxed{f^{\pi\eta\lambda.}(gK_1) := f(g) * K_2,\ \forall g \in G_1.}$$

(ii) $f(K_1) \subseteq K_2$.

Επιπροσθέτως, στην περίπτωση κατά την οποία ικανοποιούνται οι ανωτέρω συνθήκες, ισχύουν τα ακόλουθα:

(a) *Ο $f^{\pi\eta\lambda.}$ είναι μονομορφισμός* $\Longleftrightarrow K_1 = f^{-1}(K_2)$.

(b) *Ο $f^{\pi\eta\lambda.}$ είναι επιμορφισμός* $\Longleftrightarrow \mathrm{Im}(f) * K_2 = G_2$.

Απόδειξη. Εφαρμόζουμε το θεώρημα 5.5.1 για τον ομομορφισμό $\pi^{G_2}_{K_2} \circ f$ (με τις $G_1, K_1, G_2/K_2$ στη θέση των εκεί παρατεθεισών ομάδων G, K και H, αντιστοίχως, και με τον $\pi^{G_2}_{K_2} \circ f$ στη θέση τού εκεί παρατεθέντος ομομορφισμού f). Σημειωτέον ότι $\mathrm{Ker}(\pi^{G_2}_{K_2} \circ f) = \{g \in G_1\,|\,f(g) * K_2 = K_2\} = \{g \in G_1\,|\,f(g) \in K_2\} = f^{-1}(K_2)$. Εάν λοιπόν $(K_1 =)\ \mathrm{Ker}(\pi^{G_1}_{K_1}) \subseteq \mathrm{Ker}(\pi^{G_2}_{K_2} \circ f)$, τότε $f(K_1) \subseteq f(f^{-1}(K_2)) \subseteq K_2$. Και αντιστρόφως· εάν $f(K_1) \subseteq K_2$, τότε

$$K_1 \subseteq f^{-1}(f(K_1)) \subseteq f^{-1}(K_2) = \mathrm{Ker}(\pi^{G_2}_{K_2} \circ f).$$

Άρα η ανωτέρω συνθήκη (ii) ισοδυναμεί, εν προκειμένω, με τη συνθήκη τη δοθείσα στο θεώρημα 5.5.1. Εν συνεχεία, υποθέτοντας ότι ικανοποιούνται οι (i), (ii), θα αποδείξουμε τις αμφίπλευρες συνεπαγωγές (a) και (b) για τον ομομορφισμό $f^{\pi\eta\lambda.}$.

(a) Επειδή

$$\begin{aligned} &\mathrm{Ker}(f^{\pi\eta\lambda.}) = \{gK_1 \in G_1/K_1\,|\,f(g) * K_2 = K_2\} = \{gK_1 \in G_1/K_1\,|\,f(g) \in K_2\} \\ &= \{gK_1 \in G_1/K_1\,|\,g \in f^{-1}(K_2)\} = f^{-1}(K_2)/K_1 \end{aligned}$$

ο $f^{\pi\eta\lambda.}$ (λόγω τής προτάσεως 3.5.12) είναι μονομορφισμός $\Longleftrightarrow K_1 = f^{-1}(K_2)$.

(b) Επειδή

$$\mathrm{Im}(f^{\pi\eta\lambda.}) = \{f(g) * K_2 \,|g \in G_1\},$$

ο $f^{\pi\eta\lambda.}$ είναι επιμορφισμός εάν και μόνον εάν

$$(\forall x \in G_2)\,(\exists g \in G_1 : f(g) * K_2 = xK_2) \Leftrightarrow (\forall x \in G_2)\left(\exists g \in G_1 : f(g)x^{-1} \in K_2\right),$$

δηλαδή εάν και μόνον εάν $\mathrm{Im}(f) * K_2 = G_2$. □

5.5.7 Παρατήρηση. Ακόμη και εάν, υποτιθεμένου ότι ικανοποιούνται οι συνθήκες (i), (ii) τού θεωρήματος 8.3.5, ο

$$f^{\pi\eta\lambda.} : G_1/K_1 \longrightarrow G_2/K_2$$

είναι *ισομορφισμός* (ήτοι $K_1 = f^{-1}(K_2)$ και -ταυτοχρόνως- $\mathrm{Im}(f) * K_2 = G_2$), ο ίδιος ο f *δεν είναι κατ' ανάγκην* ισομορφισμός[18]. Αλλά *ούτε* ο επιμορφισμός[19]

$$(f|_{K_1})^{\wedge} : K_1 \longrightarrow f(K_1) = f(f^{-1}(K_2)),\ x \longmapsto (f|_{K_1})^{\wedge}(x) := f|_{K_1}(x) = f(x),$$

ο δημιουργούμενος ύστερα από περιορισμό τού πεδίου τιμών τής απεικονίσεως $f|_{K_1}$ στο $f(K_1)$ είναι κατ' ανάγκην ισομορφισμός[20].

5.5.8 Παραδείγματα. Ας υποθέσουμε ότι δίδονται δυο ομάδες $(G_1, \cdot), (G_2, *)$ και ότι $K_1 \trianglelefteq G_1$, $K_2 \trianglelefteq G_2$.

(i) Εάν $G_1/K_1 \cong G_2/K_2$ και (ταυτοχρόνως) $K_1 \cong K_2$, τότε *δεν έχουμε κατ' ανάγκην* $G_1 \cong G_2$.

Επί παραδείγματι, $\langle [2]_4 \rangle \lhd \mathbb{Z}_4$ και $\langle [1\,2] \circ [3\,4] \rangle \lhd \mathbf{V}$ (βλ. 5.2.6) με

$$|\langle [2]_4 \rangle| = |\langle [1\,2] \circ [3\,4] \rangle| = 2,$$

και (λόγω τής προτάσεως 3.4.19, τού (ii) τού θεωρήματος 3.5.26 και των όσων προαναφέρθησαν στο (ii) τού εδαφίου 4.4.2)

$$\left\{ \begin{array}{c} \mathbb{Z}_4/\langle [2]_4 \rangle \cong \mathbb{Z}_2 \cong \mathbf{V}/\langle [1\,2] \circ [3\,4] \rangle, \\ \langle [2]_4 \rangle \cong \mathbb{Z}_2 \cong \langle [1\,2] \circ [3\,4] \rangle \end{array} \right\} \text{ αλλά } \mathbb{Z}_4 \ncong \mathbf{V}.$$

Ένας «απτός» ισομορφισμός

$$\mathbb{Z}_4/\langle [2]_4 \rangle \xrightarrow{\cong} \mathbf{V}/\langle [1\,2] \circ [3\,4] \rangle$$

είναι ο «κανονιστικός» (υπό την έννοια τού θεωρήματος 8.3.5) ο επαγόμενος από τον (μη ενριπτικό, μη επιρριπτικό) ομομορφισμό $\mathbb{Z}_4 \longrightarrow \mathbf{V}$ που ορίζεται (σε κάθε στοιχείο τής $\mathbb{Z}_4$) ως εξής:

$$[0]_4 \longmapsto \mathrm{id}, \quad [1]_4 \longmapsto [1\,3] \circ [2\,4], \quad [2]_4 \longmapsto \mathrm{id}, \quad [3]_4 \longmapsto [1\,3] \circ [2\,4].$$

(ii) Εάν $G_1/K_1 \cong G_2/K_2$ και εάν ισχύει (ταυτοχρόνως) $G_1 \cong G_2$ (ή ακόμη και $G_1 = G_2$), τότε *δεν έχουμε κατ' ανάγκην* $K_1 \cong K_2$.

Επί παραδείγματι, μέσω τού θεωρήματος 5.1.22 τού Lagrange και των προαναφερθέντων στο εδάφιο 5.1.44 (για τη διεδρική ομάδα $\mathbf{D}_4 = \langle \alpha, \beta \rangle$) λαμβάνουμε

$$|\mathbf{D}_4 : \langle \beta \rangle| = \tfrac{|\mathbf{D}_4|}{|\langle \beta \rangle|} = 2 = \tfrac{|\mathbf{D}_4|}{|\langle \alpha, \beta^2 \rangle|} = \left|\mathbf{D}_4 : \left\langle \alpha, \beta^2 \right\rangle\right|.$$

Εξ αυτού έπεται ότι

$$\langle \beta \rangle \lhd \mathbf{D}_4 \text{ και } \left\langle \alpha, \beta^2 \right\rangle \lhd \mathbf{D}_4$$

[18] Ο f είναι επιμορφισμός $\Leftrightarrow K_2 \sqsubseteq \mathrm{Im}(f) \Leftrightarrow \mathrm{Im}(f) = G_2$ και μονομορφισμός $\Leftrightarrow \mathrm{Ker}(f) = \{e_{G_1}\}$.

[19] Σημειωτέον ότι $f(f^{-1}(K_2)) \subseteq K_2$.

[20] Ο $(f|_{K_1})^{\wedge}$ είναι μονομορφισμός $\Leftrightarrow \{e_{G_1}\} = \mathrm{Ker}(f) \cap K_1 (= \mathrm{Ker}(f|_{K_1}) = \mathrm{Ker}((f|_{K_1})^{\wedge}))$.

(βλ. 5.2.13), και ότι -ως εκ τούτου- ορίζονται οι αντίστοιχες πηλικοομάδες $\mathbf{D}_4/\langle\beta\rangle$ και $\mathbf{D}_4/\langle\alpha,\beta^2\rangle$. Παρατηρούμε ότι

$$\mathbf{D}_4/\langle\beta\rangle \cong \mathbb{Z}_2 \cong \mathbf{D}_4/\langle\alpha,\beta^2\rangle \quad \text{αλλά} \quad \langle\beta\rangle \cong \mathbb{Z}_4 \ncong \mathbf{V} \cong \langle\alpha,\beta^2\rangle .$$

(Βλ. πρόταση 3.4.19 και το (ii) τού θεωρήματος 3.5.26.) Μάλιστα, ο υποδηλούμενος ισομορφισμός

$$\mathbf{D}_4/\langle\beta\rangle \xrightarrow{\cong} \mathbf{D}_4/\langle\alpha,\beta^2\rangle$$

δεν μπορεί να είναι «κανονιστικός» (υπό την έννοια τού θεωρήματος 8.3.5) εάν αξιώσουμε από αυτόν να επάγεται από κάποιον *αυτομορφισμό* τής $\mathbf{D}_4$. (Σημειωτέον ότι ισχύει $\vartheta(\langle\beta\rangle) = \langle\beta\rangle \nsubseteq \langle\alpha,\beta^2\rangle$ για κάθε αυτομορφισμό $\vartheta \in \mathrm{Aut}(\mathbf{D}_4)$.) Μολαταύτα, υπάρχει ισομορφισμός $\mathbf{D}_4/\langle\beta\rangle \xrightarrow{\cong} \mathbf{D}_4/\langle\alpha,\beta^2\rangle$ ο οποίος *είναι* «κανονιστικός» αλλά επαγόμενος από τον (μη ενριπτικό, μη επιριπτικό) *ενδομορφισμό*[21] τής $\mathbf{D}_4$ που ορίζεται (σε κάθε στοιχείο τής $\mathbf{D}_4$) ως εξής:

$$\begin{array}{llll} \mathrm{id}_{\mathcal{E}_4} \longmapsto \mathrm{id}_{\mathcal{E}_4}, & \beta \longmapsto \mathrm{id}_{\mathcal{E}_4}, & \beta^2 \longmapsto \mathrm{id}_{\mathcal{E}_4}, & \beta^3 \longmapsto \mathrm{id}_{\mathcal{E}_4}, \\ \alpha \longmapsto \beta, & \alpha\circ\beta \longmapsto \beta, & \alpha\circ\beta^2 \longmapsto \beta, & \alpha\circ\beta^3 \longmapsto \beta. \end{array}$$

(iii) Εάν $K_1 \cong K_2$ και εάν ισχύει (ταυτοχρόνως) $G_1 \cong G_2$ (ή ακόμη και $G_1 = G_2$), τότε *δεν έχουμε κατ' ανάγκην* $G_1/K_1 \cong G_2/K_2$.

5.5.9 Πόρισμα. *Έστω $f : (G_1,\cdot) \longrightarrow (G_2,*)$ ένας επιμορφισμός ομάδων.*
(i) *Εάν $K_2 \trianglelefteq G_2$, τότε*

$$\boxed{G_1/f^{-1}(K_2) \cong G_2/K_2.}$$

(ii) *Εάν $K_1 \trianglelefteq G_1$ και $\mathrm{Ker}(f) \subseteq K_1$, τότε*

$$\boxed{G_1/K_1 \cong G_2/f(K_1).}$$

Απόδειξη. (i) Αρκεί να εφαρμοσθεί το θεώρημα 8.3.5. (Εν προκειμένω, ο κατασκευαζόμενος «κανονιστικός» ομομορφισμός $f^{\pi\eta\lambda.}$ είναι ισομορφισμός.)

(ii) Αρκεί να εφαρμοσθεί εκ νέου το θεώρημα 8.3.5. Προφανώς, ο κατασκευαζόμενος «κανονιστικός» ομομορφισμός $f^{\pi\eta\lambda.}$ είναι επιμορφισμός. Από την άλλη μεριά, επειδή

$$\left.\begin{array}{r} f^{-1}(f(K_1)) = \mathrm{Ker}(f)K_1 \ \ (\text{βλ. 5.1.6 (iii)}) \\ \mathrm{Ker}(f) \subseteq K_1 \ \ (\text{εξ υποθέσεως}) \end{array}\right\} \Rightarrow K_1 = f^{-1}(f(K_1)),$$

ο $f^{\pi\eta\lambda.}$ είναι *και* μονομορφισμός. □

5.5.10 Θεώρημα (Τύπος γινομένου). *Εάν οι H, K είναι πεπερασμένες υποομάδες μιας ομάδας $(G,\cdot)$, τότε*

$$\boxed{\mathrm{card}(HK) = \frac{|H|\,|K|}{|H\cap K|} = \mathrm{card}(KH).} \tag{5.36}$$

Απόδειξη. Ορίζουμε την επιριπτική απεικόνιση

$$f : H\times K \longrightarrow HK, \ \ (x,y) \longmapsto f(x,y) := xy.$$

[21] Η ομάδα $\mathrm{Aut}(\mathbf{D}_4)$ αποτελείται από 8 αυτομορφισμούς (και είναι ισόμορφη με την ίδια την $\mathbf{D}_4$), ενώ το μονοειδές $\mathrm{End}(\mathbf{D}_4)$ αποτελείται από 36 ενδομορφισμούς.

Αρκεί να αποδείξουμε ότι $\operatorname{card}(f^{-1}(\{z\})) = |H \cap K|\,,\ \ \forall z \in HK$, διότι έχουμε [22]

$$H \times K = \coprod_{z \in HK} f^{-1}(\{z\}) \ \text{ και } \ \operatorname{card}(H \times K) = |H|\,|K|\,.$$

Έστω τυχόν $z \in HK$. Τότε $\exists x \in H, y \in K\colon\ z = xy$ και

$$f^{-1}(\{z\}) = \{(xr, r^{-1}y)\,|r \in H \cap K\,\}. \tag{5.37}$$

Πράγματι· κάθε διατεταγμένο ζεύγος ειλημμένο από το $H \times K$ και έχον τη μορφή $(xr, r^{-1}y)$, για κάποιο $r \in H \cap K$, ανήκει στην ίνα $f^{-1}(\{z\})$ τής f υπεράνω τού z, διότι

$$f(xr, r^{-1}y) = (xr)(r^{-1}y) = x(rr^{-1})y = xe_Gy = xy = z.$$

Για την απόδειξη τού αντιστρόφου εγκλεισμού θεωρούμε τυχόν διατεταγμένο ζεύγος $(x', y') \in f^{-1}(\{z\})$. Τότε

$$f(x', y') = x'y' = z = xy \Rightarrow x^{-1}x' = yy'^{-1} =: r \in H \cap K.$$

Για το κατ' αυτόν τον τρόπο ορισθέν r έχουμε $x' = xr$ και $y' = r^{-1}y$, οπότε η (5.37) είναι αληθής. Επομένως,

$$\operatorname{card}(f^{-1}(\{z\})) = \operatorname{card}(\{(xr, r^{-1}y)\,|r \in H \cap K\,\}) = |H \cap K|\,,$$

καθότι η απεικόνιση

$$H \cap K \ni r \longmapsto (xr, r^{-1}y) \in f^{-1}(\{z\})$$

είναι αμφιρριπτική. (Κατόπιν εναλλαγής των ρόλων των H και K η δεύτερη εκ των ισοτήτων (5.36) αποδεικνύεται παρομοίως.) □

5.5.11 Σημείωση. Στο θεώρημα 5.5.10 *δεν* προϋποθέτουμε ότι το σύνολο HK είναι υποομάδα τής G. Επί παραδείγματι, εάν $G := \mathfrak{S}_3$, $H := \langle[1\,2]\rangle$ και $K := \langle[2\,3]\rangle$, τότε $|H| = |K| = 2$ και $|H \cap K| = 1$, και ο τύπος (5.36) δίδει $\operatorname{card}(H \circ K) = 4$. Προφανώς,

$$4 \nmid 6 \underset{5.1.22}{\Longrightarrow} H \circ K \nsubseteq \mathfrak{S}_3.$$

(Πρβλ. 5.1.5.) Επιπροσθέτως, $[1\,2\,3] = [1\,2\,] \circ [2\,3]$ και

$$\left.\begin{aligned} H \circ K = \{\mathrm{id},\ [1\,2]\,,\ [2\,3]\,,\ [1\,2\,3]\} \subseteq \langle H, K\rangle \sqsubseteq \mathfrak{S}_3 \\ |\langle H, K\rangle| \geqslant 4 > 3 \end{aligned}\right\} \underset{5.1.24}{\Longrightarrow} \langle H, K\rangle = \mathfrak{S}_3,$$

οπότε $\mathfrak{S}_3 = \langle[1\,2]\,, [2\,3]\rangle$. (Πρβλ. 4.2.13 (ii).)

5.5.12 Πόρισμα. *Εάν οι H, K είναι υποομάδες μιας πεπερασμένης ομάδας $(G, \cdot)$ με*

$$|H| > \sqrt{|G|} \quad \textit{και} \quad |K| > \sqrt{|G|},$$

τότε $H \cap K \neq \{e_G\}$.

Απόδειξη. Από τον τύπο τού γινομένου (5.36) έπεται άμεσα ότι

$$|G| \geqslant \operatorname{card}(HK) = \frac{|H|\,|K|}{|H \cap K|} > \frac{\sqrt{|G|}\,\sqrt{|G|}}{|H \cap K|} = \frac{|G|}{|H \cap K|},$$

ήτοι ότι $|H \cap K| > 1$. □

[22] Εάν $z, z' \in HK$ με $z \neq z'$, τότε $f^{-1}(\{z\}) \cap f^{-1}(\{z'\}) = \varnothing$, διότι εάν υπήρχε $w \in f^{-1}(\{z\}) \cap f^{-1}(\{z'\})$, τότε θα συμπεραίναμε ότι $z = f(w) = z'$.

5.5.13 Λήμμα. *Εάν υποθέσουμε ότι οι H, K είναι υποομάδες μιας ομάδας $(G, \cdot)$ και $H \trianglelefteq \langle H, K\rangle$, όπου $\langle H, K\rangle := \langle H \cup K\rangle$ (βλ. 3.3.2), τότε ισχύουν τα εξής:*

(i) $HK = \langle H, K\rangle = KH$.

(ii) $H \cap K \trianglelefteq K$.

Απόδειξη. (i) Θεωρούμε τυχόντα στοιχεία $x \in H$ και $y \in K$. Επειδή

$$\left.\begin{array}{r} x \in H \trianglelefteq \langle H, K\rangle \\ y \in \langle H, K\rangle \Rightarrow y^{-1} \in \langle H, K\rangle \end{array}\right\} \Rightarrow xy = y(y^{-1}xy) = y(\underbrace{y^{-1}x(y^{-1})^{-1}}_{\in H}) \in KH,$$

έχουμε $HK \subseteq KH$. Επιπροσθέτως, επειδή

$$\left.\begin{array}{r} x \in H \trianglelefteq \langle H, K\rangle \\ y \in \langle H, K\rangle \end{array}\right\} \Rightarrow yx = (\underbrace{yxy^{-1}}_{\in H})y \in HK,$$

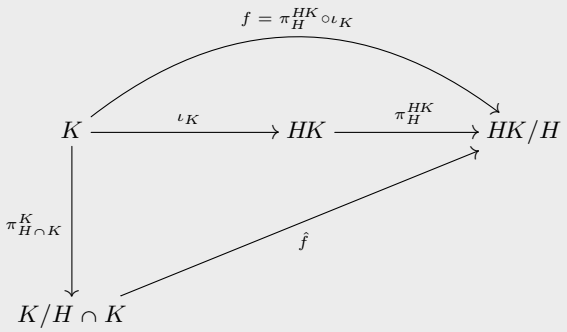
έχουμε $KH \subseteq HK$. Τελικώς λοιπόν, $HK = KH$ και το HK (σύμφωνα με την πρόταση 5.1.4) είναι μια *υποομάδα* τής G η οποία περιέχεται στην υποομάδα $\langle H, K\rangle$. Επειδή η $\langle H, K\rangle$ είναι η *ελάχιστη* υποομάδα τής G η οποία περιέχει την ένωση $H \cup K \subseteq HK$, ισχύει και ο αντίστροφος εγκλεισμός $\langle H, K\rangle \subseteq HK$.

(ii) Εάν $f := \pi_H^{HK} \circ \iota_K$, όπου $\pi_H^{HK} : HK \longrightarrow HK/H$ ο φυσικός επιμορφισμός και $\iota_K : K \longrightarrow KH,\ \ y \longmapsto \iota_K(y) := y$, τότε η f δίδεται από τον τύπο $f(y) := yH$, για κάθε $y \in K$, και (ούσα σύνθεση δύο ομομορφισμών) είναι ομομορφισμός με πυρήνα του τον $\mathrm{Ker}(f) = \{y \in K \mid yH = H\} = \{y \in K \mid y \in H\} = H \cap K$. Άρα $H \cap K \trianglelefteq K$ (σύμφωνα με το πόρισμα 5.2.31). □

5.5.14 Δεύτερο Θεώρημα Ισομορφισμών. *Έστω ότι H, K είναι δυο υποομάδες μιας ομάδας $(G, \cdot)$ ικανοποιούσες τη συνθήκη $H \trianglelefteq \langle H, K\rangle$. Εάν $f := \pi_H^{HK} \circ \iota_K$ είναι η σύνθεση τής ενθέσεως $\iota_K : K \to HK$, $y \mapsto \iota_K(y) := y$ και τού φυσικού επιμορφισμού $\pi_H^{HK} : HK \to HK/H$, τότε υφίσταται μία και μόνον απεικόνιση*

$$\hat{f} : K/\,H \cap K \longrightarrow HK/\,H,$$

τέτοια ώστε το διάγραμμα

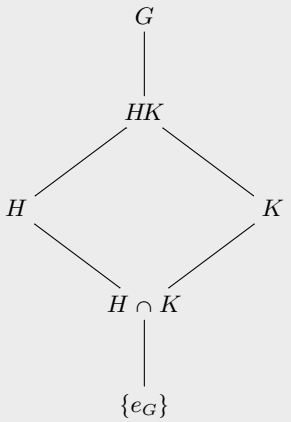


να καθίσταται μεταθετικό. Η απεικόνιση αυτή είναι ισομορφισμός. Ως εκ τούτου,

$$\boxed{K/\,H \cap K \cong HK/\,H\ (= \langle H, K\rangle\ /\,H),} \tag{5.38}$$

το δε διάγραμμα τού Hasse για το σύνολο των υποομάδων τής G που υπεισέρχονται στον ισομορφισμό (5.38) (συμπεριλαμβανομένης τής τετριμμένης και τής ιδίας τής

G) είναι το εξής:



Απόδειξη. Κατά το λήμμα 5.5.13, $HK = \langle H, K\rangle = KH$ και $\mathrm{Ker}(f) = H \cap K \trianglelefteq K$. Επομένως ορίζονται οι πηλικοομάδες HK/H και $K/H \cap K$. Έστω $(xy)H$ τυχόν στοιχείο τής πηλικοομάδας HK/H (όπου $x \in H$ και $y \in K$). Τότε

$$(xy)H = (xH)(yH) = H(yH) = (e_G H)(yH) = (e_G y)H = yH = f(y),$$

οπότε ο f είναι *επιμορφισμός* ομάδων. Εφαρμόζοντας γι' αυτόν το 1ο θεώρημα ισομορφισμών 5.5.3 κατασκευάζουμε τον ισομορφισμό

$$\hat{f} : K/H \cap K \longrightarrow HK/H, \;\; y(H \cap K) \longmapsto f(y) = yH,$$

με τις επιθυμητές ιδιότητες.

Δευτερη Απόδειξη. Επειδή $\iota_K(H \cap K) = H \cap K \subseteq H$,

$${\iota_K}^{-1}(K) = \{y \in K \,|\, \iota_K(y) = y \in H\} = H \cap K, \;\; \mathrm{Im}(\iota_K)H = KH = \langle H, K\rangle = HK,$$

ο ισχυρισμός είναι αληθής, προκύπτων άμεσα ύστερα από εφαρμογή τού θεωρήματος 8.3.5 για τις ορθόθετες υποομάδες $H \cap K$ και H των K και HK, αντιστοίχως, και τον ομομορφισμό ι_K. □

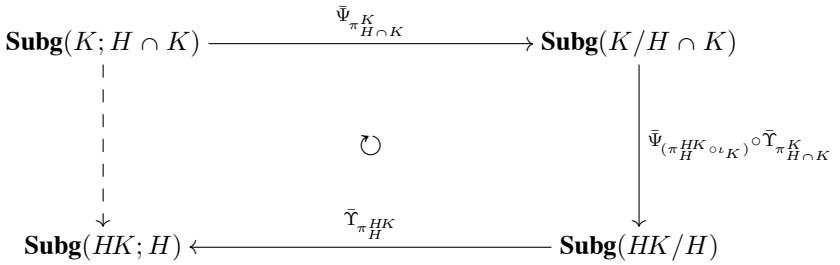
5.5.15 Παρατήρηση. (i) Σε ορισμένα συγγράμματα, στη διατύπωση τού 2ου θεωρήματος ισομορφισμών, αντί τής συνθήκης "$H \trianglelefteq \langle H, K\rangle$" παρατίθεται η συνθήκη "$H \trianglelefteq G$". Ωστόσο, η πρώτη είναι ασθενέστερη τής δεύτερης, διότι κατόπιν εφαρμογής τής προτάσεως 5.2.19 συμπεραίνουμε ότι

$$H \trianglelefteq G \Rightarrow H \trianglelefteq \langle H, K\rangle$$

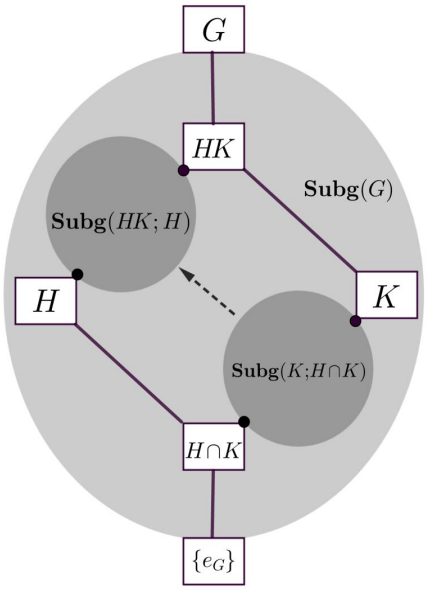
(αφού $H \sqsubseteq \langle H, K\rangle$).

(ii) Στην περίπτωση όπου οι H και K είναι πεπερασμένες υποομάδες τής ομάδας G και $H \trianglelefteq \langle H, K\rangle$, ο τύπος τού γινομένου (5.36) έπεται άμεσα από τον ισομορφισμό (5.38), τη σημείωση 5.1.21 και το θεώρημα 5.1.22 τού Lagrange. Ωστόσο, το θεώρημα 5.5.10 μας πληροφορεί ότι ο εν λόγω τύπος εξακολουθεί να ισχύει *ακόμη και όταν το σύνολο HK δεν είναι υποομάδα τής G*. (Βλ. εδ. 5.5.11.)

(iii) Σε επίπεδο υποομάδων η παρατήρηση 5.5.2 και το θεώρημα 5.5.14 δίδουν τους εξής ισομορφισμούς συνδέσμων:



Αυτός που υποδηλούται μέσω τού βέλους με τη διακεκομμένη γραμμή εικονογραφείται στο ακόλουθο:



5.5.16 Παράδειγμα. Εάν $m, n \in \mathbb{N}$ και εάν θεωρήσουμε τις υποομάδες $H := m\mathbb{Z}$ και $K := n\mathbb{Z}$ τής (κυκλικής, προσθετικής) ομάδας $(\mathbb{Z}, +)$, τότε, σύμφωνα με το (iii) και το (iv) τού πορίσματος 3.3.20, έχουμε

$$H \cap K = \text{εκπ}(m,n)\mathbb{Z} \quad \text{και} \quad H + K = \langle H, K\rangle = \text{μκδ}(m,n)\mathbb{Z}.$$

Επειδή $H := m\mathbb{Z} \trianglelefteq \langle H, K\rangle = \text{μκδ}(m,n)\mathbb{Z}$ (βλ. 3.3.20 (i) και 5.2.6), από το 2ο θεώρημα ισομορφισμών 5.5.14 έπεται ότι

$$\boxed{n\mathbb{Z}\,/\,\text{εκπ}(m,n)\mathbb{Z} \cong \text{μκδ}(m,n)\mathbb{Z}\,/m\mathbb{Z}.}$$

Εξάλλου, από την (5.34) λαμβάνουμε

$$\mathbb{Z}_{\frac{\text{εκπ}(m,n)}{n}} \cong n\mathbb{Z}\,/\,\text{εκπ}(m,n)\mathbb{Z} \cong \text{μκδ}(m,n)\mathbb{Z}\,/m\mathbb{Z} \cong \mathbb{Z}_{\frac{m}{\text{μκδ}(m,n)}},$$

απ' όπου συμπεραίνουμε ότι

$$\frac{\text{εκπ}(m,n)}{n} = \left|\mathbb{Z}_{\frac{\text{εκπ}(m,n)}{n}}\right| = \left|\mathbb{Z}_{\frac{m}{\text{μκδ}(m,n)}}\right| = \frac{m}{\text{μκδ}(m,n)}$$

ή, ισοδυνάμως, ότι $\text{μκδ}(m,n)\text{εκπ}(m,n) = mn$. (Πρβλ. πρόταση[23] 2.2.29.)

5.5.17 Παράδειγμα. Έστω $\mathbf{V}$ η ομάδα των τεσσάρων στοιχείων τού Klein (βλ. εδάφιο 4.4.2 (ii)). Ως γνωστόν, $\mathbf{V} \lhd \mathfrak{S}_4$ (βλ. 5.2.21). Έστω $K := \{\sigma \in \mathfrak{S}_4 \,|\sigma\,(4) = 4\}$. Προφανώς, $K \cong \mathfrak{S}_3$. Θα δείξουμε ότι $\mathbf{V} \circ K = \mathfrak{S}_4$. Έστω τυχούσα $\sigma \in \mathfrak{S}_4$. Εάν $\sigma\,(4) = 4$, τότε έχουμε $\sigma \in K \subseteq \mathbf{V} \circ K$. Εάν $\sigma\,(4) = j$, για κάποιον $j \in \{1,2,3\}$, τότε η συντιθέμενη μετάταξη $\tau := [j\ 4] \circ \sigma$ ανήκει στην K (διότι αφήνει το 4 αμετάβλητο). Θεωρώντας τήν αντιμετάθεση $[l\ m]$, όπου

$$\{l, m\} = \{1,2,3\} \smallsetminus \{j\},\ l \neq m,$$

[23] Η ισότητα $\text{μκδ}(m,n)\text{εκπ}(m,n) = |mn|$ ισχύει για *οιουσδήποτε* $m, n \in \mathbb{Z}\smallsetminus\{0\}$. Επειδή όμως $m\mathbb{Z} = |m|\,\mathbb{Z}$ και $n\mathbb{Z} = |n|\,\mathbb{Z}$ για *οιουσδήποτε* $m, n \in \mathbb{Z}\smallsetminus\{0\}$, *και αυτή* έπεται από τα προαναφερθέντα, αρκεί κανείς, όταν $m, n \in \mathbb{Z}\smallsetminus\{0\}$,να εργασθεί με τους $|m|$ και $|n|$ στη θέση των m και n.

συμπεραίνουμε (μέσω των (i), (v) και (vi) τής προτάσεως 4.2.3) ότι

$$\sigma = [j\ 4]^{-1} \circ \tau = [j\ 4] \circ \tau = (\underbrace{[j\ 4] \circ [l\ m]}_{\in \mathbf{V}}) \circ (\underbrace{[l\ m] \circ \tau}_{\in K}) \in \mathbf{V} \circ K.$$

Άρα όντως $\mathbf{V} \circ K = \mathfrak{S}_4$. Σημειωτέον ότι $\mathbf{V} \cap K = \{\mathrm{id}\}$, διότι κανένα από τα στοιχεία τού $\mathbf{V} \setminus \{\mathrm{id}\}$ δεν αφήνει το 4 αμετάβλητο. Ως εκ τούτου, μέσω τού 2ου θεωρήματος ισομορφισμών 5.5.14 καταλήγουμε στο ότι

$$\boxed{\mathfrak{S}_3 \cong K \cong K/\{\mathrm{id}\} \cong \mathfrak{S}_4/\mathbf{V}.}$$

5.5.18 Πόρισμα. *Έστω $(G, \cdot)$ μια πεπερασμένη ομάδα και έστω H μια ορθόθετη υποομάδα αυτής τάξεως $|H| = m$. Εάν* μκδ$(m, |G/H|) = 1$, *τότε η H είναι η μοναδική υποομάδα τής G που έχει τάξη m.*

Απόδειξη. Έστω K τυχούσα υποομάδα τής G τάξεως $|K| = m$. Κατά το 2ο θεώρημα ισομορφισμών 5.5.14,

$$K/\,H \cap K \cong HK/\,H \Longrightarrow |HK/\,H| = |K/\,H \cap K| = \frac{m}{|H \cap K|}. \tag{5.39}$$

Επειδή

$$\left.\begin{array}{l} |HK/\,H| \,|\, |G/H| \\ \text{μκδ}(m, |G/H|) = 1 \end{array}\right\} \Longrightarrow \text{μκδ}(m, |HK/\,H|) = 1 \underset{(5.39)}{\Longrightarrow} \text{μκδ}(m, \tfrac{m}{|H\cap K|}) = 1,$$

έχουμε

$$\text{μκδ}(m, \tfrac{m}{|H\cap K|}) = \tfrac{m}{|H\cap K|} = 1 \Longrightarrow m = |H \cap K| = |H| = |K|\,,$$

απ' όπου έπεται ότι $K = H$. □

5.5.19 Θεώρημα («Θεώρημα αντιστοιχίσεως ορθόθετων υποομάδων»).
Εάν $f : (G, \cdot) \longrightarrow (H, *)$ είναι ένας ομομορφισμός ομάδων και

$$\mathbf{Subg}(G; \mathrm{Ker}(f)) \ni K \overset{\bar{\Psi}_f}{\longmapsto} f(K) \in \mathbf{Subg}(\mathrm{Im}(f)) \tag{5.40}$$

η αμφίρριψη η ορισθείσα στο πόρισμα 3.5.20, τότε ισχύουν τα ακόλουθα:
(i) *Για $K_1, K_2 \in \mathbf{Subg}(G; \mathrm{Ker}(f))$ αληθεύει η κάτωθι αμφίπλευρη συνεπαγωγή*

$$\boxed{K_1 \trianglelefteq K_2 \Longleftrightarrow \bar{\Psi}_f(K_1) \trianglelefteq \bar{\Psi}_f(K_2)\,.}$$

(ii) *Για $K_1, K_2 \in \mathbf{Subg}(G; \mathrm{Ker}(f))$ με $K_1 \trianglelefteq K_2$ υφίσταται ισομορφισμός*

$$\boxed{K_2/K_1 \overset{\cong}{\longrightarrow} \bar{\Psi}_f(K_2)\,/\bar{\Psi}_f(K_1)\,.}$$

(iii) *Περιορίζοντας την αμφίρριψη (5.40) στο σύνολο*

$$\mathbf{NSubg}(G; \mathrm{Ker}(f)) = \mathbf{NSubg}(G) \cap \mathbf{Subg}(G; \mathrm{Ker}(f))$$

όλων των ορθόθετων υποομάδων τής G που περιέχουν τον πυρήνα $\mathrm{Ker}(f)$ τής f (βλ. 5.2.29), λαμβάνουμε μια αμφίρριψη

$$\boxed{\mathbf{NSubg}(G; \mathrm{Ker}(f)) \ni K \longmapsto f(K) \in \mathbf{NSubg}(\mathrm{Im}(f))}$$

η οποία καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων

$$(\mathbf{NSubg}(G;\mathrm{Ker}(f)),\trianglelefteq) \quad \textit{και} \quad (\mathbf{NSubg}(\mathrm{Im}(f)),\trianglelefteq)\,.$$

(iv) $\bar{\Psi}_f(\mathrm{NCL}_G(K_1,K_2)) = \mathrm{NCL}_G(\bar{\Psi}_f(K_1),\bar{\Psi}_f(K_2))$,
για κάθε ζεύγος $(K_1,K_2)\in \mathbf{NSubg}(G;\mathrm{Ker}(f)) \times \mathbf{NSubg}(G;\mathrm{Ker}(f))$.

ΑΠΟΔΕΙΞΗ. (i) Αυτό προκύπτει από την αμφιρριπτικότητα τής $\bar{\Psi}_f$ (βλ. 3.5.20) και την εφαρμογή τής προτάσεως 5.2.30 για τον επιμορφισμό $f|_{K_2} : K_2 \longrightarrow f(K_2)$.
(ii) Επειδή (κατά το (i)) $K_1 \trianglelefteq K_2 \Rightarrow \bar{\Psi}_f(K_1) \trianglelefteq \bar{\Psi}_f(K_2)$, ορίζεται η πηλικοομάδα $\bar{\Psi}_f(K_2)/\bar{\Psi}_f(K_1)$ και η απεικόνιση

$$\rho := \pi^{f(K_2)}_{f(K_1)} \circ f|_{K_2} : K_2 \longrightarrow f(K_2)/f(K_1)\ (= \bar{\Psi}_f(K_2)/\bar{\Psi}_f(K_1))$$

αποτελεί επιμορφισμό (ως σύνθεση δύο επιμορφισμών) με πυρήνα του την ομάδα

$$\begin{aligned}\mathrm{Ker}(\rho) &= \{x\in K_2\,|\rho(x)=f(K_1)\} = \{x\in K_2\,|f(x)*f(K_1)=f(K_1)\}\\ &= \{x\in K_2\,|f(x)\in f(K_1)\} = \{x\in K_2\,|x\in f^{-1}(f(K_1))\}\\ &= \{x\in K_2\,|x\in K_1\} = K_1 \ \ (\text{διότι } f^{-1}(f(K_1))=K_1).\end{aligned}$$

Επομένως, είναι δυνατόν να εφαρμόσουμε το 1ο θεώρημα ισομορφισμών 5.5.3 (για τον επιμορφισμό ρ) και να κατασκευάσουμε τον ισομορφισμό

$$\hat{\rho} : K_2/K_1 \longrightarrow \bar{\Psi}_f(K_2)/\bar{\Psi}_f(K_1)\,,\ \ xK_1 \longmapsto \hat{\rho}(xK_1)=\rho(x)=f(x)*\bar{\Psi}_f(K_1)\,.$$

(iii) Τούτο είναι άμεσο επακόλουθο τού[24] (i).
(iv) Επειδή η αμφίρριψη $\bar{\Psi}_f|_{\mathbf{NSubg}(G;\mathrm{Ker}(f))}$ καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων $(\mathbf{NSubg}(G;\mathrm{Ker}(f)),\trianglelefteq)$ και $(\mathbf{NSubg}(\mathrm{Im}(f)),\trianglelefteq)$, αρκεί να χρησιμοποιηθεί η ισοδυναμία των συνθηκών (i) και (iii) τής προτάσεως[25] 1.4.27, σε συνδυασμό με την πρόταση 5.2.28 και το πόρισμα 5.2.29. □

5.5.20 Πόρισμα. *Εάν* $f : (G,\cdot) \to (H,*)$ *είναι ένας ομομορφισμός ομάδων, τότε ισχύουν τα ακόλουθα*:
(i) *Για κάθε* $K\in \mathbf{Subg}(G)$ *ισχύει η ισότητα* $f^{-1}(f(K)) = K(\mathrm{Ker}(f))$.
(ii) *Για κάθε* $K\in \mathbf{Subg}(G)$ *υφίσταται ισομορφισμός*

$$\boxed{(K(\mathrm{Ker}(f)))/\mathrm{Ker}(f) \xrightarrow{\cong} f(K).}$$

(iii) *Για κάθε* $L\in \mathbf{Subg}(\mathrm{Im}(f))$ *υφίσταται ισομορφισμός*

$$\boxed{f^{-1}(L)/\mathrm{Ker}(f) \xrightarrow{\cong} L.}$$

ΑΠΟΔΕΙΞΗ. (i) Η ισότητα αυτή έχει ήδη αποδειχθεί στο (iii) τής προτάσεως 5.1.6. Σημειωτέον ότι $f(K)\in \mathbf{Subg}(\mathrm{Im}(f))$, οπότε

$$\bar{\Upsilon}_f(f(K)) = \bar{\Psi}_f^{-1}(f(K)) = f^{-1}(f(K)) = K(\mathrm{Ker}(f)) \in \mathbf{Subg}(G;\mathrm{Ker}(f)).$$

[24] Πρβλ. πρόταση 5.2.28 και πόρισμα 5.2.29.

[25] Στη διατύπωση τού θεωρήματος δεν θεωρήθηκε σκόπιμο να συμπεριληφθεί και η ιδιότητα

$$\bar{\Psi}_f(K_1\cap K_2) = \bar{\Psi}_f(K_1)\cap\bar{\Psi}_f(K_2)\,,\ \forall\,(K_1,K_2)\in \mathbf{NSubg}(G;\mathrm{Ker}(f))^2$$

(η οποία απορρέει από την ισοδυναμία των συνθηκών (i) και (ii) τής προτάσεως 1.4.27), καθότι αυτή (όπως είδαμε στο (iii) τού πορίσματος 3.5.20) ισχύει γενικότερα *για κάθε ζεύγος* $(K_1,K_2)\in \mathbf{Subg}(G;\mathrm{Ker}(f))^2$. (Σημειωτέον ότι το μέγιστο κάτω φράγμα δυο στοιχείων ειλημμένων από τον σύνδεσμο $(\mathbf{NSubg}(G;\mathrm{Ker}(f)),\trianglelefteq)$ ταυτίζεται με το μέγιστο κάτω φράγμα αυτών θεωρουμένων ως στοιχείων τού συνδέσμου $(\mathbf{Subg}(G;\mathrm{Ker}(f)),\sqsubseteq)$.)

Μάλιστα, *στην ειδική περίπτωση* κατά την οποία $K \in \mathbf{Subg}(G;\,\mathrm{Ker}(f))$, ισχύει η ισότητα $K(\mathrm{Ker}(f)) = K$ και η K απεικονίζεται μέσω τής αμφιρρίψεως $\bar{\Psi}_f$ στην $f(K)$ κατά τα ειωθότα.

(ii) Επειδή $K(\mathrm{Ker}(f)) \in \mathbf{Subg}(G;\,\mathrm{Ker}(f))$, έχουμε $\mathrm{Ker}(f) \sqsubseteq K(\mathrm{Ker}(f))$ και

$$\mathrm{Ker}(f) \trianglelefteq G \underset{5.2.19}{\Longrightarrow} \mathrm{Ker}(f) \trianglelefteq K(\mathrm{Ker}(f))$$

και το (ii) τού θεωρήματος 5.5.19 για τις $K_1 = \mathrm{Ker}(f)$ και $K_2 = K(\mathrm{Ker}(f))$ δίδει

$$\left(K(\mathrm{Ker}(f))\right)/\mathrm{Ker}(f) \cong \bar{\Psi}_f\left(\left(K(\mathrm{Ker}(f))\right)\right)/\bar{\Psi}_f\left(\mathrm{Ker}(f)\right) = f(K)/\{e_H\} \cong f(K).$$

(iii) Για κάθε $L \in \mathbf{Subg}(\mathrm{Im}(f))$ ισχύουν οι ισότητες

$$L = \left(\Psi_f \circ \bar{\Upsilon}_f\right)(L) = \bar{\Psi}_f(f^{-1}(L)) = f(f^{-1}(L))$$

και το (ii) τού θεωρήματος 5.5.19 για τις $K_1 = \mathrm{Ker}(f)$ και $K_2 = f^{-1}(L)$ δίδει τον ισομορφισμό $f^{-1}(L)/\mathrm{Ker}(f) \cong \bar{\Psi}_f(f^{-1}(L))/\bar{\Psi}_f(\mathrm{Ker}(f)) = L/\{e_H\} \cong L$, απ' όπου έπεται το ζητούμενο[26]. □

5.5.21 Πόρισμα (Θεώρημα αντιστοιχίσεως ορθόθετων υποομάδων για τον π_H^G). *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \trianglelefteq G$. Τότε για την αμφίρριψη*

$$\boxed{\mathbf{Subg}(G;H) \ni K \overset{\bar{\Psi}_{\pi_H^G}}{\longmapsto} \pi_H^G(K) = \pi_H^K(K) = K/H \in \mathbf{Subg}(G/H)}$$

ισχύουν τα ακόλουθα:

(i) *Για $K_1, K_2 \in \mathbf{Subg}(G;H)$ αληθεύει η κάτωθι αμφίπλευρη συνεπαγωγή*

$$\boxed{K_1 \trianglelefteq K_2 \Longleftrightarrow K_1/H \trianglelefteq K_2/H.}$$

Το αντίστοιχο μνημοτεχνικό διάγραμμα είναι το εξής:

$$\begin{array}{ccc}
G & \xrightarrow{\pi_H^G} & G/H \\
\big| & & \big| \\
K_2 & \xrightarrow{\pi_H^{K_2}} & K_2/H \\
\big| & & \big| \\
K_1 & \xrightarrow{\pi_H^{K_1}} & K_1/H \\
\big| & & \big| \\
H & \xrightarrow{\pi_H^H} & H/H \cong \{e_G\}
\end{array}$$

(ii) *Για $K_1, K_2 \in \mathbf{Subg}(G;H)$ με $K_1 \trianglelefteq K_2$ υφίσταται ισομορφισμός*

$$\boxed{K_2/K_1 \xrightarrow{\cong} (K_2/H)\,/\,(K_1/H)\,.}$$

(iii) *Περιορίζοντας την αμφίρριψη τού* (i) *στο σύνολο*

$$\mathbf{NSubg}(G;H) = \mathbf{NSubg}(G) \cap \mathbf{Subg}(G;H)$$

[26] Εάν $|\mathrm{Ker}(f)| < \infty$ και $|L| < \infty$, τότε από τον κατασκευασθέντα ισομορφισμό και από το θεώρημα 5.1.22 τού Lagrange έπεται η ισότητα (5.10) τού (ii) τού πορίσματος 5.1.13.

όλων των ορθόθετων υποομάδων τής ομάδας G που περιέχουν την H λαμβάνουμε μια αμφίρριψη

$$\boxed{\mathbf{NSubg}(G;H) \ni K \longmapsto K/H \in \mathbf{NSubg}(G/H)}$$

η οποία καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων

$$(\mathbf{NSubg}(G;H), \trianglelefteqslant) \quad \textit{και} \quad (\mathbf{NSubg}(G/H), \trianglelefteqslant).$$

(iv) $\mathrm{NCL}_G(K_1,K_2)/H = \mathrm{NCL}_G(K_1/H, K_2/H),\ \forall\,(K_1,K_2) \in \mathbf{NSubg}(G;H)^2$.

Απόδειξη. Αρκεί να εφαρμοσθεί το θεώρημα 5.5.19 για τον φυσικό επιμορφισμό $\pi_H^G : G \longrightarrow G/H$. □

5.5.22 Τρίτο Θεώρημα Ισομορφισμών. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \trianglelefteqslant G$. Τότε*

$$\boxed{G/K \cong (G/H)\,/\,(K/H)} \tag{5.41}$$

για κάθε $K \in \mathbf{NSubg}(G;H)$.

Απόδειξη. Λαμβανομένου υπ' όψιν τού ότι $H \sqsubseteq K, H \trianglelefteqslant G \underset{5.2.19}{\Longrightarrow} H \trianglelefteqslant K$, αυτή έπεται άμεσα ύστερα από εφαρμογή τού (ii) τού πορίσματος 5.5.21 για τις ομάδες $K_1 = K$ και $K_2 = G$. □

5.5.23 Παράδειγμα. Εάν $m,n \in \mathbb{N}$, τότε (σύμφωνα με την πρόταση 5.2.6) οι $m\mathbb{Z}$ και $n\mathbb{Z}$ είναι ορθόθετες υποομάδες τής $(\mathbb{Z},+)$. Υποθέτοντας ότι η $n\mathbb{Z}$ είναι υποομάδα τής $m\mathbb{Z}$ (που ισοδυναμεί με το ότι $m \mid n$, βλ. 3.3.20 (i)), το θεώρημα 5.5.22 μας παρέχει ισομορφισμό

$$\boxed{\mathbb{Z}/m\mathbb{Z} \xrightarrow{\cong} (\mathbb{Z}/n\mathbb{Z})\ /\ (m\mathbb{Z}/n\mathbb{Z})\,.}$$

5.5.24 Πόρισμα. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \trianglelefteqslant G$. Εάν K_1, K_2 είναι δυο υποομάδες τής G με $K_1 \trianglelefteqslant K_2$, τότε*

$$\boxed{HK_2/HK_1 \cong K_2/(K_1(K_2 \cap H)).}$$

Απόδειξη. Θεωρούμε τη σύνθεση

$$f := \pi_H^{HK_2} \circ \iota_{K_2} : K_2 \longrightarrow HK_2/H,\ \ x \longmapsto f(x) = xH,$$

όπου $\pi_H^{HK_2} : HK_2 \longrightarrow HK_2/H$ ο φυσικός επιμορφισμός και $\iota_{K_2} : K_2 \longrightarrow HK_2$, $y \longmapsto \iota_{K_2}(y) := y$ (όπως στο 2ο θεώρημα ισομορφισμών 5.5.14). Ως γνωστόν, η f είναι ένας επιμορφισμός ομάδων με πυρήνα $\mathrm{Ker}(f) = K_2 \cap H$. Από την άλλη μεριά, το (i) τού πορίσματος 5.5.20 δίδει $f^{-1}(f(K_1)) = K_1(\mathrm{Ker}(f)) = K_1(K_2 \cap H)$. Επιπροσθέτως, $K_1 \in \mathbf{NSubg}(K_2) \Longrightarrow f(K_1) \in \mathbf{NSubg}(\mathrm{Im}(f)) = \mathbf{NSubg}(f(K_2))$ και

$$f(K_1) \in \mathbf{NSubg}(\mathrm{Im}(f)) \Longrightarrow f^{-1}(f(K_1)) = K_1(K_2 \cap H) \in \mathbf{NSubg}(K_2; K_2 \cap H).$$

Κατά συνέπειαν, ορίζεται η πηλικοομάδα $K_2/K_1(K_2 \cap H)$. Εφαρμόζοντας το (ii) τού θεωρήματος 5.5.19 λαμβάνουμε

$$\begin{aligned} K_2/K_1(K_2 \cap H) &\cong \bar{\Psi}_f(K_2)\,/\bar{\Psi}_f(K_1(K_2 \cap H)) = f(K_2)/f(K_1(K_2 \cap H)) \\ &= (HK_2/H)\,/f(K_1(K_2 \cap H)). \end{aligned}$$

Εν συνεχεία παρατηρούμε ότι $f(K_1(K_2 \cap H)) = HK_1/H$. Πράγματι· εάν $a \in K_1$ και $b \in K_2 \cap H$, τότε $f(ab) = abH = aH \in HK_1/H \Longrightarrow f(K_1(K_2 \cap H)) \subseteq HK_1/H$. Και αντιστρόφως· εάν $x \in H$ και $y \in K_1 \subseteq K_2$, τότε

$$xyH = Hxy = Hy = yH = f(y) \in f(K_1) \subseteq f(K_1(K_2 \cap H)),$$

οπότε ισχύει και ο αντίστροφος εγκλεισμός $HK_1/H \subseteq f(K_1(K_2 \cap H))$. Αυτό σημαίνει ότι

$$K_2/K_1(K_2 \cap H) \cong (HK_2/H)\,/\,(HK_1/H) \cong HK_2/HK_1,$$

όπου η ύπαρξη τής τελευταίας σχέσεως ισομορφίας διασφαλίζεται από το 3ο θεώρημα ισομορφισμών 5.5.22. □

ΚΕΦΑΛΑΙΟ 6

Δακτύλιοι, ακέραιες περιοχές και σώματα

Η αλγεβρική δομή ενός *δακτυλίου*[1] καθορίζεται μέσω τού εφοδιασμού ενός μη κενού συνόλου *με δύο εσωτερικές πράξεις*. Ως προς την πρώτη εξ αυτών το θεωρούμενο σύνολο οφείλει να σχηματίζει μια *αβελιανή ομάδα*· ως προς τη δεύτερη, μια *ημιομάδα*. Επιπροσθέτως, απαιτείται και η ισχύς των *επιμεριστικών νόμων* για τον συσχετισμό των εν λόγω πράξεων. Οι *ακέραιες περιοχές* είναι εκείνοι οι μη τετριμμένοι μεταθετικοί δακτύλιοι με μοναδιαίο στοιχείο οι οποίοι δεν διαθέτουν μηδενοδιαιρέτες. Τα *σώματα*[2], από την άλλη μεριά, συγκροτούν μια ειδική υποκλάση τής κλάσεως των δακτυλίων· πρόκειται, για να ακριβολογούμε, για την υποκλάση εκείνων των *διαιρετικών δακτυλίων*, οι οποίοι συμβαίνει να είναι -ταυτοχρόνως- και μεταθετικοί.

6.1 ΔΑΚΤΥΛΙΟΙ ΚΑΙ ΥΠΟΔΑΚΤΥΛΙΟΙ

6.1.1 Ορισμός. Ένας **δακτύλιος** $(R, +, \cdot)$ είναι ένα μη κενό σύνολο R εφοδιασμένο με δύο εσωτερικές πράξεις "$+$" και "$\cdot$", που καλούνται (και συμβολίζονται ως) *πρόσθεση* και *πολλαπλασιασμός*, αντιστοίχως, ούτως ώστε

(i) το ζεύγος $(R, +)$ να είναι μια αβελιανή ομάδα,

(ii) το ζεύγος $(R, \cdot)$ να είναι μια ημιομάδα, και

(iii) η "$\cdot$" να είναι τόσον *εξ αριστερών* όσον και *εκ δεξιών επιμεριστική* ως προς την "$+$", δηλαδή για κάθε a, b και $c \in R$ να ισχύει

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c\,.$$

Το ουδέτερο στοιχείο τής ομάδας $(R, +)$ καλείται **μηδενικό στοιχείο** τού R και σημειώνεται με το 0_R. Εάν η ημιομάδα $(R, \cdot)$ διαθέτει *μοναδιαίο (= πολλαπλασιαστικώς ουδέτερο) στοιχείο* (σημειούμενο ως 1_R), δηλαδή εάν η $(R, \cdot)$ είναι ένα μονοειδές, τότε και ο R καλείται **δακτύλιος με μοναδιαίο στοιχείο** (ή **1-δακτύλιος**).

[1] Η έννοια τού *δακτυλίου* εισήχθη από τον David Hilbert (1862-1943) στο τέλος τού δεκάτου ενάτου αιώνα, αλλά ο τελικώς καθιερωθείς (φορμαλιστικός) ορισμός της εμφανίσθηκε περί τα μέσα τής δεκαετίας τού 1920.

[2] Η εισαγωγή τού όρου *σώμα* (γερμ. Körper) οφείλεται στους Leopold Kronecker (1823-1891) και Richard Dedekind (1831-1916), αν και η τελική εννοιολόγησή του (που επεκράτησε έκτοτε) αποδίδεται στον Heinrich Weber (1842-1913).

6.1.2 Σημείωση. Για λόγους συντομίας, πολλές φορές αντί τού $a \cdot b$ θα γράφουμε ab, ενώ όταν θα ομιλούμε για κάποιον «δακτύλιο R», θα υπονοούμε τη θεώρηση μιας τριάδας $(R, +, \cdot)$ όπως στον ορισμό 6.1.1 χωρίς όμως και να τη σημειώνουμε. Επίσης, εάν[3] $n \in \mathbb{N}$ και εάν τα $a_1, \ldots, a_n$ είναι στοιχεία ενός δακτυλίου R, τότε χρησιμοποιούμε ενίοτε τις βραχυγραφίες

$$\sum_{i=1}^{n} a_i := a_1 + \cdots + a_n, \qquad \prod_{i=1}^{n} a_i := a_1 \cdot \cdots \cdot a_n.$$

6.1.3 Ορισμός. Ένας δακτύλιος R λέγεται **μεταθετικός** όταν η πράξη τού πολλαπλασιασμού του είναι μεταθετική, δηλαδή όταν $ab = ba$ για κάθε $a, b \in R$.

6.1.4 Παραδείγματα. (i) Τα σύνολα $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ και $\mathbb{C}$ των ακεραίων, των ρητών, των πραγματικών και των μιγαδικών αριθμών, αντιστοίχως, εφοδιασμένα με τις συνήθεις πράξεις τής προσθέσεως και τού πολλαπλασιασμού, αποτελούν τα πιο απλά παραδείγματα μεταθετικών δακτυλίων με μοναδιαίο στοιχείο.

(ii) Έστω $(R, +, \cdot)$ τυχών δακτύλιος και έστω $\mathrm{Mat}_{m\times n}(R)$ το σύνολο όλων των $(m \times n)$-πινάκων με τις εγγραφές τους ειλημμένες από το R. (Βλ. εδ. 3.1.6.) Για οιουσδήποτε πίνακες

$$\mathbf{A} = (a_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}} \in \mathrm{Mat}_{m\times n}(R), \quad \mathbf{B} = (b_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}} \in \mathrm{Mat}_{m\times n}(R) \tag{6.1}$$

ισχύει (προφανώς) η αμφίπλευρη συνεπαγωγή

$$\mathbf{A} = \mathbf{B} \Longleftrightarrow a_{ij} = b_{ij}, \ \forall\, (i, j) \in \{1, \ldots, m\} \times \{1, \ldots, n\}.$$

Κάθε πίνακας $\mathbf{A} = (a_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}} \in \mathrm{Mat}_{m\times n}(R)$ διαθέτει m **γραμμές**

$$\Gamma\varrho_i(\mathbf{A}) := (a_{i1}\ a_{i2}\ \cdots\ a_{i\,n-1}\ a_{i\,n}) \in \mathrm{Mat}_{1\times n}(R), \quad i \in \{1, \ldots, m\},$$

και n **στήλες**

$$\Sigma\tau_j(\mathbf{A}) := \begin{pmatrix} a_{1j} \\ \vdots \\ a_{m\,j} \end{pmatrix} \in \mathrm{Mat}_{m\times 1}(R), \quad j \in \{1, \ldots, n\}.$$

(Η $\Gamma\varrho_i(\mathbf{A})$ καλείται i**-οστή γραμμή** και η $\Sigma\tau_j(\mathbf{A})$ j**-οστή στήλη τού** $\mathbf{A}$.) Προφανώς,

$$\mathbf{A} = (\Sigma\tau_1(\mathbf{A})\ \cdots\ \Sigma\tau_n(\mathbf{A})) = \begin{pmatrix} \Gamma\varrho_1(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_m(\mathbf{A}) \end{pmatrix}.$$

Εάν $r \in R$, τότε για οιονδήποτε $\mathbf{A} = (a_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}} \in \mathrm{Mat}_{m\times n}(R)$ θέτουμε

$$r\mathbf{A} := (ra_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}.$$

Το $\mathrm{Mat}_{m\times n}(R)$ καθίσταται αβελιανή ομάδα με μέσω τής προσθετικής πράξεως[4]

$$\mathbf{A} + \mathbf{B} := (a_{ij} + b_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}$$

για οιουσδήποτε πίνακες (A.3). Στην ειδική περίπτωση όπου $m = n$, το σύνολο $\mathrm{Mat}_{n\times n}(R)$ (ήτοι το σύνολο των **τετραγωνικών πινάκων**) καθίσταται δακτύλιος μέσω αυτής τής προσθετικής πράξεως και τής πολλαπλασιαστικής πράξεως

$$\mathbf{AB} := \left(\sum_{k=1}^{n} a_{i\,k} b_{k\,j} \right)_{1\leqslant i,j\leqslant n},$$

[3] Ως συνήθως, συμβολίζουμε ως $\mathbb{N}$, $\mathbb{N}_0$ τα σύνολα των φυσικών και των μη αρνητικών ακεραίων αριθμών, αντιστοίχως.

[4] Το ουδέτερο στοιχείο $0_{\mathrm{Mat}_{m\times n}(R)}$ αυτής τής ομάδας είναι ο $(m \times n)$-πίνακας, όλες οι εγγραφές τού οποίου είναι ίσες με το 0_R (και είθισται να σημειώνεται εν συντομία ως $\mathbf{0}_{m\times n}$).

για οιουσδήποτε $\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n}$ και $\mathbf{B} = (b_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{Mat}_{n\times n}(R)$. Εάν ο R έχει μοναδιαίο στοιχείο, τότε και ο $\mathrm{Mat}_{n\times n}(R)$ έχει μοναδιαίο στοιχείο, ήτοι τον *μοναδιαίο* $(n\times n)$*-πίνακα*

$$\mathbf{I}_n = \begin{pmatrix} 1_R & 0_R & \cdots & 0_R & 0_R \\ 0_R & 1_R & \cdots & 0_R & 0_R \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0_R & 0_R & \cdots & 1_R & 0_R \\ 0_R & 0_R & \cdots & 0_R & 1_R \end{pmatrix}.$$

Σημειωτέον ότι ο δακτύλιος $\mathrm{Mat}_{n\times n}(R)$ δεν είναι κατ' ανάγκην μεταθετικός, ακόμη και όταν ο ίδιος ο R είναι· εάν π.χ. ο R είναι μεταθετικός με μοναδιαίο στοιχείο $1_R \neq 0_R$, τότε ο $\mathrm{Mat}_{n\times n}(R)$ δεν είναι μεταθετικός στην περίπτωση κατά την οποία $n > 1$, αφού

$$\begin{pmatrix} 0_R & 1_R \\ 1_R & 0_R \end{pmatrix}\begin{pmatrix} 1_R & 1_R \\ 0_R & 1_R \end{pmatrix} = \begin{pmatrix} 0_R & 1_R \\ 1_R & 1_R \end{pmatrix} \neq \begin{pmatrix} 1_R & 1_R \\ 1_R & 0_R \end{pmatrix} = \begin{pmatrix} 1_R & 1_R \\ 0_R & 1_R \end{pmatrix}\begin{pmatrix} 0_R & 1_R \\ 1_R & 0_R \end{pmatrix}.$$

(Οι έννοιες: *υποπίνακας πίνακα*, *τεμαχισμένοι πίνακες*, *ελάσσονες πίνακες* κλπ. ορίζονται όπως και στη συνήθη Γραμμική Άλγεβρα. Για την εμπέδωση των απαραίτητων ιδιοτήτων των *οριζουσών πινάκων* που ανήκουν στον $\mathrm{Mat}_{n\times n}(R)$, όπου R κάποιος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο $1_R \neq 0_R$, οι αναγνώστες παροτρύνονται, στο σημείο αυτό, να ανατρέξουν στο Παράρτημα A.)

(iii) Το σύνολο $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ των άρτιων ακεραίων αριθμών με τις συνήθεις πράξεις είναι ένας μεταθετικός δακτύλιος *χωρίς* μοναδιαίο στοιχείο.

(iv) Έστω m ένας φυσικός αριθμός $\geqslant 1$ και έστω $\mathbb{Z}_m := \mathbb{Z}/\sim_m$ το *σύνολο των κλάσεων υπολοίπων (ή κλάσεων ισοτιμίας) των ακεραίων κατά μόδιο* m (ή *modulo* m). Το $\mathbb{Z}_m$ αποτελεί έναν μεταθετικό δακτύλιο (με το $[1]_m$ ως μοναδιαίο στοιχείο[5]) βάσει των συνήθων πράξεων

$$[a]_m + [b]_m := [a+b]_m \quad \text{και} \quad [a]_m \cdot [b]_m := [ab]_m$$

για κάθε ζεύγος $(a,b) \in \mathbb{Z}\times\mathbb{Z}$. (Πρβλ. (2.48), εδ. 2.4.42 και (3.1).)

(v) Έστω X ένα μη κενό σύνολο και έστω R ένας δακτύλιος. Τότε το σύνολο των απεικονίσεων $R^X := \{\text{απεικονίσεις } f : X \longrightarrow R\}$ καθίσταται δακτύλιος μέσω των «σημειακών» πράξεων

$$\begin{aligned} f+g : X \longrightarrow R, &\quad x \longmapsto f(x)+g(x) \\ f\cdot g : X \longrightarrow R, &\quad x \longmapsto f(x)\cdot g(x) \end{aligned}$$

Ιδιαιτέρως, εάν $X = \{1,\ldots,n\} \subset \mathbb{N}$, τότε μπορούμε να ταυτίζουμε το R^X με το *καρτεσιανό γινόμενο* $\underbrace{R\times R\times\cdots\times R\times R}_{n \text{ φορές}}$, το οποίο αποκτά τη δομή τού δακτυλίου μέσω των πράξεων

$$\begin{aligned} (x_1,x_2,\ldots,x_n)+(y_1,y_2,\ldots,y_n) &:= (x_1+y_1, x_2+y_2,\ldots,x_n+y_n), \\ (x_1,x_2,\ldots,x_n)\cdot(y_1,y_2,\ldots,y_n) &:= (x_1\cdot y_1, x_2\cdot y_2,\ldots,x_n\cdot y_n), \end{aligned}$$

με ουδέτερο στοιχείο ως προς την πρόσθεση το $(0_R,\ldots,0_R)$. Εξάλλου, δοθέντων n αυθαιρέτως επιλεγμένων δακτυλίων $R_1, R_2, \ldots, R_n$ μπορούμε να ορίσουμε τη δομή ενός δακτυλίου επί τού *καρτεσιανού* ή (*εξωτερικού*) *ευθέος γινομένου* τους

$$\prod_{j=1}^{n} R_j := R_1 \times \cdots \times R_n \tag{6.2}$$

[5] Όταν $m = 1$, έχουμε $[0]_1 = [1]_1$.

με τις ανάλογες πράξεις κατά παράγοντες. Ο δακτύλιος (6.2) είναι μεταθετικός εάν και μόνον εάν καθένας των παραγόντων του είναι μεταθετικός. Επιπροσθέτως, ο (6.2) έχει μοναδιαίο στοιχείο εάν και μόνον εάν καθένας των παραγόντων του έχει μοναδιαίο στοιχείο. (Μάλιστα, όταν ο (6.2) έχει μοναδιαίο στοιχείο, τότε αυτό είναι το $(1_{R_1}, \dots, 1_{R_n})$.) Κατ' αναλογίαν, εάν η $(R_j)_{j\in J}$ είναι μια μη κενή οικογένεια δακτυλίων, μπορούμε να ορίσουμε τη δομή δακτυλίου επί τού $\prod\limits_{j\in J} R_j$ μέσω των πράξεων

$$(x_j)_{j\in J} + (y_j)_{j\in J} := (x_j + y_j)_{j\in J},\ (x_j)_{j\in J} \cdot (y_j)_{j\in J} := (x_j \cdot y_j)_{j\in J}.$$

(vi) Εάν το R είναι ένα μονοσύνολο, τότε μπορεί να θεωρηθεί κατά τρόπο τετριμμένο ως δακτύλιος και γι' αυτό ονομάζεται **τετριμμένος δακτύλιος**. Σε αυτήν την περίπτωση έχουμε προφανώς $0_R = 1_R$.

(vii) Εκκινώντας από τον $(\mathbb{Z}, +, \cdot)$ μπορούμε να κατασκευάσουμε έναν άλλο μεταθετικό δακτύλιο με μοναδιαίο στοιχείο $(\mathbb{Z}, \boxplus, \boxdot)$ μέσω των πράξεων

$$a \boxplus b := a + b - 1, \qquad a \boxdot b := a + b - ab\,.$$

Το αξιοπερίεργο εδώ είναι ότι το ουδέτερο στοιχείο αυτού τού δακτυλίου ως προς την πρόσθεση $\boxplus$ είναι το 1, ενώ το μοναδιαίο στοιχείο ως προς τον πολλαπλασιασμό $\boxdot$ είναι το 0.

(viii) Τέλος, θα άξιζε να αναφερθεί ότι υπάρχουν και μη μεταθετικοί δακτύλιοι, οι οποίοι δεν διαθέτουν μοναδιαίο στοιχείο. Επί παραδείγματι, ο

$$R := \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z} \right\} \subsetneq \mathrm{Mat}_{2\times 2}(\mathbb{Z})$$

(ως προς τις συνήθεις πράξεις των 2×2 πινάκων) ή ακόμη και ο ίδιος ο $\mathrm{Mat}_{2\times 2}(2\mathbb{Z})$ είναι δακτύλιοι αυτού τού είδους.

6.1.5 Πρόταση. *Έστω R ένας δακτύλιος. Τότε ισχύουν τα εξής*:

(i) $0_R\, a = a\, 0_R = 0_R$, *για όλα τα* $a \in R$.

(ii) $(-a)\, b = a\, (-b) = -(a\, b)$, *για όλα τα* $a, b \in R$.

(iii) $(-a)\, (-b) = a\, b$, *για όλα τα* $a, b \in R$.

(iv) *Για* $m, n \in \mathbb{N}$ *και για οιαδήποτε στοιχεία* $a_1, \dots, a_m, b_1, \dots, b_n$ *τού* R *έχουμε*

$$\left(\sum_{j=1}^{m} a_j \right) \left(\sum_{k=1}^{n} b_k \right) = \sum_{j=1}^{m} \sum_{k=1}^{n} a_j\, b_k\ .$$

(v) *Εάν για οιαδήποτε* $a \in R$ *και* $n \in \mathbb{Z}$ *χρησιμοποιήσουμε τη βραχυγραφία*

$$na := \begin{cases} \underbrace{a + a + \cdots + a + a}_{n\text{-φορές}}, & \text{όταν} \quad n > 0 \\ \underbrace{(-a) + (-a) + \cdots + (-a) + (-a)}_{(-n)\text{-φορές}}, & \text{όταν} \quad n < 0 \\ 0_R\,, & \text{όταν} \quad n = 0 \end{cases}$$

από τη θεωρία των προσθετικών αβελιανών ομάδων, τότε $(na)\, b = a\, (nb) = n(a\, b)$ *για όλα τα* $n \in \mathbb{Z}$ *και όλα τα* $a, b \in R$.

(vi) *Εάν ο δακτύλιος R έχει μοναδιαίο στοιχείο και διαθέτει περισσότερα τού ενός στοιχεία, τότε* $1_R \neq 0_R$.

Απόδειξη. (i) $0_R\, a = (0_R + 0_R)\, a = 0_R\, a + 0_R\, a \Longrightarrow 0_R\, a = 0_R$. Ομοίως δείχνει κανείς ότι $a\, 0_R = 0_R$.

(ii) Προφανώς, $a\,b + a\,(-b) = a\,(b + (-b)) = a\,0_R = 0_R \Longrightarrow a\,(-b) = -(a\,b)$. Η δεύτερη ισότητα αποδεικνύεται με ανάλογο τρόπο.
(iii) Προφανώς, $(-a)\,(-b) = -(-a)\,b = -(-(a\,b)) = a\,b$ [ύστερα από διπλή εφαρμογή τής (ii)].
(iv) Θεωρούμε το m ως παγιωμένο και χρησιμοποιούμε μαθηματική επαγωγή ως προς τον n. Για $n = 1$ η ανωτέρω ισότητα γράφεται ως

$$(a_1 + \cdots + a_m)\,b_1 = a_1 b_1 + \cdots + a_m b_1$$

και είναι αληθής λόγω τής επιμεριστικής ιδιότητας τού πολλαπλασιασμού τού R ως προς την πρόσθεση. Ας υποθέσουμε ότι, για δοθέντες m, n, ισχύει η ισότητα

$$\left(\sum_{j=1}^{m} a_j\right)\,\left(\sum_{k=1}^{n} b_k\right) = \sum_{j=1}^{m}\sum_{k=1}^{n} a_j\,b_k.$$

Εφαρμόζοντας εκ νέου την επιμεριστική ιδιότητα, σε συνδυασμό με την επαγωγική μας υπόθεση, λαμβάνουμε

$$\begin{aligned}\left(\sum_{j=1}^{m} a_j\right)\,\left(\sum_{k=1}^{n+1} b_k\right) &= \left(\sum_{j=1}^{m} a_j\right)\,\left(\sum_{k=1}^{n} b_k + b_{n+1}\right)\\ &= \left(\sum_{j=1}^{m} a_j\right)\,\left(\sum_{k=1}^{n} b_k\right) + \left(\sum_{j=1}^{m} a_j\right) b_{n+1}\\ &= \sum_{j=1}^{m}\sum_{k=1}^{n} a_j\,b_k + \sum_{j=1}^{m} a_j\,b_{n+1} = \sum_{j=1}^{m}\sum_{k=1}^{n+1} a_j\,b_k.\end{aligned}$$

(v) Τούτο έπεται άμεσα από το (iv).
(vi) Επί τη βάσει τής υποθέσεώς μας, $R\setminus\{0_R\} \neq \varnothing$. Άρα για κάθε $a \in R\setminus\{0_R\}$ έχουμε $1_R a = a$, οπότε $1_R \neq 0_R$. □

6.1.6 Ορισμός. Για κάθε στοιχείο a ενός δακτυλίου R και έναν $n \in \mathbb{N}$, θέτουμε

$$\boxed{a^n := \underbrace{a\cdot a\cdot\cdots\cdot a\cdot a}_{n\ \text{φορές}}}$$

και $a^0 := 1_R$, όταν ο R διαθέτει μοναδιαίο στοιχείο. Προφανώς

$$a^m a^n = a^{m+n} \quad \text{και} \quad (a^m)^n = a^{mn}$$

για όλους τους φυσικούς αριθμούς m, n.

6.1.7 Πρόταση (Διωνυμικοί τύποι). *Για κάθε μη αρνητικό ακέραιο αριθμό n ας συμβολίσουμε ως $n!$ $:= 1\cdot 2\cdots n$ το παραγοντικό τού n, όταν $n \geqslant 1$, θέτοντας $0! := 1$, και ως*

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}$$

τον διωνυμικό συντελεστή τού n υπεράνω τού k, όπου $k \in \mathbb{Z}$, $0 \leqslant k \leqslant n$. Υποθέτοντας ότι ο R είναι ένας δακτύλιος με μοναδιαίο στοιχείο, ο n ένας παγιωμένος φυσικός αριθμός, και (για κάποιον $\nu \in \mathbb{N}$) τα $a, b, a_1, a_2, \ldots, a_\nu$, στοιχεία τού R, έχουμε:

(i) *Εάν $ab = ba$, τότε*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k}\,a^k\,b^{n-k} \tag{6.3}$$

(ii) *Εάν* $a_i a_j = a_j a_i$ *για όλους τους δείκτες* $1 \leqslant i, j \leqslant \nu$, *τότε*

$$(a_1 + a_2 + \cdots + a_\nu)^n = \sum \frac{n!}{(i_1!)\,(i_2!)\cdots(i_\nu!)}\, a_1^{i_1}\, a_2^{i_2}\, \cdots\, a_\nu^{i_\nu} \tag{6.4}$$

όπου το άθροισμα λαμβάνεται υπεράνω όλων των ν*-άδων*

$$(i_1, i_2, \ldots, i_\nu) \in (\mathbb{N}_0)^\nu$$

για τις οποίες ισχύει $i_1 + i_2 + \cdots + i_\nu = n$.

Απόδειξη. (i) Θα χρησιμοποιήσουμε την «τριγωνική ταυτότητα τού Pascal», ήτοι την:

$$\tbinom{n}{j} + \tbinom{n}{j+1} = \tbinom{n+1}{j+1} \tag{6.5}$$

για κάθε $j, 0 \leqslant j < n$, και θα εργασθούμε με μαθηματική επαγωγή ως προς τον n. Για $n = 0$ η (6.3) είναι προφανής. Υποθέτοντας ότι η (6.3) είναι αληθής για κάποιον $n \geqslant 1$, λαμβάνουμε μέσω τής επιμεριστικής ιδιότητας:

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)\sum_{k=0}^{n} \tbinom{n}{k} a^k\, b^{n-k} \\
&= \sum_{k=0}^{n} \tbinom{n}{k} a^{k+1}\, b^{n-k} + \sum_{k=0}^{n} \tbinom{n}{k} a^k\, b^{n-k+1} \quad [\text{επειδή } ab = ba] \\
&= \tbinom{n}{n} a^{n+1} + \sum_{k=0}^{n-1} \tbinom{n}{k}\, a^{k+1}\, b^{n-k} + \sum_{k=1}^{n} \tbinom{n}{k}\, a^k\, b^{n-k+1} + \tbinom{n}{0} b^{n+1} \\
&= \tbinom{n+1}{n+1} a^{n+1} + \sum_{j=0}^{n-1} \tbinom{n}{j}\, a^{j+1}\, b^{(n+1)-(j+1)} + \\
&+ \sum_{j=0}^{n-1} \tbinom{n}{j+1}\, a^{j+1}\, b^{(n+1)-(j+1)} + \tbinom{n+1}{0} b^{n+1} \\
&= \tbinom{n+1}{n+1} a^{n+1} + \sum_{j=0}^{n-1} \left(\tbinom{n}{j} + \tbinom{n}{j+1} \right) a^{j+1}\, b^{(n+1)-(j+1)} + \tbinom{n+1}{0} b^{n+1} \\
&\overset{(6.5)}{=} \tbinom{n+1}{n+1} a^{n+1} + \sum_{j=0}^{n-1} \tbinom{n+1}{j+1} a^{j+1}\, b^{(n+1)-(j+1)} + \tbinom{n+1}{0} b^{n+1} \\
&= \tbinom{n+1}{n+1} a^{n+1} + \sum_{k=0}^{n} \tbinom{n+1}{k} a^k\, b^{(n+1)-k} + \tbinom{n+1}{0} b^{n+1} = \sum_{k=0}^{n+1} \tbinom{n+1}{k} a^k\, b^{(n+1)-k}\,.
\end{aligned}$$

(ii) Για την απόδειξη τού τύπου (6.4) αρκεί να εφαρμόσουμε μαθηματική επαγωγή ως προς τον πληθικό αριθμό ν των προσθετέων. Για $\nu = 1$ ο (6.4) είναι προφανής, ενώ για $\nu = 2$ συμπίπτει με τον (6.3), αφού

$$(a_1 + a_2)^n = \sum_{k=0}^{n} \tbinom{n}{k} a_1^k\, a_2^{n-k} = \sum_{(k,j)\in\mathbb{N}_0^2 : k+j=n} \tfrac{n!}{k!\,j!}\, a_1^k\, a_2^j\,.$$

Εάν υποθέσουμε ότι ο (6.4) είναι αληθής για κάποιον $\nu \geqslant 2$, τότε θα είναι αληθής και για τον $\nu + 1$, διότι

$$\begin{aligned}
&(a_1 + a_2 + \cdots + a_\nu + a_{\nu+1})^n = ((a_1 + a_2 + \cdots + a_\nu) + a_{\nu+1})^n \\
&= \sum_{k=0}^{n} \tbinom{n}{k} (a_1 + \cdots + a_\nu)^k\, a_{\nu+1}^{n-k} = \sum_{(k,j)\in\mathbb{N}_0^2 : k+j=n} \tfrac{n!}{k!\,j!}\, (a_1 + \cdots + a_\nu)^k\, a_{\nu+1}^j\,,
\end{aligned}$$

όπου το τελευταίο άθροισμα ισούται με

$$\begin{aligned}
&\sum_{(k,j)\in\mathbb{N}_0^2:k+j=n} \frac{n!}{k!\,j!} \left(\sum_{(i_1,..,i_\nu)\in(\mathbb{N}_0)^\nu:i_1+\cdots+i_\nu=k} \frac{k!}{(i_1!)\cdots(i_\nu!)}\, a_1^{i_1}\, a_2^{i_2}\, \cdots\, a_\nu^{i_\nu} \right) a_{\nu+1}^{j} \\
&= \sum_{(k,j)\in\mathbb{N}_0^2:k+j=n} \left(\sum_{(i_1,..,i_\nu)\in(\mathbb{N}_0)^\nu:i_1+\cdots+i_\nu=k} \frac{n!k!}{k!\,j!(i_1!)\cdots(i_\nu!)}\, a_1^{i_1}\, a_2^{i_2}\, \cdots\, a_\nu^{i_\nu} a_{\nu+1}^{j} \right) \\
&= \sum_{(k,j)\in\mathbb{N}_0^2:k+j=n} \left(\sum_{(i_1,..,i_\nu)\in(\mathbb{N}_0)^\nu:i_1+\cdots+i_\nu=k} \frac{n!}{(i_1!)\cdots(i_\nu!)(j!)}\, a_1^{i_1}\, a_2^{i_2}\, \cdots\, a_\nu^{i_\nu} a_{\nu+1}^{j} \right) \\
&= \sum_{(i_1,..,i_\nu,i_{\nu+1})\in(\mathbb{N}_0)^{\nu+1}:i_1+\cdots+i_\nu+i_{\nu+1}=n} \frac{n!}{(i_1!)\cdots(i_\nu!)(i_{\nu+1}!)}\, a_1^{i_1}\, a_2^{i_2}\, \cdots\, a_\nu^{i_\nu} a_{\nu+1}^{i_{\nu+1}}
\end{aligned}$$

ύστερα από την αντικατάσταση τού αντιστοίχου τύπου για ν προσθετέους. □

6.1.8 Σημείωση. Δεδομένων των συνθηκών αμοιβαίας μεταθετικότητας των όρων μας, ανεπαίσθητες παραλλαγές των (6.3) και (6.4) παραμένουν ισχύουσες ακόμη και όταν ο δακτύλιος R *δεν* διαθέτει μοναδιαίο στοιχείο. Συγκεκριμένα, σε αυτήν την περίπτωση, μπορούμε να γράψουμε αντί τής (6.3),

$$(a+b)^n = a^n + \sum_{k=1}^{n-1} \binom{n}{k} a^k\, b^{n-k} + b^n$$

(και, αντιστοίχως, να μην εμφανίσουμε *καθόλου* στην (6.4) τους παράγοντες που είναι υψωμένοι στη μηδενική δύναμη). Ωστόσο, θα πρέπει να έχουμε πάντοτε στο νου μας ότι, όταν ένας δακτύλιος αναφοράς R δεν διαθέτει μοναδιαίο στοιχείο, το na, όπου $n\in\mathbb{Z}$ και $a\in R$, είναι στοιχείο τού R, *χωρίς* όμως το na να υποδηλοί -εν γένει- πολλαπλασιασμό δύο στοιχείων *εντός* τού R. Αντιθέτως, όταν ο R είναι δακτύλιος με μοναδιαίο, τότε το na υποδηλοί πάντοτε πολλαπλασιασμό δύο στοιχείων εντός τού R, καθότι αυτό γράφεται ως $na = (n\cdot 1_R)\,a$.

6.1.9 Ορισμός. Ένα μη κενό υποσύνολο S (τού υποκειμένου συνόλου R) ενός δακτυλίου $(R,+,\cdot)$ καλείται **υποδακτύλιος** τού $(R,+,\cdot)$ όταν το S είναι κλειστό ως προς αμφότερες τις πράξεις "$+$" και "$\cdot$" και καθίσταται αφ' εαυτού δακτύλιος (ως προς τον περιορισμό των εν λόγω πράξεων επ' αυτού).

6.1.10 Πρόταση. *Ένα μη κενό υποσύνολο S ενός δακτυλίου R είναι υποδακτύλιος τού R εάν και μόνον εάν ικανοποιούνται οι ακόλουθες συνθήκες:*

(i) $a-b := a+(-b)\in S$, *για κάθε* $a,b\in S$.

(ii) $ab\in S$, *για κάθε* $a,b\in S$.

6.1.11 Παραδείγματα. (i) Ο δακτύλιος $\mathbb{Z}$ είναι υποδακτύλιος τού $\mathbb{Q}$, ο $\mathbb{Q}$ υποδακτύλιος τού $\mathbb{R}$ και ο $\mathbb{R}$ είναι υποδακτύλιος τού $\mathbb{C}$. Επίσης, ο $2\mathbb{Z}$ είναι υποδακτύλιος τού $\mathbb{Z}$ και το $\{[0]_{10},[2]_{10},[4]_{10},[6]_{10},[8]_{10}\}$ υποδακτύλιος τού $\mathbb{Z}_{10}$.

(ii) Ο **δακτύλιος των ακεραίων τού Gauss (ή «γκαουσιανών ακεραίων»)**

$$\boxed{\mathbb{Z}[i] := \{a+bi \mid a,b\in\mathbb{Z}\} \subsetneq \mathbb{C}} \tag{6.6}$$

με πράξεις τις (συνήθεις πράξεις τού $\mathbb{C}$):

$$(a+bi)+(c+di) := (a+c)+(b+d)i,\ (a+bi)\cdot(c+di) := (ac-bd)+(ad+bc)i,$$

όπου i η «φανταστική» μονάδα, είναι (μεταθετικός) υποδακτύλιος τού δακτυλίου των μιγαδικών αριθμών, ενώ περιέχει τον $\mathbb{Z}$ ως υποδακτύλιό του. Γενικότερα, το

$$\boxed{\mathbb{Z}[\sqrt{m}] := \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\} \subsetneq \mathbb{C}} \tag{6.7}$$

όπου το $m \in \mathbb{Z}$ δεν είναι τέλειο τετράγωνο (δηλαδή $\sqrt{|m|} \notin \mathbb{Q}$), καθίσταται υποδακτύλιος τού $\mathbb{R}$, όταν $m \in \mathbb{N}$, και υποδακτύλιος τού $\mathbb{C}$, όταν $m \in \mathbb{Z} \smallsetminus \mathbb{N}_0$, καθότι για οιουσδήποτε $a + b\sqrt{m},\ a' + b'\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$, έχουμε[6]

$$\begin{cases} (a + b\sqrt{m}) - (a' + b'\sqrt{m}) = (a - a') + (b - b')\sqrt{m} \in \mathbb{Z}[\sqrt{m}], \\ (a + b\sqrt{m})\,(a' + b'\sqrt{m}) = (aa' + bmb') + (ab' + ba')\sqrt{m} \in \mathbb{Z}[\sqrt{m}]. \end{cases}$$

(iii) Κάθε δακτύλιος R έχει πάντοτε ως υποδακτυλίους τον εαυτό του και τον **τετριμμένο υποδακτύλιο** $\{0_R\}$. Ένας υποδακτύλιος S ενός δακτυλίου R με $S \subsetneq R$ λέγεται **γνήσιος υποδακτύλιος** τού R.

6.1.12 Σημείωση. Έστω S ένας υποδακτύλιος ενός δακτυλίου R. Εάν ο R είναι μεταθετικός, τότε είναι προφανές ότι και ο S είναι μεταθετικός. Ωστόσο, εάν ο R είναι μη μεταθετικός και ο S *γνήσιος* υποδακτύλιός του, ο S ενδέχεται να είναι μεταθετικός, όπως, π.χ., συμβαίνει στην περίπτωση όπου

$$S := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R \;\middle|\; b = c = 0 \right\},\ R := \mathrm{Mat}_{2\times 2}(\mathbb{Z}).$$

6.1.13 Σημείωση. Υπάρχουν υποδακτύλιοι S δακτυλίων R που συμπεριφέρονται αρκετά παράξενα όσον αφορά στην ύπαρξη ή μη μοναδιαίου στοιχείου.

(i) Ο S είναι δυνατόν να μην έχει μοναδιαίο στοιχείο, ενώ ο R να έχει, όπως π.χ. συμβαίνει στους $S = 2\mathbb{Z},\ R = \mathbb{Z}$.

(ii) Επίσης, ο S μπορεί να έχει μοναδιαίο στοιχείο, ενώ ο R να μην έχει, όπως π.χ. συμβαίνει στους $S = \{0\} \times \mathbb{R},\ R = 2\mathbb{Z} \times \mathbb{R}$.

(iii) Εάν ο R έχει μοναδιαίο στοιχείο το 1_R και $1_R \in S$, τότε $1_R = 1_S$.

(iv) Τέλος, ενδέχεται και οι δυο τους να έχουν μοναδιαία στοιχεία 1_S και 1_R, αντιστοίχως, χωρίς αυτά να είναι ίσα μεταξύ τους. Π.χ., ο $R = \mathbb{Z} \times \mathbb{Z}$ έχει ως μοναδιαίο του στοιχείο το $(1, 1)$, ενώ ο υποδακτύλιός του $S = \mathbb{Z} \times \{0\}$ το $(1, 0)$.

6.1.14 Πρόταση. *Εάν η $(S_j)_{j\in J}$ είναι μια μη κενή οικογένεια υποδακτυλίων ενός δακτυλίου R, τότε η τομή $\bigcap\limits_{j\in J} S_j$ αποτελεί έναν υποδακτύλιο τού R.*

Απόδειξη. Επειδή $0_R \in S_j$ για κάθε $j \in J$, έχουμε $0_R \in \bigcap\limits_{j\in J} S_j$, οπότε η τομή αυτή δεν είναι κενή. Εάν $a, b \in \bigcap\limits_{j\in J} S_j$, τότε

$$[a, b \in S_j,\ \forall j \in J] \Longrightarrow [a - b \in S_j,\ \forall j \in J] \Longrightarrow a - b \in \bigcap_{j\in J} S_j$$

και

$$[a, b \in S_j,\ \forall j \in J] \Longrightarrow [ab \in S_j,\ \forall j \in J] \Longrightarrow ab \in \bigcap_{j\in J} S_j.$$

Άρα η $\bigcap\limits_{j\in J} S_j$ είναι όντως ένας υποδακτύλιος τού R. (Βλ. πρόταση 6.1.10). □

[6] Η δευτεροβάθμια εξίσωση $z^2 - m = 0$, $z \in \mathbb{C}$, έχει δύο λύσεις. Εάν $m > 0$, τότε αυτές είναι οι $\pm\sqrt{m} \in \mathbb{R}$. Εάν $m < 0$, τότε αυτές είναι οι $\pm i\sqrt{-m} \in \mathbb{C}$. Προσοχή! Γράφοντας απλώς $\mathbb{Z}[\sqrt{m}]$, *στην περίπτωση όπου* $m < 0$, ορίζουμε ως $\sqrt{m}$ τον μιγαδικό αριθμό $i\sqrt{-m}$ και λαμβάνουμε

$$\sqrt{m}\sqrt{m} = (i\sqrt{-m})(i\sqrt{-m}) = i^2(\sqrt{-m})^2 = (-1)(-m) = m$$

χρησιμοποιώντας τον συνήθη πολλαπλασιασμό εντός τού $\mathbb{C}$. Ο ανωτέρω σύντομος *φορμαλιστικός* συμβολισμός δεν θα πρέπει να μας οδηγεί σε επιπόλαια συμπεράσματα. Επί παραδείγματι, η ρίζα τού γινομένου δυο *θετικών* πραγματικών αριθμών ισούται με το γινόμενο των ριζών αυτών (εντός τού $\mathbb{R}$). Τούτο *δεν γενικεύεται* για τον εν λόγω φορμαλιστικό συμβολισμό όταν $m < 0$. Εν προκειμένω, $-m = \sqrt{(-m)(-m)} = \sqrt{m \cdot m} \neq \sqrt{m}\sqrt{m} = m$.

6.1.15 Ορισμός. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο και έστω $S \subseteq R$ ένας υποδακτύλιός του έχων ως μοναδιαίο του στοιχείο το 1_R. Εάν $\varnothing \neq A \subseteq R$, τότε (μέσω τής προτάσεως 6.1.14) ορίζεται ο *ελάχιστος* (ως προς τη σχέση τού συνολοθεωρητικού εγκλεισμού) υποδακτύλιος

$$S[A] := \bigcap \{U \,|U \text{ υποδακτύλιος τού } R \text{ με } S \cup A \subseteq U\}$$

τού R (έχων ως μοναδιαίο του στοιχείο το 1_R) που περιέχει τόσον το υποσύνολο A όσον και τον S (ως υποδακτύλιό του). Λέμε ότι ο $S[A]$ είναι ο **υποδακτύλιος τού R (ή η επέκταση τού S εντός τού R) που προκύπτει ύστερα από προσάρτηση τού A στον S.** Στην ειδική περίπτωση όπου το A είναι ένα *πεπερασμένο* υποσύνολο $\{a_1, ..., a_k\}$ τού R, τότε αντί τού $S[A]$ γράφουμε απλώς $S[a_1, ..., a_k]$.

6.1.16 Πρόταση. *Εάν στον ορισμό 6.1.15 $A = \{a\}$, όπου το $a \in R$ είναι ένα στοιχείο τέτοιο, ώστε να ισχύει $as = sa$ για κάθε $s \in S$, τότε*

$$S[a] = \left\{ \sum_{j=0}^{\nu} s_j a^j \,\middle|\, \nu \in \mathbb{N}_0 \text{ και } s_0, ..., s_\nu \in S \right\}. \tag{6.8}$$

Απόδειξη. Θέτοντας

$$T := \left\{ \sum_{j=0}^{\nu} s_j a^j \,\middle|\, \nu \in \mathbb{N}_0 \text{ και } s_0, ..., s_\nu \in S \right\}$$

παρατηρούμε ότι $1_S = 1_R \in T$ (θεωρώντας ένα τέτοιο πεπερασμένο άθροισμα με $s_0 := 1_S$ και $s_j := 0$, $\forall j \in \{1, ..., \nu\}$). Για δυο στοιχεία $t = \sum_{j=0}^{\nu} s_j a^j$ και $t' = \sum_{j=0}^{\nu'} s'_j a^j$ τού T μπορούμε (δίχως βλάβη τής γενικότητας) να υποθέσουμε ότι $\nu \leqslant \nu'$ και να ορίσουμε $s'_j := 0_R$, για κάθε j με $\nu + 1 \leqslant j$ και $j \leqslant \nu'$. Επειδή το a (εξ υποθέσεως) μετατίθεται αμοιβαίως με κάθε στοιχείο τού υποδακτυλίου S, έχουμε

$$(s_j a^j)(s_{j'} a^{j'}) = s_j (a^j s_{j'}) a^{j'} = s_j (s_{j'} a^j) a^{j'} = (s_j s_{j'}) a^{j+j'}$$

για κάθε ζεύγος $(j, j') \in \{1, ..., \nu'\} \times \{1, ..., \nu'\}$, οπότε

$$t - t' = \sum_{j=0}^{\nu'} (s_j + s'_j) a^j \in T \text{ και } tt' = \sum_{\kappa=0}^{\nu+\nu'} \Big(\sum_{j=0}^{\kappa} s_j s'_{\kappa-j} \Big) a^\kappa \in T$$

και το T αποτελεί υποδακτύλιο τού R. Μάλιστα, ο T πέραν τού 1_S περιέχει *και* το $a = (1_S)a \in T$ και ισχύει $S \subseteq T$ (διότι $s_0 a^0 = s_0(1_R) = s_0$ για κάθε $s_0 \in S$). Άρα $S[a] \subseteq T$. Από την άλλη μεριά, εάν U είναι τυχών υποδακτύλιος τού R που περιέχει τόσον τον S όσον και το στοιχείο a, είναι προφανές ότι ο U περιέχει όλες τις δυνάμεις u^j, $j \in \mathbb{N}_0$, τού u, τα γινόμενα αυτών su^j, $j \in \mathbb{N}_0$, για κάθε $s \in S$, και, ως εκ τούτου, *και* όλα τα στοιχεία τού R που εκφράζονται υπό τη μορφή $\sum_{j=0}^{\nu} s_j a^j$, όπου $\nu \in \mathbb{N}_0$ και $s_0, ..., s_\nu \in S$. Επομένως, $T \subseteq S[a]$ και η ισότητα (6.8) είναι αληθής. □

6.1.17 Παράδειγμα. Εάν $R = \mathbb{Q}$ και $S = \mathbb{Z}$, τότε $\mathbb{Z}[\frac{1}{5}] = \left\{ \frac{k}{5^n} \,\middle|\, k \in \mathbb{Z}, n \in \mathbb{N}_0 \right\}$.

6.1.18 Παραδείγματα. Όταν $R = \mathbb{C}$ και $S = \mathbb{Z}$, χαρακτηριστικά παραδείγματα είναι τα εξής:

(i) Για $a = i$ (όπου i η «φανταστική» μονάδα) λαμβάνουμε τον δακτύλιο (6.6) των γκαουσιανών ακεραίων. (Ως εκ τούτου, ο $\mathbb{Z}[i]$ είναι ο ελάχιστος υποδακτύλιος τού $\mathbb{C}$ που περιέχει τα i και $\mathbb{Z}$.) Γενικότερα, εάν το $m \in \mathbb{Z}$ δεν είναι τέλειο τετράγωνο,

τότε για $a = \sqrt{m}$ λαμβάνουμε τον δακτύλιο (6.7). (Ως εκ τούτου, ο $\mathbb{Z}[\sqrt{m}]$ είναι ο ελάχιστος υποδακτύλιος τού $\mathbb{C}$ που περιέχει τα $\sqrt{m}$ και $\mathbb{Z}$.)

(ii) Εάν $\zeta_n := \exp\left(\frac{2\pi i}{n}\right) = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right), \forall n \in \mathbb{N}$, τότε για $n \geqslant 3$ και $a = \zeta_n$ λαμβάνουμε τον δακτύλιο

$$\mathbb{Z}[\zeta_n] = \left\{ \sum_{j=0}^{n-2} s_j \zeta_n^j \,\middle|\, s_0, ..., s_{n-2} \in \mathbb{Z} \right\},$$

διότι $\zeta_n^j = \zeta_n^i$, όταν $j > n$ και $j \equiv i (\mathrm{mod}\, n)$, $0 \leqslant i < n$, και[7] $\zeta_n^{n-1} = -\sum_{k=0}^{n-2} \zeta_n^k$.

6.2 ΑΚΕΡΑΙΕΣ ΠΕΡΙΟΧΕΣ ΚΑΙ ΣΩΜΑΤΑ

6.2.1 Ορισμός. Έστω R ένας δακτύλιος. Ένα στοιχείο $a \in R \setminus \{0_R\}$ καλείται **δεξιός** (και αντιστοίχως, **αριστερός**) **μηδενοδιαιρέτης** όταν υφίσταται ένα $b \in R \setminus \{0_R\}$ (αντ. $c \in R \setminus \{0_R\}$), τέτοιο ώστε $ba = 0_R$ (και αντιστοίχως, $ac = 0_R$). Ένα στοιχείο τού[8] $R \setminus \{0_R\}$ καλείται **αμφίπλευρος μηδενοδιαιρέτης** ή απλώς **μηδενοδιαιρέτης** όταν αυτό είναι ταυτοχρόνως και δεξιός και αριστερός μηδενοδιαιρέτης. Το σύνολο όλων των μηδενοδιαιρετών ενός δακτυλίου R θα συμβολίζεται ως $\mathbf{Zdv}(R)$.

6.2.2 Παράδειγμα. Στον δακτύλιο $\mathrm{Mat}_{2\times 2}(R)$, όπου R ένας δακτύλιος με μοναδιαίο στοιχείο, έχουμε

$$\begin{pmatrix} 0_R & 0_R \\ 1_R & 0_R \end{pmatrix} \in \mathbf{Zdv}\left(\mathrm{Mat}_{2\times 2}(R)\right)$$

διότι

$$\begin{pmatrix} 1_R & 0_R \\ 0_R & 0_R \end{pmatrix} \begin{pmatrix} 0_R & 0_R \\ 1_R & 0_R \end{pmatrix} = \begin{pmatrix} 0_R & 0_R \\ 0_R & 0_R \end{pmatrix},$$

και

$$\begin{pmatrix} 0_R & 0_R \\ 1_R & 0_R \end{pmatrix} \begin{pmatrix} 0_R & 0_R \\ 0_R & 1_R \end{pmatrix} = \begin{pmatrix} 0_R & 0_R \\ 0_R & 0_R \end{pmatrix}.$$

6.2.3 Παρατήρηση. Στους *μεταθετικούς* δακτυλίους κάθε αριστερός μηδενοδιαιρέτης είναι δεξιός και αντιστρόφως. Ως εκ τούτου, δεν χρειάζεται να γίνεται διάκριση μεταξύ των δύο αυτών εννοιών.

6.2.4 Πρόταση. *Στον δακτύλιο $\mathbb{Z}_m$, $m \geqslant 1$, έχουμε*

$$\boxed{\mathbf{Zdv}(\mathbb{Z}_m) = \{[k]_m \in \mathbb{Z}_m \mid 1 \leqslant k \leqslant m-1, \ \ \mu\kappa\delta(k,m) > 1\}}$$

Απόδειξη. Όταν $m = 1$, η ισότητα είναι προφανής, αφού $\mathbf{Zdv}(\mathbb{Z}_m) = \varnothing$. Από εδώ και στο εξής θα υποθέτουμε ότι $m \geqslant 2$.

" $\supseteq$ " Έστω $[k]_m \in \mathbb{Z}_m$, όπου $1 \leqslant k \leqslant m-1$, με $d := \mu\kappa\delta(k,m) > 1$. Τότε

$$\begin{aligned} [k]_m \left([m/d]_m\right) &= [km/d]_m = [(k/d)\, m]_m = [k/d]_m\, [m]_m \\ &= [k/d]_m\, [0]_m = [0]_m \Longrightarrow [k]_m \in \mathbf{Zdv}\left(\mathbb{Z}_m\right). \end{aligned}$$

" $\subseteq$ " Αυτό θα προκύψει άμεσα από την κάπως γενικότερη πρόταση 6.2.17. □

[7] Προφανώς, $0 = \zeta_n^n - 1 = (\zeta_n - 1)\left(\sum_{k=0}^{n-1} \zeta_n^k\right) \Rightarrow \sum_{k=0}^{n-1} \zeta_n^k = 0$, διότι $\zeta_n \neq 1$.

[8] Προσοχή! Ορισμένοι συγγραφείς συγκαταλέγουν *και το* 0_R στους μηδενοδιαιρέτες τού R (χαρακτηρίζοντάς το ως τον «τετριμμένο» μηδενοδιαιρέτη τού R). Ωστόσο, τούτη η *σύμβαση* **δεν** θα υιοθετηθεί εδώ!

6.2.5 Πρόταση (Νόμος διαγραφής). *Έστω R ένας δακτύλιος. Τότε ο R δεν έχει δεξιούς μηδενοδιαιρέτες εάν και μόνον εάν για όλα τα στοιχεία $a, b \in R$ και όλα τα $c \in R \setminus \{0_R\}$ ισχύει ο εξής νόμος τής διαγραφής*:

$$ca = cb \Longrightarrow a = b.$$

Κατ' αναλογίαν, ο R δεν έχει αριστερούς μηδενοδιαιρέτες εάν και μόνον εάν για όλα τα στοιχεία $a, b \in R$ και όλα τα $c \in R \setminus \{0_R\}$ ισχύει ο ακόλουθος νόμος τής διαγραφής:

$$ac = bc \Longrightarrow a = b.$$

Κατά συνέπειαν, ο R δεν έχει ούτε δεξιούς ούτε αριστερούς μηδενοδιαιρέτες εάν και μόνον εάν για όλα τα στοιχεία $a, b \in R$ και όλα τα $c \in R \setminus \{0_R\}$ ισχύει ο εξής νόμος τής διαγραφής:

$$[ca = cb \quad \text{ή} \quad ac = bc] \Longrightarrow a = b.$$

(Στους μεταθετικούς δακτυλίους οι δύο πρώτοι νόμοι διαγραφής ενσωματώνονται προδήλως σε έναν.)

Απόδειξη. Εάν ο R είναι ένας δακτύλιος χωρίς δεξιούς (και αντιστοίχως, χωρίς αριστερούς) μηδενοδιαιρέτες και $c \in R \setminus \{0\}$, τότε η ισότητα $ca = cb$ (και αντιστοίχως, η ισότητα $ac = bc$) γράφεται ως $c(a - b) = 0_R$ (και αντιστοίχως, ως $(a-b)c = 0_R$), πράγμα που σημαίνει ότι $a-b = 0_R$, δηλαδή $a = b$. Και αντιστρόφως· προϋποθέτοντας την ισχύ τού πρώτου (και αντιστοίχως, τού δεύτερου) εκ των νόμων τής διαγραφής, αρκεί να δείξουμε ότι για οιαδήποτε στοιχεία $c, d \in R$, η $cd = 0_R$ σημαίνει ότι $[c \neq 0_R \Longrightarrow d = 0_R]$ (και αντιστοίχως, ότι $[d \neq 0_R \Longrightarrow c = 0_R]$). Πράγματι· εάν $c \neq 0_R$, τότε έχουμε $cd = 0_R = c \cdot 0_R$, οπότε από τον πρώτο νόμο τής διαγραφής λαμβάνουμε $d = 0_R$, ενώ εάν $d \neq 0_R$, τότε η $cd = 0_R = 0_R \cdot d$ μας δίδει (κατ' αναλογίαν, μέσω τού δεύτερου νόμου τής διαγραφής) $c = 0_R$. □

6.2.6 Παράδειγμα. Στον δακτύλιο $\mathbb{Z}_6$ δεν ισχύει ο νόμος τής διαγραφής. (Σημειωτέον ότι $[2]_6\,[3]_6 = [6]_6 = [0]_6$, οπότε οι $[2]_6$ και $[3]_6$ είναι μηδενοδιαιρέτες. Μάλιστα, σύμφωνα με την πρόταση 6.2.4, $\mathbf{Zdv}(\mathbb{Z}_6) = \{[2]_6, [3]_6, [4]_6\}$.)

6.2.7 Ορισμός. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο[9] $1_R \neq 0_R$. Ένα στοιχείο $a \in R$ καλείται **εξ αριστερών** (και αντιστοίχως, **εκ δεξιών**) **αντιστρέψιμο** όταν $\exists b \in R$ (και αντιστοίχως, $\exists c \in R$), τέτοιο ώστε $ba = 1_R$ (και αντιστοίχως, $ac = 1_R$). Ένα τέτοιο $b \in R$ (αντ. $c \in R$) λέγεται **αριστερό** (και αντιστοίχως, **δεξιό**) **αντίστροφο**[10] τού a. Ένα στοιχείο τού R καλείται **αμφιπλεύρως αντιστρέψιμο** ή απλώς **αντιστρέψιμο** όταν αυτό είναι ταυτοχρόνως και εξ αριστερών και εκ δεξιών αντιστρέψιμο. Το σύνολο όλων των αντιστρεψίμων στοιχείων ενός μη τετριμμένου δακτυλίου R με μοναδιαίο στοιχείο θα συμβολίζεται ως $R^\times$.

6.2.8 Πρόταση. *Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο και έστω $a \in R^\times$. Εάν το a διαθέτει το b ως ένα αριστερό αντίστροφό του και το c ως ένα δεξιό αντίστροφό του, τότε $b = c$.*

[9] Η συνθήκη $1_R \neq 0_R$ ισοδυναμεί με το ότι ο R δεν είναι τετριμμένος (βλ. 6.1.4 (vi)). Πράγματι· εάν $1_R = 0_R$, τότε για κάθε $a \in R$ έχουμε $a = 1_R \cdot a = 0_R \cdot a = 0_R$, οπότε ο R οφείλει να είναι τετριμμένος. Το αντίστροφο είναι προφανές.

[10] Προσοχή! Η ύπαρξη ενός αριστερού αντιστρόφου ενός $a \in R$ δεν εγγυάται *αυτομάτως* την ύπαρξη κάποιου δεξιού αντιστρόφου του και τανάπαλιν. Επίσης, δεν αποκλείεται ένα παγιωμένο $a \in R$ να διαθέτει δεξιά (και αντιστοίχως, αριστερά) αντίστροφα *περισσότερα τού ενός*. Τούτα (όπως δείχνεται στα εδάφια 6.2.8 και 6.2.9) αλλάζουν άρδην όταν περιοριζόμαστε στα *(αμφιπλεύρως) αντιστρέψιμα* στοιχεία.

Απόδειξη. Χρησιμοποιώντας τις ισότητες $ba = 1_R = ac$ συμπεραίνουμε άμεσα ότι $c = 1_R c = (ba)c = b(ac) = b\,1_R = b$. □

6.2.9 Συμβολισμός. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο και έστω $a \in R^\times$. Τότε υπάρχει κάποιο στοιχείο τού R, ας το πούμε b, τέτοιο ώστε $ba = 1_R = ab$ (επί τη βάσει τού ορισμού 6.2.7 και τής προτάσεως 6.2.8). Το b είναι *το μόνο* στοιχείο τού R που πληροί αυτήν την ιδιότητα, διότι για οιοδήποτε $b' \in R$ με $b'a = 1_R = ab'$ έχουμε $b = b'$ (αφού το b είναι αριστερό αντίστροφο και το b' δεξιό αντίστροφο τού a και τανάπαλιν). Αυτό το b καλείται **αντίστροφο στοιχείο τού** a και θα συμβολίζεται εφεξής ως a^{-1}. (Προφανώς, $1_R^{-1} = 1_R$, $\{\pm 1_R\} \subseteq R^\times$, $0_R \notin R^\times$ και για κάθε $a \in R^\times$ έχουμε $-a \in R^\times$ με $(-a)^{-1} = -a^{-1}$.) Επίσης, για κάθε στοιχείο $a \in R^\times$ και κάθε $n \in \mathbb{N}$, θα γράφουμε εν συντομία $a^{-n} := (a^{-1})^n$. (Πρβλ. 6.1.6).

6.2.10 Πρόταση. *Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Τότε το ζεύγος $(R^\times, \cdot)$ αποτελεί μια πολλαπλασιαστική ομάδα.*

Απόδειξη. Έπεται άμεσα κατόπιν εφαρμογής τής προτάσεως 3.2.6 για το μονοειδές $(R, \cdot)$. □

6.2.11 Ορισμός. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Η ομάδα $R^\times$ καλείται **ομάδα των αντιστρεψίμων στοιχείων τού** R.

6.2.12 Σημείωση. (i) Η $R^\times$ είναι δυνατόν να είναι αβελιανή ακόμη και όταν ο R δεν είναι μεταθετικός. (Πρβλ. άσκηση 21 (v) τού φυλλαδίου 11).

(ii) Άλλοτε η $R^\times$ έχει *πεπερασμένη* τάξη, όπως στην περίπτωση θεωρήσεως τού δακτυλίου $R = \mathbb{Z}_m$, $m \geqslant 2$, με

$$\mathbb{Z}_m^\times = \{[k]_m \in \mathbb{Z}_m \mid 1 \leqslant k \leqslant m-1,\ \ \text{μκδ}\,(k,m) = 1\}$$

και $|\mathbb{Z}_m^\times| = \phi(m)$, όπου ϕ η συνάρτηση τού Euler, και άλλοτε *άπειρη*. Επί παραδείγματι, η

$$\mathbb{Z}[\sqrt{2}]^\times = \left\{\pm(1+\sqrt{2})^k \mid k \in \mathbb{Z}\right\}$$

είναι άπειρη αριθμήσιμη και η $(\text{Mat}_{n\times n}(\mathbb{R}))^\times$ άπειρη υπεραριθμήσιμη (βλ. πρόταση 6.2.14).

(iii) Εάν ο S είναι ένας μη τετριμμένος υποδακτύλιος (με μοναδιαίο στοιχείο 1_S) ενός δακτυλίου R με μοναδιαίο στοιχείο $1_R = 1_S$, τότε $S^\times \subseteq R^\times \cap S$, χωρίς να αποκλείεται ο εγκλεισμός να είναι αυστηρός. Επί παραδείγματι, όταν $R = \mathbb{R}$ και $S = \mathbb{Z}$, τότε $2 \in R^\times = \mathbb{R}\setminus\{0\}$ αλλά $2 \notin S^\times = \{\pm 1\}$.

(iv) Εάν ο S είναι ένας μη τετριμμένος υποδακτύλιος (με μοναδιαίο στοιχείο 1_S) ενός δακτυλίου R με μοναδιαίο στοιχείο $1_R \neq 1_S$, τότε ενδέχεται να υπάρχει κάποιο στοιχείο τού S που είναι αντιστρέψιμο εντός τού S και μη αντιστρέψιμο εντός τού R. Επί παραδείγματι, όταν $R := \text{Mat}_{2\times 2}(\mathbb{R})$ και $S := \left\{ \begin{pmatrix} x & x \\ x & x \end{pmatrix} \middle| \, x \in \mathbb{R} \right\}$, τότε

$$1_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = 1_S$$

και για κάθε $x \in \mathbb{R}\setminus\{0\}$ έχουμε

$$\begin{pmatrix} x & x \\ x & x \end{pmatrix} \begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix} = 1_S = \begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix} \begin{pmatrix} x & x \\ x & x \end{pmatrix},$$

οπότε

$$\begin{pmatrix} x & x \\ x & x \end{pmatrix} \in S^{\times} \text{ και } \begin{pmatrix} x & x \\ x & x \end{pmatrix} \notin R^{\times} \cap S = \{\mathbf{A} \in S \mid \det(\mathbf{A}) \neq 0\} (= \varnothing),$$

όπου ως $\det(\mathbf{A})$ συμβολίζουμε την ορίζουσα τού $\mathbf{A}$.

6.2.13 Ορισμός. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο και έστω $n \in \mathbb{N}$. Η ομάδα των αντιστρεψίμων πινάκων

$$\boxed{\mathrm{GL}_n(R) := (\mathrm{Mat}_{n\times n}(R))^{\times}}$$

τού $\mathrm{Mat}_{n\times n}(R)$ καλείται, ιδιαιτέρως, **γενική γραμμική ομάδα (βαθμού n υπεράνω τού R)**.

6.2.14 Θεώρημα. *Για κάθε μη τετριμμένο μεταθετικό δακτύλιο R με μοναδιαίο στοιχείο και για κάθε $n \in \mathbb{N}$ ισχύει η ισότητα*

$$\boxed{\mathrm{GL}_n(R) = \{\mathbf{A} \in \mathrm{Mat}_{n\times n}(R) \mid \det(\mathbf{A}) \in R^{\times}\}.} \tag{6.9}$$

Επιπροσθέτως, για κάθε $\mathbf{A} \in \mathrm{GL}_n(R)$,

$$\boxed{\det(\mathbf{A}^{-1}) = \det(\mathbf{A})^{-1}} \tag{6.10}$$

και για $n \geqslant 2$,

$$\boxed{\mathbf{A}^{-1} = \det(\mathbf{A})^{-1}\mathbf{adj}(\mathbf{A}),} \tag{6.11}$$

όπου ως $\det(\mathbf{A})$ συμβολίζουμε την ορίζουσα τού $\mathbf{A}$ και ως $\mathbf{adj}(\mathbf{A})$ τον πίνακα τον προσαρτημένο στον $\mathbf{A}$.

Απόδειξη. Βλ. θεώρημα A.2.18. □

6.2.15 Ορισμός. Ένα στοιχείο a ενός δακτυλίου R λέγεται **μηδενοδύναμο** όταν ισχύει $a^n = 0_R$ για κάποιον $n \in \mathbb{N}$. Το σύνολο όλων των μηδενοδυνάμων στοιχείων τού R θα συμβολίζεται ως $\mathrm{Nil}(R)$. (Ως **δείκτης** ενός $a \in \mathrm{Nil}(R)$ ορίζεται ο $\nu := \min\{n \in \mathbb{N} \mid a^n = 0_R\}$.)

6.2.16 Παράδειγμα. Στον δακτύλιο $R = \mathrm{Mat}_{2\times 2}(\mathbb{Z})$ έχουμε

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_R \Rightarrow \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in \mathrm{Nil}(R) \text{ (με δείκτη 2).}$$

6.2.17 Πρόταση. *Για κάθε μη τετριμμένο δακτύλιο R με μοναδιαίο στοιχείο ισχύουν οι εγκλειστικές σχέσεις:*

$$\boxed{\{1_R\} \subseteq R^{\times} \subseteq R \smallsetminus \mathrm{Zdv}(R) \subseteq (R \smallsetminus \mathrm{Nil}(R)) \cup \{0_R\} \subseteq R}$$

και

$$\boxed{\mathrm{Nil}(R) \smallsetminus \{0_R\} \subseteq \mathrm{Zdv}(R) \subseteq R \smallsetminus R^{\times} \subseteq R.}$$

Απόδειξη. Έστω τυχόν στοιχείο $a \in \mathrm{Nil}(R) \smallsetminus \{0_R\}$. Εάν το a έχει δείκτη ν, τότε (προφανώς) $a^{\nu-1} \neq 0_R$ και $a^{\nu} = a^{\nu-1}a = a\,a^{\nu-1} = 0_R \Longrightarrow a \in \mathrm{Zdv}(R)$. Έστω

τώρα ότι $b \in \mathrm{Zdv}(R)$, δηλαδή ότι υπάρχουν $c, d \in R \smallsetminus \{0_R\}$ με $cb = bd = 0_R$. Εάν υποθέσουμε ότι $b \in R^\times$, τότε θα υπάρχουν $e, g \in R$, τέτοια ώστε $eb = bg = 1_R$. Αυτό όμως μας οδηγεί σε ένα άτοπο συμπέρασμα, αφού

$$\begin{aligned} 0_R &= (0_R)\, g = (cb)\, g = c\,(bg) = c\,(1_R) = c, \quad \text{ή} \\ 0_R &= e\,(0_R) = e\,(bd) = (eb)\, d = (1_R)\, d = d\,. \end{aligned}$$

Επομένως, $\mathrm{Zdv}(R) \cap R^\times = \varnothing$. Οι λοιπές εγκλειστικές σχέσεις είναι προφανείς. □

6.2.18 Ορισμός. (i) Κάθε μεταθετικός μη τετριμμένος δακτύλιος R με μοναδιαίο στοιχείο και $\mathrm{Zdv}(R) = \varnothing$ καλείται **ακεραία περιοχή**[11]**.**

(ii) Κάθε μη τετριμμένος δακτύλιος R με μοναδιαίο στοιχείο και $R^\times = R \smallsetminus \{0_R\}$ καλείται **διαιρετικός**[12] **δακτύλιος** ή **στρεβλό σώμα**[13]**.**

(iii) Κάθε μεταθετικός διαιρετικός δακτύλιος καλείται **σώμα.**

6.2.19 Παραδείγματα. (i) Οι δακτύλιοι $\mathbb{Q}, \mathbb{R}$ και $\mathbb{C}$ αποτελούν σώματα. Από την άλλη μεριά, όπως είδαμε στα 6.1.4 (ii) και 6.2.2, ο δακτύλιος $\mathrm{Mat}_{2\times 2}(R)$, όπου το R είναι ένας εκ των $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, δεν μπορεί να είναι ούτε καν ακεραία περιοχή.

(ii) Έστω $\mathbb{H}_\mathbb{R} := \left\{ a\,\mathbf{I} + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \;\middle|\; (a,b,c,d) \in \mathbb{R}^4 \right\}$ ο υποδακτύλιος τού δακτυλίου $\mathrm{Mat}_{2\times 2}(\mathbb{C})$ ο οριζόμενος μέσω των πραγματικών γραμμικών συνδυασμών των τεσσάρων πινάκων[14]

$$\mathbf{I} := \mathbf{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \mathbf{j} := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ \mathbf{k} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ \mathbf{i} := \mathbf{jk} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Ο $\mathbb{H}_\mathbb{R}$ γράφεται ως εξής:

$$\boxed{\mathbb{H}_\mathbb{R} = \left\{ \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \middle|\ (a,b,c,d) \in \mathbb{R}^4 \right\}.}$$

Ο $\mathbb{H}_\mathbb{R}$ έχει το $1_{\mathrm{Mat}_{2\times 2}(\mathbb{C})} = \mathbf{I}$ ως μοναδιαίο του στοιχείο. Ωστόσο, *δεν* είναι μεταθετικός, διότι π.χ. $\mathbf{i} \neq -\mathbf{i} = \mathbf{kj}$. Θεωρώντας ένα στοιχείο του

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

ένας τουλάχιστον εκ των a, b, c, d οφείλει να είναι $\neq 0$, πράγμα που σημαίνει ότι και η ορίζουσά του, η οποία ισούται με $a^2 + b^2 + c^2 + d^2$, θα είναι $\neq 0$. Προφανώς, ο αντίστροφός του πίνακας

$$\frac{1}{a^2+b^2+c^2+d^2} \begin{pmatrix} a-bi & -c-di \\ c-di & a+bi \end{pmatrix} \in \left(\mathrm{Mat}_{2\times 2}(\mathbb{C})\right)^\times$$

[11] Προφανώς, ένας μη τετριμμένος μεταθετικός δακτύλιος R με μοναδιαίο στοιχείο είναι ακεραία περιοχή εάν και μόνον εάν σε αυτόν ισχύει ο νόμος τής διαγραφής (βλ. πρόταση 6.2.5) ή, ισοδυνάμως, εάν και μόνον εάν από την ισότητα $ab = 0_R$ (όπου $a, b \in R$) έπεται κατ' ανάγκην ότι είτε $a = 0_R$ είτε $b = 0_R$.

[12] Η ονομασία «διαιρετικός δακτύλιος» (ή «δακτύλιος με διαίρεση») προέρχεται από το γεγονός τού ότι σε τέτοιου είδους δακτυλίους ορίζεται πάντοτε το ab^{-1}, *για κάθε* $a \in R$ και $b \in R \smallsetminus \{0_R\}$.

[13] Προφανώς, ο πληθικός αριθμός τού υποκειμένου συνόλου μιας ακεραίας περιοχής ή ενός στρεβλού σώματος R είναι $\geqslant 2$ (αφού περιέχει τόσον το 1_R όσον και το $0_R (\neq 1_R)$).

[14] Όπως έχουμε ήδη δει, η λεγόμενη **ομάδα Q των τετρανίων** (βλ. εδ. 3.3.11), η οποία παράγεται από τα στοιχεία **j** και **k**, υπεισέρχεται ουσιωδώς στην ταξινόμηση των πεπερασμένων ομάδων τάξεως 8. (Βλ. θεώρημα 5.1.39.)

ανήκει στην ομάδα $\mathbb{H}_{\mathbb{R}}^{\times}$. Άρα ο $\mathbb{H}_{\mathbb{R}}$ αποτελεί έναν *διαιρετικό δακτύλιο*[15], ο οποίος ονομάζεται **δακτύλιος των τετρανίων**[16] **υπεράνω τού σώματος**[17] $\mathbb{R}$.

6.2.20 Πρόταση. *Κάθε μη τετριμμένος υποδακτύλιος S μιας ακεραίας περιοχής R, για τον οποίον $1_R \in S$, είναι ακεραία περιοχή.*

Απόδειξη. Επειδή $S \subseteq R$, έχουμε $1_S = 1_R$ και $\mathrm{Zdv}(S) \subseteq \mathrm{Zdv}(R) = \varnothing$. □

6.2.21 Παρατήρηση. Ο υποδακτύλιος $2\mathbb{Z}$ τού δακτυλίου $\mathbb{Z}$ *δεν* είναι ακεραία περιοχή, παρότι $\mathrm{Zdv}(2\mathbb{Z}) = \varnothing$, αφού δεν διεθέτει μοναδιαίο στοιχείο.

6.2.22 Πόρισμα. *Κάθε μη τετριμμένος υποδακτύλιος S ενός σώματος K, για τον οποίον $1_K \in S$, είναι ακεραία περιοχή.* (*Ειδικότερα, κάθε σώμα είναι ακεραία περιοχή.*)

6.2.23 Παράδειγμα. Υπάρχουν ακέραιες περιοχές που δεν είναι σώματα. Τα απλούστερα παραδείγματα μας τα παρέχουν ο δακτύλιος $\mathbb{Z}$ των ακεραίων (με τις συνήθεις πράξεις), αφού $\mathrm{Zdv}(\mathbb{Z}) = \varnothing$ και $\mathbb{Z}^{\times} = \{-1, +1\} \subsetneqq \mathbb{Z} \setminus \{0\}$, και ο δακτύλιος $\mathbb{Z}[i]$ των ακεραίων τού Gauss, αφού $\mathrm{Zdv}(\mathbb{Z}[i]) = \varnothing$ και

$$\mathbb{Z}[i]^{\times} = \{-1, +1, -i, i\} \subsetneqq \mathbb{Z}[i] \setminus \{0\}.$$

Από την άλλη μεριά, για *πεπερασμένους* μεταθετικούς δακτυλίους με μοναδιαίο στοιχείο $1_R \neq 0_R$ οι έννοιες ακεραία περιοχή και σώμα ταυτίζονται. (Βλ. πρόταση 6.2.26).

6.2.24 Σημείωση. Εάν R είναι μια ακεραία περιοχή και ο S υποδακτύλιός της με μοναδιαίο στοιχείο, ο οποίος συμβαίνει να είναι ακεραία περιοχή ως προς τις ίδιες πράξεις, τότε ο S καλείται **υποπεριοχή** τής ακεραίας περιοχής R. (Όταν ο S είναι υποπεριοχή τής R, είναι εύκολο να δειχθεί ότι έχουμε κατ' ανάγκην $1_S = 1_R$.) Επί παραδείγματι, το

$$R := \left\{ \frac{a}{2^n} \in \mathbb{Q} \;\middle|\; a \in \mathbb{Z},\ n \in \mathbb{N}_0 \right\}$$

(ως προς τις συνήθεις πράξεις προσθέσεως και πολλαπλασιασμού ρητών αριθμών) είναι υποπεριοχή τού $\mathbb{Q}$ και $\mathbb{Z} \subsetneqq R \subseteq \mathbb{Q}$. (Βλ. άσκηση 20 τού φυλλαδίου 11.)

6.2.25 Σημείωση. Εάν το L είναι ένα σώμα και το K ένας υποδακτύλιος τού L με μοναδιαίο στοιχείο, ο οποίος συμβαίνει να είναι σώμα ως προς τις ίδιες πράξεις, τότε το K καλείται **υπόσωμα** τού L και το L (σωματική) **επέκταση** τού K. (Εν τοιαύτη περιπτώσει, $1_L = 1_K$.) Επί παραδείγματι, το $\mathbb{Q}$ είναι υπόσωμα τού $\mathbb{R}$ και το $\mathbb{R}$ υπόσωμα τού $\mathbb{C}$.

---

[15] Ο $\mathbb{H}_{\mathbb{R}}$ είναι εφοδιασμένος και με τη δομή ενός *τετραδιάστατου πραγματικού διανυσματικού χώρου*, αφού οι πίνακες $\mathbf{I}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ είναι και γραμμικώς ανεξάρτητοι υπεράνω τού $\mathbb{R}$.

[16] Τα «τετράνια» επινοήθηκαν από τον William Royal Hamilton (1805-1865) το έτος 1843 ως ένα αλγεβρικό σύστημα περιέχον το σώμα $\mathbb{C}$ των μιγαδικών αριθμών (γι' αυτό λέγονται και «υπερμιγαδικοί αριθμοί»). Το στρεβλό σώμα $\mathbb{H}_{\mathbb{R}}$, πέραν τής συχνής χρήσεώς του στη Διανυσματική Ανάλυση, υπεισέρχεται και σε εφαρμογές τόσον τής σύγχρονης Αλγεβρικής Τοπολογίας όσον και τής Μαθηματικής Φυσικής.

[17] Ενίοτε, εκτός τού ιδίου τού $\mathbb{H}_{\mathbb{R}}$, χρησιμοποιούνται (σε διάφορες εφαρμογές) και υποδακτύλιοι αυτού

$$\mathbb{H}_R := \left\{ a\mathbf{I} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \;\middle|\; (a, b, c, d) \in R^4 \right\} \subseteq \mathbb{H}_{\mathbb{R}}$$

οριζόμενοι υπεράνω διαφόρων υποδακτυλίων R τού σώματος $\mathbb{R}$. (Τα στοιχεία τού $\mathbb{H}_{\mathbb{Z}}$ καλούνται, ιδιαιτέρως, **ακέραια τετράνια** και τού $\mathbb{H}_{\mathbb{Q}}$ **ρητά τετράνια**. Ο $\mathbb{H}_{\mathbb{Q}}$ είναι αφ' εαυτού στρεβλό σώμα, διότι το αντίστροφο στοιχείο κάθε μη μηδενικού στοιχείου του εντός τού $\mathbb{H}_{\mathbb{R}}$ ανήκει στον ίδιον τον $\mathbb{H}_{\mathbb{Q}}$.)

6.2.26 Πρόταση. *Κάθε πεπερασμένος μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο, ο οποίος δεν διαθέτει ούτε αριστερούς ούτε δεξιούς μηδενοδιαιρέτες, είναι διαιρετικός. Ειδικότερα, κάθε πεπερασμένη ακεραία περιοχή είναι σώμα.*

Απόδειξη. Έστω R ένας πεπερασμένος μη τετριμμένος δακτύλιος χωρίς δεξιούς ή αριστερούς μηδενοδιαιρέτες και $a \in R \setminus \{0_R\}$. Αρκεί να προσδιορισθεί ένα στοιχείο $b \in R$ με

$$ab = ba = 1_R.$$

Θεωρούμε την απεικόνιση $\beta : R \to R$, την οριζόμενη μέσω τής $\beta(c) := ac$ (και, αντιστοίχως, μέσω τής $\beta(c) := ca$) για όλα τα $c \in R$. Σύμφωνα με τον νόμο τής διαγραφής 6.2.5, για $c, c' \in R$ με $\beta(c) = \beta(c')$, λαμβάνουμε $c = c'$. Άρα η β, ως ενριπτική απεικόνιση, θα είναι και επιριπτική. Αυτό σημαίνει ότι για το 1_R θα υπάρχει ένα αρχέτυπο μέσω τής β, δηλαδή ένα $b \in R$, τέτοιο ώστε $\beta(b) = 1_R$. (Όπως έχουμε ήδη προαναφέρει, τα αριστερά και δεξιά αντίστροφα ενός αντιστρεψίμου στοιχείου a ενός τέτοιου R ταυτίζονται.) □

6.2.27 Πόρισμα. *Οι ακόλουθες συνθήκες για τον δακτύλιο $\mathbb{Z}_m$, $m \geqslant 2$, είναι ισοδύναμες:*

(i) *Ο m είναι πρώτος αριθμός.*

(ii) *Ο $\mathbb{Z}_m$ είναι μια ακεραία περιοχή.*

(iii) *Ο $\mathbb{Z}_m$ αποτελεί ένα σώμα.*

Απόδειξη. Η συνεπαγωγή (i) ⇒ (ii) έπεται από την πρόταση 6.2.4, η (ii) ⇒ (iii) από την πρόταση 6.2.26, και η (iii) ⇒ (ii) από την πρόταση 6.2.22. Τέλος, για τη συνεπαγωγή (ii) ⇒ (i) ας υποθέσουμε ότι ο m είναι σύνθετος αριθμός, δηλαδή ότι γράφεται ως γινόμενο $m = pq$ δύο άλλων ακεραίων p, q, όπου $1 < p, q < m$. Αυτό θα σήμαινε ότι

$$[m]_m = [0]_m = [p]_m [q]_m$$

με $p \neq 0$ και $q \neq 0$, πράγμα που αντίκειται στην (ii). □

6.2.28 Θεώρημα (Wedderburn, 1905). *Κάθε πεπερασμένος διαιρετικός δακτύλιος είναι σώμα.*

Απόδειξη[18]. Βλ. T.W. Hungerford: *Algebra*, Graduate Texts in Mathematics, Vol. **73**, Springer-Verlag, fifth printing, 1989, Ch. IX, Cor. 6.9, p. 462. □

6.2.29 Ορισμός. Έστω L ένα σώμα και έστω $K \subseteq L$ ένα υπόσωμα αυτού. Εάν $\varnothing \neq A \subseteq L$, τότε ορίζεται το *ελάχιστο* (ως προς τη σχέση τού συνολοθεωρητικού εγκλεισμού) υπόσωμα

$$K(A) := \bigcap \{U \,|\, U \text{ υπόσωμα τού } L \text{ με } K \cup A \subseteq U\}$$

τού L που περιέχει τόσον το υποσύνολο A όσον και το K. Λέμε ότι το $K(A)$ είναι το **υπόσωμα τού L (ή η επέκταση τού K εντός τού L) που προκύπτει ύστερα από προσάρτηση τού A στο K**. Στην ειδική περίπτωση όπου το A είναι ένα *πεπερασμένο* υποσύνολο $\{a_1, ..., a_k\}$ τού L, τότε αντί τού $K(A)$ γράφουμε απλώς $K(a_1, ..., a_k)$.

[18] Για την αρχική απόδειξη βλ. J.H.M. Wedderburn: *A theorem on finite algebras*, Trans. Amer. Math. Soc. **6** (1905), 349-352.

6.2.30 Σημείωση. Λαμβάνοντας υπ' όψιν τον ορισμό 6.1.15, διαπιστώνουμε ότι $K[A] \subseteq K(A)$, ήτοι ότι ο *υποδακτύλιος* $K[A]$ τού L που προκύπτει ύστερα από προσάρτηση τού A στο K περιέχεται (ενδεχομένως και γνησίως) εντός τού *υποσώματος* $K(A)$ τού L που προκύπτει ύστερα από προσάρτηση τού A στο K (διότι ο δακτύλιος $K[A]$ δεν είναι κατ' ανάγκην σώμα).

6.2.31 Παραδείγματα. (i) Έστω m ένας ακέραιος αριθμός που δεν είναι τέλειο τετράγωνο (δηλαδή $\sqrt{|m|} \notin \mathbb{Q}$). Είναι εύκολο να δειχθεί ότι ο υποδακτύλιος[19]

$$\boxed{\mathbb{Q}[\sqrt{m}] = \{r + s\sqrt{m} \mid r, s \in \mathbb{Q}\} \subsetneq \mathbb{C}} \tag{6.12}$$

τού σώματος $\mathbb{C}$ που προκύπτει ύστερα από προσάρτηση τού $\sqrt{m}$ στο $\mathbb{Q}$ είναι *υπόσωμα* τού $\mathbb{C}$ (βλ. το (iv) τής ασκήσεως 24 τού φυλλαδίου 11), οπότε[20]

$$\boxed{\mathbb{Q}[\sqrt{m}] = \mathbb{Q}(\sqrt{m}).}$$

Σημειωτέον ότι ισχύουν οι ακόλουθοι εγκλεισμοί:

$$\mathbb{Z} \subsetneq \mathbb{Z}[\sqrt{m}] \subsetneq \mathbb{Q}(\sqrt{m}), \quad \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{m}).$$

(ii) Αντιθέτως, για τον υποδακτύλιο τού σώματος $\mathbb{R}$ που προκύπτει ύστερα από προσάρτηση τού

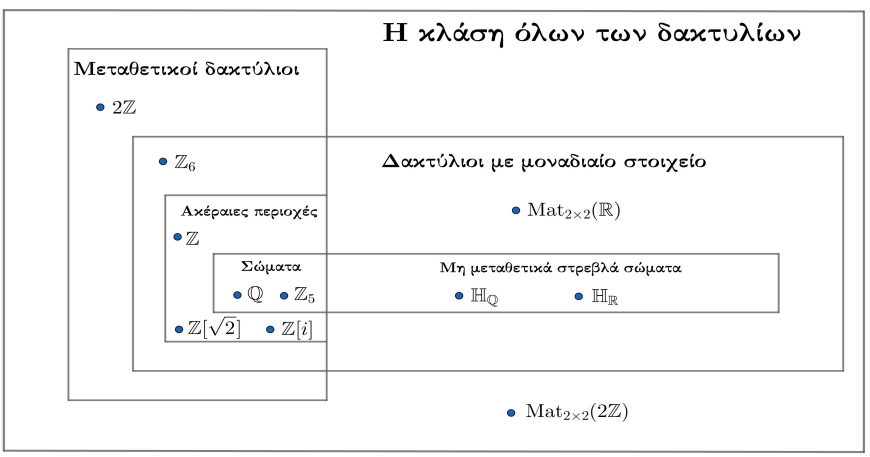
$$\boldsymbol{\pi} = 3,14159.....$$

(ήτοι τού λόγου τού μήκους τής περιφέρειας ενός κύκλου προς τη διάμετρό του) στο $\mathbb{Q}$ έχουμε

$$\boxed{\mathbb{Q}[\boldsymbol{\pi}] \underset{(6.8)}{=} \left\{ \sum_{j=0}^{\nu} r_j \pi^j \,\middle|\, \nu \in \mathbb{N}_0 \text{ και } r_0, ..., r_\nu \in \mathbb{Q} \right\} \subsetneq \mathbb{Q}(\pi),}$$

διότι $\boldsymbol{\pi}^{-1} \in \mathbb{Q}(\boldsymbol{\pi}) \setminus \mathbb{Q}[\boldsymbol{\pi}]$ (λόγω τής υπερβατικότητας τού $\boldsymbol{\pi}$).

6.2.32 Σημείωση. Κατά τα προαναφερθέντα, είναι εφικτή μια υποδιαίρεση τής κλάσεως όλων των δακτυλίων σε υποκλάσεις, βασιζόμενη σε έννοιες απορρέουσες από τις πρωταρχικές ιδιότητες τής πολλαπλασιαστικής πράξεως, την ύπαρξη ή μη μηδενοδιαιρετών και το «εύρος» τής πολλαπλασιαστικής ομάδας των αντιστρεψίμων στοιχείων. Οι εν λόγω υποκλάσεις, καθώς και χαρακτηριστικά παραδείγματα δακτυλίων ανήκοντα σε κάθε μία εξ αυτών, καταχωρίζονται στο ακόλουθο διάγραμμα:



[19] Η ισότητα (6.12) προκύπτει άμεσα από την (6.8).

[20] Αυτό το σώμα μπορεί να ιδωθεί και ως υπόσωμα τού σώματος $\mathbb{R}$ των πραγματικών αριθμών όταν $m > 0$.

6.3 ΔΑΚΤΥΛΙΟΙ ΠΟΛΥΩΝΥΜΩΝ ΚΑΙ ΕΠΙΤΥΠΩΝ ΔΥΝΑΜΟΣΕΙΡΩΝ

Δοθέντος ενός μη τετριμμένου δακτυλίου R με μοναδιαίο στοιχείο θεωρούμε το σύνολο $R^{\mathbb{N}_0}$ όλων των ακολουθιών $(a_0, a_1, a_2, \ldots\ldots)$ με τα $a_i \in R$, $i = 0, 1, 2, \ldots$, καθώς και το σύνολο $R^{(\mathbb{N}_0)}$ όλων των ακολουθιών $(a_0, a_1, a_2, \ldots\ldots)$ με τα $a_i \in R$, $i = 0, 1, 2, \ldots$, για τις οποίες υπάρχουν *το πολύ πεπερασμένου πλήθους* a_i που είναι διάφορα τού 0_R. Κάθε στοιχείο φ τού $R^{(\mathbb{N}_0)}$ γράφεται υπό τη μορφή

$$\varphi = (a_0, a_1, a_2, \ldots, a_n, 0_R, 0_R, \ldots)$$

για κάποιον ακέραιο αριθμό $n \geqslant 0$. Προφανώς, δυο στοιχεία

$$\varphi = (a_0, a_1, a_2, \ldots, a_n, \ldots), \;\; \psi = (b_0, b_1, b_2, \ldots, b_n, \ldots)$$

τού $R^{\mathbb{N}_0}$ είναι ίσα ($\varphi = \psi$) όταν $a_i = b_i, \forall i \in \mathbb{N}_0$. Επί τού $R^{\mathbb{N}_0}$ ορίζουμε πράξεις *προσθέσεως* και *πολλαπλασιασμού* ως ακολούθως:

$$\left|\begin{array}{lcl} (a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) & := & (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots), \\ \\ (a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots) & := & (c_0, c_1, c_2, \ldots), \end{array}\right.$$

όπου

$$c_m := \sum_{i+j=m} a_i b_j = a_0 b_m + a_1 b_{m-1} + \cdots + a_m b_0, \;\; \forall m \in \mathbb{N}_0. \tag{6.13}$$

Η τριάδα $(R^{\mathbb{N}_0}, +, \cdot)$ αποτελεί έναν δακτύλιο με μηδενικό του στοιχείο το $(0_R, 0_R, \ldots)$ και μοναδιαίο του στοιχείο το $(1_R, 0_R, 0_R, \ldots)$ και η τριάδα $(R^{(\mathbb{N}_0)}, +, \cdot)$ έναν υποδακτύλιο τού $(R^{\mathbb{N}_0}, +, \cdot)$ (με μοναδιαίο στοιχείο του το $(1_R, 0_R, 0_R, \ldots)$). Επίσης, *ταυτίζοντας* κάθε $a \in R$ με το $(a, 0_R, 0_R, \ldots)$ έχουμε τη δυνατότητα θεωρήσεως τού $(R, +, \cdot)$ ως έναν υποδακτύλιο τού $(R^{(\mathbb{N}_0)}, +, \cdot)$. Εισάγοντας ένα νέο σύμβολο

$$\mathsf{X} := (0_R, 1_R, 0_R, 0_R, \ldots)$$

παρατηρούμε ότι, βάσει των ως άνω πράξεων,

$$\mathsf{X}^2 = (0_R, 0_R, 1_R, 0_R, 0_R, \ldots), \;\; \mathsf{X}^3 = (0_R, 0_R, 0_R, 1_R, 0_R, 0_R, \ldots),$$

και, γενικότερα,

$$\mathsf{X}^n = (0_R, 0_R, \ldots, 0_R, \underbrace{1_R}_{n+1 \text{ θέση}}, 0_R, 0_R, \ldots), \;\; \forall n \in \mathbb{N}_0.$$

Επίσης, λόγω τής ανωτέρω ταυτίσεως, για κάθε $a \in R$ λαμβάνουμε

$$a\mathsf{X}^n = \mathsf{X}^n a = (0_R, 0_R, \ldots, 0_R, \underbrace{a}_{n+1 \text{ θέση}}, 0_R, 0_R, \ldots), \;\; \forall n \in \mathbb{N}_0.$$

Εάν λοιπόν το $(a_0, a_1, a_2, \ldots)$ είναι τυχόν στοιχείο τού $R^{\mathbb{N}_0}$, τότε μπορούμε να γράψουμε

$$(a_0, a_1, a_2, \ldots) = a_0 + a_1\mathsf{X} + a_2\mathsf{X}^2 + \cdots + a_n\mathsf{X}^n + \cdots =: \sum_{i=0}^{\infty} a_i \mathsf{X}^i.$$

Κατ' αναλογίαν, εάν το $(a_0, a_1, a_2, \ldots)$ είναι τυχόν στοιχείο τού δακτυλίου $R^{(\mathbb{N}_0)}$, όπου $a_i = 0_R$,για κάθε $i > n$, για κάποιον παγιωμένο $n \in \mathbb{N}_0$, τότε μπορούμε να γράψουμε

$$(a_0, a_1, a_2, \ldots, a_n, 0_R, 0_R, \ldots) = a_0 + a_1\mathsf{X} + a_2\mathsf{X}^2 + \cdots + a_n\mathsf{X}^n =: \sum_{i=0}^{n} a_i \mathsf{X}^i.$$

6.3.1 Ορισμός. (i) Ο ανωτέρω δακτύλιος $R^{\mathbb{N}_0}$ συμβολίζεται συνήθως ως $R[\![\mathsf{X}]\!]$ και καλείται **δακτύλιος επίτυπων δυναμοσειρών** (ή **τύποις δυναμοσειρών**) μιας **απροσδιορίστου** X με συντελεστές ειλημμένους από τον R. Τα στοιχεία του ονομάζονται **επίτυπες δυναμοσειρές** και σημειώνονται ως $\varphi(\mathsf{X}), \psi(\mathsf{X}), ..$ κ.λπ., ενώ τα εκάστοτε αναγραφόμενα $a_0, a_1, a_2, \ldots$ ονομάζονται **συντελεστές** των επίτυπων δυναμοσειρών.

(ii) Ο δακτύλιος $R^{(\mathbb{N}_0)}$ συμβολίζεται συνήθως ως $R\,[\mathsf{X}]$ και καλείται **δακτύλιος πολυωνύμων** (ή **πολυωνυμικός δακτύλιος**) μιας **απροσδιορίστου** X με συντελεστές ειλημμένους από τον R. Τα στοιχεία του ονομάζονται **πολυώνυμα** και σημειώνονται ως $\varphi(\mathsf{X}), \psi(\mathsf{X}), ..$ κ.λπ., ενώ τα εκάστοτε αναγραφόμενα $a_0, a_1, a_2, \ldots$ ονομάζονται **συντελεστές** των πολυωνύμων.

6.3.2 Παρατήρηση. Βάσει τού ορισμού τού πολλαπλασιασμού πολυωνύμων (και αντιστοίχως, επίτυπων δυναμοσειρών) είναι σαφές ότι ο δακτύλιος $R[\mathsf{X}]$ (και αντιστοίχως, ο δακτύλιος $R[\![\mathsf{X}]\!]$) είναι μεταθετικός εάν και μόνον εάν ο ίδιος ο R είναι μεταθετικός.

6.3.3 Σημείωση. Εκ των ανωτέρω συμπεραίνουμε ότι δυο επίτυπες δυναμοσειρές

$$\varphi(\mathsf{X}) = \sum_{i=0}^{\infty} a_i \mathsf{X}^i \in R[\![\mathsf{X}]\!]\,, \quad \psi(\mathsf{X}) = \sum_{i=0}^{\infty} b_i \mathsf{X}^i \in R[\![\mathsf{X}]\!]$$

είναι **ίσες** (γράφοντας $\varphi(\mathsf{X}) = \psi(\mathsf{X})$) εάν και μόνον εάν $a_i = b_i, \forall i \in \mathbb{N}_0$. Κατ' αναλογίαν, δυο πολυώνυμα

$$\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}]\,, \quad \psi(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j \in R[\mathsf{X}]$$

είναι **ίσα** ($\varphi(\mathsf{X}) = \psi(\mathsf{X})$) εάν και μόνον εάν *είτε* αμφότερα είναι ίσα με το $0_{R[\mathsf{X}]}$ *είτε*

$$\max\{\, i \in \{0, \ldots, n\} |\, a_i \neq 0_R\} = \max\{\, j \in \{0, \ldots, m\} |\, b_j \neq 0_R\} \;\; (=: k)$$

και $a_i = b_i, \;\; \forall i \in \{0, \ldots, k\}$.

6.3.4 Ορισμός. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Εάν

$$\varphi(\mathsf{X}) = \sum_{i=0}^{\infty} a_i \mathsf{X}^i \in R[\![\mathsf{X}]\!] \setminus \{0_{R[\![\mathsf{X}]\!]}\} \;\; \text{και} \;\; n := \min\{\, k \in \mathbb{N}_0 |\, a_k \neq 0_R\},$$

τότε λέμε ότι ο αριθμός $\operatorname{ord}(\varphi(\mathsf{X})) := n$ είναι **η τάξη** τής επίτυπης δυναμοσειράς $\varphi(\mathsf{X})$ και το a_0 **ο σταθερός όρος** τής $\varphi(\mathsf{X})$. Στην περίπτωση όπου $\varphi(\mathsf{X}) = 0_{R[\![\mathsf{X}]\!]}$ είναι η **μηδενική επίτυπη δυναμοσειρά**, θέτουμε εξ ορισμού $\operatorname{ord}(\varphi(\mathsf{X})) := \infty$, υπό τον όρο ότι θεσπίζουμε τη σύμβαση[21]: $\infty > n, \;\; \forall n \in \mathbb{N}_0$. Κατ' αυτόν τον τρόπο η τάξη των επίτυπων δυναμοσειρών μπορεί να εκληφθεί ως μια απεικόνιση

$$\operatorname{ord} : R[\![\mathsf{X}]\!] \longrightarrow \mathbb{N}_0 \cup \{\infty\}\,.$$

6.3.5 Λήμμα. *Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Για οιεσδήποτε επίτυπες δυναμοσειρές $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\![\mathsf{X}]\!]$ ισχύουν τα εξής:*

(i) $\operatorname{ord}(\varphi(\mathsf{X}) + \psi(\mathsf{X})) \geqslant \min\{\operatorname{ord}(\varphi(\mathsf{X})), \operatorname{ord}(\psi(\mathsf{X}))\}$.

(ii) $\operatorname{ord}(\varphi(\mathsf{X})\psi(\mathsf{X})) \geqslant \operatorname{ord}(\varphi(\mathsf{X})) + \operatorname{ord}(\psi(\mathsf{X}))$.

[21] Επίσης, στο $\mathbb{N}_0 \cup \{\infty\}$ θέτουμε $\infty + \infty := \infty$, $\infty \cdot \infty := \infty$ και $\infty + n := \infty$, $\infty \cdot n := \infty$, $\forall n \in \mathbb{N}_0$.

(iii) *Εάν* $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\![\mathsf{X}]\!] \setminus \{0_{R[\![\mathsf{X}]\!]}\}$ *και* $\operatorname{ord}(\varphi(\mathsf{X})) \neq \operatorname{ord}(\psi(\mathsf{X}))$, *τότε*

$$\operatorname{ord}\left(\varphi(\mathsf{X}) + \psi(\mathsf{X})\right) = \min\{\operatorname{ord}\left(\varphi(\mathsf{X})\right), \operatorname{ord}(\psi(\mathsf{X}))\}.$$

(iv) *Εάν ο* R *είναι ακεραία περιοχή, τότε*

$$\operatorname{ord}\left(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})\right) = \operatorname{ord}\left(\varphi(\mathsf{X})\right) + \operatorname{ord}(\psi(\mathsf{X})).$$

ΑΠΟΔΕΙΞΗ. Εάν τουλάχιστον μία εκ των $\varphi(\mathsf{X}), \psi(\mathsf{X})$ είναι ίση με την $0_{R[\![\mathsf{X}]\!]}$, τότε τα (i), (ii) και (iv) είναι προφανώς αληθή. Αρκεί λοιπόν να υποθέσουμε ότι $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\![\mathsf{X}]\!] \setminus \{0_{R[\![\mathsf{X}]\!]}\}$ και ότι

$$\varphi(\mathsf{X}) = \sum_{i=0}^{\infty} a_i \mathsf{X}^i, \ n := \operatorname{ord}(\varphi(\mathsf{X})), \quad \psi(\mathsf{X}) = \sum_{i=0}^{\infty} b_i \mathsf{X}^i, \ m := \operatorname{ord}(\psi(\mathsf{X})).$$

(i) Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $n \leqslant m$. Τότε το άθροισμα $\varphi(\mathsf{X}) + \psi(\mathsf{X})$ ισούται με

$$\sum_{i=0}^{\infty} (a_i + b_i)\, \mathsf{X}^i = \begin{cases} a_n \mathsf{X}^n + \displaystyle\sum_{i=n+1}^{\infty} (a_i + b_i)\, \mathsf{X}^i, & \text{όταν } n < m, \\ \displaystyle\sum_{i=n}^{\infty} (a_i + b_i)\, \mathsf{X}^i, & \text{όταν } n = m, \end{cases} \tag{6.14}$$

οπότε[22] $\operatorname{ord}(\varphi(\mathsf{X}) + \psi(\mathsf{X})) \geqslant n = \min\{\operatorname{ord}(\varphi(\mathsf{X})), \operatorname{ord}(\psi(\mathsf{X}))\}$.

(ii) Βάσει τής (6.13) το γινόμενο των δύο επίτυπων δυναμοσειρών μπορεί να γραφεί ως

$$\varphi(\mathsf{X})\psi(\mathsf{X}) = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) \mathsf{X}^k,$$

όπου

$$\sum_{i=0}^{k} a_i b_{k-i} = \begin{cases} a_n b_m, & \text{όταν } k = n + m, \\ 0_R, & \text{όταν } k \leqslant n + m - 1. \end{cases} \tag{6.15}$$

Κατά συνέπειαν[23], $\operatorname{ord}(\varphi(\mathsf{X})\psi(\mathsf{X})) \geqslant n + m = \operatorname{ord}(\varphi(\mathsf{X})) + \operatorname{ord}(\psi(\mathsf{X}))$.

(iii) Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $n < m$. Τότε έχουμε $a_n + b_n = a_n \neq 0_R$ και από την (6.14) έπεται ότι

$$\operatorname{ord}\left(\varphi(\mathsf{X}) + \psi(\mathsf{X})\right) = n = \min\{\operatorname{ord}\left(\varphi(\mathsf{X})\right), \operatorname{ord}(\psi(\mathsf{X}))\}.$$

(iv) Επειδή $a_n b_m \neq 0_R$, λαμβάνουμε $\operatorname{ord}(\varphi(\mathsf{X})\psi(\mathsf{X})) = \operatorname{ord}(\varphi(\mathsf{X})) + \operatorname{ord}(\psi(\mathsf{X}))$ από την (6.15). □

6.3.6 Ορισμός. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Εάν

$$\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\} \ \text{ και } \ a_n \neq 0_R,$$

τότε λέμε ότι ο αριθμός $\deg\left(\varphi(\mathsf{X})\right) := n$ είναι **ο βαθμός** τού πολυωνύμου $\varphi(\mathsf{X})$, το a_0 **ο σταθερός όρος** τού $\varphi(\mathsf{X})$ και ο $\operatorname{LC}(\varphi(\mathsf{X})) := a_n$ ο **επικεφαλής συντελεστής** (ή ο **μεγιστοβάθμιος συντελεστής**) τού $\varphi(\mathsf{X})$. Όταν $\operatorname{LC}(\varphi(\mathsf{X})) = 1_R$, τότε το $\varphi(\mathsf{X})$ καλείται **μονικό πολυώνυμο**. Στην περίπτωση όπου $\varphi(\mathsf{X}) = 0_{R[\mathsf{X}]}$ είναι το **μηδενικό πολυώνυμο**, θέτουμε εξ ορισμού $\deg(\varphi(\mathsf{X})) := -\infty$, υπό τον όρο ότι θεσπίζουμε τη σύμβαση[24]: $-\infty < n, \ \ \forall n \in \mathbb{N}_0$. Κατ' αυτόν τον τρόπο ο βαθμός

[22] Προφανώς, αυτή ισχύει ως *γνήσια* ανισότητα εάν και μόνον εάν $n = m$ και $a_n = -b_n$.

[23] Αυτή ισχύει ως *γνήσια* ανισότητα εάν και μόνον εάν $a_n b_m = 0_R$.

των πολυωνύμων μπορεί να εκληφθεί ως μια απεικόνιση

$$\deg : R[\mathsf{X}] \longrightarrow \mathbb{N}_0 \cup \{-\infty\}\,.$$

Ένα πολυώνυμο $\varphi(\mathsf{X}) \in R[\mathsf{X}]$ λέγεται **σταθερό πολυώνυμο** όταν $\deg(\varphi(\mathsf{X})) \leqslant 0$.

6.3.7 Λήμμα. *Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Για οιαδήποτε πολυώνυμα $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\mathsf{X}]$ ισχύουν τα εξής:*

(i) $\deg(\varphi(\mathsf{X}) + \psi(\mathsf{X})) \leqslant \max\{\deg(\varphi(\mathsf{X})), \deg(\psi(\mathsf{X}))\}$.

(ii) $\deg(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) \leqslant \deg(\varphi(\mathsf{X})) + \deg(\psi(\mathsf{X}))$.

(iii) *Εάν* $\deg(\varphi(\mathsf{X})) \neq \deg(\psi(\mathsf{X}))$, *τότε*

$$\deg(\varphi(\mathsf{X}) + \psi(\mathsf{X})) = \max\{\deg(\varphi(\mathsf{X})),\ \deg(\psi(\mathsf{X}))\}.$$

(iv) *Εάν* $\mathrm{LC}(\varphi(\mathsf{X}))\cdot \mathrm{LC}(\psi(\mathsf{X})) \neq 0_R$, *τότε*

$$\deg(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) = \deg(\varphi(\mathsf{X})) + \deg(\psi(\mathsf{X})).$$

ΑΠΟΔΕΙΞΗ. Εάν τουλάχιστον ένα εκ των $\varphi(\mathsf{X}), \psi(\mathsf{X})$ είναι το μηδενικό πολυώνυμο, τότε τα (i)-(iii) είναι προφανώς αληθή. Ας υποθέσουμε ότι

$$\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}]\ ,\ a_n \neq 0_R, \quad \psi(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j \in R[\mathsf{X}],\ \ b_m \neq 0_R,$$

και ας ορίσουμε $a_i := 0_R$ για κάθε $i > n$ και $b_j := 0_R$ για κάθε $j > m$.

(i) Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $n \geqslant m$. Τότε

$$\varphi(\mathsf{X}) + \psi(\mathsf{X}) = \sum_{i=0}^{n} (a_i + b_i)\, \mathsf{X}^i, \tag{6.16}$$

οπότε $\deg(\varphi(\mathsf{X}) + \psi(\mathsf{X})) \leqslant n = \max\{\deg(\varphi(\mathsf{X})), \deg(\psi(\mathsf{X}))\}$.

(ii) Βάσει τής (6.13) το γινόμενο των δύο πολυωνύμων μπορεί να γραφεί ως

$$\varphi(\mathsf{X}) \cdot \psi(\mathsf{X}) = \sum_{k\geqslant 0} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) \mathsf{X}^k,$$

όπου

$$\sum_{i=0}^{k} a_i b_{k-i} = \begin{cases} a_n b_m, & \text{όταν } k = n+m \\ \sum\limits_{i=0}^{n} a_i b_{k-i} + \sum\limits_{i=n+1}^{k} a_i b_{k-i} = 0_R, & \text{όταν } k \geqslant n+m+1 \end{cases} \tag{6.17}$$

Κατά συνέπειαν, $\deg(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) \leqslant n+m = \deg(\varphi(\mathsf{X})) + \deg(\psi(\mathsf{X}))$.

(iii) Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $n > m$. Τότε έχουμε $a_n + b_n = a_n \neq 0_R$ και από την (6.16) έπεται ότι

$$\deg(\varphi(\mathsf{X}) + \psi(\mathsf{X})) = n = \max\{\deg(\varphi(\mathsf{X})),\ \deg(\psi(\mathsf{X}))\}.$$

(iv) Επειδή $a_n b_m = \mathrm{LC}(\varphi(\mathsf{X}))\cdot \mathrm{LC}(\psi(\mathsf{X})) \neq 0_R$, από την ισότητα (6.17) λαμβάνουμε $\deg(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) = \deg(\varphi(\mathsf{X})) + \deg(\psi(\mathsf{X}))$. □

[24] Επίσης, στο $\mathbb{N}_0 \cup \{-\infty\}$ θέτουμε $(-\infty) + (-\infty) := -\infty$, $(-\infty)\cdot(-\infty) := -\infty$ και $(-\infty) + n := n$, $(-\infty)\cdot n := -\infty$, $\forall n \in \mathbb{N}_0$.

6.3.8 Παραδείγματα. Σημειωτέον ότι οι ανωτέρω ανισοϊσότητες μπορούν πράγματι να ισχύουν και ως αυστηρές ανισότητες.
(i) Εάν $\varphi(\mathsf{X}) = 2\mathsf{X} + 1$, $\psi(\mathsf{X}) = -2\mathsf{X} + 1 \in \mathbb{Z}[\mathsf{X}]$, τότε

$$0 = \deg(\varphi(\mathsf{X}) + \psi(\mathsf{X})) < \max\{\deg(\varphi(\mathsf{X})), \deg(\psi(\mathsf{X}))\} = 1.$$

(ii) Εάν $\varphi(\mathsf{X}) = [2]_4\,\mathsf{X} + [1]_4$, $\psi(\mathsf{X}) = [-2]_4\,\mathsf{X} + [1]_4 \in \mathbb{Z}_4[\mathsf{X}]$, τότε

$$\varphi(\mathsf{X}) \cdot \psi(\mathsf{X}) = [-4]_4\,\mathsf{X}^2 + [1]_4 = [1]_4\,,$$

που σημαίνει ότι $0 = \deg(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) < \deg(\varphi(\mathsf{X})) + \deg(\psi(\mathsf{X})) = 2$.

6.3.9 Πρόταση. *Έστω R μια ακεραία περιοχή. Τότε ισχύουν τα εξής:*
(i) *Για οιαδήποτε πολυώνυμα $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$ έχουμε*

$$\deg(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) = \deg(\varphi(\mathsf{X})) + \deg(\psi(\mathsf{X}))$$

και για οιεσδήποτε επίτυπες δυναμοσειρές $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\![\mathsf{X}]\!] \setminus \{0_{R[\![\mathsf{X}]\!]}\}$ έχουμε

$$\operatorname{ord}(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) = \operatorname{ord}(\varphi(\mathsf{X})) + \operatorname{ord}(\psi(\mathsf{X})).$$

(ii) *Οι δακτύλιοι $R[\mathsf{X}]$ και $R[\![\mathsf{X}]\!]$ είναι ακέραιες περιοχές.*
(iii) *Έχουμε $R[\mathsf{X}]^\times = R^\times$ (ήτοι τα αντιστρέψιμα πολυώνυμα τού $R[\mathsf{X}]$ είναι τα σταθερά πολυώνυμα τής μορφής $\varphi(\mathsf{X}) = a_0 \in R^\times$) και*

$$\varphi(\mathsf{X}) = \sum_{i=0}^{\infty} a_i \mathsf{X}^i \in R[\![\mathsf{X}]\!]^\times \iff a_0 \in R^\times.$$

Απόδειξη. (i)-(ii) Οι $R[\mathsf{X}]$ και $R[\![\mathsf{X}]\!]$ είναι μη τετριμμένοι, μεταθετικοί δακτύλιοι με μοναδιαίο τους στοιχείο το 1_R. Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$, τότε

$$\operatorname{lc}(\varphi(\mathsf{X})) \cdot \operatorname{lc}(\psi(\mathsf{X})) \neq 0_R,$$

διότι ο R δεν διαθέτει μηδενοδιαιρέτες, οπότε από το 6.3.7 (iv) έχουμε

$$\deg(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) = \deg(\varphi(\mathsf{X})) + \deg(\psi(\mathsf{X})) \in \mathbb{N}_0.$$

Συνεπώς, $\varphi(\mathsf{X}) \cdot \psi(\mathsf{X}) \neq 0_{R[\mathsf{X}]}$, οπότε ούτε ο $R[\mathsf{X}]$ δεν έχει μηδενοδιαιρέτες. Εν συνεχεία θεωρούμε $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\![\mathsf{X}]\!] \setminus \{0_{R[\![\mathsf{X}]\!]}\}$. Από το 6.3.5 (iv) έχουμε

$$\operatorname{ord}(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) = \operatorname{ord}(\varphi(\mathsf{X})) + \operatorname{ord}(\psi(\mathsf{X})) \in \mathbb{N}_0.$$

Συνεπώς, $\varphi(\mathsf{X}) \cdot \psi(\mathsf{X}) \neq 0_{R[\![\mathsf{X}]\!]}$, οπότε ούτε ο $R[\![\mathsf{X}]\!]$ δεν έχει μηδενοδιαιρέτες.
(iii) Εάν το $\varphi(\mathsf{X})$ είναι ένα αντιστρέψιμο στοιχείο τού $R[\mathsf{X}]$, τότε υπάρχει ένα πολυώνυμο $\psi(\mathsf{X}) \in R[\mathsf{X}]$, τέτοιο ώστε να ισχύει $\varphi(\mathsf{X})\psi(\mathsf{X}) = 1_{R[\mathsf{X}]}$. Τα $\varphi(\mathsf{X}), \psi(\mathsf{X})$ είναι μη μηδενικά, καθότι $1_{R[\mathsf{X}]} = 1_R \neq 0_R = 0_{R[\mathsf{X}]}$. Από το (i) συνάγεται ότι

$$0 = \deg(\varphi(\mathsf{X})\psi(\mathsf{X})) = \deg(\varphi(\mathsf{X})) + \deg(\psi(\mathsf{X})) \Longrightarrow \deg(\varphi(\mathsf{X})) = \deg(\psi(\mathsf{X})) = 0,$$

οπότε τα $\varphi(\mathsf{X}), \psi(\mathsf{X})$ είναι κατ' ανάγκην αντιστρέψιμα στοιχεία τού R. Εάν τώρα

$$\varphi(\mathsf{X}) = \sum_{i=0}^{\infty} a_i \mathsf{X}^i \in R[\![\mathsf{X}]\!],$$

έχουμε

$$\varphi(\mathsf{X}) \in R[\![\mathsf{X}]\!]^\times \iff a_0 \in R^\times.$$

Πράγματι· εάν υπάρχει $\psi(\mathsf{X}) = \sum_{i=0}^{\infty} b_i \mathsf{X}^i \in R[\![\mathsf{X}]\!]$ με $\varphi(\mathsf{X})\psi(\mathsf{X}) = 1_R$, τότε $a_0 b_0 = 1_R$, οπότε $a_0 \in R^\times$. Και αντιστρόφως· εάν $a_0 \in R^\times$, τότε μπορούμε να προσδιορίσουμε διαδοχικώς $b_0, b_1, \ldots, b_i, b_{i+1}, \ldots \in R$, ούτως ώστε να ισχύουν οι ισότητες

$$\begin{cases} b_0 a_0 = 1_R, \\ b_1 a_0 + b_0 a_1 = 0_R, \\ \vdots \\ b_i a_0 + b_{i-1} a_1 + \cdots + b_0 a_i = 0_R, \\ \vdots \end{cases}$$

Προφανώς, $b_0 = a_0^{-1}$. Έστω τυχών φυσικός αριθμός $i \in \mathbb{N}$. Υποθέτοντας ότι έχουμε ήδη προσδιορίσει τα b_j, $j \in \{0, 1, \ldots, i-1\}$, ορίζουμε ως b_i το

$$b_i := -a_0^{-1}(b_{i-1} a_1 + \cdots + b_0 a_i).$$

Θέτοντας $\psi(\mathsf{X}) := \sum_{i=0}^{\infty} b_i \mathsf{X}^i$, λαμβάνουμε $\varphi(\mathsf{X})\psi(\mathsf{X}) = 1_R$ και ο ισχυρισμός είναι αληθής. □

6.3.10 Πόρισμα. *Έστω K ένα σώμα. Τότε ισχύουν τα εξής:*
(i) *Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}] \smallsetminus \{0_{K[\mathsf{X}]}\}$, τότε*

$$\deg\left(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})\right) = \deg\left(\varphi(\mathsf{X})\right) + \deg(\psi(\mathsf{X}))$$

και $K[\mathsf{X}]^\times = K^\times = K \smallsetminus \{0_K\} = \{\varphi(\mathsf{X}) \in K[\mathsf{X}] \mid \deg(\varphi(\mathsf{X})) = 0\}$.
(ii) *Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\![\mathsf{X}]\!] \smallsetminus \{0_{K[\![\mathsf{X}]\!]}\}$, τότε*

$$\operatorname{ord}\left(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})\right) = \operatorname{ord}\left(\varphi(\mathsf{X})\right) + \operatorname{ord}(\psi(\mathsf{X}))$$

και

$$K[\![\mathsf{X}]\!]^\times = \{\varphi(\mathsf{X}) \in K[\![\mathsf{X}]\!] \mid \operatorname{ord}(\varphi(\mathsf{X})) = 0\}.$$

Επιπροσθέτως, κάθε επίτυπη δυναμοσειρά $\varphi(\mathsf{X}) \in K[\![\mathsf{X}]\!] \smallsetminus \{0_{K[\![\mathsf{X}]\!]}\}$ γράφεται υπό τη μορφή

$$\varphi(\mathsf{X}) = \mathsf{X}^{\operatorname{ord}(\varphi(\mathsf{X}))} \chi(\mathsf{X}),$$

για κάποια (μονοσημάντως ορισμένη) επίτυπη δυναμοσειρά $\chi(\mathsf{X}) \in K[\![\mathsf{X}]\!]^\times$.

Απόδειξη. Οι ισχυρισμοί περί των βαθμών τού γινομένου δύο μη μηδενικών πολυωνύμων, περί των τάξεων δύο μη μηδενικών επίτυπων δυναμοσειρών και περί των ομάδων των αντιστρεψίμων στοιχείων είναι προδήλως αληθείς βάσει των όσων απεδείχθησαν στην πρόταση 6.3.9. Έστω τώρα τυχούσα επίτυπη δυναμοσειρά

$$\varphi(\mathsf{X}) = \sum_{i=0}^{\infty} a_i \mathsf{X}^i \in K[\![\mathsf{X}]\!] \smallsetminus \{0_{K[\![\mathsf{X}]\!]}\}$$

με $n := \operatorname{ord}(\varphi(\mathsf{X}))$. Θέτοντας $\chi(\mathsf{X}) := \sum_{i=n}^{\infty} a_i \mathsf{X}^{i-n}$ λαμβάνουμε $\varphi(\mathsf{X}) = \mathsf{X}^n \chi(\mathsf{X})$. Η επίτυπη δυναμοσειρά $\chi(\mathsf{X}) \in K[\![\mathsf{X}]\!]$ είναι αντιστρέψιμη, διότι ο σταθερός της όρος a_n είναι $\neq 0_K$, οπότε ανήκει στην ομάδα $K^\times = K \smallsetminus \{0_K\}$. □

6.3.11 Πόρισμα. *Έστω K ένα σώμα. Μια επίτυπη δυναμοσειρά*

$$\varphi(\mathsf{X}) = \sum_{i=0}^{\infty} a_i \mathsf{X}^i \in K[\![\mathsf{X}]\!]$$

είναι αντιστρέψιμο στοιχείο τού δακτυλίου $K[\![\mathsf{X}]\!]$ εάν και μόνον εάν $a_0 \neq 0_K$. Επιπροσθέτως, όταν $a_0 \neq 0_K$, το αντίστροφο στοιχείο τής $\varphi(\mathsf{X})$ είναι η

$$\psi(\mathsf{X}) = \sum_{i=0}^{\infty} b_i \mathsf{X}^i \in K[\![\mathsf{X}]\!] \tag{6.18}$$

όπου $b_0 = a_0^{-1}$, $b_1 = -a_0^{-1} b_0 a_1$ και

$$b_i = -a_0^{-1}(b_{i-1}a_1 + \cdots + b_0 a_i),\ \forall i \in \mathbb{N}.$$

6.3.12 Παραδείγματα. (i) Η επίτυπη δυναμοσειρά $\sum_{i=0}^{\infty} \mathsf{X}^i \in K[\![\mathsf{X}]\!]$ (K τυχόν σώμα) έχει ως αντίστροφό της την

$$\left(\sum_{i=0}^{\infty} \mathsf{X}^i\right)^{-1} = 1_K - \mathsf{X} + 0_K + 0_K + \cdots$$

(ii) Η $\sum_{i=0}^{\infty} \binom{i+k-1}{k-1} \mathsf{X}^i \in \mathbb{Q}[\![\mathsf{X}]\!]$ (όπου $k \in \mathbb{N}$) έχει ως αντίστροφό της την

$$\left(\sum_{i=0}^{\infty} \tbinom{i+k-1}{k-1} \mathsf{X}^i\right)^{-1} = (1-\mathsf{X})^k = \sum_{j=0}^{k} \tbinom{k}{j} (-1)^j \mathsf{X}^{k-j} + 0 + 0 + \cdots$$

(iii) Η $\sum_{i=0}^{\infty} \frac{1}{i!} \mathsf{X}^i \in \mathbb{C}[\![\mathsf{X}]\!]$ έχει ως αντίστροφό της την

$$\left(\sum_{i=0}^{\infty} \tfrac{1}{i!} \mathsf{X}^i\right)^{-1} = \sum_{i=0}^{\infty} \tfrac{(-1)^i}{i!} \mathsf{X}^i,$$

καθόσον ισχύει

$$\left(\sum_{i=0}^{\infty} \tfrac{1}{i!} \mathsf{X}^i\right)\left(\sum_{i=0}^{\infty} \tfrac{(-1)^i}{i!} \mathsf{X}^i\right) = \sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} \tfrac{(-1)^k}{k!} \tfrac{1}{(i-k)!}\right) \mathsf{X}^i = 1,$$

λαμβανομένου υπ' όψιν τού ότι

$$\sum_{k=0}^{i} \tfrac{(-1)^k}{k!} \tfrac{1}{(i-k)!} = \tfrac{1}{i!} \sum_{k=0}^{i} (-1)^k \tbinom{i}{k} = \begin{cases} 0, & \text{όταν } i \neq 0, \\ 1, & \text{όταν } i = 0. \end{cases}$$

6.3.13 Σημείωση. Στο σχολείο είθισται να αντιμετωπίζουμε τα πολυώνυμα ως συνήθεις «απεικονίσεις» (επειδή εκεί γίνεται κυρίως χρήση των δακτυλίων $\mathbb{Q}$ και $\mathbb{R}$). Ωστόσο, όταν κανείς θεωρεί *τυχόντες* δακτυλίους R με μοναδιαίο στοιχείο, κάτι τέτοιο *δεν* είναι εν γένει αληθές. Εάν $\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}]$, η **απεικόνιση η επαγομένη από το** $\varphi(\mathsf{X})$ είναι εξ ορισμού η

$$\mathfrak{v}_{\varphi(\mathsf{X})} : R \longrightarrow R, \quad r \longmapsto \mathfrak{v}_{\varphi(\mathsf{X})}(r) := \varphi(r) := \sum_{i=0}^{n} a_i r^i.$$

Όμως η $R[\mathsf{X}] \longrightarrow \mathrm{AP}(R,R) = R^R,\ \varphi(\mathsf{X}) \longmapsto \mathfrak{v}_{\varphi(\mathsf{X})}$, δεν είναι κατ' ανάγκην ένριψη. Επί παραδείγματι, εάν $R = \mathbb{Z}_3$ και

$$\varphi(\mathsf{X}) = [1]_3 \mathsf{X} + [1]_3 \mathsf{X}^3, \quad \psi(\mathsf{X}) = [2]_3 \mathsf{X},$$

τότε τα $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$ -ως πολυώνυμα- είναι διαφορετικά (βλ. 6.3.3), ενώ

$$\mathfrak{v}_{\varphi(\mathsf{X})}([0]_3) = [0]_3 = \mathfrak{v}_{\psi(\mathsf{X})}([0]_3),$$
$$\mathfrak{v}_{\varphi(\mathsf{X})}([1]_3) = [2]_3 = \mathfrak{v}_{\psi(\mathsf{X})}([1]_3),$$
$$\mathfrak{v}_{\varphi(\mathsf{X})}([2]_3) = [1]_3 = \mathfrak{v}_{\psi(\mathsf{X})}([2]_3),$$

πράγμα που σημαίνει ότι $\mathfrak{v}_{\varphi(\mathsf{X})} = \mathfrak{v}_{\psi(\mathsf{X})}$.

▸ **Μετάβαση στις πολλές απροσδιορίστους**. Αυτή καθίσταται εφικτή ύστερα από επανάληψη τής διαδικασίας κατασκευής των $R[\mathsf{X}]$ και $R[\![\mathsf{X}]\!]$, όπου ο ίδιος ο R είναι ένας δακτύλιος πολυωνύμων και ένας δακτύλιος επίτυπων δυναμοσειρών, αντιστοίχως, ακολουθούμενη από αναδρομικό ορισμό.

6.3.14 Ορισμός. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο.

(i) Ο δακτύλιος $(R[\![\mathsf{X}_1]\!])\,[\![\mathsf{X}_2]\!]$ των επίτυπων δυναμοσειρών μίας απροσδιορίστου X_2 με συντελεστές ειλημμένους από τον $R[\![\mathsf{X}_1]\!]$ καλείται **δακτύλιος επίτυπων δυναμοσειρών δύο (ανεξαρτήτων) απροσδιορίστων** X_1 **και** X_2 με συντελεστές ειλημμένους από τον R και συμβολίζεται ως $R[\![\mathsf{X}_1, \mathsf{X}_2]\!]$. Κάθε $\varphi(\mathsf{X}_1, \mathsf{X}_2) \in R[\![\mathsf{X}_1, \mathsf{X}_2]\!]$ είναι τής μορφής

$$\varphi(\mathsf{X}_1, \mathsf{X}_2) = \sum_{(i,j)\in\mathbb{N}_0^2} a_{ij}\mathsf{X}_1^i\mathsf{X}_2^j, \;\; a_{ij} \in R.$$

Κατ' αναλογίαν, ο δακτύλιος $(R[\mathsf{X}_1])\,[\mathsf{X}_2]$ των πολυωνύμων μίας απροσδιορίστου X_2 με συντελεστές ειλημμένους από τον $R[\mathsf{X}_1]$ καλείται **δακτύλιος πολυωνύμων δύο (ανεξαρτήτων) απροσδιορίστων** X_1 **και** X_2 με συντελεστές ειλημμένους από τον R και συμβολίζεται ως $R[\mathsf{X}_1, \mathsf{X}_2]$. Κάθε στοιχείο

$$\varphi(\mathsf{X}_1, \mathsf{X}_2) \in R[\mathsf{X}_1, \mathsf{X}_2]$$

είναι τής μορφής

$$\varphi(\mathsf{X}_1, \mathsf{X}_2) = \sum_{(i,j)\in\Lambda} a_{ij}\mathsf{X}_1^i\mathsf{X}_2^j, \;\; a_{ij} \in R, \;\Lambda \subseteq \mathbb{N}_0^2, \;\mathrm{card}(\Lambda) < \infty.$$

(Προφανώς, ο $R[\mathsf{X}_1, \mathsf{X}_2]$ είναι υποδακτύλιος τού $R[\![\mathsf{X}_1, \mathsf{X}_2]\!]$ και επί τη βάσει των συνήθων ταυτίσεων ισχύει $1_{R[\![\mathsf{X}_1,\mathsf{X}_2]\!]} = 1_{R[\mathsf{X}_1,\mathsf{X}_2]} = 1_R$.)

(ii) Γενικότερα, για οιονδήποτε φυσικό αριθμό $n \geqslant 2$, ο δακτύλιος

$$R[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!]$$

επίτυπων δυναμοσειρών n **(ανεξαρτήτων) απροσδιορίστων** $\mathsf{X}_1, \ldots, \mathsf{X}_n$ με συντελεστές ειλημμένους από τον R ορίζεται αναδρομικώς ως

$$R[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!] := R[\![\mathsf{X}_1, \ldots, \mathsf{X}_{n-1}]\!][\![\mathsf{X}_n]\!].$$

Κατ' αναλογίαν, ο **δακτύλιος**

$$R\,[\mathsf{X}_1, \ldots, \mathsf{X}_n]$$

πολυωνύμων n **(ανεξαρτήτων) απροσδιορίστων** $\mathsf{X}_1, \ldots, \mathsf{X}_n$ με συντελεστές ειλημμένους από τον R ορίζεται αναδρομικώς ως εξής[25]:

$$R\,[\mathsf{X}_1, \ldots, \mathsf{X}_n] := R\,[\mathsf{X}_1, \ldots, \mathsf{X}_{n-1}]\,[\mathsf{X}_n]\,.$$

[25] Ο $R\,[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ (και αντιστοίχως, ο $R[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!]$) είναι μεταθετικός εάν και μόνον εάν ο ίδιος ο R είναι μεταθετικός.

6.4 Η ΧΑΡΑΚΤΗΡΙΣΤΙΚΗ ΤΩΝ ΔΑΚΤΥΛΙΩΝ

6.4.1 Ορισμός. Έστω R ένας δακτύλιος. Ας υποθέσουμε ότι υπάρχει ένας $m \in \mathbb{N}$ με την ιδιότητα

$$ma = 0_R, \quad \forall a \in R.$$

Εάν ο $n \in \mathbb{N}$ είναι ο ελάχιστος φυσικός αριθμός με αυτήν την ιδιότητα, τότε ο n λέγεται **χαρακτηριστική** τού δακτυλίου R. Εάν δεν υπάρχει κανένας $m \in \mathbb{N}$ με την ανωτέρω ιδιότητα, τότε λέμε ότι ο δακτύλιος R έχει **χαρακτηριστική** 0. Η χαρακτηριστική ενός δακτυλίου R θα συμβολίζεται ως $\text{χαρ}(R)$.

6.4.2 Παραδείγματα. (i) Οι $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ και $\mathbb{C}$ έχουν χαρακτηριστική 0.

(ii) Ο $\mathbb{Z}_m$ έχει χαρακτηριστική m.

(iii) Προφανώς, $\text{χαρ}(R) = 1 \iff$ ο R είναι τετριμμένος δακτύλιος.

6.4.3 Πρόταση. *Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Τότε*

$$\text{χαρ}\,(R) = n > 0 \iff n = \min\{m \in \mathbb{N} \mid m \cdot 1_R = 0_R\}.$$

Απόδειξη. "$\Longrightarrow$" Εξ ορισμού, εάν ο R έχει χαρακτηριστική $n > 0$, τότε $na = 0_R$ για *κάθε* $a \in R$, οπότε $n \cdot 1_R = 0_R$. Εάν υπήρχε κάποιος ακέραιος m, $0 < m < n$, τέτοιος ώστε να ισχύει $m \cdot 1_R = 0_R$, τότε θα είχαμε

$$ma = m\,(1_R \cdot a) = (m \cdot 1_R)\,a = 0_R \cdot a = 0_R, \quad \forall a \in R,$$

δηλαδή κάτι που θα αντέφασκε προς το γεγονός ότι ο n είναι ο ελάχιστος φυσικός αριθμός για τον οποίον $na = 0_R$ για κάθε $a \in R$.

"$\Longleftarrow$" Εάν ο n είναι ο ελάχιστος φυσικός αριθμός για τον οποίον $n \cdot 1_R = 0_R$, τότε για κάθε $a \in R$ έχουμε

$$na = n\,(1_R \cdot a) = (n \cdot 1_R)\,a = 0_R \cdot a = 0_R,$$

οπότε $\text{χαρ}(R) = k$, για κάποιον φυσικό αριθμό k, όπου $0 < k \leqslant n$. Επειδή όμως τότε θα ισχύει και η ισότητα $k \cdot 1_R = 0_R$, θα πρέπει (βάσει τής υποθέσεώς μας) να έχουμε $k = n$. □

6.4.4 Παράδειγμα. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Τότε

$$\text{χαρ}\,(R) = \text{χαρ}\,(R[\mathsf{X}]) = \text{χαρ}\,(R[\![\mathsf{X}]\!]).$$

Ας αποδείξουμε την πρώτη ισότητα. (Η απόδειξη τής δεύτερης είναι παρόμοια.)

Περίπτωση πρώτη. $\text{χαρ}(R[\mathsf{X}]) = n > 0$. Τότε $n = \min\{m \in \mathbb{N} | \, m \cdot 1_{R[\mathsf{X}]} = 0_{R[\mathsf{X}]}\}$. Επειδή το 1_R (και αντιστοίχως, το 0_R) ταυτίζεται (κατά τα ειωθότα) με το $1_{R[\mathsf{X}]}$ (και αντιστοίχως, με το $0_{R[\mathsf{X}]}$), λαμβάνουμε $\text{χαρ}(R) = n$.

Περίπτωση δεύτερη. Έστω ότι $\text{χαρ}(R[\mathsf{X}]) = 0$. Εάν υποθέταμε ότι $\text{χαρ}(R) = n > 0$, τότε (χρησιμοποιώντας την ίδια επιχειρηματολογία) θα είχαμε $\text{χαρ}(R[\mathsf{X}]) = n$ και θα καταλήγαμε σε άτοπο. Άρα $\text{χαρ}(R) = 0$.

6.4.5 Πρόταση. *Η χαρακτηριστική οιασδήποτε ακεραίας περιοχής R είναι είτε μηδέν είτε ένας πρώτος αριθμός.*

Απόδειξη. Έστω ότι $\text{χαρ}(R) = n \neq 0$. Υποθέτουμε πως ο n είναι σύνθετος αριθμός, ήτοι ότι είναι γινόμενο $n = kl$ δύο φυσικών αριθμών k, l, όπου $1 < k, l < n$.

Τότε $0_R = n \cdot 1_R = (kl) \cdot 1_R = (k \cdot 1_R)\,(l \cdot 1_R)$, και επειδή ο R δεν διαθέτει μηδενοδιαιρέτες λαμβάνουμε $(k \cdot 1_R) = 0_R$ ή $(l \cdot 1_R) = 0_R$, πράγμα που αντιφάσκει προς το γεγονός ότι ο n είναι ο *ελάχιστος* φυσικός αριθμός με αυτήν την ιδιότητα. (Βλ. πρόταση 6.4.3). Άρα τελικώς ο n οφείλει να είναι πρώτος αριθμός. □

6.4.6 Πρόταση. *Έστω R μια ακεραία περιοχή.*

(i) *Εάν* $\chi\alpha\rho(R) = 0$, *τότε κάθε μη μηδενικό στοιχείο τής προσθετικής ομάδας* $(R, +)$ *έχει άπειρη τάξη.*

(ii) *Εάν* $\chi\alpha\rho(R) = p$ *(p πρώτος), τότε κάθε μη μηδενικό στοιχείο τής προσθετικής ομάδας* $(R, +)$ *έχει τάξη* p.

Αποδειξη. (i) Εάν $\chi\alpha\rho(R) = 0$ και εάν θεωρήσουμε ένα $a \in R \setminus \{0_R\}$ και υποθέσουμε πως αυτό είναι τάξεως $m \in \mathbb{N}$, τότε

$$0_R = ma = (m \cdot 1_R)\, a \Longrightarrow m \cdot 1_R = 0_R,$$

ήτοι κάτι το αδύνατο. Άρα το a οφείλει να έχει άπειρη τάξη.

(ii) Εάν $\chi\alpha\rho(R) = p$ (p πρώτος) και εάν θεωρήσουμε ένα $a \in R \setminus \{0_R\}$, τότε από τον ορισμό τής χαρακτηριστικής τού R προκύπτει ότι $\mathrm{ord}(a) \leqslant p$. Όμως η ισότητα $0_R = \mathrm{ord}(a)\, a = (\mathrm{ord}\,(a) \cdot 1_R)\, a$ δίδει και πάλι $\mathrm{ord}(a) \cdot 1_R = 0_R$ (διότι ο δακτύλιος R στερείται μηδενοδιαιρετών), πράγμα που σημαίνει ότι $\mathrm{ord}(a) \geqslant p$ δυνάμει τής προτάσεως 6.4.3. Συνεπώς, $\mathrm{ord}(a) = p$. □

6.4.7 Πόρισμα. *Εάν R είναι μια πεπερασμένη ακεραία περιοχή (ήτοι ένα πεπερασμένο σώμα), τότε η χαρακτηριστική της θα είναι ένας πρώτος αριθμός.*

6.4.8 Πρόταση. *Εάν R είναι μια ακεραία περιοχή με χαρακτηριστική έναν πρώτο αριθμό p, τότε για οιαδήποτε $a, b, a_1, \ldots, a_n \in R$ έχουμε:*

(i) $(a \pm b)^p = a^p \pm b^p$.

(ii) $(a \pm b)^{p^\nu} = a^{p^\nu} \pm b^{p^\nu}$ *για κάθε* $\nu \in \mathbb{N}$.

(iii) $(a_1 + \cdots + a_n)^p = a_1^p + \cdots + a_n^p$.

(iv) $(a_1 + \cdots + a_n)^{p^\nu} = a_1^{p^\nu} + \cdots + a_n^{p^\nu}$ *για κάθε* $\nu \in \mathbb{N}$.

Αποδειξη. Αφήνεται ως άσκηση. □

ΚΕΦΑΛΑΙΟ 7

Ιδεώδη και πηλικοδακτύλιοι

Τα *ιδεώδη*[1] ενός δακτυλίου R είναι ειδικής φύσεως υποδακτύλιοι τού R που «απορροφούν» οιαδήποτε γινόμενα στοιχείων τους με στοιχεία τού R και συμπεριφέρονται «ιδεωδώς» σε ό,τι αφορά στη δόμηση *πηλικοδακτυλίων*, σε πλήρη αναλογία με ό,τι συμβαίνει με τις *ορθόθετες υποομάδες* μιας δεδομένης ομάδας.

7.1 ΙΔΕΩΔΗ

7.1.1 Ορισμός. Έστω $(R, +, \cdot)$ ένας δακτύλιος. Ένα υποσύνολο $\varnothing \neq I \subseteq R$, για το οποίο το ζεύγος $(I, +)$ αποτελεί μια υποομάδα τής προσθετικής ομάδας $(R, +)$, καλείται

- **αριστερό ιδεώδες** όταν $ra \in I$ για κάθε $r \in R$ και κάθε $a \in I$,
- **δεξιό ιδεώδες** όταν $ar \in I$ για κάθε $r \in R$ και κάθε $a \in I$, και
- **αμφίπλευρο ιδεώδες** ή απλώς **ιδεώδες** εάν το I είναι συγχρόνως και αριστερό και δεξιό ιδεώδες.

7.1.2 Παρατήρηση. (i) Κάθε (αριστερό, δεξιό ή αμφίπλευρο) ιδεώδες ενός δακτυλίου είναι υποδακτύλιος αυτού. Ωστόσο, υπάρχουν υποδακτύλιοι δακτυλίων που δεν είναι ιδεώδη τους. (Βλ., π.χ., 7.1.4 (ii).)

(ii) Σε μεταθετικούς δακτυλίους οι έννοιες αριστερό, δεξιό και αμφίπλευρο ιδεώδες ταυτίζονται.

7.1.3 Πρόταση. *Έστω $(R, +, \cdot)$ ένας δακτύλιος. Ένα μη κενό υποσύνολο I τού R είναι ένα αριστερό (και αντιστοίχως, δεξιό/αμφίπλευρο) ιδεώδες εάν και μόνον εάν ισχύουν τα εξής:*

(i) $a - b \in I$, *για οιαδήποτε* $a, b \in I$.

(ii) $ra \in I$ *(και αντιστοίχως,* $ar \in I$ / $ra, ar \in I$*) για οιαδήποτε* $a \in I,\ r \in R$.

Απόδειξη. Προφανώς η (i) ισοδυναμεί με το ότι το ζεύγος $(I, +)$ αποτελεί μια υποομάδα τής προσθετικής ομάδας $(R, +)$ τού δακτυλίου $(R, +, \cdot)$. □

[1] Το 1847 ο Ernst Eduard Kummer (1810-1893) εισήγαγε «ιδεώδεις μιγαδικούς αριθμούς» στην προσπάθειά του να διατηρήσει την ιδιότητα τής μονοσήμαντης παραγοντοποιήσεως σε κάποιους δακτυλίους αλγεβρικών αριθμών. Ωστόσο, ήταν ο Richard Dedekind (1831-1916) και η Emmy Noether (1882-1935) αυτοί που εγκαινίασαν τη χρήση «ιδεωδών» ως ειδικούς υποδακτυλίους και μετεξέλιξαν την όλη θεωρία τους, ούτως ώστε ο λογισμός με αυτά να καταστεί ένα από τα πιο απαραίτητα τεχνικά βοηθήματα των σύγχρονων αλγεβριστών.

7.1.4 Παραδείγματα. (i) Για κάθε ακέραιο n η κυκλική υποομάδα

$$n\mathbb{Z} = \{nk \quad | k \in \mathbb{Z}\}$$

τής $(\mathbb{Z}, +)$ αποτελεί ένα ιδεώδες τού δακτυλίου $(\mathbb{Z}, +, \cdot)$.

(ii) Ο υποδακτύλιος $\mathbb{Z}$ τού $\mathbb{Q}$ *δεν είναι* (ούτε δεξιό ούτε αριστερό ούτε αμφίπλευρο) ιδεώδες τού $\mathbb{Q}$, διότι π.χ. $\frac{1}{2} \in \mathbb{Q}$ και $7 \in \mathbb{Z}$, αλλά $\frac{1}{2} \cdot 7 = 7 \cdot \frac{1}{2} \notin \mathbb{Z}$.

(iii) Ορίζουμε τα

$$I := \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| \ a, b \in \mathbb{R} \right\} \subseteq \mathrm{Mat}_{2\times 2}(\mathbb{R})$$

και

$$J := \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| \ a, b \in \mathbb{R} \right\} \subseteq \mathrm{Mat}_{2\times 2}(\mathbb{R}).$$

Το I είναι δεξιό ιδεώδες τού $\mathrm{Mat}_{2\times 2}(\mathbb{R})$, διότι για οιουσδήποτε $a, b, a', b' \in \mathbb{R}$ έχουμε

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} a' & b' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a-a' & b-b' \\ 0 & 0 \end{pmatrix} \in I$$

και για οιουσδήποτε $a, b, c, d, e, f \in \mathbb{R}$,

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} c & d \\ e & f \end{pmatrix} = \begin{pmatrix} ca+eb & ad+bf \\ 0 & 0 \end{pmatrix} \in I.$$

Ωστόσο, το I δεν είναι αριστερό ιδεώδες τού $\mathrm{Mat}_{2\times 2}(\mathbb{R})$, διότι π.χ.

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \notin I.$$

Κατ' αναλογίαν, αποδεικνύεται ότι το J είναι ένα αριστερό, μη δεξιό ιδεώδες τού $\mathrm{Mat}_{2\times 2}(\mathbb{R})$.

(iv) Κάθε δακτύλιος R έχει πάντοτε τον εαυτό του και το $\{0_R\}$ ως ιδεώδη του. Το $\{0_R\}$ λέγεται **τετριμμένο**[2] (ή **μηδενικό**) **ιδεώδες**, ενώ κάθε (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες I τού R με $I \subsetneq R$ λέγεται ***γνήσιο*** *(αριστερό/δεξιό/αμφίπλευρο)* **ιδεώδες**.

(v) Εάν R είναι ένας δακτύλιος και $a \in R$, τότε είναι προφανές ότι το σύνολο

$$\boxed{Ra := \{ra \mid r \in R\}}$$

είναι ένα αριστερό και το σύνολο

$$\boxed{aR := \{ar \mid r \in R\}}$$

ένα δεξιό ιδεώδες τού R.

(vi) Έστω R ένας δακτύλιος και έστω $S \subsetneq R$ ένας γνήσιος υποδακτύλιός του. Θεωρούμε ένα μη κενό υποσύνολο $I \subseteq S$. Εάν το I είναι ένα (αριστερό/ δεξιό/ αμφίπλευρο) ιδεώδες τού R, τότε το I είναι ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού S. Αντιθέτως, εάν το I είναι ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού S, τότε το I δεν είναι κατ' ανάγκην ένα ομοειδές ιδεώδες τού R. Επί παραδείγματι, εάν $R := \mathrm{Mat}_{2\times 2}(\mathbb{R})$ και

$$I := \left\{ \begin{pmatrix} 0 & s \\ 0 & 0 \end{pmatrix} \middle| \ s \in \mathbb{R} \right\} \subsetneq \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| \ a, b, c \in \mathbb{R} \right\} =: S \subsetneq R,$$

[2] Προσοχή! Ορισμένοι συγγραφείς (την ορολογία των οποίων δεν ακολουθούμε εν προκειμένω) χαρακτηρίζουν ως *τετριμμένα ιδεώδη* ενός δακτυλίου R *αμφότερα* τα $\{0_R\}$ και R.

τότε το I είναι ένα (αμφίπλευρο) ιδεώδες τού S, διότι για $a,b,c,s,s' \in \mathbb{R}$ έχουμε

$$\begin{pmatrix} 0 & s \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & s' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & s-s' \\ 0 & 0 \end{pmatrix} \in I$$

και

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} 0 & s \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & as \\ 0 & 0 \end{pmatrix}, \ \begin{pmatrix} 0 & s \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & sc \\ 0 & 0 \end{pmatrix} \in I.$$

Από την άλλη μεριά, το I δεν είναι (αμφίπλευρο) ιδεώδες τού R, διότι π.χ.

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \notin I.$$

7.1.5 Πρόταση. *Έστω $\{I_\lambda \mid \lambda \in \Lambda\}$ μια οικογένεια αριστερών (και αντιστοίχως, δεξιών/αμφιπλεύρων) ιδεωδών ενός δακτυλίου R. Τότε η τομή $\bigcap\limits_{\lambda\in\Lambda} I_\lambda$ των μελών της αποτελεί ένα αριστερό (και αντιστοίχως, δεξιό/αμφίπλευρο) ιδεώδες τού R.*

Απόδειξη. Εάν η $\{I_\lambda \mid \lambda \in \Lambda\}$ μια οικογένεια αριστερών (και αντιστοίχως, δεξιών/αμφιπλεύρων) ιδεωδών ενός δακτυλίου R, και $r \in R$, $a,b \in \bigcap\limits_{\lambda\in\Lambda} I_\lambda$, τότε

$$(a,b \in I_\lambda,\ \forall\, \lambda \in \Lambda) \underset{[I_\lambda \text{ ιδεώδες}]}{\Longrightarrow} \left\{ \begin{array}{l} a-b \in I_\lambda \\ ra \text{ (αντ., } ar \in I_\lambda \text{ / } ra, ar \in I_\lambda) \end{array} \right\}, \forall\, \lambda \in \Lambda,$$

οπότε και η τομή $\bigcap\limits_{\lambda\in\Lambda} I_\lambda$ αποτελεί ένα αριστερό (και αντιστοίχως, ένα δεξιό/ αμφίπλευρο) ιδεώδες τού R. □

7.1.6 Πρόταση. *Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Εάν το I είναι ένα γνήσιο (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού R, τότε το I δεν περιέχει κανένα (εξ αριστερών/ εκ δεξιών / αμφιπλεύρως) αντιστρέψιμο στοιχείο τού R.*

Απόδειξη. Εάν το I είναι ένα γνήσιο (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού R και εάν υποθέσουμε ότι υπάρχει κάποιο $a \in I \setminus \{0_R\}$, ούτως ώστε να ισχύει

$$ba = 1_R \ \ (\text{αντ., } ab = 1_R \text{ / } ab = ba = 1_R)\,,$$

για κάποιο $b \in R \setminus \{0_R\}$, τότε από τον ορισμό ενός (αριστερού/ δεξιού/ αμφιπλεύρου) ιδεώδους είναι πρόδηλο ότι και τα γινόμενα αυτά (που είναι ίσα με 1_R) οφείλουν να ανήκουν στο I. Άρα

$$1_R \in I \Longrightarrow [\forall r \in R : r \cdot 1_R = r \in I, \text{ αντ., } 1_R \cdot r = r] \Longrightarrow I = R,$$

πράγμα που έχουμε εκ των προτέρων αποκλείσει. □

7.1.7 Πόρισμα. *Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Εάν το I είναι ένα γνήσιο (αριστερό/ δεξιό/ αμφίπλευρο) ιδεώδες τού R, τότε το I δεν περιέχει το 1_R.*

7.1.8 Πρόταση. *Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Ο R είναι διαιρετικός δακτύλιος.*

(ii) *Τα μόνα αριστερά ιδεώδη τού R είναι το $\{0_R\}$ και ο ίδιος ο R.*

(iii) *Τα μόνα δεξιά ιδεώδη τού R είναι το $\{0_R\}$ και ο ίδιος ο R.*

Απόδειξη. (i)⇔(ii) Εάν ο R είναι διαιρετικός δακτύλιος και I ένα αριστερό ιδεώδες αυτού με $\{0_R\} \subsetneq I$, τότε υπάρχει κάποιο $a \in I \setminus \{0_R\}$. Εξ ορισμού, το a διαθέτει αντίστροφο a^{-1}. Επειδή $1_R = a^{-1}a \in I$, έχουμε $I = R$. Και αντιστρόφως· υποθέτοντας ότι τα μόνα αριστερά ιδεώδη τού R είναι το $\{0_R\}$ και ο ίδιος ο R, και θεωρώντας οιοδήποτε στοιχείο $a \in R \setminus \{0_R\}$ και το αριστερό, μη τετριμμένο ιδεώδες Ra τού R, παρατηρούμε ότι

$$1_R \in R = Ra \Longrightarrow \exists b \in R \setminus \{0_R\} : ba = 1_R,$$

ήτοι ότι το στοιχείο a διαθέτει κάποιο εξ αριστερών αντίστροφο στοιχείο b. Επειδή $b \in R \setminus \{0_R\}$, επαναλαμβάνοντας την ανωτέρω επιχειρηματολογία για το b συμπεραίνουμε ότι

$$1_R \in R = Rb \Longrightarrow \exists c \in R \setminus \{0_R\} : cb = 1_R,$$

ήτοι ότι το b διαθέτει κάποιο εξ αριστερών αντίστροφο στοιχείο c. Επειδή το b έχει το a ως εκ δεξιών αντίστροφό του στοιχείο, έχουμε κατ' ανάγκην $a = c$ (βλ. πρόταση 6.2.8) και

$$ab = 1_R = ba \Longrightarrow a \in R^\times,$$

οπότε ο R είναι διαιρετικός δακτύλιος. Η ισοδυναμία (i)⇔(iii) αποδεικνύεται παρομοίως. □

7.1.9 Πόρισμα. *Τα μόνα αμφίπλευρα ιδεώδη ενός διαιρετικού δακτυλίου R είναι το $\{0_R\}$ και ο ίδιος ο R.*

7.1.10 Παρατήρηση. Υπάρχουν *μη μεταθετικοί*, *μη διαιρετικοί* δακτύλιοι R, όπως είναι ο $R = \mathrm{Mat}_{2\times 2}(\mathbb{R})$ (βλ. πρόταση 7.3.4), οι οποίοι δεν διαθέτουν άλλα αμφίπλευρα ιδεώδη πέραν των $\{0_R\}$ και R.

7.1.11 Πόρισμα. *Έστω R ένας μη τετριμμένος, μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Τότε ο R είναι σώμα εάν και μόνον εάν τα μόνα αμφίπλευρα ιδεώδη του είναι το $\{0_R\}$ και ο ίδιος ο R.*

7.2 ΙΔΕΩΔΗ ΠΑΡΑΓΟΜΕΝΑ ΑΠΟ ΣΥΝΟΛΑ

Μια συνήθης μέθοδος κατασκευής ιδεωδών ενός δοθέντος δακτυλίου είναι η κατά φυσικό τρόπο «παραγωγή τους» από τυχόντα υποσυνόλα τού δακτυλίου.

7.2.1 Ορισμός. Έστω $(R, +, \cdot)$ ένας δακτύλιος και έστω $A \subseteq R$. Λέμε ότι η τομή

$$\boxed{\langle A\rangle := \bigcap \{\text{ιδεώδη } I \text{ τού } R \mid I \supseteq A\}}$$

των μελών τής οικογενείας όλων των ιδεωδών αυτού, τα οποία περιέχουν το A, είναι **το ιδεώδες το παραγόμενο από το** A ή το ιδεώδες **με γεννήτορες** τα στοιχεία τού A. Όταν $A = \varnothing$, τότε $\langle A\rangle = \{0_R\}$. Κάθε ιδεώδες τού R που μπορεί να γραφεί υπό τη μορφή $\langle A\rangle$, όπου $A \subseteq R$ είναι κάποιο πεπερασμένο υποσύνολο αυτού, ας πούμε το $A = \{a_1, \ldots, a_k\}$ (όπου $k \in \mathbb{N}$), καλείται **πεπερασμένως παραγόμενο ιδεώδες** και συμβολίζεται απλούστερα ως $\langle a_1, \ldots, a_k\rangle$. Τέλος, κάθε ιδεώδες τού R που μπορεί γραφεί υπό τη μορφή $\langle a\rangle$, για κάποιο $a \in R$, καλείται **κύριο ιδεώδες** (έχον το a ως γεννήτορά του).

7.2.2 Πρόταση. *Έστω R ένας δακτύλιος και έστω $\varnothing \neq A \subseteq R$.*

(i) *Το ιδεώδες $\langle A\rangle$ το παραγόμενο από το A αποτελείται από όλα τα στοιχεία τής μορφής*

$$\sum_{i=1}^{\kappa} r_i a_i s_i + \sum_{j=1}^{\mu} r'_j a'_j + \sum_{k=1}^{\nu} a''_k s''_k + \sum_{\varrho=1}^{\xi} n_\varrho a'''_\varrho \tag{7.1}$$

$r_i, s_i, r'_j, s''_k \in R,\ \ a_i, a'_j, a''_k, a'''_\varrho \in A$ *και* $n_\varrho \in \mathbb{Z}$,

$$\forall i \in \{1, ..., \kappa\},\ \ \forall j \in \{1, ..., \mu\},\ \ \forall k \in \{1, ..., \nu\},\ \ \forall \varrho \in \{1, ..., \xi\},$$

όπου κ, μ, ν, ξ είναι θετικοί ακέραιοι αριθμοί.

(ii) *Εάν ο R είναι δακτύλιος με μοναδιαίο στοιχείο, τότε*

$$\langle A\rangle = \left\{ \sum_{i=1}^{\kappa} r_i\, a_i\, s_i \;\middle|\; r_1, \ldots, r_\kappa, s_1, \ldots, s_\kappa \in R,\ a_1, ..., a_\kappa \in A,\ \ \kappa \in \mathbb{N} \right\}.$$

(iii) *Εάν ο R είναι μεταθετικός δακτύλιος, τότε*

$$\langle A\rangle = \left\{ \sum_{i=1}^{\kappa} r_i\, a_i \ + \sum_{\varrho=1}^{\xi} n_\varrho a'_\varrho \;\middle|\; \begin{array}{c} r_1, \ldots, r_\kappa \in R,\ \ n_1, \ldots, n_\xi \in \mathbb{Z}, \\ a_1, ..., a_\kappa, a'_1, ..., a'_\xi, \in A,\ \ \ \kappa, \xi \in \mathbb{N} \end{array} \right\}.$$

(iv) *Εάν ο R είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, τότε*

$$\langle A\rangle = \left\{ \sum_{i=1}^{\kappa} r_i\, a_i \;\middle|\; r_1, \ldots, r_\kappa \in R,\ a_1, \ldots, a_\kappa \in A,\ \kappa \in \mathbb{N} \right\}.$$

Απόδειξη. (i) Έστω I το υποσύνολο τού R το απαρτιζόμενο από όλα τα στοιχεία τής μορφής (7.1). Τόσο η διαφορά δυο στοιχείων τής μορφής (7.1) όσο και το γινόμενο ενός $r \in R$ με οιοδήποτε στοιχείο τής μορφής (7.1) είναι και πάλι τής μορφής (7.1). Άρα το I είναι ένα ιδεώδες τού R που περιέχει το A (αφού -λόγω τού τελευταίου αθροίσματος- $1_{\mathbb{Z}} a = a \in I$, για κάθε $a \in A$). Κατά συνέπειαν, $\langle A\rangle \subseteq I$. Και αντιστρόφως· κάθε ιδεώδες που περιέχει το A οφείλει να περιέχει και τα αθροίσματα τής μορφής (7.1), οπότε έχουμε $I \subseteq \langle A\rangle$.

(ii) Εάν ο R είναι ένας δακτύλιος με μοναδιαίο στοιχείο, τότε τα αθροίσματα τής μορφής (7.1) μπορούν να «συμπτυχθούν» (κατά τα αναγραφόμενα), αφού

$$r\, a = r\, a\, 1_R, \quad a\, s = a\, s\, 1_R, \ \ \forall a \in A, \ \ \forall\, (r, s) \in R \times R,$$

και $na = n\,(1_R\, a) = (n\, 1_R)\,(a\, 1_R)\,,\ \forall n \in \mathbb{Z}$ και $\forall a \in A$.

(iii) Εάν ο R είναι ένας μεταθετικός δακτύλιος, τότε τα αθροίσματα τής μορφής (7.1) μπορούν και πάλι να «συμπτυχθούν» (κατά τα αναγραφόμενα), αφού

$$ras = (rs)a,\ ra = ar, \ \ \forall a \in A, \ \ \forall\, (r, s) \in R \times R.$$

(iv) Τέλος, εάν ο R είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, τότε ενσωματώνουμε στο $\langle A\rangle$ και τα δύο είδη «συμπτύξεων» τής μορφής των στοιχείων που περιγράψαμε προηγουμένως στα (ii) και (iii). □

7.2.3 Σημείωση. Εάν ο R είναι ένας δακτύλιος και $A \subseteq R$, τότε μπορεί κανείς να ορίσει και τα δεξιά/αριστερά ιδεώδη

$$\langle A\rangle_{\alpha\varrho} := \bigcap \{\, \text{αριστερά ιδεώδη } I \ \text{ τού } \ R \mid\ I \supseteq A\}$$

και

$$\langle A\rangle_{\delta} := \bigcap \{\, \text{δεξιά ιδεώδη } I \ \text{ τού } \ R \mid\ I \supseteq A\}\,,$$

αντιστοίχως, *τα παραγόμενα από το* A, και να αποδείξει τις ιδιότητές τους που αναλογούν σε αυτές που προαναφέρθηκαν στην πρόταση 7.2.2 για το $\langle A\rangle$.

7.2.4 Πόρισμα. *Έστω* R *ένας δακτύλιος και έστω* $a \in R$.

(i) *Το κύριο ιδεώδες* $\langle a\rangle$ *αποτελείται από όλα τα στοιχεία τής μορφής*

$$\sum_{j=1}^{k} r_j\, a\, s_j + r\, a + a\, s + n\, a,$$

$r, s, r_1, \ldots, r_k, s_1, \ldots, s_k \in R,\ k \in \mathbb{N}$ *και* $n \in \mathbb{Z}$.

(ii) *Εάν ο* R *είναι δακτύλιος με μοναδιαίο στοιχείο, τότε*

$$\langle a\rangle = \left\{ \sum_{j=1}^{k} r_j\, a\, s_j \;\middle|\; r_1, \ldots, r_k, s_1, \ldots, s_k \in R,\ k \in \mathbb{N} \right\}.$$

(iii) *Εάν ο* R *είναι μεταθετικός δακτύλιος, τότε* $\langle a\rangle = \{r\, a + n\, a \mid r \in R,\ n \in \mathbb{Z}\}$.

(iv) *Εάν ο* R *είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, τότε*

$$\langle a\rangle = Ra = \{r\, a \mid r \in R\}.$$

7.2.5 Παρατήρηση. Όταν ο R είναι μεταθετικός αλλά *δεν* διαθέτει μοναδιαίο στοιχείο και $a \in R$, τα ιδεώδη του $\langle a\rangle$ και Ra *δεν* είναι κατ' ανάγκην ίσα. Επί παραδείγματι, όταν $R = 2\mathbb{Z}$, τότε $\langle 2\rangle \neq (2\mathbb{Z})\, 2$, διότι $2 \in \langle 2\rangle$, ενώ $2 \notin (2\mathbb{Z})\, 2$.

7.2.6 Πρόταση. *Κάθε ιδεώδες τού δακτυλίου* $\mathbb{Z}$ *των ακεραίων αριθμών είναι τής μορφής* $\langle n\rangle = n\mathbb{Z}$, *όπου* $n \in \mathbb{Z}$. *(Οι εν λόγω γεννήτορες* n *είναι, βεβαίως, δυνατόν να περιορισθούν στα στοιχεία τού συνόλου* $\mathbb{N}_0$, *καθότι μια ενδεχόμενη αλλαγή προσήμου τού εκάστοτε θεωρούμενου* n *δεν επιφέρει διαφοροποίηση τού κυρίου ιδεώδους* $\langle n\rangle$.*) Ως εκ τούτου, κάθε ιδεώδες τού δακτυλίου* $\mathbb{Z}$ *είναι κύριο ιδεώδες.*

Απόδειξη. Έστω I ένα ιδεώδες τού $\mathbb{Z}$. Εάν $I = \{0\}$, τότε $I = \langle 0\rangle$. Εάν $\{0\} \subsetneq I$, τότε υπάρχει κάποιος ακέραιος $n \in I \setminus \{0\}$. Άρα και ο αντίθετός του $-n$ ανήκει στο $I \setminus \{0\}$ (αφού $-n = 0 - n$ με $0 \in I$ και $n \in I$). Ως εκ τούτου, *κάθε* μη τετριμμένο ιδεώδες I τού $\mathbb{Z}$ περιέχει *θετικούς ακεραίους*. Έστω $n_0 := \min\{n \in \mathbb{N} \mid n \in I\}$. Θα δείξουμε ότι $I = \langle n_0\rangle$. Πράγματι· έστω a τυχόν στοιχείο τού I. Τότε το a διαιρούμενο με το n_0 δίνει υπόλοιπο r, όπου $a = n_0 q + r$, $q, r \in \mathbb{Z},\ 0 \leqslant r < n_0$, οπότε

$$q \in \mathbb{Z},\ n_0 \in I \Longrightarrow n_0 q \in I \underset{a \in I}{\Longrightarrow} a - n_0 q = r \in I,$$

απ' όπου έπεται ότι $r = 0$ (διότι αλλιώς θα παρουσιαζόταν αντίφαση ως προς την επιλογή τού n_0). Άρα $a = n_0 q \in \langle n_0\rangle$, ήτοι $I \subseteq \langle n_0\rangle$. Από την άλλη μεριά έχουμε $\langle n_0\rangle = \{kn_0 \mid k \in \mathbb{Z}\} \subseteq I$. Άρα τελικώς $I = \langle n_0\rangle = \langle -n_0\rangle$. □

7.2.7 Παρατήρηση. Είναι προφανές ότι υφίσταται *αμφίρριψη*[3]

$$\mathbb{N}_0 \ni n \longmapsto \langle n\rangle \in \{\text{ιδεώδη τού δακτυλίου } \mathbb{Z}\}.$$

[3] Η εν λόγω απεικόνιση είναι προφανώς *επιρριπτική* και στέλνει το 0 στο τετριμμένο ιδεώδες. Η *ενριπτικότητά* της έπεται από το γεγονός ότι για οιουσδήποτε $n, n' \in \mathbb{N}$ έχουμε $\langle n\rangle \subseteq \langle n'\rangle \Leftrightarrow$ ο n' διαιρεί τον n. (Επομένως, $\langle n\rangle = \langle n'\rangle \Leftrightarrow n = n'$.)

7.3 ΔΑΚΤΥΛΙΟΙ ΜΕ «ΛΙΓΑ» ΙΔΕΩΔΗ

Υπάρχουν δακτύλιοι με *μικρό αριθμό ιδεωδών*, οι οποίοι αξίζουν ιδιαίτερης μνείας.

7.3.1 Ορισμός. Ένας μη τετριμμένος δακτύλιος R ονομάζεται **απλός δακτύλιος**[4] όταν δεν διαθέτει (αμφίπλευρα) ιδεώδη πέραν τού $\{0_R\}$ και τού R.

7.3.2 Πρόταση. *Κάθε διαιρετικός δακτύλιος είναι απλός.*

Απόδειξη. Άμεση συνέπεια τού πορίσματος 7.1.11. □

7.3.3 Πρόταση. *Ένας μη τετριμμένος μεταθετικός δακτύλιος R με μοναδιαίο στοιχείο είναι σώμα εάν και μόνον εάν είναι απλός.*

Απόδειξη. Άμεση συνέπεια τού πορίσματος 7.1.9. □

7.3.4 Πρόταση. *Εάν ο R είναι ένας διαιρετικός δακτύλιος και $n \in \mathbb{N}$, τότε ο $\mathrm{Mat}_{n\times n}(R)$ είναι ένας απλός δακτύλιος.*

Απόδειξη. Έστω $\mathbf{E}_{ij} \in \mathrm{Mat}_{n\times n}(R)$ ο βοηθητικός πίνακας ο έχων ως εγγραφή του στην i-οστή γραμμή και στην j-οστή στήλη το 1_R και ως λοιπές εγγραφές του το 0_R. Σημειωτέον ότι για οιονδήποτε $\mathbf{A} \in \mathrm{Mat}_{n\times n}(R)$ και οιουσδήποτε $i, j \in \{1, ..., n\}$ έχουμε

$$\Gamma\varrho_k(\mathbf{E}_{ij}\mathbf{A}) = \begin{cases} \Gamma\varrho_j(\mathbf{A}), & \text{όταν } k = i, \\ (0_R, ..., 0_R), & \text{όταν } k \in \{1, ..., n\}\smallsetminus\{i\}, \end{cases} \tag{7.2}$$

και

$$\Sigma\tau_k(\mathbf{A}\mathbf{E}_{ij}) = \begin{cases} \Sigma\tau_i(\mathbf{A}), & \text{όταν } k = j, \\ (0_R, ..., 0_R)^{\intercal}, & \text{όταν } k \in \{1, ..., n\}\smallsetminus\{j\}. \end{cases} \tag{7.3}$$

Για την απόδειξη τής προτάσεως θεωρούμε ένα ιδεώδες I τού $\mathrm{Mat}_{n\times n}(R)$ διάφορο τού τετριμμένου. Τότε υπάρχει ένας πίνακας $\mathbf{A} = (a_{jk})_{1\leqslant j,k\leqslant n} \in I\smallsetminus\{0_{\mathrm{Mat}_{n\times n}(R)}\}$, οπότε υφίστανται $j_0, k_0 \in \{1, ..., n\}$ με $a_{j_0k_0} \neq 0_R$. Για κάθε δείκτη $l \in \{1, ..., n\}$ οι (7.2) και (7.3) μας οδηγούν στο συμπέρασμα ότι[5]

$$\mathbf{E}_{lj_0}\,\mathbf{A}\,\mathbf{E}_{k_0l} = \mathbf{E}_{lj_0}\left(\sum_{i=1}^{n} a_{ik_0}\mathbf{E}_{ik_0}\right) = \sum_{i=1}^{n} a_{ik_0}\mathbf{E}_{lj_0}\mathbf{E}_{ik_0} = a_{j_0k_0}\mathbf{E}_{ll}.$$

Επειδή $\mathbf{A} \in I$ και $\mathbf{E}_{lj_0}, \mathbf{E}_{k_0l} \in \mathrm{Mat}_{n\times n}(R)$, τούτο σημαίνει ότι $a_{j_0k_0}\mathbf{E}_{ll} \in I$. Επιπροσθέτως, επειδή ο R είναι διαιρετικός δακτύλιος, ορίζεται το αντίστροφο στοιχείο $a_{j_0k_0}^{-1}$ τού $a_{j_0k_0}$. Ως εκ τούτου,

$$\left.\begin{array}{l} a_{j_0k_0}\mathbf{E}_{ll} \in I, \\ a_{j_0k_0}^{-1}\mathbf{E}_{ll} \in \mathrm{Mat}_{n\times n}(R) \end{array}\right\} \Longrightarrow (a_{j_0k_0}\mathbf{E}_{ll})\left(a_{j_0k_0}^{-1}\mathbf{E}_{ll}\right) = \mathbf{E}_{ll} \in I,$$

απ' όπου έπεται ότι

$$\mathbf{I}_n := \begin{pmatrix} 1_R & 0_R & \cdots & 0_R & 0_R \\ 0_R & 1_R & \cdots & 0_R & 0_R \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0_R & 0_R & \cdots & 1_R & 0_R \\ 0_R & 0_R & \cdots & 0_R & 1_R \end{pmatrix} = \sum_{l=1}^{n} \mathbf{E}_{ll} \in I.$$

[4] Ο εν λόγω ορισμός είναι ανάλογος εκείνου των *απλών ομάδων*.

[5] Ο πίνακας $a_{j_0k_0}\mathbf{E}_{ll}$ δηλοί *αριθμητικό πολλαπλασιασμό* τού $\mathbf{E}_{ll}$ με τον $a_{j_0k_0}$ και είναι -ως εκ τούτου- ο πίνακας που έχει ως εγγραφή του στη θέση (l, l) το $a_{j_0k_0}$ και σε όλες τις άλλες θέσεις εγγραφές που είναι ίσες με το 0_R.

Επειδή το μοναδιαίο στοιχείο $\mathbf{I}_n$ τού $\mathrm{Mat}_{n\times n}(R)$ ανήκει στο ιδεώδες I, έχουμε κατ' ανάγκην $I = \mathrm{Mat}_{n\times n}(R)$. □

7.3.5 Πρόταση. *Κάθε ακεραία περιοχή R, η οποία διαθέτει μόνον έναν πεπερασμένο αριθμό ιδεωδών, είναι σώμα.*

Απόδειξη. Έστω $a \in R\setminus\{0_R\}$. Θεωρούμε τα κύρια ιδεώδη $\langle a\rangle, \langle a^2\rangle, \langle a^3\rangle, \ldots$ Επειδή

$$\left[a^{k+1} = aa^k \in \langle a^k\rangle,\ \forall k \in \mathbb{N}\right] \Longrightarrow \left[\langle a^{k+1}\rangle \subseteq \langle a^k\rangle,\ \forall k \in \mathbb{N}\right],$$

σχηματίζεται η εξής ακολουθία διαδοχικώς εγκλειομένων κυρίων ιδεωδών:

$$\langle a\rangle \supseteq \langle a^2\rangle \supseteq \langle a^3\rangle \supseteq \cdots$$

Επειδή η ακεραία περιοχή R διαθέτει μόνον έναν πεπερασμένο αριθμό ιδεωδών, θα υπάρχει κάποιος $n \in \mathbb{N}$, τέτοιος ώστε να ισχύει

$$\langle a^n\rangle = \langle a^{n+1}\rangle \Longrightarrow \left[(\exists r \in R) : a^n = ra^{n+1}\right].$$

Όμως τούτο έχει ως συνέπεια ότι $a^n(1_R - ra) = 0_R$, το οποίο, συνδυαζόμενο με το ότι $a^n \in R\setminus\{0_R\}$ και το ότι ο R είναι εξ υποθέσεως ακεραία περιοχή, μας δίδει την ισότητα $ra = 1_R$, οπότε το r είναι (πολλαπλασιαστικό) αντίστροφο τού (αυθαιρέτως επιλεγμένου) μη μηδενικού στοιχείου a. □

7.4 ΛΟΓΙΣΜΟΣ ΜΕ ΙΔΕΩΔΗ

Τα ιδεώδη ενός δακτυλίου μπορούν να προστεθούν, να πολλαπλασιασθούν ή -σε ορισμένες περιπτώσεις- και να διαιρεθούν. Η εξοικείωση με τον «λογισμό με ιδεώδη» θα αποβεί χρήσιμη τόσο για ορισμένα τμήματα τής αναπτυσσόμενης θεωρίας όσο και για την ευχερέστερη επίλυση ασκήσεων.

7.4.1 Ορισμός. Έστω ότι ο R είναι ένας δακτύλιος και τα $I_1, \ldots, I_n$, $n \in \mathbb{N}$, $n \geqslant 2$, αριστερά (και αντιστοίχως, δεξιά/αμφίπλευρα) ιδεώδη του. Ορίζουμε το **άθροισμα**[6] και το **γινόμενό** τους ως:

$$\boxed{I_1 + \cdots + I_n := \sum_{j=1}^{n} I_j := \{a_1 + \cdots + a_n \mid a_j \in I_j,\ \ \forall j,\ \ 1 \leqslant j \leqslant n\}}$$

και

$$\boxed{I_1 \cdots I_n := \left\{ \begin{array}{c} \text{αθροίσματα τής μορφής} \\ \displaystyle\sum_{j=1}^{k} a_{1,j}\, a_{2,j} \cdots a_{n,j},\ \ \text{με}\ a_{\varrho,j} \in I_\varrho,\ 1 \leqslant \varrho \leqslant n,\ k \in \mathbb{N} \end{array} \right\}}$$

αντιστοίχως[7]. Είναι εύκολο να διαπιστωθεί ότι τόσο το $I_1 + \cdots + I_n$ όσο και το $I_1 \cdots I_n$ αποτελεί ένα αριστερό (και αντιστοίχως, ένα δεξιό/αμφίπλευρο) ιδεώδες τού R.

[6] Το **άθροισμα** μπορεί να ορισθεί και για *τυχούσες* οικογένειες ιδεωδών $(I_\lambda)_{\lambda\in\Lambda}$ τού R (με $\Lambda \neq \varnothing$) ως ακολούθως:

$$\sum_{\lambda\in\Lambda} I := \left\{ a_{\lambda_1} + \cdots + a_{\lambda_k} \;\middle|\; \begin{array}{c} a_j \in I_j,\ \ \forall j \in \{\lambda_1, \ldots, \lambda_k\}, \\ \text{για οιοδήποτε}\ \{\lambda_1, \ldots, \lambda_k\} \subseteq \Lambda,\ k \in \mathbb{N} \end{array} \right\}.$$

[7] Προσοχή! Μη συγχέετε το γινόμενο $IJ := \left\{ \sum_{j=1}^{k} a_j b_j \,\middle|\, a_j \in I, b_j \in J,\ k \in \mathbb{N} \right\}$ δυο ιδεωδών I, J τού R με το σύνολο $\{\, ab \mid a \in I, b \in J\}$! Το τελευταίο ενδέχεται *να μην είναι ιδεώδες* (ακόμη και αν ο R είναι μεταθετικός με

7.4.2 Σημείωση. (i) Εάν τα $I_1, \ldots, I_n$ είναι ιδεώδη ενός δακτυλίου R με μοναδιαίο στοιχείο, τότε

$$I_1 + \cdots + I_n = \langle I_1 \cup \cdots \cup I_n \rangle .$$

Πράγματι· από τον ορισμό τού $I_1 + \cdots + I_n$ ο εγκλεισμός "$\subseteq$" είναι προφανής. Και επειδή το ιδεώδες $\langle I_1 \cup \cdots \cup I_n \rangle$ ισούται με

$$\left\{ \sum_{i=1}^{\kappa} r_i\, a_i\, s_i \;\middle|\; r_1, \ldots, r_\kappa, s_1, \ldots, s_\kappa \in R,\ a_1, ..., a_\kappa \in I_1 \cup \cdots \cup I_n,\ \ \kappa \in \mathbb{N} \right\},$$

κάθε $x \in \langle I_1 \cup \cdots \cup I_n \rangle$ μπορεί (ενδεχομένως ύστερα από κάποια αναδιάταξη δεικτών) να γραφεί υπό τη μορφή $x = x_1 + x_2 + \cdots + x_n$, όπου για κάθε $j \in \{1, \ldots, n\}$,

$$x_j = \sum_{i=1}^{\kappa_j} r_i\, a_i\, s_i, \quad r_1, \ldots, r_{\kappa_j}, s_1, \ldots, s_{\kappa_j} \in R,$$

για κατάλληλα $a_1, ..., a_{\kappa_j} \in I_j$ και $\kappa_j \in \mathbb{N}$. Άρα έχουμε και

$$\langle I_1 \cup \cdots \cup I_n \rangle \subseteq I_1 + \cdots + I_n.$$

(ii) Ας σημειωθεί ότι -εν αντιθέσει προς την τομή- η *ένωση* δυο ιδεωδών ενός δακτυλίου μπορεί να *μην* αποτελεί ιδεώδες τού θεωρούμενου δακτυλίου[8]. Επί παραδείγματι, η ένωση $3\mathbb{Z} \cup 5\mathbb{Z}$ των κυρίων ιδεωδών $\langle 3 \rangle = 3\mathbb{Z}$ και $\langle 5 \rangle = 5\mathbb{Z}$ τού $\mathbb{Z}$ δεν είναι ιδεώδες τού $\mathbb{Z}$, διότι τόσον το 3 όσον και το 5 ανήκουν στην $3\mathbb{Z} \cup 5\mathbb{Z}$, αλλ' εντούτοις $2 = 5 - 3 \notin 3\mathbb{Z} \cup 5\mathbb{Z}$.

(iii) Στην περίπτωση κατά την οποία $I_1 = \cdots = I_n = I$, συμβολίζουμε το γινόμενο $I_1 \cdots I_n$ και ως I^n (ήτοι εν είδει «δυνάμεως»), προσέχοντας -όμως- να μην το συγχέουμε με το καρτεσιανό γινόμενο τού I (n φορές) με τον εαυτό του! Για κάθε ιδεώδες I ενός δακτυλίου R προκύπτει μια ακολουθία διαδοχικώς εγκλειομένων ιδεωδών

$$I \supseteq I^2 \supseteq I^3 \supseteq \cdots \supseteq I^\kappa \supseteq I^{\kappa+1} \supseteq \cdots\ ,\ \forall \kappa \in \mathbb{N}.$$

Επί παραδείγματι, εντός τού δακτυλίου $\mathbb{Z}$ των ακεραίων (πρβλ. 7.4.13 (iii)), έχουμε

$$\langle 2 \rangle \supsetneq \langle 4 \rangle \supsetneq \langle 8 \rangle \supsetneq \cdots \supsetneq \langle 2^\kappa \rangle \supsetneq \left\langle 2^{\kappa+1} \right\rangle \supsetneq \cdots\ ,\ \forall \kappa \in \mathbb{N}.$$

Οι προτάσεις 7.4.3, 7.4.4, 7.4.5 και 7.4.14, οι οποίες ακολουθούν, έχουν ως στόχο την περιγραφή ορισμένων βασικών αρχών τού «λογισμού με ιδεώδη».

7.4.3 Πρόταση. *Εάν ο R είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και $a, b \in R$, τότε*

(i) $\langle a \rangle + \langle b \rangle = \{ xa + yb \mid\ x, y \in R \}$, *και*
(ii) $\langle a \rangle \langle b \rangle = \langle ab \rangle$.

Απόδειξη. (i) Επειδή έχουμε $\langle a \rangle = Ra$ και $\langle b \rangle = Rb$, τούτο έπεται άμεσα από το 7.4.2 (i).

μοναδιαίο στοιχείο). Επί παραδείγματι, εάν στον $R = \mathbb{R}[\mathsf{X}_1, \mathsf{X}_2]$ θεωρήσουμε τα $I = J = \langle \mathsf{X}_1, \mathsf{X}_2 \rangle$, τότε τα στοιχεία X_1^2 και X_2^2 ανήκουν στο $\{ \varphi(\mathsf{X}_1, \mathsf{X}_2)\psi(\mathsf{X}_1, \mathsf{X}_2) \mid \varphi(\mathsf{X}_1, \mathsf{X}_2) \in I,\ \psi(\mathsf{X}_1, \mathsf{X}_2) \in J \}$. Ωστόσο, το άθροισμά τους $\mathsf{X}_1^2 + \mathsf{X}_2^2$ δεν ανήκει σε αυτό.

[8] Είναι εύκολο να αποδειχθεί ότι η ένωση $I \cup J$ δυο ιδεωδών I, J ενός δακτυλίου R αποτελεί ιδεώδες αυτού εάν και μόνον εάν είτε $I \subseteq J$ είτε $J \subseteq I$.

(ii) Προφανώς,

$$\begin{aligned}\langle a\rangle\langle b\rangle &= \left\{ \sum_{j=1}^{k} (r_j a)\,(s_j b) \;\middle|\; r_1,\ldots,r_k,s_1,\ldots,s_k \in R,\ k\in\mathbb{N} \right\} \\ &= \left\{ \left(\sum_{j=1}^{k} r_j s_j \right) ab \;\middle|\; r_1,\ldots,r_k,s_1,\ldots,s_k \in R,\ k\in\mathbb{N} \right\} \\ &= Rab,\end{aligned}$$

όπου $Rab = \langle ab\rangle$. □

7.4.4 Πρόταση. *Έστω ότι ο R είναι ένας δακτύλιος και I_1, I_2, I_3, I_3' τέσσερα (αριστερά, δεξιά ή αμφίπλευρα) ιδεώδη του. Τότε ισχύουν τα εξής:*
(i) $(I_1 + I_2) + I_3 = I_1 + (I_2 + I_3)$,
(ii) $(I_1\, I_2)\; I_3 = I_1\; (I_2\, I_3)$,
(iii) $I_1\; (I_2 + I_3) = (I_1\, I_2) + (I_1\, I_3)$, $(I_1 + I_2)\; I_3' = (I_1\, I_3') + (I_2\, I_3')$.

Απόδειξη. (i) Έστω τυχόν $a \in (I_1 + I_2) + I_3$. Το a γράφεται ως άθροισμα $c + a_3$, όπου $c \in I_1 + I_2$ και $a_3 \in I_3$, και το $c = a_1 + a_2$, όπου $a_1 \in I_1$ και $a_2 \in I_2$. Επομένως, λόγω της προσεταιριστικής ιδιότητας της προσθέσεως,

$$a = (a_1 + a_2) + a_3 = a_1 + (a_2 + a_3) \in I_1 + (I_2 + I_3)\,,$$

ήτοι $(I_1 + I_2) + I_3 \subseteq I_1 + (I_2 + I_3)$. Και αντιστρόφως· εάν $b \in I_1 + (I_2 + I_3)$, τότε το b γράφεται ως άθροισμα $b_1 + d$, όπου $b_1 \in I_1$ και $d \in I_2 + I_3$, και το $d = b_2 + b_3$, όπου $b_2 \in I_2$ και $b_3 \in I_3$. Επομένως, και πάλι λόγω της προσεταιριστικής ιδιότητας της προσθέσεως,

$$b = b_1 + (b_2 + b_3) = (b_1 + b_2) + b_3 \in (I_1 + I_2) + I_3.$$

Κατά συνέπειαν, $(I_1 + I_2) + I_3 = I_1 + (I_2 + I_3)$.
(ii) Έστω τυχόν $x \in (I_1\, I_2)\; I_3$. Τότε

$$x = \sum_{j=1}^{k} x_j c_j, \quad \text{όπου } k\in\mathbb{N},\ \ x_j \in I_1\, I_2,\ \ c_j \in I_3,\ \ \forall j \in \{1,\ldots,k\}.$$

Παρομοίως, για κάθε $j \in \{1,\ldots,k\}$,

$$x_j = \sum_{l=1}^{s_j} a_{jl} b_{jl}, \quad \text{όπου } s_j \in \mathbb{N},\ \ a_{jl} \in I_1,\ \ b_{jl} \in I_2,\ \ \forall l \in \{1,\ldots,s_j\}.$$

Επομένως, λόγω της επιμεριστικής ιδιότητας,

$$x = \sum_{j=1}^{k} \left(\sum_{l=1}^{s_j} a_{jl} b_{jl} \right) c_j = \sum_{j=1}^{k} \sum_{l=1}^{s_j} a_{jl}(b_{jl} c_j) \in I_1\; (I_2\, I_3) \Longrightarrow (I_1\, I_2)\; I_3 \subseteq I_1\; (I_2\, I_3)\,.$$

Αναλόγως αποδεικνύεται και η εγκλειστική σχέση $I_1\; (I_2\, I_3) \subseteq (I_1\, I_2)\; I_3$.
(iii) Έστω τυχόν $x \in I_1\; (I_2 + I_3)$. Τότε

$$x = \sum_{j=1}^{k} a_j\,(b_j + c_j)\,, \quad \text{όπου } k\in\mathbb{N},\ a_j \in I_1,\ b_j \in\ I_2,\ c_j \in I_3,\ \ \forall j \in \{1,\ldots,k\},$$

οπότε, λόγω τής επιμεριστικής ιδιότητας,

$$x = \underbrace{\sum_{j=1}^{k} a_j b_j}_{\in I_1\, I_2} + \underbrace{\sum_{j=1}^{k} a_j c_j}_{\in I_1\, I_3},$$

απ' όπου έπεται ότι $I_1\ (I_2 + I_3) \subseteq (I_1\, I_2) + (I_1\, I_3)$. Αναλόγως αποδεικνύεται και η αντίστροφη εγκλειστική σχέση, καθώς και η $(I_1 + I_2)\ I_3' = (I_1\, I_3') + (I_2\, I_3')$. □

7.4.5 Πρόταση. *Έστω ότι ο R είναι ένας δακτύλιος και τα I_1, I_2, I_3 ιδεώδη του. Τότε ισχύουν τα εξής:*
(i) $I_1\, I_2 \subseteq I_1 \cap I_2$.
(ii) $(I_1 + I_2)\ (I_1 + I_3) \subseteq I_1 + I_2\, I_3 \subseteq I_1 + (I_2 \cap I_3)$.

Απόδειξη. (i) Εάν $x \in I_1\, I_2$, τότε

$$x = \sum_{j=1}^{k} a_j b_j, \quad \text{όπου } k \in \mathbb{N},\ \ a_j \in I_1,\ \ b_j \in I_2,\ \ \forall j \in \{1, \ldots, k\}.$$

Όμως, από τον ορισμό τού ιδεώδους,

$$\left.\begin{array}{l} (a_j \in I_1 \subseteq R) \Longrightarrow (a_j b_j \in I_2) \Longrightarrow x \in I_2 \\ (b_j \in I_2 \subseteq R) \Longrightarrow (a_j b_j \in I_1) \Longrightarrow x \in I_1 \end{array}\right\} \Longrightarrow x \in I_1 \cap I_2.$$

(ii) Έστω τυχόν $x \in (I_1 + I_2)\ (I_1 + I_3)$. Τότε

$$x = \sum_{j=1}^{k} y_j z_j, \quad \text{όπου } k \in \mathbb{N},\ \ y_j \in I_1 + I_2,\ \ z_j \in I_1 + I_3,\ \ \forall j \in \{1, \ldots, k\},$$

οπότε, λόγω τής επιμεριστικής ιδιότητας και τού ότι

$$y_j = a_j + b_j, \quad z_j = c_j + d_j,$$

για κάποια $a_j \in I_1, b_j \in I_2, c_j \in I_1, d_j \in I_3, \forall j \in \{1, \ldots, k\}$, έχουμε

$$x = \left(\underbrace{\sum_{j=1}^{k} (a_j c_j + a_j d_j + b_j c_j)}_{\in I_1} + \underbrace{\sum_{j=1}^{k} b_j d_j}_{\in I_2\, I_3} \right) \in I_1 + I_2\, I_3,$$

δηλαδή $(I_1 + I_2)\ (I_1 + I_3) \subseteq I_1 + I_2\, I_3$. Η δεύτερη εγκλειστική σχέση έπεται άμεσα από την (i). □

7.4.6 Σημείωση. Οι εγκλεισμοί (i) και (ii) τής προτάσεως 7.4.5 μπορούν να είναι αυστηροί ακόμη και για μεταθετικούς δακτυλίους με μοναδιαίο στοιχείο. Επί παραδείγματι, εάν εντός τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών θεωρήσουμε τα ιδεώδη I_1, I_2, με $I_1 = I_2 := \langle 2 \rangle$, τότε

$$I_1\, I_2 = \langle 4 \rangle \subsetneqq I_1 \cap I_2 = \langle 2 \rangle .$$

Επίσης, για τα ιδεώδη $I_1 := \langle 12 \rangle$, $I_2 := \langle 20 \rangle$, $I_3 := \langle 30 \rangle$ έχουμε

$$(I_1 + I_2)\ (I_1 + I_3) = \langle 24 \rangle \subsetneqq I_1 + I_2\, I_3 = \langle 12 \rangle$$

και για τα ιδεώδη $I_1 := \langle 24 \rangle$, $I_2 := \langle 4 \rangle$, $I_3 := \langle 6 \rangle$ έχουμε

$$I_1 + I_2\, I_3 = \langle 24 \rangle \subsetneqq I_1 + (I_2 \cap I_3) = \langle 12 \rangle .$$

(Πρβλ. πόρισμα 7.4.13).

7.4.7 Πρόταση. *Έστω ότι ο R είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και τα I_1, I_2 δυο ιδεώδη του με $I_1 + I_2 = R$. Τότε*

$$I_1\, I_2 = I_1 \cap I_2.$$

Απόδειξη. Κατά το (i) τής προτάσεως 7.4.5, $I_1\, I_2 \subseteq I_1 \cap I_2$. Έστω τυχόν στοιχείο $a \in I_1 \cap I_2$. Επειδή $I_1 + I_2 = R$, υπάρχουν $b \in I_1$ και $c \in I_2$, τέτοια ώστε να ισχύει η ισότητα $b + c = 1_R$, οπότε

$$\left.\begin{aligned} a = a \cdot 1_R = a(b+c) = ab + ac \\ a \in I_2, b \in I_1 \Rightarrow ab \in I_2\, I_1 = I_1\, I_2 \\ a \in I_1, c \in I_2 \Rightarrow ac \in I_1\, I_2 \end{aligned}\right\} \Longrightarrow a \in I_1\, I_2,$$

απ' όπου έπεται και ο αντίστροφος εγκλεισμός $I_1 \cap I_2 \subseteq I_1\, I_2$. □

7.4.8 Ορισμός. Κάθε ιδεώδες I ενός δακτυλίου R, για το οποίο

$$\exists n \in \mathbb{N} : I^n = \{0_R\},$$

καλείται **μηδενοδύναμο ιδεώδες**.

7.4.9 Πρόταση. *Κάθε στοιχείο ενός μηδενοδύναμου ιδεώδους I ενός δακτυλίου R είναι μηδενοδύναμο στοιχείο τού R* (βλ. 6.2.15)*, δηλαδή $I \subseteq \mathrm{Nil}(R)$.*

Απόδειξη. Εάν το I είναι ένα μηδενοδύναμο ιδεώδες ενός δακτυλίου R, τότε υπάρχει $n \in \mathbb{N} : I^n = \{0_R\}$, οπότε $\prod_{i=1}^{n} a_i = 0_R$ για οιαδήποτε $a_1, \ldots, a_n \in I$. Ιδιαιτέρως, για κάθε $a \in I$, $a^n = 0_R$, οπότε $a \in \mathrm{Nil}(R)$. □

7.4.10 Σημείωση. Εάν το I είναι ιδεώδες ενός δακτυλίου R με $I \subseteq \mathrm{Nil}(R)$, το I δεν είναι κατ' ανάγκην μηδενοδύναμο ιδεώδες. (Για να συμβαίνει αυτό, θα πρέπει να πληρούνται κάποιες *επιπρόσθετες συνθήκες*, όπως εκείνες που περιγράφονται στην πρόταση 7.4.11.) Επί παραδείγματι, θεωρώντας τό $I := \mathrm{Nil}(R)$ (που είναι ιδεώδες βάσει τής ασκήσεως 3 τού φυλλαδίου 12) εντός τού μεταθετικού δακτυλίου $R := \prod_{\nu=1}^{\infty} \mathbb{Z}_{2^\nu}$ (βλ. 6.1.4 (iv) και (v)), παρατηρούμε ότι το I δεν είναι μηδενοδύναμο ιδεώδες. Πράγματι· υποθέτοντας την ύπαρξη κάποιου $n \in \mathbb{N} : I^n = \{0_R\}$, θα έπρεπε να ισχύει $a^n = 0_R$ *για κάθε* στοιχείο $a \in I$, πράγμα αδύνατο, διότι π.χ. για τα στοιχεία

$$a_n := ([0]_2, [0]_{2^2}, \ldots, [0]_{2^{n-1}}, [0]_{2^n}, [2]_{2^{n+1}}, [0]_{2^{n+2}}, [0]_{2^{n+3}}, \ldots) \in R$$

(τα οριζόμενα για κάθε $n \in \mathbb{N}$), έχουμε $a_n^{n+1} = 0_R$ και $a_n^n \neq 0_R$.

7.4.11 Πρόταση. *Εάν το I είναι ένα πεπερασμένως παραγόμενο ιδεώδες ενός μεταθετικού δακτυλίου R με μοναδιαίο στοιχείο και $I \subseteq \mathrm{Nil}(R)$, τότε το I είναι μηδενοδύναμο ιδεώδες.*

Απόδειξη. Εάν $I = \langle a_1, \ldots, a_\kappa \rangle$, τότε (εξ υποθέσεως) $\exists n_j \in \mathbb{N} : a_j^{n_j} = 0_R$ για κάθε $j \in \{1, \ldots, \kappa\}$. Έστω $n := \max\{n_j | \, j \in \{1, \ldots, \kappa\}\}$ και έστω x τυχόν στοιχείο τού I. Προφανώς,

$$a_j^n = 0_R, \ \forall j \in \{1, \ldots, \kappa\}. \tag{7.4}$$

Κατά το (iii) τής προτάσεως 7.2.2 υπάρχουν $r_1, \ldots, r_\kappa \in R$, τέτοια ώστε να ισχύει η ισότητα $x = \sum_{j=1}^{\kappa} r_j a_j$. Επειδή ο R είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, έχουμε (λόγω τού ορισμού τού n, των ισοτήτων (7.4) και τού τύπου (6.4))

$$\left(\sum_{j=1}^{\kappa} r_j a_j \right)^{\kappa n} = 0_R \Longrightarrow x^{\kappa n} = 0_R, \ \forall x \in I.$$

Σημειωτέον ότι για κάθε $m \in \mathbb{N}$ ισχύει (εξ ορισμού) η ισότητα

$$\begin{aligned} I^m &= \langle \{ a_{i_1} a_{i_2} \cdots a_{i_m} \,|\, 1 \leqslant i_1, i_2, \ldots, i_m \leqslant \kappa \} \rangle \\ &= \left\langle \left\{ a_1^{\lambda_1} a_2^{\lambda_2} \cdots a_\kappa^{\lambda_\kappa} \,\middle|\, (\lambda_1, \lambda_2, \ldots, \lambda_\kappa) \in \mathbb{N}_0^\kappa : \sum_{j=1}^{\kappa} \lambda_j = m \right\} \right\rangle. \end{aligned}$$

Ειδικότερα, για $m = \kappa n$ λαμβάνουμε

$$I^{\kappa n} = \left\langle \left\{ a_1^{\lambda_1} a_2^{\lambda_2} \cdots a_\kappa^{\lambda_\kappa} \,\middle|\, (\lambda_1, \lambda_2, \ldots, \lambda_\kappa) \in \mathbb{N}_0^\kappa : \sum_{j=1}^{\kappa} \lambda_j = \kappa n \right\} \right\rangle$$

Θα αποδείξουμε ότι $I^{\kappa n} = \{0_R\}$. Προς τούτο αρκεί να αποδείξουμε ότι όλοι οι γεννήτορες τού $I^{\kappa n}$ είναι ίσοι με το 0_R. Όμως κάθε γεννήτοράς του (βάσει των προαναφερθέντων) είναι τής μορφής $a_1^{\lambda_1} a_2^{\lambda_2} \cdots a_\kappa^{\lambda_\kappa}$, όπου

$$(\lambda_1, \lambda_2, \ldots, \lambda_\kappa) \in \mathbb{N}_0^\kappa : \sum_{j=1}^{\kappa} \lambda_j = \kappa n.$$

Ως εκ τούτου, υπάρχει *τουλάχιστον ένας* δείκτης $\xi \in \{1, \ldots, \kappa\}$ με[9] $\lambda_\xi \geqslant n$, απ' όπου έπεται ότι

$$\begin{aligned} a_1^{\lambda_1} a_2^{\lambda_2} \cdots a_\kappa^{\lambda_\kappa} &= a_1^{\lambda_1} \cdots a_{\xi-1}^{\lambda_{\xi-1}} a_\xi^{\lambda_\xi} a_{\xi+1}^{\lambda_{\xi+1}} \cdots a_\kappa^{\lambda_\kappa} \\ &= a_1^{\lambda_1} \cdots a_{\xi-1}^{\lambda_{\xi-1}} \left(a_\xi^n a_\xi^{\lambda_\xi - n} \right) a_{\xi+1}^{\lambda_{\xi+1}} \cdots a_\kappa^{\lambda_\kappa} \\ &= a_1^{\lambda_1} \cdots a_{\xi-1}^{\lambda_{\xi-1}} \left(0_R \cdot a_\xi^{\lambda_\xi - n} \right) a_{\xi+1}^{\lambda_{\xi+1}} \cdots a_\kappa^{\lambda_\kappa} = 0_R. \end{aligned}$$

Άρα τελικώς $I^{\kappa n} = \{0_R\}$. □

7.4.12 Ορισμός. Έστω ότι ο R είναι ένας μεταθετικός δακτύλιος και τα I, J δυο ιδεώδη του. Το **πηλίκο** $I : J$ τού I διά τού J ορίζεται ως

$$\boxed{I : J := \{ r \in R \mid ra \in I \ \text{ για κάθε } a \in J \} = \{ r \in R \mid rJ \subseteq I \}}$$

και αποτελεί ένα ιδεώδες τού R.

Οι «πράξεις» που ορίσαμε επί των ιδεωδών μεταθετικών δακτυλίων, εφαρμοζόμενες στον δακτύλιο $\mathbb{Z}$, συμπεριφέρονται ως ακολούθως:

7.4.13 Πόρισμα. *Εάν $\langle m \rangle$ και $\langle n \rangle$ είναι δύο μη τετριμμένα ιδεώδη τού δακτυλίου $\mathbb{Z}$ των ακεραίων, όπου $m, n \in \mathbb{Z} \smallsetminus \{0\}$, τότε ισχύουν τα εξής:*

(i) $\langle m \rangle \cap \langle n \rangle = \langle \text{εκπ}(m,n) \rangle$,

(ii) $\langle m \rangle + \langle n \rangle = \langle \text{μκδ}(m,n) \rangle$,

(iii) $\langle m \rangle \langle n \rangle = \langle mn \rangle$,

(iv) $\langle m \rangle : \langle n \rangle = \left\langle \frac{m}{\text{μκδ}(m,n)} \right\rangle$.

[9] Αλλιώς θα είχαμε $\sum_{j=1}^{\kappa} \lambda_j < \kappa n$.

Απόδειξη. (i) Έστω τυχόν $a \in \langle m\rangle \cap \langle n\rangle$. Τότε $a \in \langle m\rangle$ και $a \in \langle n\rangle$, οπότε έχουμε $a = \lambda m = \kappa n$, για κάποιους $\lambda, \kappa \in \mathbb{Z}$. Έστω $d := \text{μκδ}(m,n)$. Προφανώς,

$$\lambda\left(\frac{m}{d}\right) d = \kappa\left(\frac{n}{d}\right) d \Longrightarrow \lambda\left(\frac{m}{d}\right) = \kappa\left(\frac{n}{d}\right) \Longrightarrow \frac{n}{d}\Big|\, \lambda\left(\frac{m}{d}\right),$$

και επειδή $\text{μκδ}\left(\frac{m}{d}, \frac{n}{d}\right) = 1$, έχουμε $\frac{n}{d}\big|\, \lambda \Longrightarrow \lambda = \nu\, \frac{n}{d}$, για κάποιον $\nu \in \mathbb{Z}$. Κατά συνέπειαν,

$$a = \lambda m = \nu\, \frac{n}{d}\, m = \left(\frac{mn}{d}\right) \nu = \text{sign}\,(mn)\ \text{εκπ}\,(m,n)\ \nu \Longrightarrow a \in \langle \text{εκπ}(m,n)\rangle,$$

ήτοι $\langle m\rangle \cap \langle n\rangle \subseteq \langle \text{εκπ}(m,n)\rangle$. Και αντιστρόφως· εάν $a \in \langle \text{εκπ}(m,n)\rangle$, τότε έχουμε $a = \mu\, \text{εκπ}(m,n)$, για κάποιον $\mu \in \mathbb{Z}$, οπότε[10]

$$a = \mu\, \frac{|m|\ |n|}{\text{μκδ}(m,n)} = m\left(\frac{\mu\, \text{sign}\,(m)\ |n|}{\text{μκδ}(m,n)}\right) = n\left(\frac{\mu\, \text{sign}\,(n)\ |m|}{\text{μκδ}(m,n)}\right),$$

όπου $\frac{\mu\, \text{sign}(m)\, |n|}{\text{μκδ}(m,n)} \in \mathbb{Z}$ και $\frac{\mu\, \text{sign}(n)\, |m|}{\text{μκδ}(m,n)} \in \mathbb{Z}$. Συνεπώς έχουμε $a \in \langle m\rangle \cap \langle n\rangle$, δηλαδή

$$\langle \text{εκπ}(m,n)\rangle \subseteq \langle m\rangle \cap \langle n\rangle.$$

(ii) Κατά το (i) τής προτάσεως 7.4.3, $\langle m\rangle + \langle n\rangle = \{\, xm + yn \mid x, y \in \mathbb{Z}\}$. Επειδή ο μέγιστος κοινός διαιρέτης των m και n γράφεται ως ακέραιος γραμμικός συνδυασμός των m και n, έχουμε

$$\text{μκδ}(m,n) \in (\langle m\rangle + \langle n\rangle) \Longrightarrow \langle \text{μκδ}(m,n)\rangle \subseteq \langle m\rangle + \langle n\rangle.$$

Και αντιστρόφως· εάν $d := \text{μκδ}(m,n)$ και $a \in \langle m\rangle + \langle n\rangle$, τότε

$$(a = \kappa m + \lambda n, \quad \kappa, \lambda \in \mathbb{Z}) \Longrightarrow a = \left(\frac{\kappa m}{d} + \frac{\lambda n}{d}\right) d,$$

όπου $\frac{\kappa m}{d} + \frac{\lambda n}{d} \in \mathbb{Z}$, οπότε $a \in \langle \text{μκδ}(m,n)\rangle$. Τούτο σημαίνει ότι $\langle m\rangle + \langle n\rangle \subseteq \langle d\rangle$.

(iii) Προφανές επί τη βάσει τού (ii) τής προτάσεως 7.4.3.

(iv) Ας υποθέσουμε ότι $r \in \langle m\rangle : \langle n\rangle$. Τότε -εξ ορισμού- $ra \in \langle m\rangle$ για κάθε στοιχείο $a \in \langle n\rangle$. Ιδιαιτέρως, $rn \in \langle m\rangle \Rightarrow [\exists b \in \mathbb{Z} : rn = bm]$. Εάν $d := \text{μκδ}(m,n)$, τότε $\text{μκδ}(\frac{m}{d}, \frac{n}{d}) = 1$, οπότε

$$r\, \frac{n}{d} = b\, \frac{m}{d} \Longrightarrow \frac{n}{d}\Big|\, b\frac{m}{d} \Longrightarrow \frac{n}{d}\Big|\, b \Longrightarrow b = c\frac{n}{d},$$

για κάποιον $c \in \mathbb{Z}$. Άρα

$$r\, \frac{n}{d} = c\, \frac{n}{d}\, \frac{m}{d} \Longrightarrow r = c\, \frac{m}{d} = c\, \frac{m}{\text{μκδ}(m,n)} \Longrightarrow r \in \left\langle \frac{m}{\text{μκδ}(m,n)} \right\rangle,$$

ήτοι $\langle m\rangle : \langle n\rangle \subseteq \left\langle \frac{m}{\text{μκδ}(m,n)} \right\rangle$. Και αντιστρόφως· εάν $s \in \left\langle \frac{m}{\text{μκδ}(m,n)} \right\rangle$, τότε $s = \kappa \frac{m}{d}$, όπου $\kappa \in \mathbb{Z}$ και $d := \text{μκδ}(m,n)$, οπότε για *κάθε* στοιχείο λn τού $\langle n\rangle$ ($\lambda \in \mathbb{Z}$), έχουμε

$$s\lambda n = \left(\kappa \frac{m}{d}\right) \lambda n = \left(\kappa\lambda \frac{n}{d}\right) m \in \langle m\rangle \Longrightarrow s \in \langle m\rangle : \langle n\rangle,$$

ήτοι $\left\langle \frac{m}{\text{μκδ}(m,n)} \right\rangle \subseteq \langle m\rangle : \langle n\rangle$. □

[10] Για κάθε $n \in \mathbb{Z}$ θέτουμε $\text{sign}(n) := 1$ όταν $n \geqslant 0$ και $\text{sign}(n) := -1$ όταν $n < 0$.

7.4.14 Πρόταση. *Έστω ότι ο R είναι ένας μεταθετικός δακτύλιος και I_1, I_2, I_3 τρία ιδεώδη του. Τότε ισχύουν τα εξής*:

(i) $(I_1 : I_3) + (I_2 : I_3) \subseteq (I_1 + I_2) : I_3$,
(ii) $I_1 : (I_2 + I_3) = (I_1 : I_2) \cap (I_1 : I_3)\,,\ \ (I_1 \cap I_2) : I_3 = (I_1 : I_3) \cap (I_2 : I_3)\,,$
(iii) $(I_1 : I_2)\ I_2 \subseteq I_1,\ \ I_1 \subseteq ((I_1\, I_2) : I_2)\,,$
(iv) $(I_1 : I_2) : I_3 = I_1 : (I_2\, I_3) = (I_1 : I_3) : I_2$.

Απόδειξη. (i) Έστω τυχόν στοιχείο $r \in (I_1 : I_3) + (I_2 : I_3)$. Τότε $r = r_1 + r_2$, όπου $r_1 \in (I_1 : I_3)$ και $r_2 \in (I_2 : I_3)$. Ως εκ τούτου,

$$\left.\begin{matrix} r_1 I_3 \subseteq I_1 \\ r_2 I_3 \subseteq I_2 \end{matrix}\right\} \Rightarrow (r_1 + r_2)\, I_3 \subseteq I_1 + I_2,$$

απ' όπου συνάγεται ότι $r \in (I_1 + I_2) : I_3$, οπότε $(I_1 : I_3) + (I_2 : I_3) \subseteq (I_1 + I_2) : I_3$.
(ii) Έστω τυχόν $r \in I_1 : (I_2 + I_3)$. Τότε $ra \in I_1,\ \forall a \in I_2 + I_3$. Επομένως, λαμβάνοντας υπ' όψιν ότι $I_2 \subseteq I_2 + I_3$ και $I_3 \subseteq I_2 + I_3$, συμπεραίνουμε ότι

$$\left.\begin{matrix} ra \in I_1,\ \ \forall a \in I_2\ \ (\subseteq I_2 + I_3) \\ ra \in I_1,\ \ \forall a \in I_3\ \ (\subseteq I_2 + I_3) \end{matrix}\right\} \Rightarrow \left.\begin{matrix} r \in (I_1 : I_2) \\ r \in (I_1 : I_3) \end{matrix}\right\} \Longrightarrow r \in (I_1 : I_2) \cap (I_1 : I_3)\,.$$

Άρα $I_1 : (I_2 + I_3) \subseteq (I_1 : I_2) \cap (I_1 : I_3)$. Και αντιστρόφως· εάν

$$r \in (I_1 : I_2) \cap (I_1 : I_3) \Longrightarrow rI_2 \subseteq I_1 \ \text{ και } \ rI_3 \subseteq I_1,$$

οπότε $rI_2 + rI_3 = r\,(I_2 + I_3) \subseteq I_1 + I_1 = I_1 \Rightarrow r \in I_1 : (I_2 + I_3)$. Εν συνεχεία, υποθέτουμε ότι $r \in (I_1 \cap I_2) : I_3$, ήτοι ότι ισχύει $rI_3 \subseteq I_1 \cap I_2$. Επειδή $I_1 \cap I_2 \subseteq I_1$ και $I_1 \cap I_2 \subseteq I_2$, έχουμε $rI_3 \subseteq I_1$ και $rI_3 \subseteq I_2$, δηλαδή $r \in (I_1 : I_3) \cap (I_2 : I_3)$. Και αντιστρόφως· εάν $r \in (I_1 : I_3) \cap (I_2 : I_3)$, τότε $rI_3 \subseteq I_1$ και $rI_3 \subseteq I_2$, οπότε $rI_3 \subseteq I_1 \cap I_2 \Rightarrow r \in (I_1 \cap I_2) : I_3$.
(iii) Έστω τυχόν $r \in (I_1 : I_2)\ I_2$. Τότε

$$r = \sum_{j=1}^{k} a_j b_j, \quad \text{όπου } k \in \mathbb{N},\ \ a_j \in (I_1 : I_2)\,,\ \ b_j \in I_2,\ \ \forall j \in \{1, \ldots, k\},$$

οπότε

$$\left[\ \left.\begin{matrix} a_j I_2 \subseteq I_1 \\ b_j \in I_2 \end{matrix}\right\} \Longrightarrow a_j b_j \in I_1,\ \ \forall j \in \{1, \ldots, k\} \Longrightarrow r \in I_1 \right] \Longrightarrow (I_1 : I_2)\ I_2 \subseteq I_1.$$

Εν συνεχεία υποθέτουμε ότι $r \in I_1$. Προφανώς, $ra \in I_1 I_2,\ \forall a \in I_2$. Αυτό σημαίνει αυτομάτως ότι $r \in ((I_1\, I_2) : I_2)$, οπότε ισχύει και η εγκλειστική σχέση $I_1 \subseteq ((I_1\, I_2) : I_2)$.
(iv) Έστω τυχόν $r \in (I_1 : I_2) : I_3$. Τότε $ra \in I_1 : I_2,\ \forall a \in I_3$, οπότε

$$[(ra)\, b = (rb)\, a \in I_1,\ \forall a \in I_3,\ \forall b \in I_2] \Longrightarrow [rb \in I_1 : I_3,\ \forall b \in I_2] \Longrightarrow r \in (I_1 : I_3) : I_2.$$

Άρα $(I_1 : I_2) : I_3 \subseteq (I_1 : I_3) : I_2$. Και αντιστρόφως· εάν $r \in (I_1 : I_3) : I_2$, τότε $ra \in I_1 : I_3$, για κάθε $a \in I_2$, οπότε

$$[(ra)\, b = (rb)\, a \in I_1,\ \forall a \in I_2,\ \forall b \in I_3] \Longrightarrow [rb \in I_1 : I_2,\ \forall b \in I_3] \Longrightarrow r \in (I_1 : I_2) : I_3,$$

απ' όπου έπεται ότι $(I_1 : I_3) : I_2 \subseteq (I_1 : I_2) : I_3$. Άρα $(I_1 : I_2) : I_3 = (I_1 : I_3) : I_2$. Υπολείπεται να δείξουμε την ισότητα $J_1 = J_2$, όπου

$$J_1 := I_1 : (I_2\, I_3)\,, \quad J_2 := (I_1 : I_2) : I_3.$$

Μέσω τού ορισμού τού πηλίκου ιδεωδών και τής μεταθετικότητας τού δακτυλίου αναφοράς μας λαμβάνουμε

$$\left.\begin{array}{r} J_1\,(I_2\,I_3)\subseteq I_1 \\ J_2 I_3\subseteq I_1 : I_2 \end{array}\right\}\Rightarrow\left\{\begin{array}{r} (J_1 I_3)\;I_2\subseteq I_1 \\ (J_2 I_3)\,I_2\subseteq I_1 \end{array}\right\}\Rightarrow\left\{\begin{array}{r} J_1 I_3\subseteq I_1 : I_2 \\ J_2\,(I_2 I_3)\subseteq I_1 \end{array}\right\}\Rightarrow\left\{\begin{array}{r} J_1\subseteq J_2 \\ J_2\subseteq J_1 \end{array}\right\},$$

οπότε όντως $J_1 = J_2$. □

7.5 ΠΡΩΤΑ ΚΑΙ ΜΕΓΙΣΤΙΚΑ ΙΔΕΩΔΗ

7.5.1 Ορισμός. Έστω R ένας δακτύλιος. Ένα ιδεώδες $\mathfrak{p}$ τού R καλείται **πρώτο ιδεώδες** όταν $\mathfrak{p}\subsetneqq R$ και για οιαδήποτε ιδεώδη I, J τού R ισχύει η συνεπαγωγή

$$[IJ\subseteq\mathfrak{p}\Longrightarrow\text{είτε }\ I\subseteq\mathfrak{p}\ \text{ είτε }\ J\subseteq\mathfrak{p}].$$

7.5.2 Πρόταση. *Έστω $\mathfrak{p}\subsetneqq R$ ένα ιδεώδες ενός δακτυλίου R. Εάν για οιοδήποτε ζεύγος $(a,b)\in R\times R$ ισχύει η συνεπαγωγή*

$$[ab\in\mathfrak{p}\Longrightarrow\text{είτε }\ a\in\mathfrak{p}\ \text{ είτε }\ b\in\mathfrak{p}],\tag{7.5}$$

τότε το $\mathfrak{p}$ είναι πρώτο. Και αντιστρόφως· εάν το $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες ενός δακτυλίου R και ο R είναι μεταθετικός, τότε το $\mathfrak{p}$ ικανοποιεί την (7.5).

Απόδειξη. Ας υποθέσουμε εν πρώτοις ότι η συνθήκη (7.5) ικανοποιείται. Εάν τα I, J είναι ιδεώδη τού R με $IJ\subseteq\mathfrak{p}$ και $I\nsubseteq\mathfrak{p}$, τότε υπάρχει κάποιο στοιχείο $a\in I\smallsetminus\mathfrak{p}$. Για κάθε $b\in J$ έχουμε $ab\in IJ\subseteq\mathfrak{p}$, οπότε εξ υποθέσεως είτε $a\in\mathfrak{p}$ είτε $b\in\mathfrak{p}$. Επειδή $a\notin\mathfrak{p}$, αυτό σημαίνει ότι $b\in\mathfrak{p}$ *για κάθε* $b\in J$. Άρα $J\subseteq\mathfrak{p}$ και το $\mathfrak{p}$ είναι πρώτο ιδεώδες τού R. Και αντιστρόφως· εάν το $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες ενός μεταθετικού δακτυλίου R και $ab\in\mathfrak{p}$, τότε το κύριο ιδεώδες $\langle ab\rangle$ περιέχεται στο $\mathfrak{p}$. Λόγω τής μεταθετικότητας τού R (βλ. 7.2.4 (iii)) έχουμε

$$\left.\begin{array}{r}\langle a\rangle\langle b\rangle\subseteq\langle ab\rangle\subseteq\mathfrak{p}\\ \mathfrak{p}\text{ πρώτο ιδεώδες}\end{array}\right\}\Longrightarrow\text{είτε }\ \langle a\rangle\subseteq\mathfrak{p}\ \text{ είτε }\ \langle b\rangle\subseteq\mathfrak{p},$$

οπότε είτε $a\in\mathfrak{p}$ είτε $b\in\mathfrak{p}$ και το $\mathfrak{p}$ ικανοποιεί την (7.5). □

7.5.3 Παραδείγματα. (i) Το τετριμμένο ιδεώδες $\{0_R\}$ οιασδήποτε *ακεραίας περιοχής* R είναι πρώτο, διότι για οιαδήποτε $a, b\in R$ ισχύει η αμφίπλευρη συνεπαγωγή

$$ab=0_R\Longleftrightarrow\ \text{είτε } a=0_R \text{ είτε } b=0_R.$$

(ii) Το ιδεώδες $\langle 10\rangle$ τού δακτυλίου $\mathbb{Z}$ δεν είναι πρώτο, καθότι ισχύει $2\cdot 5\in\langle 10\rangle$ αλλά $2\notin\langle 10\rangle$ και $5\notin\langle 10\rangle$. Το σύνολο των πρώτων ιδεωδών τού $\mathbb{Z}$ προσδιορίζεται πλήρως στην πρόταση 7.5.4.

(iii) Το

$$I:=\left\{\sum_{i=0}^{n}a_i\mathsf{X}^i\in\mathbb{Z}[\mathsf{X}]\;\middle|\;n\in\mathbb{N}_0,\ a_0\equiv 0(\mathrm{mod}\,2)\right\}$$

είναι ένα μη κύριο ιδεώδες τού $\mathbb{Z}[\mathsf{X}]$. (Βλ. άσκηση 4 τού φυλλαδίου 12.) Επομένως, $I\subsetneqq\mathbb{Z}[\mathsf{X}]$. Επιπροσθέτως, το I είναι πρώτο ιδεώδες. Πράγματι· εάν τα

$$\varphi(\mathsf{X})=\sum_{i=0}^{n}a_i\mathsf{X}^i\in\mathbb{Z}[\mathsf{X}]\ ,\ \ \psi(\mathsf{X})=\sum_{j=0}^{m}b_j\mathsf{X}^j\in\mathbb{Z}[\mathsf{X}]$$

είναι πολυώνυμα, τέτοια ώστε $\varphi(\mathsf{X})\psi(\mathsf{X}) \in I$, τότε ο σταθερός όρος a_0b_0 τού $\varphi(\mathsf{X})\psi(\mathsf{X})$ οφείλει να είναι άρτιος ακέραιος αριθμός. Κατ' ανάγκην λοιπόν, είτε $a_0 \equiv 0 (\mathrm{mod}\, 2)$ (δηλαδή $\varphi(\mathsf{X}) \in I$) είτε $b_0 \equiv 0 (\mathrm{mod}\, 2)$ (δηλαδή $\psi(\mathsf{X}) \in I$).

(iv) Η μεταθετικότητα τού δακτυλίου R είναι *αναγκαία* για να ισχύει το αντίστροφο στην πρόταση 7.5.2. Επί παραδείγματι, ο $R = \mathrm{Mat}_{n\times n}(S)$ (όπου S ένας διαιρετικός δακτύλιος), $n \geqslant 2$, είναι μη μεταθετικός, απλός δακτύλιος (βλ. πρόταση 7.3.4), οπότε τα μόνα του ιδεώδη είναι το $\{0_R\}$ και το R. Ως εκ τούτου, εάν τα I, J είναι ιδεώδη τού R με $IJ \subseteq \{0_R\}$, έχουμε κατ' ανάγκην είτε $I = \{0_R\}$ είτε $J = \{0_R\}$. Αυτό σημαίνει ότι το τετριμμένο ιδεώδες $\{0_R\}$ είναι *πρώτο* ιδεώδες τού R. Ωστόσο, επειδή ο R διαθέτει μηδενοδιαιρέτες, η συνθήκη (7.5) *δεν* ικανοποιείται!

7.5.4 Πρόταση (Πρώτα ιδεώδη τού $\mathbb{Z}$.). *Το σύνολο των πρώτων ιδεωδών τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών απαρτίζεται από το τετριμμένο ιδεώδες και τα κύρια ιδεώδη τής μορφής $\langle p\rangle$, όπου p κάποιος πρώτος αριθμός.*

Απόδειξη. Επειδή ο δακτύλιος $\mathbb{Z}$ είναι ακεραία περιοχή, το $\{0\}$ είναι πρώτο ιδεώδες του. Εάν ο p είναι ένας πρώτος αριθμός και οι $a, b \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει $ab \in \langle p\rangle$, τότε

$$p \mid ab \Rightarrow \text{είτε } p \mid a \text{ είτε } p \mid b \Rightarrow \text{είτε } \ a \in \langle p\rangle \ \text{ είτε } \ b \in \langle p\rangle,$$

οπότε το κύριο ιδεώδες $\langle p\rangle$ είναι πρώτο (βλ. πρόταση 7.5.2). Σύμφωνα με την πρόταση 7.2.6 κάθε μη τετριμμένο ιδεώδες τού $\mathbb{Z}$ είναι τής μορφής $\langle n\rangle$ για κάποιον $n \in \mathbb{N}$. Εάν ο n είναι σύνθετος αριθμός, τότε $n = n_1n_2$ για κάποιους φυσικούς αριθμούς n_1, n_2 με $1 < n_1 < n$ και $1 < n_2 < n$. Κατά συνέπειαν, $n = n_1n_2 \in \langle n\rangle$ αλλά $n_1 \notin \langle n\rangle$ και $n_2 \notin \langle n\rangle$ (διότι κανείς εκ των n_1, n_2 δεν μπορεί να ισούται με κάποιο πολλαπλάσιο τού n). Αυτό σημαίνει ότι το ιδεώδες $\langle n\rangle$ δεν είναι πρώτο. □

7.5.5 Παρατήρηση. Ως γνωστόν, η τομή δυο ιδεωδών ενός δακτυλίου αποτελεί ένα ιδεώδες αυτού. (Βλ. πρόταση 7.1.5). Ωστόσο, η τομή δυο πρώτων ιδεωδών δεν είναι κατ' ανάγκην πρώτο ιδεώδες. Επί παραδείγματι, σύμφωνα με την πρόταση 7.5.4 και το (i) τού πορίσματος 7.4.13, τα ιδεώδη $\langle 3\rangle$ και $\langle 5\rangle$ είναι πρώτα ιδεώδη τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών αλλά η τομή τους $\langle 3\rangle \cap \langle 5\rangle = \langle 15\rangle$ δεν είναι πρώτο ιδεώδες.

7.5.6 Ορισμός. Ένα ιδεώδες $\mathfrak{m} \subsetneqq R$ ενός δακτυλίου R καλείται **μεγιστικό** (ή **μεγιστοτικό**) **ιδεώδες** όταν ισχύει η συνεπαγωγή

$$\left[\left\{\begin{array}{c}\mathfrak{m} \subseteq \mathfrak{n} \subseteq R\\ \text{για κάποιο ιδεώδες } \mathfrak{n} \text{ τού } R\end{array}\right\} \Longrightarrow \text{είτε } \mathfrak{n} = \mathfrak{m} \ \text{ είτε } \ \mathfrak{n} = R\right].$$

7.5.7 Παραδείγματα. (i) Το ιδεώδες $\mathfrak{m} := \{(x, 2y) \mid x, y \in \mathbb{Z}\}$ τού δακτυλίου $\mathbb{Z} \times \mathbb{Z}$ είναι μεγιστικό. Πράγματι· εάν το $\mathfrak{n}$ είναι ένα ιδεώδες τού $\mathbb{Z}\times\mathbb{Z}$, για το οποίο ισχύει $\mathfrak{m} \subsetneqq \mathfrak{n} \subseteq \mathbb{Z} \times \mathbb{Z}$, τότε υπάρχει κάποιο στοιχείο τής μορφής $(a, 2b + 1)$ εντός τού $\mathfrak{n}$, όπου a, b κατάλληλοι ακέραιοι αριθμοί. Επομένως,

$$\left.\begin{array}{c}(a, 2b + 1) \in \mathfrak{n}\\ (a, 2b) \in \mathfrak{m} \subsetneqq \mathfrak{n}\end{array}\right\} \Longrightarrow (a, 2b + 1) - (a, 2b) = (0, 1) \in \mathfrak{n},$$

και επειδή $(1, 0) \in \mathfrak{m}$, έχουμε $(0, 1) + (1, 0) = (1, 1) = 1_{\mathbb{Z}\times\mathbb{Z}} \in \mathfrak{n} \Longrightarrow \mathfrak{n} = \mathbb{Z} \times \mathbb{Z}$.

(ii) Το ιδεώδες

$$\mathfrak{m} = \left\{\left.\begin{pmatrix} a & b\\ 0 & 0\end{pmatrix}\right| a, b \in \mathbb{R}\right\} \subsetneqq R = \left\{\left.\begin{pmatrix} a & b\\ c & d\end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{R})\right| c = 0\right\}$$

τού δακτυλίου R είναι μεγιστικό. Πράγματι· εάν το $\mathfrak{n}$ είναι ένα ιδεώδες τού R, για το οποίο ισχύει $\mathfrak{m} \subsetneqq \mathfrak{n} \subseteq R$, τότε υπάρχει κάποιο στοιχείο

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathfrak{n} \setminus \mathfrak{m}, \text{ με } a, b \in \mathbb{R}, \ \ d \in \mathbb{R} \setminus \{0\}.$$

Επομένως,

$$\left.\begin{array}{r} \begin{pmatrix} 0 & 0 \\ 0 & d^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in \mathfrak{n} \\ \\ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in \mathfrak{m} \subsetneqq \mathfrak{n} \end{array}\right\} \Longrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathfrak{n} \Longrightarrow \mathfrak{n} = R.$$

(iii) Εντός τού δακτυλίου $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ των ακεραίων τού Gauss θεωρούμε τα ιδεώδη

$$I_p := \{a + bi \in \mathbb{Z}[i] \ : \ p \mid a \text{ και } \ p \mid b\}\,, \text{ όπου } p \text{ περιττός πρώτος.}$$

Το I_3 είναι μεγιστικό ιδεώδες τού $\mathbb{Z}[i]$. Πράγματι· εάν το J είναι ένα ιδεώδες τού $\mathbb{Z}[i]$, για το οποίο ισχύει $I_3 \subsetneqq J \subseteq \mathbb{Z}[i]$, τότε υπάρχει κάποιο στοιχείο $a + bi \in J \setminus I_3$ με τουλάχιστον ένα εκ των a, b να μην είναι ακέραιο πολλαπλάσιο τού 3. Δίχως βλάβη τής γενικότητας υποθέτουμε ότι $3 \nmid a$ και ισχυριζόμαστε ότι $3 \nmid a^2 + b^2$. Για την απόδειξη αυτού τού ισχυρισμού θα εξετάσουμε χωριστά τις έξι δυνατές περιπτώσεις που προκύπτουν όταν κανείς εργάζεται με τις κλάσεις υπολοίπων των a, b κατά μόδιο 3.

Πρώτη περίπτωση: Εάν $a \equiv 1 (\mathrm{mod}\, 3)$ και $b \equiv 0 (\mathrm{mod}\, 3)$, τότε

$$\left[a^2 \equiv a (\mathrm{mod}\, 3),\ b^2 \equiv 0 (\mathrm{mod}\, 3)\right] \Longrightarrow a^2 + b^2 \equiv a \equiv 1 \not\equiv 0 (\mathrm{mod}\, 3).$$

Δεύτερη περίπτωση: Εάν $a \equiv 1 (\mathrm{mod}\, 3)$ και $b \equiv 1 (\mathrm{mod}\, 3)$, τότε

$$\left[a^2 \equiv a (\mathrm{mod}\, 3),\ b^2 \equiv b (\mathrm{mod}\, 3)\right] \Longrightarrow a^2 + b^2 \equiv a + b \equiv 2 \not\equiv 0 (\mathrm{mod}\, 3).$$

Τρίτη περίπτωση: Εάν $a \equiv 1 (\mathrm{mod}\, 3)$ και $b \equiv 2 (\mathrm{mod}\, 3)$, τότε

$$\left[a^2 \equiv a (\mathrm{mod}\, 3),\ b^2 \equiv 2b (\mathrm{mod}\, 3)\right] \Longrightarrow a^2 + b^2 \equiv a + 2b \equiv 5 \equiv 2 \not\equiv 0 (\mathrm{mod}\, 3).$$

Τέταρτη περίπτωση: Εάν $a \equiv 2 (\mathrm{mod}\, 3)$ και $b \equiv 0 (\mathrm{mod}\, 3)$, τότε

$$\left[a^2 \equiv 2a (\mathrm{mod}\, 3),\ b^2 \equiv 0 (\mathrm{mod}\, 3)\right] \Longrightarrow a^2 + b^2 \equiv 2a \equiv 4 \equiv 1 \not\equiv 0 (\mathrm{mod}\, 3).$$

Πέμπτη περίπτωση: Εάν $a \equiv 2 (\mathrm{mod}\, 3)$ και $b \equiv 1 (\mathrm{mod}\, 3)$, τότε

$$\left[a^2 \equiv 2a (\mathrm{mod}\, 3),\ b^2 \equiv b (\mathrm{mod}\, 3)\right] \Longrightarrow a^2 + b^2 \equiv 2a + b \equiv 5 \equiv 2 \not\equiv 0 (\mathrm{mod}\, 3).$$

Έκτη περίπτωση: Εάν $a \equiv 2 (\mathrm{mod}\, 3)$ και $b \equiv 2 (\mathrm{mod}\, 3)$, τότε

$$\left[a^2 \equiv 2a (\mathrm{mod}\, 3),\ b^2 \equiv 2b (\mathrm{mod}\, 3)\right] \Longrightarrow a^2 + b^2 \equiv 2a + 2b \equiv 8 \equiv 2 \not\equiv 0 (\mathrm{mod}\, 3).$$

Επειδή λοιπόν $3 \nmid a^2 + b^2 \Longrightarrow \text{μκδ}\left(3, a^2 + b^2\right) = 1$, υπάρχουν δύο ακέραιοι αριθμοί k, l, τέτοιοι ώστε να ισχύει η ισότητα $k\left(a^2 + b^2\right) + 3l = 1$. Ως εκ τούτου,

$$a + bi \in J,\ a - bi \in \mathbb{Z}[i] \Longrightarrow (a + bi)\,(a - bi) = a^2 + b^2 \in J$$

και

$$\left.\begin{array}{r} k \in \mathbb{Z} \subsetneqq \mathbb{Z}[i] \Rightarrow k\left(a^2 + b^2\right) \in J \\ l \in \mathbb{Z} \subsetneqq \mathbb{Z}[i] \Rightarrow 3l \in I_3 \subsetneqq J \end{array}\right\} \Longrightarrow k\left(a^2 + b^2\right) + 3l = 1 \in J,$$

απ' όπου έπεται ότι $J = \mathbb{Z}[i]$ και ότι το I_3 είναι ένα μεγιστικό ιδεώδες τού $\mathbb{Z}[i]$. Ωστόσο, αξιοσημείωτο είναι το ότι το I_5 δεν είναι μεγιστικό! Πράγματι· το κύριο ιδεώδες $I'_5 = \langle 2+i\rangle$ τού $\mathbb{Z}[i]$ περιέχει *γνησίως* το I_5, αφού για κάθε $a+ib \in I_5$ έχουμε

$$a+ib = (2+i)\left(\tfrac{2a+b}{5} + \left(\tfrac{2b-a}{5}\right)i\right), \text{ όπου } \tfrac{2a+b}{5}, \tfrac{2b-a}{5} \in \mathbb{Z},$$

και $2+i \in I'_5 \smallsetminus I_5$. Θα δείξουμε ότι $I'_5 \subsetneqq \mathbb{Z}[i]$ ή, ισοδυνάμως, ότι $1 \notin I'_5$. Εάν το 1 ανήκε στο I'_5, τότε θα έπρεπε να υπάρχουν $c, d \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει η ισότητα

$$1 = (2+i)(c+di) \iff \left.\begin{array}{l} 2c-d=1 \\ c+2d=0 \end{array}\right\} \Longrightarrow c = \tfrac{2}{5},\ d = -\tfrac{1}{5},$$

από την οποία θα καταλήγαμε σε άτοπο, αφού θα είχαμε $c, d \in \mathbb{Q}\smallsetminus\mathbb{Z}$.

(iv) Το κύριο ιδεώδες $\langle \mathsf{X}\rangle$ τού $\mathbb{Z}[\mathsf{X}]$ δεν είναι μεγιστικό, αφού $\langle \mathsf{X}\rangle \subsetneqq I \subsetneqq \mathbb{Z}[\mathsf{X}]$, όπου I το ιδεώδες το ορισθέν στο εδάφιο 7.5.3 (iii).

7.5.8 Πρόταση. *Ένα γνήσιο ιδεώδες $\mathfrak{m} \subsetneqq R$ ενός δακτυλίου R είναι μεγιστικό εάν και μόνον εάν $\mathfrak{m} + \langle a\rangle = R,\ \forall a \in R\smallsetminus\mathfrak{m}$.*

Απόδειξη. Έστω $\mathfrak{m} \subsetneqq R$ ένα μεγιστικό ιδεώδες ενός δακτυλίου R. Τότε για κάθε $a \in R\smallsetminus\mathfrak{m}$ έχουμε

$$\mathfrak{m} \subsetneqq \mathfrak{m} + \langle a\rangle \subseteq R \Longrightarrow \mathfrak{m} + \langle a\rangle = R.$$

Και αντιστρόφως· εάν το $\mathfrak{m} \subsetneqq R$ είναι ένα γνήσιο ιδεώδες ενός δακτυλίου R και $\mathfrak{m} + \langle a\rangle = R$ για κάθε $a \in R\smallsetminus\mathfrak{m}$, τότε για οιοδήποτε ιδεώδες $\mathfrak{n}$ τού R, για το οποίο ισχύουν οι εγκλεισμοί $\mathfrak{m} \subsetneqq \mathfrak{n} \subseteq R$, θα υπάρχει κάποιο $b \in \mathfrak{n}\smallsetminus\mathfrak{m}$. Ως εκ τούτου,

$$\left.\begin{array}{r} \mathfrak{m} \subsetneqq \mathfrak{m} + \langle b\rangle \subseteq \mathfrak{n} \\ b \in \mathfrak{n}\smallsetminus\mathfrak{m} \subseteq R\smallsetminus\mathfrak{m} \Longrightarrow \mathfrak{m} + \langle b\rangle = R \end{array}\right\} \Longrightarrow R \subseteq \mathfrak{n} \Longrightarrow \mathfrak{n} = R.$$

Άρα το $\mathfrak{m}$ είναι μεγιστικό ιδεώδες τού R. □

7.5.9 Παράδειγμα. Έστω $R = 2\mathbb{Z}$ ο δακτύλιος των αρτίων ακεραίων. Θεωρούμε το ιδεώδες $\mathfrak{m} = \langle 4\rangle$. Σύμφωνα με το (iii) τού πορίσματος 7.2.4, αυτό το κύριο ιδεώδες μπορεί να περιγραφεί ως ακολούθως:

$$\mathfrak{m} = \langle 4\rangle = \{\, 4r + 4n \mid r \in 2\mathbb{Z},\ n \in \mathbb{Z}\} \ (= 4\mathbb{Z}).$$

Έστω a τυχόν στοιχείο τού $2\mathbb{Z}\smallsetminus\mathfrak{m}$. Το a οφείλει να είναι κάποιος άρτιος ακέραιος μη διαιρούμενος διά τού 4. Κατά συνέπειαν, θα είναι τής μορφής $a = 4\lambda + 2$, για κάποιον $\lambda \in \mathbb{Z}$. Επειδή

$$2 = 4(-\lambda) + a \in \mathfrak{m} + \langle a\rangle \Longrightarrow \langle 2\rangle \subseteq \mathfrak{m} + \langle a\rangle$$

και $\langle 2\rangle = \{\, 2r + 2n \mid r \in 2\mathbb{Z},\ n \in \mathbb{Z}\}$ $(= 2\mathbb{Z})$, έχουμε $\mathfrak{m} + \langle a\rangle = 2\mathbb{Z}$, οπότε δυνάμει τής προτάσεως 7.5.8 το $\mathfrak{m} = \langle 4\rangle$ είναι μεγιστικό ιδεώδες τού δακτυλίου $2\mathbb{Z}$.

▸ **Ύπαρξη μεγιστικών ιδεωδών.** Ο ορισμός 7.5.6 των μεγιστικών ιδεωδών είναι *αμιγώς συνολοθεωρητικός*. Μάλιστα, σύμφωνα με το κάτωθι θεώρημα 7.5.13, η *ύπαρξη* μεγιστικών ιδεωδών σε *δακτυλίους με μοναδιαίο στοιχείο* εξασφαλίζεται μέσω τού λεγομένου *λήμματος τού Zorn* 1.4.18.

7.5.10 Λήμμα τού Zorn. *Εάν το $(A, \preceq)$ είναι ένα επαγωγικώς διατεταγμένο σύνολο, τότε για οιοδήποτε $a \in A$ υπάρχει τουλάχιστον ένα μεγιστικό στοιχείο m εντός τού A, για το οποίο ισχύει $a \preceq m$.*

Στο πλαίσιο τής Θεωρίας Συνόλων αποδεικνύεται (με τη βοήθεια τής λεγομένης *υπερπεπερασμένης επαγωγής*) το εξής:

7.5.11 Θεώρημα. *Το λήμμα τού Zorn είναι ισοδύναμο τού αξιώματος τής επιλογής* 1.11.4.

7.5.12 Παρατήρηση. (i) Έστω R ένας δακτύλιος και έστω

$$\mathcal{S}_R := \{\text{ιδεώδη } I \text{ τού } R \mid I \subsetneqq R\}.$$

Το $\mathcal{S}_R$ είναι μερικώς διατεταγμένο σύνολο ως προς τη σχέση εγκλεισμού "$\subseteq$" (βλ. 1.4.2 (iv)), οπότε ένα ιδεώδες $\mathfrak{m} \subsetneqq R$ τού R είναι μεγιστικό εάν και μόνον εάν είναι *μεγιστικό στοιχείο* τού $(\mathcal{S}_R, \subseteq)$ υπό την έννοια τού ορισμού 1.4.9.

(ii) Στον ορισμό 7.5.6 υποθέσαμε ότι το $\mathfrak{m}$ είναι αμφίπλευρο ιδεώδες. Ωστόσο, κατά τον ίδιο τρόπο μπορεί κανείς να ορίσει και *αριστερά*/*δεξιά* (όχι κατ' ανάγκην αμφίπλευρα) *μεγιστικά ιδεώδη* (εάν, βεβαίως, υποθέσει ότι η απαιτούμενη συνεπαγωγή ισχύει για κάθε *αριστερό*/*δεξιό* ιδεώδες $\mathfrak{n}$ τού R).

7.5.13 Θεώρημα. *Κάθε μη τετριμμένος δακτύλιος R με μοναδιαίο στοιχείο διαθέτει πάντοτε μεγιστικά ιδεώδη. Μάλιστα, ισχύει κάτι ακόμη πιο ισχυρό: Κάθε γνήσιο ιδεώδες τού R περιέχεται σε κάποιο μεγιστικό ιδεώδες τού R.*

Απόδειξη. Έστω $I \subsetneqq R$ ένα ιδεώδες τού R και έστω[11]

$$\mathcal{S}_R(I) := \{\text{ιδεώδη } J \text{ τού } R \mid I \subseteq J \subsetneqq R\}.$$

Το $\mathcal{S}_R(I)$ είναι $\neq \varnothing$ (αφού $I \in \mathcal{S}_R(I)$) και μερικώς διατεταγμένο σύνολο ως προς τη σχέση εγκλεισμού "$\subseteq$" (βλ. 1.4.2 (iv)). Θα αποδείξουμε ότι το $(\mathcal{S}_R(I), \subseteq)$ είναι και *επαγωγικώς διατεταγμένο* (βλ. 1.4.16). Προς τούτο θεωρούμε τυχόν ολικώς διατεταγμένο υποσύνολο $B \neq \varnothing$ τού $\mathcal{S}_R(I)$ και ορίζουμε το σύνολο

$$s(B) := \bigcup \{J \in \mathcal{S}_R(I) \mid J \in B\}.$$

Προφανώς, $J \subseteq s(B)$ για κάθε $J \in B$. Θα αποδείξουμε ότι $s(B) \in \mathcal{S}_R(I)$ (ήτοι ότι το $s(B)$ είναι *ιδεώδες* τού R με $I \subseteq s(B) \subsetneqq R$). Παρατηρούμε, κατ' αρχάς, ότι $I \subseteq s(B)$ (εξ ορισμού). Εξάλλου, εάν $x, y \in s(B)$, το x ανήκει σε κάποιο $J_x \in B$ και το y σε κάποιο $J_y \in B$. Λόγω τής ολικής διατάξεως τού B ως προς τη σχέση εγκλεισμού "$\subseteq$", είτε $J_x \subseteq J_y$ είτε $J_y \subseteq J_x$. Εάν $J_x \subseteq J_y$, τότε αμφότερα τα x, y ανήκουν στο J_y, και επειδή το J_y είναι ιδεώδες τού R έχουμε

$$\left.\begin{array}{r} x - y \in J_y \subseteq s(B) \\ rx, xr, ry, yr \in J_y \subseteq s(B), \forall r \in R \end{array}\right\} \Longrightarrow s(B) \text{ ιδεώδες τού } R.$$

Με τον ίδιο τρόπο αποδεικνύουμε ότι το $s(B)$ είναι ιδεώδες τού R ακόμη και όταν $J_y \subseteq J_x$. Επιπροσθέτως,

$$[J \subsetneqq R,\ \forall J \in B] \Longrightarrow [1_R \notin J,\ \forall J \in B] \Longrightarrow 1_R \notin s(B) \Longrightarrow s(B) \subsetneqq R.$$

Συνεπώς,

$$\left.\begin{array}{r} J \subseteq s(B),\ \forall J \in B \\ s(B) \text{ ιδεώδες τού } R \\ \text{που ανήκει στο } \mathcal{S}_R(I) \end{array}\right\} \Longrightarrow \text{το } s(B) \text{ είναι } \textit{άνω φράγμα} \text{ τού } B$$

(βλ. 1.4.14 (i)). Άρα το $(\mathcal{S}_R(I), \subseteq)$ είναι όντως επαγωγικώς διατεταγμένο. Δυνάμει τού λήμματος 1.4.18 τού Zorn υπάρχει (τουλάχιστον ένα) μεγιστικό στοιχείο $\mathfrak{m}$ εντός τού $\mathcal{S}_R(I)$ με $I \subseteq \mathfrak{m}$. Το $\mathfrak{m}$ πληροί προφανώς τις επιθυμητές συνθήκες. □

[11] Για $I = \{0_R\}$ έχουμε $\mathcal{S}_R(\{0_R\}) = \mathcal{S}_R$, όπου $\mathcal{S}_R$ το σύνολο που ορίσαμε στο 7.5.12 (i).

7.5.14 Παρατήρηση. (i) Το θεώρημα 7.5.13 παραμένει εν ισχύ ακόμη και εάν κανείς αντικαταστήσει τα (αμφίπλευρα) μεγιστικά ιδεώδη (τής διατυπώσεως και τής αποδείξεώς του) με αριστερά μεγιστικά ιδεώδη (και αντιστοίχως, με δεξιά μεγιστικά ιδεώδη) χρησιμοποιώντας τά προαναφερθέντα στο εδάφιο 7.5.12 (ii).

(ii) Το θεώρημα 7.5.13 δεν μπορεί να γενικευθεί για τυχόντες *δακτυλίους χωρίς μοναδιαίο στοιχείο*. Το απλούστερο αντιπαράδειγμα είναι το εξής: Θεωρούμε την προσθετική ομάδα $(\mathbb{Q},+)$ των ρητών αριθμών και εφοδιάζουμε το $\mathbb{Q}$ με τον *τετριμμένο πολλαπλασιασμό* "$\star$":

$$\mathbb{Q}\times\mathbb{Q}\ni(a,b)\longmapsto a\star b:=0\in\mathbb{Q}.$$

Είναι άμεσος ο έλεγχος τού ότι η τριάδα $(\mathbb{Q},+,\star)$ αποτελεί έναν δακτύλιο. Επιπροσθέτως, κάθε υποομάδα τής $(\mathbb{Q},+)$ αποτελεί ένα ιδεώδες τού $(\mathbb{Q},+,\star)$ και τανάπαλιν. Αρκεί λοιπόν να αποδειχθεί ότι η $(\mathbb{Q},+)$ *στερείται μεγιστικών υποομάδων*[12] (αφού οιοδήποτε μεγιστικό ιδεώδες τού $(\mathbb{Q},+,\star)$ θα όφειλε να είναι μεγιστική υποομάδα τής $(\mathbb{Q},+)$). Ας υποθέσουμε ότι η $(\mathbb{Q},+)$ διαθέτει κάποια μεγιστική υποομάδα $H\subsetneqq\mathbb{Q}$ και ότι $\frac{r}{s}\in\mathbb{Q}\smallsetminus H$, για κάποιους $r,s\in\mathbb{Z}\smallsetminus\{0\}$. Τότε

$$H\subsetneqq H+\left\langle\frac{r}{s}\right\rangle\subseteq\mathbb{Q}\Rightarrow H+\left\langle\frac{r}{s}\right\rangle=\mathbb{Q},\tag{7.6}$$

όπου $\left\langle\frac{r}{s}\right\rangle$ η υποομάδα η παραγόμενη από το $\frac{r}{s}$. Επιπροσθέτως, $H\neq\{0\}$ (διότι π.χ. $\{0\}\subsetneqq\mathbb{Z}\subsetneqq\mathbb{Q}$). Κατά συνέπειαν, υπάρχουν $a,b\in\mathbb{Z}\smallsetminus\{0\}:\frac{a}{b}\in H$ με $b(\frac{a}{b})=a\in H$. Επειδή $\frac{r}{s}\cdot\frac{1}{as}\in\mathbb{Q}$, η (7.6) διασφαλίζει την ύπαρξη κάποιου $h\in H$ και κάποιου $t\in\mathbb{Z}$, ούτως ώστε να ισχύει η ισότητα

$$\frac{r}{s}\cdot\frac{1}{as}=h+t\left(\frac{r}{s}\right)\Rightarrow\frac{r}{s}=(as)h+(tr)a.$$

Επειδή

$$\left.\begin{array}{r}as\in\mathbb{Z},\ h\in H\Rightarrow(as)h\in H\\ tr\in\mathbb{Z},\ a\in H\Rightarrow(tr)a\in H\end{array}\right\}\Longrightarrow(as)h+(tr)a\in H$$

καταλήγουμε στο ότι $\frac{r}{s}\in H$, ήτοι σε κάτι που αντιφάσκει προς την υπόθεσή μας.

▸ **Συσχετισμός πρώτων και μεγιστικών ιδεωδών**. Στα εδάφια 7.5.15, 7.5.16 και 7.5.17 διασαφηνίζεται ο τρόπος συσχετισμού των εννοιών *πρώτο* και *μεγιστικό ιδεώδες* ενός *μεταθετικού* δακτυλίου.

7.5.15 Θεώρημα. *Εάν ο R είναι ένας μεταθετικός δακτύλιος, για τον οποίο ισχύει $RR=R$ (όπως, π.χ., στην περίπτωση κατά την οποία ο R διαθέτει μοναδιαίο στοιχείο), τότε κάθε μεγιστικό ιδεώδες $\mathfrak{m}$ τού R είναι πρώτο.*

Απόδειξη. Έστω $\mathfrak{m}$ ένα μεγιστικό ιδεώδες τού R. Υποθέτοντας ότι υπάρχουν στοιχεία $a,b\in R$, για τα οποία ισχύει $ab\in\mathfrak{m}$, όπου $a\notin\mathfrak{m}$ και $b\notin\mathfrak{m}$, έχουμε

$$\left.\begin{array}{l}\mathfrak{m}\subsetneqq\mathfrak{m}+\langle a\rangle\\ \mathfrak{m}\subsetneqq\mathfrak{m}+\langle b\rangle\end{array}\right\}\Longrightarrow R=\mathfrak{m}+\langle a\rangle=\mathfrak{m}+\langle b\rangle$$

(λόγω τής «μεγιστικότητας» τού $\mathfrak{m}$). Εξάλλου, επειδή ο R είναι μεταθετικός και $ab\in\mathfrak{m}$, συμπεραίνουμε ότι $\langle a\rangle\langle b\rangle\underset{\text{7.2.4 (iii)}}{\subseteq}\langle ab\rangle\subseteq\mathfrak{m}\subsetneqq R$. Όμως, επειδή $R=RR$, κατόπιν εφαρμογής τού (ii) τής προτάσεως 7.4.5 λαμβάνουμε

$$R=RR=(\mathfrak{m}+\langle a\rangle)(\mathfrak{m}+\langle b\rangle)\subseteq\mathfrak{m}+\underbrace{\langle a\rangle\langle b\rangle}_{\subseteq\langle ab\rangle\subseteq\mathfrak{m}}\subseteq\mathfrak{m},$$

[12] Έστω $(G,+)$ μια ομάδα. Μια υποομάδα της H καλείται **μεγιστική υποομάδα** όταν δεν υφίστανται υποομάδες K τής $(G,+)$ με $H\subsetneqq K\subsetneqq G$.

ήτοι κάτι το άτοπο, καθόσον $\mathfrak{m} \subsetneqq R$. Κατά συνέπειαν, είτε $a \in \mathfrak{m}$ είτε $b \in \mathfrak{m}$, οπότε το $\mathfrak{m}$ είναι πρώτο ιδεώδες τού R. (Βλ. πρόταση 7.5.2). □

7.5.16 Παραδείγματα. Υπάρχουν, βεβαίως, πρώτα ιδεώδη, τα οποία δεν είναι μεγιστικά. Δύο στοιχειώδη παραδείγματα είναι τα εξής:

(i) Στον δακτύλιο $\mathbb{Z}$ των ακεραίων το τετριμμένο ιδεώδες $\{0\}$ είναι πρώτο, αλλά *δεν είναι* μεγιστικό, διότι $\{0\} \subsetneqq n\mathbb{Z} \subsetneqq \mathbb{Z}$, $\forall n \in \mathbb{Z} \setminus \{0, 1\}$. Ωστόσο, όπως θα δούμε στην πρόταση 7.5.18, τα λοιπά πρώτα ιδεώδη τού $\mathbb{Z}$ *είναι* μεγιστικά.

(ii) Επειδή ο $\mathbb{Z}$ δεν έχει μηδενοδιαιρέτες, το ιδεώδες $I = \mathbb{Z} \times \{0\} = \{\, (k, 0) \mid k \in \mathbb{Z}\}$ τού $\mathbb{Z} \times \mathbb{Z}$ είναι προφανώς πρώτο. Ωστόσο, δεν είναι και μεγιστικό, διότι

$$I \subsetneqq \mathbb{Z} \times 2\mathbb{Z} \subsetneqq \mathbb{Z} \times \mathbb{Z}.$$

7.5.17 Σημείωση. Η συνθήκη $RR = R$ είναι *αναγκαία* για να ισχύει το θεώρημα 7.5.15. Εάν, επί παραδείγματι, θεωρήσουμε το ιδεώδες $\mathfrak{m} = \langle 4 \rangle$ τού δακτυλίου $2\mathbb{Z}$ των αρτίων ακεραίων, τότε το $\mathfrak{m}$ είναι μεγιστικό (βλ. εδάφιο 7.5.9) αλλά *δεν είναι πρώτο*, καθόσον έχουμε $2 \cdot 6 \in \mathfrak{m}$, παρότι $2 \notin \mathfrak{m}$ και $6 \notin \mathfrak{m}$.

7.5.18 Πρόταση (Μεγιστικά ιδεώδη τού $\mathbb{Z}$.). *Το σύνολο των μεγιστικών ιδεωδών τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών απαρτίζεται από τα κύρια ιδεώδη τής μορφής $\langle p \rangle$, όπου p κάποιος πρώτος αριθμός.*

Απόδειξη. Σύμφωνα με τα προαναφερθέντα στα εδάφια 7.5.4, 7.5.15 και 7.5.16 (i), το σύνολο των μεγιστικών ιδεωδών τού δακτυλίου $\mathbb{Z}$ περιέχεται στο σύνολο των κυρίων ιδεωδών τής μορφής $\langle p \rangle$, όπου p κάποιος πρώτος αριθμός. Αρκεί λοιπόν να δειχθεί ο αντίστροφος εγκλεισμός. Προς τούτο θεωρούμε το ιδεώδες $\langle p \rangle$, όπου p *τυχόν* πρώτος αριθμός, και υποθέτουμε ότι το $\mathfrak{n}$ είναι ένα ιδεώδες τού $\mathbb{Z}$, για το οποίο ισχύει $\langle p \rangle \subsetneqq \mathfrak{n} \subseteq \mathbb{Z}$. Κατά την πρόταση 7.2.6, $\mathfrak{n} = \langle n \rangle$, όπου n κατάλληλος φυσικός αριθμός. Προφανώς,

$$p \in \mathfrak{n} = \langle n \rangle \Rightarrow \exists k \in \mathbb{N} : p = kn \Rightarrow \text{είτε } [k = p,\ n = 1] \text{ είτε } [k = 1,\ n = p].$$

Το δεύτερο ενδεχόμενο αποκλείεται, καθόσον $\langle p \rangle \subsetneqq \mathfrak{n}$. Άρα $n = 1$, απ' όπου έπεται ότι $\mathfrak{n} = \langle 1 \rangle = \mathbb{Z}$. Αυτό σημαίνει ότι το κύριο ιδεώδες $\langle p \rangle$ είναι μεγιστικό. □

7.6 ΠΗΛΙΚΟΔΑΚΤΥΛΙΟΙ

Έστω $(R, +, \cdot)$ ένας δακτύλιος και έστω I ένα ιδεώδες του. Επειδή η προσθετική ομάδα $(R, +)$ είναι αβελιανή, το ζεύγος $\big(I, +|_{I \times I}\big)$ αποτελεί μια ορθόθετη προσθετική υποομάδα της. Επομένως υπάρχει μια καλώς ορισμένη ομάδα πηλίκων R/I με πρόσθεση[13]:

$$(a + I) + (b + I) := (a + b) + I\ ,\quad \text{για οιαδήποτε}\quad a, b \in R. \tag{7.7}$$

Το *ουδέτερο* στοιχείο $0_{R/I}$ τής $(R/I, +)$ είναι προφανώς το $0_R + I = I$. Εξάλλου, για οιαδήποτε $a, b \in R$ έχουμε $a + I = b + I \iff a - b \in I$.

7.6.1 Πρόταση. *Έστω R ένας δακτύλιος και έστω I ένα ιδεώδες αυτού. Τότε η προσθετική ομάδα πηλίκων R/I μπορεί να εφοδιασθεί με τη δομή ενός δακτυλίου όταν για οιαδήποτε $a, b \in R$ ορίσουμε τον «πολλαπλασιασμό»:*

$$(a + I)\ (b + I) := (ab) + I\ . \tag{7.8}$$

[13] $a + I := \{\, a + r \mid r \in I\}\ ,\ \forall a \in R.$

Απόδειξη. Η πράξη τού «πολλαπλασιασμού» (7.8) είναι καλώς ορισμένη. Πράγματι· εάν υποθέσουμε ότι $a+I=a'+I$, $b+I=b'+I$, για κάποια $a,a',b,b'\in R$, τότε $a'=a+r$ και $b'=b+s$, για κάποια $r,s\in I$. Επομένως,

$$a'b'=(a+r)(b+s)=ab+as+rb+rs\Longrightarrow a'b'-ab=as+rb+rs\in I,$$

απ' όπου συνάγεται ότι $ab+I=a'b'+I$. Επιπροσθέτως, η εν λόγω πράξη (7.8) είναι *προσεταιριστική*, διότι

$$\begin{aligned}&((a+I)\ (b+I))\,(c+I)=((ab)+I)\,(c+I)=(ab)\,c+I\\&=a\,(bc)+I=(a+I)\,((bc)+I)=(a+I)\ ((b+I)\,(c+I))\,,\end{aligned}$$

και τόσον *εξ αριστερών* όσον και *εκ δεξιών επιμεριστική* ως προς την πρόσθεση (7.7), διότι

$$\begin{aligned}&(a+I)\ ((b+I)+(c+I))=(a+I)\,(\,(b+c)+I)\\&=a(b+c)+I=(ab+ac)+I=(ab+I)+(ac+I)\\&=((a+I)\ (b+I))+((a+I)\ (c+I))\end{aligned}$$

και

$$\begin{aligned}&((a+I)\ +(b+I))\,(c+I)=(\,(a+b)+I)\,(c+I)\\&=(a+b)c+I=(ac+bc)+I=((ac)+I)+((bc)+I)\\&=((a+I)\ (c+I))+((b+I)\ (c+I))\,,\end{aligned}$$

για οιαδήποτε $a,b,c\in R$. □

7.6.2 Ορισμός. Ο δακτύλιος R/I ονομάζεται **πηλικοδακτύλιος** (ή **δακτύλιος κλάσεων υπολοίπων**) τού R ως προς το I.

7.6.3 Πρόταση. *Έστω I ένα ιδεώδες ενός δακτυλίου R. Τότε ισχύουν τα εξής:*

(i) *Εάν ο R είναι μεταθετικός, τότε και ο R/I είναι μεταθετικός.*

(ii) *Εάν ο R έχει μοναδιαίο στοιχείο, τότε και ο R/I έχει μοναδιαίο στοιχείο, και μάλιστα $1_{R/I}=1_R+I$.*

(iii) *Εάν ο R έχει μοναδιαίο στοιχείο και $a\in R^\times$, τότε $a+I\in(R/I)^\times$, και μάλιστα $(a+I)^{-1}=a^{-1}+I$.*

(iv) *Εάν $a\in R$, τότε $a+I\in\mathrm{Nil}(R/I)\Longleftrightarrow\exists n\in\mathbb{N}:a^n\in I$.*

(v) *Εάν $a\in R$, τότε το $a+I$ είναι ταυτοδύναμο στοιχείο τού πηλικοδακτυλίου $R/I\Longleftrightarrow a^2-a\in I$.*

Απόδειξη. (i) Εάν ο R είναι μεταθετικός, τότε για οιαδήποτε $a,b\in R$ έχουμε

$$(a+I)(b+I)=(ab)+I=(ba)+I=(b+I)(a+I).$$

(ii) Εάν ο R έχει μοναδιαίο στοιχείο, τότε για κάθε $a\in R$ έχουμε

$$(a+I)(1_R+I)=(a\cdot1_R)+I=a+I=(1_R\cdot a)+I=(1_R+I)(a+I).$$

(iii) Εάν ο R έχει μοναδιαίο στοιχείο και $a\in R^\times$, τότε $1_{R/I}=1_R+I$ και υπάρχει το αντίστροφό a^{-1} τού a, οπότε

$$(a+I)(a^{-1}+I)=(a\cdot a^{-1})+I=1_R+I=(a^{-1}\cdot a)+I=(a^{-1}+I)(a+I).$$

(iv) Εάν $a\in R$, τότε

$$\begin{aligned}a+I\in\mathrm{Nil}(R/I)&\Longleftrightarrow\exists n\in\mathbb{N}:(a+I)^n=0_{R/I}=I\\&\Longleftrightarrow\exists n\in\mathbb{N}:a^n+I=I\Longleftrightarrow\exists n\in\mathbb{N}:a^n\in I.\end{aligned}$$

(v) Έστω $a \in R$. Το $a+I$ είναι ταυτοδύναμο στοιχείο τού πηλικοδακτυλίου R/I εάν και μόνον εάν

$$(a+I)^2 + ((-a)+I) = 0_{R/I} = I \iff \left(a^2+I\right) + ((-a)+I) = I$$
$$\iff \left(a^2-a\right) + I = I \iff a^2 - a \in I,$$

οπότε και αυτή η αμφίπλευρη συνεπαγωγή είναι αληθής. □

7.6.4 Θεώρημα. *Εάν ο R είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και το $\mathfrak{p}$ ένα ιδεώδες τού R, τότε τα ακόλουθα είναι ισοδύναμα*:

(i) $\mathfrak{p} \subsetneqq R$ *και το* $\mathfrak{p}$ *είναι πρώτο ιδεώδες τού* R.

(ii) *Ο πηλικοδακτύλιος* $R/\mathfrak{p}$ *είναι ακεραία περιοχή.*

Απόδειξη. Ο πηλικοδακτύλιος $R/\mathfrak{p}$ είναι μεταθετικός με το $0_R+\mathfrak{p}$ ως μηδενικό και το $1_R+\mathfrak{p}$ ως μοναδιαίο του στοιχείο.

(i)⇒(ii): Εάν το $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες τού R, τότε $1_R+\mathfrak{p} \neq \mathfrak{p}$ αφού $\mathfrak{p} \subsetneqq R$. Για οιαδήποτε $a, b \in R$, για τα οποία ισχύει η ισότητα $(a+\mathfrak{p})(b+\mathfrak{p}) = \mathfrak{p}$, έχουμε

$$ab+\mathfrak{p} = \mathfrak{p} \Rightarrow ab \in \mathfrak{p} \Longrightarrow [\text{είτε } a \in \mathfrak{p} \text{ είτε } b \in \mathfrak{p}] \Rightarrow [\text{είτε } a+\mathfrak{p} = \mathfrak{p} \text{ είτε } b+\mathfrak{p} = \mathfrak{p}]\,.$$

Άρα ο πηλικοδακτύλιος $R/\mathfrak{p}$ είναι μια ακεραία περιοχή.

(ii)⇒(i): Εάν ο $R/\mathfrak{p}$ είναι ακεραία περιοχή, τότε $1_R+\mathfrak{p} \neq 0_R+\mathfrak{p}$, απ' όπου έπεται ότι $1_R \notin \mathfrak{p} \Longrightarrow \mathfrak{p} \subsetneqq R$. Εάν τώρα $a, b \in R$ και $ab \in \mathfrak{p}$, έχουμε

$$ab+\mathfrak{p} = \mathfrak{p} \Longrightarrow (a+\mathfrak{p})(b+\mathfrak{p}) = \mathfrak{p}.$$

Επειδή ο πηλικοδακτύλιος $R/\mathfrak{p}$ δεν διαθέτει μηδενοδιαιρέτες, από την τελευταία αυτή ισότητα συνάγεται ότι

$$[\text{είτε } \ a+\mathfrak{p} = \mathfrak{p} \ \text{ είτε } \ b+\mathfrak{p} = \mathfrak{p}] \Longrightarrow [\text{είτε } \ a \in \mathfrak{p} \ \text{ είτε } \ b \in \mathfrak{p}]\,,$$

πράγμα που σημαίνει ότι το $\mathfrak{p}$ είναι πρώτο ιδεώδες τού δακτυλίου R βάσει τής προτάσεως 7.5.2. □

7.6.5 Πόρισμα. *Έστω $\mathfrak{m}$ ένα ιδεώδες ενός μη τετριμμένου δακτυλίου R με μοναδιαίο στοιχείο. Τότε ισχύουν τα ακόλουθα*:

(i) *Εάν το $\mathfrak{m}$ είναι μεγιστικό και ο R μεταθετικός, τότε ο πηλικοδακτύλιος $R/\mathfrak{m}$ είναι σώμα.*

(ii) *Εάν ο πηλικοδακτύλιος $R/\mathfrak{m}$ είναι διαιρετικός δακτύλιος (= στρεβλό σώμα), τότε το $\mathfrak{m}$ είναι μεγιστικό ιδεώδες.*

Απόδειξη. (i) Σύμφωνα με το θεώρημα 7.5.15, το $\mathfrak{m}$, όντας εξ υποθέσεως μεγιστικό, θα είναι και πρώτο ιδεώδες τού δακτυλίου R. Συνεπώς, βάσει τού θεωρήματος 7.6.4, ο πηλικοδακτύλιος $R/\mathfrak{m}$ είναι μια ακεραία περιοχή. Αρκεί λοιπόν να δείξουμε την ύπαρξη πολλαπλασιαστικού αντιστρόφου (εντός τού $R/\mathfrak{m}$) για οιοδήποτε στοιχείο $a+\mathfrak{m} \in R/\mathfrak{m}$, με $a \in R \setminus \mathfrak{m}$. Επειδή το $\mathfrak{m}$ είναι ένα μεγιστικό ιδεώδες τού R, για οιοδήποτε μη μηδενικό στοιχείο $a+\mathfrak{m}$ τού $R/\mathfrak{m}$ έχουμε

$$\left.\begin{array}{rcl} \mathfrak{m} \subsetneqq \mathfrak{m}+\langle a\rangle \subseteq R & \Longrightarrow & \mathfrak{m}+\langle a\rangle = R \\ & & R \text{ μεταθετικός} \end{array}\right\} \Longrightarrow [\exists r \in R,\ b \in \mathfrak{m} : 1_R = b+ra]\,.$$

Επομένως, $1_R - ra = b \in \mathfrak{m}$, οπότε

$$1_R+\mathfrak{m} = (ra+b)+\mathfrak{m} = ra+\mathfrak{m} = (r+\mathfrak{m})(a+\mathfrak{m})\,,$$

απ' όπου έπεται ότι το $r+\mathfrak{m}$ είναι πολλαπλασιαστικό αντίστροφο τού $a+\mathfrak{m}$. Άρα ο πηλικοδακτύλιος $R/\mathfrak{m}$ είναι σώμα.

(ii) Εάν ο πηλικοδακτύλιος $R/\mathfrak{m}$ είναι διαιρετικός δακτύλιος, παρατηρούμε εν πρώτοις ότι $1_R+\mathfrak{m}\neq 0_R+\mathfrak{m}\Longrightarrow 1_R\notin\mathfrak{m}\Longrightarrow\mathfrak{m}\subsetneq R$. Εν συνεχεία, υποθέτουμε ότι το $\mathfrak{n}$ είναι ένα ιδεώδες τού R με $\mathfrak{m}\subsetneq\mathfrak{n}\subseteq R$. Έστω τυχόν $a\in\mathfrak{n}\smallsetminus\mathfrak{m}$. Το $a+\mathfrak{m}$ έχει (εξ υποθέσεως) πολλαπλασιαστικό αντίστροφο, ας το πούμε $b+\mathfrak{m}$, εντός τού $R/\mathfrak{m}$. Συνεπώς,

$$(a+\mathfrak{m})\,(b+\mathfrak{m})=ab+\mathfrak{m}=1_R+\mathfrak{m}\Longrightarrow ab-1_R=:c\in\mathfrak{m}\subsetneq\mathfrak{n},$$

και

$$\left.\begin{array}{r} a\in\mathfrak{n}\Longrightarrow ab\in\mathfrak{n}\\ c\in\mathfrak{n}\end{array}\right\}\Longrightarrow c-ab=1_R\in\mathfrak{n}\Longrightarrow\mathfrak{n}=R.$$

Άρα το $\mathfrak{m}$ είναι μεγιστικό ιδεώδες τού R. □

7.6.6 Σημείωση. Το 7.6.5 (i) δεν είναι πάντοτε αληθές για δακτυλίους χωρίς μοναδιαίο στοιχείο. Επί παραδείγματι, ο (μεταθετικός) δακτύλιος των αρτίων ακεραίων $2\mathbb{Z}$ περιέχει το μεγιστικό ιδεώδες $\mathfrak{m}=\langle 4\rangle$, χωρίς -όμως- ο αντίστοιχος πηλικοδακτύλιος $2\mathbb{Z}/\mathfrak{m}$ να είναι σώμα ή ακόμη και ακεραία περιοχή. Πράγματι· εντός τού πηλικοδακτυλίου υπάρχουν μηδενοδιαιρέτες, όπως π.χ. το στοιχείο $2+\mathfrak{m}\neq\mathfrak{m}$, αφού ισχύουν οι ισότητες $(2+\mathfrak{m})\,(2+\mathfrak{m})=4+\mathfrak{m}=\mathfrak{m}=0_{2\mathbb{Z}/\mathfrak{m}}$.

7.7 ΤΟΠΙΚΟΙ ΔΑΚΤΥΛΙΟΙ

7.7.1 Πρόταση. *Έστω R ένας μη τετριμμένος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και έστω*

$$\mathfrak{m}_{_R}:=R\smallsetminus R^\times.$$

Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:

(*i*) $a-b\in\mathfrak{m}_{_R}$ *για κάθε* $a,b\in\mathfrak{m}_{_R}$.

(ii) *Το* $\mathfrak{m}_{_R}$ *είναι ένα ιδεώδες τού* R.

(iii) *Το* $\mathfrak{m}_{_R}$ *είναι ένα μεγιστικό ιδεώδες τού* R.

(iv) *Για κάθε* $a\in R$ *έχουμε είτε* $a\in R^\times$ *είτε* $1_R-a\in R^\times$.

Απόδειξη. (i)⇒(ii): Θεωρούμε τυχόντα στοιχεία $a\in\mathfrak{m}_{_R}$ και $r\in R$. Αρκεί να αποδείξουμε ότι $ra\in\mathfrak{m}_{_R}$. Εάν είχαμε $ra\notin\mathfrak{m}_{_R}$, τότε $ra\in R^\times$, οπότε θα υπήρχε $b\in R$ με $(ra)b=a(rb)=1_R$. Τούτο θα σήμαινε ότι $a\in R^\times$. Άτοπο! Άρα $ra\in\mathfrak{m}_{_R}$.

(ii)⇒(iii): Λόγω τού (ii) τού πορίσματος 7.6.5 αρκεί προς τούτο να δειχθεί ότι ο πηλικοδακτύλιος $R/\mathfrak{m}_{_R}$ είναι σώμα. Μάλιστα, επειδή

$$R/\mathfrak{m}_{_R}=\left\{r+\mathfrak{m}_{_R}\mid r\in R^\times\cup\{0_R\}\right\},$$

είναι αρκετό να δειχθεί ότι $r+\mathfrak{m}_{_R}\in(R/\mathfrak{m}_{_R})^\times$ για κάθε $r\in R^\times$. Τούτο έπεται από το (iii) τής προτάσεως 7.6.3.

(iii)⇒(iv): Έστω τυχόν στοιχείο $a\in R$. Εάν ίσχυε $a\in\mathfrak{m}_{_R}$ και $1_R-a\in\mathfrak{m}_{_R}$, τότε θα καταλήγαμε στην αντίφαση: $a+(1_R-a)=1_R\in\mathfrak{m}_{_R}\Longrightarrow\mathfrak{m}_{_R}=R$.

(iv)⇒(i): Ας υποθέσουμε ότι υπάρχουν $a,b\in\mathfrak{m}_{_R}$ με $a-b\notin\mathfrak{m}_{_R}$. Τότε $a-b\in R^\times$, οπότε $\exists c\in R:(a-b)\,c=ac+(-bc)=1_R$. Εξ υποθέσεως, είτε $ac\in R^\times$ είτε $-bc\in R^\times$. Εάν $ac\in R^\times$, τότε

$$\left.\begin{array}{r} a=a\cdot 1_R=(ac)\,(a-b)\\ ac\in R^\times,\,a-b\in R^\times\end{array}\right\}\Longrightarrow a\in R^\times.$$

Άτοπο! Αναλόγως, καταλήγουμε σε άτοπο εάν υποθέσουμε ότι $-bc\in R^\times$. □

7.7.2 Ορισμός. Κάθε μη τετριμμένος μεταθετικός δακτύλιος R με μοναδιαίο στοιχείο, ο οποίος πληροί μία (και, κατ' επέκταση, και τις τέσσερεις) εκ των συνθηκών (i)-(iv) τής προτάσεως 7.7.1, ονομάζεται **τοπικός δακτύλιος**.

7.7.3 Παραδείγματα. (i) *Κάθε σώμα K είναι ένας τοπικός δακτύλιος*, διότι το $K \smallsetminus K^\times = \{0_K\}$ είναι ιδεώδες του.

(ii) Ο δακτύλιος

$$\mathbb{Z}_{\langle p\rangle} := \left\{ r \in \mathbb{Q} \mid r = \frac{a}{b},\ (a,b) \in \mathbb{Z}\times\left(\mathbb{Z}\smallsetminus\{0\}\right),\ \text{με μκδ}\,(a,b) = 1 \text{ και } p \nmid b \right\}$$

των p-αδικών κλασμάτων (όπου p πρώτος, βλ. άσκηση 10 τού φυλλαδίου 11) είναι τοπικός δακτύλιος, καθότι το (κύριο) ιδεώδες

$$\mathbb{Z}_{\langle p\rangle} \smallsetminus \mathbb{Z}_{\langle p\rangle}^\times = p\mathbb{Z}_{\langle p\rangle}$$

είναι μεγιστικό (οπότε πληρούται η συνθήκη (iii) τής προτάσεως 7.7.1). Πράγματι· εάν το I είναι ένα ιδεώδες τού $\mathbb{Z}_{\langle p\rangle}$ με $p\mathbb{Z}_{\langle p\rangle} \subsetneqq I$, τότε

$$\exists r \in I : r \notin p\mathbb{Z}_{\langle p\rangle} \Longrightarrow r = \frac{a}{b},\ (a,b) \in \mathbb{Z}\times\left(\mathbb{Z}\smallsetminus\{0\}\right),\ \text{με μκδ}\,(a,b) = 1,\ p \nmid a,\ p \nmid b.$$

Κατά συνέπειαν, $\frac{1}{r} \in \mathbb{Z}_{\langle p\rangle} \Longrightarrow \frac{1}{r}r = 1 \in I \Longrightarrow I = \mathbb{Z}_{\langle p\rangle}$.

(iii) Ο δακτύλιος $\mathbb{Z}$ των ακεραίων αριθμών δεν είναι τοπικός δακτύλιος, διότι το σύνολο $\mathbb{Z}\smallsetminus\mathbb{Z}^\times = \mathbb{Z}\smallsetminus\{\pm 1\}$ (εφοδιασμένο με την πράξη τής συνήθους προσθέσεως ακεραίων) δεν είναι ούτε καν υποομάδα τής ομάδας $(\mathbb{Z}, +)$, με αποτέλεσμα να μην ικανοποιείται η συνθήκη (i) τής προτάσεως 7.7.1.

(iv) Έστω K ένα σώμα. Ο δακτύλιος $K[\mathsf{X}]$ των πολυωνύμων μιας απροσδιορίστου με συντελεστές ειλημμένους από αυτό δεν είναι τοπικός δακτύλιος, διότι το σύνολο

$$K[\mathsf{X}] \smallsetminus K[\mathsf{X}]^\times = \{0_{K[\mathsf{X}]}\} \cup \{\varphi(\mathsf{X}) \in K[\mathsf{X}] \mid \deg(\varphi(\mathsf{X})) \geqslant 1\}$$

(εφοδιασμένο με την πράξη τής συνήθους προσθέσεως πολυωνύμων ανηκόντων στον $K[\mathsf{X}]$) δεν είναι ούτε καν υποομάδα τής ομάδας $(K[\mathsf{X}], +)$. Αντιθέτως, ο δακτύλιος δακτύλιος $K[\![\mathsf{X}]\!]$ των επίτυπων δυναμοσειρών μιας απροσδιορίστου με συντελεστές ειλημμένους από το K *είναι* τοπικός δακτύλιος. Πράγματι· ένα στοιχείο τού $K[\![\mathsf{X}]\!]$ είναι αντιστρέψιμο όταν ο σταθερός του όρος είναι $\neq 0_K$. Επομένως, το σύνολο $K[\![\mathsf{X}]\!] \smallsetminus K[\![\mathsf{X}]\!]^\times$ απαρτίζεται από εκείνες τις επίτυπες δυναμοσειρές, ο σταθερός όρος των οποίων είναι $= 0_K$ (βλ. το (iii) τής προτάσεως 6.3.9), και ισούται με

$$K[\![\mathsf{X}]\!] \smallsetminus K[\![\mathsf{X}]\!]^\times = \left\{ \varphi(\mathsf{X}) = \sum_{i=0}^{\infty} a_i \mathsf{X}^i \in K[\![\mathsf{X}]\!] \;\middle|\; a_0 = 0_K \right\} = \langle \mathsf{X} \rangle$$

ήτοι με το ιδεώδες το παραγόμενο από το X. (Άρα η συνθήκη 7.7.1 (ii) ικανοποιείται και το $\langle \mathsf{X} \rangle$ είναι κατ' ανάγκην μεγιστικό ιδεώδες τού $K[\![\mathsf{X}]\!]$). Γενικότερα, ο δακτύλιος των επίτυπων δυναμοσειρών n απροσδιορίστων $\mathsf{X}_1, \ldots, \mathsf{X}_n$ με συντελεστές ειλημμένους από το K *είναι* τοπικός δακτύλιος, καθότι

$$K[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!] \smallsetminus K[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!]^\times = \langle \mathsf{X}_1, \ldots, \mathsf{X}_n \rangle .$$

7.7.4 Πόρισμα. *Ένας μη τετριμμένος μεταθετικός δακτύλιος R με μοναδιαίο στοιχείο είναι τοπικός εάν και μόνον εάν διαθέτει ένα και μόνον μεγιστικό ιδεώδες (ήτοι το $\mathfrak{m}_R$).*

Απόδειξη. Υποθέτουμε εν πρώτοις ότι ο R είναι τοπικός δακτύλιος και ότι το $\mathfrak{m}$ είναι ένα μεγιστικό του ιδεώδες. Επειδή εξ ορισμού $\mathfrak{m} \subsetneqq R$, το $\mathfrak{m}$ δεν περιέχει κανένα αντιστρέψιμο στοιχείο τού R. Άρα $\mathfrak{m} \subseteq \mathfrak{m}_{_R} \subsetneqq R$. Κατά τον ορισμό 7.7.2 και το (iii) τής προτάσεως 7.7.1 το $\mathfrak{m}_{_R}$ είναι ένα μεγιστικό ιδεώδες τού R. Κατά συνέπειαν, $\mathfrak{m} = \mathfrak{m}_{_R}$.

Και αντιστρόφως· εάν υποθέσουμε ότι ο R είναι ένας μη τετριμμένος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο περιέχων ένα και μόνον μεγιστικό ιδεώδες $\mathfrak{m}$ και εάν $\mathfrak{m}_{_R} := R \smallsetminus R^\times$, τότε *για κάθε* $a \in \mathfrak{m}_{_R}$ έχουμε $\langle a \rangle \subsetneqq R$ (διότι προφανώς $a \notin R^\times \implies 1_R \notin \langle a \rangle$). Σύμφωνα με το θεώρημα 7.5.13 το ιδεώδες $\langle a \rangle$ οφείλει να περιέχεται σε κάποιο μεγιστικό ιδεώδες τού R. Όμως εξ υποθέσεως το $\mathfrak{m}$ είναι το μόνο μεγιστικό ιδεώδες τού R. Άρα $\langle a \rangle \subseteq \mathfrak{m} \subsetneqq R \implies a \in \mathfrak{m} \implies \mathfrak{m}_{_R} \subseteq \mathfrak{m} \subsetneqq R$. Εάν υπήρχε $b \in \mathfrak{m} \smallsetminus \mathfrak{m}_{_R}$, τότε θα είχαμε $b \in R^\times \cap \mathfrak{m}$, πράγμα άτοπο, καθόσον ισχύει $\mathfrak{m} \subsetneqq R \implies R^\times \cap \mathfrak{m} = \varnothing$. Άρα τελικώς το $\mathfrak{m}_{_R} = \mathfrak{m}$ είναι μεγιστικό ιδεώδες και ο R τοπικός δακτύλιος. □

7.7.5 Σημείωση. (i) Εξαιτίας τού πορίσματος 7.7.4 πολλοί συγγραφείς *ορίζουν* τους τοπικούς δακτυλίους ως «εκείνους τους μη τετριμμένους μεταθετικούς δακτυλίους με μοναδιαίο στοιχείο που διαθέτουν ένα και μόνον μεγιστικό ιδεώδες»· είθισται, μάλιστα, η αναφορά σε κάποιον συγκεκριμένο τοπικό δακτύλιο να συνοδεύεται από την ταυτόχρονη παράθεση τού εν λόγω ιδεώδους του.

(ii) Εάν ο R είναι ένας τοπικός δακτύλιος, τότε το ιδεώδες $\mathfrak{m}_{_R}$ είναι *το μέγιστο στοιχείο* τού συνόλου $\mathcal{S}_R$ των γνησίων ιδεωδών τού R ως προς τη σχέση εγκλεισμού "$\subseteq$" (βλ. 1.4.9 (i) και 7.5.12 (i)).

7.7.6 Πρόταση. *Η χαρακτηριστική οιουδήποτε τοπικού δακτυλίου ισούται είτε με* 0 *είτε με* p^ν, *όπου* p *πρώτος αριθμός και* $\nu \in \mathbb{N}$.

Απόδειξη. Έστω R τοπικός δακτύλιος με $\text{χαρ}(R) = n > 0$. Προφανώς, $n \geqslant 2$ (αφού ο R είναι μη τετριμμένος). Ας υποθέσουμε ότι υπάρχουν πρώτοι αριθμοί p, q με $p \mid n$, $q \mid n$ και $p \neq q$. Παρατηρούμε ότι

$$\begin{aligned} p \mid n \Rightarrow \exists k \in \mathbb{N} : n = kp \\ \Rightarrow 0 = n \cdot 1_R = k(p \cdot 1_R) \Rightarrow p \cdot 1_R \in \mathbf{Zdv}\,(R) \subseteq\ R \smallsetminus R^\times =: \mathfrak{m}_{_R} \end{aligned}$$

(βλ. προτάσεις 6.4.3 και 6.2.17). Κατ' αναλογίαν, αποδεικνύεται ότι $q \cdot 1_R \in \mathfrak{m}_{_R}$. Επειδή μκδ$(p, q) = 1$, θα υπάρχουν $s, t \in \mathbb{Z} : sp + tq = 1$, οπότε

$$\left.\begin{aligned} 1_R = (sp + tq) \cdot 1_R = s(p \cdot 1_R) + t(q \cdot 1_R) \\ s \in \mathbb{Z}, p \cdot 1_R \in \mathfrak{m}_{_R} \Rightarrow s(p \cdot 1_R) \in \mathfrak{m}_{_R} \\ t \in \mathbb{Z}, q \cdot 1_R \in \mathfrak{m}_{_R} \Rightarrow t(q \cdot 1_R) \in \mathfrak{m}_{_R} \end{aligned}\right\} \Rightarrow 1_R \in \mathfrak{m}_{_R} \Rightarrow \mathfrak{m}_{_R} = R.$$

Άτοπο! Κατά συνέπειαν, υπάρχει *ένας και μόνον* πρώτος αριθμός p που διαιρεί τον n, οπότε ο n ισούται κατ' ανάγκην με p^ν, όπου $\nu \in \mathbb{N}$. □

ΚΕΦΑΛΑΙΟ 8

Ομομορφισμοί δακτυλίων

Οι απεικονίσεις μεταξύ δυο δακτυλίων, οι οποίες τυγχάνει να μεταφέρουν τις εκάστοτε θεωρούμενες πράξεις προσθέσεως και πολλαπλασιασμού κατά τρόπο συμβατό, καλούνται *ομομορφισμοί δακτυλίων*. Οι *εμφυτεύσεις* δακτυλίων εντός άλλων διασφαλίζονται μέσω κατασκευής *μονομορφισμών*, ήτοι ενριπτικών ομομορφισμών. Οι *πυρήνες* των ομομορφισμών δακτυλίων αποτελούν ιδεώδη και κάθε ιδεώδες ενός δακτυλίου μπορεί να ιδωθεί ως πυρήνας τού λεγομένου *φυσικού επιμορφισμού*. Το *θεώρημα αντιστοιχίσεως* περιγράφει τον τρόπο συσχετισμού των ιδεωδών ενός δακτυλίου με τα ιδεώδη τής εικόνας αυτού μέσω ενός επιμορφισμού. Τέλος, τα *θεωρήματα ισομορφισμών* μάς παρέχουν χρήσιμες πληροφορίες για τις περιπτώσεις «ταυτίσεως» ορισμένων χαρακτηριστικών δακτυλίων και πηλικοδακτυλίων, κατ' αναλογίαν προς ό,τι συμβαίνει με τα συνώνυμα θεωρήματα περί ομάδων.

8.1 ΘΕΜΕΛΙΩΔΕΙΣ ΟΡΙΣΜΟΙ ΚΑΙ ΙΔΙΟΤΗΤΕΣ

8.1.1 Ορισμός. Έστω ότι $(R_1, +_1, \cdot_1)$ και $(R_2, +_2, \cdot_2)$ είναι δυο δακτύλιοι και ότι $f : R_1 \longrightarrow R_2$ είναι μια απεικόνιση. Η f καλείται **ομομορφισμός (δακτυλίων)** όταν για όλα τα $a, b \in R_1$ ισχύει

$$\boxed{f(a +_1 b) = f(a) +_2 f(b)} \quad \text{και} \quad \boxed{f(a \cdot_1 b) = f(a) \cdot_2 f(b).} \tag{8.1}$$

Ένας ομομορφισμός δακτυλίων $f : R_1 \longrightarrow R_2$ ονομάζεται

μονομορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι ενριπτική,
επιμορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι επιριπτική,
ισομορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι αμφιριπτική,
ενδομορφισμός (τού R_1)	$\underset{\text{ορσ}}{\Longleftrightarrow}$	$R_1 = R_2, +_1 = +_2$ και $\cdot_1 = \cdot_2$,
αυτομορφισμός (τού R_1)	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η f είναι αμφιριπτικός ενδομορφισμός.

(Φυσικά, αυτές οι έννοιες εμπεριέχουν τις αντίστοιχες έννοιες για τις επί μέρους δομές, δηλαδή εκείνες των εκάστοτε μετεχουσών αβελιανών προσθετικών ομάδων και πολλαπλασιαστικών ημιομάδων).

8.1.2 Σημείωση (Απλούστευση συμβολισμού.). Κατά κανόνα (για λόγους συντομίας) οι δείκτες $1, 2$ (ή οποιαδήποτε άλλη ειδική σήμανση) θα *παραλείπονται* στον

συμβολισμό των πράξεων. Ωστόσο, θα πρέπει κανείς να έχει πάντα κατά νου το ποιο "$+$" και ποιο "$\cdot$" υπονοείται κατά περίπτωση.

8.1.3 Παραδείγματα. (i) Έστω m ένας φυσικός αριθμός. Ορίζουμε την απεικόνιση

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_m, \quad n \longmapsto [n]_m \, .$$

Είναι εύκολο να αποδειχθεί ότι η f είναι ένας επιμορφισμός δακτυλίων.

(ii) Η απεικόνιση $f : \mathbb{Z} \longrightarrow 2\,\mathbb{Z}$ η οριζομένη μέσω τού τύπου $f\,(n) := 2n$ *δεν είναι* ομομορφισμός δακτυλίων, παρότι *είναι* ισομορφισμός μεταξύ των αντιστοίχων προσθετικών ομάδων!

(iii) Έστω $(2\,\mathbb{Z}, +, \star)$ ο δακτύλιος ο αποτελούμενος από τους αρτίους ακεραίους με τη συνήθη πρόσθεση και τον ακόλουθο «τροποποιημένο» πολλαπλασιασμό:

$$m \star n := \frac{m \cdot n}{2} \, .$$

Τότε η $f : \mathbb{Z} \longrightarrow 2\,\mathbb{Z}$ η οριζομένη μέσω τού τύπου $f\,(n) := 2n$ (όπως και στο (ii)) αποτελεί *ισομορφισμό δακτυλίων*.

(iv) Εάν το K είναι ένα σώμα με $\text{χαρ}(K) = p > 0$, τότε η απεικόνιση

$$f : K \longrightarrow K, \quad x \longmapsto f(x) := x^p,$$

είναι ένας ενδομορφισμός (πρβλ. πρόταση 6.4.8 (i)) και καλείται, ιδιαιτέρως, **απεικόνιση τού Frobenius**.

(v) Ο ομομορφισμός

$$\mathbb{C} \longrightarrow \mathbb{C}, \;\; z = a + ib \longmapsto a - ib = \overline{z},$$

είναι ένας αυτομορφισμός τού σώματος των μιγαδικών αριθμών.

(vi) Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων και έστω

$$\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\} \subsetneq \mathbb{C}$$

το αριθμητικό τετραγωνικό σώμα το αντιστοιχιζόμενο στον m. (Βλ. άσκηση 24 τού φυλλαδίου 11.) Τότε η απεικόνιση

$$f : \mathbb{Q}(\sqrt{m}) \longrightarrow \mathbb{Q}(\sqrt{m}), \quad f(a + b\sqrt{m}) := a - b\sqrt{m},$$

αποτελεί έναν αυτομορφισμό τού $\mathbb{Q}(\sqrt{m})$. (Βλ. άσκηση 19 τού φυλλαδίου 12.)

(vii) Η *μηδενική απεικόνιση* $f : R \longrightarrow S$ μεταξύ δυο δακτυλίων R και S, όπου $f(a) = 0_S$ για κάθε $a \in R$, είναι ένας ομομορφισμός δακτυλίων (ο λεγόμενος **μηδενικός ομομορφισμός**). Σημειωτέον ότι όταν κανείς εκ των R, S δεν είναι τετριμμένος, ο μηδενικός ομομορφισμός δεν είναι ούτε ενριπτικός ούτε επιριπτικός.

(viii) Εάν $f : R \longrightarrow S$ είναι ένας ομομορφισμός δακτυλίων και

$$\text{in}_{\text{Im}(f),S} : \text{Im}(f) \longrightarrow S, \; s \longmapsto \text{in}_{\text{Im}(f),S}(s) := s,$$

η συνήθης ένθεση τής εικόνας του εντός τού S, τότε $f = \text{in}_{\text{Im}(f),S} \circ \check{f}$, όπου

$$\boxed{\check{f} : R \longrightarrow \text{Im}(f), \; r \longmapsto \check{f}(r) := f(r),}$$

ο επιμορφισμός ο επαγόμενος μέσω τού f.

8.1.4 Πρόταση. *Έστω $f : R \longrightarrow R'$ ένας ομομορφισμός δακτυλίων. Εάν $n \in \mathbb{N}$ και εάν τα $a_1, ..., a_n$ είναι στοιχεία τού R, τότε*

$$f(\sum_{j=1}^{n} a_j) = \sum_{j=1}^{n} f(a_j) \qquad \text{και} \qquad f(\prod_{j=1}^{n} a_j) = \prod_{j=1}^{n} f(a_j).$$

Απόδειξη. Έπεται κατόπιν χρήσεως των ισοτήτων (8.1) και μαθηματικής επαγωγής ως προς τον n. □

8.1.5 Πρόταση. *Ένας ομομορφισμός δακτυλίων $f : R \longrightarrow R'$ έχει τις εξής ιδιότητες:*

(i) $f(0_R) = 0_{R'}$ *και* $f(-a) = -f(a),\ \forall a \in R$.

(ii) *Για κάθε $a \in R$ ισχύουν οι ισότητες:*

$$f(na) = n\,f(a),\ \forall n \in \mathbb{Z}, \quad \text{και} \quad f(a^n) = f(a)^n,\ \forall n \in \mathbb{N}.$$

(iii) *Εάν ο S είναι ένας υποδακτύλιος τού R, τότε η εικόνα του $f(S)$ μέσω τής f είναι ένας υποδακτύλιος τού R'.*

(iv) *Εάν ο S' είναι ένας υποδακτύλιος τού R', τότε η αντίστροφή του εικόνα $f^{-1}(S')$ μέσω τής f είναι ένας υποδακτύλιος τού R.*

(v) *Εάν ο R είναι ένας δακτύλιος με μοναδιαίο στοιχείο, τότε και ο $f(R)$ είναι δακτύλιος με μοναδιαίο στοιχείο, και μάλιστα ισχύει η ισότητα $f(1_R) = 1_{f(R)}$.*

(vi) *Εάν ο R είναι ένας δακτύλιος με μοναδιαίο στοιχείο, η f μη μηδενικός ομομορφισμός και ο R' διαιρετικός δακτύλιος ή ακεραία περιοχή, τότε $f(1_R) = 1_{R'}$.*

(vii) *Εάν ο R είναι ένας μεταθετικός δακτύλιος, τότε και ο $f(R)$ είναι μεταθετικός.*

(viii) *Εάν ο R είναι ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο και η f μη μηδενικός ομομορφισμός, τότε*

$$f(a^{-1}) \in f(R)^{\times},\ f(a^{-1}) = [f(a)]^{-1},\ \ \forall a \in R^{\times},$$

και, γενικότερα,

$$f(a^n) = f(a)^n,\ \ \forall a \in R^{\times} \text{ και } \forall n \in \mathbb{Z}.$$

(ix) *Εάν η f είναι μονομορφισμός και ο R ακεραία περιοχή (και αντιστοίχως, στεβλό σώμα/σώμα), τότε και ο $f(R)$ είναι ακεραία περιοχή (και αντιστοίχως, στρεβλό σώμα/σώμα).*

Απόδειξη. (i) Προφανώς, $f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R)$, οπότε ισχύει η ισότητα $f(0_R) = 0_{R'}$. Εξάλλου, για κάθε $a \in R$, έχουμε

$$0_{R'} = f(0_R) = f(a + (-a)) = f(a) + f(-a) \Longrightarrow f(-a) = -f(a).$$

(ii) Η απόδειξη έπεται από την πρόταση 8.1.4 και τη δεύτερη ισότητα τού (i).

(iii) Εάν υποτεθεί ότι $b_1, b_2 \in f(S)$, τότε υπάρχουν στοιχεία $a_1, a_2 \in S$, τέτοια ώστε $f(a_1) = b_1$ και $f(a_2) = b_2$. Επειδή ο S είναι ένας υποδακτύλιος τού R,

$$\left.\begin{array}{r} a_1 - a_2 \in S, \\ a_1 a_2 \in S \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} b_1 - b_2 = f(a_1) - f(a_2) = f(a_1 - a_2) \in f(S), \\ b_1 b_2 = f(a_1) f(a_2) = f(a_1 a_2) \in f(S), \end{array}\right.$$

οπότε η εικόνα $f(S)$ τού S μέσω τής f είναι όντως ένας υποδακτύλιος τού R'.

(iv) Εάν $a_1, a_2 \in f^{-1}(S')$, τότε $f(a_1) \in S'$ και $f(a_2) \in S'$. Κι επειδή ο S' είναι υποδακτύλιος τού R',

$$\left.\begin{array}{r} f(a_1 - a_2) = f(a_1) - f(a_2) \in S', \\ f(a_1 a_2) = f(a_1) f(a_2) \in S' \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} a_1 - a_2 \in f^{-1}(S'), \\ a_1 a_2 \in f^{-1}(S'), \end{array}\right.$$

ήτοι *και* η αντίστροφή του εικόνα $f^{-1}(S')$ μέσω τής f είναι ένας υποδακτύλιος τού δακτυλίου R.

(v) Έστω b τυχόν στοιχείο τού $f(R)$. Τότε υπάρχει ένα $a \in R$, τέτοιο ώστε να ισχύει η ισότητα $f(a) = b$. Άρα

$$f(1_R)f(a) = f(1_R a) = f(a), \qquad f(a)f(1_R) = f(a1_R) = f(a),$$

οπότε ο $f(R)$ είναι δακτύλιος με μοναδιαίο στοιχείο και $f(1_R) = 1_{f(R)}$.

(vi) Επειδή -εξ υποθέσεως- ο f δεν είναι ο μηδενικός ομομορφισμός, θα υπάρχει ένα $a \in R$, τέτοιο ώστε $f(a) \neq 0_{R'}$. Εξ αυτού έπεται ότι

$$f(a) \cdot 1_{R'} = f(a) = f(a \cdot 1_R) = f(a)f(1_R) \Longrightarrow f(a)\left(f(1_R) - 1_{R'}\right) = 0_{R'}.$$

Εάν ο R' είναι διαιρετικός δακτύλιος, τότε υπάρχει το αντίστροφο $f(a)^{-1}$ τού $f(a)$, με το οποίο μπορούμε να πολλαπλασιάσουμε αμφότερα τα μέλη τής ανωτέρω ισότητας και να λάβουμε $f(1_R) = 1_{R'}$. Εάν, από την άλλη μεριά, ο R' είναι ακεραία περιοχή, τότε μπορούμε να καταλήξουμε στο ίδιο συμπέρασμα κάνοντας χρήση τού νόμου τής διαγραφής 6.2.5.

(vii) Προφανώς, για κάθε $a, b \in R$, έχουμε

$$f(a)f(b) = f(ab) = f(ba) = f(b)f(a).$$

(viii) Για κάθε $a \in R^\times$ έχουμε

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(1_R) = f(a^{-1}a) = f(a^{-1})f(a).$$

Κι επειδή (λόγω τού (v)) ισχύει $f(1_R) = 1_{f(R)} \neq 0_{R'}$, έχουμε $f(a) \neq 0_{R'}$ και

$$f(a^{-1}) = [f(a)]^{-1} \in f(R)^\times.$$

Η δεύτερη ισότητα αποδεικνύεται εύκολα μέσω μαθηματικής επαγωγής.

(ix) Έστω ότι ο f είναι μονομορφισμός και ο R ακεραία περιοχή. Προφανώς, επειδή $1_R \neq 0_R$, το $f(1_R) = 1_{f(R)}$ είναι διάφορο τού $f(0_R) = 0_{R'}$. Εάν υποθέσουμε ότι $f(a), f(b) \in f(R)$, για κάποια $a, b \in R$, τέτοια ώστε να ισχύει

$$f(a)f(b) = 0_{f(R)} \Longleftrightarrow f(ab) = 0_{f(R)} = f(0_R),$$

τότε $ab = 0_R$, οπότε $a = 0_R$ ή $b = 0_R$. Συνεπώς, $f(a) = 0_{f(R)}$ ή $f(b) = 0_{f(R)}$. Άρα *και* ο $f(R)$ είναι ακεραία περιοχή.

Εν συνεχεία, ας υποθέσουμε ότι ο f είναι μονομορφισμός και ο R στρεβλό σώμα. Προφανώς, επειδή $1_R \neq 0_R$, το $f(1_R) = 1_{f(R)}$ είναι διάφορο τού $f(0_R) = 0_{R'}$. Αρκεί λοιπόν να δείξουμε ότι $f(R)^\times = f(R) \setminus \{0_{R'}\}$. Ο εγκλεισμός "$\subseteq$" είναι πρόδηλος. Ας θεωρήσουμε τυχόν $b \in f(R) \setminus \{0_{R'}\}$. Τότε υπάρχει ένα $a \in R \setminus \{0_R\}$, τέτοιο ώστε $b = f(a)$. Όμως -εξ υποθέσεως- $R \setminus \{0_R\} = R^\times$, οπότε $a \in R^\times$, πράγμα που σημαίνει ότι υπάρχει (πολλαπλασιαστικό) αντίστροφο a^{-1} τού a, για το οποίο ισχύει $f(a^{-1}) = [f(a)]^{-1} \in f(R)^\times$ (βάσει τού (viii)). Άρα $b \in f(R)^\times$, και, ως εκ τούτου, ο $f(R)$ είναι στρεβλό σώμα. (Στην περίπτωση κατά την οποία ο f είναι μονομορφισμός και ο R σώμα, αρκεί να χρησιμοποιήσουμε ό,τι προείπαμε σε συνδυασμό με το (vii).) □

8.1.6 Πρόταση. *Εάν οι $f : R \longrightarrow R'$ και $g : R' \longrightarrow R''$ είναι δυο ομομορφισμοί (και αντιστοίχως, μονομορφισμοί/επιμορφισμοί/ισομορφισμοί) δακτυλίων, και η σύνθεσή τους $g \circ f : R \longrightarrow R''$ θα είναι ομομορφισμός (και αντιστοίχως, μονομορφισμός/επιμορφισμός/ισομορφισμός) δακτυλίων.*

Απόδειξη. Εάν οι f και g είναι ομομορφισμοί δακτυλίων, τότε για όλα τα $a, b \in R$ ισχύουν οι ισότητες

$$(g \circ f)(a+b) = g(f(a+b)) = g(f(a) + f(b)) = (g \circ f)(a) + (g \circ f)(b)$$

και

$$(g \circ f)(ab) = g(f(ab)) = g(f(a)\, f(b)) = g(f(a))g(f(b)) = (g \circ f)(a)\,(g \circ f)(b),$$

οπότε και η σύνθεσή τους $g \circ f$ είναι ένας ομομορφισμός δακτυλίων. Η απόδειξη αποπερατούται λαμβάνοντας υπ' όψιν το γεγονός ότι η σύνθεση δυο ενρίψεων (και αντιστοίχως, επιρρίψεων/αμφιρρίψεων) είναι μια ένριψη (και αντιστοίχως, μια επίρριψη/αμφίρριψη). □

8.1.7 Ορισμός. Εάν οι R και R' είναι δυο δακτύλιοι, τότε γράφουμε[1] $R \cong R'$ και λέμε ότι **ο** R **είναι ισόμορφος με τον** R' (ή ότι οι R και R' **είναι ισόμορφοι**) όταν υπάρχει κάποιος ισομορφισμός δακτυλίων $f : R \longrightarrow R'$. (Κατ' αναλογίαν, το σύμβολο $R \ncong R'$ δηλοί ότι ο δακτύλιος R *δεν είναι ισόμορφος* με τον R'.)

8.1.8 Παραδείγματα. (i) Η ακεραία περιοχή $\mathbb{Z}[\sqrt{2}]$ (βλ. άσκηση 24 τού φυλλαδίου 11) είναι ισόμορφη με τον ακόλουθο δακτύλιο 2×2-πινάκων:

$$R := \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \middle| \, a, b \in \mathbb{Z} \right\} \subsetneq \mathrm{Mat}_{2\times 2}(\mathbb{Z}),$$

καθόσον υφίσταται ισομορφισμός δακτυλίων:

$$\mathbb{Z}[\sqrt{2}] \ni a + b\sqrt{2} \longmapsto \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \in R.$$

(ii) Έχουμε $\mathbb{Z}[\sqrt{2}] \ncong \mathbb{Z}[\sqrt{3}]$, διότι εάν υπήρχε ισομορφισμός δακτυλίων

$$f : \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Z}[\sqrt{3}],$$

θα έπρεπε να ισχύει

$$f(\sqrt{2})^2 = f((\sqrt{2})^2) = f(2) = f(1+1) = 2f(1) = 2 \Rightarrow f(\sqrt{2}) \in \{\pm\sqrt{2}\},$$

κάτι που θα αντέφασκε προς το ότι $\pm\sqrt{2} \notin \mathbb{Z}[\sqrt{3}]$.

(iii) Τα σώματα $\mathbb{C}$ και $\mathbb{R}$ δεν είναι ισόμορφα, διότι εάν υπήρχε ένας ισομορφισμός $f : \mathbb{C} \longrightarrow \mathbb{R}$, τότε θα έπρεπε να ισχύει

$$-1 = -f(1) = f(-1) = f(i^2) = f(i)^2$$

(όπου i η φανταστική μονάδα), κάτι που θα αντέφασκε προς το ότι $f(i) \in \mathbb{R}$.

8.1.9 Πρόταση. *Για οιουσδήποτε δακτυλίους R, R', R'' ισχύουν τα εξής*:

(i) $R \cong R$,

(ii) $R \cong R' \Longrightarrow R' \cong R$,

(iii) $[R \cong R' \text{ και } R' \cong R''] \Longrightarrow R \cong R''$.

[1] Από τούδε και στο εξής μέσω τού συμβόλου "$\cong$" θα εκφράζουμε την ύπαρξη ισομορφισμών *δακτυλίων*. Ωστόσο, επειδή (στη Θεωρία Ομάδων) χρησιμοποιήσαμε το *ίδιο* σύμβολο *και* για τους ισομορφισμούς *ομάδων*, οφείλουμε να είμαστε ιδιάτερα προσεκτικοί (πρβλ. 8.1.3 παράδειγμα (ii)). Σε περίπτωσεις στις οποίες ενδέχεται να προκληθεί σύγχυση, θα μπορούσε κανείς να χρησιμοποιήσει τα (κάπως δυσμετακίνητα) σύμβολα $\underset{\text{δακτ.}}{\cong}$ και $\underset{\text{ομάδ.}}{\cong}$, αντιστοίχως.

ΑΠΟΔΕΙΞΗ. (i) Η ταυτοτική απεικόνιση $\mathrm{id}_R : R \to R$ είναι προφανώς ένας ισομορφισμός δακτυλίων.

(ii) Εάν ο $f : R \longrightarrow R'$ είναι ένας ισομορφισμός δακτυλίων, τότε, ως αμφιρριπτική απεικόνιση, θα διαθέτει μια (μονοσημάντως ορισμένη, αμφιρριπτική) αντίστροφο f^{-1}. Αρκεί λοιπόν να αποδειχθεί ότι η f^{-1} αποτελεί ομομορφισμό δακτυλίων. Εάν $x, y \in R'$, τότε υπάρχουν $a, b \in R$ με $x = f(a)$ και $y = f(b)$. Επομένως,

$$\begin{cases} f^{-1}(x+y) = f^{-1}(f(a)+f(b)) = f^{-1}(f(a+b)) = a+b = f^{-1}(x) + f^{-1}(y), \\ f^{-1}(xy) = f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = ab = f^{-1}(x)\, f^{-1}(y), \end{cases}$$

(αφού οι f, f^{-1} αμφιρριπτικές) και η f^{-1} είναι όντως ομομορφισμός δακτυλίων.

(iii) Εάν οι $f : R \longrightarrow R'$ και $g : R' \longrightarrow R''$ είναι δυο ισομορφισμοί δακτυλίων, τότε, σύμφωνα με την πρόταση 8.1.6, *και* η σύνθεσή τους $g \circ f$ είναι ένας ισομορφισμός δακτυλίων. □

8.1.10 Σημείωση. Σύμφωνα με την πρόταση 8.1.9, η διμελής σχέση "$\cong$" ορίζει μια σχέση ισοδυναμίας επί οιουδήποτε συνόλου απαρτιζομένου από δακτυλίους (ή επί τής NBG-«κλάσεως» *όλων* των δακτυλίων). Οι κλάσεις ισοδυναμίας ως προς την "$\cong$" ονομάζονται **κλάσεις ισομορφίας**. Δυο δακτύλιοι λογίζονται ως (δακτυλιοθεωρητικώς) *ταυτιζόμενοι* όταν είναι μεταξύ τους ισόμορφοι, ήτοι όταν ανήκουν στην ίδια κλάση ισομορφίας. Ως εκ τούτου, ο δακτυλιοθεωρητικός προσδιορισμός μιας οικογενείας δακτυλίων, τα μέλη τής οποίας έχουν μια *ειδική* ιδιότητα, ισοδυναμεί με την *ταξινόμηση* των μελών της *μέχρις ισομορφισμού*[2].

8.1.11 Πόρισμα. *Εάν οι R και R' είναι δυο δακτύλιοι και $R \cong R'$, τότε ισχύουν τα εξής:*

(i) *Ο R είναι ακεραία περιοχή $\Leftrightarrow$ ο R' είναι ακεραία περιοχή.*

(ii) *Ο R είναι στεβλό σώμα $\Leftrightarrow$ ο R' είναι στεβλό σώμα.*

(iii) *Ο R είναι σώμα $\Leftrightarrow$ ο R' είναι σώμα.*

ΑΠΟΔΕΙΞΗ. Εάν η $f : R \longrightarrow R'$ είναι ένας ισομορφισμός δακτυλίων, τότε αρκεί να εφαρμοσθεί το (ix) τής προτάσεως 8.1.5 για αμφότερες τις f και f^{-1}. (Πρβλ. με το (ii) τής προτάσεως 8.1.9.) □

8.1.12 Πρόταση. *Εάν ο $f : K \longrightarrow R$ είναι ένας ομομορφισμός δακτυλίων, όπου ο K είναι ένας διαιρετικός δακτύλιος (= στρεβλό σώμα), τότε ο f είναι ή ο μηδενικός ομομορφισμός ή ένας μονομορφισμός.*

ΑΠΟΔΕΙΞΗ. Εάν ο R είναι τετριμμένος δακτύλιος, τότε ο f είναι κατ' ανάγκην ο μηδενικός ομομορφισμός. Εάν ο R είναι μη τετριμμένος δακτύλιος και ο f δεν είναι ο μηδενικός ομομορφισμός (ήτοι δεν ισχύει $f(a) = 0_R$, *για κάθε* $a \in K$), και εάν -επιπροσθέτως- υποθέσουμε ότι $f(x) = f(y)$ για κάποια $x, y \in K$, τότε

$$f(x-y) = f(x) - f(y) = 0_R. \tag{8.2}$$

Εάν $x - y \neq 0_K$, τότε το $x - y$ θα διαθέτει πολλαπλασιαστικό αντίστροφο $(x-y)^{-1}$. Αυτό, κατά το (viii) τής προτάσεως 8.1.5, σημαίνει ότι

$$f((x-y)^{-1}) \in f(K)^{\times}, \quad f((x-y)^{-1}) = (f(x-y))^{-1}. \tag{8.3}$$

Από τις (8.2) και (8.3) συνάγεται ότι $0_R = f(x-y)(f(x-y))^{-1} = 1_R$, πράγμα άτοπο. Επομένως, $x = y$, και ο f είναι κατ' ανάγκην μονομορφισμός. □

[2] Η φράση «ταξινόμηση μέχρις ισομορφισμού» ή «με ακρίβεια ισομορφισμού» (up to isomorphism) δηλοί τη «διάκριση (δακτυλίων) με μόνο κριτήριο ταυτίσεως τη διαμεσολάβηση κάποιου ισομορφισμού».

8.1.13 Πόρισμα. *Κάθε επιμορφισμός στρεβλών σωμάτων $f : K \longrightarrow L$ είναι ισομορφισμός.*

Απόδειξη. Επειδή ο πληθικός αριθμός τού L είναι $\geqslant 2$ και ο f επιμορφισμός, ο f αδυνατεί να είναι ο τετριμμένος ομομορφισμός. Κατά συνέπειαν, ο f οφείλει να είναι *και* ενριπτικός επί τη βάσει τής προτάσεως 8.1.12. □

8.1.14 Ορισμός. Εάν ο $f : R \longrightarrow R'$ είναι ένας ομομορφισμός δακτυλίων, τότε ο υποδακτύλιος $\mathrm{Ker}(f) := f^{-1}(\{0_{R'}\})$ τού R ονομάζεται **πυρήνας** τού f.

8.1.15 Πρόταση. *Ο πυρήνας* $\mathrm{Ker}(f)$ *ενός ομομορφισμού δακτυλίων $f : R \to R'$ αποτελεί ένα ιδεώδες τού R.*

Απόδειξη. Έστω ότι $r \in R$ και ότι $a, b \in \mathrm{Ker}(f)$. Τότε

$$\left.\begin{aligned} f(a-b) = f(a) - f(b) = 0_{R'} - 0_{R'} = 0_{R'}, \\ f(ar) = f(a)f(r) = 0_{R'}f(r) = 0_{R'}, \\ f(ra) = f(r)f(a) = f(r)0_{R'} = 0_{R'} \end{aligned}\right\} \Longrightarrow a-b,\ ar,\ ra \in \mathrm{Ker}(f).$$

Άρα ο $\mathrm{Ker}(f)$ είναι εξ ορισμού ένα ιδεώδες τού R. □

8.1.16 Πρόταση. *Έστω $f : R \longrightarrow R'$ ένας ομομορφισμός δακτυλίων. Τότε ο*

$$f \text{ είναι μονομορφισμός} \iff \mathrm{Ker}\,(f) = \{0_R\}\ .$$

Απόδειξη. Εάν ο f είναι μονομορφισμός δακτυλίων και a είναι ένα τυχόν στοιχείο τού πυρήνα $\mathrm{Ker}(f)$, τότε

$$f(a) = 0_{R'} = f(0_R) \underset{f \text{ ένριψη}}{\Longrightarrow} a = 0_R.$$

Άρα $\mathrm{Ker}(f) = \{0_R\}$. Και αντιστρόφως· εάν ισχύει $\mathrm{Ker}(f) = \{0_R\}$ και υποθέσουμε ότι $f(x) = f(y)$, για κάποια $x, y \in R$, τότε

$$f(x-y) = f(x) - f(y) = 0_{R'} \Longrightarrow x - y \in \mathrm{Ker}(f) = \{0_R\} \Longrightarrow x - y = 0_R,$$

δηλαδή ο ομομορφισμός f είναι ενριπτικός. □

8.1.17 Ορισμός. Λέμε ότι ο δακτύλιος R μπορεί να **εμφυτευθεί** (ή ότι είναι **εμφυτεύσιμος**) σε έναν δακτύλιο R' όταν υπάρχει ένας μονομορφισμός δακτυλίων $f : R \longrightarrow R'$.

8.1.18 Πρόταση. *Ένας δακτύλιος R είναι εμφυτεύσιμος σε έναν δακτύλιο R' εάν και μόνον εάν ο R είναι ισόμορφος με έναν υποδακτύλιο τού R'.*

Απόδειξη. Εάν ένας δακτύλιος R είναι εμφυτεύσιμος σε έναν δακτύλιο R', τότε υφίσταται κάποιος μονομορφισμός $f : R \longrightarrow R'$. Επομένως, ο μέσω αυτού επαγόμενος επιμορφισμός $\check{f} : R \longrightarrow \mathrm{Im}(f)$ (βλ. 8.1.3 (viii)) είναι ισομορφισμός. Και αντιστρόφως· εάν ο R είναι ισόμορφος με έναν υποδακτύλιο S τού R', τότε υφίσταται κάποιος ισομορφισμός $f : R \longrightarrow S$. Θεωρώντας (κατόπιν επεκτάσεως) ως πεδίο τιμών τής απεικονίσεως f το R' λαμβάνουμε τον μονομορφισμό δακτυλίων $R \ni r \longmapsto f(r) \in R'$. □

8.1.19 Πρόταση. *Κάθε δακτύλιος R μπορεί να εμφυτευθεί (όχι μονοσημάντως) σε έναν δακτύλιο R' με μοναδιαίο στοιχείο. Μάλιστα, ο R' μπορεί να επιλεγεί κατά τέτοιον τρόπο, ώστε* $\text{χαρ}(R') = 0$ *ή* $\text{χαρ}(R') = \text{χαρ}(R)$.

Απόδειξη. Θεωρούμε το καρτεσιανό γινόμενο $R' := \mathbb{Z} \times R$, όπου $\mathbb{Z}$ ο δακτύλιος των ακεραίων αριθμών. Επί τού R' ορίζονται πράξεις προσθέσεως και πολλαπλασιασμού ως ακολούθως:

(i) $(m, a) + (n, b) := (m + n, a + b)$,

(ii) $(m, a) \cdot (n, b) := (mn, mb + na + ab)$,

για οιαδήποτε $(m, a), (n, b) \in R'$. Η τριάδα $(R', +, \cdot)$ αποτελεί έναν δακτύλιο χαρακτηριστικής 0 με μοναδιαίο του στοιχείο το $(1, 0_R)$, και η απεικόνιση

$$f : R \longrightarrow R', \quad a \longmapsto (0, a)\,,$$

είναι ένας μονομορφισμός. Εάν $\text{χαρ}(R) = k > 0$, τότε μπορούμε να θεωρήσουμε ως R' το καρτεσιανό γινόμενο $R' := \mathbb{Z}_k \times R$ εφοδιασμένο με τις πράξεις:

(i) $([m]_k\,, a) + ([n]_k\,, b) := ([m + n]_k\,, a + b)$,

(ii) $([m]_k\,, a) \cdot ([n]_k\,, b) := ([mn]_k\,, mb + na + ab)$,

για κάθε $([m]_k\,, a), ([n]_k\,, b) \in R'$. Η τριάδα $(R', +, \cdot)$ αποτελεί έναν δακτύλιο χαρακτηριστικής k με μοναδιαίο του στοιχείο το $([1]_k\,, 0_R)$, και η απεικόνιση

$$f : R \longrightarrow R', \quad a \longmapsto ([0]_k\,, a)\,,$$

είναι και πάλι ένας μονομορφισμός. □

8.1.20 Σημείωση. Πολλές φορές συμβαίνει «ειδικοί» δακτύλιοι να είναι εμφυτευμένοι σε δακτυλίους «ολιγότερο ειδικούς». Επί παραδείγματι, σώματα ενδέχεται να είναι εμφυτευμένα εντός στρεβλών σωμάτων, και ακέραιες περιοχές εντός δακτυλίων με μηδενοδιαιρέτες (βλ. 8.1.21 (i) και (ii)). Ωστόσο, όπως θα δούμε στην ενότητα 8.5 (βλ. πρόταση 8.5.7), *κάθε* ακεραία περιοχή μπορεί να εμφυτευθεί κατά τρόπο φυσικό σε ένα σώμα.

8.1.21 Παραδείγματα. (i) Το σώμα $\mathbb{C}$ των μιγαδικών αριθμών είναι εμφυτευμένο στο στρεβλό σώμα $\mathbb{H}_{\mathbb{R}}$ των (πραγματικών) τετρανίων (οπότε το $\mathbb{H}_{\mathbb{R}}$ μπορεί, υπό μία άποψη, να θεωρείται ως «φυσική επέκταση» τού $\mathbb{C}$) μέσω τού ακόλουθου μονομορφισμού:

$$\boxed{\mathbb{C} \hookrightarrow \mathbb{H}_{\mathbb{R}}, \;\; a + bi \longmapsto a\mathbf{i} + b\mathbf{j} = \begin{pmatrix} a + bi & 0 \\ 0 & a - bi \end{pmatrix},}$$

όπου οι **i** και **j** είναι οι πίνακες οι εισαχθέντες στο 6.2.19 (ii). Ως εκ τούτου, στις (φυσικές) επεκτάσεις τής παρατηρήσεως 1.10.7 προστίθεται άλλη μία:

$$\boxed{\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C} \hookrightarrow \mathbb{H}_{\mathbb{R}}.}$$

(ii) Εάν στην πρόταση 8.1.19 θέσουμε $R := \mathbb{Z}$ και $R' := \mathbb{Z} \times \mathbb{Z}$ (με τη δομή δακτυλίου την ορισθείσα κατά την αποδεικτική διαδικασία!), τότε ο R είναι ακεραία περιοχή, ενώ ο R' *δεν είναι*, διότι π.χ. για κάθε $n \in \mathbb{Z} \setminus \{0\}$ ισχύει η ισότητα:

$$(-2, 2)\,(0, 2n) = (0, 0 - 4n + 4n) = (0, 0).$$

▸ **Πηλικοδακτύλιοι και φυσικοί επιμορφισμοί**. Έστω R ένας δακτύλιος και έστω I ένα ιδεώδες αυτού. Θεωρούμε τον *πηλικοδακτύλιο* R/I (βλ. 7.6.1 και 7.6.2). Η απεικόνιση

$$\boxed{\pi_I^R : R \longrightarrow R/I, \;\; \pi_I^R(r) := r + I, \;\forall r \in R,} \tag{8.4}$$

είναι προφανώς επιριπτική.

8.1.22 Λήμμα. *H (8.4) αποτελεί έναν επιμορφισμό δακτυλίων.*

Αποδειξη. Έπεται άμεσα από τις (7.7) και (7.8). □

8.1.23 Ορισμός. Η (8.4) καλείται **φυσικός επιμορφισμός** (ή **επιμορφισμός κλάσεων υπολοίπων**) τού R επί τού πηλικοδακτυλίου R/I.

Η επόμενη πρόταση δηλοί -κατ' ουσίαν- ότι οι έννοιες «πυρήνας ομομορφισμού δακτυλίων» και «ιδεώδες» μπορούν να χρησιμοποιούνται η μία αντί τής άλλης χωρίς περαιτέρω περιορισμούς.

8.1.24 Πρόταση. *Έστω R τυχών δακτύλιος. Τότε ένα υποσύνολο $\varnothing \neq I \subseteq R$ αποτελεί ένα ιδεώδες τού R εάν και μόνον εάν το I είναι ο πυρήνας ενός ομομορφισμού δακτυλίων $f : R \longrightarrow S$ (για κάποιον κατάλληλο δακτύλιο S).*

Αποδειξη. Εάν $\varnothing \neq I \subseteq R$ είναι ένα ένα ιδεώδες τού R, τότε ο φυσικός επιμορφισμός (8.4) έχει ως πυρήνα του τον $\mathrm{Ker}(\pi_I^R) = \{r \in R \mid r + I = I\} = I$. Το αντίστροφο είναι άμεση συνέπεια τής προτάσεως 8.1.15. □

8.1.25 Πόρισμα. *Ο φυσικός επιμορφισμός (8.4) είναι ισομορφισμός εάν και μόνον εάν $I = \{0_R\}$.*

Αποδειξη. Σύμφωνα με την πρόταση 8.1.16 ο π_I^R είναι μονομορφισμός εάν και μόνον εάν ο πυρήνας του (που ισούται με το I) είναι το τετριμμένο ιδεώδες. □

8.1.26 Πόρισμα. *Εάν ο R είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Ο R είναι ένα σώμα.*

(ii) *Τα μόνα ιδεώδη τού R είναι το $\{0_R\}$ και ο ίδιος ο R.*

(iii) *Το $\{0_R\}$ είναι μεγιστικό ιδεώδες τού R.*

(iv) *Κάθε μη μηδενικός ομομορφισμός δακτυλίων $f : R \longrightarrow R'$ είναι μονομορφισμός.*

Αποδειξη. Η αμφίπλευρη συνεπαγωγή (i)⇔(ii) έπεται από το πόρισμα 7.1.11, η (i)⇔(iii) από το πόρισμα 7.6.5 (αφού $R \cong R/\{0_R\}$, βλ. 8.1.11 (iii) και 8.1.25) και η συνεπαγωγή (i)⇒(iv) από την πρόταση 8.1.12. Για την απόδειξη τής συνεπαγωγής (iv)⇒(ii) αρκεί να θεωρήσουμε *τυχόν* ιδεώδες $I \subsetneqq R$ και τον $\pi_I^R : R \longrightarrow R/I$, ο οποίος είναι μη μηδενικός με $\mathrm{Ker}(\pi_I^R) = I$. Εάν υποθέσουμε ότι ο π_I^R είναι μονομορφισμός, έχουμε $I = \{0_R\}$, οπότε ο R δεν διαθέτει άλλα γνήσια ιδεώδη πέραν τού τετριμμένου. Η απόδειξη λήγει ακολουθώντας τις συνεπαγωγές (iv)⇒(ii)⇒(i). □

8.2 ΘΕΩΡΗΜΑ ΑΝΤΙΣΤΟΙΧΙΣΕΩΣ ΙΔΕΩΔΩΝ

8.2.1 Λήμμα. *Έστω $f : R \longrightarrow S$ ένας ομομορφισμός δακτυλίων. Εάν υποτεθεί ότι το I είναι ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού R και το J ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού S, τότε ισχύουν τα ακόλουθα*:

(i) *Η εικόνα $f(I)$ τού I μέσω τού f είναι ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού δακτυλίου $f(R)$.*

(ii) *Η αντίστροφη εικόνα $f^{-1}(J)$ τού J μέσω τού f είναι ένα (αριστερό/ δεξιό/αμφίπλευρο) ιδεώδες τού R.*

Απόδειξη. (i) Θεωρούμε τυχόντα στοιχεία $s \in f(R)$ και $x, y \in f(I)$. Επειδή το I είναι (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού R, υπάρχουν $r \in R$, $a, b \in I$, τέτοια ώστε $s = f(r)$, $x = f(a)$ και $y = f(b)$, και ισχύουν τα ακόλουθα:

$$\left.\begin{array}{r} x - y = f(a) - f(b) = f(a-b) \in f(I), \\ sx = f(r)f(a) = f(ra) \in f(I) \mid\ xs = f(ar) \in f(I)\ \mid\ sx, xs \in f(I) \end{array}\right\}$$

απ' όπου έπεται ότι η εικόνα $f(I)$ τού I μέσω τού f είναι ένα (αριστερό και, αντιστοίχως, δεξιό/αμφίπλευρο) ιδεώδες τού δακτυλίου $f(R)$.

(ii) Θεωρούμε τυχόντα στοιχεία $r \in R$ και $a, b \in f^{-1}(J)$. Τότε, επειδή το J είναι (αριστερό και, αντιστοίχως, δεξιό/αμφίπλευρο) ιδεώδες τού S,

$$\left.\begin{array}{r} f(a-b) = f(a) - f(b) \in J, \\ f(ra) = f(r)f(a) \in J\ \mid\ f(ar) = f(a)f(r) \in J\ \mid\ f(ra), f(ar) \in J \end{array}\right\}$$

απ' όπου έπεται ότι $a - b,\ ra \mid\ ar \mid ra, ar \in f^{-1}(J)$. Άρα το $f^{-1}(J)$ είναι εξ ορισμού ένα ομοειδές ιδεώδες τού R. □

8.2.2 Σημείωση. Εάν υποτεθεί ότι το I είναι ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού R και ότι ο f δεν είναι επιμορφισμός, η εικόνα $f(I)$ τού I μέσω τού f είναι ένα ομοειδές ιδεώδες τού δακτυλίου $f(R)$ αλλά όχι κατ' ανάγκην και τού S. Επί παραδείγματι, θεωρώντας τή συνήθη ένθεση $\mathrm{in}_{\mathbb{Z},\mathbb{Q}} : \mathbb{Z} \hookrightarrow \mathbb{Q}$, η εικόνα τού ιδεώδους $I := 2\mathbb{Z}$ τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών μέσω αυτής είναι το υποσύνολο $2\mathbb{Z}$ τού $\mathbb{Q}$ που *δεν είναι ιδεώδες* τού σώματος των ρητών αριθμών (καθότι τα μόνα ιδεώδη τού $\mathbb{Q}$ είναι τα $\{0\}$ και $\mathbb{Q}$, βλ. πόρισμα 7.1.11).

8.2.3 Πρόταση. *Έστω I ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες ενός δακτυλίου R και έστω J ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες ενός δακτυλίου S. Για κάθε ομομορφισμό δακτυλίων $f : R \longrightarrow S$ ισχύουν τα εξής:*
(i) $f\left(I \cap f^{-1}(J)\right) = f(I) \cap J$.
(ii) $f\left(f^{-1}(J)\right) = \mathrm{Im}(f) \cap J$.
(iii) $f^{-1}(J + f(I)) = f^{-1}(J) + I$.
(iv) $f^{-1}(f(I)) = \mathrm{Ker}(f) + I$.

Απόδειξη. (i) Για κάθε $r \in f^{-1}(J)$ έχουμε $f(r) \in J$, οπότε $f\left(f^{-1}(J)\right) \subseteq J$. Επειδή οι σχέσεις εγκλεισμού παραμένουν εν ισχύ κατόπιν εφαρμογής τής απεικονίσεως f, έχουμε

$$\left.\begin{array}{r} f\left(I \cap f^{-1}(J)\right) \subseteq f(I) \\ f\left(I \cap f^{-1}(J)\right) \subseteq f\left(f^{-1}(J)\right) \end{array}\right\} \Longrightarrow f\left(I \cap f^{-1}(J)\right) \subseteq f(I) \cap J.$$

Έστω τώρα τυχόν $s \in f(I) \cap J$. Προφανώς, $s \in J$ και $s = f(r)$ για κάποιο στοιχείο $r \in I$. Επειδή $f(r) \in J$, έχουμε $s \in f\left(I \cap f^{-1}(J)\right)$, οπότε ισχύει και ο αντίστροφος εγκλεισμός

$$f(I) \cap J \subseteq f\left(I \cap f^{-1}(J)\right).$$

(ii) Αρκεί να εφαρμοσθεί το (i) στην ειδική περίπτωση όπου $I = R$.

(iii) Για κάθε $a \in I$ έχουμε $f(a) \in f(I)$. Επομένως, $I \subseteq f^{-1}(f(I))$. Από το (ii) και από το γεγονός ότι οι σχέσεις εγκλεισμού παραμένουν εν ισχύ κατόπιν θεωρήσεως αντιστρόφων εικόνων προκύπτει ότι

$$f^{-1}(J) + I \subseteq f^{-1}\left(f(f^{-1}(J) + I)\right) = f^{-1}\left(f(f^{-1}(J)) + f(I)\right) \subseteq f^{-1}(J + f(I)).$$

Έστω τώρα τυχόν $r \in f^{-1}\left(J + f(I)\right)$. Επειδή $f(r) \in J + f(I)$, υπάρχουν $s \in J$ και $b \in I$, τέτοια ώστε $f(r) = s + f(b)$. Κατά συνέπειαν,

$$f(r + (-b)) = s \in J \Rightarrow r + (-b) \in f^{-1}(s) \subseteq f^{-1}(J) \Rightarrow r \in f^{-1}(J) + I,$$

οπότε ισχύει και ο αντίστροφος εγκλεισμός

$$f^{-1}\left(J + f(I)\right) \subseteq f^{-1}(J) + I.$$

(iv) Αρκεί να εφαρμοσθεί το (iii) στην ειδική περίπτωση όπου $J = \{0_S\}$. □

8.2.4 Θεώρημα («Θεώρημα αντιστοιχίσεως ιδεωδών»). *Έστω $f : R \longrightarrow S$ ένας επιμορφισμός δακτυλίων και έστω $W := \mathrm{Ker}(f)$. Τότε η*

$$\left\{ \begin{array}{c} \text{αριστερά/δεξιά/αμφίπλευρα} \\ \text{ιδεώδη τού } R \\ \text{που περιέχουν τον } W \end{array} \right\} \xrightarrow{\alpha} \left\{ \begin{array}{c} \text{αριστερά/δεξιά/αμφίπλευρα} \\ \text{ιδεώδη τού } S \end{array} \right\}$$

η οριζόμενη από τον τύπο

$$\boxed{I \longmapsto \alpha(I) := f(I)}$$

είναι μια αμφίρριψη που διατηρεί τους εγκλεισμούς, δηλαδή για οιαδήποτε ιδεώδη I_1, I_2 τού R ισχύει η συνεπαγωγή

$$W \subseteq I_1 \subsetneqq I_2 \Longrightarrow \alpha(I_1) \subsetneqq \alpha(I_2).$$

Απόδειξη. Θεωρούμε την

$$\left\{ \begin{array}{c} \text{αριστερά/δεξιά/αμφίπλευρα} \\ \text{ιδεώδη τού } S \end{array} \right\} \xrightarrow{\beta} \left\{ \begin{array}{c} \text{αριστερά/δεξιά/αμφίπλευρα} \\ \text{ιδεώδη τού } R \\ \text{που περιέχουν τον } W \end{array} \right\}$$

την οριζόμενη από τον τύπο $J \longmapsto \beta(J) := f^{-1}(J)$. Το ότι οι α, β είναι καλώς ορισμένες απεικονίσεις έπεται από το λήμμα 8.2.1. Για κάθε (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες J τού S λαμβάνουμε

$$\alpha(\beta(J)) = \alpha(f^{-1}(J)) = f(f^{-1}(J)) = \mathrm{Im}(f) \cap J = S \cap J = J$$

(βλ. 8.2.3 (ii)). Κατά συνέπειαν,

$$\alpha(\beta(J)) = J. \tag{8.5}$$

Από την άλλη μεριά, για κάθε ιδεώδες (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες I τού R που περιέχει τον πυρήνα W τού f λαμβάνουμε

$$\beta(\alpha(I)) = \beta(f(I)) = f^{-1}(f(I)) = W + I = I$$

(βλ. 8.2.3 (iv)). Κατά συνέπειαν,

$$\beta(\alpha(I)) = I. \tag{8.6}$$

Από τις (8.5) και (8.6) συμπεραίνουμε ότι η απεικόνιση α είναι αμφιρριπτική έχουσα την β ως αντίστροφό της. Τέλος, ας υποθέσουμε ότι τα I_1, I_2 είναι δυο (αριστερά/δεξιά/αμφίπλευρα) ιδεώδη τού R τα οποία περιέχουν τον W και για τα οποία ισχύει ο εγκλεισμός $I_1 \subsetneqq I_2$. Προφανώς, $f(I_1) \subseteq f(I_2)$. Κι επειδή

$$f(I_1) = f\left(I_2\right) \Rightarrow I_1 = f^{-1}(f(I_1)) = f^{-1}(f(I_2)) = I_2,$$

έχουμε $\alpha(I_1) = f(I_1) \subsetneqq f(I_2) = \alpha(I_1)$. □

8.2.5 Πόρισμα. *Έστω I ένα ιδεώδες ενός δακτυλίου R. Τότε κάθε ιδεώδες τού πηλικοδακτυλίου R/I είναι τής μορφής J/I, όπου J κάποιο (μονοσημάντως ορισμένο) ιδεώδες τού R το οποίο περιέχει το I.*

Απόδειξη. Θεωρούμε τον φυσικό επιμορφισμό $\pi_I^R : R \longrightarrow R/I$ (βλ. (8.4)). Βάσει τού θεωρήματος 8.2.4 τής αντιστοιχίσεως ιδεωδών κάθε ιδεώδες τού R/I είναι τής μορφής $\pi_I^R(J)$, όπου J κάποιο (μονοσημάντως ορισμένο) ιδεώδες τού R το οποίο περιέχει το $I = \mathrm{Ker}(\pi_I^R)$ (βλ. πρόταση 8.1.24). Το I είναι και αυτό ένα ιδεώδες τού J (όταν το J θεωρηθεί αφ' εαυτού ως δακτύλιος αναφοράς), ενώ η εικόνα $\pi_I^R(J)$ ισούται με

$$\pi_I^R(J) = \left\{ \pi_I^R(a) \;\middle|\; a \in J \right\} = \{ a + I \mid a \in J \} = J/I,$$

απ' όπου έπεται το ζητούμενο. □

8.2.6 Παράδειγμα. Για $R = \mathbb{Z}$ και $I = m\mathbb{Z}$, $m \in \mathbb{N}$, το σύνολο των ιδεωδών τού πηλικοδακτυλίου $\mathbb{Z}/m\mathbb{Z}$ είναι το $\{ d\mathbb{Z}/m\mathbb{Z} \mid \; d \in \mathbb{N} \text{ και } d \mid m \}$.

8.3 ΘΕΩΡΗΜΑΤΑ ΙΣΟΜΟΡΦΙΣΜΩΝ

Αυτά είναι τρία χαρακτηριστικά θεωρήματα (βλ. 8.3.3, 8.3.16 και 8.3.21) τα οποία περιγράφουν τον τρόπο διασυνδέσεως των ομομορφισμών δακτυλίων, των ιδεωδών δακτυλίων και των πηλικοδακτυλίων. Τα εξ αυτών εξαγόμενα πορίσματα είναι πολυποίκιλα και λίαν χρήσιμα.

8.3.1 Λήμμα. *Εάν τα A, B είναι μη κενά σύνολα και η $\pi : A \longrightarrow B$ μια απεικόνιση, τότε τα ακόλουθα είναι ισοδύναμα*[3]:

(i) *Η π είναι επιριπτική απεικόνιση.*

(ii) *Υπάρχει κάποια απεικόνιση $\gamma : B \longrightarrow A$, ούτως ώστε να ισχύει $\pi \circ \gamma = \mathrm{id}_B$.*

(iii) *Η π είναι «εκ δεξιών διαγράψιμη», δηλαδή για οιοδήποτε μη κενό σύνολο C και οιεσδήποτε απεικονίσεις $h_1 : B \longrightarrow C$ και $h_2 : B \longrightarrow C$ ισχύει η συνεπαγωγή*

$$h_1 \circ \pi = h_2 \circ \pi \Longrightarrow h_1 = h_2.$$

Απόδειξη. (i)⇒(ii) Εάν η π είναι επιριπτική απεικόνιση, τότε για κάθε στοιχείο $y \in B = \mathrm{Im}(\pi) = \pi(A)$ επιλέγουμε ένα[4] $x_y \in A$, ούτως ώστε να ισχύει $\pi(x_y) = y$, και ορίζουμε την απεικόνιση $\gamma : B \longrightarrow A,\ y \longmapsto \gamma(y) := x_y$. Τότε

$$(\pi \circ \gamma)(y) = \pi(\gamma(y)) = \pi(x_y) = y = \mathrm{id}_B(y) \Longrightarrow \pi \circ \gamma = \mathrm{id}_B.$$

(ii)⇒(iii) Υποθέτουμε ότι υπάρχει κάποια απεικόνιση $\gamma : B \longrightarrow A$, ούτως ώστε να ισχύει $\pi \circ \gamma = \mathrm{id}_B$. Για οιεσδήποτε απεικονίσεις $h_1 : B \longrightarrow C$ και $h_2 : B \longrightarrow C$ για τις οποίες ισχύει η ισότητα $h_1 \circ \pi = h_2 \circ \pi$ λαμβάνουμε

$$\begin{aligned} h_1 \circ \pi &= h_2 \circ \pi \Rightarrow (h_1 \circ \pi) \circ \gamma = (h_2 \circ \pi) \circ \gamma \\ &\Rightarrow h_1 \circ (\pi \circ \gamma) = h_2 \circ (\pi \circ \gamma) \\ &\Rightarrow h_1 = h_1 \circ \mathrm{id}_B = h_2 \circ \mathrm{id}_B = h_2. \end{aligned}$$

(iii)⇒(i) Υποθέτουμε ότι η π είναι «εκ δεξιών διαγράψιμη». Εάν το B είναι μονοσύνολο, τότε η π είναι προδήλως επιριπτική. Εάν το B περιέχει τουλάχιστον δύο στοιχεία y_1, y_2 με $y_1 \neq y_2$, τότε ορίζουμε τις απεικονίσεις

$$h_1(y) := \begin{cases} y, & \text{όταν } y \in \mathrm{Im}(\pi), \\ y_1, & \text{όταν } y \notin \mathrm{Im}(\pi), \end{cases} \qquad h_2(y) := \begin{cases} y, & \text{όταν } y \in \mathrm{Im}(\pi), \\ y_2, & \text{όταν } y \notin \mathrm{Im}(\pi). \end{cases}$$

[3] Μια απόδειξη τής συνεπαγωγής (i)⇒(iii) έχει ήδη δοθεί στο (ii) τού λήμματος 1.2.17.

[4] Αρκεί να λάβει χώρα εφαρμογή τού *αξιώματος τής επιλογής* για την οικογένεια $\left\{ f^{-1}(\{y\}) \mid y \in B \right\}$ (μη κενών) υποσυνόλων τού A.

Προφανώς, $h_1(\pi(x)) = \pi(x) = h_2(\pi(x))$ για κάθε $x \in X$, οπότε

$$h_1 \circ \pi = h_2 \circ \pi \Longrightarrow h_1 = h_2.$$

Εάν υπήρχε κάποιο $y \in B \setminus \mathrm{Im}(\pi)$, τότε θα ίσχυε

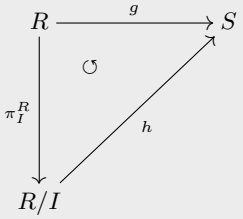
$$h_1(y) = h_2(y) \Longrightarrow y_1 = y_2,$$

ήτοι κάτι που θα αντέκειτο προς την υπόθεσή μας. Επομένως, $B = \mathrm{Im}(\pi)$. □

8.3.2 Θεώρημα («Καθολική ιδιότητα πηλικοδακτυλίου»). *Έστω I ένα ιδεώδες ενός δακτυλίου R. Τότε για κάθε ομομορφισμό δακτυλίων $g : R \longrightarrow S$ για τον οποίον ισχύει $I \subseteq \mathrm{Ker}(g)$, η*

$$\boxed{h : R/I \longrightarrow S,\ \ a + I \longmapsto h(a+I) := g(a),\ \forall a \in R,}$$

είναι καλώς ορισμένη απεικόνιση και αποτελεί έναν ομομορφισμό δακτυλίων. Αυτός είναι ο μόνος ομομορφισμός από τον πηλικοδακτύλιο R/I στον δακτύλιο S που καθιστά το διάγραμμα



μεταθετικό (ήτοι $h \circ \pi_I^R = g$). Επιπροσθέτως, ισχύουν τα ακόλουθα:

(i) *Ο h είναι μονομορφισμός $\Longleftrightarrow I = \mathrm{Ker}(g)$.*

(ii) *Ο h είναι επιμορφισμός $\Longleftrightarrow$ ο g είναι επιμορφισμός.*

Απόδειξη. Κατ' αρχάς η h είναι καλώς ορισμένη απεικόνιση, διότι εάν για κάποια $a, b \in R$ έχουμε $a + I = b + I$, τότε

$$a - b \in I \subseteq \mathrm{Ker}\,(g) \Longrightarrow g(a-b) = g(a) - g(b) = 0_{R'} \Longrightarrow g(a) = g(b).$$

Επίσης, $h \circ \pi_I^R = g$, καθότι ισχύει

$$h\left(\pi_I^R(a)\right) = h\,(a+I) = g\,(a),\ \ \forall a \in R.$$

Το ότι η h είναι και ομομορφισμός δακτυλίων συνάγεται από τις ακόλουθες ισότητες:

$$\begin{cases} h\left((a+I)+(b+I)\right) = h\left((a+b)+I\right) = g(a+b) \\ = g(a) + g(b) = h\,(a+I) + h\,(b+I)\,, \\ h\left((a+I)\,(b+I)\right) = h\,(ab+I) = g(ab) \\ = g(a)g(b) = h\,(a+I)\,h\,(b+I)\,,\ \forall (a,b) \in R \times R. \end{cases}$$

Ο ομομορφισμός h είναι ο μόνος ομομορφισμός από τον R/I στον S που καθιστά το ως άνω διάγραμμα μεταθετικό. Πράγματι· εάν $h' : R/I \longrightarrow S$ είναι *τυχών* ομομορφισμός δακτυλίων με $h' \circ \pi_I^R = g$, τότε (σύμφωνα με τη συνεπαγωγή (i)⇒(iii) τού λήμματος 8.3.1)

$$h \circ \pi_I^R = h' \circ \pi_I^R \Longrightarrow h = h'.$$

(i) Υποθέτουμε ότι ο h είναι μονομορφισμός. Έστω τυχόν $a \in \mathrm{Ker}(g)$. Τότε

$$h\,(a+I) = g(a) = 0_S = h\left(0_{R/I}\right) = h\,(I) \underset{[h\ \text{ένριψη}]}{\Longrightarrow} a + I = I \Longrightarrow a \in I.$$

Άρα $\mathrm{Ker}(g) \subseteq I$. Κι επειδή (εξ υποθέσεως) $I \subseteq \mathrm{Ker}(g)$, έχουμε $\mathrm{Ker}(g) = I$.

Και αντιστρόφως· εάν υποθέσουμε ότι $\mathrm{Ker}(g) = I$, αρκεί να δείξουμε (επί τη βάσει τής προτάσεως 8.1.16) ότι $\mathrm{Ker}(h) = \{0_{R/I}\}$. Έστω λοιπόν τυχόν $a + I \in \mathrm{Ker}(h)$. Τότε

$$g(a) = h\,(a + I) = 0_S \Longrightarrow a \in \mathrm{Ker}\,(g) = I \Longrightarrow a + I = I = 0_{R/I},$$

απ' όπου έπεται ότι πράγματι $\mathrm{Ker}(h) = \{0_{R/I}\}$.

(ii) Εάν ο h είναι επιμορφισμός, τότε και ο $g = h \circ \pi_I^R$ είναι επιμορφισμός (ως σύνθεση δύο επιμορφισμών). Και αντιστρόφως· εάν ο $g = h \circ \pi_I^R$ είναι επιμορφισμός και $s \in S$, τότε υπάρχει κάποιο $r \in R$, τέτοιο ώστε να ισχύει $g(r) = s$. Άρα το $\pi_I^R(r)$ απεικονίζεται μέσω τής h στο s και ο h είναι επιμορφισμός. □

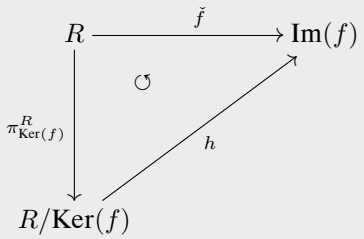
8.3.3 Πρώτο Θεώρημα Ισομορφισμών. *Έστω $f : R \longrightarrow S$ ένας ομομορφισμός δακτυλίων. Τότε*

$$\boxed{R/\mathrm{Ker}(f) \cong \mathrm{Im}\,(f) = f\,(R)\,.}$$

Συγκεκριμένα, η απεικόνιση

$$\begin{aligned} h : R/\mathrm{Ker}(f) &\longrightarrow \mathrm{Im}\,(f) = f\,(R) \\ a + \mathrm{Ker}(f) &\longmapsto h(a + \mathrm{Ker}(f)) := f\,(a)\,, \end{aligned}$$

είναι (ο μόνος) ισομορφισμός δακτυλίων που καθιστά το διάγραμμα



μεταθετικό, όπου $\check{f}$ ο επιμορφισμός ο επαγόμενος μέσω τού f (βλ. 8.1.3 (viii)).

Απόδειξη. Εφαρμόζουμε το θεώρημα 8.3.2 για το ιδεώδες $I := \mathrm{Ker}(f)$ τού R και για τον επιμορφισμό $g := \check{f}$. (Εν προκειμένω, η προϋποτεθείσα συνθήκη αυτού τού θεωρήματος ικανοποιείται, διότι $\mathrm{Ker}(f) = \mathrm{Ker}(\check{f})$.) Μάλιστα, ο κατασκευαζόμενος ομομορφισμός h είναι μονομορφισμός. Από την άλλη μεριά, η απεικόνιση h είναι, συν τοις άλλοις, και επιριπτική, καθόσον για κάθε $s \in \mathrm{Im}(f)$ υπάρχει κάποιο $r \in R$ με $s = \check{f}(r) = f(r)$, οπότε $h(r + \mathrm{Ker}(f)) = s$. □

8.3.4 Παραδείγματα. (i) Έστω $m \in \mathbb{N}$ και έστω f ο επιμορφισμός δακτυλίων

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_m, \quad n \longmapsto [n]_m\,, \quad \forall n \in \mathbb{Z}.$$

Τότε

$$\begin{aligned} \mathrm{Ker}\,(f) &= \{r \in \mathbb{Z} \mid f(r) = [0]_m\} = \{r \in \mathbb{Z} \mid [r]_m = [0]_m\} \\ &= \{r \in \mathbb{Z} \mid r = km,\ k \in \mathbb{Z}\} = \{km \mid k \in \mathbb{Z}\} = m\mathbb{Z}, \end{aligned}$$

και, σύμφωνα με το 1ο θεώρημα ισομορφισμών 8.3.3, $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$. Εξάλλου, επειδή $m\mathbb{Z} = -m\mathbb{Z}$ για κάθε $m \in \mathbb{Z} \setminus \{0\}$, έχουμε γενικότερα

$$\boxed{\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_{|m|},\ \forall m \in \mathbb{Z} \setminus \{0\}.} \tag{8.7}$$

(ii) Έστω R ο υποδακτύλιος τού $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ ο οριζόμενος ως εξής:

$$R := \left\{ \left(\begin{array}{cc} a & b \\ 0 & a \end{array} \right) \;\middle|\; a, b \in \mathbb{R} \right\},$$

και έστω f η επιρριπτική απεικόνιση

$$f : R \longrightarrow \mathbb{R}, \; \left(\begin{array}{cc} a & b \\ 0 & a \end{array} \right) \longmapsto a.$$

Τότε -όπως κανείς μπορεί εύκολα να ελέγξει- η f είναι ομομορφισμός δακτυλίων, οπότε, δυνάμει τού 1ου θεωρήματος ισομορφισμών 8.3.3,

$$\boxed{R/I \cong \mathbb{R},}$$

όπου

$$I = \mathrm{Ker}\,(f) = \left\{ \left(\begin{array}{cc} 0 & b \\ 0 & 0 \end{array} \right) \;\middle|\; b \in \mathbb{R} \right\}.$$

(iii) Έστω R ο υποδακτύλιος τού σώματος $\mathbb{Q}$ των ρητών αριθμών ο οριζόμενος ως εξής:

$$R := \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; a \in \mathbb{Z},\;\; b \in \mathbb{Z}\smallsetminus\{0\} \;\text{ και }\; \text{μκδ}\,(a,b) = 1,\;\; b \equiv 1 (\mathrm{mod}\, 2) \right\}.$$

Η επιρριπτική απεικόνιση

$$f : R \longrightarrow \mathbb{Z}_2, \;\; \tfrac{a}{b} \longmapsto f(\tfrac{a}{b}) := \left\{ \begin{array}{ll} [0]_2\,, & \text{όταν } a \equiv 0 (\mathrm{mod}\, 2), \\ [1]_2\,, & \text{όταν } a \equiv 1 (\mathrm{mod}\, 2), \end{array} \right.$$

είναι ομομορφισμός δακτυλίων και (βάσει τού θεωρήματος 8.3.3)

$$\boxed{R/\left\{ \tfrac{a}{b} \in R \;\middle|\; a \equiv 0 (\mathrm{mod}\, 2) \right\} \cong \mathbb{Z}_2.}$$

(iv) Ο επιμορφισμός δακτυλίων

$$\mathbb{Z}[\mathsf{X}] \ni \sum_{i=0}^{n} a_i \mathsf{X}^i \longmapsto a_0 \in \mathbb{Z}$$

έχει ως πυρήνα του το κύριο ιδεώδες

$$\left\{ \sum_{i=0}^{n} a_i \mathsf{X}^i \in \mathbb{Z}[\mathsf{X}] \;\middle|\; a_0 = 0 \right\} = \langle \mathsf{X} \rangle,$$

οπότε

$$\boxed{\mathbb{Z}[\mathsf{X}]/\langle \mathsf{X} \rangle \cong \mathbb{Z}.}$$

Επί τη βάσει των (i) και (iii) τού πορίσματος 8.1.11, τού θεωρήματος 7.6.4 και τού πορίσματος 7.6.5 το $\langle \mathsf{X} \rangle$ είναι πρώτο, μη μεγιστικό ιδεώδες τού $\mathbb{Z}[\mathsf{X}]$.

8.3.5 Θεώρημα (Μεταφορά ομομορφισμού σε «επίπεδο πηλικοδακτυλίων»). *Έστω $f : R \longrightarrow S$ ένας ομομορφισμός δακτυλίων. Εάν I είναι ένα ιδεώδες τού R και J ένα ιδεώδες τού S, τότε οι εξής συνθήκες είναι ισοδύναμες*:

(i) *Υφίσταται ένας και μόνον ομομορφισμός $f^{\pi\eta\lambda.} : R/I \longrightarrow S/J$ ο οποίος καθιστά το διάγραμμα*

$$\begin{array}{ccc} R & \xrightarrow{\;f\;} & S \\ {\scriptstyle \pi_I^R}\downarrow & \circlearrowleft & \downarrow{\scriptstyle \pi_J^S} \\ R/I & \xrightarrow[f^{\pi\eta\lambda.}]{} & S/J \end{array}$$

μεταθετικό, ήτοι ο «κανονιστικός» ομομορφισμός ο επαγόμενος από τον f που ορί-

ζεται από τον τύπο

$$\boxed{f^{\pi\eta\lambda.}(r+I) := f(r)+J,\ \forall r\in R.}$$

(ii) $f(I)\subseteq J$.

Επιπροσθέτως, στην περίπτωση κατά την οποία ικανοποιούνται οι ανωτέρω συνθήκες, ισχύουν τα ακόλουθα:

(a) *Ο* $f^{\pi\eta\lambda.}$ *είναι μονομορφισμός* $\Longleftrightarrow I=f^{-1}(J)$.

(b) *Ο* $f^{\pi\eta\lambda.}$ *είναι επιμορφισμός* $\Longleftrightarrow \mathrm{Im}(f)+J=S$.

Απόδειξη. Εφαρμόζουμε το θεώρημα 8.3.2 για τον ομομορφισμό $\pi_J^S\circ f$ (με τους $R, I, S/J$ στη θέση των εκεί παρατεθέντων R, I και S, αντιστοίχως, και με τον $\pi_J^S\circ f$ στη θέση τού εκεί παρατεθέντος ομομορφισμού f). Σημειωτέον ότι

$$\mathrm{Ker}(\pi_J^S\circ f)=\{r\in R\,|\,f(r)+J=J\}=\{r\in R\,|\,f(r)\in J\}=f^{-1}(J).$$

Εάν λοιπόν $(I=)\ \mathrm{Ker}(\pi_I^R)\subseteq \mathrm{Ker}(\pi_J^S\circ f)$, τότε $f(I)\subseteq f(f^{-1}(J))\subseteq J$. Και αντιστρόφως· εάν $f(I)\subseteq J$, τότε

$$I\subseteq f^{-1}(f(I))\subseteq f^{-1}(J)=\mathrm{Ker}(\pi_J^S\circ f).$$

Άρα η ανωτέρω συνθήκη (ii) ισοδυναμεί, εν προκειμένω, με τη συνθήκη τη δοθείσα στο θεώρημα 8.3.2. Εν συνεχεία, υποθέτοντας ότι ικανοποιούνται οι (i), (ii), θα αποδείξουμε τις αμφίπλευρες συνεπαγωγές (a) και (b) για τον ομομορφισμό $f^{\pi\eta\lambda.}$.

(a) Επειδή

$$\begin{aligned}\mathrm{Ker}(f^{\pi\eta\lambda.})&=\{r+I\in R/I\,|\,f(r)+J=J\}=\{r+I\in R/I\,|\,f(r)\in J\}\\&=\{r+I\in R/I\,|\,r\in f^{-1}(J)\}=f^{-1}(J)/I\end{aligned}$$

ο $f^{\pi\eta\lambda.}$ (λόγω τής προτάσεως 8.1.16) είναι μονομορφισμός $\Longleftrightarrow I=f^{-1}(J)$.

(b) Επειδή $\mathrm{Im}(f^{\pi\eta\lambda.})=\{f(r)+J\,|\,r\in R\}$, ο $f^{\pi\eta\lambda.}$ είναι επιμορφισμός εάν και μόνον εάν

$$(\forall s\in S)\,(\exists r\in R: f(r)+J=s+J)\Leftrightarrow(\forall s\in S)\,(\exists r\in R: f(r)-s\in J),$$

δηλαδή εάν και μόνον εάν $\mathrm{Im}(f)+J=S$. □

8.3.6 Πόρισμα. *Έστω ότι ο* $f: R\longrightarrow S$ *είναι ένας επιμορφισμός δακτυλίων και το* I *ένα ιδεώδες τού* R, *τέτοιο ώστε* $\mathrm{Ker}(f)\subseteq I$. *Τότε*

$$\boxed{R/I\cong S/f(I).}$$

Απόδειξη. Αρκεί να εφαρμοσθεί το θεώρημα 8.3.5. Προφανώς, ο κατασκευαζόμενος «κανονιστικός» ομομορφισμός $f^{\pi\eta\lambda.}$ είναι επιμορφισμός. Από την άλλη μεριά, επειδή

$$\left.\begin{aligned}f^{-1}(f(I))=\mathrm{Ker}(f)+I\ \ &(\text{βλ. 8.2.3 (iv)})\\ \mathrm{Ker}(f)\subseteq I\ \ &(\text{εξ υποθέσεως})\end{aligned}\right\}\Rightarrow I=f^{-1}(f(I)),$$

ο $f^{\pi\eta\lambda.}$ είναι *και* μονομορφισμός. □

8.3.7 Πόρισμα. *Έστω ότι ο* $f: R\longrightarrow S$ *είναι ένας επιμορφισμός δακτυλίων και το* J *ένα ιδεώδες τού* S. *Τότε*

$$\boxed{R/f^{-1}(J)\cong S/J.}$$

Απόδειξη. Αρκεί να εφαρμοσθεί το θεώρημα 8.3.5. (Εν προκειμένω, ο κατασκευαζόμενος «κανονιστικός» ομομορφισμός $f^{\pi\eta\lambda.}$ είναι ισομορφισμός.) □

8.3.8 Πόρισμα. *Έστω ότι ο $f : R \longrightarrow S$ είναι ένας επιμορφισμός μεταθετικών δακτυλίων με μοναδιαία στοιχεία. Τότε ισχύουν τα εξής:*

(i) *Εάν το $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες τού R που περιέχει τον πυρήνα τού f, τότε το $f(\mathfrak{p})$ είναι ένα πρώτο ιδεώδες τού S.*

(ii) *Εάν το $\mathfrak{q}$ είναι ένα πρώτο ιδεώδες τού S, τότε το $f^{-1}(\mathfrak{q})$ είναι ένα πρώτο ιδεώδες τού R που περιέχει τον πυρήνα τού f.*

ΑΠΟΔΕΙΞΗ. (i) Εάν το $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες τού δακτυλίου R που περιέχει τον πυρήνα τού f, τότε ο $R/\mathfrak{p}$ είναι ακεραία περιοχή και $R/\mathfrak{p} \cong S/f(\mathfrak{p})$ (λόγω τού θεωρήματος 7.6.4 και τού πορίσματος 8.3.6). Άρα και ο πηλικοδακτύλιος $S/f(\mathfrak{p})$ είναι ακεραία περιοχή (σύμφωνα με το (i) τού πορίσματος 8.1.11). Αυτό σημαίνει ότι το $f(\mathfrak{p})$ οφείλει να είναι πρώτο ιδεώδες τού S (εκ νέου λόγω τού θεωρήματος 7.6.4).

(ii) Εάν το $\mathfrak{q}$ είναι ένα πρώτο ιδεώδες τού δακτυλίου S, τότε ο πηλικοδακτύλιος $S/\mathfrak{q}$ είναι ακεραία περιοχή και $S/\mathfrak{q} \cong R/f^{-1}(\mathfrak{q})$ (λόγω τού θεωρήματος 7.6.4, τού πορίσματος 8.3.7 και τού (ii) τής προτάσεως 8.1.9). Άρα και ο πηλικοδακτύλιος $R/f^{-1}(\mathfrak{q})$ είναι ακεραία περιοχή (λόγω τού (i) τού πορίσματος 8.1.11). Αυτό σημαίνει ότι το $f^{-1}(\mathfrak{q})$ οφείλει να είναι πρώτο ιδεώδες τού δακτυλίου R (εκ νέου λόγω τού θεωρήματος 7.6.4). Επιπροσθέτως, $\{0_S\} \subseteq \mathfrak{q}$, οπότε $\mathrm{Ker}(f) \subseteq f^{-1}(\mathfrak{q})$. □

8.3.9 Πόρισμα (Θεώρημα αντιστοιχίσεως για πρώτα ιδεώδη).
Έστω $f : R \longrightarrow S$ ένας επιμορφισμός μεταθετικών δακτυλίων με μοναδιαία στοιχεία. Θέτουμε $W := \mathrm{Ker}(f)$ και θεωρούμε τα πρώτα φάσματα

$$\mathrm{Spec}(R) := \{\,\mathfrak{p} \mid \mathfrak{p} \text{ πρώτο ιδεώδες τού } R\}\,,\ \mathrm{Spec}(S) := \{\,\mathfrak{q} \mid \mathfrak{q} \text{ πρώτο ιδεώδες τού } S\}$$

των R και S. (Βλ. άσκηση 13 τού φυλλαδίου 12.) *Εάν $\mathrm{Spec}(S) \neq \varnothing$, τότε η*

$$\begin{array}{ccc} \mathbf{V}(W) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supseteq W\} & \longrightarrow & \mathrm{Spec}(S) \\ \mathfrak{p} & \longmapsto & f(\mathfrak{p}) \end{array} \tag{8.8}$$

είναι αμφιρριπτική απεικόνιση η οποία διατηρεί την εγκλειστική σχέση, ήτοι

$$W \subseteq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \Longrightarrow f(\mathfrak{p}_1) \subsetneq f(\mathfrak{p}_2).$$

ΑΠΟΔΕΙΞΗ. Κατά το πόρισμα 8.3.8, για κάθε $\mathfrak{p} \in \mathbf{V}(W)$ έχουμε $f(\mathfrak{p}) \in \mathrm{Spec}(S)$ και για κάθε $\mathfrak{q} \in \mathrm{Spec}(S)$ έχουμε $f^{-1}(\mathfrak{q}) \in \mathbf{V}(W)$. Επειδή $\mathfrak{p} = f^{-1}(f(\mathfrak{p}))$ για κάθε ιδεώδες $\mathfrak{p} \in \mathbf{V}(W)$ και $\mathfrak{q} = f(f^{-1}(\mathfrak{q}))$ για κάθε $\mathfrak{q} \in \mathrm{Spec}(S)$ (βλ. απόδειξη τού θεωρήματος 8.2.4), η (8.8) είναι αμφιρριπτική απεικόνιση (και μάλιστα, εκ κατασκευής, ο περιορισμός $\alpha|_{\mathbf{V}(W)}$ τής α τής ορισθείσας στο θεώρημα 8.2.4 επί τού $\mathbf{V}(W)$). Η διατήρηση τής εγκλειστικής σχέσεως αποδεικνύεται όπως στο θεώρημα 8.2.4. □

8.3.10 Σημείωση. Εάν ο $f : R \longrightarrow S$ ένας ομομορφισμός (όχι κατ' ανάγκην επιμορφισμός!) μεταθετικών δακτυλίων με μοναδιαία στοιχεία και $f(1_R) = 1_S$, τότε

$$f^{-1}(\mathfrak{q}) \in \mathrm{Spec}(R),\ \ \forall \mathfrak{q} \in \mathrm{Spec}(S),$$

οπότε, υπό την προϋπόθεση ότι $\mathrm{Spec}(S) \neq \varnothing$, ο f επάγει μια «κανονιστική» απεικόνιση (σε επίπεδο πρώτων φασμάτων):

$$\mathrm{Spec}(S) \ni \mathfrak{q} \longmapsto f^{-1}(\mathfrak{q}) \in \mathrm{Spec}(R).$$

Πράγματι· η αντίστροφη εικόνα $f^{-1}(\mathfrak{q})$ οιουδήποτε $\mathfrak{q} \in \mathrm{Spec}(S)$ είναι ένα ιδεώδες τού R (βλ. 8.2.1 (ii)), ο πηλικοδακτύλιος $S/\mathfrak{q}$ είναι ακεραία περιοχή (βλ. θεώρημα 7.6.4) και η εφαρμογή τού 1ου θεωρήματος ισομορφισμών 8.3.3 για τη σύνθεση $\pi_{\mathfrak{q}}^S \circ f$ των ομομορφισμών

$$R \xrightarrow{f} S \xrightarrow{\pi_{\mathfrak{q}}^S} S/\mathfrak{q}$$

δίδει τον ισομορφισμό

$$R/\mathrm{Ker}(\pi_{\mathfrak{q}}^S \circ f) \cong \mathrm{Im}(\pi_{\mathfrak{q}}^S \circ f) \subseteq S/\mathfrak{q}.$$

Επειδή (σύμφωνα με το (iii) τής προτάσεως 8.1.5) η εικόνα $\mathrm{Im}(\pi_{\mathfrak{q}}^S \circ f)$ είναι ένας υποδακτύλιος τής ακεραίας περιοχής $S/\mathfrak{q}$ και

$$1_{S/\mathfrak{q}} = 1_S + \mathfrak{q} = \pi_{\mathfrak{q}}^S(1_S) = \pi_{\mathfrak{q}}^S(f(1_R)) = (\pi_{\mathfrak{q}}^S \circ f)(1_R) = 1_{\mathrm{Im}(\pi_{\mathfrak{q}}^S \circ f)}$$

(βλ. 8.1.5 (v)), η πρόταση 6.2.20 μας πληροφορεί ότι η $\mathrm{Im}(\pi_{\mathfrak{q}}^S \circ f)$ είναι ακεραία περιοχή, οπότε και ο πηλικοδακτύλιος $R/\mathrm{Ker}(\pi_{\mathfrak{q}}^S \circ f)$ είναι ακεραία περιοχή (σύμφωνα με το (i) τού πορίσματος 8.1.11). Επιπροσθέτως, επειδή

$$\begin{aligned} \mathrm{Ker}(\pi_{\mathfrak{q}}^S \circ f) &= \{r \in R \mid \pi_{\mathfrak{q}}^S(f(r)) = 0_{S/\mathfrak{q}}\} \\ &= \{r \in R \mid f(r) + \mathfrak{q} = \mathfrak{q}\} \\ &= \{r \in R \mid f(r) \in \mathfrak{q}\} = f^{-1}(\mathfrak{q}), \end{aligned}$$

ο πηλικοδακτύλιος $R/f^{-1}(\mathfrak{q})$ είναι μια ακεραία περιοχή, οπότε έχουμε κατ' ανάγκην $f^{-1}(\mathfrak{q}) \in \mathrm{Spec}(R)$ (βλ. θεώρημα 7.6.4).

8.3.11 Πόρισμα. *Έστω I ένα γνήσιο ιδεώδες ενός μεταθετικού δακτυλίου R με μοναδιαίο στοιχείο. Τότε κάθε πρώτο ιδεώδες τού πηλικοδακτυλίου R/I είναι τής μορφής $\mathfrak{p}/I$, όπου $\mathfrak{p}$ κάποιο (μονοσημάντως ορισμένο) πρώτο ιδεώδες τού R το οποίο περιέχει το I.*

Απόδειξη. Έπεται άμεσα από τα πορίσματα 8.3.9 και 8.2.5. □

8.3.12 Πόρισμα. *Έστω ότι ο $f : R \longrightarrow S$ είναι ένας επιμορφισμός μεταθετικών δακτυλίων με μοναδιαία στοιχεία. Τότε ισχύουν τα εξής:*

(i) *Εάν το $\mathfrak{m}$ είναι ένα μεγιστικό ιδεώδες τού R που περιέχει τον πυρήνα τού f, τότε το $f(\mathfrak{m})$ είναι ένα μεγιστικό ιδεώδες τού S.*

(ii) *Εάν το $\mathfrak{m}'$ είναι ένα μεγιστικό ιδεώδες τού S, τότε το $f^{-1}(\mathfrak{m}')$ είναι ένα μεγιστικό ιδεώδες τού R που περιέχει τον πυρήνα τού f.*

Απόδειξη. (i) Εάν το $\mathfrak{m}$ είναι ένα μεγιστικό ιδεώδες τού R που περιέχει τον πυρήνα τού f, τότε ο πηλικοδακτύλιος $R/\mathfrak{m}$ είναι σώμα και $R/\mathfrak{m} \cong S/f(\mathfrak{m})$ (λόγω των πορισμάτων 7.6.5 και 8.3.6). Άρα και ο πηλικοδακτύλιος $S/f(\mathfrak{m})$ είναι σώμα (βλ. το (iii) τού πορίσματος 8.1.11). Αυτό σημαίνει ότι το $f(\mathfrak{m})$ οφείλει να είναι μεγιστικό ιδεώδες τού S (εκ νέου λόγω τού πορίσματος 7.6.5).

(ii) Εάν το $\mathfrak{m}'$ είναι ένα μεγιστικό ιδεώδες τού S, τότε ο πηλικοδακτύλιος $S/\mathfrak{m}'$ είναι σώμα και $S/\mathfrak{m}' \cong R/f^{-1}(\mathfrak{m}')$ (λόγω των πορισμάτων 7.6.5 και 8.3.6, και τού (ii) τής προτάσεως 8.1.9). Άρα και ο πηλικοδακτύλιος $R/f^{-1}(\mathfrak{m}')$ είναι σώμα (βλ. το (iii) τού πορίσματος 8.1.11). Αυτό σημαίνει ότι το $f^{-1}(\mathfrak{m}')$ οφείλει να είναι μεγιστικό ιδεώδες τού R (εκ νέου λόγω τού πορίσματος 7.6.5). Επιπροσθέτως, $\{0_S\} \subseteq \mathfrak{m}'$, οπότε $\mathrm{Ker}(f) \subseteq f^{-1}(\mathfrak{m}')$. □

Εν συνεχεία, παραθέτουμε ένα πόρισμα ανάλογο τού 8.3.9 *για μεγιστικά ιδεώδη*.

8.3.13 Πόρισμα (Θεώρημα αντιστοιχίσεως για μεγιστικά ιδεώδη). *Έστω $f : R \longrightarrow S$ ένας επιμορφισμός μεταθετικών δακτυλίων με μοναδιαία στοιχεία. Θέτουμε $W := \mathrm{Ker}(f)$ και θεωρούμε τα **μεγιστικά φάσματα***

$$\text{Max-Spec}(R) := \left\{ \mathfrak{m} \;\middle|\; \begin{array}{c}\mathfrak{m}\text{ μεγιστικό}\\ \text{ιδεώδες τού } R\end{array} \right\},\quad \text{Max-Spec}(S) := \left\{ \mathfrak{n} \;\middle|\; \begin{array}{c}\mathfrak{n}\text{ μεγιστικό}\\ \text{ιδεώδες τού } S\end{array} \right\}$$

των R και S. Εάν ο S είναι μη τετριμμένος, τότε η

$$\boxed{\begin{array}{ccc}\{\mathfrak{m} \in \text{Max-Spec}(R) \,|\mathfrak{m} \supseteq W\ \} & \longrightarrow & \text{Max-Spec}(S)\\ \mathfrak{m} & \longmapsto & f(\mathfrak{m})\end{array}} \tag{8.9}$$

είναι αμφιρριπτική απεικόνιση η οποία διατηρεί την εγκλειστική σχέση, ήτοι

$$W \subseteq \mathfrak{m}_1 \subsetneqq \mathfrak{m}_2 \Longrightarrow f(\mathfrak{m}_1) \subsetneqq f(\mathfrak{m}_2).$$

Απόδειξη. Κατά το πόρισμα 8.3.12, η εικόνα $f(\mathfrak{m})$ είναι ένα μεγιστικό ιδεώδες τού δακτυλίου S για κάθε μεγιστικό ιδεώδες $\mathfrak{m}$ τού R με $\mathfrak{m} \supseteq W$ και το $f^{-1}(\mathfrak{m}')$ είναι μεγιστικό ιδεώδες τού R περιέχον τον W για κάθε μεγιστικό ιδεώδες $\mathfrak{m}'$ τού S. Επειδή $\mathfrak{m} = f^{-1}(f(\mathfrak{m}))$ για κάθε μεγιστικό ιδεώδες $\mathfrak{m}$ τού R με $\mathfrak{m} \supseteq W$ και $\mathfrak{m}' = f(f^{-1}(\mathfrak{m}'))$ για κάθε μεγιστικό ιδεώδες $\mathfrak{m}'$ τού S (βλ. απόδειξη τού θεωρήματος 8.2.4), η (8.9) είναι αμφιρριπτική απεικόνιση (και μάλιστα, εκ κατασκευής, ο περιορισμός τής α τής ορισθείσας στο θεώρημα 8.2.4 επί τού συνόλου των μεγιστικών ιδεωδών τού R που περιέχουν τον W). Η διατήρηση τής εγκλειστικής σχέσεως αποδεικνύεται όπως στο θεώρημα 8.2.4. □

8.3.14 Σημείωση. Έστω $f : R \longrightarrow S$ ένας ομομορφισμός μεταθετικών δακτυλίων με μοναδιαία στοιχεία και $f(1_R) = 1_S$. Εάν ο f δεν είναι επιμορφισμός, τότε, σε αντίθεση με ό,τι συμβαίνει στην περίπτωση θεωρήσεως αντιστρόφων εικόνων πρώτων ιδεωδών (βλ. 8.3.10), η αντίστροφη εικόνα ενός μεγιστικού ιδεώδους τού S μέσω τού f δεν είναι κατ' ανάγκην μεγιστικό ιδεώδες τού R. Επί παραδείγματι, θεωρώντας τή συνήθη ένθεση $\mathrm{in}_{\mathbb{Z},\mathbb{Q}} : \mathbb{Z} \hookrightarrow \mathbb{Q}$, παρατηρούμε ότι η $\mathrm{in}_{\mathbb{Z},\mathbb{Q}}$ είναι μονομορφισμός, δεν είναι επιμορφισμός, $\mathrm{in}_{\mathbb{Z},\mathbb{Q}}(1) = 1$, το τετριμμένο ιδεώδες $\{0\}$ τού $\mathbb{Q}$ είναι μεγιστικό (βλ. πόρισμα 7.1.11), αλλά η αντίστροφη εικόνα $\mathrm{in}^{-1}_{\mathbb{Z},\mathbb{Q}}(\{0\}) = \{0\}$ τού $\{0\}$ είναι το τετριμμένο ιδεώδες τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών που *δεν είναι μεγιστικό ιδεώδες* (βλ. 7.5.16 (i)).

8.3.15 Πόρισμα. *Έστω I ένα γνήσιο ιδεώδες ενός μεταθετικού δακτυλίου R με μοναδιαίο στοιχείο. Τότε κάθε μεγιστικό ιδεώδες τού πηλικοδακτυλίου R/I είναι τής μορφής $\mathfrak{m}/I$, όπου $\mathfrak{m}$ κάποιο (μονοσημάντως ορισμένο) μεγιστικό ιδεώδες τού R το οποίο περιέχει το I.*

Απόδειξη. Έπεται άμεσα από τα πορίσματα 8.3.13 και 8.2.5. □

8.3.16 Δεύτερο Θεώρημα Ισομορφισμών. *Έστω ότι ο R είναι ένας δακτύλιος, ο S ένας υποδακτύλιος τού R και το I ένα ιδεώδες τού R. Τότε*

(i) *το $S \cap I$ είναι ένα ιδεώδες τού S,*

(ii) *το $S + I := \{\, s + a \mid s \in S,\ a \in I\}$ είναι ένας υποδακτύλιος τού R με $S \subseteq S + I$,*

(iii) *το I είναι ένα ιδεώδες τού $S + I$ και*

(iv) *υφίσταται ισομορφισμός δακτυλίων*

$$\boxed{S/(S \cap I) \cong (S + I)/I.}$$

Απόδειξη. (i) Επειδή το I είναι ένα ιδεώδες τού R, έχουμε

$$\{0_S\} = \{0_R\} \subseteq S \cap I \subseteq S.$$

Επίσης, το $S \cap I$ αποτελεί προσθετική υποομάδα τής (αβελιανής) ομάδας $(S, +)$. Έστω τώρα τυχόν $a \in S \cap I$. Προφανώς, $a \in S$ και $a \in I$. Επειδή $a \in S$ και ο S είναι υποδακτύλιος τού R, ισχύει

$$sa \in S, \;\; as \in S, \; \forall s \in S,$$

λόγω τής κλειστότητας τής πράξεως τού πολλαπλασιασμού εντός τού S. Από την άλλη μεριά, επειδή το I είναι ιδεώδες τού R,

$$sa \in I, \;\; as \in I.$$

Επομένως, $sa, as \in S \cap I$ για κάθε $s \in S$ και κάθε $a \in S \cap I$. Εξ αυτών έπεται ότι το $S \cap I$ είναι ένα ιδεώδες τού S.

(ii) Εάν $s \in S$, τότε προφανώς $s + 0_R \in S + I$, αφού $0_R \in I$. Άρα $S \subseteq S + I$. Εν συνεχεία, ας υποθέσουμε ότι $x_1, x_2 \in S + I$. Τα x_1, x_2 γράφονται ως $x_1 = s_1 + a_1$ και $x_2 = s_2 + a_2$, για κάποια $s_1, s_2 \in S$ και $a_1, a_2 \in I$. Επομένως,

$$\left.\begin{aligned} x_1x_2 = s_1s_2 + s_1a_2 + a_1s_2 + a_1a_2, \\ s_1s_2 \in S, \\ s_1a_2 + a_1s_2 + a_1a_2 \in I \end{aligned}\right\} \Longrightarrow x_1x_2 \in S + I,$$

και

$$\left.\begin{aligned} x_1 - x_2 = (s_1 - s_2) + (a_1 - a_2)\,, \\ s_1 - s_2 \in S, \\ a_1 - a_2 \in I \end{aligned}\right\} \Longrightarrow x_1 - x_2 \in S + I.$$

Άρα τελικώς το $S + I$ είναι ένας υποδακτύλιος τού R με $S \subseteq S + I$.

(iii) Έστω ότι $a, b \in I$ και $x = s + c \in S + I$, όπου $s \in S$ και $c \in I$. Τότε ο ισχυρισμός είναι αληθής λόγω τής συνεπαγωγής:

$$\left.\begin{aligned} a - b \in I \;\; (\text{διότι το } I \text{ είναι ιδεώδες τού } R) \\ sa \in I \;\; (\text{διότι } s \in R \text{ και το } I \text{ είναι ιδεώδες τού } R) \\ ca \in I \;\; (\text{διότι το } I \text{ είναι υποδακτύλιος τού } R) \end{aligned}\right\} \Longrightarrow a - b, \;\; xa \in I.$$

(iv) Έστω f η απεικόνιση

$$f : S \longrightarrow (S + I)/I, \;\; s \longmapsto s + I, \;\; \forall s \in S.$$

Προφανώς, $f = \pi_I^{S+I} \circ j$, όπου $\pi_I^{S+I} : S + I \longrightarrow (S + I)/I$ ο επιμορφισμός κλάσεων υπολοίπων και $j : S \longrightarrow S + I$ η συνήθης ένθεση $s \longmapsto s\,(+0_R)$. Κατά το 1ο θεώρημα ισομορφισμών 8.3.3, $S/\mathrm{Ker}(f) \cong f(S)$. Θα αποδείξουμε εν πρώτοις ότι $\mathrm{Ker}(f) = S \cap I$. Έστω λοιπόν τυχόν $s \in \mathrm{Ker}(f)$. Τότε

$$\left.\begin{aligned} f(s) = s + I = 0_R + I \Longrightarrow s \in I \\ s \in S \end{aligned}\right\} \Longrightarrow s \in S \cap I.$$

Και αντιστρόφως· εάν $s \in S \cap I$, τότε $f(s) = s + I = 0_R + I = I \Longrightarrow s \in \mathrm{Ker}(f)$. Άρα πράγματι $\mathrm{Ker}(f) = S \cap I$. Ως εκ τούτου, αρκεί να αποδειχθεί η ισότητα:

$f(S) = (S + I)/I$ (ήτοι ότι η f είναι επιρριπτική). Έστω τυχόν $b + I \in (S + I)/I$. Τότε $b = s + a$, για κάποια $s \in S$ και $a \in I$. Επομένως,

$$I \ni (s + a) - s = a \Longrightarrow f(s) = s + I = s + a + I = b + I,$$

πράγμα που επιβεβαιώνει την επιρριπτικότητα τής f. □

8.3.17 Πόρισμα. *Έστω ότι ο R είναι ένας δακτύλιος και τα I, J δύο ιδεώδη του. Τότε υφίστανται ισομορφισμοί*:

$$\boxed{I/(I \cap J) \cong (I + J)/J}$$

και

$$\boxed{(I + J)/(I \cap J) \cong ((I + J)/I) \times ((I + J)/J) \cong (J/(I \cap J)) \times (I/(I \cap J)).}$$

Απόδειξη. Ο πρώτος ισομορφισμός είναι άμεσος δυνάμει τού 2ου θεωρήματος ισομορφισμών 8.3.16. Για την απόδειξη των άλλων δύο ισομορφισμών ορίζουμε την

$$f : I + J \longrightarrow ((I + J)/I) \times ((I + J)/J), \quad a \longmapsto (a + I, a + J), \ \forall a \in I + J.$$

Είναι εύκολος ο έλεγχος τού ότι η f αποτελεί ομομορφισμό δακτυλίων. Ο πυρήνας της ισούται προφανώς με

$$\begin{aligned} \mathrm{Ker}(f) &= \{a \in I + J \mid f(a) = 0_{((I+J)/I)\times((I+J)/J)}\} \\ &= \{a \in I + J \mid (a + I, a + J) = (I, J)\} \\ &= \{a \in I + J \mid a \in I, \ a \in J\} = I \cap J. \end{aligned}$$

Εν συνεχεία, θα δείξουμε ότι η f είναι επιρριπτική. Έστω τυχόν

$$(a + I, b + J) \in ((I + J)/I) \times ((I + J)/J).$$

Τότε τα a, b γράφονται ως αθροίσματα $a = u+v$, $b = w+z$, για κατάλληλα $u, w \in I$ και $v, z \in J$. Κατά συνέπειαν,

$$\begin{aligned} f(v) &= (v + I, v + J) = (v + I, 0_{I+J} + J), \\ f(w) &= (w + I, w + J) = (0_{I+J} + I, w + J), \end{aligned}$$

απ' όπου συμπεραίνουμε ότι

$$f(v + w) = f(v) + f(w) = (v + I, w + J) = (u + v + I, w + z + J) = (a + I, b + J),$$

δηλαδή ότι η f είναι επιμορφισμός με $\mathrm{Ker}(f) = I \cap J$. Αρκεί η εφαρμογή τού 1ου θεωρήματος ισομορφισμών. Τέλος, ο τρίτος -κατά σειράν- ισομορφισμός έπεται κατόπιν απευθείας εφαρμογής τού 2ου θεωρήματος ισομορφισμών 8.3.16 σε αμφότερους τους παράγοντες τού μετέχοντος καρτεσιανού γινομένου δακτυλίων. □

8.3.18 Παράδειγμα. Εάν $R = \mathbb{Z}$ και $I = \langle m \rangle$, $J = \langle n \rangle$, όπου $m, n \in \mathbb{Z} \setminus \{0\}$, τότε, λαμβάνοντας υπ' όψιν τα όσα αποδείξαμε στα 7.4.13 (i), (ii), οι ισομορφισμοί οι θεσπισθέντες μέσω τού πορίσματος 8.3.17 γράφονται υπό τη μορφή:

$$\langle m \rangle / \langle \text{εκπ}(m,n) \rangle \cong \langle \text{μκδ}(m, n) \rangle / \langle n \rangle$$

και, αντιστοίχως,

$$\begin{aligned} \langle \text{μκδ}(m, n) \rangle / \langle \text{εκπ}(m,n) \rangle &\cong (\langle \text{μκδ}(m, n) \rangle / \langle m \rangle) \times (\langle \text{μκδ}(m, n) \rangle / \langle n \rangle) \\ &\cong (\langle n \rangle / \langle \text{εκπ}(m,n) \rangle) \times (\langle m \rangle / \langle \text{εκπ}(m,n) \rangle). \end{aligned}$$

8.3.19 Ορισμός. Εάν τα I, J είναι δυο ιδεώδη ενός δακτυλίου R και ισχύει η ισότητα $R = I + J$, τότε λέμε ότι τα I και J είναι **συμπρώτα**.

8.3.20 Πόρισμα. *Εάν τα I, J είναι συμπρώτα ιδεώδη ενός δακτυλίου R, τότε*

$$R/(I \cap J) \cong (R/I) \times (R/J).$$

8.3.21 Τρίτο Θεώρημα Ισομορφισμών. *Εάν ο R είναι ένας δακτύλιος και τα I, J γνήσια ιδεώδη τού R με $I \subseteq J$, τότε έχουμε*

$$R/J \cong (R/I)\ /\ (J/I).$$

Απόδειξη. Έστω f η απεικόνιση

$$f : R \longrightarrow (R/I)\ /\ (J/I)\ ,\ \ a \longmapsto (a+I)+(J/I),\ \forall a \in R.$$

Επειδή $f = \pi^{R/I}_{J/I} \circ \pi^R_I$, όπου $\pi^R_I : R \longrightarrow (R/I)$ και $\pi^{R/I}_{J/I} : R/I \longrightarrow (R/I)\ /\ (J/I)$ οι φυσικοί επιμορφισμοί, η f είναι ένας επιμορφισμός δακτυλίων. Σύμφωνα με το 1ο θεώρημα ισομορφισμών 8.3.3,

$$R/\mathrm{Ker}\,(f) \cong (R/I)\ /\ (J/I)\ .$$

Όμως

$$\begin{aligned}
\mathrm{Ker}(f) &= \left\{a \in R \mid\ f(a) = 0_{(R/I)\,/\,(J/I)}\right\} \\
&= \left\{a \in R \mid\ \pi^{R/I}_{J/I}(\pi^R_I(a)) = 0_{(R/I)\,/\,(J/I)}\right\} \\
&= \left\{a \in R \mid\ \pi^{R/I}_{J/I}(a+I) = 0_{(R/I)\,/\,(J/I)}\right\} \\
&= \left\{a \in R \mid\ a+I \in \mathrm{Ker}(\pi^{R/I}_{J/I})\right\} \\
&= \{a \in R \mid\ a+I \in (J/I)\} = J,
\end{aligned}$$

απ' όπου έπεται το ζητούμενο. □

8.3.22 Παράδειγμα. Εάν $R = \mathbb{Z}$ και $I = \langle 12\rangle = 12\mathbb{Z} \subsetneq J = \langle 3\rangle = 3\mathbb{Z}$, τότε, επειδή το ιδεώδες $3\mathbb{Z}/12\mathbb{Z}$ τού δακτυλίου $\mathbb{Z}/12\mathbb{Z}$ περιέχει εκείνες τις κλάσεις υπολοίπων τού $\mathbb{Z}/12\mathbb{Z}$, οι εκπρόσωποι των οποίων ανήκουν στο $J = 3\mathbb{Z}$, ήτοι είναι πολλαπλάσια τού 3, έχουμε $J/I = \{I,\ 3+I,\ 6+I,\ 9+I\}$ και

$$(\mathbb{Z}/I)\ /\ (J/I) = \{k + I + (J/I) \mid\ k \in \mathbb{Z},\ \ 0 \leqslant k \leqslant 11\}\,.$$

Σημειωτέον ότι υπάρχουν πολλαπλές εμφανίσεις μεταξύ αυτών των δώδεκα στοιχείων, καθότι

$$(k_1+I)-(k_2+I) \in J/I \Longleftrightarrow (k_1-k_2)+I \in J/I \Longleftrightarrow 3 \mid k_1-k_2.$$

Ως εκ τούτου, ο δακτύλιος $(\mathbb{Z}/I)\ /\ (J/I)$ συνίσταται από ακριβώς τρεις σαφώς διακεκριμένες κλάσεις ισοτιμίας:

$$(\mathbb{Z}/I)\ /\ (J/I) = \{k + I + (J/I) \mid\ k \in \mathbb{Z},\ \ 0 \leqslant k \leqslant 2\}\,.$$

Κατά το 1ο και το 3ο θεώρημα ισομορφισμών (βλ. 8.3.3 και 8.3.21),

$$\mathbb{Z}_3 = \{[0]_3\,, [1]_3\,, [2]_3\} \cong \mathbb{Z}/3\mathbb{Z} \xrightarrow{\cong} (\mathbb{Z}/I)\ /\ (J/I) = \{(J/I, 1+(J/I), 2+(J/I)\}.$$

8.4 ΕΦΑΡΜΟΓΗ: ΛΥΣΕΙΣ ΣΥΣΤΗΜΑΤΩΝ ΓΡΑΜΜΙΚΩΝ ΙΣΟΤΙΜΙΩΝ

Στην ενότητα 8.3 παρετέθησαν ορισμένα πρώτα παραδείγματα εφαρμογής των θεωρημάτων ισομορφισμών δακτυλίων (βλ. 8.3.4, 8.3.18 και 8.3.22). Εδώ θα παρουσιασθεί μια επιπρόσθετη, αρκούντως σημαντική εφαρμογή *αριθμοθεωρητικής φύσεως* σχετιζόμενη με τον προσδιορισμό τού συνόλου των λύσεων συστημάτων πεπερασμένου πλήθους γραμμικών ισοτιμιών (με έναν άγνωστο). Το κύριο θεώρημα τής παρούσας ενότητας είναι το 8.4.4, το επονομαζόμενο *Κινέζικο θεώρημα*[5] ή *θεώρημα τού Νικομάχου τού Γερασηνού*[6], για το οποίο δίδουμε μια καθαρώς «δακτυλιοθεωρητική» απόδειξη (αν και στη γενίκευσή του 8.4.9 δεν παραλείπουμε και την παράθεση μιας πιο «στοιχειώδους» προσβάσεως).

▸ **Συστήματα γραμμικών ισοτιμιών**. Έστω $k \in \mathbb{N}$, $k \geqslant 2$. Δοθέντων k φυσικών αριθμών $m_1, \ldots, m_k$ μεγαλυτέρων τού 1, k μη μηδενικών ακεραίων αριθμών $a_1, \ldots, a_k$ και k ακεραίων αριθμών $b_1, \ldots, b_k$, υπό ποίες συνθήκες είναι το σύστημα των γραμμικών ισοτιμιών

$$\left\{ \begin{array}{c} a_1 x \equiv b_1 \,(\mathrm{mod}\ m_1) \\ \vdots \\ a_k x \equiv b_k \,(\mathrm{mod}\ m_k) \end{array} \right\}$$

επιλύσιμο; Και πώς, πληρουμένων των εν λόγω συνθηκών, είναι δυνατόν να προσδιορισθεί επακριβώς το σύνολο λύσεων αυτού; (Ένας ακέραιος αριθμός x (και αντιστοίχως, η κλάση ισοτιμίας αυτού ως προς κατάλληλο μόδιο) καλείται **λύση** τού ανωτέρω συστήματος όταν ο x (και αντιστοίχως, η κλάση ισοτιμίας τού x ως προς κατάλληλο μόδιο) είναι λύση καθεμιάς εκ των ισοτιμιών του.) Κατά την πορεία που θα ακολουθήσουμε προκειμένου να καταλήξουμε σε πλήρεις απαντήσεις σε αυτά τα ερωτήματα (μέσω τού θεωρήματος 8.4.11) θα χρησιμοποιήσουμε κατάλληλους *ισομορφισμούς δακτυλίων*.

8.4.1 Λήμμα. *Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Εάν $n \in \mathbb{N}$, $n \geqslant 2$, και εάν τα $I_1, I_2, \ldots, I_n$ είναι ανά δύο συμπρώτα ιδεώδη τού R, ήτοι τέτοια, ώστε*

$$I_j + I_k = R,\ \forall\,(j,k) \in \mathbb{N}^2,\ 1 \leqslant j,k \leqslant n,\ \ j \neq k,$$

τότε

$$R = I_j + \bigcap_{1 \leqslant k \leqslant n,\ k \neq j} I_k,\ \ \forall j \in \mathbb{N},\ \ 1 \leqslant j \leqslant n.$$

Απόδειξη. Θα κάνουμε χρήση μαθηματικής επαγωγής ως προς τον n. Για $n = 2$ ο ισχυρισμός είναι προφανώς αληθής. Υποθέτουμε λοιπόν ότι είναι αληθής και για κάποιον $n = l \geqslant 2$ και εξετάζουμε την περίπτωση όπου $n = l + 1$. Επειδή ο R είναι δακτύλιος με μοναδιαίο στοιχείο, έχουμε[7] $R = RR$. Κατά συνέπειαν, για

[5] Παρότι στη βιβλιογραφία είναι γνωστό ως *Chinese remainder theorem,* πιθανολογείται πως οι Κινέζοι μαθηματικοί τού 3ου μ.Χ. αιώνα, οι οποίοι έδωσαν μια πρακτική μέθοδο επιλύσεως ενός συστήματος τριών γραμμικών ισοτιμιών, είχαν λάβει γνώση τού έργου τού Νικομάχου τού Γερασηνού, αφού το εν λόγω σύστημα περιέχει τους ίδιους αριθμούς με εκείνους τού Νικομάχου! (Άλλοι πάλι ιστορικοί υιοθετούν την αντίθετη εκδοχή, υποστηρίζοντας *είτε* ότι ο Sun-Tsu είχε ζήσει όχι τον 3ο αλλά τον 1ο μ.Χ. αιώνα και ότι αντιγραφεύς ήταν ο Νικόμαχος, *είτε* ότι το παράρτημα που αποδίδεται στον Νικόμαχο εγράφη περί τον 6ο μ.Χ. αιώνα από τον Ιωάννη τον Φιλόπονο. Την αλήθεια μάλλον δεν θα την μάθουμε ποτέ!) Η πρώτη ολοκληρωμένη απόδειξη τού θεωρήματος 8.4.4 οφείλεται στον L. Euler, ενώ μια νεότερη απόδειξη ανακαλύφθηκε (μάλλον ανεξαρτήτως) από τον C.-F. Gauss περί το έτος 1801.

[6] Ο φιλόσοφος και μαθηματικός *Νικόμαχος ο Γερασηνός* (από τα Γέρασα, μια αρχαιοελληνική πόλη στην Παλαιστίνη, 30 μίλια νοτιοανατολικά τής λίμνης Τιβεριάδος, ιδρυθείσα από τον Μ. Αλέξανδρο) θα πρέπει -εξ όσων γνωρίζουμενα έζησε σε κάποιο διάστημα μεταξύ τού μέσου τού 1ου και τού μέσου τού 2ου μ.Χ. αιώνα. Πέραν τής γνωστής του «Αριθμητικής Εισαγωγής» είχε συγγράψει και πολλά άλλα έργα, εκ των οποίων ελάχιστα τμήματα διεσώθησαν. Σε ένα συμπλήρωμα αυτής παρατίθεται (εν είδει παραρτήματος) η λύση τού συστήματος των ισοτιμιών $x \equiv 2 (\mathrm{mod}\, 3)$, $x \equiv 3 (\mathrm{mod}\, 5)$ και $x \equiv 2 (\mathrm{mod}\, 7)$. (Για να την προσδιορίσετε, εφαρμόστε τό 8.4.4!)

[7] Για δακτύλιους χωρίς μοναδιαίο κάτι τέτοιο δεν ισχύει εν γένει! Επί παραδείγματι, $(2\mathbb{Z})\,(2\mathbb{Z}) \subsetneq (2\mathbb{Z})$.

κάθε $j \in \mathbb{N}$, $1 \leqslant j \leqslant l+1$,

$$R = RR = \left(I_j + \bigcap_{1 \leqslant k \leqslant l,\ k \neq j} I_k \right) (I_j + I_{l+1}) \subseteq I_j + \bigcap_{1 \leqslant k \leqslant l+1,\ k \neq j} I_k,$$

με τη δεύτερη ισότητα ισχύουσα λόγω επαγωγικής υποθέσεως και την επακόλουθη εγκλειστική σχέση απορρέουσα από την πρόταση 7.4.5 (ii). Επειδή όμως το δεξιό μέλος εμπεριέχεται στον R, έχουμε $R = I_j + \bigcap_{1 \leqslant k \leqslant l+1,\ k \neq j} I_k$. □

8.4.2 Θεώρημα. *Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Εάν $n \in \mathbb{N}$, $n \geqslant 2$, και εάν τα $I_1, I_2, \ldots, I_n$ είναι ανά δύο συμπρώτα ιδεώδη τού R, ήτοι τέτοια ώστε*

$$I_j + I_k = R,\ \forall\, (j,k) \in \mathbb{N}^2,\ 1 \leqslant j,k \leqslant n,\ \ j \neq k,$$

τότε έχουμε

$$\boxed{R/\bigcap_{j=1}^{n} I_j \cong (R/I_1) \times \cdots \times (R/I_n)\,.}$$

Απόδειξη. Για $n = 2$ ο ισχυρισμός είναι αληθής επί τη βάσει τού πορίσματος 8.3.20. Εάν υποτεθεί ότι $n \geqslant 3$ και ότι αυτός είναι αληθής για $n-1$ όρους, τότε μέσω μαθηματικής επαγωγής και εφαρμογής τού λήμματος 8.4.1 (για $j = n$) λαμβάνουμε

$$R/\bigcap_{j=1}^{n} I_j = R/(\bigcap_{j=1}^{n-1} I_j \cap I_n) \underset{8.3.20}{\cong} \left(R/\bigcap_{j=1}^{n-1} I_j \right) \times R/I_n \underset{(\text{επαγ. υπ.})}{\cong} (R/I_1) \times \cdots \times (R/I_n)\,.$$

Δευτερη Απόδειξη. Αυτή η απόδειξη είναι καθαρώς *κατασκευαστική*. Για κάθε $j \in \{1, \ldots, n\}$ ορίζουμε την απεικόνιση

$$f : R \longrightarrow (R/I_1) \times \cdots \times (R/I_n)$$

$$r \longmapsto f(r) := (\pi^R_{I_1}(r)\,, .., \pi^R_{I_n}(r)) = (r + I_1, .., r + I_n)\,.$$

Η f είναι προφανώς ομομορφισμός δακτυλίων και $\mathrm{Ker}(f) = \bigcap_{j=1}^{n} I_j$. Θα δείξουμε ότι η f είναι και *επιρριπτική*. Έστω $\mathbf{y} = (y_1, \ldots, y_n) \in (R/I_1) \times \cdots \times (R/I_n)$. Επειδή κάθε $\pi^R_{I_j}$ είναι επιρριπτική απεικόνιση, υπάρχει $x_j \in R$, τέτοιο ώστε $\pi^R_{I_j}(x_j) = y_j$. Κατά το λήμμα 8.4.1,

$$\left[(\exists\, u_j \in I_j) \ \text{ και } \ (\exists\, v_j \in \bigcap_{1 \leqslant k \leqslant n,\ k \neq j} I_k) : u_j + v_j = 1_R \right].$$

Ως εκ τούτου, $v_j - 1_R \in I_j$ και $v_j \in I_k, \forall k \in \{1, \ldots, n\} \setminus \{j\}$, απ' όπου έπεται ότι

$$\pi^R_{I_k}(v_j) = v_j + I_k = \begin{cases} 1_R + I_k, & \text{όταν } \ k = j, \\ I_k, & \text{όταν } \ k \neq j. \end{cases}$$

Συνεπώς,

$$\begin{aligned} f\left(\sum_{j=1}^{n} x_j v_j \right) &= \left(\pi^R_{I_1}(\sum_{j=1}^{n} x_j v_j), \ldots, \pi^R_{I_n}(\sum_{j=1}^{n} x_j v_j) \right) \\ &= \left(\pi^R_{I_1}(x_1), \ldots, \pi^R_{I_n}(x_n) \right) = \mathbf{y}, \end{aligned} \tag{8.10}$$

και η f είναι όντως επιρριπτική. Αρκεί λοιπόν να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών 8.3.3, ούτως ώστε να εισπράξουμε έναν «απτό» ισομορφισμό

$$\begin{aligned} R/\bigcap_{j=1}^{n} I_j &\xrightarrow{\cong} (R/I_1)\times\cdots\times(R/I_n) \\ r+\bigcap_{j=1}^{n} I_j &\longmapsto f(r)=(r+I_1,\ldots,r+I_n) \end{aligned} \tag{8.11}$$

μεταξύ των δύο θεωρηθέντων πηλικοδακτυλίων. □

8.4.3 Πόρισμα. *Έστω n ένας φυσικός αριθμός $\geqslant 2$ και έστω*

$$n = p_1^{\nu_1} p_2^{\nu_2}\cdots p_k^{\nu_k},\ k\in\mathbb{N},$$

η κανονική παράσταση τού n ως γινομένου σαφώς διακεκριμένων πρώτων αριθμών $p_1,\ldots,p_k$, υψωμένων σε κατάλληλες δυνάμεις $\nu_1,\ldots,\nu_k\in\mathbb{N}$. Τότε έχουμε

$$\boxed{\mathbb{Z}/(n\mathbb{Z}) \cong \mathbb{Z}/(p_1^{\nu_1}\mathbb{Z})\times\cdots\times\mathbb{Z}/(p_k^{\nu_k}\mathbb{Z})\,.}$$

Απόδειξη. Εάν $k=1$, τούτο είναι προφανές. Έστω ότι $k\geqslant 2$ και ότι $I_j := p_j^{\nu_j}\mathbb{Z}$ για κάθε $j\in\{1,\ldots,k\}$. Επειδή

$$\text{μκδ}(p_j^{\nu_j}, p_l^{\nu_l}) = 1,\ \forall\,(j,l)\in\mathbb{N}^2,\ 1\leqslant j,l\leqslant k,\ \ j\neq l,$$

υπάρχουν $\lambda,\mu\in\mathbb{Z}$ με $\lambda p_j^{\nu_j}+\mu p_l^{\nu_l}=1$. Αυτό σημαίνει ότι για κάθε $x\in\mathbb{Z}$ έχουμε

$$x = x\lambda p_j^{\nu_j} + x\mu p_l^{\nu_l} \in I_j + I_l.$$

Άρα $I_j+I_l=\mathbb{Z},\ \forall\,(j,l)\in\mathbb{N}^2,\ 1\leqslant j,l\leqslant k,\ \ j\neq l$. Εν συνεχεία, θα αποδείξουμε ότι $n\mathbb{Z}=\bigcap_{j=1}^{k} I_j$. Έστω τυχόν $x\in\langle n\rangle = n\mathbb{Z}$. Τότε $x=\lambda p_1^{\nu_1}p_2^{\nu_2}\cdots p_k^{\nu_k}$ για κάποιο $\lambda\in\mathbb{Z}$, οπότε

$$[x\in I_j,\ \ \forall j\in\{1,\ldots,k\}] \Longrightarrow x\in\bigcap_{j=1}^{k} I_j.$$

Και αντιστρόφως· εάν $x\in\bigcap_{j=1}^{k} I_j$, τότε $x=\mu_1 p_1^{\nu_1}=\cdots=\mu_k p_k^{\nu_k}$ για κάποια $\mu_1,\ldots,\mu_k\in\mathbb{Z}$. Συνεπώς,

$$\left.\begin{array}{r} p_j^{\nu_j}\,|\,x,\quad \forall j\in\{1,\ldots,k\} \\ p_1,\ldots,p_k \\ \text{σαφώς διακεκριμένοι} \end{array}\right\} \Longrightarrow n=\prod_{j=1}^{k} p_j^{\nu_j}\,\Big|\,x \Longrightarrow x\in\langle n\rangle = n\mathbb{Z}.$$

Αρκεί λοιπόν να εφαρμόσουμε το θεώρημα 8.4.2. □

8.4.4 Πόρισμα (Κινέζικο Θεώρημα ή Θεώρημα τού Νικομάχου τού Γερασηνού). *Έστω $k\in\mathbb{N}$, $k\geqslant 2$. Δοθέντων k φυσικών αριθμών $m_1,\ldots,m_k$ μεγαλυτέρων τού 1 και k ακεραίων αριθμών $b_1,\ldots,b_k$, για τους οποίους ισχύει*

$$\text{μκδ}\,(m_j,m_l)=1,\ \forall\,(j,l)\in\mathbb{N}^2,\ 1\leqslant j,l\leqslant n,\ \ j\neq l,$$

το σύστημα των γραμμικών ισοτιμιών

$$\left\{\begin{array}{c} x\equiv b_1 (\text{mod } m_1) \\ \vdots \\ x\equiv b_k (\text{mod } m_k) \end{array}\right\} \tag{8.12}$$

είναι επιλύσιμο. Μάλιστα, εάν το x_0 είναι μια λύση τού (8.12), τότε αυτή είναι μονοσημάντως ορισμένη κατά μόδιο $m := \prod_{j=1}^{k} m_j$. *Ως εκ τούτου, το σύνολο των λύσεων τού συστήματος (8.12) είναι η κλάση υπολοίπων*[8]

$$x_0 + m\mathbb{Z} \ \ (\in \mathbb{Z}/\,(m\mathbb{Z})).$$

Απόδειξη. Εάν για κάθε φυσικό αριθμό n και κάθε πρώτο αριθμό p ορίσουμε ως

$$\boldsymbol{\nu}_p\,(n) := \left\{ \begin{array}{l} \text{τον εκθέτη τής μεγίστης δυνατής} \\ \text{δυνάμεως τού } p \text{ που διαιρεί τον } n \end{array} \right\} \in \mathbb{N}_0,$$

τότε, σύμφωνα με το πόρισμα 8.4.3,

$$\mathbb{Z}/\,(m\mathbb{Z}) \cong \prod_{p \text{ πρώτος},\ p|m_1} \mathbb{Z}/(p^{\boldsymbol{\nu}_p(m_1)}\mathbb{Z}) \times \cdots \times \prod_{p \text{ πρώτος},\ p|m_k} \mathbb{Z}/(p^{\boldsymbol{\nu}_p(m_k)}\mathbb{Z}),$$

και επειδή

$$m_j = \prod_{p \text{ πρώτος},\ p|m_j} p^{\boldsymbol{\nu}_p(m_j)}, \ \ \forall j \in \{1, \ldots, k\},$$

συμπεραίνουμε ότι $\mathbb{Z}/\,(m\mathbb{Z}) \cong \mathbb{Z}/(m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/(m_k\mathbb{Z})$. Εάν, μάλιστα, λάβει κανείς υπ' όψιν το 8.4.3 και τον (8.11), ο *τύπος ορισμού* αυτού τού ισομορφισμού είναι γνωστός, ήτοι ο

$$\mathbb{Z}/\,(m\mathbb{Z}) \ni \lambda + m\mathbb{Z} \longmapsto (\lambda + m_1\mathbb{Z}, \ldots, \lambda + m_k\mathbb{Z}) \in \mathbb{Z}/(m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/(m_k\mathbb{Z}). \quad (8.13)$$

Ιδιαιτέρως, το $(b_1 + m_1\mathbb{Z}, \ldots, b_k + m_k\mathbb{Z}) \in \mathbb{Z}/(m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/(m_k\mathbb{Z})$ διαθέτει ένα *μονοσημάντως ορισμένο αρχέτυπο*

$$x_0 + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$$

(κατά μόδιο m, όπου $x_0 \in \mathbb{Z}$), μέσω τού (8.13), οπότε έχουμε

$$x_0 + m_j\mathbb{Z} = b_j + m_j\mathbb{Z}, \ \forall j \in \{1, ..., k\},$$

ήτοι k ισότητες που ισοδυναμούν με τη λύση τού (8.12) κατά μόδιο m. □

8.4.5 Σημείωση. Για την εύρεση μιας λύσεως x_0 τού συστήματος (8.12) αρκεί, για κάθε δείκτη $j \in \{1, ..., k\}$, να προσδιορισθούν

$$u_j \in \langle m_j \rangle, \ \ v_j \in \langle m'_j \rangle = \bigcap_{1 \leqslant l \leqslant k,\ l \neq j} \langle m_l \rangle,$$

όπου $m'_j := \prod_{1 \leqslant l \leqslant k,\ l \neq j} m_l$, τέτοια ώστε $u_j + v_j = 1$, ή -ισοδυνάμως- $(y_j, z_j) \in \mathbb{Z}^2$, τέτοια ώστε

$$m_j y_j + m'_j z_j = 1, \ \forall j \in \{1, ..., k\}.$$

Επειδή όμως δεν θα χρειασθούμε ουσιαστικώς τα y_j, αρκεί να προσδιορίσουμε τη *μοναδική* κατά μόδιο m_j *λύση* $z_j \in \mathbb{Z}$ τής ισοτιμίας $m'_j z_j \equiv 1 (\text{mod } m_j)$ βάσει των όσων προαναφέραμε στη σημείωση 2.4.46. Εάν, επί παραδείγματι, εργασθούμε με το θεώρημα τού Euler, τότε μπορούμε να θέσουμε $z_j := {m'_j}^{\phi(m_j)-1}$. Από τα δεδομένα μας (βλ. (8.10), (8.11) και (8.13)) έπεται ότι το

$$\boxed{x_0 = \sum_{j=1}^{k} \frac{b_j z_j m}{m_j} = \sum_{j=1}^{k} b_j m'_j z_j = \sum_{j=1}^{k} b_j {m'_j}^{\phi(m_j)}} \quad (8.14)$$

-ανηγμένο κατά μόδιο m- είναι μια λύση τού συστήματος ισοτιμιών (8.12), ενώ κάθε άλλη λύση του προκύπτει κατόπιν αθροίσεως (σε αυτό) ενός ακεραίου πολλαπλασίου τού m.

[8] Εν προκειμένω, μπορούμε να *ταυτίζουμε* την $x_0 + m\mathbb{Z} \ \in \mathbb{Z}/\,(m\mathbb{Z})$ με την κλάση ισοτιμίας $[x_0]_m \in \mathbb{Z}_m$ μέσω τού ισομορφισμού (8.7).

8.4.6 Παράδειγμα. Το σύνολο των λύσεων τού συστήματος γραμμικών ισοτιμιών

$$\left\{\begin{array}{l} x \equiv 1 (\mathrm{mod}\ 3) \\ x \equiv 2 (\mathrm{mod}\ 4) \\ x \equiv 3 (\mathrm{mod}\ 5) \end{array}\right\}$$

είναι η κλάση υπολοίπων $58 + 60\mathbb{Z}$ $(\in \mathbb{Z}/60\mathbb{Z})$, διότι (κατά τον τύπο (8.14))

$$\begin{aligned} x_0 &= 1 \cdot 20^{\phi(3)} + 2 \cdot 15^{\phi(4)} + 3 \cdot 12^{\phi(5)} = 1 \cdot 20^2 + 2 \cdot 15^2 + 3 \cdot 12^4 \\ &= 1 \cdot 400 + 2 \cdot 225 + 3 \cdot 20\,736 = 63\,058 \equiv 58 (\mathrm{mod}\ 60). \end{aligned}$$

Τα τρία θεωρήματα 8.4.9, 8.4.10 και 8.4.11 που ακολουθούν αποτελούν γενικεύσεις τού 8.4.4. Μέσω αυτών το πρόβλημα τής ευρέσεως τού συνόλου των λύσεων συστημάτων γραμμικών ισοτιμιών (με έναν άγνωστο) αντιμετωπίζεται σε *πλήρη γενικότητα*.

8.4.7 Λήμμα. *Εάν $m_1, m_2 \in \mathbb{N}$ και $b_1, b_2 \in \mathbb{Z}$, τότε υπάρχει ακέραιος αριθμός x με $x \equiv b_1 (\mathrm{mod}\ m_1)$ και $x \equiv b_2 (\mathrm{mod}\ m_2)$ εάν και μόνον εάν* μκδ $(m_1, m_2) \mid b_2 - b_1$.

Απόδειξη. Εάν $x \in \mathbb{Z}$ με $x \equiv b_1 \,(\mathrm{mod}\ m_1)$ και $x \equiv b_2 \,(\mathrm{mod}\ m_2)$, τότε

$$\left.\begin{array}{l} m_1 \mid x - b_1 \\ m_2 \mid x - b_2 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} \text{μκδ}\,(m_1, m_2) \mid x - b_1 \\ \text{μκδ}\,(m_1, m_2) \mid x - b_2 \end{array}\right\} \Longrightarrow \text{μκδ}\,(m_1, m_2) \mid x - b_1 - (x - b_2)\,.$$

Και αντιστρόφως· εάν $d := \text{μκδ}(m_1, m_2)$ και $d \mid b_2 - b_1$, γράφοντας τον d ως ακέραιο γραμμικό συνδυασμό $d = k_1 m_1 + k_2 m_2,\ k_1, k_2 \in \mathbb{Z}$, και θέτοντας $\nu := \frac{k_1 (b_2 - b_1)}{d}$, λαμβάνουμε

$$m_1 \nu \equiv (d - k_2 m_2)\, \tfrac{(b_2 - b_1)}{d} \equiv b_2 - b_1 \,(\mathrm{mod}\, m_2)\,,$$

οπότε για τον ακέραιο αριθμό $x := b_1 + m_1 \nu$ ισχύουν οι ισοτιμίες $x \equiv b_1 (\mathrm{mod}\ m_1)$ και $x \equiv b_1 + (b_2 - b_1) \equiv b_2 (\mathrm{mod}\ m_2)$. □

8.4.8 Λήμμα. *Έστω $k \in \mathbb{N}, k \geqslant 2$. Δοθέντων k φυσικών αριθμών $m_1, \ldots, m_k$ έχουμε*

$$\text{μκδ}\,(\text{εκπ}\,(m_1, \ldots, m_{k-1}), m_k) = \text{εκπ}\,(\text{μκδ}\,(m_1, m_k), \ldots, \text{μκδ}\,(m_{k-1}, m_k))\,.$$

Απόδειξη. Είναι εύκολος ο έλεγχος τού ότι για οιουσδήποτε μη αρνητικούς ακεραίους $\alpha_1, \ldots, \alpha_k$ ισχύει η ισότητα

$$\min\{\max\{\alpha_1, ..., \alpha_{k-1}\}, \alpha_k\} = \max\{\min\{\alpha_1, \alpha_k\}, \min\{\alpha_2, \alpha_k\}, ..., \min\{\alpha_{k-1}, \alpha_k\}\}.$$

Μέσω αυτής και των (2.24) και (2.26) έπεται άμεσα η ζητούμενη. □

8.4.9 Θεώρημα. *Έστω $k \in \mathbb{N}, k \geqslant 2$. Δοθέντων k φυσικών αριθμών $m_1, \ldots, m_k$ μεγαλυτέρων τού 1 και k ακεραίων αριθμών $b_1, \ldots, b_k$, το σύστημα των γραμμικών ισοτιμιών*

$$\left\{\begin{array}{c} x \equiv b_1 (\mathrm{mod}\ m_1) \\ \vdots \\ x \equiv b_k (\mathrm{mod}\ m_k) \end{array}\right\} \tag{8.15}$$

είναι επιλύσιμο εάν και μόνον εάν

$$\text{μκδ}\,(m_j, m_l) \mid b_j - b_l,\ \ \forall\,(j,l) \in \mathbb{N}^2,\ 1 \leqslant j, l \leqslant k,\ \ j \neq l. \tag{8.16}$$

Μάλιστα, εάν $m := \text{εκπ}\,(m_1, m_2, ..., m_k)$ και εάν το $x_0,\ 0 \leqslant x_0 \leqslant m - 1$, είναι μια λύση τού (8.15), τότε αυτή είναι μονοσημάντως ορισμένη κατά μόδιο m. *Ως εκ τούτου, όταν ικανοποιούνται οι συνθήκες (8.16), το σύνολο των λύσεων τού συστήματος (8.15) είναι η κλάση υπολοίπων $x_0 + m\mathbb{Z}$ $(\in \mathbb{Z}/\,(m\mathbb{Z}))$.*

Απόδειξη. (i) Έστω x_0 μια λύση τού (8.15). Τότε για κάθε $j, l \in \{1, \dots, k\}$ με $j \neq l$ έχουμε

$$\left.\begin{array}{c} x_0 \equiv b_j \,(\mathrm{mod}\ m_j) \\ x_0 \equiv b_l \,(\mathrm{mod}\ m_l) \end{array}\right\} \Longrightarrow \left.\begin{array}{c} m_j \mid x_0 - b_j \\ m_l \mid x_0 - b_l \end{array}\right\} \Longrightarrow \left.\begin{array}{c} \mu\kappa\delta\,(m_j, m_l) \mid x_0 - b_j \\ \mu\kappa\delta\,(m_j, m_l) \mid x_0 - b_l \end{array}\right\} \Longrightarrow (8.16).$$

Και αντιστρόφως· ας υποθέσουμε την ισχύ των συνθηκών (8.16).

Εργαζόμενοι επαγωγικώς θα κατασκευάσουμε για κάθε $j \in \{1, \dots, k\}$ έναν ακέραιο αριθμό y_j, ούτως ώστε να ισχύουν οι ισοτιμίες

$$\left\{\begin{array}{c} y_j \equiv b_1 (\mathrm{mod}\ m_1) \\ \vdots \\ y_j \equiv b_j (\mathrm{mod}\ m_j) \end{array}\right\}.$$

Κατ' αρχάς ορίζουμε ως y_1 έναν εκπρόσωπο τής κλάσεως υπολοίπων $[b_1]_{m_1}$. Εάν $j \in \{1, \dots, k-1\}$ και υποθέσουμε ότι οι ακέραιοι $y_1, \dots, y_j$ έχουν ήδη ορισθεί, κατασκευάζουμε κατάλληλο ακέραιο y_{j+1} ως ακολούθως: Επειδή

$$y_j \equiv b_l \,(\mathrm{mod}\ m_l), \quad \forall l \in \{1, \dots, j\},$$

έχουμε

$$[m_l \mid y_j - b_l,\ \forall l \in \{1, \dots, j\}] \Longrightarrow [\mu\kappa\delta\,(m_l, m_{j+1}) \mid y_j - b_l,\ \forall l \in \{1, \dots, j\}]\,.$$

Εξ υποθέσεως,

$$\mu\kappa\delta\,(m_l, m_{j+1}) \mid b_l - b_{j+1},\ \forall l \in \{1, \dots, j\}.$$

Άρα

$$\mu\kappa\delta\,(m_l, m_{j+1}) \mid (y_j - b_l) + (b_l - b_{j+1}) = y_j - b_{j+1},\ \forall l \in \{1, \dots, j\}$$

και, ως εκ τούτου,

$$\varepsilon\kappa\pi\,(\mu\kappa\delta\,(m_1, m_{j+1}), \dots, \mu\kappa\delta\,(m_j, m_{j+1})) \mid y_j - b_{j+1}.$$

Εφαρμόζοντας λοιπόν το λήμμα 8.4.8 συμπεραίνουμε ότι

$$\mu\kappa\delta\,(\varepsilon\kappa\pi\,(m_1, \dots, m_j), m_{j+1}) \mid y_j - b_{j+1}.$$

Κατά συνέπειαν, βάσει τού λήμματος 8.4.7 υπάρχει ένας $y_{j+1} \in \mathbb{Z}$, τέτοιος ώστε

$$y_{j+1} \equiv y_j \,(\mathrm{mod}\ \varepsilon\kappa\pi\,(m_1, \dots, m_j)) \qquad y_{j+1} \equiv b_{j+1} \,(\mathrm{mod}\ m_{j+1}),$$

οπότε

$$[m_l \mid \varepsilon\kappa\pi\,(m_1, .., m_j),\ \forall l \in \{1, .., j\}] \Longrightarrow y_{j+1} \equiv y_j \equiv b_l \,(\mathrm{mod}\ m_l), \forall l \in \{1, .., j\}.$$

(ii) Έστω τώρα $m := \varepsilon\kappa\pi(m_1, m_2, ..., m_k)$ και έστω x_0 ο (μοναδικός) εκπρόσωπος τής κλάσεως υπολοίπων $[y_k]_m$ με $0 \leqslant x_0 < m$. Εάν ο x είναι ένας ακέραιος αριθμός, ο οποίος πληροί τις k ισοτιμίες (8.15), τότε έχουμε

$$[x \equiv b_\ell \equiv x_0 \,(\mathrm{mod}\ m_\ell), \forall \ell \in \{1, \dots, k\}],$$

οπότε

$$[m_\ell \mid x_0 - x,\ \forall \ell \in \{1, \dots, k\}] \Longrightarrow m \mid x_0 - x \Longrightarrow x_0 - x \in m\mathbb{Z}.$$

Και αντιστρόφως· εάν $x \in \mathbb{Z}$ και $x \equiv x_0 \,(\mathrm{mod}\ m)$, τότε έχουμε προφανώς για κάθε $\ell \in \{1, \dots, k\}$: $x \equiv b_\ell \equiv x_0 \,(\mathrm{mod}\ m_\ell)$. □

Μέσω τού θεωρήματος[9] 8.4.10 αποδεικνύεται ότι ο προσδιορισμός τής μοναδικής κατά μόδιο m λύσεως *τού συστήματος* (8.15) ανάγεται στον προσδιορισμό τής μοναδικής κατά μόδιο m λύσεως *μίας και μόνον γραμμικής ισοτιμίας* (8.17).

[9] Πρβλ. O. Ore: *The General Chinese Remainder Theorem*, The American Math. Monthly **59** (1952), no. 6, 365-370, F.T. Howard: *A Generalized Chinese Remainder Theorem*, The College Mathematics Journal **33** (2002), no. 4, 279-282.

8.4.10 Θεώρημα. *Διατηρώντας τά δεδομένα τού θεωρήματος* 8.4.9 *και προϋποθέτοντας ότι για το σύστημα των γραμμικών ισοτιμιών* (8.15) *πληρούνται οι συνθήκες* (8.16)*, θεωρούμε φυσικούς αριθμούς* $n_1, n_2, ..., n_k$*, τέτοιους ώστε να ισχύουν τα ακόλουθα*[10]:

(i) $n_j \mid m_j, \ \ \forall j \in \{1, \dots, k\}$,

(ii) $\mu\kappa\delta\,(n_j, n_l) = 1, \ \ \forall\,(j,l) \in \mathbb{N}^2, \ 1 \leqslant j, l \leqslant k, \ \ j \neq l$,

(iii) $m := \epsilon\kappa\pi\,(m_1, m_2, ..., m_k) = n_1 n_2 \cdots n_k$

και θέτουμε $N_j := \frac{m}{n_j}, \ \ \forall j \in \{1, \dots, k\}$. *Η γραμμική ισοτιμία*

$$\boxed{(N_1 + N_2 + \cdots + N_k)x \equiv (b_1 N_1 + b_2 N_2 + \cdots + b_k N_k) \,(\mathrm{mod}\ m)} \tag{8.17}$$

διαθέτει ακριβώς μία λύση κατά μόδιο m. *Επιπροσθέτως, ένας ακέραιος αριθμός* x_0 *αποτελεί τη μοναδική κατά μόδιο* m *λύση τής* (8.17) *εάν και μόνον εάν αυτός αποτελεί τη μοναδική κατά μόδιο* m *λύση τού συστήματος γραμμικών ισοτιμιών* (8.15).

Απόδειξη. Κατ' αρχάς η (8.17) διαθέτει ακριβώς μία λύση κατά μόδιο m, διότι

$$\mu\kappa\delta\,(N_1 + N_2 + \cdots + N_k, m) = 1. \tag{8.18}$$

(Βλ. πόρισμα 2.4.45.) Πράγματι· εάν p είναι ένας πρώτος αριθμός που διαιρεί το m, τότε $p \mid n_j$ για κάποιο $j \in \{1, \dots, k\}$ και λόγω τής ιδιότητας (ii) έχουμε: $p \mid N_l$ για κάθε $l \in \{1, \dots, k\}$ με $l \neq j$ και $p \nmid N_j$. Αυτό σημαίνει ότι

$$p \nmid N_1 + N_2 + \cdots + N_k$$

και ότι, ως εκ τούτου, η (8.18) είναι αληθής.

Εν συνεχεία θεωρούμε έναν ακέραιο αριθμό x_0 για τον οποίο υποθέτουμε ότι αποτελεί τη μοναδική κατά μόδιο m λύση τής (8.17). Αρκεί να δειχθεί ότι ο x_0 αποτελεί λύση *και* τού συστήματος γραμμικών ισοτιμιών (8.15). Για οιονδήποτε παγιωμένον δείκτη $j \in \{1, \dots, k\}$ έχουμε

$$b_1 N_1 + b_2 N_2 + \cdots + b_k N_k = b_j (N_1 + N_2 + \cdots + N_k) + \sum_{l \in \{1,\dots,k\} \smallsetminus \{j\}} (b_l - b_j) N_l. \tag{8.19}$$

Για κάθε $l \in \{1, \dots, k\} \smallsetminus \{j\}$ ισχύει $m_j \mid m = n_l N_l$. Επομένως,

$$\left.\begin{array}{r} \frac{m_j}{\mu\kappa\delta(m_j,n_l)} \mid \frac{n_l}{\mu\kappa\delta(m_j,n_l)} N_l \\ \mu\kappa\delta\left(\frac{m_j}{\mu\kappa\delta(m_j,n_l)}, \frac{n_l}{\mu\kappa\delta(m_j,n_l)}\right) = 1 \text{ (Βλ. 2.2.14 (ii).)} \end{array}\right\} \overset{2.2.9}{\Longrightarrow} \frac{m_j}{\mu\kappa\delta(m_j,n_l)} \mid N_l,$$

[10] Προσοχή! Οι $n_1, n_2, ..., n_k$ με τις ιδιότητες (i), (ii) και (iii) *δεν είναι κατ' ανάγκην* μονοσημάντως ορισμένοι. Εντούτοις, *υπάρχουν πάντοτε* $n_1, n_2, ..., n_k$ με αυτές τις ιδιότητες. Μια *συγκεκριμένη επιλογή* φυσικών αριθμών $n_1, n_2, ..., n_k$ (που έχουν τις ιδιότητες (i), (ii) και (iii)) γίνεται ως εξής: Έστω p τυχών πρώτος αριθμός. Εάν για οιονδήποτε $\xi \in \mathbb{N}$ υποτεθεί ότι $\boldsymbol{\nu}_p(\xi)$ είναι ο (μη αρνητικός ακέραιος) εκθέτης τής *μεγίστης δυνατής* δυνάμεως τού p που διαιρεί τον ξ, τότε *υπάρχει τουλάχιστον ένας* $j \in \{1, \dots, k\}$ με $\boldsymbol{\nu}_p(m) = \boldsymbol{\nu}_p(m_j)$. (Βλ. (2.26).) Αρκεί να θέσουμε για κάθε πρώτο αριθμό p που διαιρεί το m,

$$\mathbf{t}_p := \min\{j \in \{1, ..., k\} \,|\boldsymbol{\nu}_p(m) = \boldsymbol{\nu}_p(m_j)\},$$

και για κάθε $j \in \{1, ..., k\}$, $A_j := \{p \,|p \text{ πρώτος διαιρέτης τού } m_j \text{ με } \mathbf{t}_p = j\}$, και να ορίσουμε τον

$$n_j := \begin{cases} \prod\limits_{p \in A_j} p^{\boldsymbol{\nu}_p(m)}, & \text{όταν } A_j \neq \varnothing, \\ 1, & \text{όταν } A_j = \varnothing. \end{cases}$$

Επί παραδείγματι, εάν $m_1 = 30 = 2 \cdot 3 \cdot 5$, $m_2 = 252 = 2^2 \cdot 3^2 \cdot 7$, $m_3 = 3920 = 2^4 \cdot 5 \cdot 7^2$, τότε $m = 35280 = 2^4 \cdot 3^2 \cdot 5 \cdot 7^2$, $\mathbf{t}_2 = 3$, $\mathbf{t}_3 = 2$, $\mathbf{t}_5 = 1$ και $\mathbf{t}_7 = 3$, οπότε $A_1 = \{5\}$, $A_2 = \{2\}$, $A_3 = \{2, 7\}$ και $n_1 = 5$, $n_2 = 3^2$, $n_3 = 2^4 \cdot 7^2$.

απ' όπου συμπεραίνουμε ότι

$$\exists \lambda \in \mathbb{Z} : (b_l - b_j)N_l = \lambda(b_l - b_j)\tfrac{m_j}{\text{μκδ}(m_j,n_l)}. \tag{8.20}$$

Εξάλλου,

$$\left.\begin{array}{r} [\text{μκδ}\,(m_j,n_l) \mid n_l \text{ κα } n_l \mid m_l] \Rightarrow \text{μκδ}\,(m_j,n_l) \mid m_l \\ \text{μκδ}\,(m_j,n_l) \mid m_j \end{array}\right\} \underset{2.2.6}{\Longrightarrow} \text{μκδ}\,(m_j,n_l) \mid \text{μκδ}(m_j,m_l)$$

και επειδή $\text{μκδ}(m_j,m_l) \mid b_l - b_j$ (βλ. (8.16)), η (8.20) δίδει

$$\tfrac{\text{μκδ}(m_j,m_l)}{\text{μκδ}(m_j,n_l)} \in \mathbb{Z} \Longrightarrow m_j \mid (b_l - b_j)N_l, \ \ \forall l \in \{1,\dots,k\}. \tag{8.21}$$

Από τις (8.19), (8.21) και το (i) τής προτάσεως 2.4.4 έπεται ότι

$$b_1N_1 + b_2N_2 + \cdots + b_kN_k \equiv b_j(N_1 + N_2 + \cdots + N_k)\,(\text{mod } m_j)\,, \ \forall j \in \{1,\dots,k\}. \tag{8.22}$$

Επειδή η συνεπαγωγή "$\Longleftarrow$" τής προτάσεως 2.4.8 (εφαρμοζόμενη στην (8.17) για $x = x_0$) δίδει

$$(N_1 + N_2 + \cdots + N_k)x_0 \equiv (b_1N_1 + b_2N_2 + \cdots + b_kN_k)\,(\text{mod } m_j)\,, \ \forall j \in \{1,\dots,k\}, \tag{8.23}$$

αντικαθιστώντας τό αριστερό μέλος τής (8.22) με το αριστερό μέλος τής (8.23) λαμβάνουμε

$$(N_1+N_2+\cdots+N_k)x_0 \equiv b_j(N_1+N_2+\cdots+N_k)\,(\text{mod } m_j)\,, \ \forall j \in \{1,\dots,k\}, \tag{8.24}$$

και (ένεκα τού λήμματος 8.4.8)

$$\begin{aligned} 1 \underset{(8.18)}{=} \text{μκδ}\left(\sum_{j=1}^{k} N_j, m\right) &= \text{μκδ}\left(\text{εκπ}\,(m_1,m_2,...,m_k)\,, \sum_{j=1}^{k} N_j\right) \\ &= \text{εκπ}\left(\text{μκδ}\left(m_1, \sum_{j=1}^{k} N_j\right), \dots, \text{μκδ}\left(m_k, \sum_{j=1}^{k} N_j\right)\right), \end{aligned}$$

απ' όπου συμπεραίνουμε ότι

$$\text{μκδ}\left(m_j, \sum_{j=1}^{k} N_j\right) = \text{μκδ}\left(\sum_{j=1}^{k} N_j, m_j\right) = 1, \ \forall j \in \{1,\dots,k\}. \tag{8.25}$$

Σύμφωνα με το πόρισμα 2.4.5, από τις (8.25) και (8.24) έπεται ότι

$$x_0 \equiv b_j\,(\text{mod } m_j)\,, \ \forall j \in \{1,\dots,k\},$$

οπότε ο x_0 αποτελεί *όντως* λύση *και* τού συστήματος γραμμικών ισοτιμιών (8.15). Και αντιστρόφως· εάν υποθέσουμε ότι ο ακέραιος x_0 είναι λύση τού συστήματος (8.15), τότε από το (iv) τής προτάσεως 2.4.4 λαμβάνουμε

$$N_jx_0 \equiv N_jb_j\,(\text{mod } N_jm_j) \underset{2.4.8}{\Longrightarrow} N_jx_0 \equiv N_jb_j\,(\text{mod } \text{εκπ}\,(m_1N_1, m_2N_2, ..., m_kN_k))$$

οπότε $N_jx_0 \equiv N_jb_j \left(\text{mod } \text{εκπ}\left(m\left(\tfrac{m_1}{n_1}\right), m\left(\tfrac{m_2}{n_2}\right), ..., m\left(\tfrac{m_k}{n_k}\right)\right)\right)$ και, ως εκ τούτου,

$$\left.\begin{array}{r} m \mid m\,\text{εκπ}\left(\frac{m_1}{n_1}, \frac{m_2}{n_2}, ..., \frac{m_k}{n_k}\right) \\ N_jx_0 \equiv N_jb_j \left(\text{mod } m\,\text{εκπ}\left(\frac{m_1}{n_1}, \frac{m_2}{n_2}, ..., \frac{m_k}{n_k}\right)\right) \end{array}\right\} \Longrightarrow N_jx_0 \equiv N_jb_j\,(\text{mod } m)\,, \tag{8.26}$$

για κάθε $j \in \{1,\dots,k\}$. (Βλ. 2.2.26 (i).) Κατόπιν προσθέσεως των k ισοτιμιών (8.26) λαμβάνουμε (βάσει τού (i) τής προτάσεως 2.4.4)

$$(N_1 + N_2 + \cdots + N_k)x_0 \equiv (b_1N_1 + b_2N_2 + \cdots + b_kN_k)\,(\text{mod } m)\,.$$

Εξ αυτού συνάγεται ότι ο θεωρηθείς x_0 αποτελεί λύση *και* τής (8.17). □

8.4.11 Θεώρημα. *Έστω $k \in \mathbb{N}$, $k \geqslant 2$. Δοθέντων k φυσικών αριθμών $m_1, \ldots, m_k$ μεγαλυτέρων τού 1, k μη μηδενικών ακεραίων αριθμών $a_1, \ldots, a_k$ και k ακεραίων αριθμών $b_1, \ldots, b_k$, με $d_j := \text{μκδ}\,(a_j, m_j)$ για κάθε $j \in \{1, ..., k\}$, το σύστημα των γραμμικών ισοτιμιών*

$$\left\{ \begin{array}{c} a_1 x \equiv b_1 \,(\text{mod } m_1) \\ \vdots \\ a_k x \equiv b_k \,(\text{mod } m_k) \end{array} \right\} \tag{8.27}$$

δεν είναι επιλύσιμο εάν δεν ικανοποιούνται ταυτοχρόνως οι συνθήκες

$$d_j \mid b_j, \quad \forall j \in \{1, ..., k\}. \tag{8.28}$$

Από την άλλη μεριά, όταν οι συνθήκες (8.28) ικανοποιούνται ταυτοχρόνως, το σύνολο των λύσεων τού συστήματος (8.27) ταυτίζεται με την ένωση των συνόλων λύσεων των $\prod_{j=1}^{k} d_j$ συστημάτων γραμμικών ισοτιμιών

$$\left\{ \begin{array}{c} x \equiv c_{1,\rho_1} \,(\text{mod } m_1) \\ \vdots \\ x \equiv c_{k,\rho_k} \,(\text{mod } m_k) \end{array} \right\} \tag{8.29}$$

κατά μόδιο εκπ $(m_1, ..., m_k)$, *όπου*[11] $(\rho_1, ..., \rho_k) \in \{0, ..., d_1 - 1\} \times \cdots \times \{0, ..., d_k - 1\}$. *Εν προκειμένω, $c_{j,\rho_j} := c_j + \rho_j m_j^\star$, όπου c_j συμβολίζει τη μοναδική λύση κατά μόδιο $m_j^\star$ τής γραμμικής ισοτιμίας*

$$a_j^\star x \equiv b_j^\star \,(\text{mod } m_j^\star)\,,$$

με

$$a_j^\star := \frac{a_j}{d_j}, \quad b_j^\star := \frac{b_j}{d_j}, \quad m_j^\star := \frac{m_j}{d_j}, \ \forall j \in \{1, ..., k\}.$$

Απόδειξη. Για να υπάρχουν κοινές λύσεις τού συστήματος (8.27) θα πρέπει τουλάχιστον καθεμιά των ισοτιμιών του να είναι αφ' εαυτής επιλύσιμη. Τούτο σημαίνει (επί τη βάσει τής προτάσεως 2.4.43) ότι μκδ$(a_j, m_j) \mid b_j$ για κάθε δείκτη $j \in \{1, ..., k\}$. Από την άλλη μεριά, εάν οι συνθήκες (8.28) ικανοποιούνται ταυτοχρόνως, τότε αρκεί να εφαρμόσουμε το 2.4.4 (iv) και το πόρισμα 2.4.48 για κάθε μία εκ των αρχικών ισοτιμιών. □

8.4.12 Παρατήρηση. Προφανώς, το πρόβλημα τής ευρέσεως τού συνόλου των λύσεων τού (8.27) ανάγεται στο πρόβλημα τής ευρέσεως τής ενώσεως των συνόλων των λύσεων των $\prod_{j=1}^{k} d_j$ συστημάτων γραμμικών ισοτιμιών (8.29), ήτοι συστημάτων τού τύπου (8.15), οπότε αντιμετωπίζεται βάσει των όσων ελέχθησαν στο θεώρημα 8.4.10.

8.4.13 Παράδειγμα. Ας θεωρήσουμε το εξής σύστημα δύο γραμμικών ισοτιμιών:

$$\left\{ \begin{array}{l} 6x \equiv 3 \,(\text{mod } 21) \\ 3x \equiv 6 \,(\text{mod } 9) \end{array} \right\}. \tag{8.30}$$

Επειδή μκδ$(6, 21) = 3 \mid 3$ και μκδ$(3, 9) = 3 \mid 6$, αυτό είναι επιλύσιμο. (Βλ. (8.28) στο θεώρημα 8.4.11.) Σύμφωνα με τα προαναφερθέντα στο εδάφιο 2.4.49, η πρώτη ισοτιμία έχει τρεις (σαφώς διακεκριμένες) λύσεις mod 21, ήτοι τις $4, 11$ και $18 (\text{mod } 21)$.

[11] Για κάθε παγιωμένη k-άδα $(\rho_1, ..., \rho_k) \in \{0, ..., d_1 - 1\} \times \cdots \times \{0, ..., d_k - 1\}$ το σύστημα (8.29) διαθέτει ακριβώς μία λύση κατά μόδιο εκπ$(m_1, ..., m_k)$ υπό την προϋπόθεση ότι μκδ$(m_j, m_l) \mid c_{j,\rho_j} - c_{l,\rho_l}$, για κάθε ζεύγος $(j, l) \in \mathbb{N}^2$, $1 \leqslant j, l \leqslant k$, $j \neq l$. (Βλ. θεώρημα 8.4.9.)

Διαιρώντας στη δεύτερη ισοτιμία τα $3, 6, 9$ διά τού μκδ$(3, 9) = 3$ λαμβάνουμε την $x \equiv 2(\mathrm{mod}\ 3)$. Αυτή (σύμφωνα με τα πορίσματα 2.4.45 και 2.4.48) έχει μία και μόνον (προφανή) λύση mod 3, ήτοι την $2(\mathrm{mod}\ 3)$, οπότε η $3x \equiv 6(\mathrm{mod}\ 9)$ (λόγω τής προτάσεως 2.4.43) έχει τρεις (σαφώς διακεκριμένες) λύσεις mod 9, ήτοι τις

$$2,\ \ 2 + \tfrac{9}{3} = 5 \ \text{ και } \ 2 + 2 \cdot \tfrac{9}{3} = 8\ (\mathrm{mod}\ 9).$$

Άρα το σύνολο των λύσεων τού συστήματος γραμμικών ισοτιμιών (8.30) κατά μόδιο 63 (όπου $63 = \text{εκπ}(21, 9)$) αποτελεί την ένωση των συνόλων λύσεων των ακολούθων εννέα συστημάτων γραμμικών ισοτιμιών τής μορφής (8.15):

$$\left\{\begin{array}{l} x \equiv 4(\mathrm{mod}\ 21) \\ x \equiv 2(\mathrm{mod}\ 9) \end{array}\right\},\quad \left\{\begin{array}{l} x \equiv 4(\mathrm{mod}\ 21) \\ x \equiv 5(\mathrm{mod}\ 9) \end{array}\right\},\quad \left\{\begin{array}{l} x \equiv 4(\mathrm{mod}\ 21) \\ x \equiv 8(\mathrm{mod}\ 9) \end{array}\right\},$$

$$\left\{\begin{array}{l} x \equiv 11(\mathrm{mod}\ 21) \\ x \equiv 2(\mathrm{mod}\ 9) \end{array}\right\},\quad \left\{\begin{array}{l} x \equiv 11(\mathrm{mod}\ 21) \\ x \equiv 5(\mathrm{mod}\ 9) \end{array}\right\},\quad \left\{\begin{array}{l} x \equiv 11(\mathrm{mod}\ 21) \\ x \equiv 8(\mathrm{mod}\ 9) \end{array}\right\},$$

$$\left\{\begin{array}{l} x \equiv 18(\mathrm{mod}\ 21) \\ x \equiv 2(\mathrm{mod}\ 9) \end{array}\right\},\quad \left\{\begin{array}{l} x \equiv 18(\mathrm{mod}\ 21) \\ x \equiv 5(\mathrm{mod}\ 9) \end{array}\right\},\quad \left\{\begin{array}{l} x \equiv 18(\mathrm{mod}\ 21) \\ x \equiv 8(\mathrm{mod}\ 9) \end{array}\right\}.$$

Επειδή μκδ$(21, 9) = 3$ και $3 \nmid 2\,(= 4 - 2), 3 \nmid -1\,(= 4 - 5), 3 \nmid -4\,(= 4 - 8)$, τα πρώτα τρία συστήματα γραμμικών ισοτιμιών δεν διαθέτουν καμία λύση κατά μόδιο 63. Κατ' αναλογίαν, επειδή $3 \nmid 16\,(= 18 - 2), 3 \nmid 13\,(= 18 - 5), 3 \nmid 10\,(= 18 - 8)$, τα τελευταία τρία συστήματα γραμμικών ισοτιμιών δεν διαθέτουν καμία λύση κατά μόδιο 63. Από την άλλη μεριά, $3 \mid 9\,(= 11 - 2), 3 \mid 6\,(= 11 - 5), 3 \mid 3\,(= 11 - 8)$, οπότε τα τρία ενδιάμεσα συστήματα γραμμικών ισοτιμιών *είναι* επιλύσιμα κατά μόδιο 63. Μάλιστα, καθένα εξ αυτών έχει μία και μόνον λύση κατά μόδιο 63. Για την εύρεσή της, υιοθετώντας τόν συμβολισμό τον εισαχθέντα στο θεώρημα 8.4.10, έχουμε αφ' ενός μεν (και για τα τρία)

m	n_1	n_2	N_1	N_2	$N_1 + N_2$
63	7	9	9	7	16

αφ' ετέρου δε (για καθένα εξ αυτών)

Δεδομένα	για το 1ο	για το 2ο	για το 3ο
b_1	11	11	11
b_2	2	5	8
$b_1N_1 + b_2N_2$	113	134	155
$(b_1N_1 + b_2N_2)\,(\mathrm{mod}\, m)$	50	8	29

οπότε[12]

η μοναδική λύση mod 63 τού...	βρίσκεται μέσω τής λύσεως τής ισοτιμίας (8.17):	και είναι η εξής:
... πρώτου συστήματος	$16x \equiv 50(\mathrm{mod}\ 63)$	11
... δεύτερου συστήματος	$16x \equiv 8(\mathrm{mod}\ 63)$	32
... τρίτου συστήματος	$16x \equiv 29(\mathrm{mod}\ 63)$	53

Άρα *και* το αρχικό σύστημα γραμμικών ισοτιμιών (8.30) έχει ως λύσεις του τις[13] $11, 32$ και $53\ (\mathrm{mod}\, 63)$.

[12] Η εύρεση τής μοναδικής λύσεως mod 63 για καθεμιά εκ των ισοτιμιών τού καταλόγου που ακολουθεί προσδιορίζεται με οιονδήποτε εκ των τριών τρόπων που υποδεικνύονται στη σημείωση 2.4.46.

[13] Κατά τα αναμενόμενα, οι αριθμοί $11, 32$ και 53 επαληθεύουν *προφανώς* αμφότερες των ισοτιμιών τού (8.30).

8.4.14 Παράδειγμα. Ας θεωρήσουμε το ακόλουθο σύστημα τριών γραμμικών ισοτιμιών:

$$\left\{\begin{array}{l} 2x \equiv 4 \,(\mathrm{mod}\ 8) \\ 6x \equiv 12 \,(\mathrm{mod}\ 9) \\ x \equiv 14 \,(\mathrm{mod}\ 12) \end{array}\right\}. \tag{8.31}$$

Επειδή μκδ$(2,8) = 2 \mid 4$, μκδ$(6,9) = 3 \mid 12$ και μκδ$(1,12) = 1 \mid 14$, πληρούνται οι (8.28) στο θεώρημα 8.4.11. Διαιρώντας στην πρώτη ισοτιμία τα $2, 4, 8$ διά τού μκδ$(2,8) = 2$ λαμβάνουμε την $x \equiv 2(\mathrm{mod}\ 4)$. Αυτή (σύμφωνα με τα πορίσματα 2.4.45 και 2.4.48) έχει μία και μόνον (προφανή) λύση mod 4, ήτοι την $2(\mathrm{mod}\ 4)$, οπότε η $2x \equiv 4(\mathrm{mod}\ 8)$ (λόγω τής προτάσεως 2.4.43) έχει δύο (σαφώς διακεκριμένες) λύσεις mod 8, ήτοι τις 2 και 6 $(\mathrm{mod}\ 8)$. Διαιρώντας στη δεύτερη ισοτιμία τα $6, 12, 9$ διά τού μκδ$(6,9) = 3$ λαμβάνουμε την $2x \equiv 4(\mathrm{mod}\ 3)$. Αυτή (σύμφωνα με τα πορίσματα 2.4.45 και 2.4.48) έχει μία και μόνον (προφανή) λύση mod 3, ήτοι την $2(\mathrm{mod}\ 3)$, διότι $2^{\phi(3)-1} \cdot 4 = 8 \equiv 2(\mathrm{mod}\ 3)$, ενώ η $6x \equiv 12(\mathrm{mod}\ 9)$ (λόγω τής προτάσεως 2.4.43) έχει τρεις (σαφώς διακεκριμένες) λύσεις mod 9, ήτοι

$$2,\ \ 2 + \tfrac{9}{3} = 5 \ \text{ και } \ 2 + 2 \cdot \tfrac{9}{3} = 8 \,(\mathrm{mod}\ 9).$$

Άρα το σύνολο των λύσεων τού συστήματος γραμμικών ισοτιμιών (8.31) κατά μόδιο 72 (όπου $72 = \text{εκπ}(8,9,12)$) αποτελεί την ένωση των συνόλων λύσεων των ακολούθων έξι συστημάτων γραμμικών ισοτιμιών τής μορφής (8.15):

$$\left\{\begin{array}{l} x \equiv 2 \,(\mathrm{mod}\ 8) \\ x \equiv 2 \,(\mathrm{mod}\ 9) \\ x \equiv 14 \,(\mathrm{mod}\ 12) \end{array}\right\}, \quad \left\{\begin{array}{l} x \equiv 2 \,(\mathrm{mod}\ 8) \\ x \equiv 5 \,(\mathrm{mod}\ 9) \\ x \equiv 14 \,(\mathrm{mod}\ 12) \end{array}\right\}, \quad \left\{\begin{array}{l} x \equiv 2 \,(\mathrm{mod}\ 8) \\ x \equiv 8 \,(\mathrm{mod}\ 9) \\ x \equiv 14 \,(\mathrm{mod}\ 12) \end{array}\right\},$$

$$\left\{\begin{array}{l} x \equiv 6 \,(\mathrm{mod}\ 8) \\ x \equiv 2 \,(\mathrm{mod}\ 9) \\ x \equiv 14 \,(\mathrm{mod}\ 12) \end{array}\right\}, \quad \left\{\begin{array}{l} x \equiv 6 \,(\mathrm{mod}\ 8) \\ x \equiv 5 \,(\mathrm{mod}\ 9) \\ x \equiv 14 \,(\mathrm{mod}\ 12) \end{array}\right\}, \quad \left\{\begin{array}{l} x \equiv 6 \,(\mathrm{mod}\ 8) \\ x \equiv 8 \,(\mathrm{mod}\ 9) \\ x \equiv 14 \,(\mathrm{mod}\ 12) \end{array}\right\}.$$

Και τα έξι αυτά συστήματα είναι επιλύσιμα κατά μόδιο 72 (διότι πληρούν τις συνθήκες (8.16)). Επιπλέον, καθένα εξ αυτών διαθέτει μία και μόνον λύση κατά μόδιο 72. Για την εύρεσή της, υιοθετώντας τόν συμβολισμό τον εισαχθέντα στο θεώρημα 8.4.10, έχουμε αφ' ενός μεν (και για τα έξι)

m	n_1	n_2	n_3	N_1	N_2	N_3	$N_1+N_2+N_3$
72	8	9	1	9	8	72	89

αφ' ετέρου δε (για καθένα εξ αυτών)

Δεδομένα	για το 1ο	για το 2ο	για το 3ο
b_1	2	2	2
b_2	2	5	8
b_3	14	14	14
$b_1N_1 + b_2N_2 + b_3N_3$	1042	1066	1090
$(b_1N_1 + b_2N_2 + b_3N_3) \,(\mathrm{mod}\, m)$	34	58	10

και

Δεδομένα	για το 4ο	για το 5ο	για το 6ο
b_1	6	6	6
b_2	2	5	8
b_3	14	14	14
$b_1N_1 + b_2N_2 + b_3N_3$	1078	1102	1126
$(b_1N_1 + b_2N_2 + b_3N_3) \pmod m$	70	22	46

οπότε

η μοναδική λύση mod 72 τού...	βρίσκεται μέσω τής λύσεως τής ισοτιμίας (8.17):	και είναι η εξής:
... πρώτου συστήματος	$89x \equiv 34 (\text{mod } 72)$	2
... δεύτερου συστήματος	$89x \equiv 58 (\text{mod } 72)$	50
... τρίτου συστήματος	$89x \equiv 10 (\text{mod } 72)$	26
... τέταρτου συστήματος	$89x \equiv 70 (\text{mod } 72)$	38
... πέμπτου συστήματος	$89x \equiv 22 (\text{mod } 72)$	14
... έκτου συστήματος	$89x \equiv 46 (\text{mod } 72)$	62

Άρα *και* το αρχικό σύστημα γραμμικών ισοτιμιών (8.31) έχει ως λύσεις του τις

$$2, 14, 26, 38, 50, 62 \ (\text{mod } 72).$$

8.5 ΣΩΜΑ ΚΛΑΣΜΑΤΩΝ ΑΚΕΡΑΙΑΣ ΠΕΡΙΟΧΗΣ

Τα σώματα, από τον ίδιο τους τον ορισμό, χαίρουν λίαν ευάρεστων ιδιοτήτων, όπως, επί παραδείγματι, είναι η ύπαρξη αντιστρόφου για κάθε μη μηδενικό στοιχείο τους. Αντικείμενο τής παρούσας ενότητας είναι η απόδειξη τού ότι *κάθε* ακεραία περιοχή μπορεί να εμφυτευθεί *κατά τρόπο φυσικό* σε ένα σώμα. Αυτή επιτυγχάνεται μέσω τής γενικεύσεως τής γνωστής μεθόδου κατασκευής των ρητών αριθμών από τους ακεραίους.

8.5.1 Ορισμός. Έστω R τυχούσα ακεραία περιοχή. Επί τού $R \times (R \setminus \{0_R\})$ ορίζουμε μια διμελή σχέση "$\sim$" ως ακολούθως:

$$(a, b) \sim (c, d) \underset{\text{ορσ}}{\iff} ad = bc.$$

8.5.2 Πρόταση. *Η "$\sim$" αποτελεί μια σχέση ισοδυναμίας.*

Απόδειξη. Η "$\sim$" είναι *ανακλαστική*, διότι

$$ab = ba \Rightarrow (a, b) \sim (a, b)\,, \quad \forall (a, b) \in R \times (R \setminus \{0_R\})\,,$$

συμμετρική, διότι για οιαδήποτε ζεύγη $(a, b), (c, d) \in R \times (R \setminus \{0_R\})$ έχουμε

$$(a, b) \sim (c, d) \Rightarrow ad = bc \Rightarrow cb = da \Rightarrow (c, d) \sim (a, b)\,,$$

και, τέλος, *μεταβατική*, αφού για οιαδήποτε $(a,b),(a',b'),(a'',b'') \in R \times (R\smallsetminus\{0_R\})$ με

$$(a,b) \sim (a',b') \text{ και } (a',b') \sim (a'',b'')$$

έχουμε $ab' = ba'$ και $a'b'' = b'a''$, οπότε

$$ab''b' = ab'b'' = ba'b'' = bb'a'' = ba''b',$$

και, ως εκ τούτου,

$$\left.\begin{array}{r}(ab''-ba'')b' = 0_R \\ b' \neq 0_R\end{array}\right\} \Longrightarrow ab'' = ba'' \Longrightarrow (a,b) \sim (a'',b'')$$

(με την πρώτη εκ των ανωτέρω συνεπαγωγών οφειλόμενη στο ότι ο δακτύλιος R είναι ακεραία περιοχή). □

8.5.3 Ορισμός. Έστω R τυχούσα ακεραία περιοχή. Ως

$$\boxed{\mathbf{Fr}(R) := (R \times (R\smallsetminus\{0_R\}))\,/\sim}$$

συμβολίζουμε το σύνολο κλάσεων ισοδυναμίας ως προς την "$\sim$". Το **κλάσμα** ενός $a \in R$ «διηρημένου» διά ενός $b \in R\smallsetminus\{0_R\}$ είναι η κλάση ισοδυναμίας

$$\frac{a}{b} := [(a,b)] := \{\,(x,y) \in R \times (R\smallsetminus\{0_R\}) \mid (x,y) \sim (a,b)\}.$$

Το $\mathbf{Fr}(R)$ επιδέχεται πρόσθεση και πολλαπλασιασμό:

$$\begin{cases} \dfrac{a}{b} + \dfrac{c}{d} & := \quad \dfrac{ad+cb}{bd}, \\[2ex] \dfrac{a}{b} \cdot \dfrac{c}{d} & := \quad \dfrac{ac}{bd}. \end{cases}$$

8.5.4 Πρόταση. *Οι εν λόγω πράξεις είναι καλώς ορισμένες.*

Απόδειξη. Εάν για κάποια ζεύγη $(a,b)\,,(a',b')$ και $(c,d)\,,(c',d') \in R \times (R\smallsetminus\{0_R\})$ έχουμε $[(a,b)] = [(a',b')]$ και $[(c,d)] = [(c',d')]\,$, τότε

$$\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'} \text{ και } \frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}.$$

Πράγματι· επειδή εξ υποθέσεως

$$\left.\begin{array}{r}(a,b) \sim (a',b') \\ (c,d) \sim (c',d')\end{array}\right\} \Longrightarrow \left.\begin{array}{r} ab' = ba' \\ cd' = dc'\end{array}\right\} \Longrightarrow \left.\begin{array}{r} ab'dd' = ba'dd' \\ cd'bb' = dc'bb'\end{array}\right\},$$

(κατόπιν προσθέσεως κατά μέλη) έπεται ότι

$$ab'dd' + cd'bb' = ba'dd' + dc'bb' \Longrightarrow (ad+cb)\,b'd' = \left(a'd' + c'b'\right)bd,$$

ήτοι ότι

$$\tfrac{ad+cb}{bd} = \tfrac{a'd'+c'b'}{b'd'} \Longrightarrow \tfrac{a}{b} + \tfrac{c}{d} = \tfrac{a'}{b'} + \tfrac{c'}{d'}.$$

Εξάλλου, πολλαπλασιασμός κατά μέλη μάς οδηγεί στην ισότητα $ab'cd' = ba'dc'$, απ' όπου λαμβάνουμε

$$(ac)\left(b'd'\right) = (bd)\left(a'c'\right) \Longrightarrow \tfrac{ac}{bd} = \tfrac{a'c'}{b'd'},$$

ήτοι $\frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}$. □

8.5.5 Θεώρημα. *Το σύνολο* $\mathbf{Fr}(R)$ *των κλασμάτων μιας ακεραίας περιοχής* R *αποτελεί ένα σώμα ως προς τις ως άνω ορισθείσες πράξεις προσθέσεως και πολλαπλασιασμού. (Γι' αυτόν τον λόγο το* $\mathbf{Fr}(R)$ *ονομάζεται* ***σώμα κλασμάτων*** *τής ακεραίας περιοχής* R*.)*

Απόδειξη. (i) Η "$+$" είναι *προσεταιριστική και μεταθετική*, διότι

$$\begin{aligned}\left(\tfrac{a}{b}+\tfrac{c}{d}\right)+\tfrac{e}{f} &= \tfrac{ad+cb}{bd}+\tfrac{e}{f}=\tfrac{adf+cbf+ebd}{bdf}\\ &= \tfrac{adf+(cf+ed)b}{bdf}=\tfrac{a}{b}+\tfrac{cf+ed}{df}=\tfrac{a}{b}+\left(\tfrac{c}{d}+\tfrac{e}{f}\right)\end{aligned}$$

και $\frac{a}{b}+\frac{c}{d}=\frac{ad+cb}{bd}=\frac{cb+ad}{bd}=\frac{c}{d}+\frac{a}{b}$ για οιαδήποτε κλάσματα $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in\mathbf{Fr}(R)$.
(ii) Το *μηδενικό στοιχείο* (= ουδέτερο στοιχείο ως προς την "$+$") τού $\mathbf{Fr}(R)$ είναι το[14] $0_{\mathbf{Fr}(R)}:=\frac{0_R}{1_R}$, διότι για κάθε κλάσμα $\frac{a}{b}\in\mathbf{Fr}(R)$ έχουμε

$$\tfrac{a}{b}+\tfrac{0_R}{1_R}=\tfrac{(a\cdot 1_R)+(b\cdot 0_R)}{b\cdot 1_R}=\tfrac{a}{b}=\tfrac{(b_R\cdot b)+(1_R\cdot a)}{1_R\cdot b}=\tfrac{0_R}{1_R}+\tfrac{a}{b}.$$

(iii) Κάθε κλάσμα $\frac{a}{b}\in\mathbf{Fr}(R)$ έχει το κλάσμα $\frac{-a}{b}$ ως *αντίθετό του* ως προς την "$+$", καθότι

$$\tfrac{a}{b}+\tfrac{-a}{b}=\tfrac{ab+(-a)b}{b^2}=\tfrac{(a+(-a))b}{b^2}=\tfrac{a+(-a)}{b}=\tfrac{0_R}{b}=\tfrac{0_R}{1_R}=0_{\mathbf{Fr}(R)}$$

και

$$\tfrac{-a}{b}+\tfrac{a}{b}=\tfrac{(-a)b+ab}{b^2}=\tfrac{((-a)+a)b}{b^2}=\tfrac{(-a)+a}{b}=\tfrac{0_R}{b}=\tfrac{0_R}{1_R}=0_{\mathbf{Fr}(R)}.$$

(iv) Η "$\cdot$" είναι *προσεταιριστική και μεταθετική*, διότι

$$\left(\tfrac{a}{b}\cdot\tfrac{c}{d}\right)\cdot\tfrac{e}{f}=\left(\tfrac{ac}{bd}\right)\cdot\tfrac{e}{f}=\tfrac{(ac)e}{(bd)f}=\tfrac{a(ce)}{b(df)}=\tfrac{a}{b}\cdot\left(\tfrac{ce}{df}\right)=\tfrac{a}{b}\cdot\left(\tfrac{c}{d}\cdot\tfrac{e}{f}\right)$$

και $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}=\frac{ca}{db}=\frac{c}{d}\cdot\frac{a}{b}$ για οιαδήποτε κλάσματα $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in\mathbf{Fr}(R)$.
(v) Η "$\cdot$" είναι τόσον *εξ αριστερών* όσον και *εκ δεξιών επιμεριστική* ως προς την "$+$". Επειδή η "$\cdot$" είναι μεταθετική, αρκεί προς τούτο να ελεγχθεί η επιμεριστικότητα μόνον εκ δεξιών. Για οιαδήποτε κλάσματα $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in\mathbf{Fr}(R)$ έχουμε

$$\begin{aligned}\left(\tfrac{a}{b}+\tfrac{c}{d}\right)\cdot\tfrac{e}{f} &= \left(\tfrac{ad+cb}{bd}\right)\cdot\tfrac{e}{f}=\tfrac{(ad+cb)e}{(bd)f}=\tfrac{ade+cbe}{bdf}=\tfrac{ade}{bdf}+\tfrac{cbe}{bdf}\\ &= \tfrac{ae}{bf}+\tfrac{ce}{df}=\left(\tfrac{a}{b}\cdot\tfrac{e}{f}\right)+\left(\tfrac{c}{d}\cdot\tfrac{e}{f}\right).\end{aligned}$$

(vi) Το $1_{\mathbf{Fr}(R)}:=\frac{1_R}{1_R}$ είναι *μοναδιαίο στοιχείο*[15] (= ουδέτερο στοιχείο ως προς την "$\cdot$") τού $\mathbf{Fr}(R)$, διότι για κάθε κλάσμα $\frac{a}{b}\in\mathbf{Fr}(R)$ ισχύουν οι ισότητες

$$\tfrac{a}{b}\cdot 1_{\mathbf{Fr}(R)}=\tfrac{a}{b}\cdot\tfrac{1_R}{1_R}=\tfrac{a\cdot 1_R}{b\cdot 1_R}=\tfrac{a}{b}=\tfrac{1_R\cdot a}{1_R\cdot b}=\tfrac{1_R}{1_R}\cdot\tfrac{a}{b}=1_{\mathbf{Fr}(R)}\cdot\tfrac{a}{b}.$$

(vii) Εκ των (i)-(vi) συνάγεται ότι η τριάδα $(\mathbf{Fr}(R),+,\cdot)$ είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Επομένως, για να αποδείξουμε, επιπροσθέτως, ότι αυτός ο δακτύλιος είναι και *σώμα*, αρκεί να αποδείξουμε ότι οιοδήποτε κλάσμα $\frac{a}{b}\in\mathbf{Fr}(R)\setminus\{0_{\mathbf{Fr}(R)}\}$ είναι αντιστρέψιμο. Επειδή από τη συνθήκη $\frac{a}{b}\neq\frac{0_R}{1_R}$ προκύπτει ότι

$$a=a\cdot 1_R\neq 0_R\cdot b=0_R\Longrightarrow\tfrac{b}{a}\in\mathbf{Fr}(R),$$

εκ των ισοτήτων

$$\tfrac{a}{b}\cdot\tfrac{b}{a}=\tfrac{ab}{ba}=\tfrac{ab}{ab}=\tfrac{1_R}{1_R}=1_{\mathbf{Fr}(R)}=\tfrac{ba}{ba}=\tfrac{ba}{ab}=\tfrac{b}{a}\cdot\tfrac{a}{b}$$

συμπεραίνουμε ότι το $\frac{b}{a}$ είναι *το αντίστροφο* τού $\frac{a}{b}$. □

[14] Σημειωτέον ότι *για κάθε* $b\in R\setminus\{0_R\}$ έχουμε $\frac{0_R}{b}=\frac{0_R}{1_R}$.

[15] Σημειωτέον ότι *για κάθε* $c\in R\setminus\{0_R\}$ έχουμε $\frac{c}{c}=1_{\mathbf{Fr}(R)}$.

8.5.6 Παραδείγματα. (i) Προφανώς, $\mathbf{Fr}(\mathbb{Z}) = \mathbb{Q}$.

(ii) Εάν το K είναι ένα σώμα, το

$$\boxed{K(\mathsf{X}) := \mathbf{Fr}(K[\mathsf{X}])}$$

καλείται **σώμα των ρητών συναρτήσεων** ή **των ρητών εκφράσεων μιας απροσδιορίστου** X **υπεράνω τού** K. Κατ' αναλογίαν, το

$$\boxed{K(\mathsf{X}_1, \ldots, \mathsf{X}_n) := \mathbf{Fr}(K[\mathsf{X}_1, \ldots, \mathsf{X}_n])}$$

είναι το **σώμα των ρητών συναρτήσεων** n **απροσδιορίστων** $\mathsf{X}_1, .., \mathsf{X}_n$ **υπεράνω τού** K.

(iii) Εντός τής ακεραίας περιοχής $\mathbb{C}[\![\mathsf{Z}]\!]$ των επίτυπων δυναμοσειρών μιας μιγαδικής απροσδιορίστου Z (ήτοι μιας απροσδιορίστου Z υπεράνω τού $\mathbb{C}$) ορίζεται η υποπεριοχή

$$\mathbb{C}\{\mathsf{Z}\} := \left\{ \sum_{i=0}^{\infty} a_i \mathsf{Z}^i \in \mathbb{C}[\![\mathsf{Z}]\!] \,\middle|\, \sum_{i=0}^{\infty} a_i z^i \text{ συγκλίνουσα για κάθε } z \in \mathbb{C} \right\}.$$

Ως γνωστόν[16], $\mathbb{C}\{\mathsf{Z}\} = \mathcal{O}(\mathbb{C})$, όπου

$$\boxed{\mathcal{O}(\mathbb{C}) := \{\text{συναρτήσεις } f : \mathbb{C} \longrightarrow \mathbb{C} \,|\, f \text{ ολόμορφη}\}}$$

η ακεραία περιοχή των λεγομένων **ακεραίων συναρτήσεων** μιας μιγαδικής μεταβλητής. Το σώμα κλασμάτων της

$$\boxed{\mathcal{M}(\mathbb{C}) := \mathbf{Fr}(\mathcal{O}(\mathbb{C}))}$$

καλείται **σώμα των μερομόρφων συναρτήσεων** επί τού $\mathbb{C}$ (και τα στοιχεία του **μερόμορφες συναρτήσεις** επί τού $\mathbb{C}$, τις οποίες συναντούμε συχνά στο μάθημα τής Μιγαδικής Αναλύσεως).

(iv) Έστω R μια ακεραία περιοχή. Τότε

$$\boxed{\mathbf{Fr}(R[\mathsf{X}]) = \mathbf{Fr}(R)(\mathsf{X}) \; (:= \mathbf{Fr}(\mathbf{Fr}(R)[\mathsf{X}])),}$$

διότι έχουμε αφ' ενός μεν

$$\mathbf{Fr}(R[\mathsf{X}]) = \left\{ \frac{a_0 + a_1\mathsf{X} + \cdots + a_n\mathsf{X}^n}{b_0 + b_1\mathsf{X} + \cdots + b_m\mathsf{X}^m} \,\middle|\, \begin{array}{c} m, n \in \mathbb{N}_0, a_0, \ldots, a_n, b_0, \ldots, b_m \in R \\ \text{με } \; b_j \neq 0_R \text{ για κάποιον } \; j \in \{0, \ldots, m\} \end{array} \right\},$$

αφ' ετέρου δε

$$\mathbf{Fr}(R)(\mathsf{X}) = \left\{ \frac{r_0 + r_1\mathsf{X} + \cdots + r_n\mathsf{X}^n}{s_0 + s_1\mathsf{X} + \cdots + s_m\mathsf{X}^m} \,\middle|\, \begin{array}{c} m, n \in \mathbb{N}_0, r_0, \ldots, r_n, s_0, \ldots, s_m \in \mathbf{Fr}(R) \\ \text{με } \; s_j \neq 0_{\mathbf{Fr}(R)} \text{ για κάποιον } \; j \in \{0, \ldots, m\} \end{array} \right\}$$

$$= \left\{ \frac{\frac{a_0}{b_0} + \left(\frac{a_1}{b_1}\right)\mathsf{X} + \cdots + \left(\frac{a_n}{b_n}\right)\mathsf{X}^n}{\frac{c_0}{d_0} + \left(\frac{c_1}{d_1}\right)\mathsf{X} + \cdots + \left(\frac{c_m}{d_m}\right)\mathsf{X}^m} \,\middle|\, \begin{array}{c} r_i = \frac{a_i}{b_i}, \; s_j = \frac{c_j}{d_j}, \\ \text{όπου } (a_i, b_i), (c_j, d_j) \in R \times (R \setminus \{0_R\}), \\ \forall (i, j) \in \{0, \ldots, n\} \times \{0, \ldots, m\} \end{array} \right\}$$

$$= \mathbf{Fr}(R[\mathsf{X}]),$$

με την τελευταία ισότητα προκύπτουσα ύστερα από απαλοιφή παρονομαστών.

(v) Εάν το K είναι ένα σώμα, τότε το σώμα των κλασμάτων τής ακεραίας περιοχής

[16] Κάθε *ολόμορφη συνάρτηση* $f : \mathbb{C} \longrightarrow \mathbb{C}$ (ήτοι κάθε συνάρτηση $f : \mathbb{C} \longrightarrow \mathbb{C}$ διαθέτουσα μιγαδική παράγωγο σε κάθε σημείο τού $\mathbb{C}$) είναι *παραστάσιμη ως συγκλίνουσα δυναμοσειρά*.

$K[\![\mathsf{X}]\!]$ των επίτυπων δυναμοσειρών μιας απροσδιορίστου X με συντελεστές ειλημμένους από το K συμβολίζεται συντόμως ως ακολούθως:

$$\boxed{K(\!(\mathsf{X})\!) := \mathbf{Fr}(K[\![\mathsf{X}]\!]).}$$

Σημειωτέον ότι

$$\boxed{K(\!(\mathsf{X})\!) = \mathrm{Laur}_K[\![\mathsf{X}^{\pm 1}]\!]}$$

(με τον συμβολισμό όπως στην άσκηση 25 τού φυλλαδίου 11). Πράγματι· για τυχόν στοιχείο

$$\frac{\sum_{i=0}^{\infty} a_i \mathsf{X}^i}{\sum_{i=0}^{\infty} b_i \mathsf{X}^i} \in K(\!(\mathsf{X})\!)$$

παρατηρούμε τα εξής: Εάν $b_0 \neq 0_K$, τότε $\sum_{i=0}^{\infty} b_i \mathsf{X}^i \in K[\![\mathsf{X}]\!]^\times$ (βλ. 6.3.9 (iii)) και

$$\frac{\sum_{i=0}^{\infty} a_i \mathsf{X}^i}{\sum_{i=0}^{\infty} b_i \mathsf{X}^i} = \left(\sum_{i=0}^{\infty} a_i \mathsf{X}^i\right)\left(\sum_{i=0}^{\infty} b_i \mathsf{X}^i\right)^{-1} \in K[\![\mathsf{X}]\!].$$

Εάν $b_0 = 0_K$, τότε $l := \mathrm{ord}(\sum_{i=0}^{\infty} b_i \mathsf{X}^i) \geqslant 1$ (βλ. 6.3.4), οπότε

$$b_0 = \cdots = b_{l-1} = 0_K,\ b_l \neq 0_K \Rightarrow \sum_{i=l}^{\infty} b_i \mathsf{X}^{i-l} \in K[\![\mathsf{X}]\!]^\times$$

και

$$\frac{\sum\limits_{i=0}^{\infty} a_i \mathsf{X}^i}{\sum\limits_{i=0}^{\infty} b_i \mathsf{X}^i} = \frac{\sum\limits_{i=0}^{\infty} a_i \mathsf{X}^i}{\sum\limits_{i=l}^{\infty} b_i \mathsf{X}^i} = \frac{\sum\limits_{i=0}^{\infty} a_i \mathsf{X}^i}{\mathsf{X}^l \left(\sum\limits_{i=l}^{\infty} b_i \mathsf{X}^{i-l}\right)} = \frac{\sum\limits_{i=0}^{\infty} a_i \mathsf{X}^i \left(\sum\limits_{i=l}^{\infty} b_i \mathsf{X}^{i-l}\right)^{-1}}{\mathsf{X}^l}.$$

Κατά συνέπειαν,

$$\begin{aligned} K(\!(\mathsf{X})\!) &= \left\{ \frac{\sum_{i=0}^{\infty} c_i \mathsf{X}^i}{\mathsf{X}^l} \,\middle|\, c_i \in K,\ \forall i \in \mathbb{N}_0,\ \ l \in \mathbb{N} \right\} \\ &= \left\{ \sum_{i=0}^{l-1} c_i \mathsf{X}^{i-l} + \sum_{i=l}^{\infty} c_i \mathsf{X}^{i-l} \,\middle|\, c_i \in K,\ \forall i \in \mathbb{N}_0,\ \ l \in \mathbb{N} \right\} \\ &= \mathrm{Laur}_K[\![\mathsf{X}^{\pm 1}]\!]. \end{aligned}$$

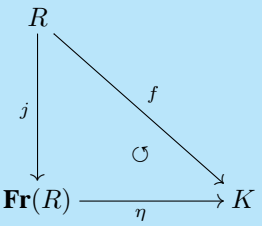
8.5.7 Πρόταση. *Κάθε ακεραία περιοχή εμφυτεύεται στο σώμα των κλασμάτων της.*

Απόδειξη. Έστω R τυχούσα ακεραία περιοχή. Τότε ο ομομορφισμός

$$j : R \longrightarrow \mathbf{Fr}(R), \quad a \longmapsto j(a) := \tfrac{a}{1_R}, \tag{8.32}$$

είναι ένας μονομορφισμός, διότι έχει το $\{a \in R \mid \frac{a}{1_R} = \frac{0_R}{1_R}\} = \{0_R\}$ ως πυρήνα του (βλ. πρόταση 8.1.16). □

8.5.8 Πρόταση (“Καθολική ιδιότητα” τού $\mathbf{Fr}(R)$.). *Έστω R μια ακεραία περιοχή. Τότε για κάθε μονομορφισμό $f : R \longrightarrow K$, όπου K ένα σώμα, υφίσταται ένας και μόνον μονομορφισμός σωμάτων $\eta : \mathbf{Fr}(R) \longrightarrow K$ ο οποίος καθιστά το διάγραμμα*



μεταθετικό (ήτοι $f = \eta \circ j$), όπου j ο μονομορφισμός (8.32).

ΑΠΟΔΕΙΞΗ. Ορίζουμε την $\eta : \mathbf{Fr}(R) \longrightarrow K$ μέσω τού τύπου

$$\eta(\tfrac{a}{b}) := f(a)\, f(b)^{-1}, \quad \forall \tfrac{a}{b} \in \mathbf{Fr}(R).$$

Η η είναι *καλώς ορισμένη* απεικόνιση, διότι για $\frac{a}{b}, \frac{a'}{b'} \in \mathbf{Fr}(R)$ με $\frac{a}{b} = \frac{a'}{b'}$ έχουμε

$$ab' = ba' \Rightarrow f(a)f(b') = f(ab') = f(ba') = f(b)f(a'),$$

οπότε

$$f(b), f(b') \in \mathbf{Fr}(R)^{\times} \Rightarrow \eta(\tfrac{a}{b}) := f(a)\, f(b)^{-1} = f\left(a'\right) f\left(b'\right)^{-1} =: \eta(\tfrac{a'}{b'}).$$

Η η είναι *ομομορφισμός*, καθότι για οιαδήποτε $\frac{a}{b}, \frac{c}{d} \in \mathbf{Fr}(R)$ έχουμε

$$\begin{aligned} \eta(\tfrac{a}{b} + \tfrac{c}{d}) &= \eta(\tfrac{ad+cb}{bd}) = f(ad+cb)\, f(bd)^{-1} \\ &= (f(a)f(d) + f(c)f(b))\, f(b)f(d)^{-1} \\ &= f(a)f(b)^{-1} + f(c)\, f(d)^{-1} = \eta(\tfrac{a}{b}) + \eta(\tfrac{c}{d}) \end{aligned}$$

και

$$\eta(\tfrac{a}{b} \cdot \tfrac{c}{d}) = \eta(\tfrac{ac}{bd}) = f(ac)\, f(bd)^{-1} = \left(f(a)f(b)^{-1}\right)\left(f(c)\, f(d)^{-1}\right) = \eta(\tfrac{a}{b})\eta(\tfrac{c}{d}).$$

Η η είναι *ενριπτική*, διότι εάν $\frac{a}{b}, \frac{c}{d} \in \mathbf{Fr}(R)$ με $\eta(\frac{a}{b}) = \eta(\frac{c}{d})$, τότε

$$f(a)\, f(b)^{-1} = f(c)\, f(d)^{-1} \Rightarrow f(a)\, f(d) = f(b)\, f(c),$$

ήτοι

$$f(ad) = f(bc) \underset{[f \text{ ένριψη}]}{\Longrightarrow} ad = cb \Longrightarrow \tfrac{a}{b} = \tfrac{c}{d},$$

απ' όπου έπεται ότι η η είναι πράγματι ένας *μονομορφισμός*. Προφανώς,

$$(\eta \circ j)(a) = \eta(j(a)) = \eta(\tfrac{a}{1_R}) = f(a)f(1_R)^{-1} = f(a) \cdot 1_K = f(a)$$

για κάθε $a \in R$, οπότε $f = \eta \circ j$. Τέλος, εάν υποτεθεί ότι υφίσταται κάποιος μονομορφισμός $\eta' : \mathbf{Fr}(R) \longrightarrow K$ για τον οποίο ισχύει η ισότητα $f = \eta' \circ j$, τότε για κάθε $\frac{a}{b} \in \mathbf{Fr}(R)$ έχουμε

$$\eta'(\tfrac{a}{b}) = \eta'(j(a)j(b^{-1})) = \eta'(j(ab^{-1})) = (\eta' \circ j)(ab^{-1}) = f(ab^{-1}) = f(a)f(b)^{-1} = \eta(\tfrac{a}{b}),$$

απ' όπου έπεται ότι $\eta' = \eta$. □

8.5.9 Πόρισμα. *Εάν η R είναι μια ακεραία περιοχή περιεχόμενη σε ένα σώμα K, τότε το*

$$\overline{R} := \left\{ ab^{-1} \middle| \, (a,b) \in R \times (R \smallsetminus \{0_R\}) \right\} \subseteq K$$

είναι το ελάχιστο υπόσωμα τού K (ως προς τη σχέση τού εγκλεισμού) το οποίο περιέχει την R και $\overline{R} \cong \mathbf{Fr}(R)$.

ΑΠΟΔΕΙΞΗ. Έστω $\iota : R \hookrightarrow K$ η συνήθης ένθεση. Επειδή η ι είναι μονομορφισμός, η πρόταση 8.5.8 μας πληροφορεί ότι υφίσταται ένας και μόνον μονομορφισμός σωμάτων $\eta : \mathbf{Fr}(R) \longrightarrow K$ με $\iota = \eta \circ j$, όπου j ο μονομορφισμός (8.32). Για κάθε $(a,b) \in R \times (R \smallsetminus \{0_R\})$ έχουμε

$$\eta(\tfrac{a}{b}) = \eta(j(a)j(b^{-1})) = \eta(j(ab^{-1})) = (\eta \circ j)(ab^{-1}) = \iota(ab^{-1}) = ab^{-1},$$

οπότε $\overline{R} = \mathrm{Im}(\eta) \cong \mathbf{Fr}(R)$. Επομένως, το $\overline{R}$ είναι αφ' εαυτού σώμα (βλ. 8.1.11 (iii)) με $R \subseteq \overline{R}$. Έστω τώρα τυχόν υπόσωμα L τού K περιέχον την ακεραία περιοχή R. Το σώμα L περιέχει το b^{-1} για κάθε στοιχείο $b \in R \smallsetminus \{0_R\}$. Κατά συνέπειαν, το L περιέχει όλα τα στοιχεία τής μορφής ab^{-1}, όπου $(a,b) \in R \times (R \smallsetminus \{0_R\})$. Αυτό σημαίνει ότι $R \subseteq L \subseteq \overline{R} \cong \mathbf{Fr}(R)$. □

8.5.10 Παράδειγμα. Η ακεραία περιοχή $\mathbb{Z}[\sqrt{2}]$ περιέχεται (εξ ορισμού) στο σώμα $\mathbb{Q}(\sqrt{2})$. (Βλ. άσκηση 24 τού φυλλαδίου 11.) Επομένως,

$$\mathbb{Z}[\sqrt{2}] \subseteq \overline{\mathbb{Z}[\sqrt{2}]} = \mathbf{Fr}(\mathbb{Z}[\sqrt{2}]) \subseteq \mathbb{Q}(\sqrt{2}).$$

Από την άλλη μεριά, κάθε στοιχείο τού $\mathbb{Q}(\sqrt{2})$ είναι τής μορφής $r + s\sqrt{2}$, όπου $r, s \in \mathbb{Q}$. Γράφοντας τα r, s ως κλάσματα $r = \frac{a}{b}$, $s = \frac{c}{d}$, για κατάλληλα ζεύγη $(a, b), (c, d) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, παρατηρούμε ότι

$$r + s\sqrt{2} = \tfrac{a}{b} + \tfrac{c}{d}\sqrt{2} = \tfrac{ad+cb\sqrt{2}}{bd} \in \mathbf{Fr}(\mathbb{Z}[\sqrt{2}]) \Rightarrow \mathbb{Q}(\sqrt{2}) \subseteq \mathbf{Fr}(\mathbb{Z}[\sqrt{2}]).$$

Εκ των ανωτέρω έπεται ότι $\mathbf{Fr}(\mathbb{Z}[\sqrt{2}]) = \mathbb{Q}(\sqrt{2})$.

8.5.11 Πόρισμα. *Για κάθε σώμα K υφίσταται ισομορφισμός $K \cong \mathbf{Fr}(K)$.*

Απόδειξη. Έπεται άμεσα ύστερα από εφαρμογή τού πορίσματος 8.5.9 στην ειδική περίπτωση κατά την οποία $R = K$ (καθόσον $\overline{K} = K$). □

8.5.12 Πρόταση. *Έστω $f : R_1 \longrightarrow R_2$ ένας ομομορφισμός ακεραίων περιοχών. Τότε η απεικόνιση*

$$\mathbf{Fr}(f) : \mathbf{Fr}(R_1) \longrightarrow \mathbf{Fr}(R_2),\ \mathbf{Fr}(f)(\tfrac{a}{b}) := \tfrac{f(a)}{f(b)},\ \forall\, (a, b) \in R_1 \times (R_1 \setminus \{0_{R_1}\}),$$

η επαγομένη μέσω τού f είναι ομομορφισμός σωμάτων. Επιπροσθέτως, ισχύουν τα εξής:

(i) *Εάν ο f είναι μονομορφισμός, τότε και ο $\mathbf{Fr}(f)$ είναι μονομορφισμός.*

(ii) *Εάν ο f είναι επιμορφισμός, τότε και ο $\mathbf{Fr}(f)$ είναι επιμορφισμός.*

(iii) *Εάν ο f είναι ισομορφισμός, τότε και ο $\mathbf{Fr}(f)$ είναι ισομορφισμός, οπότε*

$$R_1 \cong R_2 \Longrightarrow \mathbf{Fr}(R_1) \cong \mathbf{Fr}(R_2).$$

Απόδειξη. Η $\mathbf{Fr}(f)$ είναι *ομομορφισμός* σωμάτων, διότι για $\frac{a}{b}, \frac{c}{d} \in \mathbf{Fr}(R_1)$ έχουμε

$$\begin{aligned} \mathbf{Fr}(f)(\tfrac{a}{b} + \tfrac{c}{d}) &= \mathbf{Fr}(f)(\tfrac{ad+cb}{bd}) = \tfrac{f(ad+cb)}{f(bd)} = \tfrac{f(ad)+f(cb)}{f(b)f(d)} = \tfrac{f(a)f(d)+f(c)f(b)}{f(b)f(d)} \\ &= \tfrac{f(a)}{f(b)} + \tfrac{f(c)}{f(d)} = \mathbf{Fr}(f)(\tfrac{a}{b}) + \mathbf{Fr}(f)(\tfrac{c}{d}) \end{aligned}$$

και

$$\mathbf{Fr}(f)(\tfrac{a}{b} \cdot \tfrac{c}{d}) = \mathbf{Fr}(f)(\tfrac{ac}{bd}) = \tfrac{f(ac)}{f(bd)} = \tfrac{f(a)f(c)}{f(b)f(d)} = \tfrac{f(a)}{f(b)}\tfrac{f(c)}{f(d)} = \mathbf{Fr}(f)(\tfrac{a}{b})\mathbf{Fr}(f)(\tfrac{c}{d}).$$

(i) Εάν η f είναι ενριπτική, τότε και η απεικόνιση $\mathbf{Fr}(f)$ είναι ενριπτική, διότι εάν $\frac{a}{b}, \frac{c}{d} \in \mathbf{Fr}(R_1)$ με

$$\mathbf{Fr}(f)(\tfrac{a}{b}) = \mathbf{Fr}(f)(\tfrac{c}{d}),$$

τότε $\frac{f(a)}{f(b)} = \frac{f(c)}{f(d)}$, απ' όπου έπεται ότι

$$f(a)f(d) = f(c)f(b) \Longrightarrow f(ad) = f(cb) \underset{[f \text{ ενριπτική}]}{\Longrightarrow} ad = cb \Longrightarrow \tfrac{a}{b} = \tfrac{c}{d}.$$

(ii) Εάν η f είναι επιριπτική, τότε και η $\mathbf{Fr}(f)$ είναι επιριπτική, διότι για κάθε $\frac{c}{d} \in \mathbf{Fr}(R_2)$ υπάρχει ζεύγος $(a, b) \in R_1 \times (R_1 \setminus \{0_{R_1}\})$, τέτοιο ώστε να ισχύει

$$[f(a) = c, \quad f(b) = d] \Longrightarrow \mathbf{Fr}(f)(\tfrac{a}{b}) = \tfrac{f(a)}{f(b)},$$

ήτοι $\mathbf{Fr}(f)(\frac{a}{b}) = \frac{c}{d}$. Το (iii) είναι άμεση συνέπεια των (i) και (ii). □

8.6 ΠΡΩΤΑ ΣΩΜΑΤΑ

Έστω L ένα υπόσωμα τού σώματος $\mathbb{Q}$ των ρητών αριθμών. Επειδή υπάρχει πάντοτε κάποιο $a \in L \setminus \{0\}$, η -εξ ορισμού εγγυηθείσα- ύπαρξη τού (πολλαπλασιαστικού) αντιστρόφου του a^{-1} έχει ως επακόλουθο το ότι

$$a^{-1}a = 1_L = 1_{\mathbb{Q}} \in L.$$

Ως εκ τούτου, για κάθε ακέραιο $n \in \mathbb{Z}$ ισχύει $n = n \cdot 1_L = n \cdot 1_{\mathbb{Q}} \in L$, οπότε έχουμε κατ' ανάγκην την εγκλειστική σχέση $\mathbb{Z} \subseteq L \subseteq \mathbb{Q}$. Όμως, σύμφωνα με το πόρισμα 8.5.9, το $\mathbb{Q} = \mathbf{Fr}(\mathbb{Z})$ είναι το ελάχιστο σώμα (ως προς τη σχέση τού εγκλεισμού) το οποίο περιέχει την ακεραία περιοχή $\mathbb{Z}$. Άρα τελικώς $L = \mathbb{Q}$. Η ιδιότητα αυτή τού $\mathbb{Q}$ το καθιστά το πλέον τυπικό παράδειγμα των λεγομένων «πρώτων σωμάτων».

8.6.1 Ορισμός. Ένα σώμα K καλείται **πρώτο σώμα** όταν δεν περιέχει κανένα γνήσιο υπόσωμα.

8.6.2 Παράδειγμα. Πέραν τού $\mathbb{Q}$, ένα άλλο πρώτο σώμα είναι το $\mathbb{Z}_p$, όπου p πρώτος αριθμός. Πράγματι· εάν το L είναι ένα υπόσωμα τού $\mathbb{Z}_p$, τότε η (προσθετική) υποομάδα $(L, +)$ τής ομάδας $(\mathbb{Z}_p, +)$ είναι πεπερασμένη με τάξη της έναν διαιρέτη τού p (λόγω τού θεωρήματος τού Lagrange). Επειδή λοιπόν ο p είναι πρώτος, $|L| = 1$ ή $|L| = p$. Η πρώτη περίπτωση αποκλείεται, καθότι το L -ως σώμα- έχει τάξη $|L| \geqslant 2$. Επομένως, $|L| = p$, οπότε κατ' ανάγκην $L = \mathbb{Z}_p$.

8.6.3 Θεώρημα. *Κάθε σώμα K περιέχει ένα και μόνον πρώτο υπόσωμα.*

Απόδειξη. Το σώμα

$$K_0 := \bigcap \{ S \mid S \text{ υπόσωμα τού } K \} \subseteq K$$

είναι ένα πρώτο υπόσωμα τού K. Πράγματι· εάν το L είναι ένα υπόσωμα τού K_0, τότε το L είναι και υπόσωμα τού K, οπότε $K_0 \subseteq L$, απ' όπου συμπεραίνουμε ότι $L = K_0$. Υπολείπεται η απόδειξη τής μοναδικότητας τού K_0. Υποτιθεμένης τής υπάρξεως ενός άλλου πρώτου υποσώματος K_0' τού σώματος K, το $K_0 \cap K_0'$ είναι υπόσωμα τού K και $K_0 \cap K_0' \subseteq K_0$, $K_0 \cap K_0' \subseteq K_0'$. Επομένως, $K_0 \cap K_0' = K_0$ και $K_0 \cap K_0' = K_0'$, πράγμα που σημαίνει ότι $K_0 = K_0'$. □

8.6.4 Θεώρημα. (i) *Κάθε πρώτο σώμα χαρακτηριστικής μηδέν είναι ισόμορφο με το σώμα $\mathbb{Q}$ των ρητών αριθμών.*

(ii) *Κάθε πρώτο σώμα χαρακτηριστικής p (όπου p πρώτος αριθμός) είναι ισόμορφο με το σώμα $\mathbb{Z}_p$ των κλάσεων ισοτιμιών κατά μόδιο p.*

Απόδειξη. Έστω L ένα πρώτο σώμα. Ορίζουμε την απεικόνιση

$$f : \mathbb{Z} \longrightarrow L, \quad f(n) := n \cdot 1_L, \quad \forall n \in \mathbb{Z}.$$

Επειδή

$$\begin{cases} f(m+n) = (m+n) \cdot 1_L = m \cdot 1_L + n \cdot 1_L = f(m) + f(n), \\ f(mn) = (mn) \cdot 1_L = m\,(n \cdot 1_L) = (m \cdot 1_L)\,(n \cdot 1_L) = f(m) f(n), \end{cases}$$

για οιουσδήποτε $m, n \in \mathbb{Z}$, η f είναι ένας ομομορφισμός δακτυλίων. Βάσει τού 1ου θεωρήματος ισομορφισμών 8.3.3, $\mathbb{Z}/\mathrm{Ker}(f) \cong \mathrm{Im}(f) = f(\mathbb{Z})$, όπου

$$\mathrm{Ker}(f) = \{ n \in \mathbb{Z} \mid n \cdot 1_L = 0_L \}.$$

(i) Εάν το L έχει χαρακτηριστική μηδέν, τότε $\mathrm{Ker}(f)=\{0\}$, οπότε

$$\mathbb{Z}/\mathrm{Ker}\,(f)=\mathbb{Z}/\{0\}\cong\mathbb{Z}\cong\mathrm{Im}\,(f)=f(\mathbb{Z}).$$

Ως εκ τούτου, η $\mathrm{Im}\,(f)$ είναι μια ακεραία περιοχή (ισόμορφη με τον $\mathbb{Z}$) και, επειδή $\mathrm{Im}\,(f)\subseteq L$, έχουμε

$$\mathbf{Fr}\,(\mathrm{Im}\,(f))=\left\{\frac{n\cdot 1_L}{m\cdot 1_L}\;\middle|\;(n,m)\in\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0\})\right\}\subseteq\mathbf{Fr}\,(L)\cong L,$$

οπότε $L\cong\mathbf{Fr}\,(L)=\mathbf{Fr}\,(\mathrm{Im}\,(f))\cong\mathbf{Fr}\,(\mathbb{Z})=\mathbb{Q}$ (λόγω τής προτάσεως 8.5.12 και τού ότι το L είναι πρώτο σώμα).

(ii) Εάν το L έχει χαρακτηριστική p, όπου p πρώτος αριθμός, τότε, βάσει τής προτάσεως 6.4.3 έχουμε

$$p=\min\{\,|k|\in\mathbb{N}\mid\ k\in\mathbb{Z}\smallsetminus\{0\}\ \text{ με }\ k\cdot 1_L=0_L\},$$

οπότε $p\in\mathrm{Ker}(f)\Longrightarrow p\mathbb{Z}=\langle p\rangle\subseteq\mathrm{Ker}(f)$. Αλλά και για κάθε $\lambda\in\mathrm{Ker}(f)$, γράφοντας

$$\lambda=up+r,\ \ u,r\in\mathbb{Z},\quad 0\leqslant r\leqslant p-1,$$

λαμβάνουμε $0_L=\lambda\cdot 1_L=u\,(p\cdot 1_L)+(r\cdot 1_L)=0_L+r\cdot 1_L=r\cdot 1_L$, ήτοι μια ισότητα η οποία (λόγω τής ως άνω συνθήκης ελαχίστου που πληροί το p) ισχύει μόνον όταν $r=0$. Επομένως, $\lambda\in\langle p\rangle$, οπότε $\mathrm{Ker}(f)\subseteq p\mathbb{Z}=\langle p\rangle$. Τελικώς λοιπόν $\mathrm{Ker}(f)=p\mathbb{Z}=\langle p\rangle$ και

$$\mathbb{Z}/p\mathbb{Z}\cong\mathbb{Z}_p\cong\mathrm{Im}\,(f)=f(\mathbb{Z})=\{\,n\cdot 1_L\mid\ n\in\{0,1,\ldots,p-1\}\}\subseteq L,$$

απ' όπου συμπεραίνουμε ότι $L=\mathrm{Im}\,(f)\cong\mathbb{Z}_p$, διότι το L είναι πρώτο σώμα. □

8.6.5 Πόρισμα. *Κάθε σώμα K περιέχει ένα υπόσωμα L, τέτοιο ώστε*:

$$L\cong\begin{cases}\mathbb{Q}, & \text{όταν } \mathrm{χαρ}(K)=0,\\ \mathbb{Z}_p, & \text{όταν } \mathrm{χαρ}(K)=p>0.\end{cases}$$

8.6.6 Παρατήρηση. Σύμφωνα με όσα αναφέραμε στην απόδειξη τού θεωρήματος 8.6.4, εάν το L είναι ένα πρώτο σώμα, τότε

$$L\cong\left\{(n\cdot 1_L)\,(m\cdot 1_L)^{-1}\;\middle|\;(n,m)\in\mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0\})\right\},\quad\text{όταν } \mathrm{χαρ}(L)=0,$$

και

$$L=\ \{\,n\cdot 1_L\mid\ n\in\{0,1,\ldots,p-1\}\},\quad\text{όταν } \mathrm{χαρ}(L)=p>0.$$

ΚΕΦΑΛΑΙΟ 9

Δακτύλιοι που ικανοποιούν συνθήκες αλυσίδων

Στο κεφάλαιο αυτό μελετώνται οι κύριες ιδιότητες δακτυλίων που ικανοποιούν τις λεγόμενες *συνθήκες* (ανιουσών ή κατιουσών) *αλυσίδων*.

9.1 ΝΑΙΤΕΡΙΑΝΟΙ ΔΑΚΤΥΛΙΟΙ

9.1.1 Ορισμός. Έστω $\{I_n | \, n \in \mathbb{N}\}$ ένα αριθμήσιμο σύνολο αριστερών (και αντιστοίχως, δεξιών) ιδεωδών ενός δακτυλίου R. Η ακολουθία $\{I_n\}_{n\in\mathbb{N}}$ καλείται **ανιούσα αλυσίδα** αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού R όταν ισχύει ο εγκλεισμός $I_n \subseteq I_{n+1}$ για κάθε $n \in \mathbb{N}$. Μια ανιούσα αλυσίδα $\{I_n\}_{n\in\mathbb{N}}$ καλείται **στάσιμη** όταν υπάρχει κάποιος $k \in \mathbb{N}$ για τον οποίο ισχύει $I_n = I_k$ για κάθε φυσικό αριθμό $n \geqslant k$.

9.1.2 Ορισμός. Λέμε ότι ένας δακτύλιος R ικανοποιεί τη **συνθήκη των ανιουσών αλυσίδων** επί τού συνόλου των αριστερών (και αντιστοίχως, των δεξιών) ιδεωδών του όταν *κάθε* ανιούσα αλυσίδα αριστερών (και αντιστοίχως, δεξιών) ιδεωδών αυτού είναι στάσιμη.

9.1.3 Θεώρημα. *Έστω R ένας δακτύλιος. Τότε τα ακόλουθα είναι ισοδύναμα*:

(i) *Ο R ικανοποιεί τη συνθήκη των ανιουσών αλυσίδων επί τού συνόλου των αριστερών (και αντιστοίχως, των δεξιών) ιδεωδών του.*

(ii) *Κάθε μη κενό σύνολο αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού R περιέχει (τουλάχιστον) ένα μεγιστικό στοιχείο (ως προς τον συνήθη εγκλεισμό).*

Απόδειξη. (i)⇒(ii) Έστω $\mathcal{S}$ ένα μη κενό σύνολο αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού R. Τότε υπάρχει κάποιο στοιχείο, ας το πούμε I_1, εντός τού $\mathcal{S}$. Εάν το I_1 είναι μεγιστικό στοιχείο τού $\mathcal{S}$, τότε έχει καλώς. Ειδάλλως, θα υπάρχει κάποιο $I_2 \in \mathcal{S}$, τέτοιο ώστε να ισχύει $I_1 \subseteq I_2$. Εάν το I_2 είναι μεγιστικό στοιχείο τού $\mathcal{S}$, τότε έχει καλώς. Ειδάλλως, θα υπάρχει κάποιο $I_3 \in \mathcal{S}$, τέτοιο ώστε να ισχύει $I_2 \subseteq I_3$. Εφαρμόζοντας κατ' επανάληψη την ίδια (επαγωγική) συλλογιστική σχηματίζουμε μια ανιούσα αλυσίδα δεξιών (και αντιστοίχως, αριστερών) ιδεωδών τού R

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

ανηκόντων στο $\mathcal{S}$, η οποία είναι εξ υποθέσεως στάσιμη, ήτοι υπάρχει κάποιος $k \in \mathbb{N}$ για τον οποίο ισχύει $I_n = I_k$ για κάθε φυσικό αριθμό $n \geqslant k$. Το αριστερό (και αντιστοίχως, το δεξιό) ιδεώδες I_k είναι μεγιστικό στοιχείο τού $\mathcal{S}$ (βλ. 1.4.9 (i)). Πράγματι· εάν το I είναι οιοδήποτε αριστερό (και αντιστοίχως, οιοδήποτε δεξιό) ιδεώδες ανήκον στο $\mathcal{S}$ για το οποίο ισχύει $I_k \subseteq I$, τότε (λόγω τού τρόπου κατασκευής τής ως άνω αλυσίδας) θα υπάρχει κάποιος $\nu \in \mathbb{N}$ με $I \subseteq I_\nu$, οπότε

$$\left.\begin{array}{ll} I \subseteq I_\nu \subseteq I_k, & \text{όταν } \nu \leqslant k \\ I \subseteq I_\nu = I_k, & \text{όταν } \nu \geqslant k \end{array}\right\} \Longrightarrow I_k = I.$$

Άρα το I_k είναι όντως μεγιστικό στοιχείο τού $\mathcal{S}$.

(ii)⇒(i) Θεωρούμε *τυχούσα* ανιούσα αλυσίδα

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού R. Εξ υποθέσεως, το σύνολο $\{I_n | \, n \in \mathbb{N}\}$ των μελών αυτής περιέχει κάποιο μεγιστικό στοιχείο, ας πούμε το I_m (ως προς τον συνήθη εγκλεισμό). Για κάθε φυσικό αριθμό $n \geqslant m$ έχουμε $I_m \subseteq I_n$ (διότι η θεωρηθείσα αλυσίδα είναι ανιούσα), οπότε $I_m = I_n$ (λόγω τού ότι το I_m είναι μεγιστικό στοιχείο τού $\{I_n | \, n \in \mathbb{N}\}$). Άρα ο R ικανοποιεί τη συνθήκη των ανιουσών αλυσίδων επί τού συνόλου των αριστερών (και αντιστοίχως, των δεξιών) ιδεωδών του. □

9.1.4 Ορισμός. Κάθε δακτύλιος R, ο οποίος ικανοποιεί μία (και, ως εκ τούτου, και τις δύο) εκ των συνθηκών (i), (ii) τού θεωρήματος 9.1.3, ονομάζεται **εξ αριστερών** (και αντιστοίχως, **εκ δεξιών**) **δακτύλιος τής Noether** ή **εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός δακτύλιος**[1]. Ένας δακτύλιος R καλείται **ναιτεριανός δακτύλιος** όταν είναι ταυτοχρόνως και εξ αριστερών και εκ δεξιών ναιτεριανός. (Προφανώς, για τους *μεταθετικούς* δακτυλίους οι έννοιες «εξ αριστερών ναιτεριανός», «εκ δεξιών ναιτεριανός» και «ναιτεριανός» ταυτίζονται, ενώ για τους *μη μεταθετικούς* δακτυλίους είναι εν γένει διαφορετικές.) Τέλος, κάθε ναιτεριανός δακτύλιος, ο οποίος τυγχάνει να είναι ακεραία περιοχή, ονομάζεται **ναιτεριανή περιοχή**.

9.1.5 Πρόταση. *Εάν η $f : R \longrightarrow S$ είναι ένας επιμορφισμός δακτυλίων και ο R είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός δακτύλιος, τότε και ο S είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός.*

Απόδειξη. Έστω

$$J_1 \subseteq J_2 \subseteq \cdots \subseteq J_n \subseteq J_{n+1} \subseteq \cdots \tag{9.1}$$

μια ανιούσα αλυσίδα αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού S. Θέτοντας $I_\nu := f^{-1}(J_\nu)$ για κάθε $\nu \in \mathbb{N}$, σχηματίζουμε μια ανιούσα αλυσίδα αριστερών (και αντιστοίχως, δεξιών)

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

τού R (βλ. 8.2.1 (ii)). Επειδή ο R είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός, η εν λόγω αλυσίδα είναι *στάσιμη*, ήτοι υπάρχει $k \in \mathbb{N}$ με $I_n = I_k$ για κάθε φυσικό αριθμό $n \geqslant k$. Εξάλλου, επειδή εξ υποθέσεως η απεικόνιση f είναι επιρριπτική, έχουμε $J_\nu = f(f^{-1}(J_\nu)) = f(I_\nu)$ για κάθε $\nu \in \mathbb{N}$ (βλ. απόδειξη τού θεωρήματος 8.2.4), οπότε και η αλυσίδα (9.1) είναι κατ' ανάγκην στάσιμη. Ως εκ τούτου, και ο S είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός. □

[1] Προς τιμήν τής Emmy Noether (1882-1935), η οποία μελέτησε (περί τη δεκαετία τού 1920) τις ιδιότητες των αλυσίδων ιδεωδών και κατέδειξε τη θεωρητική σημασία τους.

9.1.6 Πόρισμα. *Εάν οι R και S είναι δυο ισόμορφοι δακτύλιοι και ο ένας εξ αυτών εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός, τότε και ο άλλος είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός.*

9.1.7 Πόρισμα. *Έστω R ένας εξ αριστερών (και αντιστοίχως, ένας εκ δεξιών) ναιτεριανός δακτύλιος και έστω I ένα ιδεώδες τού R. Τότε και ο πηλικοδακτύλιος R/I είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός.*

Απόδειξη. Έπεται άμεσα ύστερα από εφαρμογή τής προτάσεως 9.1.5 για τον φυσικό επιμορφισμό $\pi_I^R : R \longrightarrow R/I$. □

9.1.8 Λήμμα. *Έστω $f : R \longrightarrow S$ ένας επιμορφισμός δακτυλίων. Εάν τα I, J είναι δυο (αριστερά, δεξιά ή αμφίπλευρα) ιδεώδη τού R με*

$$I \subseteq J, \quad I \cap \mathrm{Ker}(f) = J \cap \mathrm{Ker}(f) \text{ και } \quad f(I) = f(J),$$

τότε $I = J$.

Απόδειξη. Αρκεί να αποδειχθεί ότι $J \subseteq I$. Έστω τυχόν στοιχείο $a \in J$. Προφανώς, $f(a) \in f(J) = f(I)$, οπότε υπάρχει κάποιο $b \in I$, τέτοιο ώστε να ισχύει

$$f(a) = f(b) \Longrightarrow f(a-b) = 0_S \Longrightarrow a - b \in \mathrm{Ker}(f).$$

Επειδή $b \in I \subseteq J$, έχουμε

$$a, b \in J \Longrightarrow a - b \in J \Longrightarrow a - b \in J \cap \mathrm{Ker}(f) = I \cap \mathrm{Ker}(f) \subseteq I.$$

Επομένως, $b \in I$ και $a - b \in I \Rightarrow (a-b) + b = a \in I$. Άρα όντως $J \subseteq I$. □

9.1.9 Πρόταση. *Έστω $f : R \longrightarrow S$ ένας επιμορφισμός δακτυλίων. Εάν αμφότεροι οι $\mathrm{Ker}(f)$ και S είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανοί δακτύλιοι, τότε και ο ίδιος ο R είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός.*

Απόδειξη. Θεωρούμε *τυχούσα* ανιούσα αλυσίδα αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού R

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

Εξ υποθέσεως, η ανιούσα αλυσίδα αριστερών (και αντιστοίχως, δεξιών) ιδεωδών

$$I_1 \cap \mathrm{Ker}(f) \subseteq I_2 \cap \mathrm{Ker}(f) \subseteq \cdots \subseteq I_n \cap \mathrm{Ker}(f) \subseteq I_{n+1} \cap \mathrm{Ker}(f) \subseteq \cdots$$

τού $\mathrm{Ker}(f)$ οφείλει να είναι στάσιμη, οπότε $\exists \nu \in \mathbb{N} : I_n \cap \mathrm{Ker}(f) = I_\nu \cap \mathrm{Ker}(f)$ για κάθε φυσικό αριθμό $n \geqslant \nu$. Κατ' αναλογίαν, η ανιούσα αλυσίδα αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού S

$$f(I_1) \subseteq f(I_2) \subseteq \cdots \subseteq f(I_n) \subseteq f(I_{n+1}) \subseteq \cdots$$

οφείλει να είναι στάσιμη, οπότε $\exists \xi \in \mathbb{N} : f(I_n) = f(I_\xi)$ για κάθε φυσικό αριθμό $n \geqslant \xi$. Θέτοντας $k := \max\{\nu, \xi\}$, παρατηρούμε ότι

$$I_k \subseteq I_n, \quad I_k \cap \mathrm{Ker}(f) = I_n \cap \mathrm{Ker}(f) \text{ και } \quad f(I_k) = f(I_n),$$

για κάθε φυσικό αριθμό $n \geqslant k$. Το προηγηθέν λήμμα 9.1.8 μας πληροφορεί ότι $I_n = I_k$ για κάθε φυσικό αριθμό $n \geqslant k$, οπότε και η αρχικώς θεωρηθείσα ανιούσα αλυσίδα αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού R είναι στάσιμη. Αυτό σημαίνει ότι και ο ίδιος ο δακτύλιος R είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός. □

9.1.10 Πόρισμα. *Έστω R ένας δακτύλιος. Εάν ένα ιδεώδες αυτού I (ιδωμένο ως «αυτόνομος» δακτύλιος) και ο πηλικοδακτύλιος R/I είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανοί, τότε και ο ίδιος ο R είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός δακτύλιος.*

Απόδειξη. Έπεται άμεσα ύστερα από εφαρμογή τής προτάσεως 9.1.9 για τον φυσικό επιμορφισμό $\pi_I^R : R \longrightarrow R/I$. □

9.1.11 Θεώρημα. *Για έναν μεταθετικό δακτύλιο R τα ακόλουθα είναι ισοδύναμα:*

(i) *Ο R είναι ναιτεριανός δακτύλιος.*

(ii) *Κάθε ιδεώδες τού R είναι πεπερασμένως παραγόμενο, ήτοι μπορεί να παραχθεί από πεπερασμένου πλήθους στοιχεία τού R.*

Απόδειξη. (i)⇒(ii) Έστω I *τυχόν* ιδεώδες τού R. Εάν το I είναι κύριο ιδεώδες, τότε αυτό παράγεται εξ ορισμού από ένα στοιχείο τού R. Στην περίπτωση κατά την οποία $\langle r\rangle \subsetneqq I$ *για κάθε* $r \in I$, θεωρώντας ένα στοιχείο $a_1 \in I$ και ένα στοιχείο $a_2 \in I \smallsetminus \langle a_1\rangle$ λαμβάνουμε

$$\langle a_1\rangle \subsetneqq \langle a_1, a_2\rangle \subseteq I.$$

Εάν $I = \langle a_1, a_2\rangle$, τότε το I είναι προδήλως πεπερασμένως παραγόμενο. Στην περίπτωση κατά την οποία $\langle a_1, a_2\rangle \subsetneqq I$, θεωρώντας ένα στοιχείο $a_3 \in I \smallsetminus \langle a_1, a_2\rangle$ λαμβάνουμε

$$\langle a_1\rangle \subsetneqq \langle a_1, a_2\rangle \subsetneqq \langle a_1, a_2, a_3\rangle \subseteq I.$$

Εάν $I = \langle a_1, a_2, a_3\rangle$, τότε το I είναι προδήλως πεπερασμένως παραγόμενο. Ειδάλλως, επαναλαμβάνουμε την ίδια διαδικασία θεωρώντας κάποιο $a_4 \in I \smallsetminus \langle a_1, a_2, a_3\rangle$ κ.ο.κ. Προφανώς, αυτή περατούται ύστερα από πεπερασμένου πλήθους βήματα, ήτοι $\exists k \in \mathbb{N} : I = \langle a_1, \ldots, a_k\rangle$, διότι αλλιώς θα ήταν δυνατόν να κατασκευασθεί μια μη στάσιμη ανιούσα αλυσίδα ιδεωδών τού R

$$\langle a_1\rangle \subsetneqq \langle a_1, a_2\rangle \subsetneqq \cdots \subsetneqq \langle a_1, \ldots, a_n\rangle \subsetneqq \langle a_1, \ldots, a_n, a_{n+1}\rangle \subsetneqq \cdots,$$

οπότε θα καταλήγαμε σε αντίφαση.

(ii)⇒(i) Θεωρούμε *τυχούσα* ανιούσα αλυσίδα ιδεωδών τού R

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots \tag{9.2}$$

Η ένωση $\bigcup_{n=1}^{\infty} I_n$ είναι ιδεώδες τού δακτυλίου R (βλ. άσκηση 2 τού φυλλαδίου 12), οπότε (εξ υποθέσεως) $\exists k \in \mathbb{N}$ και $a_1, \ldots, a_k \in R$, τέτοια ώστε $\bigcup_{n=1}^{\infty} I_n = \langle a_1, \ldots, a_k\rangle$. Επειδή

$$a_1, \ldots, a_k \in \bigcup_{n=1}^{\infty} I_n \Rightarrow [\exists j_1, \ldots, j_k \in \mathbb{N} : a_1 \in I_{j_1}, \ldots, a_k \in I_{j_k}],$$

θέτοντας $\nu := \max\{j_1, \ldots, j_k\}$ λαμβάνουμε

$$a_1, \ldots, a_k \in I_\nu \Longrightarrow \bigcup_{n=1}^{\infty} I_n \subseteq I_\nu.$$

Όμως το I_ν είναι ένα εκ των ιδεωδών που συγκροτούν την αλυσίδα (9.2), οπότε έχουμε την εγκλειστική σχέση $I_\nu \subseteq \bigcup_{n=1}^{\infty} I_n$. Ως εκ τούτου,

$$I_\nu = \bigcup_{n=1}^{\infty} I_n \Rightarrow [I_\nu = I_{\nu+1} = I_{\nu+2} = \cdots] \Rightarrow \text{ η (9.2) είναι στάσιμη}$$

και ο R είναι ναιτεριανός δακτύλιος. □

9.1.12 Παραδείγματα. (i) Ο δακτύλιος $\mathbb{Z}$ των ακεραίων αριθμών είναι ναιτεριανή περιοχή (βλ. πρόταση 7.2.6).

(ii) Κάθε σώμα είναι προφανώς ναιτεριανή περιοχή (αφού διαθέτει μόνον δύο ιδεώδη, τα οποία είναι κύρια ιδεώδη).

(iii) Ο δακτύλιος

$$\mathcal{C}(\mathbb{R}) := \{ f \in \mathbb{R}^{\mathbb{R}} \mid f \text{ συνεχής} \}$$

δεν είναι ναιτεριανός, διότι θέτοντας $I_n := \left\{ f \in \mathcal{C}(\mathbb{R}) \ : \ f|_{[0,\frac{1}{n}]} = 0 \right\}, \forall n \in \mathbb{N}$, τα I_n είναι ιδεώδη τού $\mathcal{C}(\mathbb{R})$ με

$$I_1 \subsetneqq I_2 \subsetneqq \cdots \subsetneqq I_n \subsetneqq I_{n+1} \subsetneqq \cdots$$

(iv) Θεωρούμε τον μη μεταθετικό δακτύλιο

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| \, a \in \mathbb{Z} \text{ και } b, c \in \mathbb{Q} \right\} \subsetneqq \mathrm{Mat}_{2\times 2}(\mathbb{Q}).$$

Θα αποδείξουμε ότι ο R είναι εκ δεξιών ναιτεριανός αλλά δεν είναι εξ αριστερών ναιτεριανός. Το υποσύνολο

$$I = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in R \middle| \, a = c = 0 \text{ και } b \in \mathbb{Q} \right\}$$

αποτελεί (αμφίπλευρο) ιδεώδες τού R, διότι για οιαδήποτε $a \in \mathbb{Z}$ και $b, b', c \in \mathbb{Q}$ έχουμε

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ab' \\ 0 & 0 \end{pmatrix} \in I$$

και

$$\begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & b'c \\ 0 & 0 \end{pmatrix} \in I.$$

Είναι εύκολο να διαπιστωθεί ότι τα μόνα *δεξιά* ιδεώδη τού R που περιέχονται στο I είναι τα (αμφίπλευρα) ιδεώδη $\{0_R\}$ και I. Άρα το I (ιδωμένο ως «αυτόνομος» δακτύλιος) είναι *εκ δεξιών* ναιτεριανός δακτύλιος. Η απεικόνιση

$$f : R \longrightarrow \mathbb{Z} \times \mathbb{Q}, \ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \longmapsto f\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right) := (a, c),$$

είναι επιμορφισμός δακτυλίων με $\mathrm{Ker}(f) = I$. Σύμφωνα με το 1ο θεώρημα ισομορφισμών 8.3.3, $R/I \cong \mathbb{Z} \times \mathbb{Q}$. Επειδή (κατά τα (i) και (ii)) οι $\mathbb{Z}$ και $\mathbb{Q}$ είναι (μεταθετικοί) ναιτεριανοί δακτύλιοι και -ιδιαιτέρως- εκ δεξιών ναιτεριανοί, ο $\mathbb{Z} \times \mathbb{Q}$ είναι εκ δεξιών ναιτεριανός. Κατ' επέκταση, και ο πηλικοδακτύλιος R/I είναι εκ δεξιών ναιτεριανός (βλ. πόρισμα 9.1.7). Από το πόρισμα 9.1.10 έπεται ότι και ο ίδιος ο R είναι εκ δεξιών ναιτεριανός. Από την άλλη μεριά, για κάθε $j \in \mathbb{N}$ τα υποσύνολα

$$I_j := \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in I \middle| \, \exists m \in \mathbb{Z} : b = \frac{m}{2^j} \right\} \subsetneqq R$$

αποτελούν *αριστερά* ιδεώδη τού R, διότι για οιαδήποτε $a, m \in \mathbb{Z}$ και $b, c \in \mathbb{Q}$ έχουμε

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & \frac{m}{2^j} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \frac{am}{2^j} \\ 0 & 0 \end{pmatrix} \in I_j.$$

Επιπροσθέτως, $I_j \subsetneqq I_{j+1}$, διότι

$$\begin{pmatrix} 0 & \frac{m}{2^j} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \frac{2m}{2^{j+1}} \\ 0 & 0 \end{pmatrix} \in I_{j+1}, \ \begin{pmatrix} 0 & \frac{1}{2^{j+1}} \\ 0 & 0 \end{pmatrix} \in I_{j+1} \setminus I_j,$$

για κάθε $m \in \mathbb{Z}$ και κάθε $j \in \mathbb{N}$. Κατά συνέπειαν, σχηματίζεται μια *μη στάσιμη* ανιούσα αλυσίδα αριστερών ιδεωδών τού R

$$I_1 \subsetneqq I_2 \subsetneqq \cdots \subsetneqq I_n \subsetneqq I_{n+1} \subsetneqq \cdots$$

Αυτό σημαίνει ότι ο R δεν είναι εξ αριστερών ναιτεριανός. (Παρομοίως κατασκευάζεται και ένα παράδειγμα ενός δακτυλίου που είναι εξ αριστερών αλλά όχι και εκ δεξιών ναιτεριανός. Βλ. άσκηση 22 τού φυλλαδίου 12.)

9.1.13 Πρόταση. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Τότε κάθε ιδεώδες τής τετραγωνικής αριθμητικής περιοχής*

$$\mathbb{Z}[\sqrt{m}] = \left\{ a + b\sqrt{m} \in \mathbb{Z} \;\middle|\; a, b \in \mathbb{Z} \right\} \subsetneqq \mathbb{C}$$

(βλ. άσκηση 24 τού φυλλαδίου 11) *μπορεί να παραχθεί από δύο (όχι κατ' ανάγκην διαφορετικά) στοιχεία. (Ως εκ τούτου, η $\mathbb{Z}[\sqrt{m}]$ είναι ναιτεριανή περιοχή.)*

Απόδειξη. Έστω I τυχόν ιδεώδες τού $\mathbb{Z}[\sqrt{m}]$. Θέτοντας

$$I_1 := I \cap \mathbb{Z}, \quad I_2 := \left\{ b \in \mathbb{Z} \mid a + b\sqrt{m} \in I, \text{ για κάποιον } a \in \mathbb{Z} \right\},$$

η απόδειξη τής προτάσεως απορρέει από τα ακόλουθα:

(i) Τα I_1 και I_2 είναι ιδεώδη τού $\mathbb{Z}$.

(ii) $I_1 \subseteq I_2$.

(iii) Σύμφωνα με την πρόταση 7.2.6 υπάρχουν $r_1, r_2 \in \mathbb{Z}$, τέτοια ώστε $I_1 = \langle r_1 \rangle$, $I_2 = \langle r_2 \rangle$. Επιπροσθέτως, επειδή $r_2 \in I_2$, υπάρχει κάποιο $c \in \mathbb{Z}$, τέτοιο ώστε να ισχύει $c + r_2\sqrt{m} \in I$. Το I ισούται με

$$I = \left\langle r_1, c + r_2\sqrt{m} \right\rangle = \mathbb{Z}[\sqrt{m}]\, r_1 + \mathbb{Z}[\sqrt{m}]\, \left(c + r_2\sqrt{m}\right). \tag{9.3}$$

Απόδειξη τού (i): Εάν $a_1, a_2 \in I_1$, τότε, επειδή ο $\mathbb{Z}$ είναι δακτύλιος και το I ιδεώδες τού $\mathbb{Z}[\sqrt{m}]$, έχουμε

$$\left.\begin{array}{r} a_1, a_2 \in \mathbb{Z} \Longrightarrow a_1 - a_2 \in \mathbb{Z} \\ a_1, a_2 \in I \Longrightarrow a_1 - a_2 \in I \end{array}\right\} \Longrightarrow a_1 - a_2 \in I_1.$$

Και εάν $k \in \mathbb{Z}$ και $a \in I_1$, τότε, κατ' αναλογίαν,

$$\left.\begin{array}{r} k, a \in \mathbb{Z} \Longrightarrow ka \in \mathbb{Z} \\ k, a \in I \Longrightarrow ka \in I \end{array}\right\} \Longrightarrow ka \in I_1.$$

Άρα το I_1 είναι ιδεώδες τού $\mathbb{Z}$. Από την άλλη μεριά, εάν $b_1, b_2 \in I_2$, τότε υπάρχουν $a_1, a_2 \in \mathbb{Z}$, ούτως ώστε

$$\left.\begin{array}{r} a_1 + b_1\sqrt{m} \in I \\ a_2 + b_2\sqrt{m} \in I \end{array}\right\} \Longrightarrow (a_1 - a_2) + (b_1 - b_2)\sqrt{m} \in I \Longrightarrow b_1 - b_2 \in I_2.$$

Και εάν $k \in \mathbb{Z}$ και $b \in I_2$, τότε υπάρχει $a \in \mathbb{Z}$, ούτως ώστε

$$\left.\begin{array}{r} a + b\sqrt{m} \in I \\ k \in \mathbb{Z} \subseteq \mathbb{Z}[\sqrt{m}] \end{array}\right\} \Longrightarrow ka + kb\sqrt{m} \in I \Longrightarrow kb \in I_2.$$

Άρα *και* το I_2 είναι ιδεώδες τού $\mathbb{Z}$.

Απόδειξη τού (ii): Για οιοδήποτε $a \in I_1$ έχουμε $a \in \mathbb{Z}$ και $a \in I$. Άρα

$$\left.\begin{array}{r} a \in I \\ \sqrt{m} \in \mathbb{Z}[\sqrt{m}] \end{array}\right\} \Longrightarrow a\sqrt{m} \in I \Longrightarrow a \in I_2.$$

Απόδειξη τού (iii): Κατ' αρχάς παρατηρούμε ότι

$$\left.\begin{array}{r} r_1 \in I_1 \Longrightarrow r_1 \in I \\ c + r_2\sqrt{m} \in I \end{array}\right\} \Longrightarrow \left\langle r_1, c + r_2\sqrt{m} \right\rangle \subseteq I.$$

Έστω τώρα τυχόν $r + s\sqrt{m} \in I$, $r, s \in \mathbb{Z}$. Επειδή $s \in I_2 = \langle r_2 \rangle$, υπάρχει κάποιο στοιχείο $s' \in \mathbb{Z} \subseteq \mathbb{Z}[\sqrt{m}]$ με $s = s'r_2$. Εξάλλου, επειδή

$$\left.\begin{array}{r} r + s\sqrt{m} \in I \\ s'\left(c + r_2\sqrt{m}\right) \in I \end{array}\right\} \Longrightarrow r + s\sqrt{m} - s'\left(c + r_2\sqrt{m}\right) = r - s'c \in I,$$

και $r - s'c \in \mathbb{Z}$, έχουμε $r - s'c \in I_1 = \langle r_1 \rangle$, οπότε υπάρχει $t \in \mathbb{Z}$, τέτοιο ώστε

$$r - s'c = t\, r_1 \Longrightarrow r = t\, r_1 + s'c.$$

Ως εκ τούτου,

$$r + s\sqrt{m} = t\, r_1 + s'\left(c + r_2\sqrt{m}\right) \in \left\langle r_1, c + r_2\sqrt{m} \right\rangle \Longrightarrow I \subseteq \left\langle r_1, c + r_2\sqrt{m} \right\rangle,$$

οπότε εν τέλει οι ισότητες (9.3) είναι αληθείς. □

9.1.14 Σημείωση. Οι υποδακτύλιοι ναιτεριανών δακτυλίων *δεν* είναι απαραιτήτως ναιτεριανοί. Τούτο έγκειται στο ότι ένα ιδεώδες ενός υποδακτυλίου δεν είναι κατ' ανάγκην ιδεώδες και ολοκλήρου τού δακτυλίου αναφοράς. Επί παραδείγματι, για κάθε $n \in \mathbb{N}$ ορίζεται μια ακεραία συνάρτηση (ήτοι μια ολόμορφη συνάρτηση μιας μεταβλητής ορισμένη επί ολοκλήρου τού $\mathbb{C}$) μέσω τού απειρογινομένου

$$f_n(z) := \pi z \prod_{k=n}^{\infty} \left(1 + \frac{z}{k}\right)\left(1 - \frac{z}{k}\right),\ \forall z \in \mathbb{C},$$

(με $f_1(z) = \sin(\pi z)$), για την οποία ισχύει

$$f_n(z) = 0 \Longleftrightarrow z \in \{0\} \cup \{\pm n, \pm(n+1), \pm(n+2), \ldots\}.$$

Επειδή

$$\langle f_1(z)\rangle \subsetneqq \langle f_2(z)\rangle \subsetneqq \cdots \subsetneqq \langle f_n(z)\rangle \subsetneqq \langle f_{n+1}(z)\rangle \subsetneqq \cdots$$

η ακεραία περιοχή $\mathcal{O}(\mathbb{C})$ είναι μη ναιτεριανός δακτύλιος (βλ. 8.5.6 (iii)), παρότι είναι εμφυτευμένη στο σώμα των κλασμάτων της $\mathcal{M}(\mathbb{C}) := \mathbf{Fr}(\mathcal{O}(\mathbb{C}))$, ήτοι στο σώμα των *μερομόρφων συναρτήσεων* (επί ολοκλήρου τού $\mathbb{C}$), και το $\mathcal{M}(\mathbb{C})$ είναι (προφανώς) ναιτεριανός δακτύλιος.

9.1.15 Θεώρημα (Θεώρημα Βάσεως τού Hilbert). *Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Εάν ο R είναι ναιτεριανός, τότε και ο πολυωνυμικός δακτύλιος $R[\mathsf{X}]$ είναι ναιτεριανός.*

Απόδειξη[2]. Υποθέτοντας ότι ο $R[\mathsf{X}]$ δεν είναι ναιτεριανός δακτύλιος θα δείξουμε ότι και ο ίδιος ο R δεν είναι ναιτεριανός. Έστω λοιπόν I ένα ιδεώδες τού $R[\mathsf{X}]$ μη πεπερασμένως παραγόμενο. Τότε, εάν

$$\varphi_1(\mathsf{X}) \in I, \text{ με } \deg(\varphi_1(\mathsf{X})) = \min\left\{\deg(\varphi(\mathsf{X}))\,|\,\varphi(\mathsf{X}) \in I \smallsetminus \{0_{R[\mathsf{X}]}\}\right\},$$

[2] Αυτή η σύντομη και πολύ κομψή απόδειξη τού θεωρήματος βάσεως τού Hilbert οφείλεται στη μαθηματικό H. Sarges. (*Ein Beweis des Hilbertschen Basissatzes*, J. reine ang. Math. **283/284** (1976), 436-437.)

μπορούμε να ορίσουμε διαδοχικώς πολυώνυμα:

$$\varphi_{k+1}(\mathsf{X}) \in I \smallsetminus \langle \varphi_1(\mathsf{X}), \ldots, \varphi_k(\mathsf{X}) \rangle ,$$

με

$$\deg(\varphi_{k+1}(\mathsf{X})) = \min \{ \deg(\varphi(\mathsf{X})) | \, \varphi(\mathsf{X}) \in I \smallsetminus \langle \varphi_1(\mathsf{X}), \ldots, \varphi_k(\mathsf{X}) \rangle \} ,$$

για $k = 1, 2, 3, \ldots$, και να θέσουμε $n_k := \deg(\varphi_k(\mathsf{X}))$, $R \ni a_k := \text{LC}(\varphi_k(\mathsf{X}))$. Κατ' αυτόν τον τρόπο τού ορισμού των $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X}), \ldots$ διασφαλίζεται αφ' ενός μεν η ισχύς των ανισοϊσοτήτων

$$n_1 \leqslant n_2 \leqslant \cdots \leqslant n_k \leqslant n_{k+1} \leqslant \cdots ,$$

αφ' ετέρου δε η ισχύς των ακολούθων εγκλειστικών σχέσεων

$$\langle a_1 \rangle \subseteq \langle a_1, a_2 \rangle \subseteq \langle a_1, a_2, a_3 \rangle \subseteq \cdots \subseteq \langle a_1, \ldots, a_k \rangle \subseteq \langle a_1, \ldots, a_k, a_{k+1} \rangle \subseteq \cdots$$

Θα δείξουμε ότι αυτή η ανιούσα αλυσίδα ιδεωδών τού R δεν είναι στάσιμη. Πράγματι· εάν για κάποιον φυσικό αριθμό k είχαμε

$$\langle a_1, \ldots, a_k \rangle = \langle a_1, \ldots, a_k, a_{k+1} \rangle ,$$

τότε το a_{k+1} θα εγράφετο ως

$$a_{k+1} = \sum_{i=1}^{k} b_i a_i , \quad (b_i \in R, \ \forall i, \ 1 \leqslant i \leqslant k) ,$$

οπότε το πολυώνυμο

$$\begin{aligned} I \smallsetminus \langle \varphi_1(\mathsf{X}), \ldots, \varphi_k(\mathsf{X}) \rangle \quad \ni \quad & \psi(\mathsf{X}) := \varphi_{k+1}(\mathsf{X}) - \sum_{i=1}^{k} b_i \, \mathsf{X}^{n_{k+1}-n_i} \, \varphi_i(\mathsf{X}) \\ = \quad & (a_{k+1}\mathsf{X}^{n_{k+1}} + \cdots) - \sum_{i=1}^{k} b_i \, \mathsf{X}^{n_{k+1}-n_i} \, (a_i \mathsf{X}^{n_i} + \cdots) \end{aligned}$$

θα είχε βαθμό $\deg(\psi(\mathsf{X})) < \deg(\varphi_{k+1}(\mathsf{X}))$, πράγμα άτοπο επί τη βάσει τής επιλογής τού $\varphi_{k+1}(\mathsf{X})$. Επομένως, η εν λόγω αλυσίδα ιδεωδών δεν είναι στάσιμη και, ως εκ τούτου, ο R δεν είναι ναιτεριανός δακτύλιος. □

9.1.16 Πόρισμα. *Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Εάν ο R είναι ναιτεριανός, τότε και ο δακτύλιος $R[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ είναι ναιτεριανός.*

Απόδειξη. Αρκεί να εφαρμοσθεί το θεώρημα 9.1.15 και μαθηματική επαγωγή ως προς τον n. □

9.1.17 Λήμμα. *Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Εάν για κάθε $m \in \mathbb{N}_0$ θέσουμε*

$$J_m := \{ \varphi(\mathsf{X}) \in R[\![\mathsf{X}]\!] | \, \text{ord}(\varphi(\mathsf{X})) \geqslant m \} , \tag{9.4}$$

τότε το J_m αποτελεί ένα ιδεώδες τού δακτυλίου $R[\![\mathsf{X}]\!]$. Επιπροσθέτως, $J_m = \langle \mathsf{X}^m \rangle$.

Απόδειξη. Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in J_m$, τότε $-\psi(\mathsf{X}) \in J_m$ ($\text{ord}(-\psi(\mathsf{X})) = \text{ord}(-\psi(\mathsf{X}))$ και $\varphi(\mathsf{X}) - \psi(\mathsf{X}) \in J_m$, διότι

$$\text{ord}\,(\varphi(\mathsf{X}) - \psi(\mathsf{X})) \geqslant \min\{\text{ord}\,(\varphi(\mathsf{X})), \text{ord}(-\psi(\mathsf{X}))\} \geqslant m.$$

(Βλ. 6.3.5 (i).) Εξάλλου, εάν $\varphi(\mathsf{X}) \in J_m$ και $\psi(\mathsf{X}) \in J_m$, τότε $\varphi(\mathsf{X})\psi(\mathsf{X}) \in J_m$, διότι

$$\operatorname{ord}\left(\varphi(\mathsf{X})\psi(\mathsf{X})\right) \geqslant \operatorname{ord}\left(\varphi(\mathsf{X})\right) + \operatorname{ord}(\psi(\mathsf{X})) \geqslant \operatorname{ord}\left(\varphi(\mathsf{X})\right) + m \geqslant m.$$

(Βλ. 6.3.5 (ii).) Άρα το J_m είναι όντως ένα ιδεώδες τού $R[\![\mathsf{X}]\!]$. Επιπροσθέτως,

$$[\varphi(\mathsf{X}) \in J_0 \Leftrightarrow \operatorname{ord}\left(\varphi(\mathsf{X})\right) \geqslant 0] \Rightarrow J_0 = R[\![\mathsf{X}]\!]$$

και για $m \in \mathbb{N}$ και $\varphi(\mathsf{X}) = \sum_{i=0}^{\infty} a_i \mathsf{X}^i \in J_m$ έχουμε $a_0 = a_1 = \cdots = a_{m-1} = 0_R$, οπότε

$$\varphi(\mathsf{X}) = \mathsf{X}^m \chi(\mathsf{X}), \quad \text{όπου} \quad \chi(\mathsf{X}) := \textstyle\sum_{i=m}^{\infty} a_i \mathsf{X}^{i-m}$$

με $\operatorname{ord}(\chi(\mathsf{X})) \geqslant 0$. Επομένως, $J_m = \langle \mathsf{X}^m \rangle$. □

9.1.18 Θεώρημα. *Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Εάν ο R είναι ναιτεριανός, τότε και ο δακτύλιος των επίτυπων δυναμοσειρών $R[\![\mathsf{X}]\!]$ με συντελεστές ειλημμένους από τον R είναι ναιτεριανός.*

Απόδειξη. Έστω $\mathcal{I}$ τυχόν ιδεώδες τού δακτυλίου $R[\![\mathsf{X}]\!]$. Εάν $\mathcal{I} = \{0_{R[\![\mathsf{X}]\!]}\}$, τότε έχουμε $\mathcal{I} = \langle 0_{R[\![\mathsf{X}]\!]} \rangle$. Εάν το $\mathcal{I}$ δεν είναι τετριμμένο, τότε για κάθε $j \in \mathbb{N}_0$ θέτουμε

$$I_j := \left\{ s_j \in R \;\middle|\; \begin{array}{c} \exists \psi_j(\mathsf{X}) \in R[\![\mathsf{X}]\!] : \operatorname{ord}(\psi_j(\mathsf{X})) > j \\ \text{και } s_j \mathsf{X}^j + \psi_j(\mathsf{X}) \in \mathcal{I} \end{array} \right\}.$$

Το I_j αποτελεί ένα ιδεώδες τού R. Πράγματι· εάν $s_j, s'_j \in I_j$, τότε υπάρχουν επίτυπες δυναμοσειρές $\psi_j(\mathsf{X}), \psi'_j(\mathsf{X}) \in R[\![\mathsf{X}]\!]$, τέτοιες ώστε να ισχύει

$$\begin{aligned} \operatorname{ord}(\psi_j(\mathsf{X})) > j \quad &\text{και} \quad s_j \mathsf{X}^j + \psi_j(\mathsf{X}) \in \mathcal{I}, \\ \operatorname{ord}(\psi'_j(\mathsf{X})) > j \quad &\text{και} \quad s'_j \mathsf{X}^j + \psi'_j(\mathsf{X}) \in \mathcal{I}. \end{aligned}$$

Άρα $\left(s_j \mathsf{X}^j + \psi_j(\mathsf{X})\right) - \left(s'_j \mathsf{X}^j + \psi'_j(\mathsf{X})\right) = \left(s_j - s'_j\right) \mathsf{X}^j + \left(\psi_j(\mathsf{X}) - \psi'_j(\mathsf{X})\right) \in \mathcal{I}$ και

$$\operatorname{ord}(\psi_j(\mathsf{X}) - \psi'_j(\mathsf{X})) \min\{\operatorname{ord}\left(\psi_j(\mathsf{X})\right), \operatorname{ord}(\psi'_j(\mathsf{X}))\} \geqslant j,$$

απ' όπου έπεται ότι $s_j - s'_j \in I_j$. Επιπλέον, εάν $r \in R$ και $s_j \in I_j$, τότε υπάρχει επίτυπη δυναμοσειρά $\psi_j(\mathsf{X}) \in R[\![\mathsf{X}]\!]$, τέτοια ώστε να ισχύει

$$\begin{aligned} & [\operatorname{ord}(\psi_j(\mathsf{X})) > j \quad \text{και} \quad s_j \mathsf{X}^j + \psi_j(\mathsf{X}) \in \mathcal{I}] \\ \Rightarrow \quad & [\operatorname{ord}(r\psi_j(\mathsf{X})) > j \quad \text{και} \quad r s_j \mathsf{X}^j + r\psi_j(\mathsf{X}) \in \mathcal{I}], \end{aligned}$$

οπότε $r s_j \in I_j$. Σημειωτέον ότι για οιοδήποτε $s_j \in I_j$ υπάρχει $\psi_j(\mathsf{X}) \in R[\![\mathsf{X}]\!]$ με

$$\begin{aligned} & [\operatorname{ord}(\psi_j(\mathsf{X})) > j \quad \text{και} \quad s_j \mathsf{X}^j + \psi_j(\mathsf{X}) \in \mathcal{I}] \\ \Rightarrow \quad & [\operatorname{ord}(\psi_j(\mathsf{X})\mathsf{X}) > j+1 \quad \text{και} \quad s_j \mathsf{X}^{j+1} + \psi_j(\mathsf{X})\mathsf{X} \in \mathcal{I}], \end{aligned}$$

απ' όπου έπεται ότι $s_j \in I_{j+1} \Rightarrow I_j \subseteq I_{j+1}$. Επειδή ο R είναι εξ υποθέσεως ναιτεριανός και

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq I_j \subseteq I_{j+1} \subseteq \cdots,$$

υπάρχει $m \in \mathbb{N}_0$, τέτοιος ώστε να ισχύει $I_j = I_m$ για κάθε $j \geqslant m$. Επιπροσθέτως, καθένα εκ των ιδεωδών $I_0, \ldots, I_m$ είναι πεπερασμένως παραγόμενο. (Βλ. θεώρημα 9.1.11.) Άρα για κάθε $j \in \{0, \ldots, m\}$ υπάρχουν $s_{j,1}, \ldots, s_{j,k_j} \in R$ ($k_j \in \mathbb{N}$) με

$$I_j = \left\langle s_{j,1}, \ldots, s_{j,k_j} \right\rangle.$$

Ιδιαιτέρως, για κάθε $i \in \{1, \ldots, k_j\}$ υπάρχουν $\psi_{j,i}(\mathsf{X}) \in R[\![\mathsf{X}]\!]$ με

$$\operatorname{ord}(\psi_{j,i}(\mathsf{X})) > j \quad \text{και} \quad \varphi_{j,i}(\mathsf{X}) := s_{j,i} \mathsf{X}^j + \psi_{j,i}(\mathsf{X}) \in \mathcal{I}.$$

Ισχυρισμός: Το ιδεώδες $\mathcal{I}$ είναι πεπερασμένως παραγόμενο. Συγκεκριμένα,

$$\mathcal{I} = \left\langle \bigcup_{j=0}^{m} \left\{ \varphi_{j,1}(\mathsf{X}), ..., \varphi_{j,k_j}(\mathsf{X}) \right\} \right\rangle. \tag{9.5}$$

Ο ισχυρισμός θα επαληθευθεί σε δύο βήματα. Στο πρώτο εξ αυτών θα αποδειχθεί ότι το ιδεώδες $\mathcal{I} \cap J_m$ τού $R[\![\mathsf{X}]\!]$ (όπου J_m το ιδεώδες το ορισθέν μέσω τής (9.4)) είναι πεπερασμένως παραγόμενο.

Βήμα 1ο. Έστω τυχούσα $\varphi(\mathsf{X}) \in \mathcal{I} \cap J_m$. Θέτοντας $n := \mathrm{ord}(\varphi(\mathsf{X}))$ αυτή μπορεί να γραφεί υπό τη μορφή $\varphi(\mathsf{X}) = s\mathsf{X}^n + \psi(\mathsf{X})$, όπου

$$s \in R \setminus \{0_R\} \text{ και } \psi(\mathsf{X}) \in R[\![\mathsf{X}]\!] : \mathrm{ord}(\psi(\mathsf{X})) \geqslant n \geqslant m.$$

Προφανώς, $s \in I_n = I_m$. Επειδή $I_m = \langle s_{m,1}, ..., s_{m,k_m} \rangle$,

$$\exists\, (r_{1,1}, ..., r_{1,k_m}) \in R^{k_m} : s = \sum_{i=1}^{k_m} r_{1,i} s_{m,i}.$$

Θέτοντας $\chi_1(\mathsf{X}) := \sum_{i=1}^{k_m} r_{1,i} \mathsf{X}^{n-m} \varphi_{m,i}(\mathsf{X})$, έχουμε $\chi_1(\mathsf{X}) \in \mathcal{I}$ και, ως εκ τούτου,

$$\varphi(\mathsf{X}) - \chi_1(\mathsf{X}) \in \mathcal{I} \quad \text{με} \quad \mathrm{ord}(\varphi(\mathsf{X}) - \chi_1(\mathsf{X})) =: n_1 \geqslant n \geqslant m.$$

Επαναλαμβάνοντας την ίδια διαδικασία (με την $\varphi(\mathsf{X}) - \chi_1(\mathsf{X})$ στη θέση τής $\varphi(\mathsf{X})$) μπορούμε να ορίσουμε μια επίτυπη δυναμοσειρά

$$\chi_2(\mathsf{X}) := \sum_{i=1}^{k_m} r_{2,i} \mathsf{X}^{n_1 - m} \varphi_{m,i}(\mathsf{X})$$

για κατάλληλα $r_{2,1}, ..., r_{2,k_m} \in R$ με $\varphi(\mathsf{X}) - \chi_1(\mathsf{X}) - \chi_2(\mathsf{X}) \in \mathcal{I}$ και

$$\mathrm{ord}(\varphi(\mathsf{X}) - \chi_1(\mathsf{X}) - \chi_2(\mathsf{X})) =: n_2 \geqslant n_1 \geqslant n \geqslant m.$$

Κατ' αυτόν τον τρόπο αποκτούμε (αναδρομικώς) μια ακολουθία επίτυπων δυναμοσειρών $(\chi_\nu(\mathsf{X}))_{\nu \in \mathbb{N}}$ ορίζοντας

$$\chi_\nu(\mathsf{X}) := \sum_{i=1}^{k_m} r_{\nu,i} \mathsf{X}^{n_\nu - m} \varphi_{m,i}(\mathsf{X})$$

για κατάλληλα $r_{\nu,1}, ..., r_{\nu,k_m} \in R$ με $\varphi(\mathsf{X}) - \sum_{\varrho=1}^{\nu} \chi_\varrho(\mathsf{X}) \in \mathcal{I}$ και

$$\mathrm{ord}(\varphi(\mathsf{X}) - \sum_{\varrho=1}^{\nu} \chi_\varrho(\mathsf{X})) =: n_\nu \geqslant n_{\nu-1} \geqslant \cdots \geqslant n_1 \geqslant n \geqslant m.$$

Εάν για κάθε $i \in \{1, ..., k_j\}$ θεωρήσουμε την επίτυπη δυναμοσειρά

$$\omega_i(\mathsf{X}) := \sum_{\nu=1}^{\infty} r_{\nu,i} \mathsf{X}^{n_\nu - m} \in R[\![\mathsf{X}]\!],$$

τότε

$$\varphi(\mathsf{X}) - \sum_{i=1}^{k_m} \omega_i(\mathsf{X}) \varphi_{m,i}(\mathsf{X}) = \varphi(\mathsf{X}) - \sum_{\nu=1}^{\infty} \chi_\nu(\mathsf{X}).$$

Επειδή η ακολουθία των τάξεων $n_\nu := \mathrm{ord}(\varphi(\mathsf{X}) - \sum_{\varrho=1}^{\nu} \chi_\varrho(\mathsf{X})), \nu = 1, 2, ...$ είναι *γνησίως αύξουσα*, λαμβάνουμε

$$\varphi(\mathsf{X}) - \sum_{\nu=1}^{\infty} \chi_\nu(\mathsf{X}) = 0_{R[\![\mathsf{X}]\!]} \Longrightarrow \varphi(\mathsf{X}) = \sum_{i=1}^{k_m} \omega_i(\mathsf{X}) \varphi_{m,i}(\mathsf{X}).$$

Κατά συνέπειαν,

$$\mathcal{I} \cap J_m = \langle \varphi_{m,1}(\mathsf{X}), ..., \varphi_{m,k_m}(\mathsf{X}) \rangle . \tag{9.6}$$

Βήμα 2ο. Στην περίπτωση όπου $m = 0$, η ισότητα (9.5) είναι προδήλως αληθής λόγω τής (9.6). Ας υποθέσουμε ότι $m \geqslant 1$ κι ας θεωρήσουμε μια επίτυπη δυναμοσειρά $\varphi(\mathsf{X}) \in \mathcal{I}$ έχουσα τάξη $\mathrm{ord}(\varphi(\mathsf{X})) = j$ για κάποιον $j \in \{0, ..., m-1\}$. Αυτή μπορεί να γραφεί υπό τη μορφή $\varphi(\mathsf{X}) = s\mathsf{X}^n + \psi(\mathsf{X})$, όπου

$$s \in R \setminus \{0_R\} \text{ και } \psi(\mathsf{X}) \in R[\![\mathsf{X}]\!] : \mathrm{ord}(\psi(\mathsf{X})) \geqslant j+1.$$

Επομένως, $s \in I_j \Rightarrow s = \sum_{i=1}^{k_j} r_{1,i} s_{j,i}$ για κατάλληλα $r_{1,1}, ..., r_{1,k_j} \in R$. Θέτοντας

$$\mathcal{I}' := \left\langle \bigcup_{j=0}^{m-1} \{\varphi_{j,1}(\mathsf{X}), ..., \varphi_{j,k_j}(\mathsf{X})\} \right\rangle \text{ και } \upsilon_1(\mathsf{X}) := \sum_{i=1}^{k_j} r_{1,i}\varphi_{j,i}(\mathsf{X}),$$

παρατηρούμε ότι $\upsilon_1(\mathsf{X}) \in \mathcal{I}' \subsetneqq \mathcal{I}$ με $\mathrm{ord}(\varphi(\mathsf{X}) - \upsilon_1(\mathsf{X})) =: j_1 \geqslant j+1 > j$. Εάν $j_1 < m$, τότε επαναλαμβάνοντας την ίδια διαδικασία (με την $\varphi(\mathsf{X}) - \upsilon_1(\mathsf{X})$ στη θέση τής $\varphi(\mathsf{X})$) μπορούμε να ορίσουμε μια επίτυπη δυναμοσειρά

$$\upsilon_2(\mathsf{X}) := \sum_{i=1}^{k_j} r_{2,i}\varphi_{j_1,i}(\mathsf{X}) \in \mathcal{I}'$$

για κατάλληλα $r_{2,1}, ..., r_{2,k_j} \in R$ με $\varphi(\mathsf{X}) - \upsilon_1(\mathsf{X}) - \upsilon_2(\mathsf{X}) \in \mathcal{I}' \subsetneqq \mathcal{I}$ και

$$\mathrm{ord}(\varphi(\mathsf{X}) - \upsilon_1(\mathsf{X}) - \upsilon_2(\mathsf{X})) =: j_2 \geqslant j_1 + 1 \geqslant j+1 > j.$$

Εάν $j_2 < m$, τότε επαναλαμβάνουμε τη διαδικασία, ορίζουμε $\upsilon_3(\mathsf{X}), \upsilon_4(\mathsf{X}), ...$ ανήκουσες στο $\mathcal{I}'$ κ.ο.κ., έως ότου συναντήσουμε εκείνον τον ελάχιστο φυσικό αριθμό ν για τον οποίο ισχύει

$$\mathrm{ord}(\varphi(\mathsf{X}) - (\upsilon_1(\mathsf{X}) + \upsilon_2(\mathsf{X}) + \cdots + \upsilon_\nu(\mathsf{X}))) \geqslant m.$$

Το άθροισμα $\upsilon(\mathsf{X}) := \upsilon_1(\mathsf{X}) + \cdots + \upsilon_\nu(\mathsf{X})$ ανήκει στο $\mathcal{I}' \subsetneqq \mathcal{I}$. Ως εκ τούτου,

$$[\varphi(\mathsf{X}) - \upsilon(\mathsf{X}) \in \mathcal{I} \text{ και } \mathrm{ord}(\varphi(\mathsf{X}) - \upsilon(\mathsf{X})) \geqslant m] \Rightarrow \varphi(\mathsf{X}) - \upsilon(\mathsf{X}) \in \mathcal{I} \cap J_m,$$

κάτι που (σε συνδυασμό με την (9.6)) σημαίνει ότι η ισότητα (9.5) είναι *και* σε αυτήν την περίπτωση αληθής. □

9.1.19 Πόρισμα. *Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Εάν ο R είναι ναιτεριανός, τότε και ο δακτύλιος $R[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!]$ είναι ναιτεριανός.*

Απόδειξη. Αρκεί να εφαρμοσθεί το θεώρημα 9.1.18 και μαθηματική επαγωγή ως προς τον n. □

9.2 ΔΑΚΤΥΛΙΟΙ ΚΥΡΙΩΝ ΙΔΕΩΔΩΝ

9.2.1 Ορισμός. Ένας δακτύλιος καλείται **δακτύλιος κυρίων ιδεωδών (=: Δ.Κ.Ι.)** όταν κάθε ιδεώδες του είναι κύριο. Επίσης, κάθε δακτύλιος κυρίων ιδεωδών, ο οποίος τυγχάνει να είναι -ταυτοχρόνως- και ακεραία περιοχή, καλείται **περιοχή κυρίων ιδεωδών (=: Π.Κ.Ι.).**

9.2.2 Πρόταση. *Κάθε Π.Κ.Ι. είναι ναιτεριανή περιοχή.*

Απόδειξη. Έπεται άμεσα από το θεώρημα 9.1.11. □

9.2.3 Πρόταση. *Κάθε σώμα είναι Π.Κ.Ι. και κάθε στρεβλό σώμα Δ.Κ.Ι.*

Απόδειξη. Τα μόνα ιδεώδη οιουδήποτε στρεβλού σώματος (= διαιρετικού δακτυλίου) είναι το τετριμμένο ιδεώδες και ο εαυτός του (βλ. 7.1.9), τα οποία είναι προφανώς κύρια ιδεώδη. Επιπροσθέτως, επειδή κάθε σώμα είναι ακεραία περιοχή (βλ. 6.2.22), οφείλει να είναι κατ' ανάγκην και Π.Κ.Ι. □

9.2.4 Πρόταση. *Ο δακτύλιος $\mathbb{Z}$ των ακεραίων είναι Π.Κ.Ι.*

Απόδειξη. Έπεται άμεσα από την πρόταση 7.2.6. □

9.2.5 Πρόταση. *Ας υποθέσουμε ότι R είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και $f : R \longrightarrow S$ ένας επιμορφισμός δακτυλίων. Εάν ο R είναι Δ.Κ.Ι., τότε και ο S είναι Δ.Κ.Ι.*

Απόδειξη. Έστω J τυχόν ιδεώδες τού S. Τότε το ιδεώδες $I = f^{-1}(J)$ είναι κύριο, ας πούμε το $I = \langle a\rangle = Ra$, για κάποιο $a \in R$. Ισχυριζόμαστε ότι

$$J = \langle f(a)\rangle = f(a)S.$$

Πράγματι· εάν $b \in J$, τότε $b = f(c)$ για κάποιο $c \in I$. Εξ αυτού έπεται ότι $c = ra$ για κάποιο $r \in R$, οπότε $b = f(c) = f(ra) = f(r)f(a) \in f(a)S$. Άρα $J = f(a)S$. □

9.2.6 Πόρισμα. *Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Εάν ο R είναι Δ.Κ.Ι., τότε και ο πηλικοδακτύλιος R/I, όπου I οιοδήποτε ιδεώδες τού R, είναι Δ.Κ.Ι.*

Απόδειξη. Αρκεί η εφαρμογή τής προτάσεως 9.2.5 για τον φυσικό επιμορφισμό $\pi_I^R : R \longrightarrow R/I$. □

9.2.7 Πόρισμα. *Εάν $m \in \mathbb{Z}\setminus\{0, \pm 1\}$, τότε ο πηλικοδακτύλιος $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_{|m|}$ είναι Π.Κ.Ι., όταν ο $|m|$ είναι πρώτος αριθμός, και Δ.Κ.Ι. (αλλά όχι και Π.Κ.Ι.), όταν ο $|m|$ είναι σύνθετος αριθμός.*

Απόδειξη. Προφανής δυνάμει των 6.2.27, 9.2.3, 8.3.4, 7.2.6, καθώς και τού πορίσματος 9.2.6. □

9.2.8 Σημείωση. Μέσω τού πορίσματος 9.2.7 διαπιστώνουμε ότι το 9.2.6 δεν είναι πάντοτε αληθές για περιοχές κυρίων ιδεωδών: Εάν το I είναι ένα μη τετριμμένο ιδεώδες μιας Π.Κ.Ι. R, τότε ο πηλικοδακτύλιος R/I (που είναι Δ.Κ.Ι.) δεν είναι κατ' ανάγκην Π.Κ.Ι.

9.2.9 Παραδείγματα. Οι δακτύλιοι

$$\mathbb{Z}_{\langle p\rangle}\ (p \text{ πρώτος, βλ. άσκηση 10 τού φυλλαδίου 11}), \quad K[\mathsf{X}],\ K[\![\mathsf{X}]\!]\ (K \text{ σώμα})$$

είναι περιοχές κυρίων ιδεωδών.

9.2.10 Ορισμός. Για κάθε $x \in \mathbb{R}$ ορίζονται οι ακέραιοι

$$\lfloor x \rfloor := \max\{\, n \in \mathbb{Z} \mid \; n \leqslant x \}, \;\; \lceil x \rceil := \min\{\, n \in \mathbb{Z} \mid \; n \geqslant x \},$$

και $\{x\} := x - \lfloor x \rfloor$. Ο $\lfloor x \rfloor$ ονομάζεται **το δάπεδο τού** x, ο $\lceil x \rceil$ **η οροφή τού** x και ο $\{x\}$ **το κλασματικό μέρος τού** x. Ο ακέραιος $\{x\}_{\text{εγγ}}$ **ο εγγύτερος τού** x, ορίζεται ως ακολούθως:

$$\{x\}_{\text{εγγ}} := \left\lfloor x + \tfrac{1}{2} \right\rfloor = \left\lceil x - \tfrac{1}{2} \right\rceil .$$

9.2.11 Πρόταση. *Ο δακτύλιος $\mathbb{Z}[i] \subsetneqq \mathbb{C}$ των ακεραίων τού Gauss είναι Π.Κ.Ι.*

Απόδειξη. Ο δακτύλιος $\mathbb{Z}[i]$ είναι ακεραία περιοχή. (Βλ. άσκηση 23 τού φυλλαδίου 11.) Έστω I ένα ιδεώδες τού $\mathbb{Z}[i]$. Εάν $I = \{0\}$, τότε $I = \langle 0 \rangle$. Εάν $\{0\} \subsetneqq I$, τότε υπάρχει κάποιο $z \in I \smallsetminus \{0\}$. Επιλέγουμε λοιπόν ένα $z_0 \in I \smallsetminus \{0\}$ για το οποίο ισχύει η ισότητα

$$|z_0| := \min\{\, |z| \;\mid\; z \in I \smallsetminus \{0\} \}.$$

Θα αποδείξουμε ότι $I = \langle z_0 \rangle$. Πράγματι· εάν $z_0 = a + bi$, για κάποιους $a, b \in \mathbb{Z}$ (με τουλάχιστον έναν εξ αυτών $\neq 0$), τότε για οιοδήποτε στοιχείο $w = a' + b'i \in I$, $a', b' \in \mathbb{Z}$, το κλάσμα w/z_0 γράφεται ως εξής:

$$\begin{aligned} \frac{w}{z_0} &= \frac{a' + b'i}{a + bi} = \frac{(a' + b'i)\,(a - bi)}{(a + bi)\,(a - bi)} \\ &= \frac{(a' + b'i)\,(a - bi)}{a^2 + b^2} = r + si \in \mathbb{Q}(i) = \mathbf{Fr}\,(\mathbb{Z}[i])\,, \end{aligned}$$

όπου $r := \frac{aa' + bb'}{a^2 + b^2} \in \mathbb{Q}$ και $s := \frac{ab' + a'b}{a^2 + b^2} \in \mathbb{Q}$. Θεωρούμε τους «εγγύτερους» ακεραίους $p := \{r\}_{\text{εγγ}}$ και $q := \{s\}_{\text{εγγ}}$ των r και s, αντιστοίχως, οπότε ισχύουν οι ανισοϊσότητες:

$$0 \leqslant |r - p| \leqslant \frac{1}{2}, \;\; 0 \leqslant |s - q| \leqslant \frac{1}{2},$$

και ορίζουμε ως $\xi := p + qi \in \mathbb{Z}[i]$. Τότε

$$\left| \frac{w}{z_0} - \xi \right| = \sqrt{(r - p)^2 + (s - q)^2} \leqslant \sqrt{\frac{1}{4} + \frac{1}{4}} = \frac{1}{\sqrt{2}} < 1. \tag{9.7}$$

Έστω $\zeta := w - z_0\xi$. Επειδή $z_0, w \in I$ και $\xi \in \mathbb{Z}[i]$ έχουμε $\zeta \in I$. Ας υποθέσουμε ότι $\zeta \neq 0$. Θέτοντας σε εφαρμογή την (9.7) λαμβάνουμε:

$$|\zeta| = |w - z_0\xi| = \left| z_0 \left(\frac{w}{z_0} - \xi \right) \right| = |z_0| \left| \frac{w}{z_0} - \xi \right| < |z_0|\,,$$

πράγμα *άτοπο* λόγω τού αρχικού τρόπου επιλογής τού z_0 (επί τη βάσει τής υποθέσεως περί ελαχίστης απόλυτης τιμής). Συνεπώς,

$$\zeta = 0 \Longrightarrow w = z_0\xi \Longrightarrow I \subseteq \langle z_0 \rangle .$$

Εξάλλου, $\langle z_0 \rangle = \{\, cz_0 \mid \; c \in \mathbb{Z}[i] \} \subseteq I$. Άρα τελικώς $I = \langle z_0 \rangle$. □

9.2.12 Σημείωση. Γενικότερα, η $\mathbb{Z}[\sqrt{m}]$ είναι Π.Κ.Ι. όταν $m \in \{-2, -1, 2, 3, 6, 7\}$.

9.2.13 Παράδειγμα. Υπάρχει, βεβαίως, και πληθώρα τετραγωνικών αριθμητικών περιοχών, οι οποίες δεν είναι Π.Κ.Ι. Επί παραδείγματι, η ακεραία περιοχή

$$\mathbb{Z}[\sqrt{-5}] = \{\, x + y\sqrt{-5} \;\mid\; x, y \in \mathbb{Z} \} \subsetneqq \mathbb{C}$$

δεν είναι Π.Κ.Ι., διότι το $I := \langle 2, 1+\sqrt{-5}\rangle$ δεν είναι κύριο ιδεώδες. Πράγματι· υποθέτοντας ότι υπάρχουν κάποιοι $a, b \in \mathbb{Z}$ (με έναν τουλάχιστον εξ αυτών διάφορο τού μηδενός), τέτοιοι ώστε

$$I = \langle a + b\sqrt{-5}\rangle = \mathbb{Z}[\sqrt{-5}]\left(a + b\sqrt{-5}\right),$$

καταλήγουμε σε κάτι το άτοπο ως ακολούθως: Επειδή $1+\sqrt{-5} \in I$, θα ισχύει

$$1 + \sqrt{-5} = \left(x + y\sqrt{-5}\right)\left(a + b\sqrt{-5}\right) = (ax - 5y) + (bx + ay)\sqrt{-5},$$

για κάποιους $x, y \in \mathbb{Z}$. Κατά συνέπειαν,

$$\left\{ \begin{array}{l} ax - 5y = 1, \\ bx + ay = 1 \end{array} \right\} \Longrightarrow \left\{ \begin{array}{l} x = \frac{a+5b}{a^2+5b^2}, \\ y = \frac{a-b}{a^2+5b^2} \end{array} \right\}. \tag{9.8}$$

Διακρίνουμε τρεις περιπτώσεις: (i) $a = b$. Τότε $x = \frac{1}{a}$, και επειδή $x \in \mathbb{Z}$, συνάγεται ότι $a = \pm 1$, οπότε $a + b\sqrt{-5} = \pm\left(1+\sqrt{-5}\right)$. Επειδή το 2 ανήκει στο I, θα πρέπει να ισχύει η ισότητα

$$2 = \left(1 + \sqrt{-5}\right)\left(\mu + \nu\sqrt{-5}\right), \tag{9.9}$$

για κάποιους $\mu, \nu \in \mathbb{Z}$. Θεωρώντας τούς συζυγείς και στα δύο μέλη τής (9.9) καταλήγουμε στην

$$2 = \left(1 - \sqrt{-5}\right)\left(\mu - \nu\sqrt{-5}\right). \tag{9.10}$$

Πολλαπλασιάζοντας κατά μέλη τις (9.9) και (9.10) λαμβάνουμε

$$4 = 6\left(\mu^2 + 5\nu^2\right). \tag{9.11}$$

Όμως η ισότητα (9.11) είναι αδύνατη, καθότι το δεξιό της μέλος είναι προφανώς > 4, όταν τουλάχιστον ένα εκ των μ, ν είναι διάφορο τού μηδενός, και είναι $= 0$, όταν $\mu = \nu = 0$.

(ii) $a \neq b$ και $b \neq 0$. Σε αυτήν την περίπτωση,

$$1 \leqslant |a-b| \leqslant |a| + |b| \leqslant a^2 + b^2 < a^2 + 5b^2 \Longrightarrow 0 < |y| = \frac{|a-b|}{a^2+5b^2} < 1,$$

(βλ. (9.8)), πράγμα άτοπο, διότι -εξ υποθέσεως- $y \in \mathbb{Z}$.

(iii) $a \neq b$ και $b = 0$. Στην τελευταία αυτή περίπτωση έχουμε (λόγω των (9.8)):

$$\mathbb{Z} \ni x = y = \frac{1}{a} \Longrightarrow a = \pm 1 \Longrightarrow a + b\sqrt{-5} = \pm 1 \Longrightarrow 1 \in I,$$

(οπότε $I = \mathbb{Z}[\sqrt{-5}]$). Τούτο όμως ισοδυναμεί με το ότι

$$1 = 2(\alpha + \sqrt{-5}\beta) + \left(1 + \sqrt{-5}\right)\left(\gamma + \sqrt{-5}\delta\right), \tag{9.12}$$

για κατάλληλους ακεραίους αριθμούς $\alpha, \beta, \gamma, \delta$. Από την (9.12) έπεται ότι

$$\left\{ \begin{array}{l} 2\alpha + \gamma - 5\delta = 1, \\ 2\beta + \gamma + \delta = 0 \end{array} \right\} \Longrightarrow 2\alpha + 10\beta + 6\gamma = 1. \tag{9.13}$$

Αλλά *και* η ισχύς τής (9.13) είναι αδύνατη, καθόσον το αριστερό της μέλος είναι ένας άρτιος και το δεξιό της μέλος ένας περιττός ακέραιος αριθμός.

9.2.14 Παραδείγματα. Άλλα παραδείγματα ανήκοντα στην κλάση των ακεραίων περιοχών που δεν είναι Π.Κ.Ι.: Ο πολυωνυμικός δακτύλιος $\mathbb{Z}[\mathsf{X}]$ (πρβλ. άσκηση 4 τού φυλλαδίου 12) και, γενικότερα, ο $R[\mathsf{X}]$, όπου R μια ακεραία περιοχή που δεν είναι σώμα, οι δακτύλιοι $K\left[\mathsf{X}_1, \ldots, \mathsf{X}_n\right]$, $K[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!]$ (όπου $n \geqslant 2$ και K σώμα) κ.ά.

9.2.15 Πρόταση. *Εάν μια ακεραία περιοχή R είναι Π.Κ.Ι., τότε ένα μη τετριμμένο ιδεώδες της είναι πρώτο εάν και μόνον εάν είναι μεγιστικό.*

Απόδειξη. Κατά το θεώρημα 7.5.15 κάθε μη τετριμμένο μεγιστικό ιδεώδες τής ακεραίας περιοχής R είναι πρώτο. Έστω τώρα I ένα μη τετριμμένο πρώτο ιδεώδες τής R και έστω J ένα ιδεώδες τής R, για το οποίο ισχύει $I \subsetneq J \subseteq R$. Επειδή η R είναι Π.Κ.Ι., υπάρχουν $a, b \in R \setminus \{0_R\}$, τέτοια ώστε $I = \langle a \rangle$ και $J = \langle b \rangle$. Επειδή $a \in \langle a \rangle \subsetneq \langle b \rangle$, υπάρχει κάποιο $c \in R \setminus \{0_R\}$ με $a = bc$. Παρατηρούμε ότι $b \notin \langle a \rangle$ (διότι αλλιώς θα είχαμε $\langle b \rangle \subseteq \langle a \rangle$), οπότε

$$c \in \langle a \rangle \Longrightarrow [\exists d \in R : c = ad] \Longrightarrow a = bc = bad = abd.$$

Καθώς $a \neq 0_R$, αυτό σημαίνει ότι $1_R = bd$ (βλ. πρόταση 6.2.5), οπότε έχουμε $1_R \in \langle b \rangle \Longrightarrow J = R$. Άρα το I είναι μεγιστικό ιδεώδες. □

9.3 ΑΡΤΙΝΙΑΝΟΙ ΔΑΚΤΥΛΙΟΙ

9.3.1 Ορισμός. Έστω $\{I_n | n \in \mathbb{N}\}$ ένα αριθμήσιμο σύνολο αριστερών (και αντιστοίχως, δεξιών) ιδεωδών ενός δακτυλίου R. Η ακολουθία $\{I_n\}_{n\in\mathbb{N}}$ καλείται **κατιούσα αλυσίδα** αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού R όταν ισχύει ο εγκλεισμός $I_n \supseteq I_{n+1}$ για κάθε $n \in \mathbb{N}$. Μια κατιούσα αλυσίδα $\{I_n\}_{n\in\mathbb{N}}$ καλείται **στάσιμη** όταν υπάρχει κάποιος $k \in \mathbb{N}$ για τον οποίο ισχύει $I_n = I_k$ για κάθε φυσικό αριθμό $n \geqslant k$.

9.3.2 Ορισμός. Λέμε ότι ένας δακτύλιος R ικανοποιεί τη **συνθήκη των κατιουσών αλυσίδων** επί τού συνόλου των αριστερών (και αντιστοίχως, των δεξιών) ιδεωδών του όταν *κάθε* κατιούσα αλυσίδα αριστερών (και αντιστοίχως, δεξιών) ιδεωδών αυτού είναι στάσιμη.

Η απόδειξη τού θεωρήματος 9.3.3 είναι παρόμοια εκείνης τού θεωρήματος 9.1.3.

9.3.3 Θεώρημα. *Έστω R ένας δακτύλιος. Τότε τα ακόλουθα είναι ισοδύναμα*:

(i) *Ο R ικανοποιεί τη συνθήκη των κατιουσών αλυσίδων επί τού συνόλου των αριστερών (και αντιστοίχως, των δεξιών) ιδεωδών του.*

(ii) *Κάθε μη κενό σύνολο αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού R περιέχει (τουλάχιστον) ένα ελαχιστικό στοιχείο (ως προς τον συνήθη εγκλεισμό).*

9.3.4 Ορισμός. Κάθε δακτύλιος R, ο οποίος ικανοποιεί μία (και, ως εκ τούτου, και τις δύο) εκ των συνθηκών (i), (ii) τού θεωρήματος 9.3.3, ονομάζεται **εξ αριστερών** (και αντιστοίχως, **εκ δεξιών**) **δακτύλιος τού Artin** ή **εξ αριστερών (και αντιστοίχως, εκ δεξιών) αρτινιανός δακτύλιος**[3]. Ένας δακτύλιος R καλείται **αρτινιανός δακτύλιος** όταν είναι ταυτοχρόνως και εξ αριστερών και εκ δεξιών αρτινιανός. (Προφανώς, για τους *μεταθετικούς* δακτυλίους οι έννοιες «εξ αριστερών αρτινιανός», «εκ δεξιών αρτινιανός» και «αρτινιανός» ταυτίζονται, ενώ για τους *μη μεταθετικούς* δακτυλίους είναι εν γένει διαφορετικές.) Τέλος, κάθε αρτινιανός δακτύλιος, ο οποίος τυγχάνει να είναι ακεραία περιοχή, ονομάζεται **αρτινιανή περιοχή**.

[3] Προς τιμήν τού Emil Artin (1898-1962), ο οποίος μελέτησε ιδιαιτέρως τις ιδιότητες των *κατιουσών* αλυσίδων ιδεωδών.

Οι αποδείξεις των προτάσεων 9.3.5 και 9.3.8, και των πορισμάτων 9.3.6 και 9.3.7 είναι παρόμοιες εκείνων των προτάσεων 9.1.5 και 9.1.9, και των πορισμάτων 9.1.6 και 9.1.7, αντιστοίχως.

9.3.5 Πρόταση. *Εάν η $f : R \longrightarrow S$ είναι ένας επιμορφισμός δακτυλίων και ο R είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) αρτινιανός δακτύλιος, τότε και ο S είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) αρτινιανός.*

9.3.6 Πόρισμα. *Εάν οι R και S είναι δυο ισόμορφοι δακτύλιοι και ο ένας εξ αυτών εξ αριστερών (και αντιστοίχως, εκ δεξιών) αρτινιανός, τότε και ο άλλος είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) αρτινιανός.*

9.3.7 Πόρισμα. *Έστω R ένας εξ αριστερών (και αντιστοίχως, ένας εκ δεξιών) αρτινιανός δακτύλιος και έστω I ένα ιδεώδες τού R. Τότε και ο πηλικοδακτύλιος R/I είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) αρτινιανός.*

9.3.8 Πρόταση. *Έστω $f : R \longrightarrow S$ ένας επιμορφισμός δακτυλίων. Εάν αμφότεροι οι $\mathrm{Ker}(f)$ και S είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) αρτινιανοί δακτύλιοι, τότε και ο ίδιος ο R είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) αρτινιανός.*

9.3.9 Πρόταση. *Κάθε αρτινιανή περιοχή είναι σώμα.*

Απόδειξη. Έστω R τυχούσα αρτινιανή περιοχή. Για οιοδήποτε $r \in R \setminus \{0_R\}$ ισχύουν οι εγκλεισμοί

$$\langle r \rangle \supseteq \left\langle r^2 \right\rangle \supseteq \left\langle r^3 \right\rangle \supseteq \cdots \supseteq \langle r^n \rangle \supseteq \left\langle r^{n+1} \right\rangle \supseteq \cdots , \ \forall n \in \mathbb{N}.$$

Επειδή η περιοχή R ικανοποιεί τη συνθήκη των κατιουσών αλυσίδων, υπάρχει κάποιος $k \in \mathbb{N}$ για τον οποίο ισχύει $I_n = I_k$ για κάθε φυσικό αριθμό $n \geqslant k$. Εξ αυτού έπεται ότι

$$r^k \in \left\langle r^k \right\rangle = \left\langle r^{k+1} \right\rangle \Rightarrow \exists a \in R : r^k = ar^{k+1},$$

οπότε $\left[r^k(1_R - ar) = 0_R,\ r^k \neq 0_R\right] \Rightarrow ar = 1_R \Rightarrow r \in R^\times$ (βλ. 6.2.5). Κατά συνέπειαν, $R^\times = R \setminus \{0_R\}$ και η R είναι σώμα. □

9.3.10 Παραδείγματα. (i) Κάθε σώμα είναι προφανώς αρτινιανή περιοχή (αφού διαθέτει μόνον δύο κύρια ιδεώδη). Μάλιστα, σύμφωνα με την πρόταση 9.3.9, *ισχύει και το αντίστροφο* (κάτι *που δεν ισχύει* για ναιτεριανές περιοχές)!

(ii) Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο και έστω $n \in \mathbb{N}$. Εάν ο R είναι ναιτεριανός (και αντιστοίχως, αρτινιανός), τότε και ο δακτύλιος $\mathrm{Mat}_{n\times n}(R)$ είναι ναιτεριανός (και αντιστοίχως, αρτινιανός), διότι υφίσταται μια αμφίρριψη μεταξύ τού συνόλου των ιδεωδών τού R και τού συνόλου των ιδεωδών τού $\mathrm{Mat}_{n\times n}(R)$ η οποία διατηρεί τη σχέση εγκλεισμού. Ιδιαιτέρως, για *κάθε* σώμα K, ο δακτύλιος $\mathrm{Mat}_{n\times n}(K)$ είναι *ταυτοχρόνως* ναιτεριανός και αρτινιανός.

(iii) Στην άσκηση 23 τού φυλλαδίου 12 δίδεται ένα παράδειγμα ενός δακτυλίου που είναι εκ δεξιών αλλά όχι και εξ αριστερών αρτινιανός.

(iv) Στην άσκηση 24 τού φυλλαδίου 12 δίδεται ένα παράδειγμα ενός δακτυλίου που είναι εξ αριστερών αλλά όχι και εκ δεξιών αρτινιανός.

(v) Ο δακτύλιος $\mathbb{Z}$ των ακεραίων είναι ναιτεριανός (βλ. 9.2.4) αλλά δεν είναι αρτινιανός, διότι η

$$\langle 2 \rangle \supsetneq \langle 4 \rangle \supsetneq \langle 8 \rangle \supsetneq \cdots \supsetneq \langle 2^n \rangle \supsetneq \left\langle 2^{n+1} \right\rangle \supsetneq \cdots , \ \forall n \in \mathbb{N}$$

είναι μια μη στάσιμη κατιούσα αλυσίδα ιδεωδών του.

(vi) Για οιοδήποτε σώμα K ο δακτύλιος $K[\mathsf{X}]$ είναι ναιτεριανός (σύμφωνα με το θεώρημα 9.1.15) αλλά δεν είναι αρτινιανός, διότι η

$$K[\mathsf{X}] \supsetneqq \langle \mathsf{X} \rangle \supsetneqq \left\langle \mathsf{X}^2 \right\rangle \supsetneqq \cdots \supsetneqq \langle \mathsf{X}^n \rangle \supsetneqq \left\langle \mathsf{X}^{n+1} \right\rangle \supsetneqq \cdots \,, \ \forall n \in \mathbb{N}$$

είναι μια μη στάσιμη κατιούσα αλυσίδα ιδεωδών του.

(vii) Στην άσκηση 25 τού φυλλαδίου 12 δίδεται ένα παράδειγμα ενός δακτυλίου που είναι αρτινιανός αλλά δεν είναι ναιτεριανός.

(viii) Εάν για οιονδήποτε θετικό πραγματικό αριθμό ρ θεωρήσουμε το ιδεώδες

$$I_\rho := \left\{ f \in \mathbb{R}^{\mathbb{R}} \middle| \, f(x) = 0 \text{ για κάθε } x \in [-\rho, \rho] \right\}$$

τού δακτυλίου $\mathbb{R}^{\mathbb{R}}$, τότε $\cdots \subsetneqq I_3 \subsetneqq I_2 \subsetneqq I_1 \subsetneqq I_{\frac{1}{2}} \subsetneqq I_{\frac{1}{3}} \subsetneqq I_{\frac{1}{4}} \subsetneqq \cdots$, οπότε η

$$I_1 \subsetneqq I_{\frac{1}{2}} \subsetneqq I_{\frac{1}{3}} \subsetneqq I_{\frac{1}{4}} \subsetneqq \cdots \subsetneqq I_{\frac{1}{n}} \subsetneqq I_{\frac{1}{n+1}}, \ \forall n \in \mathbb{N}$$

είναι μια μη στάσιμη ανιούσα αλυσίδα ιδεωδών και η

$$I_1 \supsetneqq I_2 \supsetneqq I_3 \supsetneqq \cdots \supsetneqq I_n \supsetneqq I_{n+1} \supsetneqq \cdots \,, \ \forall n \in \mathbb{N}$$

είναι μια μη στάσιμη κατιούσα αλυσίδα ιδεωδών τού $\mathbb{R}^{\mathbb{R}}$. Άρα ο δακτύλιος $\mathbb{R}^{\mathbb{R}}$ δεν είναι ούτε ναιτεριανός ούτε αρτινιανός. (Σημειωτέον ότι όλα τα ιδεώδη I_ρ περιέχονται στο μεγιστικό ιδεώδες $\left\{ f \in \mathbb{R}^{\mathbb{R}} \middle| \, f(0) = 0 \right\}$.)

Παρά το γεγονός ότι δεν υφίσταται κάποια αξιομνημόνευτη σχέση διασυνδέσεως *γενικών* ναιτεριανών και αρτινιανών δακτυλίων, τα πράγματα *διαφοροποιούνται* όταν κανείς περιορίζεται *στην κλάση των μεταθετικών δακτυλίων με μοναδιαίο στοιχείο*. Κάθε αρτινιανός μεταθετικός δακτύλιος με μοναδιαίο στοιχείο είναι κατ' ανάγκην ναιτεριανός! Συγκεκριμένα, ισχύει το εξής:

9.3.11 Θεώρημα (Y. Akizuki & C. Hopkins, 1939). *Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Ο R είναι αρτινιανός.*

(ii) *Ο R είναι ναιτεριανός και κάθε πρώτο ιδεώδες του είναι μεγιστικό.*

ΑΠΟΔΕΙΞΗ. Βλ., π.χ., I.S. Cohen: *Commutative rings with restricted minimum condition*, Duke Math. Journal **17** (1950), 27-42. □

ΚΕΦΑΛΑΙΟ 10

Διαιρετότητα στον $K[\mathsf{X}]$

Στο πλαίσιο τής Στοιχειώδους Θεωρίας Αριθμών έχουμε μελετήσει τις *ιδιότητες τής διαιρετότητας ακεραίων αριθμών*, τον τρόπο εκτελέσεως τού *ευκλειδείου αλγορίθμου διαιρέσεως*, έχουμε ορίσει τις έννοιες *μέγιστος κοινός διαιρέτης* και *ελάχιστο κοινό πολλαπλάσιο*, και έχουμε αποδείξει ότι κάθε $a \in \mathbb{Z}\setminus\{0,\pm 1\}$ παριστάται υπό τη μορφή (2.20). Στο κατ' επιλογήν μάθημα με κωδικό ΜΕΜ 226 εξηγείται λεπτομερώς το κατά πόσον και μέχρι ποίου βαθμού γενικεύονται τα ανωτέρω (που αφορούν στον δακτύλιο $\mathbb{Z}$) σε *τυχούσες ακέραιες περιοχές*. Στο τελευταίο αυτό κεφάλαιο θα περιορισθούμε (εν είδει «γεφυρώσεως» των όσων αναπτύσσονται εδώ με το ΜΕΜ 226) μόνον στη θεωρία διαιρετότητας στον πολυωνυμικό δακτύλιο $K[\mathsf{X}]$ μιας απροσδιορίστου με συντελεστές των στοιχείων του ειλημμένους από κάποιο σώμα K.

10.1 ΤΑΥΤΟΤΗΤΑ ΔΙΑΙΡΕΣΕΩΣ

Έστω K ένα σώμα. Η γνωστή *ταυτότητα διαιρέσεως* η ισχύουσα στον δακτύλιο $\mathbb{Z}$ των ακεραίων, καθώς και οι έννοιες *μέγιστος κοινός διαιρέτης* και *ελάχιστο κοινό πολλαπλάσιο*, γενικεύονται και για τα στοιχεία τού δακτυλίου $K[\mathsf{X}]$.

10.1.1 Θεώρημα (Ταυτότητα διαιρέσεως). *Δοθέντων δυο πολυωνύμων*

$$\varphi(\mathsf{X}) \in K[\mathsf{X}],\ \ \psi(\mathsf{X}) \in K[\mathsf{X}]\setminus\{0_{K[\mathsf{X}]}\},$$

υπάρχει ένα ζεύγος ***μονοσημάντως ορισμένων*** *πολυωνύμων* $\varpi(\mathsf{X}), \upsilon(\mathsf{X}) \in K[\mathsf{X}]$, *ούτως ώστε να ισχύει*

$$\boxed{\varphi(\mathsf{X}) = \varpi(\mathsf{X})\psi(\mathsf{X}) + \upsilon(\mathsf{X}),\ \ \deg\left(\upsilon(\mathsf{X})\right) < \deg\left(\psi(\mathsf{X})\right).} \tag{10.1}$$

(Όταν γράφουμε $\deg\left(\upsilon(\mathsf{X})\right) < \deg\left(\psi(\mathsf{X})\right)$ συμπεριλαμβάνουμε και την περίπτωση όπου $\upsilon(\mathsf{X}) = 0_{K[\mathsf{X}]}$ επί τη βάσει τού ορισμού τής εννοίας τού βαθμού πολυωνύμου που εισήχθη στο εδάφιο 6.3.6.)

Απόδειξη. **Βήμα 1ο**. *Ύπαρξη των* $\varpi(\mathsf{X})$, $\upsilon(\mathsf{X})$. Εάν $\deg(\varphi(\mathsf{X})) < \deg(\psi(\mathsf{X}))$, τότε θέτουμε $\varpi(\mathsf{X}) := 0_{K[\mathsf{X}]},\ \upsilon(\mathsf{X}) := \varphi(\mathsf{X})$. Στην περίπτωση όπου

$$\deg(\varphi(\mathsf{X})) =: n \geqslant m := \deg(\psi(\mathsf{X})) \geqslant 0$$

και

$$\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i,\ \psi(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j\ \ (a_n \neq 0_K, b_m \neq 0_K),$$

χρησιμοποιούμε μαθηματική επαγωγή ως προς τον βαθμό n τού $\varphi(\mathsf{X})$. Εάν $n = 0$, τότε $m = 0$ και

$$\varphi(\mathsf{X}) = a_0, \;\; \psi(\mathsf{X}) = b_0 \neq 0_K,$$

οπότε αρκεί να θέσουμε $\varpi(\mathsf{X}) := a_0 b_0^{-1}$ και $\upsilon(\mathsf{X}) := 0_{K[\mathsf{X}]}$. Ας υποθέσουμε τώρα ότι $n \geqslant 1$ και ότι ο ισχυρισμός (που αφορά μόνον στην *ύπαρξη* τού εν λόγω ζεύγους πολυωνύμων) είναι αληθής για κάθε πολυώνυμο ανήκον στον $K[\mathsf{X}]$ και έχον βαθμό $< n$. Το πολυώνυμο

$$\tilde{\varphi}(\mathsf{X}) := \varphi(\mathsf{X}) - (a_n b_m^{-1})\mathsf{X}^{n-m}\psi(\mathsf{X}) = \sum_{i=0}^{n-1} a_i \mathsf{X}^i - \sum_{j=0}^{m-1} (a_n b_m^{-1}) b_j \mathsf{X}^{n-m+j} \in K[\mathsf{X}]$$

έχει βαθμό $\leqslant n-1$. Κατά την επαγωγική μας υπόθεση υπάρχουν πολυώνυμα $\tilde{\varpi}(\mathsf{X})$, $\tilde{\upsilon}(\mathsf{X}) \in K[\mathsf{X}]$, ούτως ώστε να ισχύει

$$\tilde{\varphi}(\mathsf{X}) = \tilde{\varpi}(\mathsf{X})\psi(\mathsf{X}) + \tilde{\upsilon}(\mathsf{X}), \quad \deg\left(\tilde{\upsilon}(\mathsf{X})\right) < \deg\left(\psi(\mathsf{X})\right).$$

Επειδή $\varphi(\mathsf{X}) = \left((a_n b_m^{-1})\mathsf{X}^{n-m} + \tilde{\varpi}(\mathsf{X})\right)\psi(\mathsf{X}) + \tilde{\upsilon}(\mathsf{X})$, αρκεί να θέσουμε

$$\varpi(\mathsf{X}) := (a_n b_m^{-1})\mathsf{X}^{n-m} + \tilde{\varpi}(\mathsf{X}), \;\; \upsilon(\mathsf{X}) := \tilde{\upsilon}(\mathsf{X}).$$

Βήμα 2ο. *Μοναδικότητα των* $\varpi(\mathsf{X})$, $\upsilon(\mathsf{X})$. Έστω ότι η συνθήκη (10.1) ικανοποιείται από δύο ζεύγη πολυωνύμων $\varpi_1(\mathsf{X})$, $\upsilon_1(\mathsf{X})$ και $\varpi_2(\mathsf{X})$, $\upsilon_2(\mathsf{X})$:

$$\varphi(\mathsf{X}) = \varpi_1(\mathsf{X})\psi(\mathsf{X}) + \upsilon_1(\mathsf{X}), \quad \deg\left(\upsilon_1(\mathsf{X})\right) < \deg\left(\psi(\mathsf{X})\right),$$
$$\varphi(\mathsf{X}) = \varpi_2(\mathsf{X})\psi(\mathsf{X}) + \upsilon_2(\mathsf{X}), \quad \deg\left(\upsilon_2(\mathsf{X})\right) < \deg\left(\psi(\mathsf{X})\right).$$

Τότε $0_{K[\mathsf{X}]} = \varphi(\mathsf{X}) - \varphi(\mathsf{X}) = \left(\varpi_1(\mathsf{X}) - \varpi_2(\mathsf{X})\right)\psi(\mathsf{X}) + \left(\upsilon_1(\mathsf{X}) - \upsilon_2(\mathsf{X})\right)$, οπότε

$$\left(\varpi_1(\mathsf{X}) - \varpi_2(\mathsf{X})\right)\psi(\mathsf{X}) = \upsilon_2(\mathsf{X}) - \upsilon_1(\mathsf{X}).$$

Εάν ίσχυε $\varpi_1(\mathsf{X}) \neq \varpi_2(\mathsf{X})$, τότε θα είχαμε

$$\deg(\psi(\mathsf{X})) \leqslant \deg\left(\left(\varpi_1(\mathsf{X}) - \varpi_2(\mathsf{X})\right)\psi(\mathsf{X})\right) = \deg(\upsilon_2(\mathsf{X}) - \upsilon_1(\mathsf{X})) < \deg(\psi(\mathsf{X})).$$

Άτοπο! Συνεπώς, $\varpi_1(\mathsf{X}) = \varpi_2(\mathsf{X})$ και, ως εκ τούτου, $\upsilon_1(\mathsf{X}) = \upsilon_2(\mathsf{X})$. □

10.1.2 Ορισμός. Το πολυώνυμο $\varpi(\mathsf{X})$ στην (10.1) ονομάζεται **πηλίκο** και το $\upsilon(\mathsf{X})$ **υπόλοιπο** τής διαιρέσεως τού $\varphi(\mathsf{X})$ διά τού $\psi(\mathsf{X})$. Όταν $\upsilon(\mathsf{X}) = 0_{K[\mathsf{X}]}$, λέμε ότι το $\psi(\mathsf{X})$ **διαιρεί** (επακριβώς) το $\varphi(\mathsf{X})$ ή ότι το $\psi(\mathsf{X})$ είναι **διαιρέτης** τού $\varphi(\mathsf{X})$ ή ότι το $\varphi(\mathsf{X})$ είναι (πολυωνυμικό) **πολλαπλάσιο** τού $\psi(\mathsf{X})$. (Εν τοιαύτη περιπτώσει χρησιμοποιείται ο συμβολισμός[1]: $\psi(\mathsf{X}) \mid \varphi(\mathsf{X})$). Όταν $\upsilon(\mathsf{X}) = 0_{K[\mathsf{X}]}$ και $\deg(\varpi(\mathsf{X})) \geqslant 1$, το $\psi(\mathsf{X})$ καλείται **γνήσιος διαιρέτης** τού $\varphi(\mathsf{X})$.

10.1.3 Πρόταση. *Εάν τα* $\theta(\mathsf{X})$, $\varphi(\mathsf{X})$ *και* $\psi(\mathsf{X}), \psi_1(\mathsf{X}), \ldots, \psi_k(\mathsf{X})$ $(k \in \mathbb{N}, k \geqslant 2)$ *είναι πολυώνυμα ανήκοντα στον* $K[\mathsf{X}]$, *τότε ισχύουν τα ακόλουθα*:

(i) *Εάν* $\varphi(\mathsf{X}) \mid \psi_i(\mathsf{X})$, $\forall i \in \{1, \ldots, k\}$, *τότε* $\varphi(\mathsf{X}) \mid \sum_{i=1}^{k} \omega_i(\mathsf{X})\psi_i(\mathsf{X})$ *για οιαδήποτε* $\omega_1(\mathsf{X}), \ldots, \omega_k(\mathsf{X}) \in K[\mathsf{X}]$.

(ii) *Εάν* $\varphi(\mathsf{X}) \mid \theta(\mathsf{X})$ *και* $\psi(\mathsf{X}) \mid \varphi(\mathsf{X})$, *τότε* $\psi(\mathsf{X}) \mid \theta(\mathsf{X})$.

(iii) $a \mid \theta(\mathsf{X})$ *για κάθε* $a \in K \setminus \{0_K\}$.

(iv) *Εάν* $\varphi(\mathsf{X}) \mid \theta(\mathsf{X})$, *όπου* $\theta(\mathsf{X}) \neq 0_{K[\mathsf{X}]}$, *τότε* $\deg\left(\varphi(\mathsf{X})\right) \leqslant \deg\left(\theta(\mathsf{X})\right)$.

(v) *Εάν* $\varphi(\mathsf{X}) \mid \theta(\mathsf{X})$ *και* $\theta(\mathsf{X}) \mid \varphi(\mathsf{X})$, *τότε* $\theta(\mathsf{X}) = a\varphi(\mathsf{X})$, *για κάποιο* $a \in K \setminus \{0_K\}$.

Απόδειξη. Αφήνεται ως άσκηση. □

[1] Κατ' αντιδιαστολήν, μέσω τού συμβολισμού $\psi(\mathsf{X}) \nmid \varphi(\mathsf{X})$ υποδηλούται ότι το πολυώνυμο $\psi(\mathsf{X})$ δεν διαιρεί (επακριβώς) το πολυώνυμο $\varphi(\mathsf{X})$.

10.1.4 Λήμμα. *Εάν* $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$ *είναι δυο μονικά πολώνυμα με* $\varphi(\mathsf{X}) \mid \psi(\mathsf{X})$ *και* $\psi(\mathsf{X}) \mid \varphi(\mathsf{X})$, *τότε* $\varphi(\mathsf{X}) = \psi(\mathsf{X})$.

ΑΠΟΔΕΙΞΗ. Εξ υποθέσεως, υπάρχουν $\varpi(\mathsf{X}), \varpi'(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$, τέτοια ώστε να ισχύουν οι ισότητες $\varphi(\mathsf{X}) = \varpi(\mathsf{X})\psi(\mathsf{X})$ και $\psi(\mathsf{X}) = \varpi'(\mathsf{X})\varphi(\mathsf{X})$. Επομένως έχουμε $\varphi(\mathsf{X}) = \varpi(\mathsf{X})\varpi'(\mathsf{X})\varphi(\mathsf{X})$ και το (ii) τής προτάσεως 6.3.7 δίδει

$$\left.\begin{aligned} \deg(\varpi(\mathsf{X})\varpi'(\mathsf{X})) = \deg(\varpi(\mathsf{X})) + \deg(\varpi'(\mathsf{X})) \\ \varpi(\mathsf{X}) \neq 0_{K[\mathsf{X}]} \Rightarrow \deg(\varpi(\mathsf{X})) \geqslant 0 \\ \varpi'(\mathsf{X}) \neq 0_{K[\mathsf{X}]} \Rightarrow \deg(\varpi'(\mathsf{X})) \geqslant 0 \end{aligned}\right\} \Rightarrow \deg(\varpi(\mathsf{X})) = \deg(\varpi'(\mathsf{X})) = 0,$$

απ' όπου προκύπτει ότι $\varpi(\mathsf{X}) = \varpi'(\mathsf{X}) = 1_K$ (διότι τα $\varpi(\mathsf{X}), \varpi'(\mathsf{X})$ είναι κατ' ανάγκην μονικά πολυώνυμα) και, κατ' επέκταση, ότι $\varphi(\mathsf{X}) = \psi(\mathsf{X})$. □

10.1.5 Ορισμός. Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$, τότε ένα $\delta(\mathsf{X}) \in K[\mathsf{X}]$ καλείται **μέγιστος κοινός διαιρέτης των** $\varphi(\mathsf{X})$ **και** $\psi(\mathsf{X})$ (εντός τού $K[\mathsf{X}]$) όταν ισχύουν τα εξής:

(i) Το $\delta(\mathsf{X})$ είναι *κοινός διαιρέτης* των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$, ήτοι $\delta(\mathsf{X}) \mid \varphi(\mathsf{X})$ και $\delta(\mathsf{X}) \mid \psi(\mathsf{X})$.

(ii) Εάν $\theta(\mathsf{X}) \in K[\mathsf{X}]$ είναι *τυχόν* κοινός διαιρέτης των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$, δηλαδή εάν $\theta(\mathsf{X}) \mid \varphi(\mathsf{X})$ και $\theta(\mathsf{X}) \mid \psi(\mathsf{X})$, τότε $\theta(\mathsf{X}) \mid \delta(\mathsf{X})$.

(iii) Το $\delta(\mathsf{X})$ είναι μονικό πολυώνυμο[2].

10.1.6 Πρόταση. *Εάν* $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$, *τότε υπάρχει ένας και μόνον μέγιστος κοινός διαιρέτης* $\delta(\mathsf{X})$ *των* $\varphi(\mathsf{X})$ *και* $\psi(\mathsf{X})$. *Επιπροσθέτως, υπάρχουν* $\alpha(\mathsf{X}), \beta(\mathsf{X}) \in K[\mathsf{X}]$, *τέτοια ώστε να ισχύει* $\delta(\mathsf{X}) = \alpha(\mathsf{X})\varphi(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X})$.

ΑΠΟΔΕΙΞΗ. **Βήμα 1ο**. *Ύπαρξη τού μεγίστου κοινού διαιρέτη.* Θεωρούμε το σύνολο $\mathcal{A} := \{\kappa(\mathsf{X})\varphi(\mathsf{X}) + \mu(\mathsf{X})\psi(\mathsf{X}) | \, \kappa(\mathsf{X}), \mu(\mathsf{X}) \in K[\mathsf{X}]\}$. Προφανώς, $\mathcal{A} \neq \varnothing$ (διότι αμφότερα τα $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$ ανήκουν σε αυτό) και περιέχει μονικά πολυώνυμα (διότι εάν $\eta(\mathsf{X}) = \kappa(\mathsf{X})\varphi(\mathsf{X}) + \mu(\mathsf{X})\psi(\mathsf{X})$ είναι τυχόν μη μηδενικό στοιχείο του έχον το $c \in K \setminus \{0_K\}$ ως επικεφαλής συντελεστή, τότε το μονικό πολυώνυμο $c^{-1}\eta(\mathsf{X}) = (c^{-1}\kappa(\mathsf{X}))\varphi(\mathsf{X}) + (c^{-1}\mu(\mathsf{X}))\psi(\mathsf{X})$ ανήκει σε αυτό). Επομένως, έχουμε τη δυνατότητα επιλογής ενός *μονικού* πολυωνύμου

$$\delta(\mathsf{X}) = \alpha(\mathsf{X})\varphi(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X}) \in \mathcal{A} \;\; (\alpha(\mathsf{X}), \beta(\mathsf{X}) \in K[\mathsf{X}])$$

βαθμού $\deg(\delta(\mathsf{X})) := \min\{\deg(\theta(\mathsf{X})) | \, \theta(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}\}$. Αρκεί λοπόν να αποδειχθεί ότι το $\delta(\mathsf{X})$ πληροί τις συνθήκες (i) και (ii) τού ορισμού 10.1.5. Ξεκινούμε με την (ii). Εάν $\theta(\mathsf{X}) \in K[\mathsf{X}]$ είναι *τυχόν* κοινός διαιρέτης των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$, τότε

$$\theta(\mathsf{X}) \mid \alpha(\mathsf{X})\varphi(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X}) = \delta(\mathsf{X})$$

λόγω τού (i) τής προτάσεως 10.1.3. Εν συνεχεία, για τον έλεγχο τού ότι το $\delta(\mathsf{X})$ πληροί *και* τη συνθήκη (i) θεωρούμε τυχόν

$$\gamma(\mathsf{X}) = \kappa(\mathsf{X})\varphi(\mathsf{X}) + \mu(\mathsf{X})\psi(\mathsf{X}) \in \mathcal{A} \;\; (\kappa(\mathsf{X}), \mu(\mathsf{X}) \in K[\mathsf{X}]).$$

[2] Στο πλαίσιο τής (γενικής) Θεωρίας Δακτυλίων είθισται να μην συμπεριλαμβάνουμε τη συνθήκη (iii) στον ορισμό. Εν τοιαύτη περιπτώσει, ο μέγιστος κοινός διαιρέτης είναι μονοσημάντως ορισμένος *μόνον μέχρις πολλαπλασιασμού με κάποια μη μηδενική σταθερά* ανήκουσα στο K. Εδώ, δεν πρόκειται να χρησιμοποιήσουμε τη γενίκευση αυτού τού είδους. Θα αρκεσθούμε στη θεώρηση τού *αυστηρώς* μονοσημάντως ορισμένου, «διακεκριμένου» *μονικού* μεγίστου κοινού διαιρέτη των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$.

Σύμφωνα με το θεώρημα 10.1.1 υπάρχει ένα ζεύγος μονοσημάντως ορισμένων πολυωνύμων $\varpi(\mathsf{X}), \upsilon(\mathsf{X}) \in K[\mathsf{X}]$, ούτως ώστε να ισχύει

$$\gamma(\mathsf{X}) = \varpi(\mathsf{X})\delta(\mathsf{X}) + \upsilon(\mathsf{X}), \quad \deg(\upsilon(\mathsf{X})) < \deg(\delta(\mathsf{X})).$$

Εξ αυτού έπεται ότι

$$\begin{aligned} \upsilon(\mathsf{X}) &= \gamma(\mathsf{X}) - \varpi(\mathsf{X})\delta(\mathsf{X}) \\ &= \kappa(\mathsf{X})\varphi(\mathsf{X}) + \mu(\mathsf{X})\psi(\mathsf{X}) - \varpi(\mathsf{X})(\alpha(\mathsf{X})\varphi(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X})) \\ &= (\kappa(\mathsf{X}) - \varpi(\mathsf{X})\alpha(\mathsf{X}))\varphi(\mathsf{X}) + (\mu(\mathsf{X}) - \varpi(\mathsf{X})\beta(\mathsf{X}))\psi(\mathsf{X}) \in \mathcal{A}. \end{aligned}$$

Εάν υποθέσουμε ότι $\upsilon(\mathsf{X}) \neq 0_{K[\mathsf{X}]}$ έχον το $c \in K \setminus \{0_K\}$ ως επικεφαλής συντελεστή, τότε το μονικό πολυώνυμο $c^{-1}\upsilon(\mathsf{X})$ ανήκει στο $\mathcal{A}$ και έχει βαθμό

$$0 \leqslant \deg(c^{-1}\upsilon(\mathsf{X})) = \deg(\upsilon(\mathsf{X})) < \deg(\delta(\mathsf{X})),$$

κάτι το οποίο αντίκειται στον ορισμό τού $\delta(\mathsf{X})$. Κατά συνέπειαν, $\upsilon(\mathsf{X}) = 0_{K[\mathsf{X}]}$ και $\delta(\mathsf{X}) \mid \gamma(\mathsf{X})$. Αυτό σημαίνει ότι το $\delta(\mathsf{X})$ είναι διαιρέτης όλων των στοιχείων τού $\mathcal{A}$ (άρα και των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$).

Βήμα 2ο. *Μοναδικότητα τού μεγίστου κοινού διαιρέτη.* Εάν εκτός τού ανωτέρω $\delta(\mathsf{X})$ υπάρχει και κάποιος άλλος μέγιστος κοινός διαιρέτης $\delta'(\mathsf{X})$ των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$, τότε $\delta(\mathsf{X}) \mid \delta'(\mathsf{X})$ και $\delta'(\mathsf{X}) \mid \delta(\mathsf{X})$ (λόγω τής συνθήκης (ii) τού 10.1.5), οπότε $\delta(\mathsf{X}) = \delta'(\mathsf{X})$ δυνάμει τού λήμματος 10.1.4. □

10.1.7 Σημείωση. (i) Εφεξής θα συμβολίζουμε τον (επί τη βάσει τής προηγηθείσας προτάσεως 10.1.6 μονοσημάντως ορισμένο) μέγιστο κοινό διαιρέτη των πολυωνύμων $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$ ως μκδ$(\varphi(\mathsf{X}), \psi(\mathsf{X}))$.

(ii) Εάν $\psi(\mathsf{X}) \mid \varphi(\mathsf{X})$, τότε μκδ$(\varphi(\mathsf{X}), \psi(\mathsf{X})) = c^{-1}\psi(\mathsf{X})$, όπου $c \in K \setminus \{0_K\}$ είναι ο επικεφαλής συντελεστής τού $\psi(\mathsf{X})$.

(iii) Εάν αμφότερα τα $\varphi(\mathsf{X}), \psi(\mathsf{X})$ είναι μηδενικά, τότε γενικεύουμε την έννοια τού μεγίστου κοινού διαιρέτη θέτοντας μκδ$(\varphi(\mathsf{X}), \psi(\mathsf{X})) := 0_{K[\mathsf{X}]}$. Εάν μόνον ένα εξ αυτών, ας πούμε το $\varphi(\mathsf{X})$, είναι μηδενικό, τότε θέτουμε *εξ ορισμού*

$$\text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X})) := c^{-1}\psi(\mathsf{X}),$$

όπου $c \in K \setminus \{0_K\}$ είναι ο επικεφαλής συντελεστής τού $\psi(\mathsf{X})$ (γενικεύοντας το (ii) *και* σε αυτήν την περίπτωση).

(iv) Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]$ και $c_1, c_2 \in K \setminus \{0_K\}$, τότε

$$\boxed{\text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X})) = \text{μκδ}(c_1\varphi(\mathsf{X}), c_2\psi(\mathsf{X})).}$$

Πράγματι· εάν $\delta(\mathsf{X}) := \text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X}))$ και $\delta'(\mathsf{X}) := \text{μκδ}(c_1\varphi(\mathsf{X}), c_2\psi(\mathsf{X}))$, τότε

$$\left.\begin{array}{l} [\delta(\mathsf{X}) \mid \varphi(\mathsf{X}),\ \varphi(\mathsf{X}) \mid c_1\varphi(\mathsf{X})] \Rightarrow \delta(\mathsf{X}) \mid c_1\varphi(\mathsf{X}) \\ [\delta(\mathsf{X}) \mid \psi(\mathsf{X}),\ \psi(\mathsf{X}) \mid c_2\psi(\mathsf{X})] \Rightarrow \delta(\mathsf{X}) \mid c_2\psi(\mathsf{X}) \end{array}\right\} \Rightarrow \delta(\mathsf{X}) \mid \delta'(\mathsf{X})$$

(βλ. 10.1.3 (ii) και 10.1.5 (ii)). Από την άλλη μεριά,

$$\delta'(\mathsf{X}) \mid c_1\varphi(\mathsf{X}) \Rightarrow \exists\tilde{\varphi}(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\} : c_1\varphi(\mathsf{X}) = \tilde{\varphi}(\mathsf{X})\delta'(\mathsf{X}).$$

Επομένως, $\varphi(\mathsf{X}) = c_1^{-1}\tilde{\varphi}(\mathsf{X})\delta'(\mathsf{X}) \Rightarrow \delta'(\mathsf{X}) \mid \varphi(\mathsf{X})$. Κατ' αναλογίαν, $\delta'(\mathsf{X}) \mid \psi(\mathsf{X})$. Άρα $\delta'(\mathsf{X}) \mid \delta(\mathsf{X})$. Κατά το λήμμα 10.1.4, $\delta(\mathsf{X}) = \delta'(\mathsf{X})$.

▸ **Ευκλείδειος αλγόριθμος**. Η πρόταση 10.1.6 διασφαλίζει μόνον την ύπαρξη και τη μοναδικότητα τού μκδ$(\varphi(\mathsf{X}), \psi(\mathsf{X}))$. Δεν περιγράφει κάποια μέθοδο υπολογισμού του. Ωστόσο, δοθέντων δυο πολυωνύμων $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$ με

$\deg(\psi(\mathsf{X})) \leqslant \deg(\varphi(\mathsf{X}))$, μπορούμε να προσδιορίσουμε επακριβώς τον μέγιστο κοινό διαιρέτη τους *μέσω επαλλήλων εφαρμογών τής ταυτότητας διαιρέσεως πολυωνύμων* (γενικεύοντας καταλλήλως τον γνωστό *ευκλείδειο αλγόριθμο* τον ισχύοντα στον δακτύλιο $\mathbb{Z}$ των ακεραίων). Πράγματι· υπάρχουν μονοσημάντως ορισμένα πολυώνυμα $\varpi(\mathsf{X}), \upsilon(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει

$$\varphi(\mathsf{X}) = \varpi(\mathsf{X})\psi(\mathsf{X}) + \upsilon(\mathsf{X}), \;\; \deg(\upsilon(\mathsf{X})) < \deg(\psi(\mathsf{X})).$$

Εάν $\upsilon(\mathsf{X}) = 0_{K[\mathsf{X}]}$, τότε ο μκδ$(\varphi(\mathsf{X}), \psi(\mathsf{X}))$ είναι γνωστός (βλ. 10.1.7 (ii)). Ειδάλλως, θέτουμε $\delta(\mathsf{X}) := \text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X}))$ και $\delta'(\mathsf{X}) := \text{μκδ}(\psi(\mathsf{X}), \upsilon(\mathsf{X}))$, και παρατηρούμε (κάνοντας χρήση τού (i) τής προτάσεως 10.1.3 και τού (ii) τού ορισμού 10.1.5) ότι

$$\left.\begin{array}{c} \delta(\mathsf{X}) \mid \varphi(\mathsf{X}) \\ \delta(\mathsf{X}) \mid \varphi(\mathsf{X}) - \varpi(\mathsf{X})\psi(\mathsf{X}) = \upsilon(\mathsf{X}) \end{array}\right\} \Rightarrow \delta(\mathsf{X}) \mid \delta'(\mathsf{X})$$

και

$$\left.\begin{array}{c} \delta'(\mathsf{X}) \mid \psi(\mathsf{X}) \\ \delta(\mathsf{X}) \mid \varpi(\mathsf{X})\psi(\mathsf{X}) + \upsilon(\mathsf{X}) = \varphi(\mathsf{X}) \end{array}\right\} \Rightarrow \delta'(\mathsf{X}) \mid \delta(\mathsf{X}).$$

Ως εκ τούτου, $\delta(\mathsf{X}) = \delta'(\mathsf{X})$ (βλ. λήμμα 10.1.4). Θέτοντας

$$\upsilon_0(\mathsf{X}) := \varphi(\mathsf{X}), \;\; \varpi_1(\mathsf{X}) := \varpi(\mathsf{X}), \;\; \upsilon_1(\mathsf{X}) := \psi(\mathsf{X}), \;\; \upsilon_2(\mathsf{X}) := \upsilon(\mathsf{X})$$

και επαναμβάνοντας διαδοχικώς την ίδια διαδικασία, προσδιορίζουμε μονοσημάντως ορισμένα πολυώνυμα $\upsilon_3(\mathsf{X}), \upsilon_4(\mathsf{X}), \ldots$ και $\varpi_2(\mathsf{X}), \varpi_3(\mathsf{X}), \ldots$ με

$$\left|\begin{array}{ll} \upsilon_0(\mathsf{X}) = \varpi_1(\mathsf{X})\,\upsilon_1(\mathsf{X}) + \upsilon_2(\mathsf{X}), & \deg(\upsilon_2(\mathsf{X})) < \deg(\upsilon_1(\mathsf{X})), \\ \upsilon_1(\mathsf{X}) = \varpi_2(\mathsf{X})\,\upsilon_2(\mathsf{X}) + \upsilon_3(\mathsf{X}), & \deg(\upsilon_3(\mathsf{X})) < \deg(\upsilon_2(\mathsf{X})), \\ \upsilon_2(\mathsf{X}) = \varpi_3(\mathsf{X})\,\upsilon_3(\mathsf{X}) + \upsilon_4(\mathsf{X}), & \deg(\upsilon_4(\mathsf{X})) < \deg(\upsilon_3(\mathsf{X})), \\ \vdots & \vdots \\ \upsilon_{n-2}(\mathsf{X}) = \varpi_{n-1}(\mathsf{X})\,\upsilon_{n-1}(\mathsf{X}) + \upsilon_n(\mathsf{X}), & \deg(\upsilon_n(\mathsf{X})) < \deg(\upsilon_{n-1}(\mathsf{X})), \\ \upsilon_{n-1}(\mathsf{X}) = \varpi_n(\mathsf{X})\,\upsilon_n(\mathsf{X}), & \end{array}\right. \tag{10.2}$$

όπου για κάποιον $n \geqslant 2$ έχουμε $\upsilon_i(\mathsf{X}) \neq 0_{K[\mathsf{X}]}$ για κάθε $i \in \{0, \ldots, n\}$ και κατ' ανάγκην $\upsilon_{n+1}(\mathsf{X}) = 0_{K[\mathsf{X}]}$ (διότι οι βαθμοί των $\upsilon_1(\mathsf{X}), \upsilon_2(\mathsf{X}), \upsilon_3(\mathsf{X}), \ldots$ σχηματίζουν μια φθίνουσα ακολουθία εντός τού (επεκτεταμένου) συνόλου $\mathbb{N}_0 \cup \{-\infty\}$), και

$$\begin{aligned} &\text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X})) = \text{μκδ}(\upsilon_0(\mathsf{X}), \upsilon_1(\mathsf{X})) = \text{μκδ}(\upsilon_1(\mathsf{X}), \upsilon_2(\mathsf{X})) \\ &= \text{μκδ}(\upsilon_2(\mathsf{X}), \upsilon_3(\mathsf{X})) = \cdots = \text{μκδ}(\upsilon_{n-1}(\mathsf{X}), \upsilon_n(\mathsf{X})) = \text{μκδ}(\upsilon_n(\mathsf{X}), 0_{K[\mathsf{X}]}). \end{aligned}$$

Εξ αυτών προκύπτει ότι

$$\boxed{\text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X})) = \text{μκδ}(\upsilon_n(\mathsf{X}), 0_{K[\mathsf{X}]}) = c^{-1}\upsilon_n(\mathsf{X}),} \tag{10.3}$$

όπου $c \in K \setminus \{0_K\}$ είναι ο επικεφαλής συντελεστής τού $\upsilon_n(\mathsf{X})$. Σημειωτέον ότι μέσω τού ανωτέρω ευκλειδείου αλγορίθμου έχουμε *και* τη δυνατότητα προσδιορισμού δυο πολυωνύμων $\alpha(\mathsf{X}), \beta(\mathsf{X}) \in K[\mathsf{X}]$, τέτοιων ώστε να ισχύει

$$\boxed{\text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X})) = \alpha(\mathsf{X})\varphi(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X}).} \tag{10.4}$$

Προς τούτο θεωρούμε τα

$$\left\{\begin{array}{ll} \alpha_0(\mathsf{X}) := 1_K, & \beta_0(\mathsf{X}) := 0_K, \\ \alpha_1(\mathsf{X}) := 0_K, & \beta_1(\mathsf{X}) := 1_K, \\ \alpha_j(\mathsf{X}) = \alpha_{j-2}(\mathsf{X}) - \alpha_{j-1}(\mathsf{X})\varpi_{j-1}(\mathsf{X}), & \beta_j(\mathsf{X}) = \beta_{j-2}(\mathsf{X}) - \beta_{j-1}(\mathsf{X})\varpi_{j-1}(\mathsf{X}), \end{array}\right.$$

για κάθε $j \in \{2, \ldots, n\}$, όπου τα $\varpi_1(\mathsf{X}), \varpi_2(\mathsf{X}), \ldots, \varpi_n(\mathsf{X})$ είναι τα πηλίκα των διαιρέσεων (10.2).

10.1.8 Πρόταση. *Ως πολυώνυμα $\alpha(\mathsf{X}), \beta(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει η (10.4), μπορούν να επιλεγούν τα*

$$\boxed{\alpha(\mathsf{X}) := c^{-1}\alpha_n(\mathsf{X})} \quad \text{και} \quad \boxed{\beta(\mathsf{X}) := c^{-1}\beta_n(\mathsf{X}),} \tag{10.5}$$

όπου $c \in K \setminus \{0_K\}$ είναι ο επικεφαλής συντελεστής τού $\upsilon_n(\mathsf{X})$.

Απόδειξη. Χρησιμοποιώντας τις διαιρέσεις (10.2) θα αποδείξουμε τις ισότητες

$$\upsilon_j(\mathsf{X}) = \alpha_j(\mathsf{X})\varphi(\mathsf{X}) + \beta_j(\mathsf{X})\psi(\mathsf{X}), \quad \forall j \in \{0, 1, \ldots, n\}, \tag{10.6}$$

μέσω μαθηματικής επαγωγής ως προς τον j. Για $j = 0$ λαμβάνουμε

$$\varphi(\mathsf{X}) = \upsilon_0(\mathsf{X}) = 1_K \cdot \varphi(\mathsf{X}) + 0_K \cdot \psi(\mathsf{X}) = \alpha_0(\mathsf{X})\varphi(\mathsf{X}) + \beta_0(\mathsf{X})\psi(\mathsf{X}),$$

ενώ για $j = 1$,

$$\psi(\mathsf{X}) = \upsilon_1(\mathsf{X}) = 0_K \cdot \varphi(\mathsf{X}) + 1_K \cdot \psi(\mathsf{X}) = \alpha_1(\mathsf{X})\varphi(\mathsf{X}) + \beta_1(\mathsf{X})\psi(\mathsf{X}).$$

Υποθέτοντας ότι $\upsilon_j(\mathsf{X}) = \alpha_j(\mathsf{X})\varphi(\mathsf{X}) + \beta_j(\mathsf{X})\psi(\mathsf{X})$ για κάθε $j \in \{1, \ldots, k-1\}$, όπου $2 \leqslant k \leqslant n$, έχουμε $\upsilon_k(\mathsf{X}) = \upsilon_{k-2}(\mathsf{X}) - \varpi_{k-1}(\mathsf{X})\,\upsilon_{k-1}(\mathsf{X})$, οπότε, λόγω τής επαγωγικής υποθέσεώς μας,

$$\begin{aligned}
\upsilon_k(\mathsf{X}) &= (\alpha_{k-2}(\mathsf{X})\varphi(\mathsf{X}) + \beta_{k-2}(\mathsf{X})\psi(\mathsf{X})) - \varpi_{k-1}(\mathsf{X})\,(\alpha_{k-1}(\mathsf{X})\varphi(\mathsf{X}) + \beta_{k-1}(\mathsf{X})\psi(\mathsf{X})) \\
&= (\alpha_{k-2}(\mathsf{X}) - \alpha_{k-1}(\mathsf{X})\varpi_{k-1}(\mathsf{X}))\,\varphi(\mathsf{X}) + (\beta_{k-2}(\mathsf{X}) - \beta_{k-1}(\mathsf{X})\varpi_{k-1}(\mathsf{X}))\,\psi(\mathsf{X}) \\
&= \alpha_k(\mathsf{X})\varphi(\mathsf{X}) + \beta_k(\mathsf{X})\psi(\mathsf{X})
\end{aligned}$$

και οι (10.6) είναι όντως αληθείς. Για $j = n$ λαμβάνουμε

$$c^{-1}\upsilon_n(\mathsf{X}) = (c^{-1}\alpha_n(\mathsf{X}))\varphi(\mathsf{X}) + (c^{-1}\beta_n(\mathsf{X}))\psi(\mathsf{X}) = \text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X}))$$

(μέσω των ισοτήτων (10.3)). □

10.1.9 Σημείωση. Τα ως άνω προσδιορισθέντα πολυώνυμα (10.5) *δεν είναι* τα μόνα στοιχεία τού $K[\mathsf{X}]$ που ικανοποιούν την (10.4). Επί παραδείγματι, επειδή για τον $\delta(\mathsf{X}) := \text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X}))$

$$\exists\, \zeta(\mathsf{X}), \theta(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\} : \varphi(\mathsf{X}) = \delta(\mathsf{X})\zeta(\mathsf{X}),\ \psi(\mathsf{X}) = \delta(\mathsf{X})\theta(\mathsf{X}),$$

η ισότητα

$$\delta(\mathsf{X}) = (\alpha(\mathsf{X}) + \gamma(\mathsf{X})\theta(\mathsf{X}))\varphi(\mathsf{X}) + (\beta(\mathsf{X}) - \gamma(\mathsf{X})\zeta(\mathsf{X}))\psi(\mathsf{X})$$

ισχύει για *κάθε* $\gamma(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$ (!), καθόσον από τις

$$\delta(\mathsf{X})\zeta(\mathsf{X})\psi(\mathsf{X}) = \varphi(\mathsf{X})\psi(\mathsf{X}) = \psi(\mathsf{X})\varphi(\mathsf{X}) = \delta(\mathsf{X})\theta(\mathsf{X})\varphi(\mathsf{X})$$

προκύπτει ότι

$$\left.\begin{aligned} \delta(\mathsf{X})\,(\zeta(\mathsf{X})\psi(\mathsf{X}) - \theta(\mathsf{X})\varphi(\mathsf{X})) &= 0_{K[\mathsf{X}]} \\ \delta(\mathsf{X}) &\neq 0_{K[\mathsf{X}]} \end{aligned}\right\} \underset{\text{6.3.9 (ii)}}{\Longrightarrow} \zeta(\mathsf{X})\psi(\mathsf{X}) = \theta(\mathsf{X})\varphi(\mathsf{X}).$$

10.1.10 Παράδειγμα. Για τα $\varphi(\mathsf{X}) := \frac{1}{2}\mathsf{X}^5 + \frac{1}{4}\mathsf{X}^4 - \frac{17}{10}\mathsf{X}^3 + \frac{7}{5}\mathsf{X}^2 - \frac{6}{5}\mathsf{X} + \frac{3}{4} \in \mathbb{Q}[\mathsf{X}]$ και $\psi(\mathsf{X}) := \mathsf{X}^2 + \frac{1}{2}\mathsf{X} - 5 \in \mathbb{Q}[\mathsf{X}]$ έχουμε

$$\begin{aligned}
\varphi(\mathsf{X}) &= (\tfrac{1}{2}\mathsf{X}^3 + \tfrac{4}{5}\mathsf{X} + 1)\psi(\mathsf{X}) + (\tfrac{23}{10}\mathsf{X} + \tfrac{23}{4}), \\
\psi(\mathsf{X}) &= (\tfrac{10}{23}\mathsf{X} - \tfrac{20}{23})(\tfrac{23}{10}\mathsf{X} + \tfrac{23}{4}) + 0,
\end{aligned}$$

οπότε $\text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X})) = \frac{10}{23}(\frac{23}{10}\mathsf{X} + \frac{23}{4}) = \mathsf{X} + \frac{5}{2}$. Επιπροσθέτως,

$$\mathsf{X} + \tfrac{5}{2} = \tfrac{10}{23}\varphi(\mathsf{X}) - \left(\tfrac{5}{23}x^3 + \tfrac{8}{23}x + \tfrac{10}{23}\right)\psi(\mathsf{X}).$$

‣ **Τι συμβαίνει όταν επεκτείνουμε το σώμα αναφοράς μας;** Βάσει των όσων προαναφέρθησαν, δοθέντων δυο πολυωνύμων $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]$, γνωρίζουμε το πώς μπορούμε να προσδιορίσουμε τον μέγιστο κοινό τους διαιρέτη. Ερώτημα: Εάν L είναι μια επέκταση τού K, τότε τα $\varphi(\mathsf{X}), \psi(\mathsf{X})$, θεωρούμενα ως πολυώνυμα *ανήκοντα στον* $L[\mathsf{X}]$, διαθέτουν ωσαύτως έναν (και μόνον) μέγιστο κοινό διαιρέτη αλλά *εντός τού* $L[\mathsf{X}]$. Πώς σχετίζονται αυτοί οι δύο μέγιστοι κοινοί διαιρέτες; Η απάντηση δίδεται στην ακόλουθη πρόταση.

10.1.11 Πρόταση. *Έστω ότι* $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]$ *και ότι* L *είναι μια επέκταση τού* K. *Συμβολίζουμε ως* $\delta_K(\mathsf{X})$ *τον μέγιστο κοινό διαιρέτη των* $\varphi(\mathsf{X}), \psi(\mathsf{X})$ *εντός τού* $K[\mathsf{X}]$ *και ως* $\delta_L(\mathsf{X})$ *τον μέγιστο κοινό διαιρέτη των* $\varphi(\mathsf{X}), \psi(\mathsf{X})$ *εντός τού* $L[\mathsf{X}]$. *Τότε* $\delta_K(\mathsf{X}) = \delta_L(\mathsf{X})$.

Απόδειξη. Εάν (τουλάχιστον) ένα εκ των $\varphi(\mathsf{X}), \psi(\mathsf{X})$ είναι το μηδενικό πολυώνυμο, τότε ο ισχυρισμός είναι προδήλως αληθής. Ας υποθέσουμε ότι αμφότερα τα $\varphi(\mathsf{X}), \psi(\mathsf{X})$ είναι μη μηδενικά. Τότε (σύμφωνα με το θεώρημα 10.1.1) υπάρχουν μονοσημάντως ορισμένα πολυώνυμα $\varpi(\mathsf{X}), \upsilon(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει

$$\varphi(\mathsf{X}) = \varpi(\mathsf{X})\psi(\mathsf{X}) + \upsilon(\mathsf{X}), \quad \deg(\upsilon(\mathsf{X})) < \deg(\psi(\mathsf{X})). \tag{10.7}$$

Κατ' αναλογίαν, υπάρχουν μονοσημάντως ορισμένα $\varpi'(\mathsf{X}), \upsilon'(\mathsf{X}) \in L[\mathsf{X}]$, τέτοια ώστε να ισχύει

$$\varphi(\mathsf{X}) = \varpi'(\mathsf{X})\psi(\mathsf{X}) + \upsilon'(\mathsf{X}), \quad \deg\big(\upsilon'(\mathsf{X})\big) < \deg(\psi(\mathsf{X})).$$

Όμως η ισότητα (10.7) εξακολουθεί να ισχύει και *εντός τού* $L[\mathsf{X}]$ (διότι έχουμε $K[\mathsf{X}] \subseteq L[\mathsf{X}]$), οπότε (από την ιδιότητα τής μοναδικότητας πηλίκων και υπολοίπων) ισχύει κατ' ανάγκην

$$\varpi'(\mathsf{X}) = \varpi(\mathsf{X}) \in K[\mathsf{X}] \quad \text{και} \quad \upsilon'(\mathsf{X}) = \upsilon(\mathsf{X}) \in K[\mathsf{X}].$$

Κατά συνέπειαν, ο κατάλογος των ισοτήτων που εμφανίζονται κατά την εκτέλεση τού ευκλειδείου αλγορίθμου *εντός τού* $L[\mathsf{X}]$ ταυτίζεται με τον κατάλογο (10.2) των ισοτήτων που εμφανίζονται κατά την εκτέλεση τού ευκλειδείου αλγορίθμου *εντός τού* $K[\mathsf{X}]$. Εξ αυτού έπεται ότι $\delta_K(\mathsf{X}) = \delta_L(\mathsf{X})$. □

‣ **Μέγιστος κοινός διαιρέτης περισσοτέρων πολυωνύμων.** Άπαξ και έχει ορισθεί ο μέγιστος κοινός διαιρέτης *δύο* πολυωνύμων, ο μέγιστος κοινός διαιρέτης περισσοτέρων πολυωνύμων μπορεί να ορισθεί αναδρομικώς.

10.1.12 Ορισμός. Εάν $\varphi_1(\mathsf{X}), \ldots, \varphi_k(\mathsf{X}) \in K[\mathsf{X}]$, όπου $k \in \mathbb{N}$, $k \geqslant 3$, τότε ο **μέγιστος κοινός διαιρέτης** $\mu\kappa\delta(\varphi_1(\mathsf{X}), \ldots, \varphi_k(\mathsf{X}))$ των $\varphi_1(\mathsf{X}), \ldots, \varphi_k(\mathsf{X})$ ορίζεται μέσω τού αναδρομικού τύπου

$$\mu\kappa\delta(\varphi_1(\mathsf{X}), \ldots, \varphi_k(\mathsf{X})) := \mu\kappa\delta(\mu\kappa\delta(\varphi_1(\mathsf{X}), \ldots, \varphi_{k-1}(\mathsf{X})), \varphi_k(\mathsf{X})).$$

10.1.13 Πρόταση. *Εάν* $\varphi_1(\mathsf{X}), \ldots, \varphi_k(\mathsf{X}) \in K[\mathsf{X}]$, *όπου* $k \in \mathbb{N}$, $k \geqslant 2$, *τότε υφίστανται πολυώνυμα* $\omega_1(\mathsf{X}), \ldots, \omega_k(\mathsf{X}) \in K[\mathsf{X}]$, *τέτοια ώστε να ισχύει*

$$\mu\kappa\delta(\varphi_1(\mathsf{X}), \ldots, \varphi_k(\mathsf{X})) = \omega_1(\mathsf{X})\varphi_1(\mathsf{X}) + \cdots + \omega_k(\mathsf{X})\varphi_k(\mathsf{X}).$$

Απόδειξη. Λόγω τού αναδρομικού ορισμού 10.1.12 τού μεγίστου κοινού διαιρέτη πολυωνύμων περισσοτέρων των δύο, η απόδειξη ανάγεται επαγωγικώς στην επαλήθευση τού ισχυρισμού όταν $k = 2$. Εν τοιαύτη περιπτώσει χρησιμοποιούμε την πρόταση 10.1.6. (Φυσικά, είναι δυνατός και ο ακριβής *προσδιορισμός* μιας τέτοιας k-άδας πολυωνύμων $\omega_1(\mathsf{X}), \ldots, \omega_k(\mathsf{X}) \in K[\mathsf{X}]$ μέσω επαναλαμβανόμενης εφαρμογής τής προτάσεως 10.1.8.) □

10.1.14 Ορισμός. Έστω ότι $\varphi_1(\mathsf{X}), \dots, \varphi_k(\mathsf{X}) \in K[\mathsf{X}]$, όπου $k \in \mathbb{N}$, $k \geqslant 2$. Λέμε ότι αυτά τα πολυώνυμα είναι

(i) **πρώτα μεταξύ τους** όταν $\mu\kappa\delta(\varphi_1(\mathsf{X}), \dots, \varphi_k(\mathsf{X})) = 1_K$, και

(ii) **πρώτα μεταξύ τους (ή σχετικώς πρώτα) ανά δύο** όταν

$$\mu\kappa\delta(\varphi_i(\mathsf{X}), \varphi_j(\mathsf{X})) = 1_K$$

για οιουσδήποτε $i, j \in \{1, \dots, k\}$, $i < j$.

(Σημειωτέον ότι εάν ικανοποιείται η συνθήκη (ii), τότε ικανοποιείται αυτομάτως και η συνθήκη (i). Ωστόσο, το αντίστροφο δεν είναι εν γένει αληθές όταν $k \geqslant 3$.)

10.1.15 Πόρισμα. *Εάν $\varphi_1(\mathsf{X}), \dots, \varphi_k(\mathsf{X}) \in K[\mathsf{X}]$, $k \in \mathbb{N}$, $k \geqslant 2$, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Τα $\varphi_1(\mathsf{X}), \dots, \varphi_k(\mathsf{X})$ είναι πρώτα μεταξύ τους.*

(ii) *Υφίστανται πολυώνυμα $\omega_1(\mathsf{X}), \dots, \omega_k(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει*

$$\omega_1(\mathsf{X})\varphi_1(\mathsf{X}) + \cdots + \omega_k(\mathsf{X})\varphi_k(\mathsf{X}) = 1_K.$$

Απόδειξη. (i)⇒(ii) Έπεται άμεσα από την πρόταση 10.1.13.

(ii)⇒(i) Προφανώς, $1_K \mid \omega_i(\mathsf{X})$, $\forall i \in \{1, \dots, k\}$. Επιπροσθέτως, για οιοδήποτε $\theta(\mathsf{X}) \in K[\mathsf{X}]$, για το οποίο ισχύει $\theta(\mathsf{X}) \mid \omega_i(\mathsf{X})$, $\forall i \in \{1, \dots, k\}$, έχουμε

$$\theta(\mathsf{X}) \mid \omega_1(\mathsf{X})\varphi_1(\mathsf{X}) + \cdots + \omega_k(\mathsf{X})\varphi_k(\mathsf{X}) = 1_K.$$

(Βλ. 10.1.3 (iii) και (i).) Επομένως, $\mu\kappa\delta(\varphi_1(\mathsf{X}), \dots, \varphi_k(\mathsf{X})) = 1_K$ (επί τη βάσει τού ορισμού 10.1.5). □

10.1.16 Πόρισμα. *Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}), \theta(\mathsf{X}) \in K[\mathsf{X}]$ με $\mu\kappa\delta(\varphi(\mathsf{X}), \psi(\mathsf{X})) = 1_K$ και υποθέσουμε ότι $\varphi(\mathsf{X}) \mid \psi(\mathsf{X})\theta(\mathsf{X})$, τότε $\varphi(\mathsf{X}) \mid \theta(\mathsf{X})$.*

Απόδειξη. Σύμφωνα με το πόρισμα 10.1.15 υφίστανται $\alpha(\mathsf{X}), \beta(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει $\alpha(\mathsf{X})\varphi(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X}) = 1_K$. Εάν $\varphi(\mathsf{X}) \mid \psi(\mathsf{X})\theta(\mathsf{X})$, τότε

$$\theta(\mathsf{X}) = \alpha(\mathsf{X})\varphi(\mathsf{X})\theta(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X})\theta(\mathsf{X})$$

με $\varphi(\mathsf{X}) \mid \alpha(\mathsf{X})\varphi(\mathsf{X})\theta(\mathsf{X})$ και $\varphi(\mathsf{X}) \mid \beta(\mathsf{X})\psi(\mathsf{X})\theta(\mathsf{X})$, οπότε $\varphi(\mathsf{X}) \mid \theta(\mathsf{X})$. □

10.1.17 Πόρισμα. *Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}), \theta(\mathsf{X}) \in K[\mathsf{X}]$ με $\mu\kappa\delta(\varphi(\mathsf{X}), \psi(\mathsf{X})) = 1_K$, τότε ισχύει η συνεπαγωγή*

$$\left.\begin{array}{l} \varphi(\mathsf{X}) \mid \theta(\mathsf{X}) \\ \psi(\mathsf{X}) \mid \theta(\mathsf{X}) \end{array}\right\} \Longrightarrow \varphi(\mathsf{X})\psi(\mathsf{X}) \mid \theta(\mathsf{X}).$$

Απόδειξη. Σύμφωνα με το πόρισμα 10.1.15 υφίστανται $\alpha(\mathsf{X}), \beta(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει $\alpha(\mathsf{X})\varphi(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X}) = 1_K$. Εάν $\varphi(\mathsf{X}) \mid \theta(\mathsf{X})$ και $\psi(\mathsf{X}) \mid \theta(\mathsf{X})$, τότε

$$\theta(\mathsf{X}) = \alpha(\mathsf{X})\varphi(\mathsf{X})\theta(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X})\theta(\mathsf{X})$$

με $\varphi(\mathsf{X})\psi(\mathsf{X}) \mid \varphi(\mathsf{X})\theta(\mathsf{X})$ και $\varphi(\mathsf{X})\psi(\mathsf{X}) \mid \psi(\mathsf{X})\theta(\mathsf{X})$, οπότε $\varphi(\mathsf{X})\psi(\mathsf{X}) \mid \theta(\mathsf{X})$. □

▸ **Ελάχιστο κοινό πολλαπλάσιο.** Ο ορισμός αυτού προκύπτει από τον 10.1.5 ύστερα από *εναλλαγή των ρόλων* διαιρετών και πολλαπλασίων ως ακολούθως:

10.1.18 Ορισμός. Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$, τότε ένα $\eta(\mathsf{X}) \in K[\mathsf{X}]$ καλείται **ελάχιστο κοινό πολλαπλάσιο των** $\varphi(\mathsf{X})$ **και** $\psi(\mathsf{X})$ (εντός τού $K[\mathsf{X}]$) όταν ισχύουν τα εξής:

(i) Το $\eta(\mathsf{X})$ είναι *κοινό πολλαπλάσιο* των πολυωνύμων $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$, ήτοι έχουμε $\varphi(\mathsf{X}) \mid \eta(\mathsf{X})$ και $\psi(\mathsf{X}) \mid \eta(\mathsf{X})$.

(ii) Εάν $\theta(\mathsf{X}) \in K[\mathsf{X}]$ είναι *τυχόν* κοινό πολλαπλάσιο των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$, δηλαδή εάν $\varphi(\mathsf{X}) \mid \theta(\mathsf{X})$ και $\psi(\mathsf{X}) \mid \theta(\mathsf{X})$, τότε $\eta(\mathsf{X}) \mid \theta(\mathsf{X})$.

(iii) Το $\eta(\mathsf{X})$ είναι μονικό πολυώνυμο.

10.1.19 Πρόταση. *Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$, τότε υπάρχει ένα και μόνον ελάχιστο κοινό πολλαπλάσιο $\eta(\mathsf{X})$ των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$. Τούτο ορίζεται ως εξής:*

$$\eta(\mathsf{X}) := c^{-1}\varphi(\mathsf{X})\psi'(\mathsf{X}) = c^{-1}\psi(\mathsf{X})\varphi'(\mathsf{X}), \tag{10.8}$$

όπου $\varphi'(\mathsf{X}), \psi'(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$ είναι τα μονοσημάντως ορισμένα πολυώνυμα για τα οποία ισχύει

$$\varphi(\mathsf{X}) = \text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X}))\varphi'(\mathsf{X}),\ \psi(\mathsf{X}) = \text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X}))\psi'(\mathsf{X})$$

και c ο επικεφαλής συντελεστής τού $\varphi(\mathsf{X})\psi'(\mathsf{X}) = \psi(\mathsf{X})\varphi'(\mathsf{X})$.

ΑΠΟΔΕΙΞΗ. **Βήμα 1ο**. *Ύπαρξη τού ελαχίστου κοινού πολλαπλασίου.* Θέτοντας $\delta(\mathsf{X}) := \text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X}))$ παρατηρούμε ότι

$$\delta(\mathsf{X})\varphi(\mathsf{X})\psi'(\mathsf{X}) = \varphi(\mathsf{X})\psi(\mathsf{X}) = \psi(\mathsf{X})\varphi(\mathsf{X}) = \delta(\mathsf{X})\psi(\mathsf{X})\varphi'(\mathsf{X}),$$

απ' όπου προκύπτει ότι

$$\left.\begin{array}{r} \delta(\mathsf{X})\left(\varphi(\mathsf{X})\psi'(\mathsf{X}) - \psi(\mathsf{X})\varphi'(\mathsf{X})\right) = 0_{K[\mathsf{X}]} \\ \delta(\mathsf{X}) \neq 0_{K[\mathsf{X}]} \end{array}\right\} \underset{6.3.9\ \text{(ii)}}{\Longrightarrow} \varphi(\mathsf{X})\psi'(\mathsf{X}) = \psi(\mathsf{X})\varphi'(\mathsf{X}).$$

Το (μέσω τής (10.8) οριζόμενο) *μονικό* πολυώνυμο $\eta(\mathsf{X})$ είναι (προφανώς) *κοινό πολλαπλάσιο* των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$. Έστω $\theta(\mathsf{X}) \in K[\mathsf{X}]$ *τυχόν* κοινό πολλαπλάσιο των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$. Τότε

$$\left\{\begin{array}{c} \exists\, \varphi''(\mathsf{X}) \in K[\mathsf{X}] : \theta(\mathsf{X}) = \varphi(\mathsf{X})\varphi''(\mathsf{X}) \\ \text{και } \exists \psi''(\mathsf{X}) \in K[\mathsf{X}] : \theta(\mathsf{X}) = \psi(\mathsf{X})\psi''(\mathsf{X}). \end{array}\right\}$$

Σύμφωνα με την πρόταση 10.1.6 υπάρχουν $\alpha(\mathsf{X}), \beta(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει $\delta(\mathsf{X}) = \alpha(\mathsf{X})\varphi(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X})$. Προφανώς,

$$\delta(\mathsf{X}) = \delta(\mathsf{X})\alpha(\mathsf{X})\varphi'(\mathsf{X}) + \delta(\mathsf{X})\beta(\mathsf{X})\psi'(\mathsf{X}) = \delta(\mathsf{X})(\alpha(\mathsf{X})\varphi'(\mathsf{X}) + \beta(\mathsf{X})\psi'(\mathsf{X}))$$

και

$$\left.\begin{array}{r} \delta(\mathsf{X})\left(\alpha(\mathsf{X})\varphi'(\mathsf{X}) + \beta(\mathsf{X})\psi'(\mathsf{X}) - 1_K\right) = 0_{K[\mathsf{X}]} \\ \delta(\mathsf{X}) \neq 0_{K[\mathsf{X}]} \end{array}\right\} \underset{6.3.9\ \text{(ii)}}{\Longrightarrow} \alpha(\mathsf{X})\varphi'(\mathsf{X}) + \beta(\mathsf{X})\psi'(\mathsf{X}) = 1_K.$$

Εξ αυτού έπεται ότι

$$\begin{aligned} &(\alpha(\mathsf{X})\psi''(\mathsf{X}) + \beta(\mathsf{X})\varphi''(\mathsf{X}))\varphi(\mathsf{X})\psi'(\mathsf{X}) \\ &= \alpha(\mathsf{X})\underbrace{\varphi(\mathsf{X})\psi'(\mathsf{X})}_{=\psi(\mathsf{X})\varphi'(\mathsf{X})}\psi''(\mathsf{X}) + \beta(\mathsf{X})\underbrace{\varphi(\mathsf{X})\varphi''(\mathsf{X})}_{=\theta(\mathsf{X})}\psi'(\mathsf{X}) \\ &= \alpha(\mathsf{X})\theta(\mathsf{X})\varphi'(\mathsf{X}) + \beta(\mathsf{X})\theta(\mathsf{X})\psi'(\mathsf{X}) = (\alpha(\mathsf{X})\varphi'(\mathsf{X}) + \beta(\mathsf{X})\psi'(\mathsf{X}))\theta(\mathsf{X}) = \theta(\mathsf{X}). \end{aligned}$$

Άρα το $\eta(\mathsf{X})$ είναι ελάχιστο κοινό πολλαπλάσιο των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$, διότι

$$\left.\begin{array}{r} \eta(\mathsf{X}) \mid c\left(c^{-1}\varphi(\mathsf{X})\psi'(\mathsf{X})\right) = \varphi(\mathsf{X})\psi'(\mathsf{X}) \\ \varphi(\mathsf{X})\psi'(\mathsf{X}) \mid \theta(\mathsf{X}) \end{array}\right\} \Rightarrow \eta(\mathsf{X}) \mid \theta(\mathsf{X}).$$

Βήμα 2ο. *Μοναδικότητα τού ελαχίστου κοινού πολλαπλασίου.* Εάν τα $\eta(\mathsf{X}), \eta'(\mathsf{X})$ είναι ελάχιστα κοινά πολλαπλάσια των $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]\setminus\{0_{K[\mathsf{X}]}\}$, τότε έχουμε $\eta(\mathsf{X}) \mid \eta'(\mathsf{X})$ και $\eta'(\mathsf{X}) \mid \eta(\mathsf{X})$ (λόγω τής 10.1.18 (ii)), οπότε $\eta(\mathsf{X}) = \eta'(\mathsf{X})$ δυνάμει τού λήμματος 10.1.4. □

10.1.20 Σημείωση. (i) Το ανωτέρω ορισθέν ελάχιστο κοινό πολλαπλάσιο δυο πολυωνύμων $\varphi(\mathsf{X}) \in K[\mathsf{X}]\setminus\{0_{K[\mathsf{X}]}\}$ και $\psi(\mathsf{X}) \in K[\mathsf{X}]\setminus\{0_{K[\mathsf{X}]}\}$ θα σημειώνεται εφεξής ως εκπ$(\varphi(\mathsf{X}), \psi(\mathsf{X}))$.

(ii) Εάν $\psi(\mathsf{X}) \mid \varphi(\mathsf{X})$, τότε εκπ$(\varphi(\mathsf{X}), \psi(\mathsf{X})) = c^{-1}\varphi(\mathsf{X})$, όπου $c \in K\setminus\{0_K\}$ είναι ο επικεφαλής συντελεστής τού $\varphi(\mathsf{X})$.

(iii) Εάν αμφότερα τα $\varphi(\mathsf{X}), \psi(\mathsf{X})$ είναι μηδενικά, τότε γενικεύουμε την έννοια τού ελαχίστου κοινού πολλαπλασίου θέτοντας εκπ$(\varphi(\mathsf{X}), \psi(\mathsf{X})) := 0_{K[\mathsf{X}]}$. Εάν μόνον ένα εξ αυτών, ας πούμε το $\psi(\mathsf{X})$, είναι μηδενικό, τότε θέτουμε *εξ ορισμού* εκπ$(\varphi(\mathsf{X}), \psi(\mathsf{X})) := c^{-1}\varphi(\mathsf{X})$, όπου $c \in K\setminus\{0_K\}$ είναι ο επικεφαλής συντελεστής τού $\varphi(\mathsf{X})$ (γενικεύοντας το (ii) *και* σε αυτήν την περίπτωση).

(iv) Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]$ και $c_1, c_2 \in K\setminus\{0_K\}$, τότε

$$\boxed{\text{εκπ}(\varphi(\mathsf{X}), \psi(\mathsf{X})) = \text{εκπ}(c_1\varphi(\mathsf{X}), c_2\psi(\mathsf{X})).}$$

Πράγματι· εάν $\eta(\mathsf{X}) := \text{εκπ}(\varphi(\mathsf{X}), \psi(\mathsf{X}))$ και $\eta'(\mathsf{X}) := \text{εκπ}(c_1\varphi(\mathsf{X}), c_2\psi(\mathsf{X}))$, τότε

$$\left.\begin{array}{l} [\varphi(\mathsf{X}) \mid c_1\varphi(\mathsf{X}),\ c_1\varphi(\mathsf{X}) \mid \eta'(\mathsf{X})] \Rightarrow \varphi(\mathsf{X}) \mid \eta'(\mathsf{X}) \\ [\psi(\mathsf{X}) \mid c_2\psi(\mathsf{X}),\ c_2\psi(\mathsf{X}) \mid \eta'(\mathsf{X})] \Rightarrow \psi(\mathsf{X}) \mid \eta'(\mathsf{X}) \end{array}\right\} \Rightarrow \eta(\mathsf{X}) \mid \eta'(\mathsf{X})$$

(βλ. 10.1.3 (ii) και 10.1.18 (ii)). Από την άλλη μεριά,

$$\left\{\begin{array}{l} \eta(\mathsf{X}) = c_1^{-1}\left(c_1\eta(\mathsf{X})\right) \Rightarrow c_1\eta(\mathsf{X}) \mid \eta(\mathsf{X}) \\ \eta(\mathsf{X}) = c_2^{-1}\left(c_2\eta(\mathsf{X})\right) \Rightarrow c_2\eta(\mathsf{X}) \mid \eta(\mathsf{X}) \end{array}\right\},$$

οπότε

$$\left.\begin{array}{l} [c_1\varphi(\mathsf{X}) \mid c_1\eta(\mathsf{X}),\ c_1\eta(\mathsf{X}) \mid \eta(\mathsf{X})] \Rightarrow c_1\varphi(\mathsf{X}) \mid \eta(\mathsf{X}) \\ [c_2\psi(\mathsf{X}) \mid c_2\eta(\mathsf{X}),\ c_2\eta(\mathsf{X}) \mid \eta(\mathsf{X})] \Rightarrow c_2\psi(\mathsf{X}) \mid \eta(\mathsf{X}) \end{array}\right\} \Rightarrow \eta'(\mathsf{X}) \mid \eta(\mathsf{X}).$$

Κατά το λήμμα 10.1.4, $\eta(\mathsf{X}) = \eta'(\mathsf{X})$.

(v) Άπαξ και έχει ορισθεί το ελάχιστο κοινό πολλαπλάσιο *δύο* πολυωνύμων, το ελάχιστο κοινό πολλαπλάσιο περισσοτέρων πολυωνύμων μπορεί να ορισθεί αναδρομικώς: Εάν $\varphi_1(\mathsf{X}), \ldots, \varphi_k(\mathsf{X}) \in K[\mathsf{X}]$, όπου $k \in \mathbb{N}$, $k \geqslant 3$, τότε

$$\text{εκπ}(\varphi_1(\mathsf{X}), \ldots, \varphi_k(\mathsf{X})) := \text{εκπ}(\text{εκπ}(\varphi_1(\mathsf{X}), \ldots, \varphi_{k-1}(\mathsf{X})), \varphi_k(\mathsf{X})).$$

10.2 ΘΕΣΕΙΣ ΜΗΔΕΝΙΣΜΟΥ ΠΟΛΥΩΝΥΜΩΝ

10.2.1 Ορισμός. Για οιοδήποτε στοιχείο λ ενός σώματος K ορίζεται η **συνάρτηση $\mathfrak{y}_\lambda$ πολυωνυμικής αποτιμήσεως στο λ** ως εξής:

$$K[\mathsf{X}] \ni \sum_{i=0}^{n} a_i\mathsf{X}^i = \varphi(\mathsf{X}) \xmapsto{\mathfrak{y}_\lambda} \mathfrak{y}_\lambda(\varphi(\mathsf{X})) := \varphi(\lambda) := \sum_{i=0}^{n} a_i\lambda^i \in K.$$

10.2.2 Σημείωση. Εάν $\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in K[\mathsf{X}]$, τότε η **συνάρτηση η επαγομένη από το** $\varphi(\mathsf{X})$ είναι η

$$\mathfrak{v}_{\varphi(\mathsf{X})} : K \longrightarrow K, \quad \lambda \longmapsto \mathfrak{v}_{\varphi(\mathsf{X})}(\lambda) := \mathfrak{y}_\lambda(\varphi(\mathsf{X})) = \varphi(\lambda) = \sum_{i=0}^{n} a_i \lambda^i$$

και μέσω αυτής ορίζεται ο ομομορφισμός δακτυλίων

$$\boxed{K[\mathsf{X}] \longrightarrow K^K, \quad \varphi(\mathsf{X}) \longmapsto \mathfrak{v}_{\varphi(\mathsf{X})},}$$

που δεν είναι κατ' ανάγκην μονομορφισμός δακτυλίων! (Βλ. εδ. 6.3.13.) Μια ικανή συνθήκη για να είναι μονομορφισμός δίδεται στο πόρισμα 10.2.9.

10.2.3 Ορισμός. Έστω L μια επέκταση ενός σώματος K και έστω $\varphi(\mathsf{X}) \in K[\mathsf{X}]$. Ένα στοιχείο $\lambda \in L$ ονομάζεται **θέση μηδενισμού**[3] (ή **σημείο μηδενισμού**) τού πολυωνύμου $\varphi(\mathsf{X})$ **εντός τού** L όταν

$$\mathfrak{y}_\lambda(\varphi(\mathsf{X}))) := \varphi(\lambda) = 0_L \ (= 0_K),$$

δηλαδή όταν η τιμή τού $\varphi(\mathsf{X})$ για $\mathsf{X} = \lambda$ είναι το μηδενικό στοιχείο.

10.2.4 Πρόταση. *Έστω K ένα σώμα. Εάν $\lambda \in K$ και $\varphi(\mathsf{X}) \in K[\mathsf{X}]$, τότε ισχύουν τα εξής:*

(i) *Το υπόλοιπο τής διαιρέσεως τού $\varphi(\mathsf{X})$ διά τού $\mathsf{X} - \lambda$ ισούται με το $\varphi(\lambda)$.*

(ii) *Το λ είναι μια θέση μηδενισμού τού $\varphi(\mathsf{X})$ εντός τού K εάν και μόνον εάν*

$$\mathsf{X} - \lambda \mid \varphi(\mathsf{X}).$$

Απόδειξη. (i) Σύμφωνα με το θεώρημα 10.1.1 υπάρχουν μονοσημάντως ορισμένα πολυώνυμα $\varpi(\mathsf{X})$ και $\upsilon(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει

$$\varphi(\mathsf{X}) = (\mathsf{X} - \lambda)\varpi(\mathsf{X}) + \upsilon(\mathsf{X}), \ \ \deg(\upsilon(\mathsf{X})) < \deg(\mathsf{X} - \lambda) = 1.$$

Επομένως, $\upsilon(\mathsf{X}) = a \in K$, οπότε

$$a = \varphi(\mathsf{X}) - (\mathsf{X} - \lambda)\varpi(\mathsf{X}) \Longrightarrow a = \varphi(\lambda).$$

(ii) Το λ είναι μια θέση μηδενισμού τού $\varphi(\mathsf{X})$ (εντός τού K) εάν και μόνον εάν το υπόλοιπο τής διαιρέσεως τού $\varphi(\mathsf{X})$ διά τού $\mathsf{X}-\lambda$ είναι το $0_{K[\mathsf{X}]}$, πράγμα που σημαίνει ότι $\mathsf{X} - \lambda \mid \varphi(\mathsf{X})$. □

10.2.5 Πόρισμα. *Εάν τα στοιχεία $\lambda_1, \ldots, \lambda_k \in K$ ($k \in \mathbb{N}$) είναι k σαφώς διακεκριμένες θέσεις μηδενισμού ενός πολυωνύμου $\varphi(\mathsf{X}) \in K[\mathsf{X}]$, τότε*

$$(\mathsf{X} - \lambda_1)(\mathsf{X} - \lambda_2)\cdots(\mathsf{X} - \lambda_k) \mid \varphi(\mathsf{X}).$$

Απόδειξη. Όταν $k = 1$, αυτό είναι αληθές λόγω τής προτάσεως 10.2.4. Θα εργασθούμε με τη βοήθεια τής μαθηματικής επαγωγής. Υποθέτουμε ότι ο ισχυρισμός είναι αληθής για $k-1$ θέσεις μηδενισμού, οπότε

$$\varphi(\mathsf{X}) = (\mathsf{X} - \lambda_1)(\mathsf{X} - \lambda_2)\cdots(\mathsf{X} - \lambda_{k-1})\,\psi(\mathsf{X})$$

[3] Εδώ, χρησιμοποιούμε τον όρο *θέση μηδενισμού* ακολουθώντας τή γερμανική ορολογία, η οποία, εν προκειμένω, είναι περισσότερο ακριβής απ' ό,τι η αγγλική· ο διαχωρισμός τού όρου Nullstelle από τον όρο Wurzel (αγγλ. *root*, ελλ. *ρίζα*) είναι επιβεβλημένη, καθότι ένα μιγαδικό πολυώνυμο $\varphi(\mathsf{X}) \in \mathbb{C}[\mathsf{X}]$ μπορεί να μηδενίζεται όταν $\mathsf{X} = \lambda \in \mathbb{C}$, χωρίς, ωστόσο, το λ να προκύπτει από επίλυση τής εξισώσεως $\varphi(\mathsf{X}) = 0$ μέσω αποκλειστικής χρήσεως *ριζικών*. (Από την άλλη όμως μεριά, ονομάζουμε, π.χ., τις θέσεις μηδενισμού τής εξισώσεως $\mathsf{X}^\nu = 1$ ν-οστές *ρίζες τής μονάδας*.)

για κάποιο $\psi(\mathsf{X}) \in K[\mathsf{X}]$. Κατόπιν αποτιμήσεως των δύο μελών τής ανωτέρω ισότητας για $\mathsf{X} = \lambda_k$ λαμβάνουμε

$$0_K = \varphi(\lambda_k) = (\lambda_k - \lambda_1)\,(\lambda_k - \lambda_2) \cdots (\lambda_k - \lambda_{k-1})\,\psi(\lambda_k),$$

απ' όπου προκύπτει ότι $\psi(\lambda_k) = 0_K$ (λόγω τής αρχικής υποθέσεώς μας). Άρα το $\mathsf{X} - \lambda_k$ διαιρεί το πολυώνυμο $\psi(\mathsf{X})$, οπότε ο ισχυρισμός είναι εμφανώς αληθής και για k θέσεις μηδενισμού. □

10.2.6 Πόρισμα. *Κάθε πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$ διαθέτει (συνολικώς) το πολύ* $\deg(\varphi(\mathsf{X}))$ *θέσεις μηδενισμού εντός τού K.*

Απόδειξη. Έπεται από το πόρισμα 10.2.5 και το (iv) τής προτάσεως 10.1.3. □

10.2.7 Πόρισμα. *Εάν ένα πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ διαθέτει εντός τού K θέσεις μηδενισμού, το πλήθος των οποίων υπερβαίνει τον βαθμό του, τότε το $\varphi(\mathsf{X})$ είναι το μηδενικό πολυώνυμο.*

10.2.8 Πόρισμα. *Εάν δυο πολυώνυμα $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$ λαμβάνουν τις ίδιες τιμές σε σαφώς διακεκριμένα στοιχεία τού K, το πλήθος των οποίων υπερβαίνει το* $\max\{\deg(\varphi(\mathsf{X})), \deg(\psi(\mathsf{X}))\}$*, τότε έχουμε $\varphi(\mathsf{X}) = \psi(\mathsf{X})$.*

10.2.9 Πόρισμα. *Εάν το (υποκείμενο σύνολο ενός σώματος) K είναι απειροσύνολο, τότε η*

$$K[\mathsf{X}] \longrightarrow K^K, \quad \varphi(\mathsf{X}) \longmapsto \mathfrak{v}_{\varphi(\mathsf{X})},$$

(βλ. 6.3.13*) αποτελεί έναν μονομορφισμό δακτυλίων.*

Απόδειξη. Θεωρούμε τυχόντα πολυώνυμα $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]$ και τις αντίστοιχες συναρτήσεις $\mathfrak{v}_{\varphi(\mathsf{X})}$ και $\mathfrak{v}_{\psi(\mathsf{X})}$. Εάν ισχύει $\mathfrak{v}_{\varphi(\mathsf{X})} = \mathfrak{v}_{\psi(\mathsf{X})}$, τότε η διαφορά $\varphi(\mathsf{X}) - \psi(\mathsf{X})$ έχει ως θέσεις μηδενισμού της όλα τα στοιχεία τού (υποκειμένου συνόλου τού) K. Δυνάμει τού πορίσματος 10.2.7 έχουμε $\varphi(\mathsf{X}) - \psi(\mathsf{X}) = 0_{K[\mathsf{X}]}$, ήτοι $\varphi(\mathsf{X}) = \psi(\mathsf{X})$. □

10.2.10 Πρόταση (Τύπος παρεμβολής τού Lagrange). *Έστω $n \in \mathbb{N}$ και έστω K ένα σώμα με πληθικό αριθμό* $\mathrm{card}(K) \geqslant n+1$*. Εάν τα $a_0, a_1, \ldots, a_n$ είναι $n+1$ σαφώς διακεκριμένα στοιχεία τού K και τα $c_0, c_1, \ldots, c_n$ τυχόντα (όχι κατ' ανάγκην σαφώς διακεκριμένα) στοιχεία τού K, τότε υπάρχει ένα μονοσημάντως ορισμένο πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ βαθμού $\leqslant n$ (βλ.* (10.10)*), τέτοιο ώστε να ισχύει*

$$\varphi(a_k) = c_k, \quad \forall k \in \{0, 1, \ldots, n\}.$$

Απόδειξη. Το ότι ένα τέτοιου είδους πολυώνυμο θα είναι μονοσημάντως ορισμένο έπεται προφανώς από το πόρισμα 10.2.8. Αρκεί λοιπόν να αποδειχθεί η ύπαρξή του. Προς τούτο ορίζουμε πολυώνυμα $\ell_i(\mathsf{X}) \in K[\mathsf{X}]$, $0 \leqslant i \leqslant n$, ως εξής:

$$\ell_i(\mathsf{X}) := \prod_{j \in \{0,1,\ldots,n\} \setminus \{i\}} (a_i - a_j)^{-1}\,(\mathsf{X} - a_j)\,. \tag{10.9}$$

Προφανώς, $\deg(\ell_i(\mathsf{X})) = n$ και για κάθε $(i,k) \in \{0,1,\ldots,n\} \times \{0,1,\ldots,n\}$ έχουμε

$$\ell_i(a_k) = \begin{cases} 0_K, & \text{όταν } i \neq k, \\ 1_K, & \text{όταν } i = k. \end{cases}$$

Κατά συνέπειαν, το πολυώνυμο

$$\boxed{\varphi(\mathsf{X}) := \sum_{i=0}^{n} c_i \ell_i(\mathsf{X})} \tag{10.10}$$

έχει την επιθυμητή ιδιότητα. □

10.2.11 Ορισμός. Τα (10.9) ονομάζονται **πολυώνυμα τού Lagrange**[4] (για τα στοιχεία $a_0, a_1, \ldots, a_n$), ενώ ο τύπος (10.10), ο οποίος μας παρέχει το $\varphi(\mathsf{X})$, είναι γνωστός ως **τύπος παρεμβολής τού Lagrange**.

10.2.12 Παράδειγμα. Εάν $K = \mathbb{Q}$, $n = 4$, και

$$\left\{ \begin{array}{ccccc} a_0 = -5, & a_1 = -2, & a_2 = 0, & a_3 = 2, & a_4 = 5, \\ c_0 = 0, & c_1 = -3, & c_2 = 0, & c_3 = 0, & c_4 = 1 \end{array} \right\}$$

τότε τα πολυώνυμα τού Lagrange που απαιτούνται είναι μόνον τα

$$\left\{ \begin{array}{l} \ell_1(\mathsf{X}) = -\frac{1}{168}\mathsf{X}\,(\mathsf{X}-2)\,(\mathsf{X}-5)\,(\mathsf{X}+5)\,, \\ \ell_4(\mathsf{X}) = \frac{1}{1050}\mathsf{X}\,(\mathsf{X}-2)\,(\mathsf{X}+2)\,(\mathsf{X}+5)\,. \end{array} \right.$$

Ο τύπος παρεμβολής τού Lagrange δίδει το πολυώνυμο

$$\varphi(\mathsf{X}) = c_1\ell_1(\mathsf{X}) + c_4\ell_4(\mathsf{X}) = \tfrac{79}{4200}\mathsf{X}^4 - \tfrac{13}{420}\mathsf{X}^3 - \tfrac{1891}{4200}\mathsf{X}^2 + \tfrac{367}{420}\mathsf{X}.$$

10.2.13 Ορισμός. Έστω K τυχόν σώμα και έστω $\varphi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$. Για κάθε $\lambda \in K$ θέτουμε

$$\boxed{\text{mult}\,(\varphi(\mathsf{X}); \lambda) := \max\left\{k \in \mathbb{N}_0 : (\mathsf{X}-\lambda)^k \mid \varphi(\mathsf{X})\right\}.}$$

Προφανώς, εάν $\text{mult}(\varphi(\mathsf{X}); \lambda) = m$, τότε $m \geqslant 1 \Leftrightarrow$ το λ είναι μια θέση μηδενισμού τού $\varphi(\mathsf{X})$. Όταν $m \geqslant 1$, λέμε ότι το λ είναι μια θέση μηδενισμού τού $\varphi(\mathsf{X})$ *με πλήθος πολλαπλών εμφανίσεων* ή -απλούστερα- **με πολλαπλότητα** ίση με m. Το λ ονομάζεται, ιδιαιτέρως, **απλή** (και αντιστοίχως, **πολλαπλή** ή **επαναλαμβανόμενη**) **θέση μηδενισμού** τού $\varphi(\mathsf{X})$ όταν $m = 1$ (και αντιστοίχως, όταν $m \geqslant 2$).

10.2.14 Πρόταση. *Εάν $\varphi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$, $\lambda \in K$ και $m \in \mathbb{N}$, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) $\text{mult}(\varphi(\mathsf{X}); \lambda) = m$.

(ii) $\exists \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\} : \varphi(\mathsf{X}) = (\mathsf{X}-\lambda)^m\,\psi(\mathsf{X})$ *με* $\psi(\lambda) \neq 0_K$.

Απόδειξη. (i)⇒(ii) Εάν $\text{mult}(\varphi(\mathsf{X}); \lambda) = m$, τότε $(\mathsf{X}-\lambda)^m \mid \varphi(\mathsf{X})$, οπότε υπάρχει κάποιο $\psi(\mathsf{X}) \neq 0_{K[\mathsf{X}]}$ με $\varphi(\mathsf{X}) = (\mathsf{X}-\lambda)^m\,\psi(\mathsf{X})$. Εάν ίσχυε $\psi(\lambda) = 0_K$, τότε (σύμφωνα με το (ii) τής προτάσεως 10.2.4) θα είχαμε $\mathsf{X} - \lambda \mid \psi(\mathsf{X})$, οπότε $(\mathsf{X}-\lambda)^{m+1} \mid \varphi(\mathsf{X})$, κάτι που θα αντέκειτο στον ορισμό τής πολλαπλότητας τής θέσεως μηδενισμού λ τού $\varphi(\mathsf{X})$. Άρα $\psi(\lambda) \neq 0_K$.

[4] Προς τιμήν τού Joseph-Louis Lagrange (1736-1813) ο οποίος δημοσίευσε ένα άρθρο επ' αυτών το 1795 (αν και είχαν ανακαλυφθεί ήδη από το 1779 από τον Edward Waring (1736-1798) και απέρρεαν εύκολα και από έναν άλλον τύπο δημοσιευθέντα το 1783 από τον Leonhand Euler (1707-1783)).

(ii)⇒(i) Εάν $\exists\,\psi(\mathsf{X}) \in K[\mathsf{X}]\setminus\{0_{K[\mathsf{X}]}\} : \varphi(\mathsf{X}) = (\mathsf{X}-\lambda)^m\,\psi(\mathsf{X})$ με $\psi(\lambda) \neq 0_K$, τότε $(\mathsf{X}-\lambda)^m \mid \varphi(\mathsf{X})$. Ας υποθέσουμε ότι υπάρχει κάποιος $m' \in \mathbb{N}$, $m' > m$, με $(\mathsf{X}-\lambda)^{m'} \mid \varphi(\mathsf{X})$. Τότε υπάρχει κάποιο $\theta(\mathsf{X}) \in K[\mathsf{X}]\setminus\{0_{K[\mathsf{X}]}\}$, τέτοιο ώστε να ισχύει

$$\varphi(\mathsf{X}) = (\mathsf{X}-\lambda)^m\,\psi(\mathsf{X}) = (\mathsf{X}-\lambda)^{m'}\,\theta(\mathsf{X}).$$

Εξ αυτού έπεται ότι

$$(\mathsf{X}-\lambda)^m\,\psi(\mathsf{X}) = (\mathsf{X}-\lambda)^m\,(\mathsf{X}-\lambda)^{m'-m}\,\theta(\mathsf{X}) \Longrightarrow \psi(\mathsf{X}) = (\mathsf{X}-\lambda)^{m'-m}\,\theta(\mathsf{X}),$$

ήτοι ότι $\psi(\lambda) = 0_K$. Άτοπο! Επομένως, $\mathrm{mult}(\varphi(\mathsf{X});\lambda) = m$. □

10.2.15 Ορισμός. Ως **απεικόνιση επίτυπης παραγωγίσεως** (ή **τύποις παραγωγίσεως**) ορίζεται η

$$\boxed{\mathcal{D} : K[\mathsf{X}] \longrightarrow K[\mathsf{X}],\ \mathcal{D}\left(\sum_{i=0}^{n} a_i\mathsf{X}^i\right) := \sum_{i=1}^{n} i a_i \mathsf{X}^{i-1}.}$$

Η εικόνα $\mathcal{D}(\varphi(\mathsf{X}))$ ενός πολυωνύμου $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ μέσω αυτής καλείται **επίτυπη παράγωγος** (ή **τύποις παράγωγος**) τού $\varphi(\mathsf{X})$.

10.2.16 Λήμμα. *Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]$ και $c \in K$, τότε ισχύουν τα εξής:*
(i) $\mathcal{D}(c\,\varphi(\mathsf{X})) = c\,\mathcal{D}(\varphi(\mathsf{X}))$.
(ii) $\mathcal{D}(\varphi(\mathsf{X}) + \psi(\mathsf{X})) = \mathcal{D}(\varphi(\mathsf{X})) + \mathcal{D}(\psi(\mathsf{X}))$.
(iii) $\mathcal{D}(\varphi(\mathsf{X})\psi(\mathsf{X})) = \mathcal{D}(\varphi(\mathsf{X}))\psi(\mathsf{X}) + \mathcal{D}(\psi(\mathsf{X}))\varphi(\mathsf{X})$.

Απόδειξη. Έστω ότι

$$\varphi(\mathsf{X}) = \textstyle\sum_{i=0}^{n} a_i\mathsf{X}^i \ \text{ και } \ \psi(\mathsf{X}) = \sum_{j=0}^{m} b_j\mathsf{X}^j.$$

Δίχως βλάβη τής γενικότητας υποθέτουμε ότι $n \geqslant m$ και θέτουμε $b_i := 0_K$ για κάθε δείκτη $i \in \{m+1, \ldots, n\}$.
(i)-(ii) Προφανώς,

$$\mathcal{D}(c\,\varphi(\mathsf{X})) = \mathcal{D}(c\sum_{i=0}^{n} a_i\mathsf{X}^i) = \mathcal{D}(\sum_{i=0}^{n} ca_i\mathsf{X}^i) = \sum_{i=1}^{n} cia_i\mathsf{X}^{i-1} = c\sum_{i=1}^{n} ia_i\mathsf{X}^{i-1} = c\,\mathcal{D}(\varphi(\mathsf{X}))$$

και

$$\mathcal{D}(\varphi(\mathsf{X}))+\mathcal{D}(\psi(\mathsf{X})) = \sum_{i=1}^{n} ia_i\mathsf{X}^{i-1}+\sum_{j=1}^{m} jb_j\mathsf{X}^{j-1} = \sum_{i=1}^{n} i(a_i+b_i)\mathsf{X}^{i-1} = \mathcal{D}(\varphi(\mathsf{X})+\psi(\mathsf{X})).$$

(iii) Κατ' αρχάς παρατηρούμε ότι για κάθε $(i,j) \in \mathbb{N}_0 \times \mathbb{N}_0$ με $(i,j) \neq (0,0)$ ισχύει

$$\mathcal{D}(\mathsf{X}^i\mathsf{X}^j) = \mathcal{D}(\mathsf{X}^{i+j}) = (i+j)\mathsf{X}^{i+j-1} = \left(i\mathsf{X}^{i-1}\right)\mathsf{X}^j + \left(j\mathsf{X}^{j-1}\right)\mathsf{X}^i = \mathcal{D}(\mathsf{X}^i)\mathsf{X}^j + \mathcal{D}(\mathsf{X}^j)\mathsf{X}^i$$

και $\mathcal{D}(\mathsf{X}^0\mathsf{X}^0) = \mathcal{D}(1_K \cdot 1_K) = \mathcal{D}(1_K) = 0_K = \mathcal{D}(\mathsf{X}^0)\mathsf{X}^0 + \mathcal{D}(\mathsf{X}^0)\mathsf{X}^0$. Εν συνεχεία, συμπεραίνουμε ότι

$$\begin{aligned}
\mathcal{D}(\varphi(\mathsf{X})\psi(\mathsf{X})) &= \mathcal{D}\left(\sum_{i=0}^{n}\sum_{j=0}^{m}\left(a_i\mathsf{X}^i\right)\left(b_j\mathsf{X}^j\right)\right)\\
&= \sum_{i=0}^{n}\sum_{j=0}^{m} a_ib_j\mathcal{D}(\mathsf{X}^i\mathsf{X}^j) = \sum_{i=0}^{n}\sum_{j=0}^{m} a_ib_j(\mathcal{D}(\mathsf{X}^i)\mathsf{X}^j + \mathcal{D}(\mathsf{X}^j)\mathsf{X}^i)\\
&= \left(\sum_{i=0}^{n} a_i\mathcal{D}(\mathsf{X}^i)\right)\left(\sum_{j=0}^{m} b_j\mathsf{X}^j\right) + \left(\sum_{j=0}^{m} b_j\mathcal{D}(\mathsf{X}^j)\right)\left(\sum_{i=0}^{n} a_i\mathsf{X}^i\right)\\
&= \mathcal{D}\left(\sum_{i=0}^{n} a_i\mathsf{X}^i\right)\left(\sum_{j=0}^{m} b_j\mathsf{X}^j\right) + \mathcal{D}\left(\sum_{j=0}^{m} b_j\mathsf{X}^j\right)\left(\sum_{i=0}^{n} a_i\mathsf{X}^i\right)\\
&= \mathcal{D}(\varphi(\mathsf{X}))\psi(\mathsf{X}) + \mathcal{D}(\psi(\mathsf{X}))\varphi(\mathsf{X})
\end{aligned}$$

κάνοντας χρήση των (i) και (ii). □

10.2.17 Σημείωση. (i) Για κάθε $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ έχουμε

$$\deg(\mathcal{D}(\varphi(\mathsf{X}))) \begin{cases} = \deg(\varphi(\mathsf{X})) - 1, & \text{όταν } \text{χαρ}(K) \nmid \deg(\varphi(\mathsf{X})), \\ < \deg(\varphi(\mathsf{X})) - 1, & \text{όταν } \text{χαρ}(K) \mid \deg(\varphi(\mathsf{X})). \end{cases}$$

(ii) Εάν $\varphi_1(\mathsf{X}), \ldots, \varphi_k(\mathsf{X}) \in K[\mathsf{X}]$ ($k \in \mathbb{N}$, $k \geqslant 2$), τότε η ισότητα 10.2.16 (iii) γενικεύεται επαγωγικώς ως εξής:

$$\mathcal{D}\left(\prod_{j=1}^{k} \varphi_j(\mathsf{X})\right) = \sum_{i=1}^{k} \mathcal{D}\left(\varphi_i(\mathsf{X})\right) \prod_{j \in \{1,\ldots,k\} \smallsetminus \{i\}} \varphi_j(\mathsf{X}). \tag{10.11}$$

(iii) Οι *υψηλότερης τάξεως επίτυπες παράγωγοι* ενός $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ ορίζονται κατά τα ειωθότα:

$$\boxed{\mathcal{D}^i(\varphi(\mathsf{X})) := \begin{cases} \varphi(\mathsf{X}), & \text{όταν } i = 0, \\ \mathcal{D}(\mathcal{D}^{i-1}(\varphi(\mathsf{X}))), & \text{όταν } i \geqslant 1. \end{cases}}$$

Συγκεκριμένα, εάν $\varphi(\mathsf{X}) = \sum_{j=0}^{n} a_j \mathsf{X}^j$, $a_n \neq 0_K$, τότε

$$\mathcal{D}^i(\varphi(\mathsf{X})) = \begin{cases} i! \left(\sum_{j=i}^{n} \binom{j}{i} a_j \mathsf{X}^{j-i}\right), & \text{όταν } 0 \leqslant i \leqslant n, \\ 0_{K[\mathsf{X}]}, & \text{όταν } i > n. \end{cases}$$

(iv) Εάν $\text{χαρ}(K) = p$ (p πρώτος), τότε

$$\mathcal{D}^p(\varphi(\mathsf{X})) = 0_{K[\mathsf{X}]}$$

για κάθε $\varphi(\mathsf{X}) \in K[\mathsf{X}]$.

10.2.18 Πρόταση (Κανόνας τού Leibniz). *Εάν* $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]$, *τότε για κάθε* $i \in \mathbb{N}_0$ *έχουμε*

$$\boxed{\mathcal{D}^i(\varphi(\mathsf{X})\psi(\mathsf{X})) = \sum_{k=0}^{i} \binom{i}{k} \mathcal{D}^k(\varphi(\mathsf{X})) \mathcal{D}^{i-k}(\psi(\mathsf{X}))}. \tag{10.12}$$

Απόδειξη. Η ισότητα (10.12) είναι προφανής για $i = 0$ και $i = 1$ (βλ. 10.2.16 (iii)). Εάν υποθέσουμε ότι $i \geqslant 2$ και ότι αυτή είναι αληθής για το $i - 1$, τότε

$$\begin{aligned}
&\mathcal{D}^i(\varphi(\mathsf{X})\psi(\mathsf{X})) = \mathcal{D}(\mathcal{D}^{i-1}(\varphi(\mathsf{X})\psi(\mathsf{X}))) \\
&= \mathcal{D}\left(\sum_{l=0}^{i-1} \binom{i-1}{l} \mathcal{D}^l(\varphi(\mathsf{X})) \mathcal{D}^{i-1-l}(\psi(\mathsf{X}))\right) = \sum_{l=0}^{i-1} \binom{i-1}{l} \mathcal{D}(\mathcal{D}^l(\varphi(\mathsf{X})) \mathcal{D}^{i-1-l}(\psi(\mathsf{X}))) \\
&= \sum_{l=0}^{i-1} \binom{i-1}{l} \mathcal{D}^{l+1}(\varphi(\mathsf{X})) \mathcal{D}^{i-1-l}(\psi(\mathsf{X})) + \sum_{l=0}^{i-1} \binom{i-1}{l} \mathcal{D}^l(\varphi(\mathsf{X})) \mathcal{D}^{i-l}(\psi(\mathsf{X})) \\
&= \sum_{k=1}^{i} \binom{i-1}{k-1} \mathcal{D}^k(\varphi(\mathsf{X})) \mathcal{D}^{i-k}(\psi(\mathsf{X})) + \sum_{k=0}^{i-1} \binom{i-1}{k} \mathcal{D}^k(\varphi(\mathsf{X})) \mathcal{D}^{i-k}(\psi(\mathsf{X})) \\
&= \sum_{k=1}^{i} \left(\binom{i-1}{k-1} + \binom{i-1}{k}\right) \mathcal{D}^k(\varphi(\mathsf{X})) \mathcal{D}^{i-k}(\psi(\mathsf{X})) + \varphi(\mathsf{X}) \mathcal{D}^i(\psi(\mathsf{X})) \\
&= \sum_{k=1}^{i} \binom{i}{k} \mathcal{D}^k(\varphi(\mathsf{X})) \mathcal{D}^{i-k}(\psi(\mathsf{X})) + \varphi(\mathsf{X}) \mathcal{D}^i(\psi(\mathsf{X})) = \sum_{k=0}^{i} \binom{i}{k} \mathcal{D}^k(\varphi(\mathsf{X})) \mathcal{D}^{i-k}(\psi(\mathsf{X})),
\end{aligned}$$

όπου η δεύτερη ισότητα προκύπτει από την επαγωγική μας υπόθεση, η τρίτη από το (ii) τού λήμματος 10.2.16, η τέταρτη από το (iii) τού λήμματος 10.2.16 και η προτελευταία από την τριγωνική ταυτότητα τού Pascal. Άρα η (10.12) είναι αληθής *για κάθε* $i \in \mathbb{N}_0$. □

10.2.19 Πρόταση (Τύπος τού Taylor). *Εάν το* $\varphi(\mathsf{X}) \in K[\mathsf{X}]\setminus\{0_{K[\mathsf{X}]}\}$ *είναι ένα πολυώνυμο βαθμού* n *και η χαρακτηριστική τού* K *είναι είτε* 0 *είτε* $> n$*, τότε*

$$\boxed{\varphi(\mathsf{X}) = \sum_{i=0}^{n} (i!)^{-1}\, \mathcal{D}^i(\varphi(\mathsf{X}))\big|_{\mathsf{X}=\lambda}\, (\mathsf{X}-\lambda)^i,\ \forall \lambda \in K.} \tag{10.13}$$

Απόδειξη[5]. Επειδή για οιουσδήποτε $i, j \in \{0,\dots,n\}$, $i \leqslant j$, ισχύει

$$\mathcal{D}^i(\mathsf{X}^j) = j(j-1)\cdots(j-i+1)\mathsf{X}^{j-i} = i!\tbinom{j}{i}\mathsf{X}^{j-i} \Rightarrow \mathcal{D}^i(\mathsf{X}^j)\Big|_{\mathsf{X}=\lambda} = i!\tbinom{j}{i}\lambda^{j-i},$$

συνάγεται (μέσω τού δυωνυμικού τύπου και των προϋποτεθέντων περιορισμών για την $\text{χαρ}(K)$) ότι

$$\mathsf{X}^j = ((\mathsf{X}-\lambda)+\lambda)^j = \sum_{i=0}^{j} \tbinom{j}{i}\lambda^{j-i}(\mathsf{X}-\lambda)^i = \sum_{i=0}^{j} (i!)^{-1}\, \mathcal{D}^i(\mathsf{X}^j)\Big|_{\mathsf{X}=\lambda}\, (\mathsf{X}-\lambda)^i.$$

Εάν $\varphi(\mathsf{X}) = \sum_{j=0}^{n} a_j\mathsf{X}^j$, τότε[6]

$$\begin{aligned}
&\sum_{i=0}^{n} (i!)^{-1}\, \mathcal{D}^i\Big(\sum_{j=0}^{n} a_j\mathsf{X}^j\Big)\Big|_{\mathsf{X}=\lambda} (\mathsf{X}-\lambda)^i = \sum_{i=0}^{n}\sum_{j=0}^{n} a_j\, (i!)^{-1}\, \mathcal{D}^i(\mathsf{X}^j)\big|_{\mathsf{X}=\lambda}\, (\mathsf{X}-\lambda)^i \\
&= \sum_{j=0}^{n} a_j \left(\sum_{i=0}^{n} (i!)^{-1}\, \mathcal{D}^i(\mathsf{X}^j)\big|_{\mathsf{X}=\lambda}\, (\mathsf{X}-\lambda)^i\right) = \sum_{j=0}^{n} a_j\mathsf{X}^j = \varphi(\mathsf{X})
\end{aligned}$$

(λόγω των (i) και (ii) τού λήμματος 10.2.16). □

10.2.20 Θεώρημα. *Εάν* $\varphi(\mathsf{X}) \in K[\mathsf{X}]\setminus\{0_{K[\mathsf{X}]}\}$, $\lambda \in K$, $m \in \mathbb{N}$, *και η χαρακτηριστική τού* K *είναι είτε* 0 *είτε* $> n := \deg(\varphi(\mathsf{X}))$*, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) $\text{mult}(\varphi(\mathsf{X});\lambda) = m$.

(ii) *Το* λ *είναι θέση μηδενισμού καθενός εκ των*

$$\varphi(\mathsf{X}), \mathcal{D}(\varphi(\mathsf{X})), \mathcal{D}^2(\varphi(\mathsf{X})), \dots, \mathcal{D}^{m-1}(\varphi(\mathsf{X})), \tag{10.14}$$

αλλά δεν είναι θέση μηδενισμού τού $\mathcal{D}^m(\varphi(\mathsf{X}))$.

Απόδειξη. (i)⇒(ii) Εάν $\text{mult}(\varphi(\mathsf{X});\lambda) = m$, τότε

$$\exists \psi(\mathsf{X}) \in K[\mathsf{X}]\setminus\{0_{K[\mathsf{X}]}\} : \varphi(\mathsf{X}) = (\mathsf{X}-\lambda)^m\, \psi(\mathsf{X}) \text{ με } \psi(\lambda) \neq 0_K.$$

(Βλ. 10.2.14 (i)⇒(ii).) Εφαρμόζοντας για οιονδήποτε $i \in \{0,\dots,m\}$ τον κανόνα (10.12) τού Leibniz λαμβάνουμε

$$\mathcal{D}^i(\varphi(\mathsf{X})) = \sum_{k=0}^{i} \tbinom{i}{k}\mathcal{D}^k((\mathsf{X}-\lambda)^m)\mathcal{D}^{i-k}(\psi(\mathsf{X})),$$

όπου $\mathcal{D}^k((\mathsf{X}-\lambda)^m) = k!\binom{m}{k}(\mathsf{X}-\lambda)^{m-k}$. Επομένως,

$$\begin{aligned}
\mathcal{D}^i(\varphi(\mathsf{X})) &= \underbrace{i!\tbinom{m}{i}(\mathsf{X}-\lambda)^{m-i}\,\psi(\mathsf{X})}_{\text{ο όρος για } k=i} + \sum_{k=0}^{i-1} \tbinom{i}{k} k!\tbinom{m}{k}(\mathsf{X}-\lambda)^{m-k}\,\mathcal{D}^{i-k}(\psi(\mathsf{X})) \\
&= i!\tbinom{m}{i}(\mathsf{X}-\lambda)^{m-i}\,\psi(\mathsf{X}) + (\mathsf{X}-\lambda)^{m-i+1}\,\theta_i(\mathsf{X}),
\end{aligned}$$

[5] Ο τύπος (10.13) πρόκειται για την επίτυπη εκδοχή μιας ειδικής περιπτώσεως τού τύπου τού Άγγλου μαθηματικού Brook Taylor (1685-1731) τού εισαχθέντος το 1715 για πραγματικές n φορές παραγωγίσιμες πραγματικές συναρτήσεις (που συναντούμε στον Απειροστικό Λογισμό). Όταν $\lambda = 0_K$, αυτός δίδει τον γνωστό τύπο τού (Σκωτσέζου μαθηματικού) Colin MacLaurin (1698-1746).

[6] Για την εικόνα $\mathfrak{y}_\lambda(\mathcal{D}^i(\varphi(\mathsf{X})))$ τής i-οστής επίτυπης παραγώγου ενός πολυωνύμου $\varphi(\mathsf{X})$ μέσω τής $\mathfrak{y}_\lambda$ ($\lambda \in K$) χρησιμοποιείται η συντομογραφία $\mathcal{D}^i(\varphi(\mathsf{X}))\big|_{\mathsf{X}=\lambda}$ για να αποφεύγεται σύγχυση. (Ο συμβολισμός $\mathcal{D}^i(\varphi(\lambda))$ θα μπορούσε να εκληφθεί ως η i-οστή επίτυπη παράγωγος τής *σταθεράς* $\mathfrak{y}_\lambda(\varphi(\mathsf{X})) = \varphi(\lambda)$, η οποία ισούται με 0_K όταν $i \geqslant 1$.)

όπου $\theta_i(\mathsf{X}) := \sum_{k=0}^{i-1} \binom{i}{k} k! \binom{m}{k} (\mathsf{X}-\lambda)^{(i-1)-k}\, \mathcal{D}^{i-k}(\psi(\mathsf{X}))$. Επειδή

$$\big(\mathcal{D}^i(\varphi(\mathsf{X}))\big)\big|_{\mathsf{X}=\lambda} = \begin{cases} 0_K, & \text{όταν } 0 \leqslant i \leqslant m-1, \\ m!\psi(\lambda), & \text{όταν } i = m, \end{cases}$$

με $m!\psi(\lambda) \neq 0_K$ (λόγω των υποθέσεών μας περί τής $\mathrm{χαρ}(K)$), ο ισχυρισμός είναι αληθής.

(ii)⇒(i) Εάν το λ είναι θέση μηδενισμού καθενός εκ των (10.14) αλλά δεν είναι θέση μηδενισμού τού $\mathcal{D}^m(\varphi(\mathsf{X}))$, τότε ο τύπος (10.13) τού Taylor γράφεται ως εξής:

$$\varphi(\mathsf{X}) = \sum_{i=m}^{n} (i!)^{-1}\, \mathcal{D}^i(\varphi(\mathsf{X}))\big|_{\mathsf{X}=\lambda} (\mathsf{X}-\lambda)^i = (\mathsf{X}-\lambda)^m \psi(\mathsf{X}),$$

όπου

$$\psi(\mathsf{X}) := \sum_{i=m}^{n} (i!)^{-1}\, \mathcal{D}^i(\varphi(\mathsf{X}))\Big|_{\mathsf{X}=\lambda} (\mathsf{X}-\lambda)^{i-m} \Rightarrow \psi(\lambda) = (m!)^{-1}\, \mathcal{D}^m(\varphi(\mathsf{X}))|_{\mathsf{X}=\lambda} \neq 0_K.$$

Αυτό σημαίνει ότι $\mathrm{mult}(\varphi(\mathsf{X}); \lambda) = m$ (βλ. 10.2.14 (ii)⇒(i)). □

10.2.21 Παραδείγματα. (i) Εάν $\varphi(\mathsf{X}) := \mathsf{X}^\nu - \nu\mathsf{X} + \nu - 1 \in \mathbb{C}[\mathsf{X}]$, όπου $\nu \in \mathbb{N}$, $\nu \geqslant 2$, τότε

$$\mathcal{D}^i(\varphi(\mathsf{X})) = \begin{cases} \nu\mathsf{X}^{\nu-1} - \nu, & \text{όταν } i = 1, \\ \nu(\nu-1)\mathsf{X}^{\nu-2}, & \text{όταν } i = 2, \\ i!\binom{\nu}{i}\mathsf{X}^{\nu-i}, & \text{όταν } 3 \leqslant i \leqslant \nu, \\ 0_{\mathbb{C}[\mathsf{X}]}, & \text{όταν } i > \nu. \end{cases}$$

Το 1 είναι διπλή θέση μηδενισμού τού $\varphi(\mathsf{X})$, διότι

$$\varphi(1) = \mathcal{D}(\varphi(\mathsf{X}))|_{\mathsf{X}=1} = 0,\ \ \mathcal{D}^2(\varphi(\mathsf{X}))\big|_{\mathsf{X}=1} = \nu(\nu-1) \neq 0.$$

Επιπροσθέτως, οιαδήποτε θέση μηδενισμού $\lambda \in \mathbb{C}\smallsetminus\{1\}$ τού $\varphi(\mathsf{X})$ είναι απλή, διότι εάν ίσχυε

$$\mathcal{D}(\varphi(\mathsf{X}))|_{\mathsf{X}=\lambda} = \nu(\lambda^{\nu-1} - 1) = 0 \Rightarrow \lambda^{\nu-1} = 1,$$

τότε θα καταλήγαμε σε άτοπο, αφού

$$\left.\begin{aligned} \varphi(\lambda) = 0 \Rightarrow \lambda(\lambda^{\nu-1} - \nu) = 1 - \nu \\ \lambda^{\nu-1} = 1 \end{aligned}\right\} \underset{\nu\neq 1}{\Longrightarrow} \lambda = 1.$$

(ii) Θεωρούμε το

$$\varphi(\mathsf{X}) := \mathsf{X}^\nu - a \in K[\mathsf{X}],$$

όπου $\nu \in \mathbb{N}$ και $a \in K\smallsetminus\{0_K\}$. Εάν είτε $\mathrm{χαρ}(K) = 0$ είτε $\mathrm{χαρ}(K) \nmid \nu$ και το λ είναι ένα στοιχείο μιας επεκτάσεως K' τού K, εντός τής οποίας ισχύει $\lambda^\nu = a$, τότε

$$\mathcal{D}(\varphi(\mathsf{X}))|_{\mathsf{X}=\lambda} = \nu\lambda^{\nu-1} \neq 0_{K'}.$$

Αυτό σημαίνει ότι το $\varphi(\mathsf{X})$, ιδωμένο ως στοιχείο τού $L[\mathsf{X}]$, όπου L *τυχούσα επέκταση* τού K, δεν διαθέτει καμία πολλαπλή θέση μηδενισμού. Αντιθέτως, εάν $\mathrm{χαρ}(K) = p$ (p πρώτος), τότε $\mathcal{D}(\varphi(\mathsf{X})) = p\mathsf{X}^{p-1} = 0_{K[\mathsf{X}]}$. Εν τοιαύτη περιπτώσει, κάθε θέση μηδενισμού λ τού $\varphi(\mathsf{X})$ έχει πολλαπλότητα $\mathrm{mult}(\varphi(\mathsf{X}); \lambda) = p$, διότι

$$\varphi(\mathsf{X}) = \mathsf{X}^p - a = \mathsf{X}^p - \lambda^p = (\mathsf{X}-\lambda)^p.$$

10.3 ΑΝΑΓΩΓΑ ΠΟΛΥΩΝΥΜΑ

Όπως οι ακέραιοι αριθμοί έχουν τους πρώτους αριθμούς ως «δομικούς τους λίθους», έτσι και τα πολυώνυμα τα ανήκοντα στον $K[\mathsf{X}]$ (όπου K τυχόν σώμα) αποσυντίθενται σε γινόμενα «αναγώγων» πολυωνύμων.

10.3.1 Ορισμός. Έστω K ένα σώμα. Ένα πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ θετικού βαθμού καλείται **ανάγωγο πολυώνυμο υπεράνω τού** K (ή **ανάγωγο πολυώνυμο εντός τού** $K[\mathsf{X}]$) όταν δεν υπάρχουν πολυώνυμα $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει η ισότητα

$$\varphi(\mathsf{X}) = \varphi_1(\mathsf{X})\varphi_2(\mathsf{X}) \tag{10.15}$$

με $1 \leqslant \deg(\varphi_1(\mathsf{X})) < \deg(\varphi(\mathsf{X}))$ και $1 \leqslant \deg(\varphi_2(\mathsf{X})) < \deg(\varphi(\mathsf{X}))$ (ή, ισοδυνάμως, όταν μια παράσταση (10.15) τού $\varphi(\mathsf{X})$ υφίσταται μόνον υπό την προϋπόθεση ότι ακριβώς ένα εκ των $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})$ είναι σταθερό, μη μηδενικό πολυώνυμο).

10.3.2 Παρατήρηση. Η αναφορά τού σώματος υπεράνω τού οποίου ένα δοθέν πολυώνυμο είναι (ή δεν είναι) ανάγωγο είναι απαραίτητη. Επί παραδείγματι, το $\mathsf{X}^2 + 1$ είναι ανάγωγο υπεράνω τού $\mathbb{R}$ άλλά δεν είναι ανάγωγο υπεράνω τού $\mathbb{C}$, διότι $\mathsf{X}^2 + 1 = (\mathsf{X} + i)(\mathsf{X} - i)$, όπου i η φανταστική μονάδα.

10.3.3 Σημείωση. (i) Έστω K τυχόν σώμα. Κάθε πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ βαθμού 1 είναι -προφανώς- ανάγωγο. Ο έλεγχος τού κατά πόσον ένα πολυώνυμο βαθμού $\geqslant 2$ είναι ανάγωγο δεν είναι εν γένει κάτι το τετριμμένο. Τα ανάγωγα πολυώνυμα υπεράνω τού $\mathbb{R}$ μπορούν να χαρακτηρισθούν πλήρως (βλ. πρόταση 10.5.3). Όπως θα δούμε στην επομένη ενότητα (βλ. εδ. 10.4.16 (iii), 10.4.17 και 10.4.19), τα ανάγωγα πολυώνυμα υπεράνω τού $\mathbb{C}$ είναι μόνον τα πρωτοβάθμια. Ωστόσο, ακόμη και υπεράνω τού $\mathbb{Q}[\mathsf{X}]$ ένας *γενικός* χαρακτηρισμός των αναγώγων πολυωνύμων φαντάζει εξαιρετικά δύσκολος.

(ii) Κατά το 10.2.4 (ii) δεν υπάρχει κανένα ανάγωγο πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ βαθμού $\geqslant 2$ που να έχει θέσεις μηδενισμού εντός τού K. Το αντίστροφο δεν είναι εν γένει αληθές. Επί παραδείγματι, το πολυώνυμο $(\mathsf{X}^2 + 3)^2 \in \mathbb{R}[\mathsf{X}]$ δεν έχει καμία θέση μηδενισμού εντός τού $\mathbb{R}$, αλλ' εντούτοις δεν είναι ανάγωγο υπεράνω αυτού. Μολαταύτα, υπό ορισμένες ειδικές προϋποθέσεις ισχύει ενίοτε και το αντίστροφο.

10.3.4 Πρόταση. *Έστω $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ με $\deg(\varphi(\mathsf{X})) \in \{2, 3\}$. Εάν το $\varphi(\mathsf{X})$ δεν διαθέτει θέσεις μηδενισμού εντός τού K, τότε είναι ανάγωγο υπεράνω τού K.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι το $\varphi(\mathsf{X})$ δεν είναι ανάγωγο υπεράνω τού K. Τότε το $\varphi(\mathsf{X})$ γράφεται ως γινόμενο δύο μη σταθερών πολυωνύμων

$$\varphi(\mathsf{X}) = \varphi_1(\mathsf{X})\varphi_2(\mathsf{X})$$

με $\deg(\varphi_1(\mathsf{X})) < \deg(\varphi(\mathsf{X}))$ και $\deg(\varphi_2(\mathsf{X})) < \deg(\varphi(\mathsf{X}))$. Επειδή

$$\deg(\varphi(\mathsf{X})) = \deg(\varphi_1(\mathsf{X})) + \deg(\varphi_2(\mathsf{X})) \in \{2, 3\},$$

τουλάχιστον ένα εκ των $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})$ οφείλει να έχει βαθμό ίσον με το 1. Αλλά κάθε πολυώνυμο τού $K[\mathsf{X}]$ με βαθμό ίσον με το 1 είναι τής μορφής $a\mathsf{X} + b$, όπου $a \neq 0$, και έχει ως θέση μηδενισμού του το $-a^{-1}b \in K$. Άτοπο! □

10.3.5 Πρόταση. *Έστω $\varphi(\mathsf{X}) \in K[\mathsf{X}]$. Εάν $\deg(\varphi(\mathsf{X})) \geqslant 1$, τότε υφίσταται τουλάχιστον ένα ανάγωγο πολυώνυμο υπεράνω τού K το οποίο είναι διαιρέτης τού $\varphi(\mathsf{X})$.*

Απόδειξη. Έστω $\mathcal{A} := \{\alpha(\mathsf{X}) \in K[\mathsf{X}] : \deg(\alpha(\mathsf{X})) \geqslant 1 \text{ και } \alpha(\mathsf{X}) \mid \varphi(\mathsf{X})\}$. Το σύνολο $\mathcal{A}$ είναι μη κενό διότι $\varphi(\mathsf{X}) \in \mathcal{A}$. Θέτουμε $n_0 := \min\{\deg(\alpha(\mathsf{X}))| \alpha(\mathsf{X}) \in \mathcal{A}\}$ και θεωρούμε τυχόν στοιχείο $\psi(\mathsf{X}) \in \mathcal{A}$ βαθμού $\deg(\psi(\mathsf{X})) = n_0$. Τότε το $\psi(\mathsf{X})$ είναι ένα ανάγωγο πολυώνυμο υπεράνω τού K το οποίο διαιρεί το $\varphi(\mathsf{X})$. Πράγματι· $n_0 \geqslant 1$ και εάν υποθέσουμε ότι υπάρχουν πολυώνυμα $\psi_1(\mathsf{X}), \psi_2(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει η ισότητα

$$\psi(\mathsf{X}) = \psi_1(\mathsf{X})\psi_2(\mathsf{X})$$

με $1 \leqslant \deg(\psi_1(\mathsf{X})) < \deg(\psi(\mathsf{X}))$ και $1 \leqslant \deg(\psi_2(\mathsf{X})) < \deg(\psi(\mathsf{X}))$, τότε καταλήγουμε σε άτοπο, καθόσον για $i = 1, 2$ έχουμε

$$\left.\begin{matrix}\psi_i(\mathsf{X}) \mid \psi(\mathsf{X}) \\ \psi(\mathsf{X}) \mid \varphi(\mathsf{X})\end{matrix}\right\} \Longrightarrow \left.\begin{matrix}\psi_i(\mathsf{X}) \mid \varphi(\mathsf{X}) \\ \deg(\psi_i(\mathsf{X})) \geqslant 1\end{matrix}\right\} \Rightarrow \psi_i(\mathsf{X}) \in \mathcal{A}$$

με $1 \leqslant \deg(\psi_i(\mathsf{X})) < \deg(\psi_1(\mathsf{X})) + \deg(\psi_2(\mathsf{X})) = \deg(\psi(\mathsf{X})) = n_0$ (κάτι το οποίο αντίκειται στον ορισμό τού $\psi(\mathsf{X})$). □

10.3.6 Λήμμα. *Εάν $\theta(\mathsf{X}) \in K[\mathsf{X}]$, τότε για κάθε πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ που είναι ανάγωγο υπεράνω τού K ισχύει είτε $\varphi(\mathsf{X}) \mid \theta(\mathsf{X})$ είτε* μκδ$(\varphi(\mathsf{X}), \theta(\mathsf{X})) = 1_K$.

Απόδειξη. Σύμφωνα με το θεώρημα 10.1.1, υπάρχει ζεύγος μονοσημάντως ορισμένων πολυωνύμων $\varpi(\mathsf{X}), \upsilon(\mathsf{X}) \in K[\mathsf{X}]$, ούτως ώστε να ισχύει

$$\theta(\mathsf{X}) = \varpi(\mathsf{X})\varphi(\mathsf{X}) + \upsilon(\mathsf{X}), \quad \deg(\upsilon(\mathsf{X})) < \deg(\varphi(\mathsf{X})).$$

Εάν $\upsilon(\mathsf{X}) = 0_{K[\mathsf{X}]}$, τότε $\varphi(\mathsf{X}) \mid \theta(\mathsf{X})$. Εάν $\upsilon(\mathsf{X}) \neq 0_{K[\mathsf{X}]}$, τότε $\varphi(\mathsf{X}) \nmid \theta(\mathsf{X})$ και

$$\text{μκδ}(\varphi(\mathsf{X}), \theta(\mathsf{X})) = \text{μκδ}(\varphi(\mathsf{X}), \upsilon(\mathsf{X})).$$

Θέτοντας $\delta(\mathsf{X}) := \text{μκδ}(\varphi(\mathsf{X}), \upsilon(\mathsf{X}))$ παρατηρούμε ότι

$$\delta(\mathsf{X}) \mid \varphi(\mathsf{X}) \Rightarrow \exists \alpha(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\} : \varphi(\mathsf{X}) = \alpha(\mathsf{X})\delta(\mathsf{X}) \tag{10.16}$$

και

$$\delta(\mathsf{X}) \mid \upsilon(\mathsf{X}) \underset{\text{10.1.3 (iv)}}{\Longrightarrow} 0 \leqslant \deg(\delta(\mathsf{X})) \leqslant \deg(\upsilon(\mathsf{X})) < \deg(\varphi(\mathsf{X})). \tag{10.17}$$

Επειδή το $\varphi(\mathsf{X})$ είναι εξ υποθέσεως ανάγωγο υπεράνω τού K, από την (10.16) και το (ii) τής προτάσεως 6.3.7 συνάγουμε ότι (ακριβώς) ένα εκ των $\alpha(\mathsf{X}), \delta(\mathsf{X})$ είναι σταθερό μη μηδενικό (ήτοι βαθμού 0) και

$$\deg(\alpha(\mathsf{X})) + \deg(\delta(\mathsf{X})) = \deg(\varphi(\mathsf{X})) > 0.$$

Αυτό σημαίνει ότι *είτε* ισχύει $\deg(\alpha(\mathsf{X})) = 0$ και $\deg(\delta(\mathsf{X})) = \deg(\varphi(\mathsf{X}))$ *είτε* $\deg(\delta(\mathsf{X})) = 0$ και $\deg(\alpha(\mathsf{X})) = \deg(\varphi(\mathsf{X}))$. Το πρώτο ενδεχόμενο αποκλείεται λόγω τής (10.17). Επομένως, $\deg(\delta(\mathsf{X})) = 0$ (διότι $\delta(\mathsf{X}) \neq 0_{K[\mathsf{X}]}$) και $\delta(\mathsf{X}) = 1_K$ (διότι ο μέγιστος κοινός διαιρέτης $\delta(\mathsf{X})$ είναι εξ ορισμού *μονικό* πολυώνυμο). □

10.3.7 Λήμμα. *Εάν τα $\varphi(\mathsf{X}), \theta_1(\mathsf{X}), \ldots, \theta_n(\mathsf{X}) \in K[\mathsf{X}]$ ($n \in \mathbb{N}$) είναι ανάγωγα πολυώνυμα υπεράνω τού K, τότε ισχύει η συνεπαγωγή*

$$\varphi(\mathsf{X}) \mid \prod_{j=1}^{n} \theta_j(\mathsf{X}) \Longrightarrow \exists j_0 \in \{1, \ldots, n\} : \varphi(\mathsf{X}) = c\,\theta_{j_0}(\mathsf{X}),$$

για κάποια σταθερά $c \in K \setminus \{0_K\}$.

Απόδειξη. Υποθέτουμε ότι $\varphi(\mathsf{X}) \mid \prod_{j=1}^{n} \theta_j(\mathsf{X})$. Κατ' αρχάς θα αποδείξουμε ότι

$$\exists j_0 \in \{1, \ldots, n\} : \varphi(\mathsf{X}) \mid \theta_{j_0}(\mathsf{X}). \tag{10.18}$$

Εάν $\varphi(\mathsf{X}) \mid \theta_1(\mathsf{X})$, τότε η (10.18) είναι προφανής (με $j_0 = 1$). Εάν $\varphi(\mathsf{X}) \nmid \theta_1(\mathsf{X})$, τότε (σύμφωνα με το λήμμα 10.3.6 και το πόρισμα 10.1.16)

$$\left.\begin{array}{r} \text{μκδ}(\varphi(\mathsf{X}), \theta_1(\mathsf{X})) = 1_K \\ \varphi(\mathsf{X}) \mid \theta_1(\mathsf{X}) \left(\prod_{j=2}^{n} \theta_j(\mathsf{X})\right) \end{array}\right\} \Rightarrow \varphi(\mathsf{X}) \mid \prod_{j=2}^{n} \theta_j(\mathsf{X}).$$

Εάν $\varphi(\mathsf{X}) \mid \theta_2(\mathsf{X})$, τότε η (10.18) ισχύει (με $j_0 = 2$). Εάν $\varphi(\mathsf{X}) \nmid \theta_2(\mathsf{X})$, τότε ομοίως

$$\left.\begin{array}{r} \text{μκδ}(\varphi(\mathsf{X}), \theta_2(\mathsf{X})) = 1_K \\ \varphi(\mathsf{X}) \mid \theta_2(\mathsf{X}) \left(\prod_{j=3}^{n} \theta_j(\mathsf{X})\right) \end{array}\right\} \Rightarrow \varphi(\mathsf{X}) \mid \prod_{j=3}^{n} \theta_j(\mathsf{X}).$$

Επαναλαμβάνοντας (εν ανάγκη) την ίδια διαδικασία (το πολύ $n-2$ ακόμη φορές) εντοπίζουμε τελικώς (με την ίδια συλλογιστική) έναν $j_0 \leqslant n$ για τον οποίο η (10.18) είναι αληθής. Επειδή αμφότερα τα $\varphi(\mathsf{X})$ και $\theta_{j_0}(\mathsf{X})$ είναι ανάγωγα υπεράνω τού K, έχουμε κατ' ανάγκην ότι $\varphi(\mathsf{X}) = c\,\theta_{j_0}(\mathsf{X})$, για κάποια σταθερά $c \in K \smallsetminus \{0_K\}$. □

10.3.8 Θεώρημα. *Κάθε πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ βαθμού $\geqslant 1$ γράφεται ως γινόμενο*

$$\boxed{\varphi(\mathsf{X}) = c \prod_{\nu=1}^{r} \theta_\nu(\mathsf{X})} \tag{10.19}$$

αναγώγων (υπεράνω τού K) μονικών πολυωνύμων $\theta_1(\mathsf{X}), \ldots, \theta_r(\mathsf{X}) \in K[\mathsf{X}]$ (όπου $r \in \mathbb{N}$) και μιας σταθεράς $c \in K \smallsetminus \{0_K\}$. Η παράσταση αυτή είναι μονοσημάντως ορισμένη υπό την ακόλουθη έννοια: Εάν

$$\varphi(\mathsf{X}) = c \prod_{\nu=1}^{r} \theta_\nu(\mathsf{X}) = c' \prod_{j=1}^{l} \theta'_j(\mathsf{X}), \tag{10.20}$$

όπου $c' \in K \smallsetminus \{0_K\}$ και $\theta'_1(\mathsf{X}), \ldots, \theta'_l(\mathsf{X}) \in K[\mathsf{X}]$ ($l \in \mathbb{N}$) ανάγωγα (υπεράνω τού K) μονικά πολυώνυμα, τότε $c = c'$, $r = l$ και υπάρχει μια μετάταξη $\sigma \in \mathfrak{S}_r$, ούτως ώστε να ισχύει

$$\theta_\nu(\mathsf{X}) = \theta'_{\sigma(\nu)}(\mathsf{X}), \ \forall \nu \in \{1, \ldots, r\}. \tag{10.21}$$

Απόδειξη. Μέσω μαθηματικής επαγωγής ως προς τον $n := \deg(\varphi(\mathsf{X}))$.

▸ *Ύπαρξη τής παραστάσεως* (10.19). Εάν $n = 1$, τότε ο ισχυρισμός είναι αληθής, καθόσον τα πρωτοβάθμια πολυώνυμα είναι ανάγωγα. Ας υποθέσουμε ότι $n \geqslant 2$ και ότι αυτός είναι αληθής και για όλα τα μη σταθερά πολυώνυμα βαθμού $< n$. Εάν το $\varphi(\mathsf{X})$ *είναι* ανάγωγο, τότε (εξ ορισμού) $\varphi(\mathsf{X}) = c\,\hat{\varphi}(\mathsf{X})$, όπου το $\hat{\varphi}(\mathsf{X}) \in K[\mathsf{X}]$ είναι μονικό και ανάγωγο υπεράνω τού K, και c ο επικεφαλής συντελεστής τού $\varphi(\mathsf{X})$. Εάν το $\varphi(\mathsf{X})$ *δεν είναι* ανάγωγο, τότε γράφεται ως γινόμενο $\varphi(\mathsf{X}) = \varphi_1(\mathsf{X})\varphi_2(\mathsf{X})$ δύο μη σταθερών πολυωνύμων $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})$ με βαθμούς $\deg(\varphi_1(\mathsf{X})) < \deg(\varphi(\mathsf{X}))$ και $\deg(\varphi_2(\mathsf{X})) < \deg(\varphi(\mathsf{X}))$. Σύμφωνα με την επαγωγική μας υπόθεση, υπάρχουν φυσικοί αριθμοί r_1, r_2, σταθερές $c_1, c_2 \in K \smallsetminus \{0_K\}$ και πολυώνυμα $\theta_1^{[1]}(\mathsf{X}), \ldots, \theta_{r_1}^{[1]}(\mathsf{X}) \in K[\mathsf{X}]$ και $\theta_1^{[2]}(\mathsf{X}), \ldots, \theta_{r_2}^{[2]}(\mathsf{X}) \in K[\mathsf{X}]$, ούτως ώστε να ισχύει

$$\varphi_1(\mathsf{X}) = c_1 \prod_{\nu=1}^{r_1} \theta_\nu^{[1]}(\mathsf{X}), \quad \varphi_2(\mathsf{X}) = c_2 \prod_{j=1}^{r_2} \theta_j^{[2]}(\mathsf{X}).$$

Κατά συνέπειαν, και σε αυτήν την περίπτωση το $\varphi(\mathsf{X})$ διαθέτει μια παράσταση τής μορφής (10.19), καθότι

$$\varphi(\mathsf{X}) = \underbrace{c_1 c_2}_{\in K\smallsetminus\{0_K\}} \left(\prod_{\nu=1}^{r_1} \theta_\nu^{[1]}(\mathsf{X})\right)\left(\prod_{j=1}^{r_2} \theta_j^{[2]}(\mathsf{X})\right).$$

▸ *Περί τού μονοσημάντου τής παραστάσεως* (10.19). Εκκινούμε από δυο τυχούσες (τέτοιου είδους) παραστάσεις (10.20) τού $\varphi(\mathsf{X})$. Εάν $n = 1$, τότε ο ισχυρισμός είναι προδήλως αληθής. Ας υποθέσουμε ότι $n \geqslant 2$ και ότι αυτός είναι αληθής και για όλα τα μη σταθερά πολυώνυμα βαθμού $< n$. Η ισότητα $c = c'$ έπεται άμεσα ύστερα από σύγκριση των επικεφαλής συντελεστών. Επειδή

$$\theta_r(\mathsf{X}) \mid \prod_{\nu=1}^{r} \theta_\nu(\mathsf{X}) = \prod_{j=1}^{l} \theta'_j(\mathsf{X}),$$

υπάρχει κάποιος δείκτης $j_0 \in \{1, \ldots, l\}$, τέτοιος ώστε να ισχύει $\theta_r(\mathsf{X}) = a\,\theta'_{j_0}(\mathsf{X})$, για κάποια σταθερά $a \in K\smallsetminus\{0_K\}$ (βλ. λήμμα 10.3.7). Εν προκειμένω, αυτή η σταθερά a οφείλει να ισούται με 1_K (διότι αμφότερα τα $\theta_r(\mathsf{X})$ και $\theta'_{j_0}(\mathsf{X})$ είναι εξ υποθέσεως μονικά), οπότε $\theta_r(\mathsf{X}) = \theta'_{j_0}(\mathsf{X})$.

Περίπτωση πρώτη. Έχουμε $l = 1 \Leftrightarrow r = 1$ (διότι αλλιώς στο ένα μέλος τής ανωτέρω ισότητας θα είχαμε ένα μη ανάγωγο πολυώνυμο και στο άλλο ένα ανάγωγο πολυώνυμο). Άρα ο ισχυρισμός είναι προδήλως αληθής όταν $l = 1$.

Περίπτωση δεύτερη. Υποθέτουμε ότι $l \geqslant 2$. (Βάσει των προαναφερθέντων έχουμε $r \geqslant 2$.) Έστω $\tau\,(= \tau^{(j_0,l)}) \in \mathfrak{S}_l$ η αντιμετάθεση με τύπους ορισμού της τους

$$\tau\,(j) := j,\ \forall j \in \{1, \ldots, l\}\smallsetminus\{j_0, l\},\ \text{και}\ \tau\,(j_0) := l,\ \tau\,(l) := j_0.$$

Από την ισότητα $\theta_r(\mathsf{X}) = \theta'_{\tau(l)}(\mathsf{X})$ έπεται ότι

$$\prod_{\nu=1}^{r} \theta_\nu(\mathsf{X}) = \prod_{j=1}^{l} \theta'_{\tau(j)}(\mathsf{X}) \Rightarrow \prod_{\nu=1}^{r-1} \theta_\nu(\mathsf{X}) = \prod_{j=1}^{l-1} \theta'_{\tau(j)}(\mathsf{X}).$$

Επειδή $\deg\left(\prod_{\nu=1}^{r-1} \theta_\nu(\mathsf{X})\right) < n$, από την επαγωγική μας υπόθεση συνάγεται ότι $r - 1 = l - 1 \Rightarrow r = l$ και ότι υπάρχει μια μετάταξη $\rho \in \mathfrak{S}_{r-1}$, ούτως ώστε να ισχύει

$$\theta_\nu(\mathsf{X}) = \theta'_{\rho(\tau(\nu))}(\mathsf{X}),\ \forall \nu \in \{1, \ldots, r-1\}.$$

Θεωρώντας τή μετάταξη $\sigma \in \mathfrak{S}_r$ με τύπους ορισμού της τους $\sigma(\nu) := \rho(\tau\,(\nu))$, $\forall \nu \in \{1, \ldots, r-1\}$, και $\sigma(r) := \tau\,(r) = j_0$, καταλήγουμε στις ισότητες (10.21). □

10.3.9 Σημείωση. (i) Η (μέχρις αναδιατάξεως των παραγόντων) μονοσημάντως ορισμένη παράσταση (10.19) καλείται **παράσταση τού** $\varphi(\mathsf{X})$ **ως γινομένου αναγώγων μονικών πολυωνύμων** ή **αποσύνθεση τού** $\varphi(\mathsf{X})$ **σε γινόμενο αναγώγων μονικών πολυωνύμων**[7].

(ii) Εάν στην παράσταση (10.19) τυγχάνει να ισχύει

$$\theta_1(\mathsf{X}) = \theta_2(\mathsf{X}) = \cdots = \theta_r(\mathsf{X}) =: \psi(\mathsf{X}),$$

τότε $\varphi(\mathsf{X}) = c\,\psi(\mathsf{X})^r$. Ειδάλλως, για να συμπτύξουμε στην (10.19) όσα εκ των $\theta_1(\mathsf{X}), \theta_2(\mathsf{X}), \ldots, \theta_r(\mathsf{X})$ είναι πολλαπλώς εμφανιζόμενα (με την εισαγωγή δυνάμεων) μπορούμε (πιθανώς ύστερα από μια αναδιάταξη δεικτών) να υποθέσουμε ότι

$$\theta_1(\mathsf{X}) = \cdots = \theta_{j_1}(\mathsf{X}), \theta_{j_1+1}(\mathsf{X}) = \cdots = \theta_{j_2}(\mathsf{X}), \cdots\cdots, \theta_{j_{k-1}+1}(\mathsf{X}) = \cdots = \theta_{j_k}(\mathsf{X})$$

[7] Εν προκειμένω, για λόγους συντομίας, *υπονοείται σιωπηρώς* ότι στην εν λόγω αποσύνθεση συμπεριλαμβάνεται (προτασσόμενος σε αυτήν) ο επικεφαλής συντελεστής c τού $\varphi(\mathsf{X})$. (Παρότι ο ίδιος, ως πολυώνυμο βαθμού 0, *δεν είναι* ανάγωγο πολυώνυμο, το γινόμενο αυτού με οιοδήποτε εκ των $\theta_1(\mathsf{X}), \ldots, \theta_n(\mathsf{X})$ *είναι* ανάγωγο αλλά *δεν είναι* μονικό για $c \neq 1_K$. Γι' αυτόν τον λόγο ορισμένοι συγγραφείς αποφεύγουν να χρησιμοποιούν το επίθετο *μονικός* στη σχετική ορολογία, έστω κι αν δι' αυτού τού τρόπου αποδυναμώνουν εν μέρει το τι ακριβώς δίδει το θεώρημα 10.3.8!)

για κατάλληλα $\{j_1, j_2, \dots, j_k\} \subseteq \{1, \dots, r\},\ 2 \leqslant k \leqslant r$, με

$$1 \leqslant j_1 < j_2 < \cdots < j_{k-1} < j_k = r$$

και $\theta_{j_i}(\mathsf{X}) \neq \theta_{j_{i'}}(\mathsf{X})$ για οιουσδήποτε $i, i' \in \{1, \dots, k\}$, $i \neq i'$. Θέτοντας

$$m_1 := j_1,\ m_2 := j_2 - j_1,\ \dots,\ m_k := j_k - j_{k-1}, \quad \psi_i(\mathsf{X}) := \theta_{j_i}(\mathsf{X}),\ \forall i \in \{1, \dots, k\},$$

το $\varphi(\mathsf{X})$ γράφεται ως

$$\boxed{\varphi(\mathsf{X}) = c \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i}} \tag{10.22}$$

Η παράσταση (10.22) καλείται **συνεπτυγμένη αποσύνθεση τού** $\varphi(\mathsf{X})$ (σε γινόμενο αναγώγων μονικών πολυωνύμων) και είναι (σε πολλές περιπτώσεις) πιο εύχρηστη από την (10.19). Μάλιστα, έχουμε και τη δυνατότητα να την *γενικεύσουμε ελαφρώς*, ούτως ώστε, συν τοις άλλοις, να μπορούμε να συμπεριλαμβάνουμε σε αυτήν ακόμη και τα σταθερά πολυώνυμα. Προς τούτο αρκεί να επιτρέπουμε σε κάποιους (ή και σε όλους) τους εκθέτες $m_1, \dots, m_k$ να λαμβάνουν *και* την τιμή 0.

(iii) Ενίοτε, όταν εργαζόμαστε με δύο (ή περισσότερα) πολυώνυμα, είναι αρκούντως διευκολυντικό το να υιοθετούμε την εξής *σύμβαση*: Γράφουμε (λαμβάνοντας υπ' όψιν τα προαναφερθέντα στο (ii)) τις (υπό την ευρεία έννοια) συνεπτυγμένες αποσυνθέσεις τους κατά τέτοιον τρόπο, ώστε τα σε αυτές εμφανιζόμενα ανάγωγα μονικά πολυώνυμα να είναι τα *ίδια*. (Τούτο επιτυγχάνεται με την συμπερίληψη *όλων* των αναγώγων μονικών παραγόντων που εμφανίζονται σε *όλα* τα θεωρούμενα πολυώνυμα στις εν λόγω *υπό την ευρεία έννοια* συνεπτυγμένες αποσυνθέσεις, καθόσον είναι δυνατόν να προσθέτουμε παράγοντες υψούμενους στο 0 κατά το δοκούν.) Επί παραδείγματι, *οιαδήποτε* $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X}) \in K[\mathsf{X}]$ μπορούν να γραφούν υπό τη μορφή

$$\varphi_1(\mathsf{X}) = c_1 \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[1]}},\ \varphi_2(\mathsf{X}) = c_2 \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[2]}}$$

όπου $c_1, c_2 \in K, \psi_1(\mathsf{X}), \dots, \psi_k(\mathsf{X})$ ανάγωγα και μονικά και $m_i^{[1]}, m_i^{[2]} \in \mathbb{N}_0$ κατάλληλοι εκθέτες για κάθε $i \in \{1, \dots, k\}$. Σημειωτέον ότι

$$\varphi_1(\mathsf{X}) = \varphi_2(\mathsf{X}) \Leftrightarrow [c_1 = c_2 \text{ και } m_i^{[1]} = m_i^{[2]}, \forall i \in \{1, \dots, k\}].$$

10.3.10 Πόρισμα. *Έστω $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ τυχόν πολυώνυμο και έστω (10.22) η συνεπτυγμένη αποσύνθεση αυτού (υπό την ευρεία έννοια,* βλ. 10.3.9 (iii)). *Εάν $\alpha(\mathsf{X}) \in K[\mathsf{X}]$, τότε ισχύει η αμφίπλευρη συνεπαγωγή*

$$\alpha(\mathsf{X}) \mid \varphi(\mathsf{X}) \Longleftrightarrow \left[\begin{array}{c} \alpha(\mathsf{X}) = a \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i'}, \\ \text{για κάποιους } m_1', \dots, m_k' \in \mathbb{N}_0 : m_i' \leqslant m_i, \\ \forall i \in \{1, .., k\}, \text{ και κάποιο } a \in K : a \mid c \end{array}\right]$$

Απόδειξη. Η συνεπαγωγή "$\Leftarrow$" είναι προφανής. Θα αποδείξουμε την "$\Rightarrow$". Υποθέτουμε ότι $\alpha(\mathsf{X}) \mid \varphi(\mathsf{X})$. Τότε υπάρχει κάποιο $\beta(\mathsf{X}) \in K[\mathsf{X}]$, τέτοιο ώστε να ισχύει $\varphi(\mathsf{X}) = \alpha(\mathsf{X})\beta(\mathsf{X})$. Εάν

$$\alpha(\mathsf{X}) = a \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i'},\ \beta(\mathsf{X}) = b \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i''},\ a, b \in K,$$

είναι οι (υπό την ευρεία έννοια) συνεπτυγμένες αποσυνθέσεις των $\alpha(\mathsf{X})$ και $\beta(\mathsf{X})$ (νοούμενες όπως στο εδ. 10.3.9 (iii)), τότε

$$\varphi(\mathsf{X}) = ab \left(\prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i'}\right) \left(\prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i''}\right) = ab \left(\prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i'+m_i''}\right),$$

οπότε $c = ab$ και $m_i = m_i' + m_i'' \geqslant m_i'$ για κάθε $i \in \{1, \ldots, k\}$. □

10.3.11 Πόρισμα. *Εάν τα* $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]$ *είναι ανάγωγα υπεράνω τού* K *και μονικά, και* $\varphi(\mathsf{X}) \mid \psi(\mathsf{X})^m$ *για κάποιον* $m \in \mathbb{N}$, *τότε* $\varphi(\mathsf{X}) = \psi(\mathsf{X})^{m'}$ *για κάποιον* $m' \in \mathbb{N}$, *όπου* $m' \leqslant m$.

Αποδειξη. Έπεται άμεσα από το πόρισμα 10.3.10. □

10.3.12 Πόρισμα. *Εάν τα* $\varphi(\mathsf{X}), \theta(\mathsf{X}) \in K[\mathsf{X}]$ *είναι ανάγωγα υπεράνω τού* K *και μονικά, και* $\varphi(\mathsf{X}) \neq \theta(\mathsf{X})$, *τότε*

$$\text{μκδ}(\varphi(\mathsf{X})^m, \theta(\mathsf{X})^n) = 1_K, \ \forall (m, n) \in \mathbb{N} \times \mathbb{N}.$$

Αποδειξη. Ας υποθέσουμε ότι το $\delta(\mathsf{X}) := \text{μκδ}(\varphi(\mathsf{X})^m, \theta(\mathsf{X})^n)$ έχει βαθμό $\geqslant 1$. Σύμφωνα με την πρόταση 10.3.5 υφίσταται τουλάχιστον ένα ανάγωγο πολυώνυμο $\psi(\mathsf{X})$ υπεράνω τού K το οποίο διαιρεί το $\delta(\mathsf{X})$. Αυτό εκφράζεται ως γινόμενο $\psi(\mathsf{X}) = c\hat{\psi}(\mathsf{X})$ μιας σταθεράς $c \in K \smallsetminus \{0_K\}$ (που ισούται με τον επικεφαλής συντελεστή του) και ενός αναγώγου (υπεράνω τού K) *μονικού* πολυωνύμου $\hat{\psi}(\mathsf{X})$. Προφανώς,

$$\left.\begin{array}{l} \hat{\psi}(\mathsf{X}) \mid \psi(\mathsf{X}) \\ \psi(\mathsf{X}) \mid \delta(\mathsf{X}) \end{array}\right\} \Longrightarrow \hat{\psi}(\mathsf{X}) \mid \delta(\mathsf{X})$$

και, ως εκ τούτου,

$$\left.\begin{array}{l} \delta(\mathsf{X}) \mid \varphi(\mathsf{X}) \\ \delta(\mathsf{X}) \mid \theta(\mathsf{X}) \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \hat{\psi}(\mathsf{X}) \mid \varphi(\mathsf{X}) \\ \hat{\psi}(\mathsf{X}) \mid \theta(\mathsf{X}) \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \hat{\psi}(\mathsf{X}) \mid \varphi(\mathsf{X})^m \\ \hat{\psi}(\mathsf{X}) \mid \theta(\mathsf{X})^n \end{array}\right\}.$$

Επειδή $\deg(\hat{\psi}(\mathsf{X})) \geqslant 1$, το πόρισμα 10.3.11 μας πληροφορεί ότι

$$\left\{\begin{array}{l} \exists m' \in \mathbb{N},\ m' \leqslant m : \hat{\psi}(\mathsf{X}) = \varphi(\mathsf{X})^{m'} \\ \exists n' \in \mathbb{N},\ n' \leqslant n : \hat{\psi}(\mathsf{X}) = \theta(\mathsf{X})^{n'} \end{array}\right\} \Rightarrow \varphi(\mathsf{X})^{m'} = \theta(\mathsf{X})^{n'},$$

οπότε $m' = n'$ και $\varphi(\mathsf{X}) = \theta(\mathsf{X})$ (λόγω τού μονοσημάντου τής παραστάσεως (10.19)). Άτοπο! Επομένως, $\deg(\delta(\mathsf{X})) = 0$ (διότι $\delta(\mathsf{X}) \neq 0_{K[\mathsf{X}]}$) και $\delta(\mathsf{X}) = 1_K$ (διότι ο μέγιστος κοινός διαιρέτης $\delta(\mathsf{X})$ είναι εξ ορισμού *μονικό* πολυώνυμο). □

10.3.13 Πόρισμα. *Εάν τα* $\varphi_1(\mathsf{X}), \ldots, \varphi_k(\mathsf{X}) \in K[\mathsf{X}]$, $k \in \mathbb{N}$, $k \geqslant 2$, *είναι πολυώνυμα θετικού βαθμού και πρώτα μεταξύ τους ανά δύο, τότε*

$$\text{μκδ}\left(\textstyle\prod_{j=1}^{k-1} \varphi_j(\mathsf{X}), \varphi_k(\mathsf{X})\right) = 1_K.$$

Αποδειξη. Ας υποθέσουμε ότι το $\delta(\mathsf{X}) := \text{μκδ}(\prod_{j=1}^{k-1} \varphi_j(\mathsf{X}), \varphi_k(\mathsf{X}))$ έχει βαθμό $\geqslant 1$. Σύμφωνα με την πρόταση 10.3.5 υφίσταται τουλάχιστον ένα ανάγωγο πολυώνυμο $\psi(\mathsf{X})$ υπεράνω τού K το οποίο διαιρεί το $\delta(\mathsf{X})$. Αυτό εκφράζεται ως γινόμενο $\psi(\mathsf{X}) = c\hat{\psi}(\mathsf{X})$ μιας σταθεράς $c \in K \smallsetminus \{0_K\}$ (που ισούται με τον επικεφαλής συντελεστή του) και ενός αναγώγου (υπεράνω τού K) *μονικού* πολυωνύμου $\hat{\psi}(\mathsf{X})$. Προφανώς,

$$\left.\begin{array}{l} \hat{\psi}(\mathsf{X}) \mid \psi(\mathsf{X}) \\ \psi(\mathsf{X}) \mid \delta(\mathsf{X}) \end{array}\right\} \Longrightarrow \hat{\psi}(\mathsf{X}) \mid \delta(\mathsf{X})$$

και, ως εκ τούτου,

$$\left.\begin{array}{l} \delta(\mathsf{X}) \mid \prod_{j=1}^{k-1} \varphi_j(\mathsf{X}) \\ \delta(\mathsf{X}) \mid \varphi_k(\mathsf{X}) \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \hat{\psi}(\mathsf{X}) \mid \prod_{j=1}^{k-1} \varphi_j(\mathsf{X}) \\ \hat{\psi}(\mathsf{X}) \mid \varphi_k(\mathsf{X}) \end{array}\right\}.$$

Επειδή $\hat{\psi}(\mathsf{X}) \mid \prod_{j=1}^{k-1} \varphi_j(\mathsf{X})$, υπάρχει κάποιος $j_0 \in \{1, \ldots, k-1\}$, τέτοιος ώστε να ισχύει $\hat{\psi}(\mathsf{X}) \mid \varphi_{j_0}(\mathsf{X})$. Τούτο προκύπτει από το ότι το $\hat{\psi}(\mathsf{X})$, όντας ανάγωγο (υπεράνω τού K) και μονικό, οφείλει να συμπεριλαμβάνεται στους (ανάγωγους) παράγοντες τής συνεπτυγμένης αποσυνθέσεως *τουλάχιστον ενός* εκ των $\varphi_1(\mathsf{X}), \ldots, \varphi_k(\mathsf{X})$. Εκ των ανωτέρω έπεται ότι

$$\left.\begin{array}{l} \hat{\psi}(\mathsf{X}) \mid \varphi_{j_0}(\mathsf{X}) \\ \hat{\psi}(\mathsf{X}) \mid \varphi_k(\mathsf{X}) \end{array}\right\} \Longrightarrow \hat{\psi}(\mathsf{X}) \mid \text{μκδ}(\varphi_{j_0}(\mathsf{X}), \varphi_k(\mathsf{X})) = 1_K.$$

Άτοπο! Κατά συνέπειαν, $\deg(\delta(\mathsf{X})) = 0$ (διότι $\delta(\mathsf{X}) \neq 0_{K[\mathsf{X}]}$) και $\delta(\mathsf{X}) = 1_K$ (διότι ο μέγιστος κοινός διαιρέτης $\delta(\mathsf{X})$ είναι εξ ορισμού *μονικό* πολυώνυμο). □

10.3.14 Πρόταση. *Έστω ότι τα πολυώνυμα $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$ έχουν τις*

$$\varphi_1(\mathsf{X}) = c_1 \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[1]}}, \ \varphi_2(\mathsf{X}) = c_2 \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[2]}}$$

ως συνεπτυγμένες αποσυνθέσεις τους (υπό την ευρεία έννοια). Τότε ισχύουν τα εξής:

(i) *Ο μέγιστος κοινός διαιρέτης των $\varphi_1(\mathsf{X})$ και $\varphi_2(\mathsf{X})$ είναι το πολυώνυμο*

$$\boxed{\text{μκδ}(\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})) = \prod_{i=1}^{k} \psi_i(\mathsf{X})^{\min\{m_i^{[1]}, m_i^{[2]}\}}.} \tag{10.23}$$

(ii) *Το ελάχιστο κοινό πολλαπλάσιο των $\varphi_1(\mathsf{X})$ και $\varphi_2(\mathsf{X})$ είναι το*

$$\boxed{\text{εκπ}(\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})) = \prod_{i=1}^{k} \psi_i(\mathsf{X})^{\max\{m_i^{[1]}, m_i^{[2]}\}}.} \tag{10.24}$$

Απόδειξη. (i) Κατ' αρχάς,

$$\text{μκδ}(\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})) = \text{μκδ}\Big(\prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[1]}}, \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[2]}}\Big)$$

(βλ. 10.1.7 (iv)). Επειδή $\min\{m_i^{[1]}, m_i^{[2]}\} \leqslant m_i^{[1]}$ και $\min\{m_i^{[1]}, m_i^{[2]}\} \leqslant m_i^{[2]}$ για κάθε $i \in \{1, \ldots, k\}$, το πολυώνυμο $\prod_{i=1}^{k} \psi_i(\mathsf{X})^{\min\{m_i^{[1]}, m_i^{[2]}\}}$ διαιρεί αμφότερα τα $\prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[1]}}$ και $\prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[2]}}$ (βλ. πόρισμα 10.3.10). Εκτός τούτου, εάν

$$\theta(\mathsf{X}) = c \prod_{i=1}^{k} \psi_i(\mathsf{X})^{n_i}$$

είναι η (υπό την ευρεία έννοια) συνεπτυγμένη αποσύνθεση ενός κοινού διαιρέτη $\theta(\mathsf{X})$ των $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})$, τότε

$$[n_i \leqslant m_i^{[1]} \ \text{ και } \ n_i \leqslant m_i^{[2]}] \Rightarrow n_i \leqslant \min\{m_i^{[1]}, m_i^{[2]}\}, \ \forall i \in \{1, \ldots, k\}.$$

(Σημειωτέον ότι $c \in K \setminus \{0_K\} \Rightarrow c \mid 1_K$, καθώς ισχύει $cc^{-1} = 1_K$.) Επομένως, $\theta(\mathsf{X}) \mid \prod_{i=1}^{k} \psi_i(\mathsf{X})^{\min\{m_i^{[1]}, m_i^{[2]}\}}$ (εκ νέου μέσω τού πορίσματος 10.3.10) και η (10.23) είναι αληθής (βλ. 10.1.5).

(ii) Κατ' αρχάς,

$$\text{εκπ}(\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})) = \text{εκπ}\Big(\prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[1]}}, \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[2]}}\Big)$$

(βλ. 10.1.20 (iv)). Επειδή $\max\{m_i^{[1]}, m_i^{[2]}\} \geqslant m_i^{[1]}$ και $\max\{m_i^{[1]}, m_i^{[2]}\} \geqslant m_i^{[2]}$ για κάθε $i \in \{1, \dots, k\}$, αμφότερα τα $\prod_{i=1}^k \psi_i(\mathsf{X})^{m_i^{[1]}}$ και $\prod_{i=1}^k \psi_i(\mathsf{X})^{m_i^{[2]}}$ διαιρούν το πολυώνυμο $\prod_{i=1}^k \psi_i(\mathsf{X})^{\max\{m_i^{[1]}, m_i^{[2]}\}}$ (βλ. πόρισμα 10.3.10). Εκτός τούτου, εάν

$$\zeta(\mathsf{X}) = c \prod_{i=1}^k \psi_i(\mathsf{X})^{n_i}$$

είναι η (υπό την ευρεία έννοια) συνεπτυγμένη αποσύνθεση ενός κοινού πολλαπλασίου $\zeta(\mathsf{X})$ των $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})$, τότε

$$[n_i \geqslant m_i^{[1]} \text{ και } n_i \geqslant m_i^{[2]}] \Rightarrow n_i \geqslant \max\{m_i^{[1]}, m_i^{[2]}\}, \ \forall i \in \{1, \dots, k\}.$$

Επομένως, $\prod_{i=1}^k \psi_i(\mathsf{X})^{\max\{m_i^{[1]}, m_i^{[2]}\}} \mid \zeta(\mathsf{X})$ (εκ νέου μέσω τού πορίσματος 10.3.10) και η (10.24) είναι αληθής (βλ. 10.1.18). □

10.4 ΔΙΑΣΠΑΣΕΙΣ ΣΕ ΠΡΩΤΟΒΑΘΜΙΟΥΣ ΠΑΡΑΓΟΝΤΕΣ

Το ακόλουθο λήμμα γενικεύει το προηγηθέν πόρισμα 10.2.5.

10.4.1 Λήμμα. *Έστω $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ ένα πολυώνυμο βαθμού $n \geqslant 1$. Εάν υποθέσουμε ότι τα στοιχεία $\lambda_1, \dots, \lambda_k \in K$ ($k \in \mathbb{N}$, $k \leqslant n$) είναι k σαφώς διακεκριμένες θέσεις μηδενισμού τού $\varphi(\mathsf{X})$ και ότι*

$$(\mathsf{X} - \lambda_1)^{\nu_1} \mid \varphi(\mathsf{X}), \ \dots\dots, \ (\mathsf{X} - \lambda_k)^{\nu_k} \mid \varphi(\mathsf{X}),$$

για κάποιους $\nu_1, \dots, \nu_k \in \mathbb{N}$, τότε $\prod_{i=1}^k (\mathsf{X} - \lambda_i)^{\nu_i} \mid \varphi(\mathsf{X})$.

Απόδειξη. Θα χρησιμοποιήσουμε μαθηματική επαγωγή ως προς τον k. Για $k = 1$ τούτο είναι προφανές. Υποθέτουμε ότι $k \geqslant 2$ και ότι ο ισχυρισμός είναι αληθής για $k-1$ σαφώς διακεκριμένες θέσεις μηδενισμού τού $\varphi(\mathsf{X})$. Το $\mathsf{X} - \lambda_i$ (όντας πρωτοβάθμιο πολυώνυμο) είναι ανάγωγο υπεράνω τού K για κάθε $i \in \{1, \dots, k\}$. Εξάλλου, για οιουσδήποτε $i, j \in \{1, \dots, k\}$, $i \neq j$, έχουμε

$$\lambda_i \neq \lambda_j \Rightarrow \mathsf{X} - \lambda_i \neq \mathsf{X} - \lambda_j \underset{10.3.12}{\Longrightarrow} \mu\kappa\delta((\mathsf{X} - \lambda_i)^{\nu_i}, (\mathsf{X} - \lambda_j)^{\nu_j}) = 1_K.$$

Κατά το πόρισμα 10.3.13,

$$\mu\kappa\delta(\textstyle\prod_{i=1}^{k-1} (\mathsf{X} - \lambda_i)^{\nu_i}, (\mathsf{X} - \lambda_k)^{\nu_k}) = 1_K. \tag{10.25}$$

Σύμφωνα με την αρχική και την επαγωγική μας υπόθεση,

$$\left.\begin{array}{c} (\mathsf{X} - \lambda_k)^{\nu_k} \mid \varphi(\mathsf{X}) \\ \displaystyle\prod_{i=1}^{k-1} (\mathsf{X} - \lambda_i)^{\nu_i} \mid \varphi(\mathsf{X}) \end{array}\right\} \Longrightarrow \prod_{i=1}^{k} (\mathsf{X} - \lambda_i)^{\nu_i} \mid \varphi(\mathsf{X})$$

(μέσω τής (10.25) και τού πορίσματος 10.1.17). □

10.4.2 Λήμμα. *Έστω $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ ένα πολυώνυμο βαθμού $n \geqslant 1$. Εάν τα στοιχεία $\lambda_1, \dots, \lambda_k \in K$ ($k \in \mathbb{N}$, $k \leqslant n$) είναι (όλες) οι σαφώς διακεκριμένες θέσεις μηδενισμού τού $\varphi(\mathsf{X})$, τότε υπάρχει $\psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$, τέτοιο ώστε το $\varphi(\mathsf{X})$ να γράφεται υπό τη μορφή*

$$\varphi(\mathsf{X}) = \left(\prod_{i=1}^{k} (\mathsf{X} - \lambda_i)^{m_i} \right) \psi(\mathsf{X}), \tag{10.26}$$

όπου $m_i = \mathrm{mult}(\varphi(\mathsf{X}); \lambda_i)$, $\psi(\lambda_i) \neq 0_K$, $\forall i \in \{1, \dots, k\}$, *και* $\sum_{i=1}^{k} m_i \leqslant n$.

Απόδειξη. Επειδή $(\mathsf{X} - \lambda_i)^{m_i} \mid \varphi(\mathsf{X})$ για κάθε $i \in \{1, \dots, k\}$, το λήμμα 10.4.1 μας πληροφορεί ότι το γινόμενό τους είναι διαιρέτης τού $\varphi(\mathsf{X})$. Ως εκ τούτου, το $\varphi(\mathsf{X})$ γράφεται υπό τη μορφή (10.26) για κάποιο κατάλληλο $\psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$ και

$$[m_i \geqslant 1,\ \forall i \in \{1, \dots, k\}] \Rightarrow n = \deg(\psi(\mathsf{X})) + \sum_{i=1}^{k} m_i \geqslant \sum_{i=1}^{k} m_i.$$

Επιπροσθέτως, $\psi(\lambda_i) \neq 0_K$, για κάθε $i \in \{1, \dots, k\}$, διότι εάν υπήρχε κάποιος δείκτης $i_0 \in \{1, \dots, k\}$ με $\psi(\lambda_{i_0}) = 0_K$, τότε θα είχαμε $\mathsf{X} - \lambda_{i_0} \mid \psi(\mathsf{X})$ και θα καταλήγαμε στο ότι $(\mathsf{X} - \lambda_{i_0})^{m_{i_0}+1} \mid \varphi(\mathsf{X})$ (ήτοι σε κάτι που θα αντέκειτο στον ορισμό τής πολλαπλότητας $m_{i_0} = \mathrm{mult}(\varphi(\mathsf{X}); \lambda_{i_0})$). □

10.4.3 Ορισμός. Έστω L μια επέκταση ενός σώματος K και έστω $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ βαθμού $n \geqslant 1$. Εάν υπάρχουν (όχι κατ' ανάγκην σαφώς διακεκριμένα) στοιχεία $\lambda_1, \dots, \lambda_n$ τού L, τέτοια ώστε να ισχύει η ισότητα

$$\varphi(\mathsf{X}) = c\,(\mathsf{X} - \lambda_1)(\mathsf{X} - \lambda_2) \cdots (\mathsf{X} - \lambda_n) \tag{10.27}$$

(για κάποιο $c \in K \setminus \{0_K\}$), τότε λέμε ότι το πολυώνυμο $\varphi(\mathsf{X})$ **διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού** L.

10.4.4 Θεώρημα (Κριτήριο μη ύπαρξεως πολλαπλών θ.μ.). *Εάν $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ είναι ένα πολυώνυμο βαθμού $n \geqslant 1$ το οποίο διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω μιας (όχι κατ' ανάγκην γνήσιας) επεκτάσεως L τού K, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Το $\varphi(\mathsf{X})$ δεν διαθέτει καμία πολλαπλή θέση μηδενισμού εντός τού L (δηλαδή τα $\lambda_1, \dots, \lambda_n$ σε μια παράστασή του (10.27) είναι σαφώς διακεκριμένα).*

(ii) $\mathrm{μκδ}(\varphi(\mathsf{X}), \mathcal{D}(\varphi(\mathsf{X}))) = 1_K\ (= 1_L)$.

Απόδειξη. *Επισήμανση*: Επειδή ο μέγιστος κοινός διαιρέτης των $\varphi(\mathsf{X}), \mathcal{D}(\varphi(\mathsf{X}))$ *εντός τού* $K[\mathsf{X}]$ ισούται με τον μέγιστο κοινό διαιρέτη των $\varphi(\mathsf{X}), \mathcal{D}(\varphi(\mathsf{X}))$ *εντός τού* $L[\mathsf{X}]$ (βλ. πρόταση 10.1.11), στην απόδειξη οι υπολογισμοί θα γίνουν (για ευνόητους λόγους) *εντός τού* $L[\mathsf{X}]$.

(i)⇒(ii) Ας υποθέσουμε ότι το πολυώνυμο $\mathrm{μκδ}(\varphi(\mathsf{X}), \mathcal{D}(\varphi(\mathsf{X})))$ έχει βαθμό $\geqslant 1$. Επειδή το $\varphi(\mathsf{X})$ διασπάται (εξ υποθέσεως) σε πρωτοβάθμιους παράγοντες υπεράνω τού L, υπάρχει κάποιος κοινός διαιρέτης και, ως εκ τούτου, και κάποια κοινή θέση μηδενισμού $\lambda \in L$ των $\varphi(\mathsf{X}), \mathcal{D}(\varphi(\mathsf{X}))$, οπότε

$$\left\{ \begin{array}{l} \exists \alpha(\mathsf{X}) \in L[\mathsf{X}] : \varphi(\mathsf{X}) = (\mathsf{X} - \lambda)\alpha(\mathsf{X}), \\ \exists \beta(\mathsf{X}) \in L[\mathsf{X}] : \mathcal{D}(\varphi(\mathsf{X})) = (\mathsf{X} - \lambda)\beta(\mathsf{X}). \end{array} \right\}$$

Επομένως, $(\mathsf{X} - \lambda)\beta(\mathsf{X}) = \mathcal{D}((\mathsf{X} - \lambda)\alpha(\mathsf{X})) = \alpha(\mathsf{X}) + (\mathsf{X} - \lambda)\mathcal{D}(\alpha(\mathsf{X}))$ και

$$\mathsf{X} - \lambda \mid \alpha(\mathsf{X}) \Longrightarrow (\mathsf{X} - \lambda)^2 \mid \varphi(\mathsf{X}).$$

Τούτο σημαίνει ότι το $\lambda \in L$ είναι μια πολλαπλή (τουλάχιστον διπλή) θέση μηδενισμού τού $\varphi(\mathsf{X})$. Άτοπο!

(ii)⇒(i) Έστω λ *τυχούσα* θέση μηδενισμού τού $\varphi(\mathsf{X})$ *εντός τού* L με πολλαπλότητα $m \geqslant 1$. Η πρόταση 10.2.14 (με το L στη θέση τού εκεί παρατεθέντος K) μας πληροφορεί ότι

$$\exists \psi(\mathsf{X}) \in L[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\} : \varphi(\mathsf{X}) = (\mathsf{X} - \lambda)^m\, \psi(\mathsf{X})$$

με $\psi(\lambda) \neq 0_K$. Επειδή (σύμφωνα με το (iii) τού λήμματος 10.2.16) ισχύει

$$\mathcal{D}(\varphi(\mathsf{X})) = m\,(\mathsf{X}-\lambda)^{m-1}\,\psi(\mathsf{X}) + (\mathsf{X}-\lambda)^m\,\mathcal{D}(\psi(\mathsf{X})),$$

έχουμε

$$\left.\begin{array}{l}(\mathsf{X}-\lambda)^{m-1} \mid \varphi(\mathsf{X}) \\ (\mathsf{X}-\lambda)^{m-1} \mid \mathcal{D}(\varphi(\mathsf{X}))\end{array}\right\} \Rightarrow (\mathsf{X}-\lambda)^{m-1} \mid \text{μκδ}(\varphi(\mathsf{X}), \mathcal{D}(\varphi(\mathsf{X}))) = 1_L,$$

ήτοι $m-1 = \deg((\mathsf{X}-\lambda)^{m-1}) \leqslant 0 \Rightarrow m = 1$. □

10.4.5 Παρατήρηση. Το κριτήριο 10.4.4 είναι λίαν χρήσιμο, καθώς μας επιτρέπει να ελέγξουμε το κατά πόσον το $\varphi(\mathsf{X})$ διαθέτει (ή δεν διαθέτει) πολλαπλές θέσεις μηδενισμού εντός τού L *χωρίς* να υποχρεούμεθα *να υπολογίσουμε τις θέσεις μηδενισμού του*! (Δοθέντος ενός συγκεκριμένου $\varphi(\mathsf{X})$, για την πρακτική εφαρμογή του είναι αρκετό να εκτελεσθεί ένας και μόνον ευκλείδειος αλγόριθμος.)

Το επόμενο θεώρημα δίδει δύο ικανές και αναγκαίες συνθήκες, υπό τις οποίες ένα (μη σταθερό) πολυώνυμο $\varphi(\mathsf{X}) \in K\,[\mathsf{X}]$ διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού (ιδίου τού) K.

10.4.6 Θεώρημα. *Εάν $\varphi(\mathsf{X}) \in K\,[\mathsf{X}]$ είναι ένα πολυώνυμο βαθμού $n \geqslant 1$, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Το $\varphi(\mathsf{X})$ διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού K.*

(ii) *Εάν το $\theta(\mathsf{X}) \in K[\mathsf{X}]$ είναι ένας ανάγωγος (υπεράνω τού K) διαιρέτης τού $\varphi(\mathsf{X})$, τότε* $\deg(\theta(\mathsf{X})) = 1$.

(iii) *Υπάρχουν $\lambda_1, \ldots, \lambda_k \in K$ ($k \in \mathbb{N},\ k \leqslant n$), τέτοια ώστε να ισχύει η ισότητα* $\sum_{i=1}^{k} \text{mult}(\varphi(\mathsf{X}); \lambda_i) = n$.

Απόδειξη. (i)⇒(ii) Εάν υπάρχουν (όχι κατ' ανάγκην σαφώς διακεκριμένα) στοιχεία $\lambda_1, \ldots, \lambda_n$ τού K, τέτοια ώστε να ισχύει η ισότητα

$$\varphi(\mathsf{X}) = c(\mathsf{X}-\lambda_1)(\mathsf{X}-\lambda_2)\cdots(\mathsf{X}-\lambda_n),$$

(για κάποιο $c \in K \setminus \{0_K\}$) και το $\theta(\mathsf{X}) \in K[\mathsf{X}]$ είναι ένας ανάγωγος διαιρέτης τού $\varphi(\mathsf{X})$, τότε εφαρμόζοντας το λήμμα 10.3.7 για τα $\theta(\mathsf{X})$ και $\varphi(\mathsf{X})$ συμπεραίνουμε ότι

$$\exists i_0 \in \{1, \ldots, n\} :\ \theta(\mathsf{X}) = c\,(\mathsf{X}-\lambda_{i_0})\,,$$

για κάποιο $c \in K \setminus \{0_K\}$, οπότε $\deg(\theta(\mathsf{X})) = 1$.

(ii)⇒(iii) Έστω ότι τα $\lambda_1, \ldots, \lambda_k \in K$ ($k \in \mathbb{N},\ k \leqslant n$) είναι (όλες) οι σαφώς διακεκριμένες θέσεις μηδενισμού τού $\varphi(\mathsf{X})$. Σύμφωνα με το λήμμα 10.4.2 υπάρχει $\psi(\mathsf{X}) \in K\,[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$, τέτοιο ώστε το $\varphi(\mathsf{X})$ να γράφεται υπό τη μορφή

$$\varphi(\mathsf{X}) = \left(\prod_{i=1}^{k} (\mathsf{X}-\lambda_i)^{m_i}\right) \psi(\mathsf{X}),$$

όπου $m_i = \text{mult}(\varphi(\mathsf{X}); \lambda_i)$, $\psi(\lambda_i) \neq 0_K$, $\forall i \in \{1, \ldots, k\}$. Εάν υποθέσουμε ότι $\deg(\psi(\mathsf{X})) \geqslant 1$, τότε (σύμφωνα με την πρόταση 10.3.5) υπάρχει κάποιος ανάγωγος διαιρέτης $\theta(\mathsf{X}) \in K[\mathsf{X}]$ τού $\psi(\mathsf{X})$ (και, κατ' επέκταση, και τού $\varphi(\mathsf{X})$, διότι $\psi(\mathsf{X}) \mid \varphi(\mathsf{X})$). Εξ υποθέσεως, $\deg(\theta(\mathsf{X})) = 1$, οπότε το $\theta(\mathsf{X})$ διαθέτει μια θέση μηδενισμού $\lambda \in K$. Κατά συνέπειαν,

$$\theta(\lambda) = 0_K \Rightarrow \psi(\lambda) = 0_K \Rightarrow \varphi(\lambda) = 0_K \Rightarrow \exists i_0 \in \{1, \ldots, k\} : \lambda = \lambda_{i_0}.$$

Αυτό σημαίνει ότι $\psi(\lambda_{i_0}) = 0_K$. Άτοπο! Άρα $\deg(\psi(\mathsf{X})) = 0$ και $\sum_{i=1}^{k} m_i = n$.

(iii)⇒(i) Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι ισχύει $\mathrm{mult}(\varphi(\mathsf{X}); \lambda_i) \geqslant 1$ για κάθε $i \in \{1, \ldots, k\}$ (διότι εάν υπάρχει ένα μη κενό υποσύνολο $\mathcal{A} \subsetneqq \{1, \ldots, k\}$ με $\mathrm{mult}(\varphi(\mathsf{X}); \lambda_j) = 0$ για κάθε $j \in \mathcal{A}$, μπορούμε να χρησιμοποιήσουμε την ίδια επιχειρηματολογία για τα υπολειπόμενα λ_j, $j \in \{1, \ldots, k\} \setminus \mathcal{A}$). Κατά το λήμμα 10.4.2 το $\varphi(\mathsf{X})$ γράφεται υπό τη μορφή (10.26). Εξ αυτής έπεται ότι

$$\sum_{i=1}^{k} m_i = n = \deg(\psi(\mathsf{X})) + \sum_{i=1}^{k} m_i \Rightarrow \deg(\psi(\mathsf{X})) = 0,$$

οπότε το $\psi(\mathsf{X})$ είναι σταθερό μη μηδενικό πολυώνυμο και το $\varphi(\mathsf{X})$ διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού K. □

Εάν το $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ είναι ένα πολυώνυμο βαθμού $n \geqslant 1$ το οποίο διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού K, τότε αναπτύσσοντας το γινόμενο τού δευτέρου μέλους στην (10.27) καταλήγουμε σε σχέσεις μεταξύ των συντελεστών τού $\varphi(\mathsf{X})$ και των αθροισμάτων όλων των γινομένων των $\lambda_1, \ldots, \lambda_n$ λαμβανομένων ανά k (των λεγομένων k-αστών *στοιχειωδών συμμετρικών συναρτήσεων* των $\lambda_1, \ldots, \lambda_n$), όπου $k \in \{1, \ldots, n\}$. Αυτές είχαν γίνει αντικείμενο μελέτης (σε ειδικές περιπτώσεις και για $K = \mathbb{R}$) ήδη από τα τέλη τού 16ου αιώνα, αναφέρονται δε σε εργασίες των Γάλλων μαθηματικών François Viète (1540-1603) και Albert Girard (1595-1632). Ο πρώτος (γνωστός και υπό το εκλατινισμένο επίθετο Vieta) περιορίσθηκε σε πολυώνυμα με θέσεις μηδενισμού που πληρούν κάποιες ειδικές συνθήκες, ενώ ο δεύτερος εξέτασε τη γενική περίπτωση (τρεις δεκαετίες αργότερα) και προέβη σε συστηματικότερη παρουσίαση των σχετικών τύπων.

10.4.7 Θεώρημα (Τύποι τού Viète). *Έστω $\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in K[\mathsf{X}]$ ένα πολυώνυμο βαθμού $n \geqslant 1$ το οποίο διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού K. Εάν οι θέσεις μηδενισμού του είναι τα (όχι κατ' ανάγκην σαφώς διακεκριμένα) στοιχεία $\lambda_1, \ldots, \lambda_n \in K$ και εάν θέσουμε*

$$\boxed{s_k := \sum_{\substack{(j_1, \ldots, j_k) \in \mathbb{N}^k : \\ 1 \leqslant j_1 < \cdots < j_k \leqslant n}} \lambda_{j_1} \lambda_{j_2} \cdots \lambda_{j_k}, \ \forall k \in \{1, \ldots, n\},} \tag{10.28}$$

και $s_0 := 1$, τότε

$$\boxed{s_k = (-1_K)^k \, a_n^{-1} \, a_{n-k}, \ \forall k \in \{0, 1, \ldots, n\},} \tag{10.29}$$

ή, ισοδυνάμως,

$$\boxed{a_i = (-1_K)^{n-i} \, a_n s_{n-i}, \ \forall i \in \{0, 1, \ldots, n\}.} \tag{10.30}$$

(Όταν $k = 1$, τότε υπονοείται ότι το άθροισμα (10.28) είναι το $\lambda_1 + \cdots + \lambda_n$.)

Απόδειξη. Προφανώς, $a_n \neq 0_K$ και

$$\varphi(\mathsf{X}) = a_n(\mathsf{X} - \lambda_1)(\mathsf{X} - \lambda_2) \cdots (\mathsf{X} - \lambda_n)$$

είναι η διάσπαση τού $\varphi(\mathsf{X})$ σε πρωτοβάθμιους παράγοντες υπεράνω τού K. Επειδή

$$a_n^{-1} \varphi(\mathsf{X}) = (\mathsf{X} - \lambda_1)(\mathsf{X} - \lambda_2) \cdots (\mathsf{X} - \lambda_n),$$

αρκεί να αποδείξουμε την ισότητα

$$(\mathsf{X}-\lambda_1)(\mathsf{X}-\lambda_2)\cdots(\mathsf{X}-\lambda_n)=\mathsf{X}^n+\sum_{k=1}^{n}(-1_K)^k s_k \mathsf{X}^{n-k}. \tag{10.31}$$

Εάν $n=1$, τότε $s_1=\lambda_1$ και η (10.31) είναι αληθής. Υποθέτοντας ότι $n\geqslant 2$ και ότι ισχύει η ισότητα

$$\prod_{\nu=1}^{n-1}(\mathsf{X}-\lambda_\nu)=\mathsf{X}^{n-1}+\sum_{\varrho=1}^{n-1}(-1_K)^\varrho \sum_{\substack{(i_1,\ldots,i_\varrho)\in\mathbb{N}^\varrho:\\ 1\leqslant i_1<\cdots<i_\varrho\leqslant n-1}} \lambda_{i_1}\cdots\lambda_{i_\varrho}\mathsf{X}^{n-1-\varrho}$$

(για $n-1$ παράγοντες) παρατηρούμε ότι

$$\begin{aligned}
&(\mathsf{X}^{n-1}+\sum_{\varrho=1}^{n-1}(-1_K)^\varrho \sum_{\substack{(i_1,\ldots,i_\varrho)\in\mathbb{N}^\varrho:\\ 1\leqslant i_1<\cdots<i_\varrho\leqslant n-1}} \lambda_{i_1}\cdots\lambda_{i_\varrho}\mathsf{X}^{n-1-\varrho})(\mathsf{X}-\lambda_n)\\
&=\mathsf{X}^n+\sum_{k=1}^{n-1}(-1_K)^k\left(\sum_{\substack{(i_1,\ldots,i_k)\in\mathbb{N}^k:\\ 1\leqslant i_1<\cdots<i_k\leqslant n-1}}\lambda_{i_1}\cdots\lambda_{i_k}+\left(\sum_{\substack{(i'_1,\ldots,i'_{k-1})\in\mathbb{N}^{k-1}:\\ 1\leqslant i'_1<\cdots<i'_{k-1}\leqslant n-1}}\lambda_{i'_1}\cdots\lambda_{i'_{k-1}}\right)\lambda_n\right)\mathsf{X}^{n-k}\\
&+(-1_K)^n\lambda_1\cdots\lambda_n
\end{aligned}$$

όπου

$$\sum_{\substack{(i_1,\ldots,i_k)\in\mathbb{N}^k:\\ 1\leqslant i_1<\cdots<i_k\leqslant n-1}}\lambda_{i_1}\cdots\lambda_{i_k}+\left(\sum_{\substack{(i'_1,\ldots,i'_{k-1})\in\mathbb{N}^{k-1}:\\ 1\leqslant i'_1<\cdots<i'_{k-1}\leqslant n-1}}\lambda_{i'_1}\cdots\lambda_{i'_{k-1}}\right)\lambda_n=s_k,$$

οπότε η (10.31) είναι αληθής και σε αυτήν την περίπτωση. □

10.4.8 Παράδειγμα. Θεωρούμε το $\varphi(\mathsf{X}):=(\mathsf{X}+1)^{2\nu+1}-(\mathsf{X}-1)^{2\nu+1}\in\mathbb{C}\,[\mathsf{X}]$ (όπου $\nu\in\mathbb{N}$). Προφανώς,

$$\begin{aligned}
\varphi(\mathsf{X}) &= \sum_{i=0}^{2\nu+1}\tbinom{2\nu+1}{i}\mathsf{X}^i-\sum_{i=0}^{2\nu+1}(-1)^{2\nu+1-i}\tbinom{2\nu+1}{i}\mathsf{X}^i\\
&= 2\,(2\nu+1)\,\mathsf{X}^{2\nu}+2\tbinom{2\nu+1}{3}\mathsf{X}^{2\nu-2}+\cdots+2\,(2\nu+1)\,(\nu+1)\,\mathsf{X}^2+2,
\end{aligned}$$

οπότε $\deg(\varphi(\mathsf{X}))=2\nu$ (με τους συντελεστές των περιττών δυνάμεων τού X ίσους με το 0). Επειδή $\varphi(1)=2^{2\nu+1}\neq 0$, για $z\in\mathbb{C}\smallsetminus\{1\}$ έχουμε

$$\varphi(z)=0\Leftrightarrow\left(\tfrac{z+1}{z-1}\right)^{2\nu+1}=1\Leftrightarrow\exists k\in\{0,\ldots,2\nu\}:\tfrac{z+1}{z-1}=\mathbf{e}^{\frac{2k\pi i}{2\nu+1}}.$$

Η τιμή $k=0$ αποκλείεται (για προφανείς λόγους). Για $k\in\{1,\ldots,2\nu\}$ λαμβάνουμε[8]

$$\tfrac{z+1}{z-1}=\mathbf{e}^{\frac{2k\pi i}{2\nu+1}}\Leftrightarrow z=\frac{\mathbf{e}^{\frac{2k\pi i}{2\nu+1}}+1}{\mathbf{e}^{\frac{2ik\pi}{2\nu+1}}-1}=\frac{\mathbf{e}^{\frac{k\pi i}{2\nu+1}}+\mathbf{e}^{-\frac{k\pi i}{2\nu+1}}}{\mathbf{e}^{\frac{k\pi i}{2\nu+1}}-\mathbf{e}^{-\frac{k\pi i}{2\nu+1}}}=-i\cot(\tfrac{k\pi}{2\nu+1})=-\frac{i}{\tan(\frac{k\pi}{2\nu+1})}.$$

Επομένως το $\varphi(z)$ διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού $\mathbb{C}$ ως εξής:

$$\varphi(\mathsf{X})=2\,(2\nu+1)\prod_{k=1}^{2\nu}\left(\mathsf{X}+i\cot(\tfrac{k\pi}{2\nu+1})\right).$$

[8] Ο ορισμός τής συναρτήσεως τής *εφαπτομένης* επεκτείνεται και στο $\mathbb{C}$ ως εξής:

$$\mathbb{C}\ni z\longmapsto\tan(z):=i\left(\frac{\mathbf{e}^{-iz}-\mathbf{e}^{iz}}{\mathbf{e}^{-iz}+\mathbf{e}^{iz}}\right)$$

και η *συνεφαπτομένη* τού z είναι η $\cot(z):=\frac{1}{\tan(z)}$.

Οι τύποι τού Viète οδηγούν, εν προκειμένω, σε ενδιαφέρουσες τριγωνομετρικές ταυτότητες για τις μετέχουσες συνεφαπτομένες. Π.χ.,

$$\sum_{k=1}^{2\nu}\left(-i\cot(\tfrac{k\pi}{2\nu+1})\right)=0\Rightarrow\sum_{k=1}^{2\nu}\cot(\tfrac{k\pi}{2\nu+1})=0,$$

$$\sum_{1\leqslant j<k\leqslant 2\nu}\cot(\tfrac{j\pi}{2\nu+1})\cot(\tfrac{k\pi}{2\nu+1})=-\tfrac{1}{2(2\nu+1)}\left(2\tbinom{2\nu+1}{3}\right)=-\tfrac{\nu(2\nu-1)}{3}$$

και (από τον τελευταίο τύπο)

$$\prod_{k=1}^{2\nu}\left(-i\cot(\tfrac{k\pi}{2\nu+1})\right)=\tfrac{1}{2\nu+1}\Longrightarrow\prod_{k=1}^{\nu}\cot(\tfrac{k\pi}{2\nu+1})=\tfrac{1}{\sqrt{2\nu+1}}.$$

Στην *Invention Nouvelle en l'Algèbre* (1629) ο Girard επεξέτεινε την έρευνά του επί των στοιχειωδών συμμετρικών συναρτήσεων $s_1, s_2, \ldots$ και κατόρθωσε να τις συσχετίσει και με τα *αθροίσματα δυνάμεων* των $\lambda_1, \ldots, \lambda_n$. Οι εξαχθέντες αναδρομικοί τύποι ανακαλύφθηκαν εκ νέου από τον Isaac Newton (1642-1727) περί το 1666. Έκτοτε έχουν δοθεί πολλές (διαφορετικές) αποδείξεις τους.

10.4.9 Θεώρημα (Τύποι των Girard και Newton I). *Έστω* $\varphi(\mathsf{X})=\sum_{i=0}^{n}a_i\mathsf{X}^i\in K[\mathsf{X}]$ *ένα πολυώνυμο βαθμού* $n\geqslant 1$ *το οποίο διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού* K. *Εάν οι θέσεις μηδενισμού του είναι τα (όχι κατ' ανάγκην σαφώς διακεκριμένα) στοιχεία* $\lambda_1,\ldots,\lambda_n\in K$ *και*

$$\boxed{t_\nu:=\lambda_1^\nu+\cdots+\lambda_n^\nu,\ \forall\nu\in\mathbb{N}_0,}\tag{10.32}$$

τότε για οιονδήποτε $k\in\mathbb{N}$ *ισχύει η σχέση*

$$\boxed{t_k-s_1t_{k-1}+s_2t_{k-2}-\cdots+(-1_K)^ns_nt_{k-n}=0_K,}\tag{10.33}$$

όταν $k\geqslant n$, *και η σχέση*

$$\boxed{t_k-s_1t_{k-1}+s_2t_{k-2}-\cdots+(-1_K)^{k-1}s_{k-1}t_1+(-1_K)^kks_k=0_K,}\tag{10.34}$$

όταν $1\leqslant k\leqslant n$, *όπου τα* $s_1, s_2, \ldots$ *είναι τα αθροίσματα* (10.28).

Απόδειξη. *Περίπτωση πρώτη.* Εάν $k\geqslant n$, τότε εφαρμόζοντας σε αμφότερα μέλη τής ισότητας (10.31):

$$\sum_{j=0}^{n}(-1_K)^js_j\mathsf{X}^{n-j}=(\mathsf{X}-\lambda_1)(\mathsf{X}-\lambda_2)\cdots(\mathsf{X}-\lambda_n)$$

τη συνάρτηση $\mathfrak{y}_{\lambda_i}$ πολυωνυμικής αποτιμήσεως στο λ_i λαμβάνουμε

$$\sum_{j=0}^{n}(-1_K)^js_j\lambda_i^{n-j}=0_K,\ \forall i\in\{1,\ldots,n\}.\tag{10.35}$$

Αρκεί να πολλαπλασιάσουμε αμφότερα τα μέλη των ισοτήτων (10.35) με λ_i^{k-n}:

$$\sum_{j=0}^{n}(-1_K)^js_j\lambda_i^{k-j}=0_K,\ \forall i\in\{1,\ldots,n\},$$

και να τις αθροίσουμε, κατόπιν τούτου, κατά μέλη

$$\sum_{i=1}^{n}\sum_{j=0}^{n}(-1_K)^js_j\lambda_i^{k-j}=\sum_{j=0}^{n}(-1_K)^js_j\sum_{i=1}^{n}\lambda_i^{k-j}=\sum_{j=0}^{n}(-1_K)^js_jt_{k-j}=0_K.$$

Περίπτωση δεύτερη. Εάν $1 \leqslant k \leqslant n$, τότε θέτουμε

$$\beta_i(\mathsf{X}) := \prod_{l \in \{1,\ldots,n\} \smallsetminus \{i\}} (\mathsf{X} - \lambda_l),$$

και εκφράζουμε την επίτυπη παράγωγο $\mathcal{D}(\hat{\varphi}(\mathsf{X}))$ τού

$$\hat{\varphi}(\mathsf{X}) := a_n^{-1}\varphi(\mathsf{X}) = (\mathsf{X} - \lambda_1)\cdots(\mathsf{X} - \lambda_n) = \sum_{j=0}^{n} (-1_K)^j s_j \mathsf{X}^{n-j}$$

αφ' ενός μεν ως

$$\mathcal{D}(\hat{\varphi}(\mathsf{X})) = \sum_{i=1}^{n} \beta_i(\mathsf{X}), \tag{10.36}$$

(βλ. (10.11)), αφ' ετέρου δε ως

$$\mathcal{D}(\hat{\varphi}(\mathsf{X})) = \mathcal{D}\left(\sum_{j=0}^{n} (-1_K)^j s_j \mathsf{X}^{n-j}\right) = \sum_{j=0}^{n-1} (-1_K)^j\,(n-j)\,s_j \mathsf{X}^{n-j-1}. \tag{10.37}$$

Επειδή $\hat{\varphi}(\mathsf{X}) = (\mathsf{X} - \lambda_i)\beta_i(\mathsf{X})$ για κάθε $i \in \{1, \ldots, n\}$, έχουμε

$$\begin{aligned} \hat{\varphi}(\mathsf{X}) &= \hat{\varphi}(\mathsf{X}) - \hat{\varphi}(\lambda_i) = \sum_{j=0}^{n} (-1_K)^j s_j \mathsf{X}^{n-j} - \sum_{j=0}^{n} (-1_K)^j s_j \lambda_i^{n-j} \\ &= \sum_{j=0}^{n-1} (-1_K)^j s_j (\mathsf{X}^{n-j} - \lambda_i^{n-j}). \end{aligned}$$

Ως γνωστόν, για κάθε $(i, j) \in \{1, \ldots, n\} \times \{0, 1, \ldots, n-1\}$ ισχύει

$$\mathsf{X}^{n-j} - \lambda_i^{n-j} = (\mathsf{X} - \lambda_i)\left(\sum_{\nu=0}^{n-j-1} \lambda_i^{\nu} \mathsf{X}^{n-j-1-\nu}\right),$$

οπότε

$$\begin{aligned} \hat{\varphi}(\mathsf{X}) &= (\mathsf{X} - \lambda_i)\left(\sum_{j=0}^{n-1} (-1_K)^j s_j \left(\sum_{\nu=0}^{n-j-1} \lambda_i^{\nu} \mathsf{X}^{n-j-1-\nu}\right)\right) \\ &= (\mathsf{X} - \lambda_i)\left(\sum_{j=0}^{n-1} \left(\sum_{\varrho=0}^{j} (-1_K)^{\varrho} s_j \lambda_i^{j-\varrho}\right) \mathsf{X}^{n-j-1}\right) \end{aligned}$$

(κατόπιν αναδιατάξεως τής αθροίσεως). Αυτό σημαίνει ότι

$$\beta_i(\mathsf{X}) = \sum_{j=0}^{n-1} \left(\sum_{\varrho=0}^{j} (-1_K)^{\varrho} s_j \lambda_i^{j-\varrho}\right) \mathsf{X}^{n-j-1}, \ \forall i \in \{1, \ldots, n\}. \tag{10.38}$$

(καθόσον ο $K\,[\mathsf{X}]$ είναι ακεραία περιοχή). Αθροίζοντας τις (10.38) κατά μέλη λαμβάνουμε μέσω τής (10.36):

$$\begin{aligned} \mathcal{D}(\hat{\varphi}(\mathsf{X})) &= \sum_{i=1}^{n} \beta_i(\mathsf{X}) = \sum_{j=0}^{n-1} \left(\sum_{\varrho=0}^{j} (-1_K)^{\varrho} s_j \left(\sum_{i=1}^{n} \lambda_i^{j-\varrho}\right)\right) \mathsf{X}^{n-j-1} \\ &= \sum_{j=0}^{n-1} \left(\sum_{\varrho=0}^{j} (-1_K)^{\varrho} s_j t_{j-\varrho}\right) \mathsf{X}^{n-j-1}. \end{aligned} \tag{10.39}$$

Συγκρίνοντας τους συντελεστές τού X^{n-j-1} στις δύο εκφράσεις (10.39) και (10.37) τού πολυωνύμου $\mathcal{D}(\hat{\varphi}(\mathsf{X}))$ για $j = k = 1, \ldots, n-1$ καταλήγουμε στη σχέση

$$\sum_{\varrho=0}^{k-1} (-1_K)^{\varrho} s_k t_{k-\varrho} + (-1_K)^k n s_k = (-1_K)^k\,(n-k)\,s_k,$$

από την οποία έπεται η (10.34) για $k \leqslant n-1$. Το ότι η (10.34) είναι αληθής *και* για $k = n$ είναι πρόδηλο από ό,τι απεδείχθη στην πρώτη περίπτωση. □

10.4.10 Σημείωση. Μια ελαφρά παραλλαγή τής αποδείξεως τής (10.34) έχει ως εξής: Αντί να εκκινήσουμε από την

$$\sum_{k=0}^{n}(-1_K)^k s_k \mathsf{X}^{n-k} = (\mathsf{X}-\lambda_1)\cdots(\mathsf{X}-\lambda_n), \tag{10.40}$$

εκκινούμε από την

$$\sum_{k=0}^{n}(-1_K)^k s_k \mathsf{X}^{k} = (1_K-\lambda_1\mathsf{X})\cdots(1_K-\lambda_n\mathsf{X}) \tag{10.41}$$

(η οποία αποδεικνύεται είτε επαγωγικώς είτε μέσω[9] τής (10.40)). Επίτυπη παραγώγιση των μελών τής (10.41) δίδει

$$\sum_{k=1}^{n}(-1_K)^k k s_k \mathsf{X}^{k-1} = \sum_{i=1}^{n}(-\lambda_i)\prod_{l\in\{1,\ldots,n\}\smallsetminus\{i\}}(1_K-\lambda_l\mathsf{X})$$

και (κατόπιν πολλαπλασιασμού αμφοτέρων των μελών με X)

$$\begin{aligned}
&\sum_{k=1}^{n}(-1_K)^k k s_k \mathsf{X}^{k} = -\sum_{i=1}^{n}(\lambda_i\mathsf{X})\prod_{l\in\{1,\ldots,n\}\smallsetminus\{i\}}(1_K-\lambda_l\mathsf{X})\\
&= -\left(\sum_{i=1}^{n}(\lambda_i\mathsf{X})(1_K-(\lambda_i\mathsf{X}))^{-1}\right)\prod_{l=1}^{n}(1_K-\lambda_l\mathsf{X})\\
&= -\left(\sum_{i=1}^{n}\sum_{j=1}^{\infty}(\lambda_i\mathsf{X})^j\right)\prod_{l=1}^{n}(1_K-\lambda_l\mathsf{X})\\
&= -\left(\sum_{j=1}^{\infty}\left(\sum_{i=1}^{n}\lambda_i^j\right)\mathsf{X}^j\right)\left(\sum_{l=0}^{n}(-1_K)^l s_l\mathsf{X}^l\right)\\
&= \left(\sum_{j=1}^{\infty}t_j\mathsf{X}^j\right)\left(\sum_{l=0}^{n}(-1_K)^{l-1}s_l\mathsf{X}^l\right).
\end{aligned}$$

(Στη δεύτερη και στην τρίτη ισότητα χρησιμοποιήσαμε το ότι η επίτυπη δυναμοσειρά $\sum_{j=0}^{\infty}(\lambda_i\mathsf{X})^j$ είναι αντιστρέψιμη εντός τής ακεραίας περιοχής $K[\![\mathsf{X}]\!]$, έχουσα ως αντίστροφό της το $1_K-(\lambda_i\mathsf{X})$, οπότε

$$(\lambda_i\mathsf{X})(1_K-(\lambda_i\mathsf{X}))^{-1} = \textstyle\sum_{j=1}^{\infty}(\lambda_i\mathsf{X})^j.$$

Πρβλ. εδ. 6.3.12 (i).) Η (10.34) προκύπτει άμεσα από το ότι ο συντελεστής τού X^k, $k\in\{1,\ldots,n\}$, στο γινόμενο

$$\left(\sum_{j=1}^{\infty}t_j\mathsf{X}^j\right)\left(\sum_{l=0}^{n}(-1_K)^{l-1}s_l\mathsf{X}^l\right) = (t_1\mathsf{X}+t_2\mathsf{X}^2+\cdots)(-1_K+s_1\mathsf{X}-s_2\mathsf{X}^2+\cdots)$$

είναι ίσος με $\sum_{\varrho=1}^{k}(-1_K)^{k-\varrho-1}t_\varrho s_{k-\varrho}$.

10.4.11 Πόρισμα (Τύποι των Girard και Newton II). *Έστω* $\varphi(\mathsf{X})=\sum_{i=0}^{n}a_i\mathsf{X}^i\in K[\mathsf{X}]$ *ένα πολυώνυμο βαθμού* $n\geqslant 1$ *το οποίο διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού* K. *Εάν οι θέσεις μηδενισμού του είναι τα (όχι κατ' ανάγκην σαφώς διακεκριμένα) στοιχεία* $\lambda_1,\ldots,\lambda_n\in K$, *τότε για οιονδήποτε* $k\in\mathbb{N}$ *ισχύει η σχέση*

$$\boxed{a_nt_k+a_{n-1}t_{k-1}+a_{n-2}t_{k-2}+\cdots+a_0t_{k-n}=0_K,} \tag{10.42}$$

[9] Εν προκειμένω, μπορεί να εφαρμοσθεί το ακόλουθο *κλασικό τέχνασμα*: Η (10.40) εξακολουθεί να ισχύει αν το X αντικατασταθεί με το $\frac{1}{\mathsf{X}}$, ήτοι με το αντίστροφο τού X εντός τού σώματος κλασμάτων $K(\mathsf{X}):=\mathbf{Fr}(K[\mathsf{X}])$ τής ακεραίας περιοχής $K[\mathsf{X}]$ (Βλ. εδ. 10.6.1). Πολλαπλασιάζοντας λοιπόν (ύστερα από αυτήν την αντικατάσταση) αμφότερα τα μέλη τής προκύπτουσας ισότητας με X^n λαμβάνουμε την (10.41).

όταν $k \geqslant n$, *και η σχέση*

$$\boxed{a_n t_k + a_{n-1} t_{k-1} + a_{n-2} t_{k-2} + \cdots + a_{n-k+1} t_1 + k a_{n-k} = 0_K,} \tag{10.43}$$

όταν $1 \leqslant k \leqslant n$, *όπου τα* $t_1, t_2, \ldots$ *είναι τα αθροίσματα* (10.32).

ΑΠΟΔΕΙΞΗ. Η (10.42) (και αντιστοίχως, η (10.43)) έπεται άμεσα από τις σχέσεις (10.33) και (10.29) (και αντιστοίχως, από τις (10.34) και (10.29)). □

▸ **Σώματα διασπάσεως**. Για να μετατρέψει κανείς δοθέν $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ που δεν διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού K σε διασπώμενο (ούτως ώστε να είναι σε θέση να εκμεταλλευθεί τις προαναφερθείσες όμορφες ιδιότητες των διασπώμενων) αρκεί να επεκτείνει καταλλήλως το σώμα αναφοράς K εφαρμόζοντας το θεώρημα 10.4.12 τού Leopold Kronecker (1823-1891) (και το συνακόλουθό του 10.4.15 που το ισχυροποιεί[10]).

10.4.12 Θεώρημα (Kronecker, 1887). *Για οιοδήποτε* $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ *βαθμού* $\geqslant 1$ *υφίσταται κάποια επέκταση* L *τού* K, *υπεράνω τής οποίας το* $\varphi(\mathsf{X})$ *διασπάται σε πρωτοβάθμιους παράγοντες.*

10.4.13 Ορισμός. Έστω $\varphi(\mathsf{X}) \in K[\mathsf{X}]$. Μια επέκταση L τού K καλείται **σώμα διασπάσεώς** του όταν το $\varphi(\mathsf{X})$

(i) διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω αυτής και

(ii) δεν διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω οιουδήποτε γνησίου υποσώματός της.

Η συνθήκη (ii) μπορεί να αντικατασταθεί με την ακόλουθη:

(ii)′ Εάν οι $\lambda_1, \ldots, \lambda_n$ είναι οι (όχι κατ' ανάγκην σαφώς διακεκριμένες) θέσεις μηδενισμού τού $\varphi(\mathsf{X})$ εντός τού L, τότε $L = K(\lambda_1, \ldots, \lambda_n)$.

10.4.14 Παραδείγματα. (i) Το $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\} \subsetneq \mathbb{R}$ αποτελεί σώμα διασπάσεως τού

$$\varphi(\mathsf{X}) := \mathsf{X}^2 - 2 \in \mathbb{Q}[\mathsf{X}],$$

διότι

$$\varphi(\mathsf{X}) = (\mathsf{X} - \sqrt{2})(\mathsf{X} - (-\sqrt{2})) \in \mathbb{Q}(\sqrt{2}), \;\; \mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2}).$$

Σημειωτέον ότι *και* το $\psi(\mathsf{X}) := \mathsf{X}^4 - 2\mathsf{X}^3 - 3\mathsf{X}^2 + 4\mathsf{X} + 2 \in \mathbb{Q}[\mathsf{X}]$ έχει το $\mathbb{Q}(\sqrt{2})$ ως (ένα) σώμα διασπάσεώς του, διότι

$$\psi(\mathsf{X}) = (\mathsf{X} - \sqrt{2})(\mathsf{X} - (-\sqrt{2}))(\mathsf{X} - (1 + \sqrt{2}))(\mathsf{X} - (1 - \sqrt{2}))$$

και $1 \pm \sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

(ii) Το πολυώνυμο

$$\theta(\mathsf{X}) := (\mathsf{X}^2 - 2)(\mathsf{X}^2 + 1) \in \mathbb{Q}[\mathsf{X}]$$

διαθέτει δύο θέσεις μηδενισμού εντός τού $\mathbb{Q}(\sqrt{2})$ αλλά δεν διασπάται *πλήρως* σε πρωτοβάθμιους παράγοντες υπεράνω αυτού. Άρα το $\mathbb{Q}(\sqrt{2})$ δεν είναι σώμα διασπάσεως τού $\theta(\mathsf{X})$. Ένα σώμα διασπάσεώς του είναι το

$$\mathbb{Q}(\sqrt{2}, i) \subsetneq \mathbb{C}$$

(όπου i η φανταστική μονάδα). Από την άλλη μεριά, παρότι το $\theta(\mathsf{X})$ διασπάται σε πρωτοβάθμιους παράγοντες *και* υπεράνω τού $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt[3]{2}, i)$, αυτό το σώμα δεν αποτελεί σώμα διασπάσεώς του (διότι περιέχει πλεονάζοντα στοιχεία και δεν πληροί, ως εκ τούτου, τη συνθήκη 10.4.13 (ii)′).

[10] Οι αποδείξεις αυτών των θεωρημάτων παραλείπονται, καθώς ανήκουν στη Θεωρία Σωμάτων.

10.4.15 Θεώρημα. *Κάθε πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ βαθμού $\geqslant 1$ διαθέτει (τουλάχιστον ένα) σώμα διασπάσεως. Επιπροσθέτως, για δυο σώματα διασπάσεως L_1, L_2 ενός πολυωνύμου $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ βαθμού $\geqslant 1$ υφίσταται πάντοτε ένας ισομορφισμός σωμάτων $f : L_1 \longrightarrow L_2$ με $f|_K = \mathrm{id}_K$.*

▸ **Αλγεβρικώς κλειστά σώματα**. Η έννοια τού σώματος διασπάσεως ορίζεται για ένα (και μόνον) δοθέν (μη σταθερό) πολυώνυμο. Ωστόσο, υπάρχουν κάποια ειδικής φύσεως σώματα K, τα λεγόμενα *αλγεβρικώς κλειστά σώματα,* υπεράνω των οποίων *κάθε* $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ βαθμού $\geqslant 1$ διασπάται σε πρωτοβάθμιους παράγοντες.

10.4.16 Θεώρημα. *Δοθέντος ενός σώματος K, οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Κάθε πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ βαθμού $n \geqslant 1$ διαθέτει τουλάχιστον μία θέση μηδενισμού ανήκουσα στο K.*

(ii) *Κάθε πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ βαθμού $n \geqslant 1$ διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού K.*

(iii) *Κάθε ανάγωγο πολυώνυμο υπεράνω τού K έχει βαθμό* 1.

Απόδειξη. (i)⇒(ii) Έστω $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ τυχόν πολυώνυμο βαθμού $n \geqslant 1$. Κατά την υπόθεσή μας, το $\varphi(\mathsf{X})$ διαθέτει τουλάχιστον μία θέση μηδενισμού ανήκουσα στο K. Εάν τα $\lambda_1, \ldots, \lambda_k \in K$ ($k \in \mathbb{N},\ k \leqslant n$) είναι (όλες) οι σαφώς διακεκριμένες θέσεις μηδενισμού του εντός τού K, τότε (σύμφωνα με το λήμμα 10.4.2) υπάρχει πολυώνυμο $\psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$, τέτοιο ώστε το $\varphi(\mathsf{X})$ να γράφεται υπό τη μορφή

$$\varphi(\mathsf{X}) = \left(\prod_{i=1}^{k} (\mathsf{X} - \lambda_i)^{m_i} \right) \psi(\mathsf{X}),$$

όπου $m_i = \mathrm{mult}(\varphi(\mathsf{X}); \lambda_i)$, $\psi(\lambda_i) \neq 0_K$, $\forall i \in \{1, \ldots, k\}$, και

$$\sum_{i=1}^{k} m_i \leqslant n.$$

Εάν ο βαθμός τού $\psi(\mathsf{X})$ ήταν $\geqslant 1$, τότε σύμφωνα με την υπόθεσή μας (για το $\psi(\mathsf{X})$!) θα υπήρχε τουλάχιστον μία θέση μηδενισμού $\lambda \in K$ τού $\psi(\mathsf{X})$. Αυτή θα ήταν θέση μηδενισμού *και* τού $\varphi(\mathsf{X})$, οπότε θα είχαμε $\lambda = \lambda_{i_0}$ για κάποιον $i_0 \in \{1, \ldots, k\}$, ήτοι κάτι που θα ήταν αδύνατο. Τούτο σημαίνει ότι $\deg(\psi(\mathsf{X})) = 0$, δηλαδή ότι το $\psi(\mathsf{X})$ είναι σταθερό και $\sum_{i=1}^{k} m_i = n$. Άρα το $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού K.

(ii)⇒(iii) Έστω $\theta(\mathsf{X})$ τυχόν ανάγωγο πολυώνυμο υπεράνω τού K. Σύμφωνα με την υπόθεσή μας υπάρχουν $\lambda_1, \ldots, \lambda_n \in K$, τέτοια ώστε να ισχύει η ισότητα

$$\theta(\mathsf{X}) = c\,(\mathsf{X} - \lambda_1)(\mathsf{X} - \lambda_2) \cdots (\mathsf{X} - \lambda_n)$$

για κάποιο $c \in K \setminus \{0_K\}$. Από την ιδιότητα τής μοναδικότητας τής παραστάσεώς του ως γινομένου αναγώγων μονικών πολυωνύμων (την περιγραφόμενη στο θεώρημα 10.3.8) συνάγεται ότι $n = 1$, οπότε $\deg(\theta(\mathsf{X})) = 1$.

(iii)⇒(i) Έστω $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ τυχόν πολυώνυμο βαθμού $n \geqslant 1$. Υποθέτουμε ότι

$$\varphi(\mathsf{X}) = c \prod_{\nu=1}^{r} \theta_\nu(\mathsf{X})$$

είναι η παράστασή του ως γινομένου αναγώγων μονικών πολυωνύμων (όπου $r \in \mathbb{N}$, $c \in K \setminus \{0_K\}$). Σύμφωνα με την υπόθεσή μας, καθένα εκ των $\theta_\nu(\mathsf{X})$, $\nu \in \{1, \ldots, r\}$, έχει βαθμό 1 και, ως εκ τούτου, (ακριβώς) μία θέση μηδενισμού εντός τού K. Επειδή $r \geqslant 1$, το $\varphi(\mathsf{X})$ διαθέτει τουλάχιστον μία θέση μηδενισμού ανήκουσα στο K. □

10.4.17 Ορισμός. Ένα σώμα K καλείται **αλγεβρικώς κλειστό** όταν πληροί μία (και, κατ' επέκταση, και τις τρεις) εκ των συνθηκών τού θεωρήματος 10.4.16.

10.4.18 Πρόταση. *Εάν το K είναι ένα σώμα αλγεβρικώς κλειστό, τότε (το υποκείμενο σύνολό του) είναι κατ' ανάγκην απειροσύνολο.*

Απόδειξη. Έστω $K = \{a_1, \ldots, a_q\}$ ένα πεπερασμένο σώμα. Εάν υποθέσουμε ότι το K είναι αλγεβρικώς κλειστό, τότε καταλήγουμε σε άτοπο, καθότι το πολυώνυμο

$$\varphi(\mathsf{X}) := (\mathsf{X} - a_1)(\mathsf{X} - a_2)\cdots(\mathsf{X} - a_q) + 1_K \in K\,[\mathsf{X}]$$

δεν διαθέτει καμία θέση μηδενισμού ανήκουσα στο K. □

10.4.19 Θεώρημα (Θεμελιώδες Θεώρημα τής Άλγεβρας). *Το σώμα $\mathbb{C}$ των μιγαδικών αριθμών είναι αλγεβρικώς κλειστό.*

Το θεώρημα 10.4.19 πρωτοαπεδείχθη το έτος 1799 από τον μέγα Γερμανό μαθηματικό C.-F. Gauss· εν τω μεταξύ υπάρχουν πολλές δεκάδες πιο σύγχρονων αποδείξεων, οι γνωστότερες των οποίων προέρχονται από τη Μιγαδική Ανάλυση, την Άλγεβρα και την Αλγεβρική Τοπολογία. Για περισσότερες πληροφορίες και σύντομες ιστορικές σημειώσεις ο ενδιαφερόμενος αναγνώστης παραπέμπεται στο σύγγραμμα των B. Fine και G. Rosenberger: *Το Θεμελιώδες Θεώρημα τής Άλγεβρας* (σε μετάφραση των Φ. Λιούτση και N. Μαρμαρίδη), εκδόσεις Leader Books, Αθήνα, 2001.

10.4.20 Σημείωση. (i) Στις παραδόσεις τής Αφηρημένης Άλγεβρας αποδεικνύεται ότι *κάθε σώμα K διαθέτει μια αλγεβρικώς κλειστή επέκταση* και μάλιστα ότι υπάρχει μια (μέχρις ισομορφισμού σωμάτων μονοσημάντως ορισμένη) *ελαχίστη* (τέτοιου είδους) *επέκταση* $\overline{K}$ τού K, η οποία καλείται **αλγεβρική θήκη** (ή **αλγεβρικό έγκλεισμα**) τού K. Πολλές φορές, δοθέντος ενός $\varphi(\mathsf{X}) \in K\,[\mathsf{X}]$ βαθμού $n \geqslant 1$ (όπου K *τυχόν* σώμα), είναι αρκετό το να εργαζόμαστε με την αλγεβρική θήκη $\overline{K}$ τού K αντί να αναζητούμε το σώμα διασπάσεώς του. Επειδή το $\varphi(\mathsf{X}) \in K\,[\mathsf{X}] \subseteq \overline{K}\,[\mathsf{X}]$ μπορεί να εκληφθεί ως πολυώνυμο τού $\overline{K}\,[\mathsf{X}]$, διασπάται πάντοτε σε πρωτοβάθμιους παράγοντες υπεράνω τού $\overline{K}$ (κάτι που είθισται να χρησιμοποιείται ευρέως κατά την επιχειρηματολογία που εφαρμόζεται σε ποικίλες αποδεικτικές τεχνικές).

(ii) Επειδή η αλγεβρική θήκη τού σώματος $\mathbb{R}$ είναι το $\mathbb{C}$, *κάθε* $\varphi(\mathsf{X}) \in \mathbb{R}\,[\mathsf{X}] \subseteq \mathbb{C}\,[\mathsf{X}]$ βαθμού $n \geqslant 1$, εκλαμβανόμενο ως πολυώνυμο τού $\mathbb{C}\,[\mathsf{X}]$, διασπάται πάντοτε σε πρωτοβάθμιους παράγοντες υπεράνω τού $\mathbb{C}$.

10.5 ΠΟΛΥΩΝΥΜΑ ΜΕ ΠΡΑΓΜΑΤΙΚΟΥΣ ΣΥΝΤΕΛΕΣΤΕΣ

Δύο σημαντικές ιδιότητες των πολυωνύμων με πραγματικούς συντελεστές περιγράφονται στις προτάσεις 10.5.2 και 10.5.3.

10.5.1 Λήμμα. *Έστω $\varphi(\mathsf{X}) \in \mathbb{R}\,[\mathsf{X}]$ ένα πολυώνυμο βαθμού $n > 1$. Εάν ο μιγαδικός αριθμός $z = a + ib \in \mathbb{C}$ είναι μια θέση μηδενισμού τού $\varphi(\mathsf{X})$, τότε το ίδιο ισχύει και για τον συζυγή του $\overline{z} = a - ib$. Επιπροσθέτως, εάν $z \in \mathbb{C} \setminus \mathbb{R}$, τότε*

$$\mathsf{mult}(\varphi(\mathsf{X}); z) = \mathsf{mult}(\varphi(\mathsf{X}); \overline{z}).$$

Απόδειξη. Εάν $\varphi(\mathsf{X}) = a_0 + a_1\mathsf{X} + \cdots + a_n\mathsf{X}^n$ και $\varphi(z) = 0$, τότε

$$\begin{aligned} 0 = \overline{\varphi(z)} \;&= \overline{a_0 + a_1 z + \cdots + a_n z^n} = \overline{a_0} + \overline{a_1 z} + \cdots + \overline{a_n z^n} \\ &= \overline{a_0} + \overline{a_1}\,\overline{z} + \cdots + \overline{a_n}\,\overline{z^n} = a_0 + a_1\,\overline{z} + \cdots + a_n\,\overline{z}^n = \varphi(\overline{z}), \end{aligned}$$

οπότε και ο συζυγής $\overline{z}$ τού z αποτελεί μια θέση μηδενισμού τού $\varphi(\mathsf{X})$. Εάν

$$m := \mathrm{mult}(\varphi(\mathsf{X}); z), \quad m' := \mathrm{mult}(\varphi(\mathsf{X}); \overline{z})$$

και $b \neq 0$, τότε (σύμφωνα με την πρόταση 10.2.14 και το λήμμα 10.4.1)

$$\exists \psi(\mathsf{X}) \in \mathbb{C}[\mathsf{X}] \setminus \{0_{\mathbb{C}[\mathsf{X}]}\} : \varphi(\mathsf{X}) = (\mathsf{X} - z)^m \, (\mathsf{X} - \overline{z})^{m'} \, \psi(\mathsf{X})$$

με $\psi(z) \neq 0$ και $\psi(\overline{z}) \neq 0$. Ας υποθέσουμε ότι $m > m'$. Τότε

$$\varphi(\mathsf{X}) = (\mathsf{X} - (a+ib))^m \, (\mathsf{X} - (a-ib))^{m'} \, \psi(\mathsf{X}) = \big((\mathsf{X}-a)^2 + b^2\big)^{m'} \, \gamma(\mathsf{X}),$$

όπου το $\gamma(\mathsf{X}) := (\mathsf{X} - (a+ib))^{m-m'} \, \psi(\mathsf{X})$ (ως πηλίκο δύο πολυωνύμων με πραγματικούς συντελεστές) ανήκει στον $\mathbb{R}[\mathsf{X}]$ και έχει τον $z = a + ib$ ως μια θέση μηδενισμού του. Άρα, σύμφωνα με την ήδη αποδειχθείσα ιδιότητα, θα δέχεται ως θέση μηδενισμού του και τον συζυγή του $\overline{z} = a - ib$, οπότε

$$\gamma(\overline{z}) = \gamma(a - ib) = (-2bi)^{m-m'} \, \psi(\overline{z}) = 0.$$

Τούτο είναι αδύνατον, καθόσον $b \neq 0$ και $\psi(\overline{z}) \neq 0$. Με τον ίδιο τρόπο αποδεικνύεται ότι δεν μπορεί να ισχύει ούτε η ανισότητα $m < m'$. Άρα $m = m'$. □

10.5.2 Πρόταση. *Κάθε πολυώνυμο $\varphi(\mathsf{X}) \in \mathbb{R}[\mathsf{X}]$ περιττού βαθμού διαθέτει (τουλάχιστον) μία πραγματική θέση μηδενισμού.*

Αποδειξη πρωτη (ανεξάρτητη τού 10.4.19). Έστω $\varphi(\mathsf{X}) \in \mathbb{R}[\mathsf{X}]$ τυχόν πολυώνυμο βαθμού $n = 2k+1$, $k \in \mathbb{N}_0$. Αυτό μπορεί να θεωρηθεί ως πραγματική συνεχής συνάρτηση

$$\varphi : \mathbb{R} \longrightarrow \mathbb{R}, \, x \longmapsto \varphi(x) := a_0 + a_1 x + \cdots + a_n x^n.$$

(Πρβλ. εδ. 6.3.13 και 10.2.9.) Δίχως βλάβη τής γενικότητας υποθέτουμε ότι $a_n > 0$. (Όταν $a_n < 0$, η απόδειξη είναι πανομοιότυπη.) Παρατηρούμε ότι

$$\lim_{n \longrightarrow -\infty} \varphi(x) = \lim_{n \longrightarrow -\infty} (a_n x^n) = -\infty, \quad \lim_{n \longrightarrow \infty} \varphi(x) = \lim_{n \longrightarrow \infty} (a_n x^n) = \infty$$

(διότι $a_n > 0$ και ο n είναι περιττός). Άρα υπάρχουν κάποιοι $x_1, x_2 \in \mathbb{R}$, $x_1 < x_2$, τέτοιοι ώστε να ισχύει $\varphi(x_1) < 0$ και $\varphi(x_2) > 0$. Σύμφωνα με το *θεώρημα τής ενδιάμεσης τιμής*[11],

$$\exists \xi \in \mathbb{R} : x_1 < \xi < x_2 \ \text{ και } \ \varphi(\xi) = 0.$$

Αποδειξη δευτερη. Έστω $\varphi(\mathsf{X}) \in \mathbb{R}[\mathsf{X}]$ τυχόν πολυώνυμο βαθμού $n = 2k+1$, $k \in \mathbb{N}_0$. Εάν $k = 0$, τότε $\varphi(\mathsf{X}) = a\mathsf{X} + b$ για κάποιους $a \in \mathbb{R} \setminus \{0\}$, $b \in \mathbb{R}$, έχον τον πραγματικό αριθμό $-a^{-1}b$ ως (μοναδική) θέση μηδενισμού. Ας υποθέσουμε ότι ο ισχυρισμός είναι αληθής για πολυώνυμα (με πραγματικούς συντελεστές) βαθμού $2k+1$ για κάποιον $k \geqslant 0$ και ότι το $\varphi(\mathsf{X})$ έχει βαθμό $2(k+1)+1$. Κατά το Θεμελιώδες Θεώρημα τής Άλγεβρας 10.4.19, $\exists z \in \mathbb{C} : \varphi(z) = 0$. Κατά το λήμμα 10.5.1 ο συζυγής $\overline{z}$ τού z θα αποτελεί μια μιγαδική θέση μηδενισμού τού $\varphi(\mathsf{X})$. Θεωρώντας τό $\varphi(\mathsf{X})$ ως πολυώνυμο τού $\mathbb{C}[\mathsf{X}]$, λαμβάνουμε

$$\mathsf{X} - z \mid \varphi(\mathsf{X}) \ \text{ και } \ \mathsf{X} - \overline{z} \mid \varphi(\mathsf{X}),$$

οπότε (δυνάμει τού πορίσματος 10.2.5 και τού ότι $z \neq \overline{z}$, αφού $z \in \mathbb{C} \setminus \mathbb{R}$)

$$(\mathsf{X} - z)\,(\mathsf{X} - \overline{z}) \mid \varphi(\mathsf{X}). \tag{10.44}$$

[11] **Θεώρημα τής ενδιάμεσης τιμής**: Εάν $\varphi : [x_1, x_2] \longrightarrow \mathbb{R}$ είναι μια συνεχής συνάρτηση με $\varphi(x_1) < \varphi(x_2)$ και $y \in \mathbb{R}$, $\varphi(x_1) < y < \varphi(x_2)$, τότε $\exists \xi \in \mathbb{R} : x_1 < \xi < x_2$ και $\varphi(\xi) = y$.

Όμως το

$$(\mathsf{X}-z)\,(\mathsf{X}-\overline{z}) = \mathsf{X}^2 - (z+\overline{z})\,\mathsf{X} + z\overline{z}$$

έχει πραγματικούς συντελεστές, διότι -ως γνωστόν- τόσον το άθροισμα $z+\overline{z}$ όσον και το γινόμενο $z\overline{z}$ δυο συζυγών μιγαδικών αριθμών είναι ένας πραγματικός αριθμός. Άρα

$$\exists \varpi(\mathsf{X}) \in \mathbb{R}\,[\mathsf{X}] \smallsetminus \{0_{\mathbb{R}[\mathsf{X}]}\} : \varphi(\mathsf{X}) = \varpi(\mathsf{X})\,\underbrace{(\mathsf{X}^2 - (z+\overline{z})\,\mathsf{X} + z\overline{z})}_{\in \mathbb{R}[\mathsf{X}]\smallsetminus\{0_{\mathbb{R}[\mathsf{X}]}\}}.$$

(Παρά το γεγονός ότι η διαίρεση (10.44) εκτελείται *εντός τού* $\mathbb{C}\,[\mathsf{X}]$, το πηλίκο $\varpi(\mathsf{X})$ έχει κατ' ανάγκην *πραγματικούς* συντελεστές, καθόσον δεν αλλάζει τίποτα εάν αυτή εκτελεσθεί *εντός τού* $\mathbb{R}\,[\mathsf{X}]$. Βλ. την απόδειξη τής προτάσεως 10.1.11 για τα σώματα $K=\mathbb{R}$ και $L=\mathbb{C}$.) Επειδή

$$\deg(\varpi(\mathsf{X})) = 2k+1,$$

το $\varpi(\mathsf{X})$ (σύμφωνα με την επαγωγική υπόθεσή μας) διαθέτει (τουλάχιστον) μία πραγματική θέση μηδενισμού. Άρα *και* το $\varphi(\mathsf{X})$ διαθέτει (τουλάχιστον) μία πραγματική θέση μηδενισμού και ο ισχυρισμός είναι αληθής.

Απόδειξη τρίτη. Έστω $\varphi(\mathsf{X}) \in \mathbb{R}\,[\mathsf{X}]$ τυχόν πολυώνυμο περιττού βαθμού n. Κατά το Θεμελιώδες Θεώρημα τής Άλγεβρας 10.4.19 αυτό διαθέτει (εν συνόλω, προσμετρουμένων και των τυχόν πολλαπλών εμφανίσεώς τους) n μιγαδικές θέσεις μηδενισμού $z_1,\ldots,z_n$. Μάλιστα, σύμφωνα με το δεύτερο μέρος τού λήμματος 10.5.1, $\operatorname{card}(\{\,z\in\mathbb{C}\smallsetminus\mathbb{R} \mid \varphi(z)=0\}) \in 2\mathbb{Z}$. Άρα η διάσπαση τού $\varphi(\mathsf{X})$ σε πρωτοβάθμιους παράγοντες υπεράνω τού $\mathbb{C}$ είναι κατ' ανάγκην τής μορφής

$$\varphi(\mathsf{X}) = c\left(\prod_{z\in\mathcal{A}\cap(\mathbb{C}\smallsetminus\mathbb{R})}(\mathsf{X}-z)\right)\left(\prod_{z\in\mathcal{A}\cap\mathbb{R}}(\mathsf{X}-z)\right),$$

όπου $c\in\mathbb{C}\smallsetminus\{0\}$ και $\mathcal{A} := \{z_1,\ldots,z_n\}$. Επειδή ο n είναι περιττός και

$$\deg\left(\prod_{z\in\mathcal{A}\cap(\mathbb{C}\smallsetminus\mathbb{R})}(\mathsf{X}-z)\right) \in 2\mathbb{Z},$$

έχουμε κατ' ανάγκην $\operatorname{card}(\mathcal{A}\cap\mathbb{R}) \geqslant 1$. □

10.5.3 Πρόταση (Ανάγωγα πολυώνυμα με πραγματικούς συντελεστές). *Ένα πολυώνυμο $\varphi(\mathsf{X}) \in \mathbb{R}\,[\mathsf{X}]$ είναι ανάγωγο υπεράνω τού $\mathbb{R}$ εάν και μόνον εάν είναι τής μορφής*

$$\begin{cases} \varphi(\mathsf{X}) = a\mathsf{X}+b, & \text{όπου } a\in\mathbb{R}\smallsetminus\{0\}, \text{ ή} \\ \varphi(\mathsf{X}) = a\mathsf{X}^2+b\mathsf{X}+c, & \text{όπου } a,b,c\in\mathbb{R} \text{ με } b^2-4ac<0. \end{cases}$$

Απόδειξη. Εάν $\varphi(\mathsf{X}) = a\mathsf{X}+b$, όπου $a\neq 0$, τότε το $\varphi(\mathsf{X})$ είναι προφανώς ανάγωγο υπεράνω τού $\mathbb{R}$. Ένα πολυώνυμο τής μορφής $\varphi(\mathsf{X}) = a\mathsf{X}^2+b\mathsf{X}+c$ είναι ανάγωγο υπεράνω τού $\mathbb{R}$ (βλ. την πρόταση 10.3.4) εάν και μόνον εάν δεν διαθέτει καμία πραγματική θέση μηδενισμού. Αλλά τούτο ισοδυναμεί με το ότι η διακρίνουσα b^2-4ac είναι αρνητική. Επομένως, για την αποπεράτωση τής αποδείξεως αρκεί να διαπιστώσουμε ότι δεν υπάρχουν ανάγωγα πολυώνυμα $\varphi(\mathsf{X})\in\mathbb{R}\,[\mathsf{X}]$ βαθμού $\geqslant 3$ υπεράνω τού $\mathbb{R}$. Ας υποθέσουμε ότι ένα τέτοιου είδους ανάγωγο πολυώνυμο $\varphi(\mathsf{X})$ υπάρχει. Βάσει τού Θεμελιώδους Θεωρήματος τής Άλγεβρας το $\varphi(\mathsf{X})$ θα διαθέτει (τουλάχιστον) μία θέση μηδενισμού $z\in\mathbb{C}$. Προφανώς, $z\notin\mathbb{R}$, διότι αλλιώς το $\varphi(\mathsf{X})$

δεν θα είναι ανάγωγο υπεράνω τού $\mathbb{R}$. Κατά το λήμμα 10.5.1 ο συζυγής $\overline{z}$ τού z θα αποτελεί θέση μηδενισμού τού $\varphi(\mathsf{X})$. Θεωρώντας τό $\varphi(\mathsf{X})$ ως πολυώνυμο τού $\mathbb{C}[\mathsf{X}]$, λαμβάνουμε

$$\mathsf{X}-z \mid \varphi(\mathsf{X}) \ \text{ και } \ \mathsf{X}-\overline{z} \mid \varphi(\mathsf{X}),$$

οπότε (δυνάμει τού πορίσματος 10.2.5 και τού ότι $z \neq \overline{z}$, αφού $z \in \mathbb{C}\setminus\mathbb{R}$)

$$(\mathsf{X}-z)\,(\mathsf{X}-\overline{z}) \mid \varphi(\mathsf{X}).$$

Όμως το $(\mathsf{X}-z)\,(\mathsf{X}-\overline{z}) = \mathsf{X}^2 - (z+\overline{z})\,\mathsf{X} + z\overline{z}$ έχει πραγματικούς συντελεστές. Άρα το $\varphi(\mathsf{X})$ δεν είναι ανάγωγο υπεράνω τού $\mathbb{R}$. Άτοπο! □

10.5.4 Πόρισμα. *Για κάθε πολυώνυμο $\varphi(\mathsf{X}) \in \mathbb{R}[\mathsf{X}]$ βαθμού $\geqslant 1$ υπάρχουν φυσικοί αριθμοί k, l, μη αρνητικοί ακέραιοι αριθμοί $m_1, \ldots, m_k, n_1, \ldots, n_l$ (με τουλάχιστον έναν εξ αυτών $\neq 0$), και πραγματικοί αριθμοί $b_1, \ldots, b_k, \mathrm{A}_1, \ldots, \mathrm{A}_l, \mathrm{B}_1, \ldots, \mathrm{B}_l$ και $c \neq 0$, τέτοιοι ώστε να ισχύει $\mathrm{A}_j^2 - 4\mathrm{B}_j < 0$ για κάθε $j \in \{1, \ldots, l\}$ και*

$$\varphi(\mathsf{X}) = c\left(\prod_{i=1}^{k}(\mathsf{X}+b_i)^{m_i}\right)\left(\prod_{j=1}^{l}(\mathsf{X}^2+\mathrm{A}_j\mathsf{X}+\mathrm{B}_j)^{n_j}\right). \tag{10.45}$$

Απόδειξη. Έπεται άμεσα από την πρόταση 10.5.3. Η παράσταση (10.45) αποτελεί τη συνεπτυγμένη (υπό την ευρεία έννοια) αποσύνθεση τού $\varphi(\mathsf{X})$ υπεράνω τού $\mathbb{R}$. □

10.5.5 Παράδειγμα. Εάν $\nu \in \mathbb{N}$, τότε το $\mathsf{X}^\nu - 1 \in \mathbb{R}[\mathsf{X}]$ διαθέτει ν (απλές) μιγαδικές θέσεις μηδενισμού, ήτοι τις *ν-οστές ρίζες τής μονάδας* ζ_ν^k, $k \in \{0, 1, \ldots, \nu-1\}$, όπου $\zeta_\nu := \mathbf{e}^{\frac{2\pi i}{\nu}} = \cos\left(\frac{2\pi}{\nu}\right) + i\sin\left(\frac{2\pi}{\nu}\right)$. Άρα διασπάται σε πρωτοβάθμιους παράγοντες *υπεράνω τού* $\mathbb{C}$ ως ακολούθως:

$$\mathsf{X}^\nu - 1 = \prod_{k=0}^{\nu-1}\left(\mathsf{X}-\zeta_\nu^k\right).$$

Σημειωτέον ότι $\zeta_\nu^k\overline{\zeta_\nu^k} = 1$ για κάθε $k \in \{0, 1, \ldots, \nu-1\}$ και

$$\zeta_\nu^k + \overline{\zeta_\nu^k} = \begin{cases} 2\cos\left(\frac{k\pi}{\varrho}\right), & \text{όταν } \nu = 2\varrho,\ \varrho \in \mathbb{N}, \\ 2\cos\left(\frac{2k\pi}{2\varrho+1}\right), & \text{όταν } \nu = 2\varrho+1,\ \varrho \in \mathbb{N}_0, \end{cases}$$

οπότε

$$\left(\mathsf{X}-\zeta_\nu^k\right)\left(\mathsf{X}-\overline{\zeta_\nu^k}\right) = \begin{cases} \mathsf{X}^2 - 2\cos\left(\frac{k\pi}{\varrho}\right)\mathsf{X} + 1, & \text{όταν } \nu = 2\varrho,\ \varrho \in \mathbb{N}, \\ \mathsf{X}^2 - 2\cos\left(\frac{2k\pi}{2\varrho+1}\right)\mathsf{X} + 1, & \text{όταν } \nu = 2\varrho+1,\ \varrho \in \mathbb{N}_0. \end{cases}$$

Κατά συνέπειαν, η συνεπτυγμένη αποσύνθεση (10.45) τού $\mathsf{X}^\nu - 1$ *υπεράνω τού σώματος* $\mathbb{R}$ είναι η

$$\mathsf{X}^\nu - 1 = \begin{cases} \mathsf{X}-1, & \text{όταν } \nu = 1, \\ (\mathsf{X}-1)\,(\mathsf{X}+1), & \text{όταν } \nu = 2, \\ (\mathsf{X}-1)\,(\mathsf{X}+1)\prod_{k=1}^{\varrho-1}(\mathsf{X}^2 - 2\cos\left(\frac{k\pi}{\varrho}\right)\mathsf{X}+1), & \text{όταν } \nu = 2\varrho,\ \varrho \geqslant 2, \\ (\mathsf{X}-1)\prod_{k=1}^{\varrho}(\mathsf{X}^2 - 2\cos\left(\frac{2k\pi}{2\varrho+1}\right)\mathsf{X}+1), & \text{όταν } \nu = 2\varrho+1,\ \varrho \geqslant 1. \end{cases}$$

(Ως εκ τούτου, οι *πραγματικές* θέσεις μηδενισμού αυτού είναι τα 1 και -1 όταν ο ν είναι άρτιος, και μόνον το 1 όταν ο ν είναι περιττός.)

10.6 ΠΕΡΙ ΤΟΥ ΣΩΜΑΤΟΣ ΤΩΝ ΡΗΤΩΝ ΕΚΦΡΑΣΕΩΝ

Για οιοδήποτε σώμα K οι δακτύλιοι $K[\mathsf{X}]$ και $K[\![\mathsf{X}]\!]$ είναι ακέραιες περιοχές (βλ.6.3.9 (ii)), με την πρώτη υποπεριοχή τής δεύτερης. Επομένως, ορίζονται τα *σώματα κλασμάτων* αυτών (βλ. εδ. 8.5.6 (ii) και (v))

$$\boxed{K(\mathsf{X}) := \mathbf{Fr}(K[\mathsf{X}])} \quad \text{και} \quad \boxed{K(\!(\mathsf{X})\!) := \mathbf{Fr}(K[\![\mathsf{X}]\!])}$$

(με το πρώτο υπόσωμα τού δευτέρου).

10.6.1 Ορισμός. Το σώμα $K(\mathsf{X})$ καλείται, ιδιαιτέρως, **σώμα των ρητών εκφράσεων** μιας απροσδιορίστου X υπεράνω τού K, τα δε στοιχεία του **πολυωνυμικά κλάσματα** (ή **ρητές εκφράσεις** ή **ρητές συναρτήσεις** ως προς την X). Κάθε πολυωνυμικό κλάσμα έχον ως παρονομαστή του μια δύναμη ενός ανάγωγου μονικού πολυωνύμου και ως αριθμητή του ένα πολυώνυμο βαθμού μικροτέρου τού βαθμού τού παρονομαστή του, καλείται **απλό** (ή **μερικό**) **πολυωνυμικό κλάσμα** (υπεράνω τού K).

Θα αποδείξουμε ότι *κάθε* πολυωνυμικό κλάσμα μπορεί να εκφρασθεί μονοσημάντως ως άθροισμα (πεπερασμένου πλήθους) απλών πολυωνυμικών κλασμάτων και ενός ειδικού πολυωνύμου (τού λεγομένου *ακεραίου μέρους του*).

10.6.2 Λήμμα. *Κάθε πολυωνυμικό κλάσμα* $\frac{\varphi(\mathsf{X})}{\psi(\mathsf{X})} \in K(\mathsf{X})$ *γράφεται κατά τρόπο μοναδικό υπό τη μορφή*

$$\boxed{\frac{\varphi(\mathsf{X})}{\psi(\mathsf{X})} = \varpi(\mathsf{X}) + \frac{\upsilon(\mathsf{X})}{\psi(\mathsf{X})},} \tag{10.46}$$

όπου $\varpi(\mathsf{X}), \upsilon(\mathsf{X}) \in K[\mathsf{X}]$ *με* $\deg(\upsilon(\mathsf{X})) < \deg(\psi(\mathsf{X}))$. *Η μοναδικότητα, μάλιστα, αυτή διατηρείται και υπό την ακόλουθη ευρύτερη έννοια*: *Εάν*

$$\frac{\varphi(\mathsf{X})}{\psi(\mathsf{X})} = \varpi'(\mathsf{X}) + \frac{\upsilon'(\mathsf{X})}{\psi'(\mathsf{X})}, \tag{10.47}$$

όπου $\varpi'(\mathsf{X}), \upsilon'(\mathsf{X}) \in K[\mathsf{X}], \psi'(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$, *με* $\deg(\upsilon'(\mathsf{X})) < \deg(\psi'(\mathsf{X}))$, *τότε*

$$\varpi'(\mathsf{X}) = \varpi(\mathsf{X}) \ \textit{και} \ \frac{\upsilon'(\mathsf{X})}{\psi'(\mathsf{X})} = \frac{\upsilon(\mathsf{X})}{\psi(\mathsf{X})}. \tag{10.48}$$

Απόδειξη. Σύμφωνα με το θεώρημα 10.1.1 υπάρχει ένα ζεύγος μονοσημάντως ορισμένων πολυωνύμων $\varpi(\mathsf{X}), \upsilon(\mathsf{X}) \in K[\mathsf{X}]$, ούτως ώστε να ισχύει

$$\varphi(\mathsf{X}) = \varpi(\mathsf{X})\psi(\mathsf{X}) + \upsilon(\mathsf{X}), \quad \deg(\upsilon(\mathsf{X})) < \deg(\psi(\mathsf{X})).$$

Εξ αυτού έπεται η (10.46). Επιπροσθέτως, εάν ισχύει η (10.47), τότε

$$K[\mathsf{X}] \ni \varpi(\mathsf{X}) - \varpi'(\mathsf{X}) = \frac{\upsilon'(\mathsf{X})}{\psi'(\mathsf{X})} - \frac{\upsilon(\mathsf{X})}{\psi(\mathsf{X})} = \frac{\upsilon'(\mathsf{X})\psi(\mathsf{X}) - \upsilon(\mathsf{X})\psi'(\mathsf{X})}{\psi(\mathsf{X})\psi'(\mathsf{X})},$$

και από τις ανισότητες $\deg(\upsilon(\mathsf{X})) < \deg(\psi(\mathsf{X}))$ και $\deg(\upsilon'(\mathsf{X})) < \deg(\psi'(\mathsf{X}))$ προκύπτει ότι

$$\deg(\upsilon(\mathsf{X})) + \deg(\upsilon'(\mathsf{X})) < \deg(\psi(\mathsf{X})\psi'(\mathsf{X})),$$
$$\deg(\upsilon(\mathsf{X})\psi'(\mathsf{X})) + \deg(\upsilon'(\mathsf{X})\psi(\mathsf{X})) \leqslant \deg(\upsilon(\mathsf{X})) + \deg(\upsilon'(\mathsf{X})),$$
$$\deg(\upsilon'(\mathsf{X})\psi(\mathsf{X}) - \upsilon(\mathsf{X})\psi'(\mathsf{X})) \leqslant \deg(\upsilon(\mathsf{X})\psi'(\mathsf{X})) + \deg(\upsilon'(\mathsf{X})\psi(\mathsf{X})).$$

Ως εκ τούτου,

$$\left.\begin{array}{r}\psi(\mathsf{X})\psi'(\mathsf{X}) \mid \upsilon'(\mathsf{X})\psi(\mathsf{X}) - \upsilon(\mathsf{X})\psi'(\mathsf{X}) \\ \deg(\upsilon'(\mathsf{X})\psi(\mathsf{X}) - \upsilon(\mathsf{X})\psi'(\mathsf{X})) < \deg(\psi(\mathsf{X})\psi'(\mathsf{X}))\end{array}\right\} \Rightarrow \varpi(\mathsf{X}) - \varpi'(\mathsf{X}) = 0_{K[\mathsf{X}]},$$

καταλήγοντας στις ισότητες (10.48). □

10.6.3 Ορισμός. Το $\varpi(\mathsf{X})$ καλείται **ακέραιο μέρος** και το $\frac{\upsilon(\mathsf{X})}{\psi(\mathsf{X})}$ **αμιγώς κλασματικό μέρος** τού $\frac{\varphi(\mathsf{X})}{\psi(\mathsf{X})} \in K(\mathsf{X})$.

10.6.4 Θεώρημα. *Το αμιγώς κλασματικό μέρος* $\frac{\upsilon(\mathsf{X})}{\psi(\mathsf{X})}$ *οιουδήποτε πολυωνυμικού κλάσματος* (10.46) *γράφεται κατά τρόπο μοναδικό υπό τη μορφή*

$$\boxed{\frac{\upsilon(\mathsf{X})}{\psi(\mathsf{X})} = \sum_{i=1}^{k}\left(\sum_{j=1}^{m_i}\frac{\beta_{i,j}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i-j+1}}\right),} \tag{10.49}$$

όπου

$$\psi(\mathsf{X}) = c\prod_{i=1}^{k}\psi_i(\mathsf{X})^{m_i}$$

είναι η συνεπτυγμένη αποσύνθεση τού $\psi(\mathsf{X})$ (βλ. 10.3.9 (ii)) *και* $\beta_{i,j}(\mathsf{X}) \in K[\mathsf{X}]$ *πολυώνυμα με*

$$\deg(\beta_{i,j}(\mathsf{X})) < \deg(\psi_i(\mathsf{X})),\ \forall j \in \{1,\dots,m_i\} \text{ και } \forall i \in \{1,\dots,k\}.$$

Απόδειξη. **Βήμα 1ο**. *Υπάρχουν πολυώνυμα* $\alpha_1(\mathsf{X}),\dots,\alpha_k(\mathsf{X}) \in K[\mathsf{X}]$ *μονοσημάντως ορισμένα μέσω των ιδιοτήτων* $\deg(\alpha_i(\mathsf{X})) < \deg(\psi_i(\mathsf{X})^{m_i})$, $\forall i \in \{1,\dots,k\}$, *και*

$$\frac{\upsilon(\mathsf{X})}{\psi(\mathsf{X})} = \frac{c^{-1}\upsilon(\mathsf{X})}{\prod_{i=1}^{k}\psi_i(\mathsf{X})^{m_i}} = \sum_{i=1}^{k}\frac{\alpha_i(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i}}. \tag{10.50}$$

Θα χρησιμοποιήσουμε μαθηματική επαγωγή ως προς τον k. Όταν $k = 1$, αρκεί να τεθεί $\alpha_1(\mathsf{X}) := c^{-1}\upsilon(\mathsf{X})$. Όταν $k = 2$,

$$\psi_1(\mathsf{X}) \neq \psi_2(\mathsf{X}) \underset{10.3.12}{\Longrightarrow} \mu\kappa\delta(\psi_1(\mathsf{X})^{m_1}, \psi_2(\mathsf{X})^{m_2}) = 1_K$$
$$\underset{10.1.15}{\Longrightarrow} \exists\omega_1(\mathsf{X}),\omega_2(\mathsf{X}) \in K[\mathsf{X}] : \omega_1(\mathsf{X})\psi_1(\mathsf{X})^{m_1} + \omega_2(\mathsf{X})\psi_2(\mathsf{X})^{m_2} = 1_K,$$

οπότε

$$\left(c^{-1}\upsilon(\mathsf{X})\right)\omega_1(\mathsf{X})\psi_1(\mathsf{X})^{m_1} + \left(c^{-1}\upsilon(\mathsf{X})\right)\omega_2(\mathsf{X})\psi_2(\mathsf{X})^{m_2} = c^{-1}\upsilon(\mathsf{X}). \tag{10.51}$$

Εάν ισχύει $\deg(\left(c^{-1}\upsilon(\mathsf{X})\right)\omega_2(\mathsf{X})) < \deg(\psi_1(\mathsf{X})^{m_1})$, τότε θα ισχύει και η ανισότητα

$$\deg(\left(c^{-1}\upsilon(\mathsf{X})\right)\omega_1(\mathsf{X})) < \deg(\psi_2(\mathsf{X})^{m_2}),$$

διότι $\deg(c^{-1}\upsilon(\mathsf{X})) < \deg(\psi_1(\mathsf{X})^{m_1}\psi_2(\mathsf{X})^{m_2})$ και

$$\deg(\left(c^{-1}\upsilon(\mathsf{X})\right)\omega_2(\mathsf{X})\psi_2(\mathsf{X})^{m_2}) < \deg(\psi_1(\mathsf{X})^{m_1}\psi_2(\mathsf{X})^{m_2}).$$

Εν τοιαύτη περιπτώσει θέτουμε

$$\alpha_1(\mathsf{X}) := \left(c^{-1}\upsilon(\mathsf{X})\right)\omega_2(\mathsf{X}),\ \alpha_2(\mathsf{X}) := \left(c^{-1}\upsilon(\mathsf{X})\right)\omega_1(\mathsf{X}). \tag{10.52}$$

Εάν ισχύει $\deg(\big(c^{-1}\upsilon(\mathsf{X})\big)\,\omega_2(\mathsf{X})) \geqslant \deg(\psi_1(\mathsf{X})^{m_1})$, τότε

$$\exists\,\zeta(\mathsf{X}),\eta(\mathsf{X})\in K[\mathsf{X}]:\big(c^{-1}\upsilon(\mathsf{X})\big)\,\omega_2(\mathsf{X})=\zeta(\mathsf{X})\psi_1(\mathsf{X})^{m_1}+\eta(\mathsf{X})$$

με $\deg(\eta(\mathsf{X}))<\deg(\psi_1(\mathsf{X})^{m_1})$ και η (10.51) δίδει

$$\big(\big(c^{-1}\upsilon(\mathsf{X})\big)\,\omega_1(\mathsf{X})+\zeta(\mathsf{X})\psi_2(\mathsf{X})^{m_2}\big)\,\psi_1(\mathsf{X})^{m_1}+\eta(\mathsf{X})\psi_2(\mathsf{X})^{m_2}=c^{-1}\upsilon(\mathsf{X}).\quad(10.53)$$

Επειδή οι βαθμοί των $c^{-1}\upsilon(\mathsf{X})$ και $\eta(\mathsf{X})\psi_2(\mathsf{X})^{m_2}$ είναι $<\deg(\psi_1(\mathsf{X})^{m_1}\psi_2(\mathsf{X})^{m_2})$, από την (10.53) προκύπτει ότι

$$\deg(\big(c^{-1}\upsilon(\mathsf{X})\big)\,\omega_1(\mathsf{X})+\zeta(\mathsf{X})\psi_2(\mathsf{X})^{m_2})<\deg(\psi_2(\mathsf{X})^{m_2}).$$

Εν τοιαύτη περιπτώσει θέτουμε

$$\alpha_1(\mathsf{X}):=\eta(\mathsf{X}),\ \alpha_2(\mathsf{X}):=\big(c^{-1}\upsilon(\mathsf{X})\big)\,\omega_1(\mathsf{X})+\zeta(\mathsf{X})\psi_2(\mathsf{X})^{m_2}.\quad(10.54)$$

Τα (μέσω των (10.52) και (10.54)) ορισθέντα πολυώνυμα $\alpha_1(\mathsf{X}),\alpha_2(\mathsf{X})$ είναι τα μοναδικά πολυώνυμα για τα οποία ισχύει η (10.50) για $k=2$. Πράγματι· εάν

$$\frac{\upsilon(\mathsf{X})}{\psi(\mathsf{X})}=\frac{\alpha_1(\mathsf{X})}{\psi_1(\mathsf{X})^{m_1}}+\frac{\alpha_2(\mathsf{X})}{\psi_2(\mathsf{X})^{m_2}}=\frac{\alpha_1'(\mathsf{X})}{\psi_1(\mathsf{X})^{m_1}}+\frac{\alpha_2'(\mathsf{X})}{\psi_2(\mathsf{X})^{m_2}},$$

όπου $\alpha_1'(\mathsf{X}),\alpha_2'(\mathsf{X})\in K[\mathsf{X}]$ με

$$\deg(\alpha_1'(\mathsf{X}))<\deg(\psi_1(\mathsf{X})^{m_1}),\ \deg(\alpha_2'(\mathsf{X}))<\deg(\psi_2(\mathsf{X})^{m_2}),$$

τότε $\frac{\alpha_1(\mathsf{X})-\alpha_1'(\mathsf{X})}{\psi_1(\mathsf{X})^{m_1}}=\frac{\alpha_2(\mathsf{X})-\alpha_2'(\mathsf{X})}{\psi_2(\mathsf{X})^{m_2}}$, οπότε

$$\left.\begin{aligned}\psi_1(\mathsf{X})^{m_1}(\alpha_2(\mathsf{X})-\alpha_2'(\mathsf{X}))=\psi_2(\mathsf{X})^{m_2}\,(\alpha_1(\mathsf{X})-\alpha_1'(\mathsf{X}))\\ \text{μκδ}(\psi_1(\mathsf{X})^{m_1},\psi_2(\mathsf{X})^{m_2})=1_K\end{aligned}\right\}\underset{10.1.16}{\Longrightarrow}\psi_1(\mathsf{X})^{m_1}\mid\alpha_1(\mathsf{X})-\alpha_1'(\mathsf{X})$$

και

$$\left.\begin{aligned}\deg(\alpha_1(\mathsf{X}))<\deg(\psi_1(\mathsf{X})^{m_1})\\ \deg(\alpha_1'(\mathsf{X}))<\deg(\psi_1(\mathsf{X})^{m_1})\\ \deg\left(\alpha_1(\mathsf{X})-\alpha_1'(\mathsf{X})\right)\\ \leqslant\max\{\deg\left(\alpha_1(\mathsf{X})\right),\deg(\alpha_1'(\mathsf{X}))\}\end{aligned}\right\}\Longrightarrow\deg\left(\alpha_1(\mathsf{X})-\alpha_1'(\mathsf{X})\right)<\deg(\psi_1(\mathsf{X})^{m_1}).$$

Επομένως,

$$\left.\begin{aligned}\psi_1(\mathsf{X})^{m_1}\mid\alpha_1(\mathsf{X})-\alpha_1'(\mathsf{X})\\ \deg(\alpha_1(\mathsf{X})-\alpha_1'(\mathsf{X}))<\deg(\psi_1(\mathsf{X})^{m_1})\end{aligned}\right\}\Rightarrow\alpha_1(\mathsf{X})-\alpha_1'(\mathsf{X})=0_{K[\mathsf{X}]},$$

απ' όπου έπεται ότι $\alpha_1(\mathsf{X})=\alpha_1'(\mathsf{X})$ και $\alpha_2(\mathsf{X})=\alpha_2'(\mathsf{X})$. Εν συνεχεία, υποθέτουμε ότι $k\geqslant 3$ και ότι ο ισχυρισμός είναι αληθής για πολυώνυμα, το πλήθος των οποίων είναι $<k$. Επειδή $\text{μκδ}(\prod_{i=1}^{k-1}\psi_i(\mathsf{X})^{m_i},\psi_k(\mathsf{X})^{m_k})=1_K$ (βλ. πόρισμα 10.3.13), υπάρχουν μονοσημάντως ορισμένα $\alpha(\mathsf{X}),\alpha_k(\mathsf{X})\in K[\mathsf{X}]$ με

$$\deg(\alpha(\mathsf{X}))<\deg(\textstyle\prod_{i=1}^{k-1}\psi_i(\mathsf{X})^{m_i}),\ \deg(\alpha_k(\mathsf{X}))<\deg(\psi_k(\mathsf{X})^{m_k}),$$

τέτοια ώστε να ισχύει

$$\frac{\upsilon(\mathsf{X})}{\psi(\mathsf{X})}=\frac{c^{-1}\upsilon(\mathsf{X})}{\prod\limits_{i=1}^{k}\psi_i(\mathsf{X})^{m_i}}=\frac{\alpha(\mathsf{X})}{\prod\limits_{i=1}^{k-1}\psi_i(\mathsf{X})^{m_i}}+\frac{\alpha_k(\mathsf{X})}{\psi_k(\mathsf{X})^{m_k}}.\quad(10.55)$$

Κατά την επαγωγική μας υπόθεση υπάρχουν μονοσημάντως ορισμένα πολυώνυμα $\alpha_1(\mathsf{X}),\ldots,\alpha_{k-1}(\mathsf{X})\in K[\mathsf{X}]$, τέτοια ώστε να ισχύει

$$\frac{\alpha(\mathsf{X})}{\prod_{i=1}^{k-1}\psi_i(\mathsf{X})^{m_i}}=\sum_{i=1}^{k-1}\frac{\alpha_i(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i}} \tag{10.56}$$

και $\deg(\alpha_i(\mathsf{X}))<\deg(\psi_i(\mathsf{X})^{m_i})$, $\forall i\in\{1,\ldots,k-1\}$. Η (10.50) έπεται από τις (10.55) και (10.56).

Βήμα 2ο. *Για κάθε $i\in\{1,\ldots,k\}$ υπάρχουν μονοσημάντως ορισμένα πολυώνυμα $\beta_{i,1}(\mathsf{X}),\ldots,\beta_{i,m_i}(\mathsf{X})\in K[\mathsf{X}]$ με*

$$\deg(\beta_{i,j}(\mathsf{X}))<\deg(\psi_i(\mathsf{X})),\ \forall j\in\{1,\ldots,m_i\},$$

και

$$\frac{\alpha_i(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i}}=\sum_{j=1}^{m_i}\frac{\beta_{i,j}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i-j+1}}. \tag{10.57}$$

Πράγματι· εάν ορίσουμε ως $\beta_{i,1}(\mathsf{X})$ το υπόλοιπο τής διαιρέσεως τού $\alpha_i(\mathsf{X})$ διά τού $\psi_i(\mathsf{X})$, ως $\beta_{i,2}(\mathsf{X})$ το υπόλοιπο τής διαιρέσεως τού πηλίκου της διά τού $\psi_i(\mathsf{X})$ κ.ο.κ., λαμβάνουμε διαδοχικώς

$$\begin{aligned}
&\alpha_i(\mathsf{X})=\varpi_{i,1}(\mathsf{X})\,\psi_i(\mathsf{X})+\beta_{i,1}(\mathsf{X}), && \deg(\beta_{i,1}(\mathsf{X}))<\deg(\psi_i(\mathsf{X})),\\
&\varpi_{i,1}(\mathsf{X})=\varpi_{i,2}(\mathsf{X})\,\psi_i(\mathsf{X})+\beta_{i,2}(\mathsf{X}), && \deg(\beta_{i,2}(\mathsf{X}))<\deg(\psi_i(\mathsf{X})),\\
&\varpi_{i,2}(\mathsf{X})=\varpi_{i,3}(\mathsf{X})\,\psi_i(\mathsf{X})+\beta_{i,3}(\mathsf{X}), && \deg(\beta_{i,3}(\mathsf{X}))<\deg(\psi_i(\mathsf{X})),\\
&\vdots && \vdots\\
&\varpi_{i,m_i-3}(\mathsf{X})=\varpi_{i,m_i-2}(\mathsf{X})\,\psi_i(\mathsf{X})+\beta_{i,m_i-2}(\mathsf{X}), && \deg(\beta_{i,m_i-2}(\mathsf{X}))<\deg(\psi_i(\mathsf{X})),\\
&\varpi_{i,m_i-2}(\mathsf{X})=\varpi_{i,m_i-1}(\mathsf{X})\,\psi_i(\mathsf{X})+\beta_{i,m_i-1}(\mathsf{X}), && \deg(\beta_{i,m_i-1}(\mathsf{X}))<\deg(\psi_i(\mathsf{X})),
\end{aligned}$$

όπου

$$\deg(\varpi_{i,j})<\deg\left(\psi_i(\mathsf{X})^{m_i-j}\right),\ \forall j\in\{1,\ldots,m_i-1\}.$$

Θέτοντας $\beta_{i,m_i}(\mathsf{X}):=\varpi_{i,m_i-1}(\mathsf{X})$ συμπεραίνουμε ότι

$$\frac{\alpha_i(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i}}=\frac{\varpi_{i,1}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i-1}}+\frac{\beta_{i,1}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i}}=\frac{\varpi_{i,2}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i-2}}+\frac{\beta_{i,2}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i-1}}+\frac{\beta_{i,1}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i}}=\cdots$$

καταλήγοντας στην (10.57). Απομένει να αποδειχθεί ότι τα κατ' αυτόν τον τρόπο ορισθέντα πολυώνυμα $\beta_{i,1}(\mathsf{X}),\ldots,\beta_{i,m_i}(\mathsf{X})$ είναι τα μόνα πολυώνυμα με αυτήν την ιδιότητα. Εάν

$$\frac{\alpha_i(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i}}=\sum_{j=1}^{m_i}\frac{\beta'_{i,j}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i-j+1}}, \tag{10.58}$$

για κάποια $\beta'_{i,1}(\mathsf{X}),\ldots,\beta'_{i,m_i}(\mathsf{X})\in K[\mathsf{X}]$ με

$$\deg(\beta'_{i,j}(\mathsf{X}))<\deg(\psi_i(\mathsf{X})),\ \forall j\in\{1,\ldots,m_i\},$$

τότε (ύστερα από αφαίρεση τής (10.58) από την (10.57) κατά μέλη) λαμβάνουμε

$$\sum_{j=1}^{m_i}\frac{\beta_{i,j}(\mathsf{X})-\beta'_{i,j}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i-j+1}}=0_{K(\mathsf{X})}. \tag{10.59}$$

Πολλαπλασιασμός αμφοτέρων των μελών τής (10.59) με $\psi_i(\mathsf{X})^{m_i-1}$ δίδει

$$\frac{\beta_{i,1}(\mathsf{X})-\beta'_{i,1}(\mathsf{X})}{\psi_i(\mathsf{X})}=-\sum_{j=2}^{m_i}(\beta_{i,j}(\mathsf{X})-\beta'_{i,j}(\mathsf{X}))\psi_i(\mathsf{X})^{j-2}\in K[\mathsf{X}],$$

απ' όπου έπεται ότι

$$\left.\begin{array}{r}\psi_i(\mathsf{X}) \mid \beta_{i,1}(\mathsf{X}) - \beta'_{i,1}(\mathsf{X}) \\ \deg(\beta_{i,1}(\mathsf{X}) - \beta'_{i,1}(\mathsf{X})) < \deg(\psi_i(\mathsf{X}))\end{array}\right\} \Rightarrow \beta_{i,1}(\mathsf{X}) - \beta'_{i,1}(\mathsf{X}) = 0_{K[\mathsf{X}]}.$$

Τώρα η (10.59) γράφεται ως εξής:

$$\sum_{j=2}^{m_i} \frac{\beta_{i,j}(\mathsf{X}) - \beta'_{i,j}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i-j+1}} = 0_{K(\mathsf{X})}.$$

Επαναλαμβάνοντας την ίδια επιχειρηματολογία (με τα πολυώνυμα $\beta_{i,2}(\mathsf{X}), \beta'_{i,2}(\mathsf{X})$ στη θέση των πολυωνύμων $\beta_{i,1}(\mathsf{X}), \beta'_{i,1}(\mathsf{X})$ κ.ο.κ.) συμπεραίνουμε τελικώς ότι ισχύει $\beta_{i,2}(\mathsf{X}) = \beta'_{i,2}(\mathsf{X}), \ldots, \beta_{i,m_i}(\mathsf{X}) = \beta'_{i,m_i}(\mathsf{X})$. □

10.6.5 Ορισμός. Η (μονοσημάντως ορισμένη) παράσταση ενός πολυωνυμικού κλάσματος $\frac{\varphi(\mathsf{X})}{\psi(\mathsf{X})} \in K(\mathsf{X})$, η οποία δίδεται από τις (10.46) και (10.49), καλείται **διάσπαση** (αυτού) **σε απλά** (ή σε **μερικά**) **πολυωνυμικά κλάσματα**.

10.6.6 Παρατήρηση. (i) Κάθε απλό πολυωνυμικό κλάσμα υπεράνω τού $\mathbb{C}$ είναι τής μορφής

$$\frac{a}{(\mathsf{X}+b)^k}, \quad \text{όπου} \quad k \in \mathbb{N},\ a, b \in \mathbb{C}.$$

(ii) Κάθε απλό πολυωνυμικό κλάσμα υπεράνω τού $\mathbb{R}$ είναι τής μορφής

$$\frac{a}{(\mathsf{X}+b)^k} \quad \text{ή} \quad \frac{r\mathsf{X}+s}{(\mathsf{X}^2+\mathrm{A}\mathsf{X}+\mathrm{B})^l},$$

όπου $k, l \in \mathbb{N},\ a, b, r, s, \mathrm{A}, \mathrm{B} \in \mathbb{R}$, $\mathrm{A}^2 - 4\mathrm{B} < 0$.

10.6.7 Παραδείγματα. (i) Εάν $a, b, c, r, s \in \mathbb{R}$ και $(a-b)(b-c)(c-a) \neq 0$, τότε

$$\begin{aligned}\frac{\mathsf{X}^2+r\mathsf{X}+s}{(\mathsf{X}-a)(\mathsf{X}-b)(\mathsf{X}-c)} &= \frac{(a-b)^{-1}(a-c)^{-1}(a^2+ra+s)}{\mathsf{X}-a} \\ &\quad + \frac{(b-c)^{-1}(c-a)^{-1}(b^2+rb+s)}{\mathsf{X}-b} + \frac{(c-a)^{-1}(a-b)^{-1}(c^2+rc+s)}{\mathsf{X}-c}.\end{aligned}$$

(ii) Παράδειγμα με μη μηδενικό ακέραιο μέρος:

$$\frac{\mathsf{X}^5-2\mathsf{X}^4+3\mathsf{X}^3+2\mathsf{X}^2+\mathsf{X}+1}{(\mathsf{X}-1)^3} = \mathsf{X}^2+\mathsf{X}+3+\frac{9}{\mathsf{X}-1}+\frac{11}{(\mathsf{X}-1)^2}+\frac{4}{(\mathsf{X}-1)^3}.$$

(iii) Ένα κατά τι πιο σύνθετο παράδειγμα είναι το εξής:

$$\frac{1}{\mathsf{X}^8+\mathsf{X}^7-\mathsf{X}^4-\mathsf{X}^3} = -\frac{1}{\mathsf{X}}+\frac{1}{\mathsf{X}^2}-\frac{1}{\mathsf{X}^3}+\frac{9/8}{\mathsf{X}+1}+\frac{1/4}{(\mathsf{X}+1)^2}+\frac{1/8}{\mathsf{X}-1}-\frac{1/4(\mathsf{X}+1)}{\mathsf{X}^2+1}.$$

Παράρτημα A

Περί πινάκων

Λίαν χρήσιμες (πολλαπλασιαστικές) ομάδες πινάκων προκύπτουν ως (ειδικής φύσεως) υποομάδες τής ομάδας των αντιστρεψίμων στοιχείων τού δακτυλίου $\mathrm{Mat}_{n\times n}(R)$ των τετραγωνικών πινάκων με τις εγγραφές τους ειλημμένες από έναν μη τετριμμένο δακτύλιο R με μοναδιαίο στοιχείο.

A.1 ΘΕΜΕΛΙΩΔΕΙΣ ΟΡΙΣΜΟΙ ΚΑΙ ΙΔΙΟΤΗΤΕΣ

Έστω $(R,+,\cdot)$ τυχών δακτύλιος. Για οιοδήποτε ζεύγος $(m,n)\in\mathbb{N}\times\mathbb{N}$ θεωρούμε το σύνολο $\mathrm{Mat}_{m\times n}(R)$ των $(m\times n)$-πινάκων με τις εγγραφές τους ειλημμένες από τον R (βλ. 3.1.6). Κάθε πίνακας

$$\boxed{\mathbf{A}=(a_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}\in\mathrm{Mat}_{m\times n}(R)} \tag{A.1}$$

διαθέτει m **γραμμές**[1]

$$\Gamma\varrho_i(\mathbf{A}):=(a_{i1}\ a_{i2}\ \cdots\ a_{i\,n-1}\ a_{i\,n})\in\mathrm{Mat}_{1\times n}(R),\ \ i\in\{1,\ldots,m\},$$

και n **στήλες**

$$\Sigma\tau_j(\mathbf{A}):=\begin{pmatrix}a_{1j}\\ \vdots\\ a_{m\,j}\end{pmatrix}\in\mathrm{Mat}_{m\times 1}(R),\ \ j\in\{1,\ldots,n\}.$$

(Η $\Gamma\varrho_i(\mathbf{A})$ καλείται i-**οστή γραμμή** και η $\Sigma\tau_j(\mathbf{A})$ j-**οστή στήλη τού** $\mathbf{A}$.) Προφανώς,

$$\mathbf{A}=(\Sigma\tau_1(\mathbf{A})\ \cdots\ \Sigma\tau_n(\mathbf{A}))=\begin{pmatrix}\Gamma\varrho_1(\mathbf{A})\\ \vdots\\ \Gamma\varrho_m(\mathbf{A})\end{pmatrix}. \tag{A.2}$$

• Για οιουσδήποτε πίνακες

$$\mathbf{A}=(a_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}\in\mathrm{Mat}_{m\times n}(R),\ \ \mathbf{B}=(b_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}\in\mathrm{Mat}_{m\times n}(R) \tag{A.3}$$

ισχύει (προφανώς) η αμφίπλευρη συνεπαγωγή

$$\mathbf{A}=\mathbf{B}\Longleftrightarrow a_{ij}=b_{ij},\ \forall\,(i,j)\in\{1,\ldots,m\}\times\{1,\ldots,n\}.$$

[1] Συχνά χρησιμοποιείται η ταύτιση τού $\mathrm{Mat}_{1\times n}(R)$ με το R^n (οπότε οι γραμμές αποτελούνται από διατεταγμένες n-άδες στοιχείων τού R).

• Εάν $r \in R$, τότε για οιονδήποτε πίνακα (A.1) θέτουμε

$$\boxed{r\mathbf{A} := (ra_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}.}$$

• Το $\mathrm{Mat}_{m\times n}(R)$ καθίσταται αβελιανή ομάδα με μέσω τής προσθετικής πράξεως[2]

$$\boxed{\mathbf{A}+\mathbf{B} := (a_{ij}+b_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}} \tag{A.4}$$

για οιουσδήποτε πίνακες (A.3) (Πρβλ. 3.1.6).

• Κάθε πίνακας (A.1) έχων το ίδιο πλήθος γραμμών και στηλών (ήτοι $m = n$) καλείται **τετραγωνικός πίνακας**. Το υποσύνολο εγγραφών $\{a_{ii} | \, i \in \{1,\dots,n\}\}$ δοθέντος πίνακα $\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{Mat}_{n\times n}(K)$ καλείται **κυρία διαγώνιος** και το $\{a_{i,n+1-i} | \, i \in \{1,\dots,n\}\}$ **δευτερεύουσα διαγώνιος** τού $\mathbf{A}$.

A.1.1 Ορισμός (Ανάστροφος πίνακα). Ο **ανάστροφος** ενός $(m\times n)$-πίνακα (A.1) είναι ο $(n\times m)$-πίνακας

$$\mathbf{A}^{\intercal} = (a'_{st})_{\substack{1\leqslant s\leqslant n\\ 1\leqslant t\leqslant m}} \in \mathrm{Mat}_{n\times m}(R),$$

όπου $a'_{st} := a_{ts}$ για κάθε ζεύγος $(s,t) \in \{1,\dots,n\}\times\{1,\dots,m\}$. Σημειωτέον ότι[3]

$$\Gamma\varrho_s(\mathbf{A}^{\intercal}) = \Sigma\tau_s(\mathbf{A})^{\intercal}, \Sigma\tau_t(\mathbf{A}^{\intercal}) = \Gamma\varrho_t(\mathbf{A})^{\intercal}, \forall\,(s,t) \in \{1,..,n\}\times\{1,..,m\}. \tag{A.5}$$

A.1.2 Πρόταση. *Εάν* $\mathbf{A},\mathbf{B} \in \mathrm{Mat}_{m\times n}(R)$ *και* $r \in R$, *τότε ισχύουν τα εξής*:
(i) $(\mathbf{A}^{\intercal})^{\intercal} = \mathbf{A}$.
(ii) $(r\mathbf{A})^{\intercal} = r\,(\mathbf{A}^{\intercal})$.
(iii) $(\mathbf{A}+\mathbf{B})^{\intercal} = \mathbf{A}^{\intercal}+\mathbf{B}^{\intercal}$.

Απόδειξη. (i) Τούτο έπεται άμεσα από τις ισότητες (A.5).
(ii)-(iii) Εάν $\mathbf{A} = (a_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}$, $\mathbf{B} = (b_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}$ και

$$c_{ij} := ra_{ij},\ d_{ij} := a_{ij}+b_{ij},\ \forall\,(i,j) \in \{1,\dots,m\}\times\{1,\dots,n\},$$

τότε $(r\mathbf{A})^{\intercal} = (c'_{st})_{\substack{1\leqslant s\leqslant n\\ 1\leqslant t\leqslant m}}$, $(\mathbf{A}+\mathbf{B})^{\intercal} = (d'_{st})_{\substack{1\leqslant s\leqslant n\\ 1\leqslant t\leqslant m}}$, με

$$c'_{st} = c_{ts} = ra_{ts},\ d'_{st} = d_{ts} = a_{ts}+b_{ts},\ \forall\,(s,t) \in \{1,\dots,n\}\times\{1,\dots,m\}.$$

Επομένως, $(r\mathbf{A})^{\intercal} = r\,(\mathbf{A}^{\intercal})$ και $(\mathbf{A}+\mathbf{B})^{\intercal} = \mathbf{A}^{\intercal}+\mathbf{B}^{\intercal}$. □

A.1.3 Ορισμός. Στην ειδική περίπτωση όπου $m = n$, το σύνολο $\mathrm{Mat}_{n\times n}(R)$ (ήτοι το σύνολο των *τετραγωνικών πινάκων*) καθίσταται *δακτύλιος* μέσω τής προσθετικής πράξεως (A.4) και τής πολλαπλασιαστικής πράξεως

$$\boxed{\mathbf{AB} := \left(\sum_{k=1}^{n} a_{i\,k}b_{k\,j}\right)_{1\leqslant i,j\leqslant n},}$$

για οιουσδήποτε $\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n}$ και $\mathbf{B} = (b_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{Mat}_{n\times n}(R)$. Εάν ο R έχει μοναδιαίο στοιχείο, τότε και ο $\mathrm{Mat}_{n\times n}(R)$ έχει μοναδιαίο στοιχείο. Αυτό

[2] Το ουδέτερο στοιχείο $0_{\mathrm{Mat}_{m\times n}(R)}$ αυτής τής ομάδας είναι ο $(m\times n)$-πίνακας, όλες οι εγγραφές τού οποίου είναι ίσες με το 0_R (και είθισται να σημειώνεται εν συντομία ως $\mathbf{0}_{m\times n}$).

[3] Στην ειδική περίπτωση όπου $m = n$, οι εγγραφές τού $\mathbf{A}^{\intercal}$ αποκτώνται ύστερα από *κατοπτρισμό* των εγγραφών τού $\mathbf{A}$ ως προς την κυρία διαγώνιό του.

είναι ο λεγόμενος **μοναδιαίος πίνακας**

$$\mathbf{I}_n := \begin{pmatrix} 1_R & 0_R & \cdots & 0_R & 0_R \\ 0_R & 1_R & \cdots & 0_R & 0_R \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0_R & 0_R & \cdots & 1_R & 0_R \\ 0_R & 0_R & \cdots & 0_R & 1_R \end{pmatrix}$$

με όλες τις εγγραφές τις ανήκουσες στην κυρία διαγώνιό του ίσες με το 1_R και με τις λοιπές εγγραφές του ίσες με το 0_R. Προφανώς,

$$\mathbf{I}_n = (\delta_{ij})_{1\leqslant i,j\leqslant n}, \text{ όπου } \delta_{ij} := \begin{cases} 1_R, & \text{όταν } i = j, \\ 0_R, & \text{όταν } i \neq j, \end{cases}$$

είναι το λεγόμενο **σύμβολο τού Kronecker**.

Α.1.4 Σημείωση. (i) Εάν υποθέσουμε ότι ο R έχει μοναδιαίο στοιχείο και εάν για κάθε ζεύγος $(i, j) \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ ορίσουμε τον πίνακα

$$\boxed{\mathbf{E}_{ij} := (\delta_{\mu i}\delta_{\nu j})_{1\leqslant \mu,\nu\leqslant n} \in \mathrm{Mat}_{n\times n}(R),}$$

ήτοι τον πίνακα τον έχοντα ως εγγραφή του στην i-οστή γραμμή και στην j-οστή στήλη το 1_R και ως λοιπές εγγραφές του το 0_R, τότε παρατηρούμε ότι *κάθε* τετραγωνικός πίνακας $\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{Mat}_{n\times n}(R)$ γράφεται ως εξής:

$$\mathbf{A} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}\mathbf{E}_{ij}.$$

(ii) Εάν ο R είναι μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο, τότε *για κάθε* $n > 1$ ο δακτύλιος $\mathrm{Mat}_{n\times n}(R)$ *δεν είναι* μεταθετικός, ακόμη και όταν ο ίδιος ο R είναι. (Βλ. Α.2.19.)

Α.1.5 Πρόταση. *Για οιουσδήποτε πίνακες* $\mathbf{A}, \mathbf{B} \in \mathrm{Mat}_{n\times n}(R)$ *ισχύει η ισότητα*

$$\boxed{(\mathbf{AB})^{\intercal} = \mathbf{B}^{\intercal}\mathbf{A}^{\intercal}.}$$

Απόδειξη. Αφήνεται ως άσκηση. □

Α.1.6 Παραδείγματα (Ειδικοί τετραγωνικοί πίνακες). Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο.

(i) Ένας πίνακας

$$\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{Mat}_{n\times n}(R) \tag{Α.6}$$

καλείται **διαγώνιος πίνακας** όταν υπάρχει κάποια n-άδα $(a_1, \ldots, a_n) \in R^n$, τέτοια ώστε να ισχύει

$$a_{ij} = \delta_{ij}a_i = \begin{cases} a_i, & \text{όταν } i = j, \\ 0_R, & \text{όταν } i \neq j. \end{cases}$$

Εν τοιαύτη περιπτώσει, σημειώνουμε τον $\mathbf{A}$ εν συντομία ως

$$\mathrm{diag}(a_1, \ldots, a_n).$$

Προφανώς, $\mathbf{I}_n = \mathrm{diag}(1_R, 1_R, \ldots, 1_R, 1_R)$. Το σύνολο των διαγωνίων πινάκων το συμβολίζουμε ως

$$\mathrm{Diag}_n(R) := \{\, \mathrm{diag}(a_1, \ldots, a_n) \mid (a_1, \ldots, a_n) \in R^n \,\}.$$

(ii) Ένας πίνακας (A.6) καλείται **άνω τριγωνικός** (και αντιστοίχως, **κάτω τριγωνικός**) όταν ισχύει $a_{ij} = 0_R$ για $i > j$ (και αντιστοίχως, για $i < j$), ήτοι όταν είναι τής μορφής

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ 0_R & a_{22} & a_{23} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & a_{n-2\,n} \\ \vdots & & \ddots & \ddots & a_{n-1\,n} \\ 0_R & \cdots & \cdots & 0_R & a_{nn} \end{pmatrix} \text{ και } \mathbf{A} = \begin{pmatrix} a_{11} & 0_R & \cdots & \cdots & 0_R \\ a_{21} & a_{22} & 0_R & & \vdots \\ a_{31} & a_{32} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0_R \\ a_{n1} & \cdots & a_{n\,n-2} & a_{n\,n-1} & a_{nn} \end{pmatrix},$$

αντιστοίχως, και **αυστηρώς άνω τριγωνικός** (και αντιστοίχως, **αυστηρώς κάτω τριγωνικός**) όταν $a_{ij} = 0_R$ για $i \geqslant j$ (και αντιστοίχως, για $i \leqslant j$), ήτοι όταν είναι τής μορφής

$$\mathbf{A} = \begin{pmatrix} 0_R & a_{12} & a_{13} & \cdots & a_{1n} \\ 0_R & 0_R & a_{23} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & a_{n-2\,n} \\ \vdots & & \ddots & \ddots & a_{n-1\,n} \\ 0_R & \cdots & \cdots & 0_R & 0_R \end{pmatrix} \text{ και } \mathbf{A} = \begin{pmatrix} 0_R & 0_R & \cdots & \cdots & 0_R \\ a_{21} & 0_R & 0_R & & \vdots \\ a_{31} & a_{32} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0_R \\ a_{n1} & \cdots & a_{n\,n-2} & a_{n\,n-1} & 0_R \end{pmatrix},$$

αντιστοίχως. Τα σύνολα των άνω, κάτω, αυστηρώς άνω και αυστηρώς κάτω πινάκων τα συμβολίζουμε ως

$$\mathrm{UT}_n(R),\ \mathrm{LT}_n(R),\ \mathrm{SUT}_n(R) \ \text{ και } \ \mathrm{SLT}_n(R),$$

αντιστοίχως[4].

(iii) Ένας πίνακας (A.6) καλείται **μοναδιαίως άνω τριγωνικός** (και αντιστοίχως, **μοναδιαίως κάτω τριγωνικός**) όταν είναι τής μορφής

$$\mathbf{A} = \begin{pmatrix} 1_R & a_{12} & a_{13} & \cdots & a_{1n} \\ 0_R & 1_R & a_{23} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & a_{n-2\,n} \\ \vdots & & \ddots & \ddots & a_{n-1\,n} \\ 0_R & \cdots & \cdots & 0_R & 1_R \end{pmatrix} \text{ και } \mathbf{A} = \begin{pmatrix} 1_R & 0_R & \cdots & \cdots & 0_R \\ a_{21} & 1_R & 0_R & & \vdots \\ a_{31} & a_{32} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0_R \\ a_{n1} & \cdots & a_{n\,n-2} & a_{n\,n-1} & 1_R \end{pmatrix},$$

αντιστοίχως. Τα σύνολα αυτών των πινάκων τα συμβολίζουμε ως $\mathrm{UT}_n^{[1]}(R)$ και $\mathrm{LT}_n^{[1]}(R)$, αντιστοίχως.

A.1.7 Σημείωση. (i) Τα $\mathrm{Diag}_n(R)$, $\mathrm{UT}_n(R)$, $\mathrm{LT}_n(R)$, $\mathrm{SUT}_n(R)$ και $\mathrm{SLT}_n(R)$ αποτελούν υποδακτυλίους τού δακτυλίου $\mathrm{Mat}_{n\times n}(R)$. Οι $\mathrm{Diag}_n(R)$, $\mathrm{UT}_n(R)$ και $\mathrm{LT}_n(R)$ έχουν τον $\mathbf{I}_n$ ως μοναδιαίο τους στοιχείο. (Αντιθέτως, οι $\mathrm{SUT}_n(R)$ και $\mathrm{SLT}_n(R)$ είναι δακτύλιοι χωρίς μοναδιαίο στοιχείο.)

(ii) Το $\mathrm{SUT}_n(R)$ είναι ένας υποδακτύλιος τού δακτυλίου $\mathrm{UT}_n(R)$.

(iii) Το $\mathrm{SLT}_n(R)$ είναι ένας υποδακτύλιος τού δακτυλίου $\mathrm{LT}_n(R)$.

(iv) Το $\mathrm{Diag}_n(R)$ είναι ένας υποδακτύλιος τού δακτυλίου $\mathrm{UT}_n(R) \cap \mathrm{LT}_n(R)$.

(v) Οι κάτωθι αμφίπλευρες συνεπαγωγές είναι προφανείς:

$$\left\{ \begin{array}{c} \mathbf{A} \in \mathrm{UT}_n(R) \Leftrightarrow \mathbf{A}^{\intercal} \in \mathrm{LT}_n(R), \\ \mathbf{A} \in \mathrm{SUT}_n(R) \Leftrightarrow \mathbf{A}^{\intercal} \in \mathrm{SLT}_n(R), \\ \mathbf{A} \in \mathrm{UT}_n^{[1]}(R) \Leftrightarrow \mathbf{A}^{\intercal} \in \mathrm{LT}_n^{[1]}(R). \end{array} \right\}$$

[4]Οι βραχυγραφίες Diag, UT, LT, SUT και SLT επελέγησαν κατά τέτοιον τρόπο, ώστε να θυμίζουν τα αρχικά των όρων **diag**onal, **u**pper **t**riangular, **l**ower **t**riangular, **s**trictly **u**pper **t**riangular, **s**trictly **l**ower **t**riangular.

A.2 ΟΡΙΖΟΥΣΕΣ ΚΑΙ ΣΗΜΑΝΤΙΚΕΣ ΟΜΑΔΕΣ ΠΙΝΑΚΩΝ

Έστω R ένας *μη τετριμμένος μεταθετικός* δακτύλιος *με μοναδιαίο στοιχείο* και έστω $n \in \mathbb{N}$. Η ομάδα των αντιστρεψίμων στοιχείων (*αντιστρεψίμων πινάκων*) τού δακτυλίου $\mathrm{Mat}_{n\times n}(R)$ (που καλείται, ιδιαιτέρως, *γενική γραμμική ομάδα* βαθμού n υπεράνω τού R και συμβολίζεται ως $\mathrm{GL}_n(R)$) μπορεί να περιγραφεί (μέσω τού θεωρήματος A.2.18) με τη βοήθεια των *οριζουσών* των πινάκων των ανηκόντων σε αυτόν. Γι' αυτόν τον λόγο είναι απαραίτητη η παράθεση των *κύριων ιδιοτήτων* των οριζουσών. Επιπρόσθετες σημαντικές *ομάδες πινάκων* προκύπτουν ως υποομάδες τής προαναφερθείσας ομάδας.

A.2.1 Ορισμός. Έστω τυχών πίνακας $\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{Mat}_{n\times n}(R)$. Το στοιχείο

$$\det(\mathbf{A}) := \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} := \sum_{\sigma\in\mathfrak{S}_n} \mathrm{sgn}(\sigma) \left(\prod_{i=1}^{n} a_{i\,\sigma(i)} \right)$$

τού R καλείται **ορίζουσα** τού $\mathbf{A}$ (όπου $\mathfrak{S}_n$ η συμμετρική ομάδα και $\mathrm{sgn}(\sigma)$ η εικόνα οιασδήποτε $\sigma \in \mathfrak{S}_n$ μέσω τής απεικονίσεως προσημάνσεως

$$\mathrm{sgn}{:}\mathfrak{S}_n \longrightarrow \{\pm 1\},$$

(βλ. εδάφια 4.1.1 και 4.3.1).

A.2.2 Παραδείγματα. Για $n = 2$ λαμβάνουμε $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$ και για $n = 3$,

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{31} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}.$$

A.2.3 Πρόταση. *Για κάθε* $\mathbf{A} \in \mathrm{Mat}_{n\times n}(R)$ *ισχύει η ισότητα*

$$\det(\mathbf{A}^{\intercal}) = \det(\mathbf{A}), \tag{A.7}$$

δηλαδή η ορίζουσα οιουδήποτε τετραγωνικού πίνακα ισούται με την ορίζουσα τού αναστρόφου του.

Απόδειξη. Εάν $\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n}$, τότε $\mathbf{A}^{\intercal} = (a'_{rs})_{1\leqslant r,s\leqslant n}$, όπου

$$a'_{rs} := a_{sr},\ \forall (r,s) \in \{1,\ldots,n\} \times \{1,\ldots,n\}.$$

Παρατηρούμε ότι

$$\begin{aligned} \det(\mathbf{A}^{\intercal}) &= \sum_{\sigma\in\mathfrak{S}_n} \mathrm{sgn}(\sigma) \left(\prod_{i=1}^{n} a'_{i\,\sigma(i)} \right) = \sum_{\sigma\in\mathfrak{S}_n} \mathrm{sgn}(\sigma) \left(\prod_{i=1}^{n} a_{\sigma(i)\,i} \right) \\ &= \sum_{\sigma\in\mathfrak{S}_n} \mathrm{sgn}(\sigma) \left(\prod_{j=1}^{n} a_{j\,\sigma^{-1}(j)} \right) = \sum_{\sigma\in\mathfrak{S}_n} \mathrm{sgn}(\sigma^{-1}) \left(\prod_{j=1}^{n} a_{j\,\sigma^{-1}(j)} \right) \\ &= \sum_{\sigma\in\mathfrak{S}_n} \mathrm{sgn}(\sigma) \left(\prod_{j=1}^{n} a_{j\,\sigma(j)} \right) = \det(\mathbf{A}), \end{aligned}$$

όπου η τέταρτη ισότητα έπεται από το ότι

$$\operatorname{sign}(\sigma) = \operatorname{sign}(\sigma^{-1})$$

για κάθε $\sigma \in \mathfrak{S}_n$ (βλ. 4.3.5 (ii)) και η πέμπτη από το ότι η $\mathfrak{S}_n \ni \sigma \longmapsto \sigma^{-1} \in \mathfrak{S}_n$ είναι αμφιρριπτική. □

A.2.4 Σημείωση. Λόγω τής (A.7) η ορίζουσα τού $\mathbf{A}$ μπορεί να γραφεί και υπό τη μορφή

$$\det(\mathbf{A}) = \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma) \left(\prod_{i=1}^{n} a_{\sigma(i)\, i} \right). \tag{A.8}$$

A.2.5 Πρόταση. *Εάν όλες οι εγγραφές κάποιας γραμμής (και αντιστοίχως, κάποιας στήλης) ενός* $\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n} \in \operatorname{Mat}_{n\times n}(R)$ *είναι ίσες με* 0_R, *τότε* $\det(\mathbf{A}) = 0_R$.

Απόδειξη. Εάν $\exists k \in \{1,\dots,n\}$: $\Gamma\varrho_k(\mathbf{A}) = \mathbf{0}_{1\times n}$ $(:= 0_{\operatorname{Mat}_{1\times n}(R)})$, τότε

$$\det(\mathbf{A}) = \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma) \left(\left(\prod_{i\in\{1,\dots,n\}\smallsetminus\{k\}} a_{i\,\sigma(i)} \right) \underbrace{a_{k\,\sigma(k)}}_{=0_R} \right) = 0_R.$$

Εάν $\exists k \in \{1,\dots,n\}$: $\Sigma\tau_k(\mathbf{A}) = \mathbf{0}_{n\times 1}$, τότε

$$\det(\mathbf{A}) = \det(\mathbf{A}^{\intercal}) = 0_R$$

λόγω τής προτάσεως A.2.3, τής ισότητας $\Sigma\tau_k(\mathbf{A}) = \Gamma\varrho_k(\mathbf{A}^{\intercal})$ και τής προηγηθείσας επιχειρηματολογίας. □

A.2.6 Πόρισμα. $\det(\mathbf{0}_{n\times n}) = 0_R,\ \forall n \in \mathbb{N}$.

Απόδειξη. Έπεται άμεσα από την πρόταση A.2.5. □

A.2.7 Πρόταση. *Εάν* $\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n} \in \operatorname{Mat}_{n\times n}(R)$ $(n \geqslant 2)$ *με* $\Sigma\tau_i(\mathbf{A}) = \Sigma\tau_j(\mathbf{A})$ *(και αντιστοίχως, με* $\Gamma\varrho_i(\mathbf{A}) = \Gamma\varrho_j(\mathbf{A})$*) για κάποιους* $i, j \in \{1,\dots,n\}$, $i < j$, *τότε* $\det(\mathbf{A}) = 0_R$.

Απόδειξη. Εάν $\Sigma\tau_i(\mathbf{A}) = \Sigma\tau_j(\mathbf{A})$ για κάποιους δείκτες $i, j \in \{1,\dots,n\}$, $i < j$, τότε θέτοντας $\tau := [i\ j]$ και λαμβάνοντας υπ' όψιν ότι

$$\mathfrak{S}_n = \mathfrak{A}_n \coprod (\mathfrak{A}_n \circ \tau)$$

(βλ. απόδειξη τής προτάσεως 4.3.9), συμπεραίνουμε ότι

$$\begin{aligned}
\det(\mathbf{A}) &= \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma) \left(\prod_{i=1}^{n} a_{i\,\sigma(i)} \right) \\
&= \sum_{\sigma\in\mathfrak{A}_n} \left(\prod_{i=1}^{n} a_{i\,\sigma(i)} \right) - \sum_{\rho\in\mathfrak{A}_n\circ\tau} \left(\prod_{i=1}^{n} a_{i\,\rho(i)} \right) \\
&= \sum_{\sigma\in\mathfrak{A}_n} \left(\prod_{i=1}^{n} a_{i\,\sigma(i)} \right) - \sum_{\sigma\in\mathfrak{A}_n} \left(\prod_{i=1}^{n} a_{i\,\sigma(\tau(i))} \right).
\end{aligned}$$

Επειδή $\tau(i) = j, \tau(j) = i$ και

$$\tau(k) = k, \quad \forall k \in \{1,\dots,n\}\smallsetminus\{i,j\},$$

έχουμε για κάθε μετάταξη $\sigma \in \mathfrak{A}_n$

$$\prod_{i=1}^{n} a_{i\,\sigma(\tau(i))} = a_{i\,\sigma(\tau(i))} a_{j\,\sigma(\tau(j))} \prod_{k\in\{1,\ldots,n\}\smallsetminus\{i,j\}} a_{k\ \sigma(\tau(k))}$$

$$= a_{i\,\sigma(j)} a_{j\,\sigma(i)} \prod_{k\in\{1,\ldots,n\}\smallsetminus\{i,j\}} a_{k\ \sigma(k)}$$

$$= a_{i\,\sigma(i)} a_{j\,\sigma(j)} \prod_{k\in\{1,\ldots,n\}\smallsetminus\{i,j\}} a_{k\ \sigma(k)} = \prod_{i=1}^{n} a_{i\,\sigma(i)}$$

(με την προτελευταία ισότητα οφειλόμενη στο ότι $\Sigma\tau_i(\mathbf{A}) = \Sigma\tau_j(\mathbf{A})$), οπότε λαμβάνουμε $\det(\mathbf{A}) = 0_R$. Εάν $\Gamma\varrho_i(\mathbf{A}) = \Gamma\varrho_j(\mathbf{A})$ για κάποιους $i, j \in \{1, \ldots, n\}$, $i < j$, τότε $\Sigma\tau_i(\mathbf{A}^\intercal) = \Sigma\tau_j(\mathbf{A}^\intercal)$, οπότε βάσει τής προηγηθείσας επιχειρηματολογίας (αλλά με τον $\mathbf{A}^\intercal$ στη θέση τού $\mathbf{A}$) λαμβάνουμε $\det(\mathbf{A}^\intercal) = 0_R$ και, κατ' επέκταση, $\det(\mathbf{A}) = 0_R$ (μέσω τής (A.7)). □

Α.2.8 Λήμμα. *Εάν* $\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{Mat}_{n\times n}(R)$, $\mathbf{b} = (b_1, \ldots, b_n) \in \mathrm{Mat}_{1\times n}(R)$, *και* $r, r' \in R$, *τότε*

$$\det\begin{pmatrix} \Gamma\varrho_1(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_{k-1}(\mathbf{A}) \\ r\Gamma\varrho_k(\mathbf{A}) + r'\mathbf{b} \\ \Gamma\varrho_{k+1}(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_n(\mathbf{A}) \end{pmatrix} = r\det(\mathbf{A}) + r'\det\begin{pmatrix} \Gamma\varrho_1(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_{k-1}(\mathbf{A}) \\ \mathbf{b} \\ \Gamma\varrho_{k+1}(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_n(\mathbf{A}) \end{pmatrix}$$

και

$$\det\left(\Sigma\tau_1(\mathbf{A})\ \cdots\ \Sigma\tau_{k-1}(\mathbf{A})\ (r\Sigma\tau_k(\mathbf{A}) + r'\mathbf{b}^\intercal)\ \Sigma\tau_{k+1}(\mathbf{A})\ \cdots\ \Sigma\tau_n(\mathbf{A})\right)$$
$$= r\det(\mathbf{A}) + r'\det\left(\Sigma\tau_1(\mathbf{A})\ \cdots\ \Sigma\tau_{k-1}(\mathbf{A})\ \mathbf{b}^\intercal\ \Sigma\tau_{k+1}(\mathbf{A})\ \cdots\ \Sigma\tau_n(\mathbf{A})\right)$$

για κάθε $k \in \{1, ..., n\}$. (Όταν $k = 1$(και αντιστοίχως, όταν $k = n$), η ειδικής φύσεως γραμμή (στήλη) τοποθετείται στην πρώτη (και αντιστοίχως, στην n-οστή) θέση και οι γραμμές (στήλες) με δείκτες 1 έως $k-1$ (και αντιστοίχως, με δείκτες $k+1$έως n) παραλείπονται.)

Απόδειξη. Για οιονδήποτε $k \in \{1, ..., n\}$ η ορίζουσα τού πίνακα

$$(c_{ij})_{1\leqslant i,j\leqslant n} = \mathbf{C} := \begin{pmatrix} \Gamma\varrho_1(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_{k-1}(\mathbf{A}) \\ r\Gamma\varrho_k(\mathbf{A}) + r'\mathbf{b} \\ \Gamma\varrho_{k+1}(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_n(\mathbf{A}) \end{pmatrix} \in \mathrm{Mat}_{n\times n}(R)$$

γράφεται ως ακολούθως:

$$\det(\mathbf{C}) = \sum_{\sigma\in\mathfrak{S}_n} \mathrm{sgn}(\sigma) \left(\prod_{i=1}^{n} c_{i\,\sigma(i)}\right)$$

$$= \sum_{\sigma\in\mathfrak{S}_n} \mathrm{sgn}(\sigma) \left(\prod_{i\in\{1,\ldots,n\}\smallsetminus\{k\}} a_{i\,\sigma(i)}\right) (ra_{k\,\sigma(k)} + r'b_{\sigma(k)})$$

$$= r\left(\sum_{\sigma\in\mathfrak{S}_n} \mathrm{sgn}(\sigma) \left(\prod_{i=1}^{n} a_{i\,\sigma(i)}\right)\right) + r'\left(\sum_{\sigma\in\mathfrak{S}_n} \mathrm{sgn}(\sigma) \left(\prod_{i\in\{1,\ldots,n\}\smallsetminus\{k\}} a_{i\,\sigma(i)}\right) b_{\sigma(k)}\right),$$

οπότε η 1η ισότητα είναι αληθής. Η 2η ισότητα αποδεικνύεται παρομοίως. □

Α.2.9 Πρόταση. *Για κάθε* $\mathbf{A} \in \mathrm{Mat}_{n\times n}(R)$ *ισχύουν τα εξής*:

(i) (a) *Εάν* $n \geqslant 2$ *και* $k, l \in \{1, ..., n\}$ *με* $k \neq l$, *τότε για κάθε* $r \in R$ *έχουμε*

$$\det \begin{pmatrix} \Gamma\varrho_1(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_{k-1}(\mathbf{A}) \\ \Gamma\varrho_k(\mathbf{A}) + r\Gamma\varrho_l(\mathbf{A}) \\ \Gamma\varrho_{k+1}(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_n(\mathbf{A}) \end{pmatrix} = \det(\mathbf{A}).$$

(b) *Εάν* $k \in \{1, ..., n\}$ *και* $r \in R$, *τότε*

$$\det \begin{pmatrix} \Gamma\varrho_1(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_{k-1}(\mathbf{A}) \\ r\Gamma\varrho_k(\mathbf{A}) \\ \Gamma\varrho_{k+1}(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_n(\mathbf{A}) \end{pmatrix} = r\det(\mathbf{A}).$$

(ii) (a) *Εάν* $n \geqslant 2$ *και* $k, l \in \{1, ..., n\}$ *με* $k \neq l$, *τότε για κάθε* $r \in R$ *έχουμε*

$$\det\left(\Sigma\tau_1(\mathbf{A}) \ \cdots \ \Sigma\tau_{k-1}(\mathbf{A}) \ (\Sigma\tau_k(\mathbf{A}) + r\Sigma\tau_l(\mathbf{A})) \ \Sigma\tau_{k+1}(\mathbf{A}) \ \cdots \ \Sigma\tau_n(\mathbf{A})\right) = \det(\mathbf{A}).$$

(b) *Εάν* $k \in \{1, ..., n\}$ *και* $r \in R$, *τότε*

$$\det\left(\Sigma\tau_1(\mathbf{A}) \ \cdots \ \Sigma\tau_{k-1}(\mathbf{A}) \ (r\Sigma\tau_k(\mathbf{A})) \ \Sigma\tau_{k+1}(\mathbf{A}) \ \cdots \ \Sigma\tau_n(\mathbf{A})\right) = r\det(\mathbf{A}).$$

(iii) *Για κάθε* $r \in R$ *ισχύει η ισότητα*

$$\det(r\mathbf{A}) = r^n \det(\mathbf{A}).$$

(iv) *Για κάθε* $\tau \in \mathfrak{S}_n$ *ισχύουν οι ισότητες*

$$\det \begin{pmatrix} \Gamma\varrho_{\tau(1)}(\mathbf{A}) \\ \vdots \\ \vdots \\ \Gamma\varrho_{\tau(n)}(\mathbf{A}) \end{pmatrix} = \det\left(\Sigma\tau_{\tau(1)}(\mathbf{A}) \ \cdots \ \Sigma\tau_{\tau(n)}(\mathbf{A})\right) = \mathrm{sgn}(\tau)\det(\mathbf{A}).$$

Απόδειξη. (i) (a) Προφανώς,

$$\det \begin{pmatrix} \Gamma\varrho_1(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_{k-1}(\mathbf{A}) \\ \Gamma\varrho_k(\mathbf{A}) + r\Gamma\varrho_l(\mathbf{A}) \\ \Gamma\varrho_{k+1}(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_n(\mathbf{A}) \end{pmatrix} = \det(\mathbf{A}) + r\det \begin{pmatrix} \Gamma\varrho_1(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_{k-1}(\mathbf{A}) \\ \Gamma\varrho_l(\mathbf{A}) \\ \Gamma\varrho_{k+1}(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_n(\mathbf{A}) \end{pmatrix} = \det(\mathbf{A}),$$

με την πρώτη ισότητα συναγόμενη από το λήμμα Α.2.8 και τη δεύτερη από το ότι η $\Gamma\varrho_l(\mathbf{A})$ εμφανίζεται (στον δεύτερο προσθετέο) τόσον στη θέση k όσον και στη θέση l (βλ. πρόταση Α.2.7).

(b) Έπεται κατόπιν εφαρμογής τού λήμματος Α.2.8 (για $r' = 0_R$).

(ii) Τα (a) και (b) προκύπτουν άμεσα από τα (a) και (b) τού (i) (λαμβάνοντας υπ' όψιν την πρόταση Α.2.3).

(iii) Αρκεί να εφαρμοσθεί n φορές το (i) (b) (για τις n γραμμές τού $r\mathbf{A}$).

(iv) Έστω τυχούσα μετάταξη $\tau \in \mathfrak{S}_n$. Η απεικόνιση $\mathfrak{S}_n \ni \sigma \longmapsto \tau \circ \sigma \in \mathfrak{S}_n$ είναι αμφιριπτική (έχουσα την $\mathfrak{S}_n \ni \sigma \longmapsto \tau^{-1} \circ \sigma \in \mathfrak{S}_n$ ως αντίστροφό της). Επίσης, για κάθε $\sigma \in \mathfrak{S}_n$ έχουμε

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau)^2 \operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau^2 \circ \sigma) = \operatorname{sgn}(\tau)\operatorname{sgn}(\tau \circ \sigma). \tag{A.9}$$

(Βλ. 4.3.5 (i).) Η ορίζουσα τού πίνακα

$$(b_{ij})_{1 \leqslant i,j \leqslant n} = \mathbf{B} := \begin{pmatrix} \Gamma\varrho_{\tau(1)}(\mathbf{A}) \\ \vdots \\ \vdots \\ \Gamma\varrho_{\tau(n)}(\mathbf{A}) \end{pmatrix} \in \operatorname{Mat}_{n\times n}(R)$$

(με $b_{ij} = a_{\tau(i)\, j}, \forall\, (i,j) \in \{1,\ldots,n\} \times \{1,\ldots,n\}$) γράφεται ως ακολούθως:

$$\begin{aligned} \det(\mathbf{B}) &\underset{(A.8)}{=} \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma) \left(\prod_{i=1}^{n} b_{\sigma(i)\, i} \right) = \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma) \left(\prod_{i=1}^{n} a_{\tau(\sigma(i))\, i} \right) \\ &\underset{(A.9)}{=} \operatorname{sgn}(\tau) \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\tau\circ\sigma) \left(\prod_{i=1}^{n} a_{(\tau\circ\sigma)(i)\, i} \right) \\ &= \operatorname{sgn}(\tau) \sum_{\rho\in\mathfrak{S}_n} \operatorname{sgn}(\rho) \left(\prod_{i=1}^{n} a_{\rho(i)\, i} \right) \underset{(A.8)}{=} \operatorname{sgn}(\tau) \det(\mathbf{A}). \end{aligned}$$

Η δεύτερη ισότητα (που αφορά στις στήλες) αποδεικνύεται παρομοίως. □

A.2.10 Πρόταση (Ορίζουσα άνω/κάτω τριγωνικού πίνακα). *Η ορίζουσα οιουδήποτε πίνακα* $\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{UT}_n(R) \cup \mathrm{LT}_n(R)$ *ισούται με το γινόμενο των εγγραφών τής κυρίας διαγωνίου του*:

$$\boxed{\det(\mathbf{A}) = \prod_{i=1}^{n} a_{ii}.} \tag{A.10}$$

Ιδιαιτέρως, $\det(\operatorname{diag}(a_1,\ldots,a_n)) = \prod_{i=1}^{n} a_i, \forall (a_1,\ldots,a_n) \in R^n$, *και* $\det(\mathbf{I}_n) = 1_R$.

Απόδειξη. Εάν $\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{UT}_n(R)$, τότε εξ ορισμού $a_{ij} = 0_R$ για όλους τους δείκτες $i, j \in \{1,\ldots,n\}$ με $i > j$. Για $n = 1$ η (A.10) είναι προφανής. Για $n \geqslant 2$ και για κάθε $\sigma \neq \mathrm{id}$ υπάρχει κατ' ανάγκην κάποιος $k \in \{1,\ldots,n\}$ με $k > \sigma(k)$, οπότε

$$\det(\mathbf{A}) = \prod_{i=1}^{n} a_{ii} + \sum_{\sigma\in\mathfrak{S}_n\smallsetminus\{\mathrm{id}\}} \operatorname{sgn}(\sigma) \left(\left(\prod_{i\in\{1,\ldots,n\}\smallsetminus\{k\}} a_{i\,\sigma(i)} \right) \underbrace{a_{k\,\sigma(k)}}_{=0_K} \right) = \prod_{i=1}^{n} a_{ii}.$$

Άρα η (A.10) είναι αληθής και για $n \geqslant 2$. Εάν $\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{LT}_n(R)$, τότε

$$\det(\mathbf{A}) = \det(\mathbf{A}^{\intercal}) = \prod_{i=1}^{n} a_{ii}$$

λόγω τής προτάσεως A.2.3 και τού ότι $\mathbf{A}^{\intercal} \in \mathrm{UT}_n(R)$. □

A.2.11 Θεώρημα (Τύπος γινομένου). *Η ορίζουσα τού γινομένου δύο (τετραγωνικών) πινάκων* $\mathbf{A}, \mathbf{B} \in \operatorname{Mat}_{n\times n}(R)$ *ισούται με το γινόμενο των οριζουσών τους, ήτοι*

$$\boxed{\det(\mathbf{AB}) = \det(\mathbf{A}) \det(\mathbf{B}).} \tag{A.11}$$

Ως εκ τούτου, $\det(\mathbf{AB}) = \det(\mathbf{BA})$.

Απόδειξη. Εάν $n = 1$, τότε η (A.11) είναι προφανής. Εάν $n \geqslant 2$, τότε θέτοντας $\mathbf{C} := \mathbf{AB}$, όπου $\mathbf{B} := (b_{ij})_{1\leqslant i,j\leqslant n}$, παρατηρούμε ότι για κάθε $j \in \{1, ..., n\}$ ισχύει η ισότητα

$$\Sigma\tau_j(\mathbf{C}) = \sum_{k=1}^{n} b_{kj}\Sigma\tau_k(\mathbf{A}).$$

Επομένως,

$$\begin{aligned}
&\det(\mathbf{C}) = \det\left(\Sigma\tau_1(\mathbf{C})\,\Sigma\tau_2(\mathbf{C})\,\cdots\,\Sigma\tau_n(\mathbf{C})\right)\\
&= \det\left(\left(\sum_{k_1=1}^{n} b_{k_1 1}\Sigma\tau_{k_1}(\mathbf{A})\right)\Sigma\tau_2(\mathbf{C})\,\cdots\,\Sigma\tau_n(\mathbf{C})\right)\\
&\underset{\text{A.2.8}}{=} \sum_{k_1=1}^{n} b_{k_1 1}\det\left(\Sigma\tau_{k_1}(\mathbf{A})\,\Sigma\tau_2(\mathbf{C})\,\cdots\,\Sigma\tau_n(\mathbf{C})\right)\\
&= \sum_{k_1=1}^{n} b_{k_1 1}\det\left(\Sigma\tau_{k_1}(\mathbf{A})\left(\sum_{k_2=1}^{n} b_{k_2 2}\Sigma\tau_{k_2}(\mathbf{A})\right)\Sigma\tau_3(\mathbf{C})\,\cdots\,\Sigma\tau_n(\mathbf{C})\right)\\
&= \sum_{k_1=1}^{n}\sum_{k_2=1}^{n} b_{k_1 1}b_{k_2 2}\det\left(\Sigma\tau_{k_1}(\mathbf{A})\,\Sigma\tau_{k_2}(\mathbf{A})\,\Sigma\tau_3(\mathbf{C})\,\cdots\,\Sigma\tau_n(\mathbf{C})\right)\\
&= \cdots = \sum_{k_1=1}^{n}\sum_{k_2=1}^{n}\cdots\sum_{k_n=1}^{n}\left(\prod_{j=1}^{n} b_{k_j j}\right)\det\left(\Sigma\tau_{k_1}(\mathbf{A})\,\Sigma\tau_{k_2}(\mathbf{A})\,\cdots\,\Sigma\tau_{k_n}(\mathbf{A})\right).
\end{aligned}$$

Το ανωτέρω πολλαπλό άθροισμα περιέχει n^n προσθετέους! Εντούτοις, πολλοί εξ αυτών μηδενίζονται. Πράγματι· *κάθε* προσθετέος αντιστοιχεί στην επιλογή μίας (και μόνον) διατεταγμένης n-άδας

$$(k_1, \ldots, k_n) \in \underbrace{\{1, \ldots, n\} \times \cdots \times \{1, \ldots, n\}}_{n\ \text{φορές}}. \tag{A.12}$$

Για τους προσθετέους που αντιστοιχούν σε n-άδες (A.12) με $k_\mu = k_\nu$ για κάποιους $\mu, \nu \in \{1, .., n\}$, $\mu < \nu$, έχουμε $\det\left(\Sigma\tau_{k_1}(\mathbf{A})\,\Sigma\tau_{k_2}(\mathbf{A})\,\cdots\,\Sigma\tau_{k_n}(\mathbf{A})\right) = 0_R$. (Βλ. πρόταση A.2.7.) Άρα υπολείπονται μόνον οι προσθετέοι που αντιστοιχούν σε n-άδες (A.12) για τις οποίες (για οιοδήποτε $(\mu, \nu) \in \{1, \ldots, n\} \times \{1, \ldots, n\}$) ισχύει η συνεπαγωγή $\mu \neq \nu \Longrightarrow k_\mu \neq k_\nu$. Τούτη ισοδυναμεί με την ενριπτικότητα τής απεικονίσεως

$$\{1, \ldots, n\} \ni \nu \longmapsto k_\nu \in \{1, \ldots, n\}.$$

Επειδή κάθε ενριπτική απεικόνιση από ένα πεπερασμένο σύνολο στον εαυτό του είναι κατ' ανάγκην αμφιρριπτική και οι αμφιρριπτικές απεικονίσεις από το $\{1, \ldots, n\}$ επί τού $\{1, \ldots, n\}$ είναι (εξ ορισμού) τα στοιχεία τής $\mathfrak{S}_n$, αρκεί (για τον προσδιορισμό τής ορίζουσας $\det(\mathbf{C}) \in R$) να αντικαταστήσουμε το ανωτέρω πολλαπλό άθροισμα με ένα άθροισμα που να περιλαμβάνει μόνον εκείνες τις n-άδες $(k_1, \ldots, k_n)$ για τις οποίες υπάρχει $\sigma \in \mathfrak{S}_n$ με $k_\nu = \sigma(\nu)$, $\forall \nu \in \{1, \ldots, n\}$. Ως εκ τούτου,

$$\begin{aligned}
&\det(\mathbf{C}) = \sum_{\sigma\in\mathfrak{S}_n}\left(\prod_{j=1}^{n} b_{\sigma(j)\,j}\right)\det\left(\Sigma\tau_{\sigma(1)}(\mathbf{A})\,\Sigma\tau_{\sigma(2)}(\mathbf{A})\,\cdots\,\Sigma\tau_{\sigma(n)}(\mathbf{A})\right)\\
&\underset{\text{A.2.9 (iv)}}{=} \sum_{\sigma\in\mathfrak{S}_n}\left(\prod_{j=1}^{n} b_{\sigma(j)\,j}\right)\operatorname{sgn}(\sigma)\det(\mathbf{A}) = \sum_{\sigma\in\mathfrak{S}_n}\operatorname{sgn}(\sigma)\left(\prod_{j=1}^{n} b_{\sigma(j)\,j}\right)\det(\mathbf{A})\\
&\underset{\text{(A.8)}}{=} \det(\mathbf{B})\det(\mathbf{A}) = \det(\mathbf{A})\det(\mathbf{B}),
\end{aligned}$$

και η (A.11) είναι αληθής. □

Α.2.12 Ορισμός. Έστω τυχών πίνακας $\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{Mat}_{n\times n}(R)$ $(n \geqslant 2)$. Για κάθε διατεταγμένο ζεύγος $(i,j) \in \{1,\ldots,n\} \times \{1,\ldots,n\}$, συμβολίζουμε ως

$$\boxed{\mathbf{A}^{\sharp}_{[i,j]} \in \mathrm{Mat}_{(n-1)\times(n-1)}\,(R)}$$

τον υποπίνακα τού $\mathbf{A}$ τον προκύπτοντα ύστερα από *διαγραφή* τής i-οστής γραμμής $\Gamma\varrho_i(\mathbf{A})$ και τής j-οστής στήλης $\Sigma\tau_j(\mathbf{A})$:

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,j-1} & a_{1,j} & a_{1,j+1} & \cdots & a_{1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,j-1} & a_{i-1,j} & a_{i-1,j+1} & \cdots & a_{i-1,n} \\ a_{i,1} & \cdots & a_{i,j-1} & a_{i,j} & a_{i,j+1} & \cdots & a_{i,n} \\ a_{i+1,1} & \cdots & a_{i+1,j-1} & a_{i+1,j} & a_{i+1,j+1} & \cdots & a_{i+1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,j-1} & a_{n,j} & a_{n,j+1} & \cdots & a_{n,n} \end{pmatrix},$$

ήτοι τον $\mathbf{A}^{\sharp}_{[i,j]} := (a^{\sharp}_{st})_{1\leqslant s,t\leqslant n-1}$, όπου

$$a^{\sharp}_{st} := \begin{cases} a_{st}, & \text{όταν } 1 \leqslant s \leqslant i-1 \text{ και } 1 \leqslant t \leqslant j-1, \\ a_{s+1,t}, & \text{όταν } i \leqslant s \leqslant n-1 \text{ και } 1 \leqslant t \leqslant j-1, \\ a_{s,t+1}, & \text{όταν } 1 \leqslant s \leqslant i-1 \text{ και } j \leqslant t \leqslant n-1, \\ a_{s+1,t+1}, & \text{όταν } i \leqslant s \leqslant n-1 \text{ και } j \leqslant t \leqslant n-1. \end{cases}$$

Το στοιχείο

$$\boxed{\mathrm{cof}_{ij}(\mathbf{A}) := (-1)^{i+j}\,\det(\mathbf{A}^{\sharp}_{[i,j]}) \in R}$$

τού δακτυλίου αναφοράς ονομάζεται **συμπαράγοντας (ή αλγεβρικό συμπλήρωμα) τού $\mathbf{A}$ ως προς το ζεύγος δεικτών** i,j, και ο

$$\boxed{\mathbf{adj}\,(\mathbf{A}) := ((\mathrm{cof}_{ij}(\mathbf{A}))_{1\leqslant i,j\leqslant n})^{\intercal} \in \mathrm{Mat}_{n\times n}\,(R)}$$

ο πίνακας ο προσαρτημένος στον $\mathbf{A}$.

Α.2.13 Λήμμα. *Έστω* $\mathbf{A} = (a_{\mu\nu})_{1\leqslant\mu,\nu\leqslant n} \in \mathrm{Mat}_{n\times n}(R)$ $(n \geqslant 2)$. *Για οιουσδήποτε υποδείκτες* $i,j \in \{1,...,n\}$ *ισχύει η συνεπαγωγή*

$$[a_{kj} = 0_R,\ \forall k \in \{1,..,n\}\smallsetminus\{i\}] \Rightarrow \det(\mathbf{A}) = (-1)^{i+j}\,a_{ij}\,\det(\mathbf{A}^{\sharp}_{[i,j]}) = a_{ij}\mathrm{cof}_{ij}(\mathbf{A}).$$

Απόδειξη. Για κάθε μετάταξη $\sigma \in \mathfrak{S}_n$, για την οποία ισχύει $\sigma\,(n) = n$, η

$$\overline{\sigma} : \{1,...,n-1\} \longrightarrow \{1,...,n-1\},\ \overline{\sigma}(k) := \sigma(k),\ \forall k \in \{1,...,n-1\},$$

είναι μια μετάταξη ανήκουσα στην $\mathfrak{S}_{n-1}$ με $\mathrm{sgn}(\overline{\sigma}) = \mathrm{sgn}(\sigma)$ και η απεικόνιση

$$\{\,\sigma \in \mathfrak{S}_n \,|\, \sigma\,(n) = n\} \longrightarrow \mathfrak{S}_{n-1},\ \sigma \longmapsto \overline{\sigma},$$

ισομορφισμός ομάδων. Θέτοντας

$$\rho := \begin{bmatrix} 1 & \ldots & j-1 & j & j+1 & \ldots & n-1 & n \\ 1 & \ldots & j-1 & j+1 & j+2 & \ldots & n & j \end{bmatrix} \in \mathfrak{S}_n,$$

παρατηρούμε ότι $\rho = [j\ n]\circ[j\ n-1]\circ\cdots\circ[j\ j+2]\circ[j\ j+1]$, οπότε $\mathrm{sgn}(\rho) = (-1)^{n-j}$. (Βλ. 4.3.3 και 4.3.5 (i).) Ο πίνακας

$$\mathbf{B} := \left(\Sigma\tau_{\rho(1)}\,(\mathbf{A})\ \Sigma\tau_{\rho(2)}\,(\mathbf{A})\ \cdots\ \Sigma\tau_{\rho(n)}\,(\mathbf{A})\right)$$

έχει ως ορίζουσά του την $\det(\mathbf{B}) \underset{\text{A.2.9 (iv)}}{=} \operatorname{sgn}(\rho)\det(\mathbf{A}) = (-1)^{n-j}\det(\mathbf{A})$. Θέτοντας, κατ' αναλογίαν,

$$\tau := \begin{bmatrix} 1 & \dots & i-1 & i & i+1 & \dots & n-1 & n \\ 1 & \dots & i-1 & i+1 & i+2 & \dots & n & i \end{bmatrix} \in \mathfrak{S}_n,$$

παρατηρούμε ότι $\tau = [i\,n]\circ[i\,n-1]\circ\cdots\circ[i\,i+2]\circ[i\,i+1]$, οπότε $\operatorname{sgn}(\rho) = (-1)^{n-i}$. Ο πίνακας

$$(c_{st})_{1\leqslant s,t\leqslant n} = \mathbf{C} := \begin{pmatrix} \Gamma\varrho_{\tau(1)}(\mathbf{B}) \\ \vdots \\ \vdots \\ \Gamma\varrho_{\tau(n)}(\mathbf{B}) \end{pmatrix}$$

έχει ως ορίζουσά του την $\det(\mathbf{C}) \underset{\text{A.2.9 (iv)}}{=} \operatorname{sgn}(\tau)\det(\mathbf{B}) = (-1)^{n-i}(-1)^{n-j}\det(\mathbf{A})$, οπότε

$$\det(\mathbf{A}) = (-1)^{i+j}\det(\mathbf{C}). \tag{A.13}$$

Επειδή

$$[a_{kj} = 0_R,\ \forall k \in \{1,\dots,n\}\setminus\{i\}] \Rightarrow [c_{kn} = 0_R,\ \forall k \in \{1,\dots,n-1\}],$$

έχουμε

$$\det(\mathbf{C}) = \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma)\left(\prod_{i=1}^{n} c_{i\,\sigma(i)}\right) = \sum_{\{\,\sigma\in\mathfrak{S}_n \mid \sigma(n)=n\}} \operatorname{sgn}(\sigma)\left(\prod_{i=1}^{n-1} c_{i\,\sigma(i)}\right) c_{nn}$$

$$= c_{nn}\left(\sum_{\overline{\sigma}\in\mathfrak{S}_{n-1}} \operatorname{sgn}(\overline{\sigma})\left(\prod_{i=1}^{n-1} c_{i\,\overline{\sigma}(i)}\right)\right) = c_{nn}\det(\mathbf{C}^{\sharp}_{[n,n]}).$$

Αρκεί λοιπόν να χρησιμοποιηθεί η (A.13) σε συνδυασμό με τις ισότητες $c_{nn} = a_{ij}$ και $\mathbf{C}^{\sharp}_{[n,n]} = \mathbf{A}^{\sharp}_{[i,j]}$. □

A.2.14 Πρόταση. *Έστω τυχών* $\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{Mat}_{n\times n}(R)$ $(n \geqslant 2)$.
(i) *Εάν* $j \in \{1,\dots,n\}$, *τότε*

$$\boxed{\det(\mathbf{A}) = \sum_{k=1}^{n} a_{kj}\operatorname{cof}_{kj}(\mathbf{A}) = \sum_{k=1}^{n} (-1)^{k+j} a_{kj}\det(\mathbf{A}^{\sharp}_{[k,j]}).} \tag{A.14}$$

(Ανάπτυγμα τής $\det(\mathbf{A})$ **ως προς τις εγγραφές τής στήλης** $\Sigma\tau_j(\mathbf{A})$.)

(ii) *Εάν* $i \in \{1,\dots,n\}$, *τότε*

$$\boxed{\det(\mathbf{A}) = \sum_{k=1}^{n} a_{ik}\operatorname{cof}_{ik}(\mathbf{A}) = \sum_{k=1}^{n} (-1)^{i+k} a_{ik}\det(\mathbf{A}^{\sharp}_{[i,k]}).} \tag{A.15}$$

(Ανάπτυγμα τής $\det(\mathbf{A})$ **ως προς τις εγγραφές τής γραμμής** $\Gamma\varrho_i(\mathbf{A})$.)

Απόδειξη. (i) Θεωρούμε τα n στοιχεία

$$\mathbf{e}_k := (0_R,\dots,0_R,\ \underbrace{1_R}_{k\text{-οστή συντεταγμένη}},0_R,\dots,0_R) \in R^n,\ k \in \{1,\dots,n\},$$

και εφράζουμε μέσω αυτών την j-οστή στήλη τού $\mathbf{A}$ ως ακολούθως:

$$\Sigma\tau_j(\mathbf{A}) = \sum_{k=1}^{n} a_{kj}\mathbf{e}_k^{\intercal}.$$

Προφανώς,

$$\det(\mathbf{A}) = \det\left(\Sigma\tau_1(\mathbf{A}) \ \cdots \ \Sigma\tau_{j-1}(\mathbf{A}) \ \left(\sum_{k=1}^{n} a_{kj}\mathbf{e}_k^\intercal\right) \ \Sigma\tau_{j+1}(\mathbf{A}) \ \cdots \ \Sigma\tau_n(\mathbf{A})\right)$$

$$\underset{\text{A.2.8}}{=} \sum_{k=1}^{n} a_{kj} \det\left(\Sigma\tau_1(\mathbf{A}) \ \cdots \ \Sigma\tau_{j-1}(\mathbf{A}) \, \mathbf{e}_k^\intercal \, \Sigma\tau_{j+1}(\mathbf{A}) \ \cdots \ \Sigma\tau_n(\mathbf{A})\right)$$

$$\underset{\text{A.2.13}}{=} \sum_{k=1}^{n} a_{kj} \left((-1)^{k+j} \cdot 1_R \cdot \det(\mathbf{A}^\sharp_{[k,j]})\right) = \sum_{k=1}^{n} (-1)^{k+j} a_{kj} \det(\mathbf{A}^\sharp_{[k,j]}).$$

(ii) Επειδή $\mathbf{A}^\intercal = (a'_{rs})_{1\leqslant r,s\leqslant n}$, όπου $a'_{rs} := a_{sr}$, $\forall (r,s) \in \{1,\ldots,n\} \times \{1,\ldots,n\}$, έχουμε (κατόπιν αναπτύξεως τής $\det(\mathbf{A}^\intercal)$ ως προς τις εγγραφές τής $\Sigma\tau_i(\mathbf{A}^\intercal)$)

$$\det(\mathbf{A}) \underset{\text{(A.7)}}{=} \det(\mathbf{A}^\intercal) \underset{\text{(i)}}{=} \sum_{k=1}^{n} (-1)^{k+i} a'_{ki} \det((\mathbf{A}^\intercal)^\sharp_{[k,i]})$$

$$= \sum_{k=1}^{n} (-1)^{i+k} a_{ik} \det((\mathbf{A}^\intercal)^\sharp_{[k,i]}) = \sum_{k=1}^{n} (-1)^{i+k} a_{ik} \det((\mathbf{A}^\sharp_{[i,k]})^\intercal)$$

$$\underset{\text{(A.7)}}{=} \sum_{k=1}^{n} (-1)^{i+k} a_{ik} \det((\mathbf{A}^\sharp_{[i,k]})).$$

Άρα αμφότερες οι (A.14) και (A.15) είναι αληθείς. □

A.2.15 Θεώρημα. *Για κάθε* $\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{Mat}_{n\times n}(R)$ $(n \geqslant 2)$ *ισχύουν οι ισότητες*

$$\boxed{\mathbf{adj}\,(\mathbf{A})\ \mathbf{A} = \det(\mathbf{A})\ \mathbf{I}_n = \mathbf{A}\,\mathbf{adj}\,(\mathbf{A})\,.} \tag{A.16}$$

Απόδειξη. Για οιουσδήποτε $i, j \in \{1, ..., n\}$ η εγγραφή τού πίνακα $\mathbf{adj}\,(\mathbf{A})\ \mathbf{A}$ η ευρισκόμενη στην i-στή του γραμμή και στην j-οστή του στήλη είναι η

$$\sum_{k=1}^{n} (-1)^{i+k} a_{kj} \det(\mathbf{A}^\sharp_{[k,i]})$$

$$\underset{(*)}{=} \begin{cases} \det\left(\Sigma\tau_1(\mathbf{A}) \ \cdots \ \Sigma\tau_{i-1}(\mathbf{A}) \, \Sigma\tau_j(\mathbf{A}) \, \Sigma\tau_{i+1}(\mathbf{A}) \ \cdots \ \Sigma\tau_{j-1}(\mathbf{A}) \, \Sigma\tau_j(\mathbf{A}) \, \Sigma\tau_{j+1}(\mathbf{A}) \ \cdots \ \Sigma\tau_n(\mathbf{A})\right), \\ \text{όταν } i \leqslant j \text{ και} \\ \det\left(\Sigma\tau_1(\mathbf{A}) \ \cdots \ \Sigma\tau_{j-1}(\mathbf{A}) \, \Sigma\tau_j(\mathbf{A}) \, \Sigma\tau_{j+1}(\mathbf{A}) \ \cdots \ \Sigma\tau_{i-1}(\mathbf{A}) \, \Sigma\tau_j(\mathbf{A}) \, \Sigma\tau_{i+1}(\mathbf{A}) \ \cdots \ \Sigma\tau_n(\mathbf{A})\right), \\ \text{όταν } j \leqslant i, \end{cases}$$

$$= \begin{cases} \det(\mathbf{A}), & \text{όταν } i = j, \\ 0_R, & \text{όταν } i \neq j \text{ (βλ. πρόταση A.2.7).} \end{cases}$$

(Η ορίζουσα τού δεξιού μέλους στην $(*)$ έχει το άθροισμα τού αριστερού μέλους ως ανάπτυγμα ως προς την i-οστή στήλη.) Άρα $\mathbf{adj}\,(\mathbf{A})\ \mathbf{A} = \det(\mathbf{A})\ \mathbf{I}_n$. Η ισότητα $\mathbf{A}\,\mathbf{adj}\,(\mathbf{A}) = \det(\mathbf{A})\ \mathbf{I}_n$ αποδεικνύεται παρομοίως (κάνοντας χρήση τού (ii) τής προτάσεως A.2.14). □

A.2.16 Ορισμός. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο και έστω $n \in \mathbb{N}$. Μέσω τού μονοειδούς $(\mathrm{Mat}_{n\times n}(R), \cdot)$ ορίζεται η (πολλαπλασιαστική) ομάδα των αντιστρεψίμων πινάκων

$$\boxed{\mathrm{GL}_n(R) := (\mathrm{Mat}_{n\times n}(R))^\times}$$

με τις εγγραφές τους ειλημμένες από τον R, η οποία καλείται, ιδιαιτέρως, **γενική γραμμική ομάδα (βαθμού** n **υπεράνω τού** R**)**.

Α.2.17 Πρόταση. *Για κάθε* $\mathbf{A} \in \mathrm{GL}_n(R)$ *(όπου* R *τυχών μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο) έχουμε* $\mathbf{A}^\intercal \in \mathrm{GL}_n(R)$ *και*

$$\boxed{(\mathbf{A}^\intercal)^{-1} = (\mathbf{A}^{-1})^\intercal.}$$

Απόδειξη. Επειδή $\mathbf{A}\mathbf{A}^{-1} = \mathbf{A}^{-1}\mathbf{A} = \mathbf{I}_n$ και (προφανώς) $(\mathbf{I}_n)^\intercal = \mathbf{I}_n$, από την πρόταση Α.1.5 προκύπτει ότι

$$(\mathbf{A}^{-1})^\intercal \mathbf{A}^\intercal = \left(\mathbf{A}\mathbf{A}^{-1}\right)^\intercal = \mathbf{I}_n = \left(\mathbf{A}^{-1}\mathbf{A}\right)^\intercal = \mathbf{A}^\intercal (\mathbf{A}^{-1})^\intercal,$$

οπότε ο $\mathbf{A}^\intercal$ είναι αντιστρέψιμος και $(\mathbf{A}^\intercal)^{-1} = (\mathbf{A}^{-1})^\intercal$. □

Α.2.18 Θεώρημα. *Για κάθε μη τετριμμένο μεταθετικό δακτύλιο* R *με μοναδιαίο στοιχείο και για κάθε* $n \in \mathbb{N}$ *ισχύει η ισότητα*

$$\boxed{\mathrm{GL}_n(R) = \{\mathbf{A} \in \mathrm{Mat}_{n\times n}(R) \mid \det(\mathbf{A}) \in R^\times\}.} \tag{Α.17}$$

Επιπροσθέτως, για κάθε $\mathbf{A} \in \mathrm{GL}_n(R)$,

$$\boxed{\det(\mathbf{A}^{-1}) = \det(\mathbf{A})^{-1}} \tag{Α.18}$$

και για $n \geqslant 2$,

$$\boxed{\mathbf{A}^{-1} = \det(\mathbf{A})^{-1}\mathbf{adj}(\mathbf{A}).} \tag{Α.19}$$

Απόδειξη. Για $n = 1$ οι ισότητες (Α.17) και (Α.18) είναι προφανείς. Ας υποθέσουμε από εδώ και στο εξής ότι $n \geqslant 2$. Εάν $\mathbf{A} \in \mathrm{Mat}_{n\times n}(R)$ και $\det(\mathbf{A}) \in R^\times$, τότε θέτοντας $\mathbf{B} := \det(\mathbf{A})^{-1}\mathbf{adj}(\mathbf{A})$ συμπεραίνουμε μέσω τής (Α.16) ότι

$$\mathbf{A}\mathbf{B} = \mathbf{I}_n = \mathbf{B}\mathbf{A} \Rightarrow \mathbf{A} \in \mathrm{GL}_n(R).$$

Και αντιστρόφως· εάν $\mathbf{A} \in \mathrm{GL}_n(R)$, τότε υπάρχει αντίστροφο στοιχείο $\mathbf{A}^{-1}$ τού $\mathbf{A}$. Κατά το θεώρημα Α.2.11 και την πρόταση Α.2.10,

$$\mathbf{A}\mathbf{A}^{-1} = \mathbf{I}_n = \mathbf{A}^{-1}\mathbf{A} \Rightarrow \det(\mathbf{A}) \cdot \det(\mathbf{A}^{-1}) = 1_R = \det(\mathbf{A}^{-1}) \cdot \det(\mathbf{A}),$$

οπότε $\det(\mathbf{A}) \in R^\times$ και $\det(\mathbf{A})^{-1} = \det(\mathbf{A}^{-1})$. (Η ισότητα (Α.19) έπεται άμεσα από την (Α.16).) □

Α.2.19 Σημείωση. Η γενική γραμμική ομάδα $\mathrm{GL}_n(R)$ *δεν* είναι αβελιανή στην περίπτωση όπου $n \geqslant 2$. Επί παραδείγματι, θεωρώντας τούς αντιστρέψιμους πίνακες

$$\mathbf{A} := \mathbf{E}_{1,2} + \mathbf{E}_{2,1}, \quad \mathbf{B} := \mathbf{E}_{1,1} + \mathbf{E}_{1,2} + \mathbf{E}_{2,2}$$

(όπου $\mathbf{E}_{i,j} \in \mathrm{Mat}_{n\times n}(R)$ όπως ορίσθηκαν στο Α.1.4 (i)), διαπιστώνουμε ότι

$$\mathbf{A}\mathbf{B} = \mathbf{E}_{1,2} + \mathbf{E}_{2,1} + \mathbf{E}_{2,2} \neq \mathbf{E}_{1,1} + \mathbf{E}_{1,2} + \mathbf{E}_{2,1} = \mathbf{B}\mathbf{A}.$$

Α.2.20 Παραδείγματα. (i) $\mathrm{GL}_n(F) = \{\mathbf{A} \in \mathrm{Mat}_{n\times n}(F) \mid \det(\mathbf{A}) \neq 0_F\}$ για κάθε σώμα F (διότι $F^\times = F \smallsetminus \{0_F\}$).

(ii) Επειδή $\mathrm{card}(\mathrm{GL}_n(\mathbb{R})) = \mathrm{card}(\mathbb{R} \smallsetminus \{0\}) = \mathrm{card}(\mathbb{R}) = \mathfrak{c} > \aleph_0$, η $\mathrm{GL}_n(\mathbb{R})$ είναι ομάδα άπειρη (και μάλιστα *υπεραριθμήσιμη*).

(iii) $\mathrm{GL}_n(\mathbb{Z}) = \{\mathbf{A} \in \mathrm{Mat}_{n\times n}(\mathbb{Z}) \mid \det(\mathbf{A}) \in \{\pm 1\}\}$.

A.2.21 Πόρισμα. *Εάν R είναι ένας μη τετριμμένος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, τότε οι ομάδες των αντιστρεψίμων στοιχείων των υποδακτυλίων $\mathrm{UT}_n(R)$ και $\mathrm{LT}_n(R)$ τού $\mathrm{Mat}_{n\times n}(R)$ (βλ.* A.1.6 (ii) *και* A.1.7 (i)*) είναι οι*

$$\mathrm{UT}_n(R)^\times = \left\{\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{UT}_n(R) \;\middle|\; a_{ii} \in R^\times \,, \forall i \in \{1,\dots,n\}\right\}$$

και

$$\mathrm{LT}_n(R)^\times = \left\{\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{LT}_n(R) \;\middle|\; a_{ii} \in R^\times \,, \forall i \in \{1,\dots,n\}\right\}.$$

Απόδειξη. Επειδή $\mathrm{UT}_n(R)^\times \subseteq \mathrm{GL}_n(R) \cap \mathrm{UT}_n(R)$ (βλ. A.1.7 (i) και 6.2.12 (iii)), για κάθε αντιστρέψιμο άνω τριγωνικό πίνακα $\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n}$ ισχύει

$$\det(\mathbf{A}) \underset{(A.10)}{=} \prod_{i=1}^{n} a_{ii} \in R^\times \Longrightarrow [a_{ii} \in R^\times, \forall i \in \{1,\dots,n\}].$$

Επομένως, $\mathrm{UT}_n(R)^\times \subseteq \{\mathbf{A} = (a_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{UT}_n(R) \mid a_{ii} \in R^\times \,, \forall i \in \{1,\dots,n\}\}$. Ο αντίστροφος εγκλεισμός "$\supseteq$" είναι προφανής. Η δεύτερη ισότητα (που αφορά στους αντιστρέψιμους κάτω τριγωνικούς πίνακες) αποδεικνύεται παρομοίως. □

A.2.22 Πρόταση. *Εάν R είναι ένας μη τετριμμένος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, τότε το σύνολο*

$$\boxed{\mathrm{SL}_n(R) := \{\mathbf{A} \in \mathrm{GL}_n(R) \mid \det(\mathbf{A}) = 1_R\}}$$

*αποτελεί μια υποομάδα τής $\mathrm{GL}_n(R)$ (τη λεγόμενη **ειδική γραμμική ομάδα** βαθμού n υπεράνω τού R) που είναι γνήσια όταν $1_R \neq -1_R$.*

Απόδειξη. Προφανώς, $\mathbf{I}_n \in \mathrm{SL}_n(R)$ και για οιουσδήποτε πίνακες $\mathbf{A}, \mathbf{B} \in \mathrm{SL}_n(R)$ έχουμε

$$\det\left(\mathbf{A}\mathbf{B}^{-1}\right) = \det(\mathbf{A})\det\left(\mathbf{B}^{-1}\right) = \det(\mathbf{A})\det(\mathbf{B})^{-1} = 1_R$$

(δυνάμει των (A.11) και (A.18)), οπότε $\mathrm{SL}_n(R) \sqsubseteq \mathrm{GL}_n(R)$ (βλ. πρόταση 3.2.16). Εξάλλου, όταν $1_R \neq -1_R$, έχουμε[5]

$$\begin{pmatrix} -1_R & 0_R & \cdots & 0_R & 0_R \\ 0_R & 1_R & \cdots & 0_R & 0_R \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0_R & 0_R & \cdots & 1_R & 0_R \\ 0_R & 0_R & \cdots & 0_R & 1_R \end{pmatrix} \in \mathrm{GL}_n(R) \smallsetminus \mathrm{SL}_n(R)\,,$$

απ' όπου έπεται ότι $\mathrm{SL}_n(R) \sqsubset \mathrm{GL}_n(R)$. □

A.2.23 Πρόταση. *Εάν R είναι ένας μη τετριμμένος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, τότε το σύνολο $\mathrm{UT}_n^{[1]}(R)$ (και αντιστοίχως, το $\mathrm{LT}_n^{[1]}(R)$, βλ.* A.1.6 (iii)*), εφοδιαζόμενο με τον πολλαπλασιασμό τετραγωνικών πινάκων, αποτελεί μια υποομάδα τής $\mathrm{SL}_n(R)$ (τη λεγόμενη **ομάδα των μοναδιαίως άνω,** και αντιστοίχως, **των μοναδιαίως κάτω τριγωνικών** $(n\times n)$**-πινάκων** υπεράνω τού R).*

Απόδειξη. Αφήνεται ως άσκηση. □

A.2.24 Παράδειγμα. Για οιονδήποτε μη τετριμμένο μεταθετικό δακτύλιο R με μοναδιαίο στοιχείο η ομάδα των μοναδιαίως άνω τριγωνικών (3×3)-πινάκων

$$\mathbf{Heis}(R) := \mathrm{UT}_3^{[1]}(R) = \left\{ \begin{pmatrix} 1_R & a & c \\ 0_R & 1_R & b \\ 0_R & 0_R & 1_R \end{pmatrix} \middle| \, a,b,c \in R \right\}$$

[5] Αντιθέτως, για το σώμα $\mathbb{Z}_2$ χαρακτηριστικής 2 λαμβάνουμε $\mathrm{SL}_2(\mathbb{Z}_2) = \mathrm{GL}_2(\mathbb{Z}_2)$.

καλείται (κλασική) **ομάδα τού Heisenberg** υπεράνω τού R.

A.2.25 Ορισμός. Μέσω των προτάσεων A.1.5, A.2.17 και 3.2.16 είναι άμεσος ο έλεγχος τού ότι το σύνολο

$$\boxed{\mathrm{O}_n(F) := \left\{\mathbf{A} \in \mathrm{GL}_n(F) \;\middle|\; \mathbf{A}^{\intercal} = \mathbf{A}^{-1}\right\}}$$

αποτελεί μια υποομάδα τής $(\mathrm{GL}_n(F), \cdot)$ για οιοδήποτε σώμα F. Αυτή η υποομάδα καλείται, ιδιαιτέρως, **ορθογώνια ομάδα** βαθμού n (και τα στοιχεία της **ορθογώνιοι πίνακες**) υπεράνω τού F, ενώ η ομάδα

$$\boxed{\mathrm{SO}_n(F) := \mathrm{O}_n(F) \cap \mathrm{SL}_n(F)}$$

καλείται **ειδική ορθογώνια ομάδα** βαθμού n υπεράνω τού F.

A.2.26 Ορισμός. Για οιοδήποτε σώμα F ορίζουμε τον $(2n \times 2n)$-πίνακα

$$\widehat{\mathbf{I}}_n := \left(\begin{array}{c|c} \mathbf{0}_{n\times n} & \mathbf{I}_n \\ \hline -\mathbf{I}_n & \mathbf{0}_{n\times n} \end{array}\right) \in \mathrm{GL}_{2n}(F).$$

Το σύνολο[6]

$$\boxed{\mathrm{Sp}_n(F) := \left\{\mathbf{A} \in \mathrm{GL}_{2n}(F) \;\middle|\; \mathbf{A}^{\intercal} \cdot \widehat{\mathbf{I}}_n = \widehat{\mathbf{I}}_n \cdot \mathbf{A}^{-1}\right\}}$$

αποτελεί μια υποομάδα τής $(\mathrm{GL}_{2n}(F), \cdot)$, τη λεγόμενη **συμπλεκτική ομάδα** βαθμού n υπεράνω τού F. (Τα στοιχεία τής $\mathrm{Sp}_n(F)$ καλούνται **συμπλεκτικοί πίνακες** υπεράνω τού F.)

A.2.27 Παρατήρηση. (i) $\mathbf{A} \in \mathrm{Sp}_n(F) \iff \mathbf{A}^{\intercal} \in \mathrm{Sp}_n(F)$ (διότι $\widehat{\mathbf{I}}_n^{-1} = -\widehat{\mathbf{I}}_n$).
(ii) Εάν $n = 1$, τότε $\mathrm{Sp}_1(F) = \mathrm{SL}_2(F)$. Πράγματι· για κάθε $\mathbf{A} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(F)$ έχουμε αφ' ενός μεν

$$\mathbf{A}^{\intercal} \cdot \widehat{\mathbf{I}}_1 = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} 0_F & 1_F \\ -1_F & 0_F \end{pmatrix} = \begin{pmatrix} -c & a \\ -d & b \end{pmatrix},$$

αφ' ετέρου δε

$$\widehat{\mathbf{I}}_1 \cdot \mathbf{A}^{-1} = \begin{pmatrix} 0_F & 1_F \\ -1_F & 0_F \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = (ad - bc)^{-1} \begin{pmatrix} -c & a \\ -d & b \end{pmatrix}.$$

Προφανώς, $\mathbf{A}^{\intercal} \cdot \widehat{\mathbf{I}}_1 = \widehat{\mathbf{I}}_1 \cdot \mathbf{A}^{-1} \Leftrightarrow (ad - bc)^{-1} = 1_F \Leftrightarrow ad - bc = 1_F$.

A.2.28 Ορισμός. Εάν ως $\overline{z}$ συμβολίσουμε τον *συζυγή* οιουδήποτε $z \in \mathbb{C}$ και $\mathbf{A} = (z_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{Mat}_{n\times n}(\mathbb{C})$, τότε λέμε ότι ο πίνακας $\overline{\mathbf{A}} := (\overline{z_{ij}})_{1\leqslant i,j\leqslant n}$ είναι ο **συζυγής** και ο πίνακας $\overline{\mathbf{A}}^{\intercal}$ ο **αναστροφοσυζυγής** τού $\mathbf{A}$.

A.2.29 Πρόταση. *Εάν* $\mathbf{A}, \mathbf{B} \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ *και* $z \in \mathbb{C}$, *τότε ισχύουν τα κάτωθι*:
(i) $\overline{\mathbf{A} + \mathbf{B}} = \overline{\mathbf{A}} + \overline{\mathbf{B}}$, $\overline{z\mathbf{A}} = \overline{z}\,\overline{\mathbf{A}}$ *και* $\overline{\mathbf{A} \cdot \mathbf{B}} = \overline{\mathbf{A}} \cdot \overline{\mathbf{B}}$.
(ii) $\overline{\mathbf{A}^{\intercal}} = \overline{\mathbf{A}}^{\intercal}$.

[6] Προσοχή! Ορισμένοι συγγραφείς χρησιμοποιούν το σύμβολο $\mathrm{Sp}_{2n}(F)$ *αντί τού* $\mathrm{Sp}_n(F)$.

(iii) *Εάν* $\mathbf{A} \in \mathrm{GL}_n(\mathbb{C})$, *τότε* $\overline{\mathbf{A}} \in \mathrm{GL}_n(\mathbb{C})$ *και* $(\overline{\mathbf{A}})^{-1} = \overline{\mathbf{A}^{-1}}$.

Αποδειξη. Αφήνεται ως άσκηση. □

Α.2.30 Ορισμός. Μέσω των προτάσεων Α.1.5, Α.2.17, Α.2.29 και 3.2.16 είναι άμεσος ο έλεγχος τού ότι το σύνολο

$$\boxed{\mathrm{U}_n(\mathbb{C}) := \left\{ \mathbf{A} \in \mathrm{GL}_n(\mathbb{C}) \;\middle|\; \overline{\mathbf{A}}^{\mathsf{T}} = \mathbf{A}^{-1} \right\}}$$

αποτελεί μια υποομάδα τής $(\mathrm{GL}_n(\mathbb{C}), \cdot)$. Αυτή η υποομάδα καλείται, ιδιαιτέρως, **μοναδιακή ομάδα** βαθμού n (και τα στοιχεία της **μοναδιακοί πίνακες**) υπεράνω τού $\mathbb{C}$, ενώ η ομάδα

$$\boxed{\mathrm{SU}_n(\mathbb{C}) := \mathrm{U}_n(\mathbb{C}) \cap \mathrm{SL}_n(\mathbb{C})}$$

καλείται **ειδική μοναδιακή ομάδα** βαθμού n υπεράνω τού $\mathbb{C}$.

Α.2.31 Παρατήρηση. Εάν χρησιμοποιήσουμε τη συνήθη «ταύτιση» των $\mathbb{C}^n$ και $\mathbb{R}^{2n}$ μέσω τής αμφιρρίψεως

$$\mathbb{C}^n \ni (z_1, ..., z_n) \longmapsto (x_1, ..., x_n, y_1, ..., y_n) \in \mathbb{R}^{2n},$$

όπου $z_j := x_j + iy_j$, $\forall j \in \{1, ..., n\}$, τότε μπορούμε να ταυτίσουμε την $\mathrm{GL}_n(\mathbb{C})$ με μια υποομάδα τής $\mathrm{GL}_{2n}(\mathbb{R})$ και να συμπεράνουμε ότι

$$\mathrm{U}_n(\mathbb{C}) = \mathrm{O}_{2n}(\mathbb{R}) \cap \mathrm{GL}_n(\mathbb{C}) = \mathrm{O}_{2n}(\mathbb{R}) \cap \mathrm{Sp}_n(\mathbb{R}) = \mathrm{GL}_n(\mathbb{C}) \cap \mathrm{Sp}_n(\mathbb{R}).$$