ΚΕΦΑΛΑΙΟ 1

Εισαγωγικές έννοιες

Το πρώτο κεφάλαιο είναι εισαγωγικό. Σε αυτό παγιώνονται ορισμένοι βασικοί συμβολισμοί, περιγράφονται κάποιες σημαντικές ιδιότητες εσωτερικών πράξεων και δίδονται χαρακτηριστικά παραδείγματα *ομαδοειδών*, *ημιομάδων* και *μονοειδών* (που αποτελούν τους «προπομπούς» των *ομάδων*).

1.1 ΣΥΜΒΟΛΙΣΜΟΙ ΚΑΙ ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ

► **Σύμβολα από τη Θεωρία Συνόλων**. Συνήθη σύμβολα από τον προτασιακό και τον συνολοθεωρητικό λογισμό, όπως π.χ. τα σύμβολα «$\in$», «$\forall$», «$\exists$», «$\Longrightarrow$», «$\Longleftrightarrow$», «$=$», τού «ανήκειν», τού «για κάθε», τού «υπάρχειν», τής απλής και αμφίπλευρης συνεπαγωγής, και τού «ίσον», αντιστοίχως, καθώς και τα σύμβολα «$\cup$», «$\cap$», «$\subseteq$», «$\subsetneq$», «$\times$», «$\varnothing$», τής «ενώσεως», τής «τομής», τού (συνολοθεωρητικού) «περιέχεσθαι» και «γνησίως περιέχεσθαι», τού «καρτεσιανού γινομένου» και τού κενού συνόλου, χρησιμοποιούνται ελευθέρως εντός τού κυρίως κειμένου.

► **Σύνολα αριθμών**. Τηρούμε τους «συνήθεις» συμβολισμούς: $\mathbb{Z}$ για το σύνολο των *ακεραίων αριθμών*, $\mathbb{N} := \{\, a \in \mathbb{Z} |\ a > 0\}$ για το σύνολο των *φυσικών αριθμών* (ήτοι των θετικών ακεραίων), $\mathbb{N}_0 := \{\, a \in \mathbb{Z} |\ a \geq 0\}$ για το σύνολο των *μη αρνητικών ακεραίων αριθμών*, $\mathbb{Q}, \mathbb{R}, \mathbb{C},$ για τα σύνολα των *ρητών*, των *πραγματικών* και *μιγαδικών αριθμών*, και $\mathbb{Q}_{>0}, \mathbb{R}_{>0}$ για τα σύνολα των *θετικών ρητών* και *θετικών πραγματικών αριθμών*, αντιστοίχως.

► **Το σύνολο $\mathbb{Z}_m$**. Η διμελής σχέση ισοτιμίας (κατά παγιωμένο μόδιο $m \in \mathbb{N}$):

$$a \sim_m b \underset{\text{ορσ}}{\Longleftrightarrow} a \equiv b (\mathrm{mod}\, m)$$

αποτελεί μια σχέση ισοδυναμίας επί τού συνόλου $\mathbb{Z}$ των ακεραίων. Για να δώσουμε έμφαση στην εξάρτηση από το m συμβολίζουμε ως

$$..., [-2]_m, [-1]_m, [0]_m, [1]_m, [2]_m, ...$$

τις κλάσεις ισοδυναμίας των ακεραίων αριθμών (ως προς τη σχέση " $\sim_m$ ") και ως $\mathbb{Z}_m := \mathbb{Z}/\sim_m$το *σύνολο των κλάσεων υπολοίπων (ή κλάσεων ισοτιμίας) των ακεραίων κατά μόδιο* m (ή *modulo* m). Το ανωτέρω σύνολο γράφεται (βάσει τής προτάσεως Β.4.37) σε «ανηγμένη» μορφή[1] ως ακολούθως:

$$\mathbb{Z}_m = \{[0]_m, [1]_m, ..., [m-1]_m\}. \tag{1.1}$$

► **Προαπαιτούμενες γνώσεις**. Υποτίθεται ότι οι αναγνώστες είναι εξοικειωμένοι με τις έννοιες τής απεικονίσεως, τής συνθέσεως απεικονίσεων, τού μεταθετικού διαγράμματος, τής ενριπτικής (= 1-1), επιριπτικής (= επί-) και αμφιριπτικής (= ένα προς ένα και επί) απεικονίσεως[2] (και τής αντιστρόφου μιας αμφιριπτικής απεικονίσεως), τής σχέσεως ισοδυναμίας και τής σχέσεως διατάξεως (βλ. παράρτημα **Α**), τού λογισμού με πληθικούς αριθμούς συνόλων[3], καθώς και με τις βασικές έννοιες από τη Στοιχειώδη Θεωρία Αριθμών (διαιρετότητα ακεραίων, μκδ, εκπ, πρώτοι αριθμοί, ισοτιμίες κ.λπ.) και τη Γραμμική Άλγεβρα (που συνοψίζονται στα παραρτήματα **Β**, **D** και **Ε**), και με τις αποδεικτικές μεθόδους τής «εις άτοπον απαγωγής» και τής «μαθηματικής επαγωγής» (πρώτης[4] και δεύτερης[5] μορφής).

1.2 ΕΣΩΤΕΡΙΚΕΣ ΠΡΑΞΕΙΣ

1.2.1 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

[1] Τούτο σημαίνει ότι τα εντός των αγκίστρων αναγραφόμενα στοιχεία είναι *σαφώς διακεκριμένα* (ήτοι ανά δύο διαφορετικά, αποκλείοντας την επανάληψη κάποιου εξ αυτών).

[2] Ενίοτε, αντί των όρων *ενριπτική /επιριπτική /αμφιριπτική απεικόνιση* χρησιμοποιούνται οι (συντομότεροι) όροι *ένριψη /επίριψη /αμφίριψη*.

[3] Ο *πληθικός αριθμός* ενός συνόλου Ω θα συμβολίζεται ως $\mathrm{card}(\Omega)$.

[4] **Πρώτη μορφή μαθηματικής επαγωγής**. Έστω $n_0 \in \mathbb{N}_0$. Εάν ο ΠΡ(n) είναι ένας προτασιακός τύπος με σύνολο αναφοράς του το $\{\, n \in \mathbb{N}_0 \mid n \geq n_0 \}$, τέτοιος ώστε

(i) η πρόταση ΠΡ(n_0) να είναι αληθής και

(ii) η συνεπαγωγή ΠΡ$(k) \Rightarrow$ ΠΡ$(k+1)$ να ισχύει για κάθε ακέραιο αριθμό $k \geq n_0$,

τότε *η πρόταση* ΠΡ(n) *είναι αληθής για κάθε ακέραιο αριθμό* $n \geq n_0$.

[5] **Δεύτερη μορφή μαθηματικής επαγωγής**. Έστω $n_0 \in \mathbb{N}_0$. Εάν ο ΠΡ(n) είναι ένας προτασιακός τύπος με σύνολο αναφοράς του το $\{\, n \in \mathbb{N}_0 \mid n \geq n_0 \}$, τέτοιος ώστε

(i) η πρόταση ΠΡ(n_0) να είναι αληθής και

(ii) η συνεπαγωγή

$$\left.\begin{array}{r} \text{ΠΡ}(n_0), \\ \text{ΠΡ}(n_0+1), \\ \vdots \\ \text{και ΠΡ}(k) \end{array}\right\} \Longrightarrow \text{ΠΡ}(k+1)$$

να ισχύει για κάθε ακέραιο αριθμό $k \geq n_0$, τότε *η πρόταση* ΠΡ(n) *είναι αληθής για κάθε ακέραιο αριθμό* $n \geq n_0$.

διάφορα τού κενού, τα οποία είναι εφοδιασμένα με μία τουλάχιστον (εσωτερική ή εξωτερική) πράξη[6].

Πρόκειται να εστιάσουμε την προσοχή μας στις κύριες ιδιότητες ορισμένων αλγεβρικών δομών που αποτελούνται από μη κενά σύνολα εφοδιασμένα με *μία και μόνον εσωτερική πράξη* (ομαδοειδή, ημιομάδες, μονοειδή και ομάδες), αν και δεν θα παραλείψουμε να αναφερόμαστε εν συντομία και σε κάποιες άλλες δομές όταν αυτό κρίνεται απαραίτητο ως *συμπληρωματική πληροφορία*. (Πρβλ. παραρτήματα **C**, **D** και **E**.)

1.2.2 Σημείωση. Έστω $\psi : A \times A \longrightarrow A$ μια εσωτερική πράξη επί ενός συνόλου $A \neq \varnothing$. Θεωρούμε τυχόν υποσύνολο $C \neq \varnothing$ τού A. Προφανώς, ο περιορισμός $\psi|_{C\times C} : C \times C \longrightarrow A$ τής απεικονίσεως ψ στο σύνολο $C \times C$ ορίζει μια εσωτερική πράξη *επί τού* C (υπό την έννοια τού 1.2.1) 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

$$\boxed{\mathrm{Im}(\psi|_{C\times C}) \subseteq C.} \tag{1.2}$$

Στην περίπτωση κατά την οποία ισχύει ο εγκλεισμός (1.2) 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 θεωρούμενων αλγεβρικών δομών.)

1.2.3 Ορισμός. Έστω $\psi : A \times A \longrightarrow A$ μια εσωτερική πράξη επί ενός $A \neq \varnothing$.
(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**).

1.2.4 Σημείωση. Η $\psi : A \times A \longrightarrow A$ είναι προσεταιριστική εάν και μόνον εάν το ακόλουθο διάγραμμα είναι μεταθετικό:

$$\begin{array}{ccc} A \times A \times A & \xrightarrow{\psi\times \mathrm{id}_A} & A \times A \\ \downarrow{\scriptstyle \mathrm{id}_A\times\psi} & & \downarrow{\scriptstyle \psi} \\ A \times A & \xrightarrow[\psi]{} & A \end{array}$$

[6]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*). Βλ. παράρτημα **E**.

Εν προκειμένω, υπονοείται η ταύτιση των $(A \times A) \times A$ και $A \times (A \times A)$ με το[7] $A \times A \times A$ (όπου τα στοιχεία τής μορφής $((x, y), z)$ και $(x, (y, z))$ ταυτίζονται με το (x, y, z)).

1.2.5 Παραδείγματα. Έστω Ω ένα σύνολο. Εάν ως $\mathfrak{P}(\Omega)$ συμβολίσουμε το δυναμοσύνολό του[8], τότε ισχύουν τα εξής:

(i) Η απεικόνιση

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

αποτελεί μια εσωτερική πράξη επί τού $\mathfrak{P}(\Omega)$, η οποία είναι προσεταιριστική και μεταθετική.

(ii) Το ίδιο ισχύει και για την απεικόνιση

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

(iii) Η απεικόνιση

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

(όπου[9] $A \triangle B := (A \smallsetminus B) \cup (B \smallsetminus A)$ η *συμμετρική διαφορά* των A και B) είναι ωσαύτως προσεταιριστική και μεταθετική.

(iv) Η απεικόνιση

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

δεν είναι (εν γένει) ούτε προσεταιριστική ούτε μεταθετική.

1.2.6 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

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

[7] 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 $z = z'$.

[8] Το **δυναμοσύνολο** $\mathfrak{P}(\Omega)$ τού Ω είναι το σύνολο που έχει ως στοιχεία του όλα τα υποσύνολα τού Ω. 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!)

[9] $A \smallsetminus B := \{ x \in A \mid x \notin B \}$.

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

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

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

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

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!

1.2.8 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.*

ΑΠΟΔΕΙΞΗ. 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. □

1.2.9 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.

1.2.10 Παραδείγματα. Έστω Ω ένα σύνολο. Το δυναμοσύνολο $\mathfrak{P}(\Omega)$ τού Ω διαθέτει πάντοτε ουδέτερο στοιχείο ως προς τις εσωτερικές (μεταθετικές) πράξεις τις ορισθείσες επ' αυτού στα (i), (ii) και (iii) τού εδαφίου 1.2.5. Συγκεκριμένα, το ουδέτερο στοιχείο του ως προς την πράξη 1.2.5 (i) είναι το $\varnothing$, ως προς την 1.2.5 (ii) το Ω και ως προς την πράξη 1.2.5 (iii) το $\varnothing$.

1.2.11 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[10] 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

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

1.2.12 Παράδειγμα. Έστω A ένα μη κενό σύνολο και έστω $A^A = \text{ΑΠ}(A, A)$ το σύνολο των απεικονίσεων[11] από το A στο A. 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. Προφανώς, η *ταυτοτική απεικόνιση*[12] id_A αποτελεί το ουδέτερο στοιχείο τού A^A ως προς την ψ. Επίσης, ως γνωστόν, 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*.

1.2.13 Πρόταση. *Ας 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.*

[10] Κατά την πρόταση 1.2.8 το e είναι μονοσημάντως ορισμένο.

[11] Γενικότερα, εάν τα A, B είναι δυο μη κενά σύνολα, τότε το σύνολο των απεικονίσεων από το A στο B συμβολίζεται ως $\text{ΑΠ}(A, B)$ ή ως B^A. (Σημειωτέον ότι το σύμβολο B^A, το οποίο φαντάζει κατά τι «παράξενο» εκ πρώτης όψεως, πιθανώς να είναι το πλέον κατάλληλο για να εκφράσει αυτές τις απεικονίσεις, τουλάχιστον στο πλαίσιο τής Θεωρίας Συνόλων, καθώς ισχύει η ισότητα $\text{card}(B^A) = \text{card}(B)^{\text{card}(A)}$.)

[12] Πρόκειται για την απεικόνιση $\text{id}_A : A \longrightarrow A$ με $\text{id}_A(a) := a, \forall a \in A$.

ΑΠΟΔΕΙΞΗ. Προφανώς,

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

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. □

1.2.14 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.

1.2.15 Παραδείγματα. Έστω Ω ένα σύνολο. Στο εδάφιο 1.2.10 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 1.2.5. Είναι εύκολο να διαπιστωθεί ότι δεν υφίσταται συμμετρικό στοιχείο οιουδήποτε μη κενού συνόλου $A \in \mathfrak{P}(\Omega)$ ως προς την 1.2.5 (i), ότι δεν υφίσταται συμμετρικό στοιχείο οιουδήποτε γνησίου υποσυνόλου A τού συνόλου Ω ως προς την 1.2.5 (ii) και ότι κάθε $A \in \mathfrak{P}(\Omega)$ έχει ως (μοναδικό του) συμμετρικό στοιχείο ως προς την 1.2.5 (iii) το ίδιο το A.

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

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

είναι εσωτερικές πράξεις επ' αυτών. Θεωρούμε την εσωτερική πράξη

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

την οριζόμενη επί τού καρτεσιανού γινομένου[13] $A \times B$. *Τότε ισχύουν τα εξής*:

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

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

(iii) *Εάν τα e_A, e_B είναι (εξ αριστερών/εκ δεξιών/αμφιπλεύρως) ουδέτερα στοιχεία*

[13] Σημειωτέον ότι $(\phi, \psi) = (\phi \times \psi) \circ \vartheta$, όπου

$$\phi \times \psi : (A \times A) \times (B \times B) \longrightarrow A \times B, \;\; ((x,y),(z,t)) \longmapsto (\phi(x,y), \psi(z,t))$$

το *καρτεσιανό γινόμενο* των ϕ και ψ, και $\vartheta : (A \times B) \times (A \times B) \longrightarrow (A \times A) \times (B \times B)$ η *αμφίρριψη* η οριζόμενη από τον τύπο $\vartheta((x,z),(y,t)) := ((x,y),(z,t))$.

τού A και B ως προς τις πράξεις χ 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 (χ, ψ).

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

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

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

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

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

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

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

οπότε το (e_A, e_B) είναι εξ αριστερών ουδέτερο στοιχείο τού $A \times B$ ως προς την πράξη (χ, 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 χ και ψ, αντιστοίχως, τότε

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

Οι λοιπές περιπτώσεις αντιμετωπίζονται παρομοίως. □

1.2.17 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 $\psi\left(x, y\right)$ 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 "$\circledcirc$",

$$A \times A \longrightarrow A,\ (x, y) \longmapsto x \circledcirc y \tag{1.3}$$

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

$$(x \circledcirc y) \circledcirc z = x \circledcirc (y \circledcirc z) \tag{1.4}$$

για οιαδήποτε $x, y, z \in A$, *μεταθετική* όταν[14]

$$x \circledcirc y = y \circledcirc x \tag{1.5}$$

για οιαδήποτε $x, y \in A$, κ.ο.κ.

1.2.18 Παρατήρηση. Δοθείσας μιας προσεταιριστικής πράξεως (1.3), η ισότητα (1.4) μας πληροφορεί ότι η διπλή εκτέλεση τής "$\circledcirc$" μεταξύ τριών στοιχείων x, y και z (διατηρώντας τή σειρά παραθέσεως των x, y, z αμετάβλητη) *δεν επηρεάζεται από τη μετακίνηση των παρενθέσεων*[15]. Κατά συνέπειαν, καθ' οιονδήποτε τρόπο και 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.

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

Λαμβάνουμε, εν τοιαύτη περιπτώσει, εκ νέου το ίδιο αποτέλεσμα; Όπως δείχνει η επόμενη πρόταση, η απάντηση είναι όντως καταφατική, και μάλιστα σε πλήρη γενικότητα.

1.2.19 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 $(a_1, a_2,..., a_n) \in A^n$ 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 $a_1, a_2,..., a_n$, 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* $\nu \in \mathbb{N}$, $\nu \leq n$, ορίζουμε μια απεικόνιση

$$f_\nu : A^\nu \longrightarrow \mathfrak{P}(A)$$

[14] Όταν ισχύει η (1.5), τότε λέμε ότι τα x και y **μετατίθενται αμοιβαίως** ύστερα από εφαρμογή τής πράξεως "$\circledcirc$".

[15] 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).

μέσω τού αναδρομικού τύπου $f_1 := \mathrm{id}_A$ και

$$f_\nu\left(\xi_1,\xi_2,...,\xi_\nu\right) := \left\{ b \circledcirc c \;\middle|\; \begin{array}{l} b \in f_l\left(\xi_1,...,\xi_l\right),\ c \in f_m\left(\xi_{l+1},...,\xi_\nu\right) \\ \text{για κάποια } \ l,m \in \mathbb{N} : l+m=\nu \end{array} \right\}.$$

Τα στοιχεία τού υποσυνόλου $f_n\left(a_1,a_2,...,a_n\right) \subseteq A$ είναι ουσιαστικώς όλοι οι δυνατοί σχηματισμοί τού

$$\text{“}a_1 \circledcirc \cdots \circledcirc a_n\text{”}$$

(με παγιωμένη τη σειρά παραθέσεως των $a_1,...,a_n$) κατόπιν παρεμβολής οιωνδήποτε (δυνατών) «παρενθέσεων», όπως π.χ. είναι ο σχηματισμός

$$\left(\left(a_1 \circledcirc a_2\right) \circledcirc \left(a_3 \circledcirc a_4\right)\right) \circledcirc \left(a_5 \circledcirc \left(a_6 \circledcirc a_7\right)\right)$$

για $n=7$. Ισχυριζόμαστε ότι ισχύει η ισότητα

$$f_n\left(a_1,a_2,...,a_n\right) = \{(\cdots((a_1 \circledcirc a_2) \circledcirc a_3) \circledcirc \cdots)\cdots) \circledcirc a_n\},\ \ \forall n \in \mathbb{N}, \tag{1.6}$$

ήτοι ότι το σύνολο $f_n\left(a_1,a_2,...,a_n\right)$ 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 (1.6), τότε αποδεικνύεται *αυτομάτως* και η πρόταση 1.2.19). Όταν $n \leq 3$, η (1.6) είναι προφανής. Για $n \geq 4$ εφαρμόζουμε τη δεύτερη μορφή τής μαθηματικής επαγωγής ως προς το n εκκινώντας από το $n_0 = 3$. Η επαγωγική μας υπόθεση είναι η εξής:

$$f_j(\xi_1,\xi_2,...,\xi_j) = \{(\cdots((\xi_1 \circledcirc \xi_2) \circledcirc \xi_3) \circledcirc \cdots)\cdots) \circledcirc \xi_j\},$$

για *οιαδήποτε* $(\xi_1,\xi_2,...,\xi_j) \in A^j$, όπου $j,k \in \mathbb{N}$ και $3 \leq j \leq k$. Θεωρούμε το σύνολο

$$f_{k+1}\left(a_1,...,a_{k+1}\right) \subseteq A.$$

Εξ ορισμού, *οιοδήποτε* στοιχείο του $d \in f_{k+1}\left(a_1,a_2,...,a_{k+_{\mathbb{N}}1}\right)$ γράφεται υπό τη μορφή

$$d = b \circledcirc c, \quad b \in f_l\left(a_1,...,a_l\right),\ c \in f_m\left(a_{l+1},...,a_{k+1}\right),$$

όπου $l,m \in \mathbb{N}$, τέτοιοι ώστε $l+m = k+1$. Εξετάζουμε δύο περιπτώσεις χωριστά:
(a) Εάν $m=1$, ήτοι $c = a_{k+1}$, τότε, κατά την επαγωγική μας υπόθεση,

$$b = (\cdots((a_1 \circledcirc a_2) \circledcirc a_3) \circledcirc \cdots)\cdots) \circledcirc a_k,$$

οπότε

$$d = ((\cdots((a_1 \circledcirc a_2) \circledcirc a_3) \circledcirc \cdots)\cdots) \circledcirc a_k) \circledcirc a_{k+1}.$$

(b) Εάν $m > 1$ και $q = m-1$, τότε κατά την επαγωγική μας υπόθεση

$$c = w \circledcirc a_{k+1}, \ \text{ για κάποιο } \ w \in f_q\left(a_{l+1},...,a_k\right),$$

και $b = (\cdots((a_1 \circledcirc a_2) \circledcirc a_3) \circledcirc \cdots) \cdots) \circledcirc a_l$. Τούτο σημαίνει ότι

$$\begin{aligned} d &= [(\cdots((a_1 \circledcirc a_2) \circledcirc a_3) \circledcirc \cdots) \cdots) \circledcirc a_l] \circledcirc [w \circledcirc a_{k+1}] \\ &= [(\cdots((a_1 \circledcirc a_2) \circledcirc a_3) \circledcirc \cdots) \cdots) \circledcirc a_l \circledcirc w] \circledcirc a_{k+1} \end{aligned}$$

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 $a_1,...,a_k$, 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

$$d = ((\cdots((a_1 \circledcirc a_2) \circledcirc a_3) \circledcirc \cdots) \cdots) \circledcirc a_k) \circledcirc a_{k+1}.$$

Από τα (a) και (b) συμπεραίνουμε ότι η (1.6) είναι αληθής *για κάθε* $n \in \mathbb{N}$. □

1.3 ΟΜΑΔΟΕΙΔΗ, ΗΜΙΟΜΑΔΕΣ ΚΑΙ ΜΟΝΟΕΙΔΗ

1.3.1 Ορισμός. Κάθε ζεύγος $(A, \circledcirc)$, αποτελούμενο από ένα μη κενό σύνολο A και μία εσωτερική πράξη

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

επί τού A, ονομάζεται **ομαδοειδές**[16]. (Το A καλείται **υποκείμενο σύνολο** τού ομαδοειδούς $(A, \circledcirc)$.)

1.3.2 Ορισμός. Έστω $(A, \circledcirc)$ ένα ομαδοειδές. Το $(A, \circledcirc)$ καλείται

(i) **προσεταιριστικό ομαδοειδές** ή **ημιομάδα** όταν η πράξη "$\circledcirc$" είναι *προσεταιριστική* (βλ. 1.2.3 (i)),

(ii) **μεταθετικό ομαδοειδές** ή **αβελιανό ομαδοειδές** όταν η πράξη "$\circledcirc$" είναι *μεταθετική* (βλ. 1.2.3 (ii)), και

(iii) **αβελιανή ημιομάδα** όταν αυτό είναι ταυτοχρόνως προσεταιριστικό και αβελιανό ομαδοειδές.

1.3.3 Ορισμός. Κάθε ημιομάδα (και αντιστοίχως, κάθε αβελιανή ημιομάδα) η οποία διαθέτει *ουδέτερο στοιχείο* ως προς την πράξη την ορισθείσα επ' αυτής (βλ. 1.2.6 (iii)) ονομάζεται **μονοειδές** (και αντιστοίχως, **αβελιανό μονοειδές**).

1.3.4 Σημείωση. Εάν μια ημιομάδα (ή, γενικότερα, ένα ομαδοειδές) διαθέτει ουδέτερο στοιχείο, τότε αυτό, σύμφωνα με την πρόταση 1.2.8, είναι μονοσημάντως ορισμένο.

[16] Αντ' αυτού χρησιμοποιείται ενίοτε και ο όρος **μάγμα**.

1.3.5 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. 1.2.5(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. 1.2.12).
(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[17] "$+$" και "$\cdot$":

$$([a]_m, [b]_m) \longmapsto [a]_m + [b]_m, \quad ([a]_m, [b]_m) \longmapsto [a]_m \cdot [b]_m. \tag{1.7}$$

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 Β.4.41 και Β.4.42.)
(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. 1.2.5 (i), (ii) και (iii), και 1.2.10.)

[17] Επειδή κατά την εφαρμογή των ορισμών (Β.51) οι ακέραιοι $a + b$ και ab ενδέχεται να είναι $\geq m$ (ακόμη και όταν οι a και b είναι ειλημμένοι από το σύνολο $\{0, 1, \ldots, m-1\}$), εάν επιθυμούμε να παραμείνουμε στην περιγραφή (1.1) 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.

1.3.6 Παράδειγμα. Εάν οι m και n είναι δυο φυσικοί αριθμοί και το A ένα μη κενό σύνολο, τότε κάθε απεικόνιση

$$f : \{1, 2,..., m\} \times \{1, 2,..., n\} \longrightarrow A \tag{1.8}$$

ονομάζεται $(m \times n)$-**πίνακας** με τις «εγγραφές[18]» του ειλημμένες από το A. Αντί τού σχετικώς δύσχρηστου συμβολισμού (1.8) 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 $(a_{jk})_{1\leq j\leq m, 1\leq k\leq n}$, όπου

$$a_{jk} := f\,(j, k)\,,\ \forall\,(j, k) \in \{1, 2,..., m\} \times \{1, 2,..., n\}.$$

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

$$(a_{jk})_{1\leq j\leq m, 1\leq k\leq n}\ \widehat{\circledcirc}\ (b_{jk})_{1\leq j\leq m, 1\leq k\leq n} := (a_{jk} \circledcirc b_{jk})_{1\leq j\leq m, 1\leq k\leq n},$$

για κάθε ζεύγος

$$((a_{jk})_{1\leq j\leq m, 1\leq k\leq n}, (b_{jk})_{1\leq j\leq m, 1\leq k\leq n}) \in \mathrm{Mat}_{m\times n}(A) \times \mathrm{Mat}_{m\times n}(A).$$

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**[19]. Εν προκειμένω, το $(\mathrm{Mat}_{m\times n}(A), +)$ είναι *αβελιανό μονοειδές*.

[18] Οι **εγγραφές** (αγγλ. entries) ενός πίνακα (1.8) είναι οι $m \times n$ εικόνες τής f.

[19] Το ίδιο σύμβολο "$+$" χρησιμοποιείται *και* για τη σημείωση τής προσθέσεως πινάκων με τις εγγραφές τους ειλημμένες από *τυχόντες* δακτυλίους $(R, +, \cdot)$. Βλ. (D.4).

Ασκήσεις

1-1. Επί τού $\mathbb{N}$ ορίζονται οι εσωτερικές πράξεις $(m,n) \longmapsto m *_1 n := m^n$,

$$(m,n) \longmapsto m *_2 n := \text{μκδ}(m,n) \ \text{ και } \ (m,n) \longmapsto m *_3 n := \text{εκπ}(m,n).$$

Να αποδειχθούν τα ακόλουθα:

(i) Η "$*_1$" δεν είναι ούτε προσεταιριστική ούτε μεταθετική, το δε 1 είναι ουδέτερο στοιχείο *μόνον εκ δεξιών* (ως προς αυτήν).

(ii) Η "$*_2$" είναι προσεταιριστική και μεταθετική, το δε 1 είναι ουδέτερο στοιχείο.

(iii) Η "$*_3$" είναι προσεταιριστική και μεταθετική, αλλά δεν υφίσταται ουδέτερο στοιχείο ως προς αυτήν.

1-2. Επί τού συνόλου $\mathbb{R}\setminus\{0\}$ ορίζονται οι εσωτερικές πράξεις

$$(x,y) \longmapsto x \star_1 y := |x-y| \ \text{ και } \ (x,y) \longmapsto x \star_2 y := \max\{x,y\}.$$

Να εξετασθεί το κατά πόσον η "$\star_1$"(και αντιστοίχως, η "$\star_2$") είναι (ή δεν είναι) προσεταιριστική ή/και μεταθετική.

1-3. Να αποδειχθεί ότι το ομαδοειδές $(\mathbb{R}, \boxdot)$, όπου

$$(x,y) \longmapsto x \boxdot y := \sqrt[3]{x^3+y^3},$$

είναι αβελιανό μονοειδές.

1-4. Να αποδειχθεί ότι το $\mathbb{Q}\setminus\{0\}$, εφοδιαζόμενο με την πράξη τής συνήθους διαιρέσεως, είναι ένα ομαδοειδές. Εν συνεχεία, να εξετασθεί το κατά πόσον αυτό είναι (ή δεν είναι) (i) προσεταιριστικό και (ii) αβελιανό.

1-5. Θεωρούμε ένα μη κενό σύνολο A εφοδιασμένο με μια εσωτερική πράξη "$\circledcirc$", η οποία ικανοποιεί την ακόλουθη συνθήκη:

$$(a \circledcirc b) \circledcirc (c \circledcirc d) = (a \circledcirc c) \circledcirc (b \circledcirc d), \ \ \forall\, (a,b,c,d) \in A^4.$$

Υποθέτοντας ότι το ομαδοειδές $(A, \circledcirc)$ διαθέτει ουδέτερο στοιχείο, να αποδειχθεί ότι είναι *και* προσεταιριστικό *και* αβελιανό.

1-6. Να εξετασθεί η ύπαρξη εξ αριστερών και εκ δεξιών ουδετέρων στοιχείων τού ομαδοειδούς $(\mathbb{R}, \star)$, όπου

$$x \star y := |x|\, y, \ \ \forall\, (x,y) \in \mathbb{R} \times \mathbb{R}.$$

1-7. Θεωρούμε το σύνολο $\mathbb{R}$ εφοδιασμένο με την εσωτερική πράξη "$\circledast$", όπου

$$x \circledast y := xy + x + y, \ \ \forall\, (x,y) \in \mathbb{R} \times \mathbb{R}.$$

Διαθέτει το ομαδοειδές $(\mathbb{R}, \circledast)$ ουδέτερο στοιχείο; Και αν ναι, τότε ποια $x \in \mathbb{R}$ επιδέχονται συμμετρικά στοιχεία ως προς την "$\circledast$"; Ποιες θα είναι οι απαντήσεις στα ίδια ερωτήματα στην περίπτωση κατά την οποία, αντί τού ομαδοειδούς $(\mathbb{R}, \circledast)$, θεωρήσουμε το $(\mathbb{Z}, \circledast|_{\mathbb{Z}})$;

1-8. Επί τού συνόλου $\mathbb{R}$ ορίζουμε μια εσωτερική πράξη "$\odot$" ως ακολούθως:

$$x \odot y := ax + ay + bxy + c, \ \ \forall\, (x, y) \in \mathbb{R} \times \mathbb{R},$$

όπου $a, b, c \in \mathbb{R}$. Υποθέτοντας ότι το ομαδοειδές $(\mathbb{R}, \odot)$ έχει το $e \in \mathbb{R}$ ως ουδέτερό του στοιχείο και ότι κάθε $x \in \mathbb{R} \setminus \{d\}$ διαθέτει συμμετρικό στοιχείο ως προς την "$\odot$", όπου d είναι ένας πραγματικός αριθμός διάφορος τού e, να προσδιορισθούν τα a, b, c συναρτήσει των d και e.

1-9. Έστω $(\mathbb{R}, *)$ το ομαδοειδές το οριζόμενο μέσω τής εσωτερικής πράξεως:

$$x * y := x + y + x^2 y^2, \ \ \forall\, (x, y) \in \mathbb{R} \times \mathbb{R}.$$

Να αποδειχθεί ότι το $(\mathbb{R}, *)$ είναι ένα αβελιανό, μη προσεταιριστικό ομαδοειδές με ουδέτερο στοιχείο, καθώς και το ότι υπάρχουν στοιχεία τού $\mathbb{R}$ τα οποία διαθέτουν δύο συμμετρικά στοιχεία, ένα συμμετρικό στοιχείο ή και κανένα συμμετρικό στοιχείο ως προς την πράξη "$*$".

1-10. Για ποιες τιμές τού $n \in \mathbb{N}$ είναι το ομαδοειδές $(\mathbb{Q}, \boxdot_n)$, όπου

$$(r, s) \longmapsto r \boxdot_n s := \frac{r + s}{n},$$

ημιομάδα;

ΚΕΦΑΛΑΙΟ 2

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.

2.1 ΘΕΜΕΛΙΩΔΕΙΣ ΟΡΙΣΜΟΙ ΚΑΙ ΙΔΙΟΤΗΤΕΣ

2.1.1 Ορισμός. Ένα μονοειδές $(G, \circledcirc)$ (με το G ως υποκείμενο σύνολό του) καλείται **ομάδα**[1] όταν για κάθε στοιχείο τού G υπάρχει το συμμετρικό του ως προς την $\circledcirc$ (πρβλ. πρόταση 1.2.8). 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[2] $|G| = \infty$). Μια ομάδα G λέγεται **μεταθετική** ή **αβελιανή** (ή **ομάδα τού Abel**[3]) όταν η πράξη, με την οποία είναι εφοδιασμένη, είναι μεταθετική.

2.1.2 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. 1.3.5 (viii)) αποτελεί (σύμφωνα με την πρόταση B.4.41) μια αβελιανή ομάδα με ουδέτερό της στοιχείο το $[0]_m$ και αντίθετο

[1] Σε πολλές περιπτώσεις όπου δεν υφίσταται κίνδυνος συγχύσεως (για το ποια πράξη υπονοείται) συμβολίζουμε τις ομάδες μόνον με κεφαλαία (λατινικά) γράμματα.

[2] Εν κανείς χρησιμοποιήσει τον συνήθη τρόπο συγκρίσεως πληθικών αριθμών (στο πλαίσιο τής Θεωρίας Συνόλων), η συνθήκη $|G| = \infty$ ισοδυναμεί με την $|G| \geq \aleph_0 := \mathrm{card}(\mathbb{N})$, όπου $\aleph_0$ είναι το «άλεφ μηδέν».

[3] Προς τιμήν τού Νορβηγού μαθηματικού Niels Henrik Abel (1802-1829).

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. 1.3.5 (viii)), με ουδέτερό του στοιχείο το $[1]_m$, δεν είναι ομάδα όταν $m\geq 2$, 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. 1.2.15 και 1.3.5 (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 1.3.6 αποτελεί μια ομάδα, καθότι κάθε

$$(a_{jk})_{1\leq j\leq m,1\leq k\leq n}\in\mathrm{Mat}_{m\times n}(A)$$

έχει τον πίνακα $(-a_{jk})_{1\leq j\leq m,1\leq k\leq n}$ ως συμμετρικό του στοιχείο ως προς την "+".

2.1.3 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 για την** $(G,\circledcirc)$). Εάν $G=\{g_1,...,g_k\}$, $k\in\mathbb{N}$, 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 $g_i\circledcirc g_j$, $1\leq i,j\leq k$. Κάθε στοιχείο τής ομάδας εμφανίζεται *μόνον μία φορά* σε κάθε γραμμή και σε κάθε στήλη.

2.1.4 Σημείωση. Η ιεράρχηση των (NBG-) κλάσεων των δομών που έχουμε συναντήσει μέχρι στιγμής έχει ως εξής:

$$\{\text{ομάδες}\}\subsetneqq\{\text{μονοειδή}\}\subsetneqq\{\text{ημιομάδες}\}\subsetneqq\{\text{ομαδοειδή}\}.$$

Από τα προηγηθέντα παραδείγματα 1.3.5 και 2.4.2 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 2.1.6.

2.1.5 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 "$\cdot$".

2.1.6 Πρόταση. *Έστω $(M,\cdot)$ ένα μονοειδές. Τότε το ζεύγος $(M^\times,\cdot)$ αποτελεί μια ομάδα.*

ΑΠΟΔΕΙΞΗ. 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. 1.2.2). Επιπροσθέτως, εάν το x είναι τυχόν στοιχείο τού $M^\times$ και το y συμμετρικό στοιχείο του, τότε το y (λόγω τής προτάσεως 1.2.13) 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. □

2.1.7 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 $(\mathbb{Q}\smallsetminus\{0\},\cdot)$, $(\mathbb{R}\smallsetminus\{0\},\cdot)$ και $(\mathbb{C}\smallsetminus\{0\},\cdot)$, αντιστοίχως.

(ii) Μέσω τού αβελιανού μονοειδούς $(\mathbb{Z},\cdot)$ (όπου "$\cdot$" ο συνήθης πολλαπλασιασμός) δημιουργείται η πολλαπλασιαστική ομάδα με υποκείμενο σύνολό της το $\mathbb{Z}^\times = \{1,-1\}$.

(iii) Μέσω τού αβελιανού μονοειδούς $(\mathbb{Z}_m,\cdot)$, $m \in \mathbb{N}$, δημιουργείται η πολλαπλασιαστική ομάδα που έχει ως υποκείμενο σύνολό της το[4]

$$\boxed{\mathbb{Z}_m^\times = \{[k]_m \in \mathbb{Z}_m \mid k \in \mathbb{N},\ \ k \le m,\ \ \text{μκδ}\,(k,m) = 1\,\}}$$

και τάξη $\phi\,(m)$, όπου $\phi : \mathbb{N} \longrightarrow \mathbb{N}$ η *συνάρτηση φι τού Euler*

$$m \longmapsto \phi\,(m) := \text{card}\{\,k \in \mathbb{N} \mid\ k \le m \text{ και } \text{μκδ}\,(k,m) = 1\}. \tag{2.1}$$

(Πρβλ. Β.4.15 και Β.4.43.) Η $(\mathbb{Z}_m^\times,\cdot)$ καλείται **ομάδα των αντιστρέψιμων κλάσεων υπολοίπων κατά το μόδιο** m. (Σημειωτέον ότι για κάθε πρώτο αριθμό p έχουμε $\mathbb{Z}_p^\times = \mathbb{Z}_p\smallsetminus\{[0]_p\}$.)

[4] Επειδή $[0]_m = [m]_m$, ισχύει και η ισότητα $\mathbb{Z}_m^\times = \{\,[k]_m \in \mathbb{Z}_m \mid k \in \mathbb{Z},\ \ 0 \le k \le m-1,\ \ \text{μκδ}\,(k,m) = 1\,\}$. (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).)

(iv) Έστω $(R,+,\cdot)$ ένας μεταθετικός μη τετριμμένος δακτύλιος με μοναδιαίο (πολλαπλασιαστικό) στοιχείο 1_R και έστω $n\in\mathbb{N}$. Ας συμβολίσουμε ως 0_R το ουδέτερο στοιχείο τής ομάδας $(R,+)$. Το σύνολο $\mathrm{Mat}_{n\times n}(R)$ των $(n\times n)$-πινάκων καθίσταται δακτύλιος μέσω τής των (συνήθων) πράξεων τής *προσθέσεως* και τού *πολλαπλασιασμού πινάκων*:

$$\mathbf{A}+\mathbf{B}:=(a_{jk}+b_{jk})_{1\le j,k\le n}\,,\ \mathbf{AB}:=(a_{j\,1}b_{1\,k}+a_{j\,2}b_{2\,k}+\cdots+a_{j\,n}b_{n\,k})_{1\le j,k\le n}\,,$$

για οιουσδήποτε $\mathbf{A}=(a_{jk})_{1\le j,k\le n}$, $\mathbf{B}=(b_{jk})_{1\le j,k\le n}\in\mathrm{Mat}_{n\times n}(R)$, 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 $(\mathrm{Mat}_{n\times n}(R),\cdot)$ ορίζεται η **γενική γραμμική ομάδα**

$$\boxed{\mathrm{GL}_n(R):=(\mathrm{Mat}_{n\times n}(R))^\times=\{\mathbf{A}\in\mathrm{Mat}_{n\times n}(R)\mid\det(\mathbf{A})\in R^\times\}\,,}$$

(**βαθμού** n **υπεράνω τού** R), όπου $\det(\mathbf{A})$ δηλοί την *ορίζουσα* τού $\mathbf{A}$. (Βλ. θεώρημα D.2.18).

2.1.8 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).

2.1.9 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Τότε ισχύουν τα ακόλουθα*:
(i) *Για κάθε $a,b,g\in G$ έχουμε*

$$\left.\begin{array}{rcl} ag=bg & \Longrightarrow & a=b\\ ga=gb & \Longrightarrow & a=b\end{array}\right\}\ \text{(Νόμοι διαγραφής)}$$

(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 $x=a^{-1}b$ και $y=ba^{-1}$, αντιστοίχως, ως μοναδικές τους λύσεις.*

ΑΠΟΔΕΙΞΗ. (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 1.2.8).

(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 1.2.19 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 $k \geq 3$ 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. □

2.1.10 Ορισμός. («Δυνάμεις» στοιχείων) Έστω $(G, \cdot)$ μια ομάδα. Για κάθε $n \in \mathbb{Z}$ εισάγουμε τη βραχυγραφία

$$\boxed{g^n := \begin{cases} \underbrace{g\,g\,\cdots\,g}_{n\ \text{φορές}}, & \text{όταν} \quad n > 0, \\ \left(g^{-n}\right)^{-1}, & \text{όταν} \quad n < 0, \\ e_G\,, & \text{όταν} \quad n = 0, \end{cases}}$$

εν είδει[5] «δυνάμεως».

2.1.11 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.)

ΑΠΟΔΕΙΞΗ. (i) Κατ' αρχάς υποθέτουμε ότι αμφότεροι οι m, n είναι θετικοί. Διατηρώντας τόν n παγιωμένο, θα εφαρμόσουμε κλασική μαθηματική επαγωγή ως προς

[5] 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».

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 2.1.9 (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 $\{k \in \mathbb{Z} \,|\, k \leq -1\}$, εκκινώντας από τον $m = -1$. Όταν $m = -1$, ο ισχυρισμός είναι προφανώς αληθής λόγω τού 2.1.9 (ii). Έχοντας τις

$$g^{-m} = \left(g^{-1}\right)^m = (g^m)^{-1}$$

ως επαγωγική μας υπόθεση, μέσω τού (i) και των 2.1.9 (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. □

2.1.12 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

$$(xy)^n = x^n y^n,\ \forall n \in \mathbb{Z}, \ \text{ και } \ x^m y^n = y^n x^m,\ \forall (m,n) \in \mathbb{Z} \times \mathbb{Z},$$

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*.

2.1.13 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. 1.2.2) 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[6] $H \sqsubseteq G$.

2.1.14 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): $H \sqsubset G$.

2.1.15 Παρατήρηση. (i) Κάθε υποομάδα H μιας *πεπερασμένης* ομάδας $(G, \cdot)$ είναι πεπερασμένη, διότι $|H| \leq |G| < \infty$. (Φυσικά, μια *άπειρη* ομάδα διαθέτει πάντοτε[7] 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[8] 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 τριάδα

[6] Κατ' αντιστοιχίαν, ο συμβολισμός "$H \not\sqsubseteq G$" θα σημαίνει ότι το υποσύνολο H τού G *δεν είναι υποομάδα* τής ομάδας $(G, \cdot)$ (ως προς την $\cdot|_{H\times H}$).

[7] Επειδή το μονοσύνολο $\{e_G\}$ αποτελεί πάντοτε υποομάδα οιασδήποτε ομάδας $(G, \cdot)$ (πρβλ. 2.1.21 (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.

[8] Εάν η $(G, \cdot)$ είναι μη αβελιανή, τότε η $\{e_G\}$ είναι προφανώς *αβελιανή* υποομάδα της.

$(x,y,z) \in H \times H \times H$ 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 $(G,\cdot)$.

2.1.16 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) $ab^{-1} \in H, \forall (a,b) \in H \times H$.

ΑΠΟΔΕΙΞΗ. (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

$$e_H h = h e_H = h, \quad \forall h \in H.$$

Επειδή κάθε $h \in H$ ανήκει και στην G, έχουμε $he_G = h$, οπότε το μονοσήμαντο τής επιλύσεως των προκειμένων εξισώσεων (βλ. 2.1.9 (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 $H \sqsubseteq G$. □

2.1.17 Παρατήρηση. Οι συνθήκες (ii) (a) και (iii) (a) συμπεριελήφθησαν στην πρόταση 2.1.16 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 $e_G \in H$.

2.1.18 Πόρισμα. *Έστω $(G,\cdot)$ μια ομάδα. Τότε για κάθε $H \sqsubseteq G$ έχουμε $e_H = e_G$.*

2.1.19 Πόρισμα. *Έστω $(G,\cdot)$ μια ομάδα και έστω $\varnothing \neq H \subseteq G$. Εάν το H είναι πεπερασμένο σύνολο*[9]*, τότε τα* (i) *και* (ii) *είναι ισοδύναμα*:

(i) $H \sqsubseteq G$.

(ii) $ab \in H, \forall (a,b) \in H \times H$.

ΑΠΟΔΕΙΞΗ. Η συνεπαγωγή (i)⇒(ii) είναι προφανής (λόγω τής συνεπαγωγής (i)⇒(ii) (b) στην πρόταση 2.1.16). Επειδή $H \neq \varnothing$, για να ισχύει η αντίστροφη συνεπαγωγή (ii)⇒(i) αρκεί να ελεγχθεί ότι $h^{-1} \in H, \forall h \in H$ (βλ. 2.1.17). 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,

$$\left.\begin{array}{r} \{h^n \mid n \in \mathbb{N}\} \subseteq H \\ \text{card}(H) < \infty \ \text{(εξ υποθέσεως)} \end{array}\right\} \Rightarrow \exists i,j \in \mathbb{N},\ i > j : h^i = h^j.$$

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 $h^{-1} \in H$. □

2.1.20 Πόρισμα. *Έστω $(G,\cdot)$ μια ομάδα. Εάν $H \sqsubseteq G$ και $\varnothing \neq K \subseteq H$, τότε*

$$K \sqsubseteq G \Longleftrightarrow K \sqsubseteq H.$$

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 2.1.16 και τής παρατηρήσεως 2.1.17). 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). □

2.1.21 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 2.1.16).

(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 2.1.16, 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

[9] 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 $-n \notin H,\ \forall n \in H$).

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**

$$\boxed{\mathbb{S}^1 := \{z \in \mathbb{C} \mid |z| = 1\},}$$

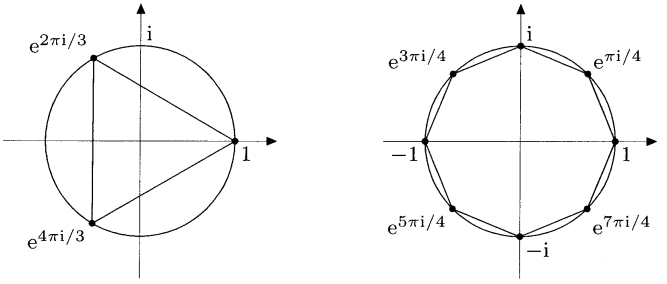
εφοδιασμένος με τον συνήθη πολλαπλασιασμό μιγαδικών αριθμών, αποτελεί υποομάδα τής $(\mathbb{C}\setminus\{0\}, \cdot)$. Επίσης, το σύνολο των n-**οστών ριζών τής μονάδας**[10]

$$\boxed{\mathcal{E}_n := \{z \in \mathbb{C} \mid z^n = 1\}, \;\; n \in \mathbb{N},}$$

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[11] $\mathcal{E}_n = \left\{\zeta_n^k \mid k \in \{0, 1, ..., n-1\}\right\}$. Όταν $n \geq 3$, τα στοιχεία τής ομάδας $\mathcal{E}_n$ (ιδωμένα ως σημεία τού μιγαδικού επιπέδου $\mathbb{C}$) αποτελούν τις κορυφές ενός κανονικού n-γώνου[12] 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:



(vii) Έστω $(R, +, \cdot)$ ένας μη τετριμμένος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο 1_R και έστω $n \in \mathbb{N}$. Το σύνολο

$$\boxed{\mathbf{SL}_n(R) := \{\mathbf{A} \in \mathbf{GL}_n(R) \mid \det(\mathbf{A}) = 1_R\},}$$

[10] Το σύμβολο "$\mathcal{E}$" προέρχεται από το πρώτο γράμμα τής (γερμανικής) λέξεως Einheitswurzel (= ρίζα τής μονάδας).

[11] Εάν $z = re^{i\theta}$, $r \in \mathbb{R}_{>0}$, $0 \leq \theta < 2\pi$, είναι ένα στοιχείο τής $\mathcal{E}_n$, τότε

$$z^n = 1 \Leftrightarrow r^n = e^{in\theta} = 1 \Leftrightarrow r = 1, \; \theta \in \left\{ \left. \frac{2\pi k i}{n} \right| \; k \in \{0, 1, ..., n-1\} \right\}.$$

[12] Έστω $n \in \mathbb{N}$, $n \geq 3$. Ένα κυρτό πολύγωνο καλείται **κανονικό** n-**γωνο** όταν διαθέτει n ισομήκεις πλευρές (και, κατ' επέκταση, n ίσες γωνίες).

εφοδιασμένο με τον πολλαπλασιασμό $(n \times n)$-πινάκων, αποτελεί μια υποομάδα τής $(\mathrm{GL}_n(R), \cdot)$ που είναι, μάλιστα, *γνήσια* υποομάδα στην περίπτωση όπου $1_R \neq -1_R$ (βλ. 2.1.7 (iv) και πρόταση D.2.22). 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

$$\begin{array}{c} \mathrm{GL}_n(\mathbb{R}) = \{\mathbf{A} \in \mathrm{Mat}_{n\times n}(\mathbb{R}) \mid \det(\mathbf{A}) \neq 0\} \quad \sqsupset \mathrm{SL}_n(\mathbb{R}) \\ \bigsqcup \\ \mathrm{O}_n(\mathbb{R}) := \left\{\mathbf{A} \in \mathrm{GL}_n(\mathbb{R}) \;\middle|\; \mathbf{A}^{\intercal} = \mathbf{A}^{-1}\right\} \\ \bigsqcup \\ \mathrm{SO}_n(\mathbb{R}) := \mathrm{O}_n(\mathbb{R}) \cap \mathrm{SL}_n(\mathbb{R}), \end{array}$$

όπου $\mathbf{A}^{\intercal}$ ο ανάστροφος[13] 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

$$\begin{array}{c} \mathrm{GL}_n(\mathbb{C}) = \{\mathbf{A} \in \mathrm{Mat}_{n\times n}(\mathbb{C}) \mid \det(\mathbf{A}) \neq 0\} \quad \sqsupset \mathrm{SL}_n(\mathbb{C}) \\ \bigsqcup \\ \mathrm{U}_n(\mathbb{C}) := \left\{\mathbf{A} \in \mathrm{GL}_n(\mathbb{C}) \;\middle|\; \overline{\mathbf{A}}^{\intercal} = \mathbf{A}^{-1}\right\} \\ \bigsqcup \\ \mathrm{SU}_n(\mathbb{C}) := \mathrm{U}_n(\mathbb{C}) \cap \mathrm{SL}_n(\mathbb{C}), \end{array}$$

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**.

2.1.22 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 $H_1 \sqsubseteq H_3$.*

ΑΠΟΔΕΙΞΗ. Το (i) είναι προφανές. Τα (ii)-(iii) έπονται άμεσα από τις αντίστοιχες ιδιότητες τού συνολοθεωρητικού εγκλεισμού " $\subseteq$ ", την πρόταση 2.1.16 και το πόρισμα 2.1.20. □

[13] Ο **ανάστροφος** ενός τετραγωνικού πίνακα είναι αυτός που προκύπτει όταν καθιστούμε τις γραμμές του στήλες (και τις στήλες του γραμμές).

2.1.23 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.

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. 2.1.16 (iii)). □

2.1.24 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 $2\mathbb{Z} \cup 3\mathbb{Z} \not\sqsubseteq \mathbb{Z}$.

2.1.25 Πρόταση. *Εάν οι* H, K *είναι δυο υποομάδες μιας ομάδας* $(G,\cdot)$, *τότε ισχύει η αμφίπλευρη συνεπαγωγή* :

$$H \cup K \sqsubseteq G \Leftrightarrow \textit{είτε}\ \ H \sqsubseteq K\ \ \textit{είτε}\ \ K \sqsubseteq H.$$

ΑΠΟΔΕΙΞΗ. "⇒" Ας υποθέσουμε ότι $H \not\sqsubseteq K$ και $K \not\sqsubseteq H$. Τότε

$$\exists x \in H \smallsetminus K \text{ και } \exists y \in K \smallsetminus H.$$

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. Α. 2.4) είναι υποβοηθητικά στη μελέτη ενός πεπερασμένου υποσυνόλου υποομάδων δοθείσας ομάδας (και, ειδικότερα, τού συνόλου *όλων* των υποομάδων δοθείσας *πεπερασμένης* ομάδας).

2.1.26 Πρόταση. *Έστω* $(G,\cdot)$ *μια ομάδα. Τότε το ζεύγος* $(\mathbf{Subg}(G),\sqsubseteq)$, *όπου*[14]

$$\boxed{\mathbf{Subg}(G) := \{H \in \mathfrak{P}(G) \mid H \sqsubseteq G\},}$$

και, γενικότερα, το ζεύγος $(\mathfrak{X},\sqsubseteq)$, *όπου* $\varnothing \neq \mathfrak{X} \subseteq \mathbf{Subg}(G)$, *αποτελεί μερικώς διατεταγμένο σύνολο* (βλ. A.2.1).

ΑΠΟΔΕΙΞΗ. Αυτή έπεται άμεσα από την πρόταση 2.1.22. □

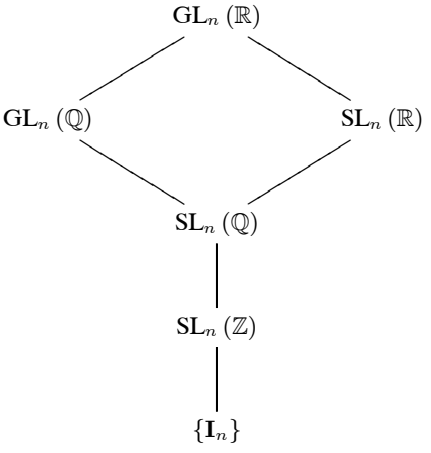
2.1.27 Παραδείγματα. Τα διαγράμματα τού Hasse για τα μερικώς διατεταγμένα σύνολα $(\mathbf{Subg}(\mathbb{Z}_2),\sqsubseteq)$ και $(\mathbf{Subg}(\mathbb{Z}_4),\sqsubseteq)$ των ομάδων $(\mathbb{Z}_2,+)$ και $(\mathbb{Z}_4,+)$ είναι τα εξής:

(Ένας γενικότερος χαρακτηρισμός των $(\mathbf{Subg}(\mathbb{Z}_m),\sqsubseteq)$ για *οιουσδήποτε* $m \in \mathbb{N}$ θα δοθεί αργότερα στο εδάφιο 2.4.26 (ii).)

2.1.28 Παράδειγμα. Έστω $n \in \mathbb{N}$, $n \geq 2$. 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



[14] 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 2.4.10).

2.1.29 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. A.2.2 (i), A.2.22, A.2.23 (i) και A.2.25), διότι (όπως έχουμε ήδη προαναφέρει στο εδάφιο 2.1.24) η ένωση δυο υποομάδων τής $(G,\cdot)$ δεν είναι κατ' ανάγκην υποομάδα της. Για να καταστήσουμε το σύνολο $\mathbf{Subg}(G)$ σύνδεσμο (βλ. A.2.22) οφείλουμε να αντικαταστήσουμε τη σχέση εγκλεισμού " $\subseteq$ " με τη σχέση " $\sqsubseteq$ ".

2.1.30 Πρόταση. *Το μερικώς διατεταγμένο σύνολο* $(\mathbf{Subg}(G),\sqsubseteq)$ *είναι σύνδεσμος για κάθε ομάδα* $(G,\cdot)$ (βλ. A.2.22). *Μάλιστα, για οιεσδήποτε* $H,K\in\mathbf{Subg}(G)$ *έχουμε*

$$H\wedge K=H\cap K,\quad H\vee K=\bigcap\{L\in\mathbf{Subg}(G)\mid H\cup K\subseteq L\}.$$

ΑΠΟΔΕΙΞΗ. Εάν $H,K\in\mathbf{Subg}(G)$, τότε

$$\left.\begin{array}{r}2.1.23\Rightarrow H\cap K\in\mathbf{Subg}(G)\\ H\cap K\subseteq H\ \text{ και }\ H\cap K\subseteq K\end{array}\right\}\underset{2.1.20}{\Longrightarrow}H\cap K\sqsubseteq H\ \text{ και }\ H\cap K\sqsubseteq K.$$

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

$$\left.\begin{array}{r}N\in\mathbf{Subg}(G)\\ N\subseteq H\ \text{ και }\ N\subseteq K\Rightarrow N\cap N=N\subseteq H\cap K\end{array}\right\}\underset{2.1.20}{\Longrightarrow}N\sqsubseteq H\cap K.$$

Κατά συνέπειαν, η τομή $H\cap K$ είναι το (κατ' ανάγκην μοναδικό, λόγω τής προτάσεως A.2.16) *μέγιστο κάτω φράγμα* τού $\{K,H\}$ ως προς την " $\sqsubseteq$ ". Επιπροσθέτως, από την πρόταση 2.1.23 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 2.1.20)

$$H\sqsubseteq\bigcap\{L\in\mathbf{Subg}(G)\mid H\cup K\subseteq L\}\ \text{ και }K\sqsubseteq\bigcap\{L\in\mathbf{Subg}(G)\mid H\cup K\subseteq L\}.$$

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

$$H\subseteq\Xi\ \text{ και }\ K\subseteq\Xi\Rightarrow H\cup K\subseteq\Xi\Rightarrow\bigcap\{L\in\mathbf{Subg}(G)\mid H\cup K\subseteq L\}\subseteq\Xi,$$

οπότε

$$\left.\begin{array}{r}\Xi\in\mathbf{Subg}(G)\\ \bigcap\{L\in\mathbf{Subg}(G)\mid H\cup K\subseteq L\}\subseteq\Xi\end{array}\right\}\underset{2.1.20}{\Longrightarrow}\bigcap\{L\in\mathbf{Subg}(G)\mid H\cup K\subseteq L\}\sqsubseteq\Xi.$$

Κατά συνέπειαν, η τομή $\bigcap\{L\in\mathbf{Subg}(G)\mid H\cup K\subseteq L\}$ είναι το (κατ' ανάγκην μοναδικό, λόγω τής προτάσεως A.2.16) *ελάχιστο άνω φράγμα* τού $\{K,H\}$ ως προς την " $\sqsubseteq$ ". □

2.1.31 Σημείωση. Με ανάλογο τρόπο αποδεικνύεται ότι ο $(\mathbf{Subg}(G), \sqsubseteq)$ είναι *πλήρης σύνδεσμος*. (Βλ. εδάφιο A.2.24 (iii).) Επί παραδείγματι, εάν $(H_j)_{\,j\in J}$ είναι τυχούσα οικογένεια υποομάδων τής G, τότε

$$\bigwedge_{j\in J} H_j = \bigcap_{j\in J} H_j \;\text{ και }\; \bigvee_{j\in J} H_j = \bigcap \left\{ L \in \mathbf{Subg}(G) \;\middle|\; \bigcup_{j\in J} H_j \subseteq L \right\}.$$

2.1.32 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 υποσύνδεσμος τού $(\mathbf{Subg}(G), \sqsubseteq)$.

ΑΠΟΔΕΙΞΗ. Για οιεσδήποτε $H, K \in \mathbf{Subg}(G;L)$, έχουμε $H \wedge K \in \mathbf{Subg}(G;L)$ και $H \vee K \in \mathbf{Subg}(G;L)$. □

2.1.33 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.

2.1.34 Ορισμός. Έστω $(G,\cdot)$ μια ομάδα με[15] $|G| \geq 2$.

(i) Κάθε υποομάδα της ανήκουσα στο

$$\mathbf{Min\text{-}Subg}(G) := \left\{ H \;\middle|\; \begin{array}{c} H \text{ ελαχιστικό στοιχείο} \\ \text{τού } \mathbf{Subg}(G)\smallsetminus\{\{e_G\}\} \\ \text{ως προς την " } \sqsubseteq|_{\mathbf{Subg}(G)\smallsetminus\{\{e_G\}\}} \text{ "} \end{array} \right\}$$

καλείται **ελαχιστική υποομάδα τής** G, ενώ κάθε υποομάδα της ανήκουσα στο

$$\mathbf{Max\text{-}Subg}(G) := \left\{ H \;\middle|\; \begin{array}{c} H \text{ μεγιστικό στοιχείο} \\ \text{τού } \mathbf{Subg}(G)\smallsetminus\{G\} \\ \text{ως προς την " } \sqsubseteq|_{\mathbf{Subg}(G)\smallsetminus\{G\}} \text{ "} \end{array} \right\}$$

καλείται **μεγιστική υποομάδα τής** G. (Πρβλ. A.2.6 και A.2.10.)

(ii) Έστω ΙΔ μια (ειδική) ιδιότητα[16] που αφορά σε υποομάδες (ή που χαρακτηρίζει ρητώς κάποιες υποομάδες) τής G. Κάθε υποομάδα τής G ανήκουσα στο

$$\mathbf{Min\text{-}Subg}(G) \cap \{H \in \mathbf{Subg}(G) \mid \text{η } H \text{ έχει την ιδιότητα ΙΔ}\} \qquad (2.2)$$

[15] Κάθε ομάδα με αυτήν την ιδιότητα καλείται **μη τετριμμένη ομάδα** (Βλ. εδάφιο 2.4.24.)

[16] Παραδείγματα τέτοιων ιδιοτήτων: Το να είναι μια υποομάδα *πεπερασμένη*, το να είναι *αβελιανή* (βλ. 2.1.1), το να είναι *πεπερασμένως παραγόμενη* (βλ. 2.2.8), το να είναι *κυκλική* (βλ. 2.2.15), το να είναι *περιοδική* (βλ. 2.3.1), το να είναι *ορθόθετη* (βλ. 4.2.2) κ.ά.

καλείται **ελαχιστική υποομάδα τής** G **με την ιδιότητα** ΙΔ και κάθε υποομάδα τής G ανήκουσα στο

$$\mathbf{Max\text{-}Subg}(G) \cap \{H \in \mathbf{Subg}(G) \mid \text{η } H \text{ έχει την ιδιότητα ΙΔ}\} \tag{2.3}$$

καλείται **μεγιστική υποομάδα τής** G **με την ιδιότητα** ΙΔ. Μια $H \in \mathbf{Subg}(G)$ ανήκει στο (2.2) εάν και μόνον εάν ικανοποιείται η εξής συνθήκη: *Για οιαδήποτε* $K \in \mathbf{Subg}(G)$, *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 $H \in \mathbf{Subg}(G)$ ανήκει στο (2.3) εάν και μόνον εάν ικανοποιείται η εξής συνθήκη: *Για οιαδήποτε* $L \in \mathbf{Subg}(G)$, *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 (2.2) (και αντιστοίχως, το σύνολο (2.3)) 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.

2.1.35 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 $\{[0]_{12}, [2]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12}\}$ και $\{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}$). Από την άλλη μεριά, για την $(\mathbb{Z}_4, +)$ έχουμε

$$\mathbf{Min\text{-}Subg}(\mathbb{Z}_4) = \{[0]_4, [2]_4\} = \mathbf{Max\text{-}Subg}(\mathbb{Z}_4)$$

και για την $(\mathbb{Z}_2, +)$, $\mathbf{Min\text{-}Subg}(\mathbb{Z}_2) = \mathbb{Z}_2$ και $\mathbf{Max\text{-}Subg}(\mathbb{Z}_2) = \{[0]_2\}$ (!) (Πρβλ. 2.4.27 (ii) και 2.1.27.) Τα εν λόγω σύνολα υποομάδων για την $(\mathbb{Z}_m, +)$, όπου m *οιοσδήποτε* φυσικός αριθμός ≥ 2, περιγράφονται στο εδάφιο 2.4.26 (ii).

(ii) Είναι προφανές ότι, για πεπερασμένες ομάδες G, αμφότερα τα $\mathbf{Min\text{-}Subg}(G)$ και $\mathbf{Max\text{-}Subg}(G)$ είναι σύνολα μη κενά. Ωστόσο, υπάρχουν άπειρες ομάδες, όπως, π.χ., η $(\mathbb{Z}, +)$ ή η $(\mathbb{Q}, +)$ (ή οποιαδήποτε άλλη άπειρη ομάδα που «στερείται στρέψεως», βλ. 2.3.1 (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. 2.3.6 (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 $\text{card}(G) \geq 2$. Εάν για μια $H \in \mathbf{Subg}(G)$ ως ΙΔ λάβουμε, π.χ., «το να είναι η H αβελιανή», τότε κάθε υποομάδα τής G ανήκουσα στο (2.3), ήτοι κάθε υποομάδα τής G «που δεν περιέχεται γνησίως σε κάποια αβελιανή υποομάδα τής G» ονομάζεται (εν συντομία) *μεγιστική αβελιανή υποομάδα τής* G.

2.1.36 Σημείωση. Ενίοτε, επιβάλλεται η (μερική, αλλά σαφώς υποδηλούμενη) «χαλάρωση» των αξιώσεων τού ορισμού 2.1.34. 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* $\mathbf{Subg}(G)$ ως προς την " $\sqsubseteq$ " το οποίο απαρτίζεται από εκείνες τις υποομάδες τής G που έχουν την ιδιότητα ΙΔ. Επί παραδείγματι, στο αμέσως επόμενο εδάφιο 2.2.1 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 $\mathbf{Subg}(G)$ 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[17].

2.2 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.

2.2.1 Ορισμός. Για *τυχόν υποσύνολο* X τού υποκειμένου συνόλου G μιας ομάδας $(G, \cdot)$, χαρακτηρίζουμε την τομή[18]

$$\boxed{\langle X\rangle := \bigcap \{H \in \mathbf{Subg}(G) \mid X \subseteq H\},} \tag{2.4}$$

η οποία είναι η ελάχιστη υποομάδα τής $(G, \cdot)$ που περιέχει το X, ως **την υποομάδα τής** $(G, \cdot)$ **την παραγόμενη από το** X.

2.2.2 Συμβολισμός. (i) Εάν οι H και K είναι δυο υποομάδες μιας ομάδας $(G, \cdot)$, θα συμβολίζουμε εφεξής ως

$$\boxed{\langle H, K\rangle := \langle H \cup K\rangle = \bigcap \{L \in \mathbf{Subg}(G) \mid H \cup K \subseteq L\}\ (= H \vee K),}$$

την υποομάδα της την παραγόμενη από το σύνολο $X = H \cup K$ (η οποία, σύμφωνα με την πρόταση 2.1.30, 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

[17] Επί παραδείγματι, ο «ορθοθέτης» $\mathrm{N}_G(X)$ ενός $\varnothing \neq X \subseteq G$ είναι η *μέγιστη υποομάδα τής G εντός τής οποίας το X είναι ορθόθετο* (βλ. 5.2.7 (i)), η «μεταθέτρια υποομάδα» G' τής G *είναι η ελάχιστη ορθόθετη υποομάδα τής G, ούτως ώστε η G/G' να είναι αβελιανή* (βλ. 5.5.12), κ.λπ.

[18] Εάν το X είναι *πεπερασμένο*, ας πούμε $X = \{x_1, ..., x_k\}$, τότε (για λόγους οικονομίας) γράφουμε $\langle x_1, ..., x_k\rangle$ αντί τού $\langle\{x_1, ..., x_k\}\rangle$.

$(G,\cdot)$, θα συμβολίζουμε ως

$$\boxed{\langle\{\,H_j|\,j\in J\}\rangle := \left\langle \bigcup_{j\in J} H_j \right\rangle}$$

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. 2.1.31.)

2.2.3 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Εάν*[19] *$\varnothing \neq X \subseteq G$, τότε η υποομάδα* (2.4)*, για την οποία λέμε ότι έχει το X ως **το σύνολο ή το σύστημα γεννητόρων** της* (*ή ως **το παράγον υποσύνολό** της*)*, ισούται με*

$$\langle X\rangle = \left\{x_1^{\varepsilon_1}\,\cdots\,x_k^{\varepsilon_k}\;\middle|\;(x_1,..,x_k)\in X^k \text{ και } \varepsilon_j\in\mathbb{Z},\ \forall j\in\{1,..,k\}, k\in\mathbb{N}\right\}. \quad (2.5)$$

ΑΠΟΔΕΙΞΗ. Το σύνολο

$$H := \left\{x_1^{\varepsilon_1}\,\cdots\,x_k^{\varepsilon_k}\;\middle|\;(x_1,..,x_k)\in X^k \text{ και } \varepsilon_j\in\mathbb{Z},\ \forall j\in\{1,..,k\}, k\in\mathbb{N}\right\}$$

είναι μια υποομάδα τής G. Πράγματι· το H περιέχει (προφανώς) το ουδέτερο στοιχείο τής G και για κάθε ζεύγος $\left(x_1^{\varepsilon_1}\,x_2^{\varepsilon_2}\,\cdots\,x_k^{\varepsilon_k}, y_1^{\varrho_1}\,y_2^{\varrho_2}\,\cdots\,y_\nu^{\varrho_\nu}\right)\in H\times H$ έχουμε

$$\left(x_1^{\varepsilon_1}\,x_2^{\varepsilon_2}\,\cdots\,x_k^{\varepsilon_k}\right)\left(y_1^{\varrho_1}\,y_2^{\varrho_2}\,\cdots\,y_\nu^{\varrho_\nu}\right)^{-1} = x_1^{\varepsilon_1}\,x_2^{\varepsilon_2}\,\cdots\,x_k^{\varepsilon_k}\,y_\nu^{-\varrho_\nu}\,\cdots\,y_2^{-\varrho_2}y_1^{-\varrho_1}\in H$$

(πρβλ. 2.1.9 (iii) και 2.1.16 (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 $\langle X\rangle = H$. □

2.2.4 Παρατήρηση. (i) Με ανάλογο τρόπο αποδεικνύεται ότι

$$\langle X\rangle = \left\{x_1^{\varepsilon_1}\,\cdots\,x_k^{\varepsilon_k}\,\middle|(x_1,..,x_k)\in X^k \text{ και } \varepsilon_j\in\{\pm1\}, \forall j\in\{1,..,k\}, k\in\mathbb{N}\right\}. \quad (2.6)$$

Ενίοτε, η παράσταση (2.6) τού $\langle X\rangle$ είναι πιο εύχρηστη από την (2.5). Επίσης, λόγω τής (2.6), αντί τής (2.5) μπορεί, εναλλακτικώς, να χρησιμοποιηθεί (ύστερα από κατάλληλη εφαρμογή τού 2.1.11 (i)) η

$$\langle X\rangle := \left\{x_1^{\varepsilon_1}\,\cdots\,x_k^{\varepsilon_k}\;\middle|\;\begin{array}{c} x_i\in X,\ \varepsilon_i\in\mathbb{Z},\ x_i\neq x_j,\\ \forall(i,j)\in\{1,..,k\}^2 \text{ με } i\neq j,\ k\in\mathbb{N}\end{array}\right\}. \quad (2.7)$$

(ii) Για μια διευκολυντική περιγραφή των στοιχείων δοθείσας ομάδας $(G,\cdot)$ (μέσω τής (2.7)) είναι εμφανώς σημαντική η εύρεση παραγόντων συνόλων *τής ίδιας τής* $(G,\cdot)$ (ήτοι υποσυνόλων $\varnothing\neq X\subseteq G$ με $\langle X\rangle = G$).

[19] Εάν $X=\varnothing$, τότε $\langle\varnothing\rangle = \langle\{e_G\}\rangle = \{e_G\}$ είναι η *τετριμμένη* υποομάδα τής G.

2.2.5 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 $\left\{\,\frac{1}{n}\big|\,n\in\mathbb{N}\right\}$ και $\left\{\,\frac{1}{n!}\big|\,n\in\mathbb{N}\right\}$ αποτελούν παράγοντα σύνολα[20] τής ομάδας $(\mathbb{Q},+)$.

(iii) Το σύνολο $\{-1\}\cup\{p\,|p$ πρώτος αριθμός$\}$ είναι ένα σύνολο γεννητόρων τής πολλαπλασιαστικής ομάδας $(\mathbb{Q}\smallsetminus\{0\},\cdot)$. (Βλ. Β.3.10 και Β.3.3).

(iv) Τόσον το σύνολο των πρώτων αριθμών όσον και το σύνολο[21] $\left\{\,\frac{1}{p}\Big|\,p$ πρώτος αριθμός$\right\}$ παράγουν την πολλαπλασιαστική ομάδα $(\mathbb{Q}_{>0},\cdot)$.

2.2.6 Πόρισμα. *Εάν $(H_j)_{j\in J}$ είναι μια οικογένεια υποομάδων μιας ομάδας $(G,\cdot)$, τότε*

$$\langle\{\,H_j|\,j\in J\}\rangle=\left\{g\in G\;\middle|\;\begin{array}{c}g=h_{j_1}h_{j_2}\cdots h_{j_k},\text{όπου}\\ h_{j_\rho}\in H_{j_\rho},\ \forall\rho\in\{1,...,k\},\ k\in\mathbb{N}\end{array}\right\}.$$

ΑΠΟΔΕΙΞΗ. 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. 2.1.9 (iii) και 2.1.16 (iii)). Επειδή[22] $h\in K$ 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, για την οποία ισχύει $\bigcup_{j\in J}H_j\subseteq B$. Τότε, για κάθε στοιχείο $h_{j_1}h_{j_2}\cdots h_{j_k}$ τής 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 $\langle\{\,H_j|\,j\in J\}\rangle=K$. □

2.2.7 Σημείωση. Επειδή μια ομάδα μπορεί να παράγεται από διάφορα υποσύνολα τού υποκειμένου συνόλου της, γίνεται αντιληπτό ότι η περιγραφή (2.5) καθίσταται αρκούντως βοηθητική μόνον όταν κανείς περιορίζεται στη θεώρηση εκείνων που έχουν τον *μικρότερο δυνατό* πληθικό αριθμό[23]. Ωστόσο, θα πρέπει να

[20] Καθε ρητός αριθμός $\frac{a}{b}\in\mathbb{Q}_{>0}$ ($a\in\mathbb{Z},b\in\mathbb{Z}\smallsetminus\{0\}$) γράφεται ως $\frac{a}{b}=(\text{sign}(b)a)\frac{1}{|b|}=(\text{sign}(b)a(|b|-1)!)\frac{1}{|b|!}$.

[21] Έστω τυχόν στοιχείο $\frac{a}{b}\in\mathbb{Q}_{>0}$ ($a\in\mathbb{Z},b\in\mathbb{Z}\smallsetminus\{0\},ab>0$). Εάν $a=b$, τότε $\frac{a}{b}=1=\left(\frac{1}{p}\right)^0$ για κάθε πρώτο αριθμό p. Εάν $a\neq b$ και $|a|\geq 2$, $|b|\geq 2$, τότε θεωρώντας τις κανονικές παραστάσεις (Β.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 $|b|\geq 2$] είτε [$|a|\geq 2$ και $|b|=1$], χρησιμοποιούμε μόνον μία παράσταση αυτού τού είδους.) Άρα $\mathbb{Q}_{>0}\subseteq\left\langle\left\{\,\frac{1}{p}\Big|\,p$ πρώτος αριθμός$\right\}\right\rangle$. Ο αντίστροφος εγκλεισμός είναι προφανής.

[22] 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).

[23] Ακόμη και για μια *πεπερασμένη* ομάδα G (με $|G|\geq 2$) τα γνωστά ή πιθανά άνω φράγματα τού αριθμού

$$\text{min.gen}(G):=\min\{\,\text{card}(X)|\,X\in\mathfrak{P}(G)\smallsetminus\{\varnothing\}:\langle X\rangle=G\}$$

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.

2.2.8 Ορισμός. Μια ομάδα καλείται **πεπερασμένως παραγόμενη** όταν διαθέτει ένα πεπερασμένο σύνολο γεννητόρων.

2.2.9 Παράδειγμα. (Ομάδα των ακεραίων τού Gauss) Θεωρούμε *το σύνολο των ακεραίων τού Gauss*

$$\boxed{\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\} \subsetneqq \mathbb{C},}$$

όπου i η φανταστική μονάδα. Μέσω τού 2.1.16 (iii) αποδεικνύεται εύκολα ότι το $\mathbb{Z}[i]$ (εφοδιασμένο με τη συνήθη *πρόσθεση* μιγαδικών αριθμών) αποτελεί μια άπειρη 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**.

2.2.10 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 $(\mathrm{GL}_2(\mathbb{Z}), \cdot)$ 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

$$H = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle .$$

εξαρτώνται από την εσώτερη δόμηση τής G και, ως εκ τούτου, από προβλήματα ταξινομήσεων. Επίσης, η απεικόνιση $G \mapsto \mathrm{min.gen}(G)$ δεν επιδεικνύει «καλή συμπεριφορά» ως προς τις υποομάδες των ομάδων αναφοράς. (Επί παραδείγματι, όπως θα δούμε στο (iii) τού πορίσματος 3.2.13, για τη συμμετρική ομάδα $\mathfrak{S}_n$, $n \geq 3$, έχουμε $\mathrm{min.gen}(\mathfrak{S}_n) = 2$. Όμως για την υποομάδα της $H := \langle [1\ 2], [3\ 4], \ldots, [2i-1\ 2i], \ldots \rangle$ ισχύει $\mathrm{min.gen}(H) = \lfloor \frac{n}{2} \rfloor$.) Για διάφορες ιδιότητες τού $\mathrm{min.gen}(G)$ 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.

2.2.11 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. Β.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 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 $\mathbf{i}^{-1} = -\mathbf{i},\ \mathbf{j}^{-1} = -\mathbf{j},\ \mathbf{k}^{-1} = -\mathbf{k}$.)

2.2.12 Σημείωση. (i) Κάθε πεπερασμένη ομάδα είναι προδήλως πεπερασμένως παραγόμενη.

(ii) Το υποκείμενο σύνολο οιασδήποτε πεπερασμένως παραγόμενης ομάδας είναι το πολύ αριθμήσιμο[24]. 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.

2.2.13 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

$$s=n_1\tfrac{a_1}{b_1}+\cdots+n_k\tfrac{a_k}{b_k}=\frac{\sum_{i=1}^{k}n_ia_i\left(\prod_{j\in\{1,\dots,k\}\setminus\{i\}}b_j\right)}{b_1\cdots b_k}$$

για κάποιους $n_1,...,n_k\in\mathbb{Z}$. Π.χ., θέτοντας $c_i:=a_i\left(\prod_{j\in\{1,\dots,k\}\setminus\{i\}}b_j\right)$ για κάθε $i\in\{1,...,k\}$, για τον $s:=\frac{1}{2b_1\cdots b_k}$ θα ίσχυε

$$\tfrac{1}{2b_1\cdots b_k}=\tfrac{\sum_{i=1}^{k}n_ic_i}{b_1\cdots b_k}\Rightarrow 2\left(\sum_{i=1}^{k}n_ic_i\right)=1, \tag{2.8}$$

πράγμα άτοπο, καθότι *δεν υφίστανται* $n_1,...,n_k\in\mathbb{Z}$ ικανοποιούντες την εξίσωση (2.8). (Το αριστερό μέλος τής (2.8) είναι ένας άρτιος και το δεξιό της ένας περιττός ακέραιος αριθμός.)

2.2.14 Σημείωση. Υπάρχουν *υποομάδες* απείρων αλλά πεπερασμένως παραγομένων ομάδων *που δεν είναι πεπερασμένως παραγόμενες*. (Βλ. άσκηση **2-31**.) Ικανές συνθήκες, για να είναι μια υποομάδα μιας πεπερασμένως παραγόμενης ομάδας αφ' εαυτής πεπερασμένως παραγόμενη, δίδονται στις προτάσεις 4.1.56 και 9.6.9.

2.2.15 Ορισμός. Μια ομάδα καλείται **κυκλική** (ή **μονογενής**) όταν μπορεί να παραχθεί (υπό την έννοια τού 2.2.1) από ένα *μονοσύνολο*[25]. (Για *κάθε* ομάδα G εισάγουμε τον συμβολισμό $\mathbf{CSubg}(G):=\{\,H\in\mathbf{Subg}(G)|\,H$ κυκλική$\}$.)

2.2.16 Παραδείγματα. (i) Η $(\mathbb{Z},+)$ (όπως προαναφέραμε στο 2.2.5 (i)) είναι κυκλική. Το ίδιο ισχύει και για την $(n\mathbb{Z},+)$, για οιονδήποτε $n\in\mathbb{Z}$.

[24]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 $\mathrm{card}(Y)\leq 2n$ και κάθε στοιχείο τής G γράφεται (λόγω τής (2.6)) υπό τη μορφή $y_1y_2\cdots y_k$, όπου $(y_1,...,y_k)\in Y^k$ για κάποιον $k\in\mathbb{N}$, οπότε $|G|\leq\mathrm{card}(\bigcup_{k\in\mathbb{N}}Y^k)\leq\aleph_0$, διότι η ένωση μιας αριθμήσιμης οικογενείας πεπερασμένων συνόλων είναι το πολύ αριθμήσιμη.

[25]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 $G=\langle g\rangle$.

(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. 2.2.9), εφοδιαζόμενο με τον συνήθη *πολλαπλασιασμό* μιγαδικών αριθμών, καθίσταται αβελιανό μονοειδές. Μέσω τού $(\mathbb{Z}[i], \cdot)$ δημιουργείται η πολλαπλασιαστική ομάδα που έχει ως υποκείμενο σύνολό της το $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ (βλ. πρόταση 2.1.6). Η $(\mathbb{Z}[i]^\times, \cdot)$ είναι κυκλική, διότι[26]

$$\mathbb{Z}[i]^\times = \langle i \rangle = \langle -i \rangle .$$

(iv) Η ομάδα $(\mathcal{E}_n, \cdot)$, $n \in \mathbb{N}$, των n-οστών ριζών τής μονάδας (βλ. 2.1.21 (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. 2.2.13) 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. 2.2.12 (ii).)

2.2.17 Πρόταση. *Κάθε κυκλική ομάδα είναι αβελιανή.*

ΑΠΟΔΕΙΞΗ. 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 2.1.11 λαμβάνουμε

$$xy = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = yx,$$

οπότε η G είναι όντως αβελιανή. □

2.2.18 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» $g^n, n = 0, \pm 1, \pm 2, ...$ 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,*

$$\langle g \rangle = \left\{ e_G, g, g^2, ..., g^{l-1} \right\},$$

όπου $l := \min\{ k \in \mathbb{N} \mid g^k = e_G \}$.

ΑΠΟΔΕΙΞΗ. Αρκεί να δείξουμε το ότι ο ισχυρισμός στη δεύτερη περίπτωση είναι αληθής. Κατ' αρχάς, επειδή υπάρχουν ακέραιοι n, m, με $n > m$, τέτοιοι ώστε $g^{n-m} = e_G$, 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

[26] 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 $\mathbb{Z}[i]^\times = \langle -i \rangle$.

υπάρχουν μοναδικοί ακέραιοι q, r με $0 \leq r < l$, τέτοιοι ώστε να ισχύει $\nu = ql + r$ (βλ. Β.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 $e_G, g, g^2, ..., g^{l-1}$ είναι σαφώς διακεκριμένα. Εάν υποτεθεί ότι υπάρχουν μ, $\nu \in \{0, 1, ..., l-1\}$, για τους οποίους ισχύει $\mu > \nu$ και $g^{\mu} = g^{\nu}$, τότε $g^{\mu-\nu} = e_G$, $1 \leq \mu - \nu \leq l-1$, πράγμα που αντίκειται στην επιλογή τού l ως τής ελαχίστης δυνάμεως με αυτήν την ιδιότητα.□

2.2.19 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* [27].

ΑΠΟΔΕΙΞΗ. (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 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 $0 \leq r < d$, ήτοι $n \equiv r \,(\mathrm{mod}\, d)$ (βλ. Β.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. □

2.2.20 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) $\langle m\mathbb{Z}, n\mathbb{Z} \rangle = \text{μκδ}(m, n)\mathbb{Z}$.

[27] Επομένως, $\mathbf{Subg}(G) = \mathbf{CSubg}(G)$ για κάθε κυκλική ομάδα G.

ΑΠΟΔΕΙΞΗ. 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

$$m\mathbb{Z} \supseteq n\mathbb{Z} \Longleftrightarrow m \mid n.$$

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 $m\mathbb{Z} \supseteq n\mathbb{Z}$. Εν συνεχεία θα αποδείξουμε ότι

$$m\mathbb{Z} \sqsupseteq n\mathbb{Z} \Longleftrightarrow m \mid n.$$

Προφανώς, $m\mathbb{Z} \sqsupseteq n\mathbb{Z} \Rightarrow m\mathbb{Z} \supseteq n\mathbb{Z} \Rightarrow m \mid n$ (από ό,τι προείπαμε). Και αντιστρόφως· εάν $m \mid n$, τότε

$$\left.\begin{array}{r} m\mathbb{Z} \supseteq n\mathbb{Z} \text{ (από ό,τι προείπαμε)} \\ \mathbb{Z} \sqsupseteq m\mathbb{Z} \text{ (βλ. 2.1.21 (iii))} \end{array}\right\} \underset{2.1.20}{\Longrightarrow} m\mathbb{Z} \sqsupseteq n\mathbb{Z}.$$

(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 2.2.19 $\exists k \in \mathbb{N} : m\mathbb{Z} \cap n\mathbb{Z} = k\mathbb{Z}$. 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

$$m \mid |l| \text{ και } n \mid |l| \Rightarrow |l|\,\mathbb{Z} \sqsubseteq m\mathbb{Z} \text{ και } |l|\,\mathbb{Z} \sqsubseteq n\mathbb{Z},$$

οπότε

$$|l|\,\mathbb{Z} \sqsubseteq m\mathbb{Z} \cap n\mathbb{Z} = k\mathbb{Z} \Rightarrow k \mid |l| \underset{\text{B.1.5 (i)}}{\Longrightarrow} k \mid l \underset{\text{B.2.25}}{\Longrightarrow} k = \text{εκπ}\,(m, n)\,.$$

(iv) Σύμφωνα με το (i) τής προτάσεως 2.2.19 $\exists \kappa \in \mathbb{N} : \langle m\mathbb{Z}, n\mathbb{Z}\rangle = \kappa\mathbb{Z}$. 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

$$|\lambda| \mid m \text{ και } |\lambda| \mid n \Rightarrow m\mathbb{Z} \sqsubseteq |\lambda|\,\mathbb{Z} \text{ και } n\mathbb{Z} \sqsubseteq |\lambda|\,\mathbb{Z}.$$

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

$$\kappa\mathbb{Z} = \langle m\mathbb{Z}, n\mathbb{Z}\rangle \sqsubseteq |\lambda|\,\mathbb{Z} \Rightarrow |\lambda| \mid \kappa \underset{\text{B.1.5 (i)}}{\Longrightarrow} \lambda \mid \kappa \underset{\text{B.2.6}}{\Longrightarrow} \kappa = \text{μκδ}\,(m, n)\,,$$

και η απόδειξη λήγει εδώ. □

2.3 ΤΑΞΗ ΣΤΟΙΧΕΙΟΥ ΜΙΑΣ ΟΜΑΔΑΣ

2.3.1 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

$$\mathrm{tors}(G):=\left\{g\in G\,\middle|\,g^k=e_G,\ \text{για κάποιον } k\in\mathbb{N}\right\}$$

το αποτελούμενο από όλα τα στοιχεία τής G που έχουν πεπερασμένη τάξη καλείται **σύνολο στρέψεως**[28] 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[29] 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**.

2.3.2 Παρατήρηση. Εάν $g\in G$, τότε, σύμφωνα με την πρόταση 2.2.18, έχουμε:

$$\mathrm{ord}\,(g)=|\langle g\rangle|\,. \tag{2.9}$$

2.3.3 Παράδειγμα. Στην $(\mathbb{Z}_4,+)$ τα στοιχεία $[0]_4,[1]_4,[2]_4$ και $[3]_4$ έχουν τάξη $1,4,2$ και 4, αντιστοίχως.

2.3.4 Παράδειγμα. Στην ομάδα των τετρανίων $\mathbf{Q}$ (βλ. 2.2.11) καθένα των στοιχείων $\mathbf{j}$ και $\mathbf{k}$ έχει τάξη 4.

2.3.5 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.

---

[28] 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 2.1.12, $(g_1g_2^{-1})^{kl}=g_1^{kl}(g_2^{-1})^{kl}=(g_1^k)^l(g_2^l)^{-k}=e_G\cdot e_G=e_G$, οπότε $g_1g_2^{-1}\in G$ και, ως εκ τούτου, $\mathrm{tors}(G)\sqsubseteq G$ επί τη βάσει τού κριτηρίου 2.1.16 (i)⇔(iii).)

[29] Προφανώς, $\mathrm{ord}(g)=1\iff g=e_G$.

2.3.6 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. 2.1.21 (vi)) αποτελεί *περιοδική* υποομάδα[30] 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. 2.1.21 (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

$$\boxed{\mathcal{E}_{p^\infty} := \bigcup_{n\in\mathbb{N}} \mathcal{E}_{p^n} = \left\{z \in \mathbb{C}\,\middle|z^{p^n} = 1,\ \text{για κάποιον } n \in \mathbb{N}\right\} \sqsubset \mathcal{E}_\infty \sqsubset \mathbb{S}^1}$$

τής $\mathcal{E}_\infty$ η απαρτιζόμενη από τις p^n-οστές ρίζες τής μονάδας, όπου p *τυχών* πρώτος αριθμός.

2.3.7 Πρόταση. *Έστω $(G, \cdot)$ μια πεπερασμένη ομάδα. Τότε η G είναι κυκλική εάν και μόνον εάν υπάρχει κάποιο $g \in G$ με* $\mathrm{ord}(g) = |G|$.

ΑΠΟΔΕΙΞΗ. Εάν η G είναι κυκλική, τότε $\exists g \in G : G = \langle g\rangle$, οπότε -βάσει τής (2.9)-

$$\mathrm{ord}(g) = |\langle g\rangle| = |G|\,.$$

Και αντιστρόφως· εάν υπάρχει κάποιο $g \in G$ με $\mathrm{ord}(g) = |G|$, τότε

$$|\langle g\rangle| = |G| \ \text{ και } \ \langle g\rangle \subseteq G \Longrightarrow G = \langle g\rangle\,,$$

οπότε η G είναι κυκλική. □

2.3.8 Πρόταση. *Έστω $(G, \cdot)$ μια ομάδα. Εάν $g \in G$ και* $\mathrm{ord}(g) = n \in \mathbb{N}$, *τότε*

$$(g^m = e_G,\ \textit{για κάποιον } m \in \mathbb{Z}) \Longleftrightarrow n\,|m\ .$$

ΑΠΟΔΕΙΞΗ. Εάν $n\,|m$, τότε $\exists q \in \mathbb{Z} : m = nq$. Επομένως,

$$g^m = g^{nq} = (g^n)^q = (e_G^n)^q = e_G^q = e_G.$$

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 $0 \le r < n$. Ως εκ τούτου,

$$g^m = g^{nq+r} = (g^n)^q\, g^r = (e_G^n)^q\, g^r = e_G^q g^r = e_G g^r = g^r.$$

Όμως ο n είναι ο ελάχιστος φυσικός αριθμός για τον οποίο ισχύει $g^n = e_G$. Άρα έχουμε $r = 0$ και $n\,|m$. □

[30] 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 $(z_1 z_2^{-1})^{mn} = z_1^{mn}(z_2^{-1})^{mn} = (z_1^m)^n (z_2^n)^{-m} = 1\cdot 1 = 1$, έχουμε $z_1 z_2^{-1} \in \mathcal{E}_\infty$. Άρα $\mathcal{E}_\infty \sqsubset \mathbb{C}\smallsetminus\{0\}$. (Βλ. κριτήριο 2.1.16 (i)⇔(iii)).

2.3.9 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Τότε ισχύουν τα ακόλουθα*:

(i) $\text{ord}(g)=\text{ord}\left(g^{-1}\right), \forall g\in G$.

(ii) $\text{ord}\left(g_2g_1g_2^{-1}\right)=\text{ord}(g_1), \forall (g_1,g_2)\in G\times G$.

(iii) $\text{ord}(g_1g_2)=\text{ord}(g_2g_1), \forall (g_1,g_2)\in G\times G$.

(iv) *Εάν κάθε στοιχείο τής G έχει τάξη το πολύ 2, τότε η G είναι αβελιανή.*

(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 $m\geq n$, για κάθε $m\in\mathbb{N}$ για το οποίο $\left(g^{-1}\right)^m=e_G$. Όμως

$$\begin{aligned}&\left(g^{-1}\right)^m=e_G\Longrightarrow g^{-m}=e_G\Longrightarrow (g^{-m})^{-1}=e_G^{-1}=e_G\\ &\Longrightarrow g^m=e_G\underset{2.3.8}{\Longrightarrow} n\,|m\Longrightarrow n\leq m.\end{aligned}$$

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 $\left(g_2g_1g_2^{-1}\right)^n=g_2g_1^ng_2^{-1}$. Επειδή -εξ υποθέσεως- $g_1^n=e_G$, έχουμε

$$\left(g_2g_1g_2^{-1}\right)^n=g_2e_Gg_2^{-1}=g_2g_2^{-1}=e_G.$$

Για να αποδείξουμε ότι $\text{ord}\left(g_2g_1g_2^{-1}\right)=n$ αρκεί να ισχύει $m\geq n$, για κάθε $m\in\mathbb{N}$ για το οποίο $\left(g_2g_1g_2^{-1}\right)^m=e_G$. Όμως

$$\left(g_2g_1g_2^{-1}\right)^m=g_2g_1^mg_2^{-1}=e_G\Longrightarrow g_2^{-1}g_2g_1^mg_2^{-1}g_2=g_2^{-1}e_Gg_2\Longrightarrow g_1^m=e_G,$$

οπότε $m\geq n$. Και αντιστρόφως· εάν $\text{ord}\left(g_2g_1g_2^{-1}\right)=n$, τότε, εφαρμόζοντας την ήδη αποδειχθείσα συνεπαγωγή (με εναλλαγή των ρόλων των g_1 και $g_2g_1g_2^{-1}$, καθώς και των g_2 και g_2^{-1}), λαμβάνουμε

$$\text{ord}\left(g_2g_1g_2^{-1}\right)=n\Longrightarrow \text{ord}\left(g_2^{-1}\left(g_2g_1g_2^{-1}\right)g_2\right)=\text{ord}\,(g_1)=n.$$

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

$$\text{ord}\left(g_2 g_1 g_2^{-1}\right) = \infty \Longrightarrow \text{ord}\left(g_2^{-1}\left(g_2 g_1 g_2^{-1}\right) g_2\right) = \text{ord}\left(g_1\right) = \infty.$$

(iii) Επειδή $g_1 g_2 = g_1 \left(g_2 g_1\right) g_1^{-1}$, 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 $(ab)^{mn} \underset{2.1.12}{=} a^{mn}b^{mn} = (a^m)^n (b^n)^m = e_G^n e_G^m = e_G$, η τάξη τού ab είναι κατ' ανάγκην πεπερασμένη και $\text{ord}(ab) \leq mn$. Έστω $r \in \mathbb{N}$, τέτοιος ώστε $(ab)^r = e_G$. Προφανώς,

$$\left.\begin{array}{c} e_G = (ab)^{rm} \underset{2.1.12}{=} a^{rm}b^{rm} = (a^m)^r b^{rm} = b^{rm} \\ e_G = (ab)^{rn} \underset{2.1.12}{=} a^{rn}b^{rn} = a^{rn}(b^n)^r = a^{rn} \end{array}\right\} \underset{2.3.8}{\Longrightarrow} \left\{\begin{array}{c} n \mid rm \\ \text{και} \\ m \mid rm \end{array}\right\}$$

$$\underset{\text{B.2.9}}{\Longrightarrow} \left\{\begin{array}{c} n \mid r \\ \text{και} \\ m \mid r \end{array}\right\} \underset{\text{B.2.10}}{\Longrightarrow} mn \mid r \Rightarrow mn \leq r \Rightarrow mn \leq \text{ord}(ab).$$

Κατά συνέπειαν, $\text{ord}(ab) = mn$. □

2.3.10 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) $H = \left\langle g^{\text{μκδ}(m,n)} \right\rangle$.

ΑΠΟΔΕΙΞΗ. (i) Κατά την πρόταση 2.2.19 η $H = \langle a \rangle$ είναι μια κυκλική υποομάδα τής G. Αρκεί λοιπόν να προσδιορίσουμε την τάξη της. Σύμφωνα με την πρόταση 2.3.8, εάν $k \in \mathbb{N}$, τότε $a^k = e_G \Longleftrightarrow g^{nk} = e_G \Longleftrightarrow m \,|nk$. Άρα

$$|H| = \min\{\, k \in \mathbb{N} \mid \, m \,|nk \,\}.$$

Έστω $d := \text{μκδ}(m, n)$. Βάσει τού θεωρήματος B.2.5 υπάρχουν $\mu, \nu \in \mathbb{Z}$, τέτοιοι ώστε

$$d = \mu m + \nu n \Longrightarrow 1 = \mu\left(\frac{m}{d}\right) + \nu\left(\frac{n}{d}\right). \tag{2.10}$$

Από την τελευταία ισότητα συνάγεται ότι οι $\frac{m}{d}$ και $\frac{n}{d}$ είναι σχετικώς πρώτοι (βλ. πόρισμα Β.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 μκδ$(\frac{n}{d}, \frac{m}{d}) = 1$, η ανωτέρω συνθήκη ισοδυναμεί με την: $\frac{m}{d} \big| \, k$ (βλ. πόρισμα Β.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 (2.10),

$$g^d = g^{\mu m + \nu n} = (g^m)^\mu \, (g^n)^\nu = e_G^\mu \, (g^n)^\nu = e_G \, (g^n)^\nu = (g^n)^\nu \Longrightarrow g^d \in \langle g^n \rangle \,,$$

οπότε και η $\left\langle g^d \right\rangle$ είναι υποομάδα τής H. □

2.3.11 Πόρισμα. *Έστω $(G, \cdot)$ μια ομάδα και έστω $(m, n) \in \mathbb{N}^2$. Εάν $g \in G$, τότε ισχύει η συνεπαγωγή*

$$\text{ord}\,(g) = m \Longrightarrow \text{ord}\,(g^n) = \frac{m}{\text{μκδ}\,(m, n)}.$$

ΑΠΟΔΕΙΞΗ. Προφανής βάσει τής προτάσεως 2.3.10 και τού (2.9). □

2.3.12 Πόρισμα. *Έστω $(G, \cdot)$ μια ομάδα και έστω $(m, n) \in \mathbb{N}^2$. Εάν $g \in G$, τότε ισχύει η συνεπαγωγή*

$$[\text{ord}\,(g) = m \ \textit{και} \ \ n \,|m] \Longrightarrow \text{ord}\,(g^n) = \frac{m}{n}.$$

2.3.13 Παραδείγματα. (i) Εάν η $(G, \cdot)$ είναι μια ομάδα, $g \in G$ και ord$(g) = 12$, τότε, επί παραδείγματι,

$$\text{ord}\left(g^9\right) = \frac{12}{\text{μκδ}\,(12, 9)} = \frac{12}{3} = 4, \ \text{ord}\left(g^{10}\right) = \frac{12}{\text{μκδ}\,(12, 10)} = \frac{12}{2} = 6.$$

(ii) Εντός τής $(\mathbb{Z}_{48}, +)$ έχουμε 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

$$\text{ord}\,(3\ [4]_{48}) = \frac{12}{\text{μκδ}\,(12, 3)} = \frac{12}{3} = 4, \ \text{ord}\,(5\ [4]_{48}) = \frac{12}{\text{μκδ}\,(12, 5)} = \frac{12}{1} = 12.$$

Γενικότερα, ισχύει το ακόλουθο:

2.3.14 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*:

$$\text{ord}\left([n]_m\right) = \frac{m}{\text{μκδ}\,(m,n)}.$$

ΑΠΟΔΕΙΞΗ. Επειδή $|\mathbb{Z}_m| = m$, $\mathbb{Z}_m = \langle [1]_m \rangle \Longrightarrow \text{ord}([1]_m) = |\langle [1]_m \rangle| = m$ και $[n]_m = n\,[1]_m$, συνάγεται ότι $\text{ord}([n]_m) = \text{ord}(n\,[1]_m) = \frac{m}{\text{μκδ}(m,n)}$ μέσω εφαρμογής τού πορίσματος 2.3.11. □

2.3.15 Πόρισμα. *Έστω $(G, \cdot)$ μια ομάδα και έστω $g \in G$ με* $\text{ord}(g) = \kappa_1\kappa_2$, *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 $g = g_1 g_2$ με* $\text{ord}(g_1) = \kappa_1$ *και* $\text{ord}(g_2) = \kappa_2$.

ΑΠΟΔΕΙΞΗ. 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 Β.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. Β.2.14 (i) και Β.2.8), οπότε

$$\text{ord}(g_1) \underset{2.3.11}{=} \frac{\kappa_1\kappa_2}{\text{μκδ}\,(\kappa_1\kappa_2, \lambda_2\kappa_2)} = \frac{\kappa_1\kappa_2}{\kappa_2} = \kappa_1$$

και, κατ' αναλογίαν, $\text{ord}(g_2) = \frac{\kappa_1\kappa_2}{\kappa_1} = \kappa_2$. □

2.3.16 Πόρισμα. *Έστω ότι η $G = \{e, g, g^2, ..., g^{m-1}\} = \langle g \rangle$ (όπου $e = e_G$) είναι μια πεπερασμένη κυκλική ομάδα τάξεως $m \in \mathbb{N}$ και ότι $k, l \in \{0, ..., m-1\}$. Τότε*

$$\left\langle g^k \right\rangle = \left\langle g^l \right\rangle \Longleftrightarrow \text{μκδ}\,(k,m) = \text{μκδ}\,(l,m)\,.$$

ΑΠΟΔΕΙΞΗ. 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 2.3.10 (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 2.3.10 (ii), ισχύουν οι ισότητες $\left\langle g^k \right\rangle = \left\langle g^d \right\rangle = \left\langle g^l \right\rangle$. □

2.3.17 Πόρισμα. *Έστω ότι η $G = \{e, g, g^2, ..., g^{m-1}\}$ (όπου $e = e_G$) είναι μια πεπερασμένη κυκλική ομάδα τάξεως $m \in \mathbb{N}$ και ότι $k \in \{0, ..., m-1\}$. Τότε η $\left\langle g^k \right\rangle$ παράγει την G εάν και μόνον εάν* $\text{μκδ}(k,m) = 1$. *Ως εκ τούτου,*

$$\text{card}\left(\{\text{γεννήτορες τής } G\}\right) = \phi\,(m)\,,$$

όπου ϕ η συνάρτηση φι τού Euler (βλ. Β.4.15).

2.3.18 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: $\mathbb{Z}_8 = \langle [1]_8 \rangle = \langle [3]_8 \rangle = \langle [5]_8 \rangle = \langle [7]_8 \rangle$.

2.3.19 Πρόταση. (Πεπερασμένες ομάδες τάξεως το πολύ 3) *Όλες οι ομάδες τάξεως* ≤ 3 *είναι κυκλικές.*

ΑΠΟΔΕΙΞΗ. 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 2.1.9 (i)). Τούτο σημαίνει ότι $g^2 = e$, οπότε $\text{ord}(g) = 2$. Από την πρόταση 2.3.7 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 2.3.7 και το πόρισμα 2.3.16 έπεται ότι η $(G, \cdot)$ είναι κυκλική με $G = \langle x \rangle = \langle x^2 \rangle$. □

2.3.20 Σημείωση. Μια ομάδα τάξεως 4 δεν είναι κατ' ανάγκην κυκλική· ωστόσο, οφείλει να είναι *αβελιανή*, όπως θα δούμε στο θεώρημα 3.5.6.

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 2.3.21 και τα συνακόλουθα πορίσματα 2.3.23 και 2.4.25 μας παρέχουν μια πλήρη (και αρκετά εύκολη) περιγραφή τόσον τού τρόπου σχηματισμού όσον και τού πλήθους των διαθέσιμων υποομάδων.

2.3.21 Θεώρημα. *Έστω* $G = \{e, g, g^2, ..., g^{m-1}\}$ *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 μια μονοσημάντως ορισμένη υποομάδα τάξεως* n.

ΑΠΟΔΕΙΞΗ. (i) Εάν $n \,|m$, τότε $\frac{m}{n} \,|m$, οπότε -κατά το πόρισμα 2.3.12-

$$\text{ord}(g^{\frac{m}{n}}) = \left|\left\langle g^{\frac{m}{n}} \right\rangle\right| = \frac{m}{m/n} = n,$$

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 $k \in \{0,...,m-1\}$ (πρβλ. 2.2.19 (ii)), τότε (λόγω τής 2.3.10 (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 $\exists k_1, k_2 \in \{0,...,m-1\} : H_1 = \left\langle g^{k_1} \right\rangle,\ \ H_2 = \left\langle g^{k_2} \right\rangle$. 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 2.3.10 (ii)- τούτο σημαίνει ότι $H_1 = H_2$. □

2.3.22 Πόρισμα. *Έστω $G = \{e, g, g^2,..., g^{m-1}\}$ μια πεπερασμένη κυκλική ομάδα τάξεως $m \in \mathbb{N}$ (όπου $e = e_G$). Σύμφωνα με το* (ii) *τού θεωρήματος* 2.3.21, *για κάθε θετικό ακέραιο διαιρέτη n τού m υφίσταται μία και μόνον υποομάδα τής G τάξεως n. Αυτή είναι η*

$$\left\langle g^{\frac{m}{n}} \right\rangle = \{\, x \in G |\, x^n = e\}.$$

ΑΠΟΔΕΙΞΗ. Το ότι η $\left\langle g^{\frac{m}{n}} \right\rangle$ είναι η μοναδική υποομάδα τής G τάξεως n έχει ήδη αποδειχθεί. Προφανώς[31],

$$\left\langle g^{\frac{m}{n}} \right\rangle = \{e, g^{\frac{m}{n}}, g^{\frac{2m}{n}},..., g^{\frac{(n-1)m}{n}}\}$$

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

$$g^{kn} = e \underset{2.3.8}{\Longrightarrow} \text{ord}(g) = m \mid kn \Rightarrow [\exists l \in \mathbb{N} : kn = lm].$$

Επειδή $0 \le k = \frac{lm}{n} \le m-1 \Rightarrow 0 \le l \le \frac{(m-1)n}{m} \le m-1$, έχουμε

$$x = g^k = (g^{\frac{m}{n}})^l \in \left\langle g^{\frac{m}{n}} \right\rangle,$$

οπότε ισχύει και ο αντίστροφος εγκλεισμός $\{\, x \in G |\, x^n = e\} \subseteq \left\langle g^{\frac{m}{n}} \right\rangle$. □

2.3.23 Πόρισμα. *Έστω ότι η $G = \{e, g, g^2,..., g^{m-1}\}$ είναι μια πεπερασμένη κυκλική ομάδα τάξεως $m \in \mathbb{N}$ (όπου $e = e_G$) και ότι οι*[32] *$d_1, d_2,..., d_\nu$ είναι οι θετικοί ακέραιοι διαιρέτες τού m. Τότε οι $\left\langle g^{d_1} \right\rangle, \left\langle g^{d_2} \right\rangle,..., \left\langle g^{d_\nu} \right\rangle$ είναι όλες οι σαφώς διακεκριμένες (ήτοι οι ανά δύο διαφορετικές) υποομάδες τής G.*

[31] Όταν $n \ge 2$, 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

$$g^{\frac{im}{n}} g^{-\frac{m}{n}} = g^{\frac{jm}{n}} g^{-\frac{m}{n}} \Rightarrow g^i = g^j \Rightarrow g^{i-j} = e \underset{2.3.8}{\Longrightarrow} \text{ord}(g) = m \mid i-j \Rightarrow m \le i-j,$$

και θα οδηγούμεθα σε κάτι που είναι άτοπο (διότι $m \ge n > n-1 \ge i-j$).

[32] Για τον υπολογισμό τού ν βλ. το (i) τής προτάσεως Β.3.15.

ΑΠΟΔΕΙΞΗ. Επειδή $d_j | m$, για κάθε $j \in \{1,2,...,\nu\}$, έχουμε μκδ$(d_j, m) = d_j$. Εάν λοιπόν για κάποιους $j, j' \in \{1,2,...,\nu\}$ ισχύει $\langle g^{d_j} \rangle = \langle g^{d_{j'}} \rangle$, τότε

$$\left|\langle g^{d_j} \rangle\right| = \left|\langle g^{d_{j'}} \rangle\right| \Longrightarrow d_j = \text{μκδ}\,(d_j, m) = \text{μκδ}\,(d_{j'}, m) = d_{j'},$$

απ' όπου έπεται ότι $j = j'$. □

► **Ομάδες πεπερασμένου εκθέτη**. Η παρούσα ενότητα κλείνει με τον ορισμό των ομάδων πεπερασμένου εκθέτη και την παράθεση των βασικών ιδιοτήτων τού εκθέτη πεπερασμένων ομάδων.

2.3.24 Ορισμός. (Εκθέτης περιοδικής ομάδας)
Έστω $(G, \cdot)$ μια περιοδική ομάδα. Εάν το σύνολο

$$\{\, n \in \mathbb{N} |\, g^n = e_G,\, \forall g \in G\} \tag{2.11}$$

δεν είναι κενό, τότε λέμε ότι η G είναι μια **ομάδα πεπερασμένου εκθέτη**. Εν τοιαύτη περιπτώσει ορίζουμε ως **εκθέτη**[33] $\exp(G)$ **τής** G το ελάχιστο στοιχείο αυτού τού συνόλου[34]. Εάν, αντιθέτως, το (2.11) είναι κενό, τότε είθισται να λέμε ότι η G είναι μια **ομάδα μη φρασσόμενου εκθέτη**[35] (και να γράφουμε $\exp(G) = \infty$).

2.3.25 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* $\exp(H) \mid \exp(G)$.

ΑΠΟΔΕΙΞΗ. (i) Επειδή, σύμφωνα με την πρόταση 2.3.8, το σύνολο (2.11) 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), $\text{ord}(g) \mid \exp(G)$ *για κάθε* $g \in G$, 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 Β.2.25.) □

[33] Προσοχή! Ορισμένοι συγγραφείς ονομάζουν *κάθε* στοιχείο τού (2.11) εκθέτη τής G και για τον $\exp(G)$ χρησιμοποιούν τον όρο *ελάχιστος εκθέτης*. (Εδώ *δεν* ακολουθείται αυτή η ορολογία.)

[34] Από το (i) τής προτάσεως 2.3.25 έπεται ότι *κάθε πεπερασμένη* ομάδα είναι ομάδα πεπερασμένου εκθέτη. Ωστόσο, υπάρχουν και περιοδικές ομάδες πεπερασμένου εκθέτη που έχουν *άπειρη* τάξη. (Βλ. 7.1.95 (ii).)

[35] Η $\mathcal{E}_\infty$ (βλ. 2.3.6 (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.

2.3.26 Πρόταση. *Για κάθε πεπερασμένη αβελιανή*[36] *ομάδα* $(G,\cdot)$ *ισχύει η ισότητα*:

$$\exp(G) = \max\{\,\mathrm{ord}(g)|\, g \in G\}\,.$$

ΑΠΟΔΕΙΞΗ. Εάν $l := \max\{\,\mathrm{ord}(g)|\, g \in G\}\,$, τότε, σύμφωνα με το (ii) τής προτάσεως 2.3.25, $l \mid \exp(G)$. Θα αποδείξουμε ότι $\exp(G) = \text{εκπ}(\{\,\mathrm{ord}(g)|\, g \in G\}) \mid l$. Προς τούτο αρκεί (λόγω τής προτάσεως Β.2.25) να δείξουμε ότι $\mathrm{ord}(g) \mid l$ *για κάθε* $g \in G$. Θα εργασθούμε με «εις άτοπον απαγωγή». Υποθέτουμε ότι υπάρχει κάποιο $y \in G$ με $\mathrm{ord}(y) \nmid l$. Τότε $\mathrm{ord}(y) \geq 2$ και για οιοδήποτε $x \in G$ με $\mathrm{ord}(x) = l$ υπάρχουν (βάσει τού λήμματος Β.3.14) κάποιοι $m, n, j \in \mathbb{N}$, $i \in \mathbb{N}_0$ και κάποιος πρώτος αριθμός p, ούτως ώστε να ισχύει

$$\mathrm{ord}(x) = l = p^i m \ \text{ και } \ \mathrm{ord}(y) = p^j n, \ \text{όπου} \ \ p \nmid m,\ p \nmid n \ \text{ και } \ j > i.$$

Κατά το πόρισμα 2.3.11,

$$\mathrm{ord}(x^{p^i}) = \frac{l}{\text{μκδ}(l, p^i)} = \frac{l}{p^i} = m, \ \mathrm{ord}(y^n) = \frac{p^j n}{\text{μκδ}(p^j n, n)} = \frac{p^j n}{n} = p^j.$$

Επειδή $p \nmid m \Rightarrow \text{μκδ}(m,p) = 1 \underset{\text{Β.2.13}}{\Longrightarrow} \text{μκδ}(m, p^j) = 1$ και η G είναι αβελιανή, έχουμε

$$\mathrm{ord}(\underbrace{x^{p^i} y^n}_{\in G}) \underset{\text{2.3.9 (v)}}{=} mp^j = lp^{j-i} > l,$$

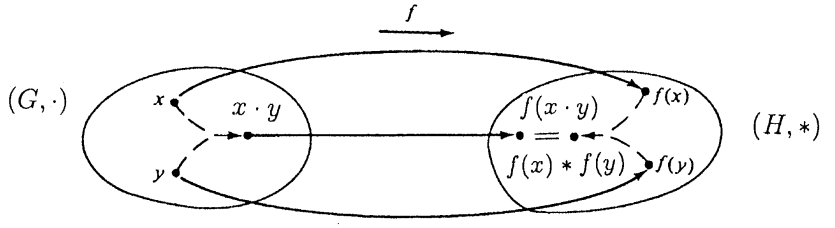
κάτι που αντίκειται στον ορισμό τού l. Άρα $\exp(G) \mid l \Rightarrow \exp(G) = l$. □

2.4 ΟΜΟΜΟΡΦΙΣΜΟΙ, ΙΣΟΜΟΡΦΙΣΜΟΙ ΚΑΙ ΑΥΤΟΜΟΡΦΙΣΜΟΙ ΟΜΑΔΩΝ

2.4.1 Ορισμός. Έστω ότι οι $(G,\cdot)$ και $(H,*)$ είναι δυο ομάδες. Μια απεικόνιση[37] $f : G \longrightarrow H$ καλείται **ομομορφισμός (ομάδων)** όταν για οιαδήποτε $x, y \in G$ ισχύει η ισότητα

$$\boxed{f(x \cdot y) = f(x) * f(y),} \tag{2.12}$$

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).



[36] Υπάρχουν πεπερασμένες μη αβελιανές ομάδες για τις οποίες αυτή η ισότητα δεν ισχύει. Επί παραδείγματι, η συμμετρική ομάδα $\mathfrak{S}_3$ (βλ. εδ. 3.2.2) έχει ένα στοιχείο τάξεως 1, 3 στοιχεία τάξεως 2 και 2 στοιχεία τάξεως 3. Επομένως, $\exp(\mathfrak{S}_3) = \text{εκπ}(1,2,3) = 6 > 3 = \max\{\,\mathrm{ord}(\sigma)|\, \sigma \in \mathfrak{S}_3\}$.

[37] Όταν επιθυμούμε να τονίσουμε το ποιες είναι οι πράξεις αναφοράς μας, γράφουμε $f : (G,\cdot) \longrightarrow (H,*)$.

2.4.2 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.

2.4.3 Πρόταση. *Εάν η $f : (G,\cdot) \longrightarrow (H,*)$ είναι ένας ομομορφισμός ομάδων, τότε ισχύουν τα εξής*:
(i) $f\left(e_G\right) = e_H$.
(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* $\mathrm{ord}(g) = n\in\mathbb{N}$, *τότε* $\mathrm{ord}(f(g)) = m\in\mathbb{N}$ *και* $m\mid n$.

ΑΠΟΔΕΙΞΗ. (i) Επειδή λόγω τής (2.12), $f\left(e_G\right) * f\left(e_G\right) = f\left(e_G\cdot e_G\right) = f\left(e_G\right)$, έχουμε

$$f\left(e_G\right) * f\left(e_G\right) * f\left(e_G\right)^{-1} = f\left(e_G\right) * f\left(e_G\right)^{-1} \Longrightarrow f\left(e_G\right) = f\left(e_G\right) * f\left(e_G\right)^{-1} = e_H.$$

(ii) Για κάθε $g\in G$,

$$f\left(g\right) * f\left(g^{-1}\right) = f\left(gg^{-1}\right) = f\left(e_G\right) = e_H = f\left(g^{-1}g\right) = f\left(g^{-1}\right) * f\left(g\right),$$

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 $n\geq 1$. 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 $n\in\mathbb{Z}\setminus\mathbb{N}_0$, τότε $-n>0$, οπότε εφαρμόζοντας το ανωτέρω αποδειχθέν για τον $-n$, το (ii), καθώς και το (iii) τής προτάσεως 2.1.11, 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 $\mathrm{ord}(g) = n\in\mathbb{N}$. Τότε $g^n = e_G$, οπότε

$$f(g^n) = f(g)^n = f(e_G) = e_H \underset{2.3.8}{\Longrightarrow} \mathrm{ord}(f(g)) = m\in\mathbb{N} \ \text{ και } \ m\mid n,$$

με τις πρώτες ισότητες ισχύουσες λόγω των (i) και (iii). □

2.4.4 Λήμμα. *Εάν η* $f : (G, \cdot) \longrightarrow (H, *)$ *είναι ένας ομομορφισμός ομάδων, τότε ισχύουν τα εξής*:

(i) *Η εικόνα* $\mathrm{Im}(f) = f(G)$ *τής* G *μέσω τής* f *είναι μια υποομάδα τής* H.

(ii) *Το σύνολο*

$$\boxed{\mathrm{Ker}\,(f) := f^{-1}(e_H) = \{\, g \in G \mid f(g) = e_H \}}$$

(*που καλείται, ιδιαιτέρως,* ***πυρήνας τής*** f) *είναι μια υποομάδα τής* G.

ΑΠΟΔΕΙΞΗ. (i) Κατά το 2.4.3 (i), $e_H = f(e_G) \in f(G)$. Εξάλλου, εάν $h, h' \in f(G)$, τότε υπάρχουν στοιχεία $g, g' \in K$ με $f(g) = h$ 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 2.1.16.

(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

$$f(gg'^{-1}) = f(g) * f(g'^{-1}) = f(g) * f(g)^{-1} = e_H * e_H^{-1} = e_H.$$

Συνεπώς $gg'^{-1} \in \mathrm{Ker}(f)$ και αρκεί να εφαρμόσουμε εκ νέου το (iii) τής προτάσεως 2.1.16. □

2.4.5 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**[38].

2.4.6 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* $f(K)$ *μέσω τής* f *είναι μια υποομάδα τής* $f(G)$.

(ii) *Εάν* $L \sqsubseteq \mathrm{Im}(f)$, *τότε η αντίστροφη εικόνα της* $f^{-1}(L) = \{\, g \in G \mid f(g) \in L \}$ *μέσω τής* f *είναι μια υποομάδα τής* G *έχουσα τον πυρήνα* $\mathrm{Ker}(f)$ *τής* f *ως υποομάδα της.*

ΑΠΟΔΕΙΞΗ. (i) Κατά το (i) τού λήμματος 2.4.4 η εικόνα $f(G)$ τής G μέσω τής f αποτελεί μια υποομάδα τής H. Επειδή το ουδέτερο στοιχείο e_G τής G απεικονίζεται μέσω τής f στο ουδέτερο στοιχείο τής H (που ταυτίζεται με το ουδέτερο στοιχείο τής $f(G)$), έχουμε $e_H \in f(K)$. Εξάλλου, εάν $u, v \in f(K)$, 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 $f(K)$ είναι μια υποομάδα τής H δυνάμει τού (iii) τής προτάσεως 2.1.16.

[38] Όταν για τις πράξεις των G και H χρησιμοποιείται ο προσθετικός συμβολισμός, είθισται αντί τού όρου *τετριμμένος ομομορφισμός* να χρησιμοποιείται ο όρος **μηδενικός ομομορφισμός**.

(ii) Επειδή το ουδέτερο στοιχείο e_G τής G απεικονίζεται μέσω τής f στο ουδέτερο στοιχείο τής $\mathrm{Im}(f)$ (που ταυτίζεται με το ουδέτερο στοιχείο τής ομάδας L), έχουμε $e_G \in f^{-1}(L)$. Εξάλλου, εάν $x, y \in f^{-1}(L)$, τότε ισχύει

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

διότι η L είναι υποομάδα τής G. Συνεπώς $xy^{-1} \in f^{-1}(L)$ και αρκεί να εφαρμόσουμε εκ νέου το (iii) τής προτάσεως 2.1.16. Τέλος, επειδή

$$\{e_H\} \subseteq L \Rightarrow \mathrm{Ker}(f) = f^{-1}(\{e_H\}) \subseteq f^{-1}(L),$$

έχουμε $\mathrm{Ker}(f) \sqsubseteq G, \mathrm{Ker}(f) \subseteq f^{-1}(L) \underset{2.1.20}{\Longrightarrow} \mathrm{Ker}(f) \sqsubseteq f^{-1}(L)$. □

2.4.7 Πόρισμα. (Θεώρημα αντιστοιχίσεως υποομάδων μέσω ομομορφισμών.) *Εάν η* $f : (G, \cdot) \longrightarrow (H, *)$ *είναι ένας ομομορφισμός ομάδων, τότε ορίζεται η απεικόνιση*

$$\boxed{\mathbf{Subg}(G; \mathrm{Ker}(f)) \ni K \overset{\Psi_f}{\longmapsto} f(K) \in \mathbf{Subg}(\mathrm{Im}(f))}$$

από το σύνολο $\mathbf{Subg}(G;\mathrm{Ker}(f))$ *των υποομάδων τής* G *που περιέχουν τον πυρήνα τής* f *στο σύνολο* $\mathbf{Subg}(\mathrm{Im}(f))$ *των υποομάδων τής εικόνας* $\mathrm{Im}(f)$ *τής* f. *Η* Ψ_f *είναι αμφιριπτική έχουσα την*

$$\mathbf{Subg}(\mathrm{Im}(f)) \ni L \overset{\Upsilon_f}{\longmapsto} f^{-1}(L) \in \mathbf{Subg}(G; \mathrm{Ker}(f))$$

ως αντίστροφό της. (*Ειδικότερα, κάθε υποομάδα τής* $\mathrm{Im}(f)$ *οφείλει να είναι τής μορφής* $f(K)$, *όπου* K *μια υποομάδα τής* G *που περιέχει τον πυρήνα τής* f.) *Επιπροσθέτως, ισχύουν τα ακόλουθα:*

(i) *Για* $K_1, K_2 \in \mathbf{Subg}(G;\mathrm{Ker}(f))$ *αληθεύει η κάτωθι αμφίπλευρη συνεπαγωγή*

$$K_1 \sqsubseteq K_2 \Longleftrightarrow \Psi_f(K_1) \sqsubseteq \Psi_f(K_2).$$

(ii) *Η* Ψ_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. 2.1.30, 2.1.32, και Α.2.26).

(iii) $\Psi_f(K_1 \cap K_2) = \Psi_f(K_1) \cap \Psi_f(K_2),\ \forall (K_1, K_2) \in \mathbf{Subg}(G; \mathrm{Ker}(f))^2$.

(iv) $\Psi_f(\langle K_1, K_2 \rangle) = \langle \Psi_f(K_1), \Psi_f(K_2) \rangle,\ \forall (K_1, K_2) \in \mathbf{Subg}(G; \mathrm{Ker}(f))^2$.

ΑΠΟΔΕΙΞΗ. Το ότι οι

$$\Psi_f : \mathbf{Subg}(G; \mathrm{Ker}(f)) \longrightarrow \mathbf{Subg}(\mathrm{Im}(f)) \ \text{ και } \ \Upsilon_f : \mathbf{Subg}(\mathrm{Im}(f)) \longrightarrow \mathbf{Subg}(G; \mathrm{Ker}(f))$$

είναι «καλώς ορισμένες» έπεται από την πρόταση 2.4.6. Ας θεωρήσουμε τυχούσα $K \in \mathbf{Subg}(G;\mathrm{Ker}(f))$. Προφανώς,

$$(\Upsilon_f \circ \Psi_f)(K) = \Upsilon_f(\Psi_f(K)) = f^{-1}(f(K)) \supseteq K,$$

(με τον εγκλεισμό αυτόν γνωστό από τη Θεωρία Συνόλων). Έστω $x \in f^{-1}(f(K))$. Τότε $f(x) \in f(K) \Rightarrow \exists u \in K : f(u) = f(x)$, οπότε

$$f(xu^{-1}) = f(x) * f(u^{-1}) = f(x) * f(u)^{-1} = f(u) * f(u)^{-1} = e_H.$$

Τούτο σημαίνει ότι $xu^{-1} \in \mathrm{Ker}(f) \subseteq K \Rightarrow x = \left(xu^{-1}\right) u \in K$. Κατά συνέπειαν,

$$f^{-1}(f(K)) = K \Rightarrow \Upsilon_f\left(\Psi_f\left(K\right)\right) = K,$$

οπότε $\Upsilon_f \circ \Psi_f = \mathrm{id}_{\mathbf{Subg}(G;\mathrm{Ker}(f))}$. Έστω τώρα τυχούσα $L \in \mathbf{Subg}(\mathrm{Im}(f))$. Προφανώς,

$$\left(\Psi_f \circ \Upsilon_f\right)(L) = \Psi_f\left(\Upsilon_f\left(L\right)\right) = f(f^{-1}(L)) \subseteq L,$$

(με τον εγκλεισμό αυτόν γνωστό από τη Θεωρία Συνόλων). Έστω $y \in L$. Επειδή $L \sqsubseteq \mathrm{Im}(f) = f(G)$,

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

Άρα $L \subseteq f\left(f^{-1}\left(L\right)\right)$ και, ως εκ τούτου, $f\left(f^{-1}\left(L\right)\right) = L \Longrightarrow \Psi_f\left(\Upsilon_f\left(L\right)\right) = L$, οπότε $\Psi_f \circ \Upsilon_f = \mathrm{id}_{\mathbf{Subg}(\mathrm{Im}(f))}$. Εκ των ανωτέρω συνάγεται ότι η Ψ_f είναι αμφιριπτική έχουσα την Υ_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

$$\left.\begin{array}{r} K_1 \subseteq K_2 \Rightarrow f(K_1) = \Psi_f\left(K_1\right) \subseteq \Psi_f\left(K_2\right) = f(K_2) \\ K_2 \sqsubseteq G \Rightarrow \Psi_f\left(K_2\right) = f(K_2) \sqsubseteq \mathrm{Im}(f) \end{array}\right\} \underset{2.1.20}{\Longrightarrow} \Psi_f\left(K_1\right) \sqsubseteq \Psi_f\left(K_2\right).$$

Επίσης, για οιαδήποτε $(K_1, K_2) \in \mathbf{Subg}(G;\mathrm{Ker}(f))^2$ με $\Psi_f\left(K_1\right) \sqsubseteq \Psi_f\left(K_2\right)$ έχουμε

$$\Upsilon_f\left(\Psi_f\left(K_1\right)\right) = K_1 \subseteq K_2 = \Upsilon_f\left(\Psi_f\left(K_2\right)\right),$$

οπότε $K_2 \sqsubseteq G, K_1 \subseteq K_2 \underset{2.1.20}{\Longrightarrow} K_1 \sqsubseteq K_2$.

(ii) Λόγω τού (i) αμφότερες οι Ψ_f και Υ_f είναι ισότονες (ήτοι *διατηρούν* τη μερική διάταξη " $\sqsubseteq$ "), οπότε η Ψ_f καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων $(\mathbf{Subg}(G;\mathrm{Ker}(f)), \sqsubseteq)$ και $(\mathbf{Subg}(\mathrm{Im}(f)), \sqsubseteq)$ (βλ. A.2.26). 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 A.2.27. □

2.4.8 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) $f(f^{-1}(L)) = \mathrm{Im}(f) \cap L$.

ΑΠΟΔΕΙΞΗ. (i) Για κάθε $g \in f^{-1}\left(L\right)$ έχουμε $f(g) \in L$, οπότε $f\left(f^{-1}\left(L\right)\right) \subseteq L$. Επειδή οι σχέσεις εγκλεισμού παραμένουν εν ισχύ κατόπιν εφαρμογής τής 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 $h \in f\left(K \cap f^{-1}(L)\right)$, οπότε ισχύει και ο αντίστροφος εγκλεισμός $f(K) \cap L \subseteq f\left(K \cap f^{-1}(L)\right)$.

(ii) Αρκεί να εφαρμοσθεί το (i) στην ειδική περίπτωση όπου $K = G$. □

2.4.9 Πρόταση. *Έστω $X \neq \varnothing$ ένα σύνολο γεννητόρων μιας ομάδας $(G, \cdot)$* (βλ. ορισμό 2.2.1 και πρόταση 2.2.3)*. 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*: $f_1|_X = f_2|_X \Longleftrightarrow f_1 = f_2$.

ΑΠΟΔΕΙΞΗ. (i) Έστω $h \in f(G)$. Τότε $\exists g \in G : h = f(g)$. Επειδή $G = \langle X \rangle$, η πρόταση 2.2.3 μας πληροφορεί ότι

$$\exists k \in \mathbb{N} : g = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}, \text{ για κάποια } x_j \in X \text{ και κάποια } \varepsilon_j \in \mathbb{Z}, \qquad (2.13)$$

$\forall j, 1 \leq j \leq k$. 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 (2.13). 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 $f_1 = f_2$. □

2.4.10 Ορισμός. Έστω $f : (G, \cdot) \longrightarrow (H, *)$ ένας ομομορφισμός ομάδων. Ο f καλείται

μονομορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι ενριπτική,
επιμορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι επιρριπτική,
ισομορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι αμφιρριπτική,
ενδομορφισμός (**τής** G)	$\underset{\text{ορσ}}{\Longleftrightarrow}$	$G = H$ και "$\cdot$" = "$*$",
αυτομορφισμός (**τής** G)	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η f είναι αμφιρριπτικός ενδομορφισμός τής G.

2.4.11 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 2.4.2 (i) είναι μονομορφισμός. Οι ομομορφισμοί μ_a οι ορισθέντες στο 2.4.2 (ii) είναι αυτομορφισμοί τής $(\mathbb{R}, +)$ για 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 $n \geq 2$.

(iv) Η ακόλουθη απεικόνιση είναι ένας ισομορφισμός μεταξύ τής $(\mathbb{Z}_4, +)$ και τής $(\mathbb{Z}[i]^\times, \cdot)$ (βλ. 2.2.16 (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 $\mathbf{GL}_2(\mathbb{R})$ (βλ. 2.1.7 (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 $\mathbf{SO}_2(\mathbb{R})$ (βλ. 2.1.21 (viii)):

$$\mathbb{S}^1 \ni \exp(i\theta) \longmapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \in \mathbf{SO}_2(\mathbb{R}) \quad (0 \leq \theta < 2\pi).$$

(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:

$$2 = f(r) = f(\tfrac{r}{2} + \tfrac{r}{2}) = f(\tfrac{r}{2})f(\tfrac{r}{2}) = f(\tfrac{r}{2})^2 \underset{f(\frac{r}{2}) \in \mathbb{Q}_{>0}}{\Longrightarrow} f(\tfrac{r}{2}) = \sqrt{2} \in \mathbb{R} \smallsetminus \mathbb{Q}_{>0}.$$

2.4.12 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).*

ΑΠΟΔΕΙΞΗ. (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). □

2.4.13 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 $(H, *)$, εφοδιαζόμενο με την εσωτερική πράξη τής συνθέσεως απεικονίσεων (βλ. 2.4.12 (i)), καθίσταται ημιομάδα. (Το σύνολο των ενδομορφισμών και, αντιστοίχως, το σύνολο των αυτομορφισμών *μιας* ομάδας ως προς αυτήν την πράξη καθίσταται *μονοειδές* και, αντιστοίχως, *ομάδα*. Βλ. πρόταση 2.4.29.)

(ii) Στην περίπτωση όπου η $(H, *)$ είναι *αβελιανή*, το $\mathrm{Hom}(G, H)$, εφοδιαζόμενο με μια (άλλη, 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. Βλ., π.χ., εδάφια 5.4.39, 7.1.20, 7.1.77 και 7.6.55.)

2.4.14 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 $f : G \longrightarrow H$.

2.4.15 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).*

ΑΠΟΔΕΙΞΗ. 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. □

2.4.16 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[39] $G\cong H$) όταν υπάρχει κάποιος ισομορφισμός[40] ομάδων $f: G\longrightarrow H$.

2.4.17 Πρόταση. *Μια ομάδα $(G,\cdot)$ είναι εμφυτεύσιμη σε μια ομάδα $(H,*)$ εάν και μόνον εάν η G είναι ισόμορφη με μια υποομάδα τής H.*

ΑΠΟΔΕΙΞΗ. 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. 2.4.4 (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 $G\ni g\longmapsto f(g)\in H$. □

2.4.18 Παράδειγμα. Όπως είδαμε στο εδάφιο 2.4.11 (vi), η $(\mathbb{C}\setminus\{0\},\cdot)$ εμφυτεύεται στη γενική γραμμική ομάδα $\mathrm{GL}_2(\mathbb{R})$.

2.4.19 Πρόταση. *Έστω $f: (G,\cdot)\longrightarrow(H,*)$ ένας ισομορφισμός ομάδων. Τότε ισχύουν τα ακόλουθα*:

(i) $|G|=|H|$.

(ii) *H G είναι αβελιανή εάν και μόνον εάν η H είναι αβελιανή.*

(iii) *H 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.* 2.3.1 (i)), *τότε και η H είναι περιοδική (και τανάπαλιν).*

ΑΠΟΔΕΙΞΗ. (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 2.4.3 συμπεραίνουμε ότι

$$\left.\begin{array}{l} h=f(g)^\nu\Rightarrow H\subseteq\langle f(g)\rangle \\ f(g)\in H\Rightarrow\langle f(g)\rangle\subseteq H \end{array}\right\}\Longrightarrow H=\langle f(g)\rangle\,.$$

[39] Κατ' αναλογίαν, ο συμβολισμός $G\ncong H$ θα δηλοί ότι η G δεν είναι ισόμορφη με την H.

[40] Ενίοτε, για να τονίσουμε (π.χ., σε μεταθετικά διαγράμματα και αλλού) ότι ένας ομομορφισμός ομάδων $f: G\longrightarrow H$ είναι *ισομορφισμός*, γράφουμε $f: G\xrightarrow{\cong} H$.

Το αντίστροφο αποδεικνύεται παρομοίως.

(iv) Έστω $g \in G$ τάξεως $\text{ord}(g) = n \in \mathbb{N}$. Τότε $\text{ord}(f(g)) = m \in \mathbb{N}$ και $m \mid n$. (Βλ. 2.4.3 (iv).) Επειδή

$$f(g)^m = f(g^m) = e_H \underset{2.3.8}{\Longrightarrow} g^m \in \text{Ker}(f) = \{e_G\} \Rightarrow g^m = e_G \Rightarrow n \mid m,$$

έχουμε τελικώς $m = n$. Εάν $\text{ord}(g) = \infty$, 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 $\text{ord}(f(g)) = \infty$.

(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 2.4.3 συνάγεται ότι

$$h^{n_x} = f(x)^{n_x} = f(x^{n_x}) = f(e_G) = e_H \Rightarrow \text{ord}(h) < \infty.$$

Το αντίστροφο αποδεικνύεται παρομοίως. □

2.4.20 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. 2.2.16 (i) και (v)).

(ii) Αμφότερες οι ομάδες $(\mathbb{Z}_8^\times, \cdot)$ και $(\mathbb{Z}_{10}^\times, \cdot)$ έχουν τάξη 4. (Βλ. 2.1.7 (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 $\text{ord}([3]_{10}) = 4$ (διότι $[3]_{10}^2 = [9]_{10}, [3]_{10}^3 = [7]_{10}$, και $[3]_{10}^4 = [1]_{10}$), θα έπρεπε (λόγω τού 2.4.19 (iv)) να ισχύει $\text{ord}(f([3]_{10})) = 4$, κάτι αδύνατον, καθόσον

$$\text{ord}([1]_8) = 1,\ \text{ord}([3]_8) = \text{ord}([5]_8) = \text{ord}([7]_8) = 2.$$

(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*, 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 2.4.19.)

(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 $\text{ord}(i) = 4$ (όπου i η φανταστική μονάδα), θα έπρεπε (λόγω τού (iv) τής προτάσεως 2.4.19) να ισχύει $\text{ord}(f(i)) = 4$, κάτι αδύνατον, καθόσον η εξίσωση $x^4 = 1$ έχει μόνον τις λύσεις ± 1 εντός τού $\mathbb{R}$ (με $\text{ord}(1) = 1$, $\text{ord}(-1) = 2$ στην $(\mathbb{R}\setminus\{0\}, \cdot)$).

2.4.21 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* $G_2 \cong G_3] \Rightarrow G_1 \cong G_3$.

ΑΠΟΔΕΙΞΗ. (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 αμφιριπτική απεικόνιση, διαθέτει μια (μονοσημάντως ορισμένη, αμφιρριπτική) αντίστροφο f^{-1}. Αρκεί λοιπόν να αποδειχθεί ότι η f^{-1} αποτελεί ομομορφισμό 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 2.4.12, *και* η σύνθεσή τους $g \circ f$ είναι ένας ισομορφισμός ομάδων. □

2.4.22 Σημείωση. Σύμφωνα με την πρόταση 2.4.21, 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* [41].

► **Ταξινόμηση των κυκλικών ομάδων και των υποομάδων αυτών**. Το ακόλουθο θεώρημα μας παρέχει τη δυνατότητα πλήρους *ταξινομήσεως* των κυκλικών ομάδων *μέχρις ισομορφισμού*.

2.4.23 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 $(G, \cdot) \cong (\mathbb{Z}_m, +)$.*

ΑΠΟΔΕΙΞΗ. 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

$$(\mathbb{Z}, +) \longrightarrow (G, \cdot), \quad n \longmapsto g^n,$$

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 2.2.18), κάτι που θα αντέφασκε προς την υπόθεσή μας. Επιπροσθέτως, η εν λόγω απεικόνιση είναι και *ομομορφισμός ομάδων*, διότι (σύμφωνα με το 2.1.11 (i)) έχουμε

$$g^{n+n'} = g^n g^{n'}, \ \forall (n, n') \in \mathbb{Z} \times \mathbb{Z}.$$

[41] Η φράση «ταξινόμηση μέχρις ισομορφισμού» ή «με ακρίβεια ισομορφισμού» (up to isomorphism) δηλοί τη «διάκριση (ομάδων) με μόνο κριτήριο ταυτίσεως τη διαμεσολάβηση κάποιου ισομορφισμού».

(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

$$n,n'\in\{0,1,...,m-1\}:[n]_m=[n']_m\,,$$

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. 2.1.11 (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 2.4.15). □

2.4.24 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 2.4.23) ισόμορφη με την $(\{[0]_1\},+)$. Κατ' αυτόν τον τρόπο ταξινομούνται *ομαδοθεωρητικώς όλες οι ομάδες τάξεως* 1 (πρβλ. σημείωση 2.4.22). 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 2.1.21 (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).

2.4.25 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* 2.4.23 (i) *και* 2.2.19 (i), *οι υποομάδες της είναι ακριβώς οι κυκλικές ομάδες*[42]

[42]Σημειωτέον ότι η $\mathbb{N}_0\ni d\longmapsto\left\langle g^d\right\rangle$ είναι μια *αμφίρριψη*. (Πράγματι· εάν $d\neq d'$, τότε $\left\langle g^d\right\rangle\neq\left\langle g^{d'}\right\rangle$, απ' όπου έπεται η ενριπτικότητά της, διότι από την ισότητα $\left\langle g^d\right\rangle=\left\langle g^{d'}\right\rangle$ θα καταλήγαμε στο ότι η G είναι πεπερασμένη, πράγμα άτοπο. Η επιρριπτικότητα είναι σαφής επί τη βάσει των προηγηθέντων επιχειρημάτων. Βλ. απόδειξη τής προτάσεως 2.2.18.)

$\langle g^d \rangle$, *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* 2.3.23.

Κάνοντας χρήση τού θεωρήματος 2.4.23, σε συνδυασμό με το θεώρημα αντιστοιχίσεως υποομάδων 2.4.7, 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 2.4.25 ισχυροποιείται ως ακολούθως:

2.4.26 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* $(\mathbf{Subg}(\mathbb{Z}), \sqsupseteq)$ (*ήτοι τον ανάστροφο σύνδεσμο τού* $(\mathbf{Subg}(\mathbb{Z}), \sqsubseteq)$, βλ. 2.1.26, A.2.23 (iv), και A.2.26). *Η δεύτερη καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων* $(\mathbf{Subg}(\mathbb{Z}), \sqsupseteq)$ *και* $(\mathbf{Subg}(G), \sqsupseteq)$, *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. B.2.34), *και* $G = \langle g \rangle$, *για κάποιο* $g \in G$, *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 $(\mathfrak{D}_m, |)$ *και* $(\mathbf{Subg}(\mathbb{Z}_m), \sqsubseteq)$. *Η δεύτερη καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων* $(\mathbf{Subg}(\mathbb{Z}_m), \sqsubseteq)$ *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* $m \geq 2$ *και* $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *είναι η κανονική παράσταση* (B.19) *τού* m *ως γινομένου πρώτων αριθμών, τότε η* G *διαθέτει* k *ελαχιστικές και* k *μεγιστικές υποομάδες. Συγκεκριμένα,*

$$\mathbf{Min\text{-}Subg}(G) = \left\{ \left\langle g^{(p_1^{\alpha_1 - 1} p_2^{\alpha_2} \cdots p_k^{\alpha_k})} \right\rangle, \left\langle g^{(p_1^{\alpha_1} p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k})} \right\rangle, ..., \left\langle g^{(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k - 1})} \right\rangle \right\}$$

και $\mathbf{Max\text{-}Subg}(G) = \{\langle g^{p_1} \rangle, \langle g^{p_2} \rangle, ..., \langle g^{p_k} \rangle\}$.

ΑΠΟΔΕΙΞΗ. (i) Το ότι η πρώτη απεικόνιση είναι αμφίρριψη και ότι καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων $(\mathbb{N}_0, |)$ και $(\mathbf{Subg}(\mathbb{Z}), \sqsupseteq)$ έπεται από το (i) τής

προτάσεως 2.2.19 και το (i) τού πορίσματος 2.2.20. Το ότι η δεύτερη απεικόνιση είναι αμφίρριψη και ότι καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων

$$(\mathbf{Subg}(\mathbb{Z}), \sqsupseteq) \quad \text{και} \quad (\mathbf{Subg}(G), \sqsupseteq),$$

(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 θεωρήματος αντιστοιχίσεως υποομάδων 2.4.7 για τον ισομορφισμό

$$(\mathbb{Z}, +) \longrightarrow (G, \cdot), \;\; n \longmapsto g^n,$$

τον θεσπισθέντα στο (i) τού θεωρήματος 2.4.23. 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 4.1.34, 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 $d \in \mathbb{N}$, $d \geq 2$, και $d \mid p$. (Βλ. 2.2.19 (i) και 2.2.20 (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 $m \in \mathbb{N}$, $m \geq 2$ (βλ. 2.2.19 (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. Β.3.2 και 2.2.20 (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[43] 2.3.21 και το πόρισμα 2.3.23 (πρβλ. 2.3.14). 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 θεωρήματος αντιστοιχίσεως υποομάδων 2.4.7 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 2.4.23. Επιπροσθέτως, εάν $m \geq 2$ και $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ είναι η κανονική παράσταση (Β.19) τού m ως γινομένου πρώτων αριθμών (με $\alpha_1, ..., \alpha_k \in \mathbb{N}$), τότε οι φυσικοί αριθμοί

$$p_1^{\alpha_1 - 1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \; p_1^{\alpha_1} p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k}, \; ..., \; p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k - 1}$$

[43] Σημειωτέον ότι για οιουσδήποτε $d_1, d_2 \in \mathfrak{D}_m$ έχουμε $d_1 \mid d_2 \Leftrightarrow \frac{m}{d_2} \mid \frac{m}{d_1} \Leftrightarrow \left\langle \left[\frac{m}{d_1}\right]_m \right\rangle \sqsubseteq \left\langle \left[\frac{m}{d_2}\right]_m \right\rangle$.

αποτελούν τα *μεγιστικά στοιχεία* τού $(\mathfrak{D}_m \setminus \{m\}, |)$ και οι πρώτοι αριθμοί $p_1, p_2, ..., p_k$ τα *ελαχιστικά στοιχεία* τού $(\mathfrak{D}_m \setminus \{1\}, |)$ (βλ. Α.2.10 και Β.3.14), 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 $\mathbf{Max\text{-}Subg}(\mathbb{Z}_m) = \{ \langle [p_1]_m \rangle, \langle [p_2]_m \rangle, ..., \langle [p_k]_m \rangle \}$. □

2.4.27 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

$$\mathbb{Z}_{12} = \{ [0]_{12}, [1]_{12}, [2]_{12}, [3]_{12}, [4]_{12}, [5]_{12}, [6]_{12}, [7]_{12}, [8]_{12}, [9]_{12}, [10]_{12}, [11]_{12} \}$$

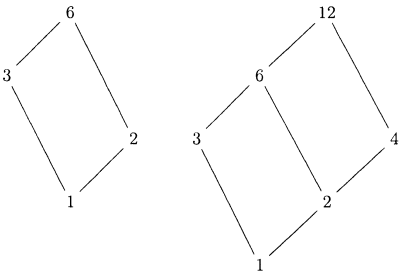
είναι η τετριμμένη $\{[0]_{12}\}$, ολόκληρη η $\mathbb{Z}_{12}$, καθώς και οι

$$\langle [6]_{12} \rangle = \{ [0]_{12}, [6]_{12} \},$$
$$\langle [4]_{12} \rangle = \{ [0]_{12}, [4]_{12}, [8]_{12} \},$$
$$\langle [3]_{12} \rangle = \{ [0]_{12}, [3]_{12}, [6]_{12}, [9]_{12} \},$$
$$\langle [2]_{12} \rangle = \{ [0]_{12}, [2]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12} \}.$$

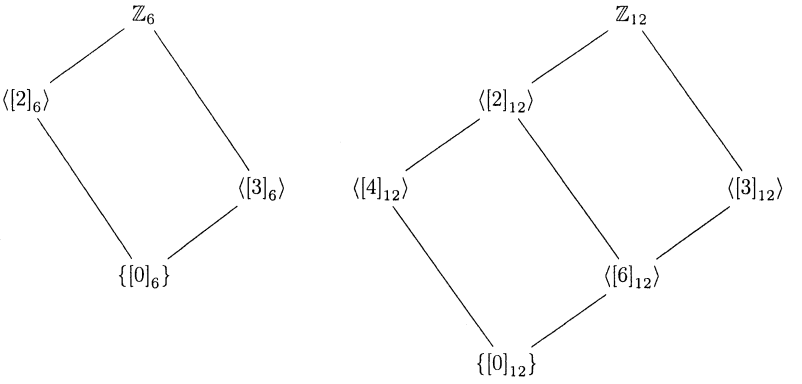
Η αμφίρριψη $\mathfrak{D}_{12} \longrightarrow \mathbf{Subg}(\mathbb{Z}_{12})$ είναι η εξής:

$$1 \longmapsto \langle [0]_{12} \rangle, \quad 2 \longmapsto \langle [6]_{12} \rangle, \quad 3 \longmapsto \langle [4]_{12} \rangle,$$
$$4 \longmapsto \langle [3]_{12} \rangle, \quad 6 \longmapsto \langle [2]_{12} \rangle, \quad 12 \longmapsto \mathbb{Z}_{12}.$$

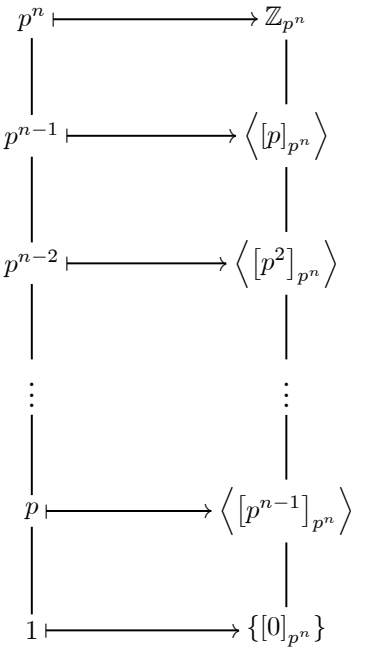
Τα διαγράμματα τού Hasse για τους συνδέσμους των διαιρετών στα (i) και (ii) είναι τα



ενώ τα αντίστοιχα διαγράμματα για τους συνδέσμους των υποομάδων είναι τα



2.4.28 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 $\mathrm{Aut}(G)$).

2.4.29 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 2.4.12 και 2.4.21. (Το ουδέτερο στοιχείο αυτών είναι η ταυτοτική απεικόνιση id_G.) □

2.4.30 Σημείωση. (i) Προφανώς, $\mathrm{End}(G)^\times = \mathrm{Aut}(G)$. (Βλ. 2.1.5.)

(ii) Όταν η ομάδα G είναι *αβελιανή*, η τριάδα $(\mathrm{End}(G), +, \circ)$, (όπου "$+$" η πράξη η εισαχθείσα στο εδάφιο 2.4.13 (ii)) καθίσταται *δακτύλιος με μοναδιαίο στοιχείο*.

2.4.31 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. 2.4.9 (i)). □

Για ορισμένες ειδικές ομάδες $(G, \cdot)$ είναι δυνατός ένας λεπτομερής χαρακτηρισμός τής $(\mathrm{Aut}(G), \circ)$. Επί παραδείγματι, τα θεωρήματα 2.4.32 και 2.4.33 μας παρέχουν την ταξινόμηση των ομάδων αυτομορφισμών των κυκλικών ομάδων και τής (αβελιανής, μη κυκλικής) ομάδας $(\mathbb{Q}, +)$, αντιστοίχως, *μέχρις ισομορφισμού* [44].

2.4.32 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. 2.1.7 (iii)).

ΑΠΟΔΕΙΞΗ. (i) Έστω G μια άπειρη κυκλική ομάδα και έστω g κάποιος γεννήτοράς της. Από το (i) τού θεωρήματος 2.4.23 γνωρίζουμε ότι η απεικόνιση

$$\lambda : (\mathbb{Z}, +) \longrightarrow (G, \cdot), \quad n \longmapsto \lambda(g) := g^n,$$

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·

$$\vartheta(n) = \begin{cases} \vartheta(\underbrace{1 + \cdots + 1}_{n \text{ φορές}}) = \underbrace{\vartheta(1) + \cdots + \vartheta(1)}_{n \text{ φορές}} = n \cdot \vartheta(1), & \text{όταν } n > 0, \\ \vartheta(0) = 0 \cdot \vartheta(1), & \text{όταν } n = 0, \\ \vartheta(\underbrace{(-1) + \cdots + (-1)}_{-n \text{ φορές}}) = (-n) \cdot \vartheta(-1) = n \cdot \vartheta(1), & \text{όταν } n < 0. \end{cases}$$

[44] Σημειωτέον ότι, συν τοις άλλοις, κατά την αποδεικτική πορεία των θεωρημάτων 2.4.32 και 2.4.33 *περιγράφονται διεξοδικώς* οι εν λόγω αυτομορφισμοί.

Κατά συνέπειαν[45], $\mathrm{End}(\mathbb{Z}) = \{\,\vartheta_\kappa \mid \kappa \in \mathbb{Z}\}$, όπου

$$\vartheta_\kappa : \mathbb{Z} \longrightarrow \mathbb{Z},\ n \longmapsto \vartheta_\kappa(n) := \kappa n.$$

Σημειωτέον ότι οι ϑ_κ είναι ενριπτικές για κάθε $\kappa \in \mathbb{Z}\setminus\{0\}$. Έστω $\kappa \in \mathbb{Z}\setminus\{0\}$, 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 (2.9) και 2.4.19 (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 2.4.9. Λαμβάνοντας υπ' όψιν το πόρισμα 2.3.17 συμπεραίνουμε ότι

$$\langle g\rangle = G = \left\langle g^k\right\rangle \Longrightarrow \text{μκδ}(k,m) = 1,$$

οπότε υφίστανται το πολύ $\phi(m)$ αυτομορφισμοί τής G, όπου ϕ η συνάρτηση τού Euler (βλ. (2.1)). Άρα

$$|\mathrm{Aut}(G)| \leq \phi(m) = \left|\mathbb{Z}_m^\times\right|. \tag{2.14}$$

Από τη άλλη μεριά, *για κάθε* $k \in \mathbb{N}$ *με* $k \leq m$ *και* $\text{μκδ}(k,m) = 1$ 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 2.2.17 και παρατήρηση 2.1.12). Επειδή $G = \left\langle g^k\right\rangle$ (και πάλι λόγω τού πορίσματος 2.3.17) έχουμε

$$G = \left\langle g^k\right\rangle = \left\{ \left(g^k\right)^l \;\middle|\; l \in \mathbb{Z}\right\} = \left\{ \left(g^l\right)^k \;\middle|\; l \in \mathbb{Z}\right\} = \vartheta_k(G),$$

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

$$|\mathrm{Aut}(G)| \geq \phi(m) \underset{(2.14)}{\Longrightarrow} |\mathrm{Aut}(G)| = \phi(m)$$

[45] Εν προκειμένω, ως δακτύλιος (βλ. 2.4.30 (ii)), ο $\mathrm{End}(\mathbb{Z})$ είναι ισόμορφος τού δακτυλίου των ακεραίων αριθμών.

$$\Longrightarrow \mathrm{Aut}(G) = \{\, \vartheta_k \mid k \in \mathbb{N} \text{ με } k \leq m \text{ και } \mu\kappa\delta(k,m) = 1\}.$$

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 επιριπτική. Επειδή κάθε επιριπτική απεικόνιση από ένα πεπερασμένο σύνολο επί ενός συνόλου που έχει τον ίδιο πληθικό αριθμό είναι κατ' ανάγκην ενριπτική (και, ως εκ τούτου, αμφιριπτική), συνάγεται τελικώς η f είναι ένας ισομορφισμός ομάδων. □

2.4.33 Θεώρημα. (Ομάδα αυτομορφισμών τής $(\mathbb{Q},+)$) *Η ομάδα* $(\mathrm{Aut}(\mathbb{Q}),\circ)$ *των αυτομορφισμών τής* $(\mathbb{Q},+)$ *είναι ισόμορφη με την (πολλαπλασιαστική) ομάδα* $(\mathbb{Q}\smallsetminus\{0\},\cdot)$.

ΑΠΟΔΕΙΞΗ. 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[46], $\mathrm{End}(\mathbb{Q}) = \{\, \vartheta_\ell \mid \ell \in \mathbb{Q}\}$, 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. □

[46] Ως δακτύλιος (βλ. 2.4.30 (ii)) ο $\mathrm{End}(\mathbb{Q})$ είναι ισόμορφος τού σώματος των ρητών αριθμών.

2.4.34 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[47] $|\mathrm{Aut}(G)| \leq (|G|-1)!$). Αντιθέτως, εάν η G είναι άπειρη ομάδα, τότε άλλοτε η ομάδα αυτομορφισμών της είναι άπειρη (όπως, π.χ., είδαμε στο θεώρημα 2.4.33 για την ομάδα των αυτομορφισμών τής $(\mathbb{Q},+)$) και άλλοτε πεπερασμένη[48] (όπως, π.χ., είδαμε στα 2.4.23 (i) και 2.4.32 (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. 2.3.1 (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 $|G|<\infty$ (βλ. πόρισμα 9.3.10), ενώ μπορεί να είναι αβελιανή μόνον σε ειδικές περιπτώσεις[49] όταν $|G|=\infty$. Επίσης, δεν υπάρχει καμία άπειρη μη αβελιανή 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 (πρβλ. 5.4.37 (ii)).

(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[50]. Όταν η H είναι πεπερασμένη, τότε υφίστανται μόνον *πεπερασμένου πλήθους* (μη ισόμορφες)

---

[47] 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 3.1.1 και 3.1.3.) Επειδή $\vartheta(e_G)=e_G$, για κάθε $\vartheta\in\mathrm{Aut}(G)$, έχουμε $|\mathrm{Aut}(G)|\leq(|G|-1)!$.

[48] 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.

[49] 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.

[50] 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.

πεπερασμένες ομάδες G με[51] $\mathrm{Aut}(G) \cong H$. Τούτο παύει να ισχύει όταν στην G επιτραπεί να είναι άπειρη: Π.χ., ο D.J.S. Robinson[52] έχει κατασκευάσει για τη συμμετρική ομάδα $H = \mathfrak{S}_4$ (τάξεως 24, βλ. 3.1.3) 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) $G_1 \ncong G_2$. (Επί παραδείγματι, το $(\mathbf{V}, \mathfrak{S}_3)$ αποτελεί ένα τέτοιου είδους ζεύγος. Βλ. εδάφια 3.5.6, 3.5.8 (ii) και 5.4.32 (ii).)

(v) Υπάρχουν *γνήσιες* υποομάδες H πεπερασμένων ομάδων G, τέτοιες ώστε να ισχύει $|\mathrm{Aut}(H)| > |\mathrm{Aut}(G)|$. (Βλ. άσκηση ??).

(vi) Τέλος, είναι αξιοπρόσεκτο το ότι υπάρχουν και κάποιες ειδικές ομάδες G για τις οποίες ισχύει $|\mathrm{Aut}(G)| = |G|$ (βλ., π.χ., πόρισμα 9.3.3, στην περίπτωση όπου η G είναι πεπερασμένη αβελιανή) ή ακόμη και $\mathrm{Aut}(G) \cong G$. (Για τη συμμετρική ομάδα $\mathfrak{S}_n$, $n \geq 3$, $n \neq 6$, και τις διεδρικές ομάδες $\mathbf{D}_3, \mathbf{D}_4$ και $\mathbf{D}_6$ που έχουν αυτήν την ιδιότητα, βλ. εδάφια 6.3.6 και 7.6.36.)

Ασκήσεις

2-1. Έστω $(G, \cdot)$ μια ημιομάδα. Να αποδειχθούν τα ακόλουθα:

(i) Η $(G, \cdot)$ είναι ομάδα εάν και μόνον εάν για οιαδήποτε στοιχεία $a, b \in G$ οι «εξισώσεις» $ax = b$ και $ya = b$ είναι επιλύσιμες (ως προς x και y).

(ii) Εάν για κάθε $g \in G$ υπάρχει μοναδικό στοιχείο $\widetilde{g} \in G$ με $g\widetilde{g}g = g$, τότε η $(G, \cdot)$ είναι ομάδα.

2-2. Έστω m ένας φυσικός αριθμός και $E := \{0, 1, ..., m-1\}$. Επί τού E ορίζεται η εσωτερική πράξη:

$$a * b := \begin{cases} a+b, & \text{όταν } a+b < m, \\ r, & \text{όταν } a+b = m+r, \ \ 0 \leq r < m. \end{cases}$$

για κάθε $a, b \in E$. Να δειχθεί ότι το ζεύγος $(E, *)$ αποτελεί ομάδα τάξεως m.

2-3. Έστω $H := \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$. Επί τού H ορίζεται η εσωτερική πράξη:

$$(\alpha, \beta, \gamma) * (\xi, \eta, \zeta) := \left(\alpha + (-1)^{\beta}\, \xi, \beta + (-1)^{\gamma}\, \eta, (-1)^{\xi}\, \gamma + \zeta\right).$$

Να αποδειχθεί ότι το ζεύγος $(H, *)$ αποτελεί μια μη αβελιανή ομάδα.

2-4. Έστω $(G, \cdot)$ μια ομάδα έχουσα τάξη $|G| = n \in \mathbb{N}$. Για οιαδήποτε n-άδα στοιχείων $(g_1, ..., g_n) \in G^n$ να αποδειχθεί η ύπαρξη φυσικών αριθμών k, m για τους οποίους ισχύει $1 \leq k \leq m \leq n$ και $g_k g_{k+1} \cdots g_{m-1} g_m = e_G$.

[51] Βλ. H.K. Iyer, ό.π., Thm. 3.1, σελ. 657-658.

[52] D.J.S. Robinson: *Groups with prescribed automorphism group*, Proc. Edinburgh Math. Soc. (2) **25** (1982), 217-227.

2-5. Έστω $(G,\cdot)$ μια ομάδα. Εάν $x,y\in G$ με $xy=yx$, να δειχθεί ότι

$$(xy)^n=x^ny^n,\ \forall n\in\mathbb{Z},\ \text{ και }\ x^my^n=y^nx^m,\ \forall(m,n)\in\mathbb{Z}\times\mathbb{Z}.$$

2-6. Έστω $(G,\cdot)$ μια ομάδα. Υποθέτοντας ότι
(a) $(ab)^2=(ba)^2,\forall\,(a,b)\in G\times G$, και (b) $(\forall a\in G)\left(a^2=e_G\Longrightarrow a=e_G\right)$,
να αποδειχθεί ότι ισχύουν τα ακόλουθα:
(i) $x^2=yx^2y^{-1},\ \forall\,(x,y)\in G\times G$,
(ii) $yxy^{-1}=y^{-1}xy,\ \forall\,(x,y)\in G\times G$,
(iii) η $(G,\cdot)$ είναι αβελιανή.

2-7. Έστω $(G,\cdot)$ μια ομάδα για την οποία υπάρχει κάποιος $k\in\mathbb{N}$, τέτοιος ώστε να ισχύει

$$(ab)^{k+j}=a^{k+j}b^{k+j},\ \ \forall(a,b)\in G\times G\ \text{ και }\ \forall j\in\{0,1,2\}.$$

Να αποδειχθεί ότι η εν λόγω ομάδα είναι αβελιανή.

2-8. Έστω $(G,\cdot)$ μια ομάδα. Για κάθε $n\in\mathbb{Z}$ να αποδειχθεί ότι

$$\left(aba^{-1}\right)^n=ab^na^{-1},\quad\forall\,(a,b)\in G\times G.$$

2-9. Εάν $(G,\cdot)$ είναι μια ομάδα και $a,b\in G$ τέτοια, ώστε να ισχύει $b^{-1}ab=a^\nu$ για κάποιον $\nu\in\mathbb{Z}$, να αποδειχθεί ότι $b^{-m}a^nb^m=a^{n\nu^m},\ \forall\,(m,n)\in\mathbb{Z}\times\mathbb{Z}$.

2-10. Έστω $(G,\cdot)$ μια ομάδα. Εάν $x,y\in G$, να αποδειχθούν οι συνεπαγωγές
(i) $[xy^2=y^3x\ \text{ και }\ x^3y=yx^2]\Longrightarrow x=y=e_G$, και
(ii) $[x^2=e_G\ \text{ και }\ x^{-1}y^2x=y^3]\Longrightarrow y^5=e_G$.

2-11. Έστω $(G,\cdot)$ μια ομάδα. Εάν $x,y,z\in G$, να αποδειχθεί η συνεπαγωγή

$$[x^{-1}yx=y^2,\ y^{-1}zy=z^2\ \text{ και }\ z^{-1}xz=x^2]\Longrightarrow x=y=z=e_G.$$

2-12. Έστω $(G,\cdot)$ μια ομάδα. Εάν $(m,n)\in\mathbb{N}^2$ με μκδ$(m,n)=1$ είναι τέτοιοι, ώστε να ισχύει

$$a^mb^m=b^ma^m\ \text{ και }a^nb^n=b^na^n,\ \forall(a,b)\in G\times G,$$

να αποδειχθεί οτι η $(G,\cdot)$ είναι κατ' ανάγκην αβελιανή.

2-13. Έστω $(G,\cdot)$ μια ομάδα και έστω S ένα μη κενό σύνολο. Εάν η $f:S\longrightarrow G$ είναι μια αμφίρριψη, να αποδειχθεί ότι το ζεύγος $(S,\odot)$ είναι μια ομάδα όταν -εξ ορισμού- $x\odot y:=f^{-1}\left(f(x)\cdot f(y)\right),\ \forall\,(x,y)\in S\times S$.

2-14. Να εξακριβωθεί ότι τα $H:=\{\,2^n\,|\,n\in\ \mathbb{Z}\}$ και $K:=\left\{\,\frac{1+2n}{1+2m}\,\middle|\,n,m\in\ \mathbb{Z}\right\}$ αποτελούν υποομάδες τής ομάδας $(\mathbb{Q}\setminus\{0\},\cdot)$.

2-15. Έστω H μια υποομάδα τής $(\mathbb{R},+)$. Να αποδειχθεί ότι το $K := \{\, 2^x \mid x \in H\}$ είναι υποομάδα τής $(\mathbb{R}\smallsetminus\{0\},\cdot)$.

2-16. Να αποδειχθεί ότι το

$$H := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{Mat}_{2\times 2}(\mathbb{Z}) \;\middle|\; a+b+c+d=0 \right\}$$

αποτελεί μια υποομάδα τής $(\mathbf{Mat}_{2\times 2}(\mathbb{Z}),+)$.

2-17. Έστω $(G,\cdot)$ μια αβελιανή ομάδα. Να αποδειχθεί ότι τα σύνολα $H_m, m\in\mathbb{Z}$, όπου $H_m := \{\, g\in G \mid g^m = e_G\}$, είναι υποομάδες τής G.

2-18. Έστω $(G,\cdot)$ μια πεπερασμένη ομάδα. Εάν $A\subseteq G$ με $\mathrm{card}(A) > \frac{|G|}{2}$ και $g\in G$, να αποδειχθεί η ύπαρξη στοιχείων $a,b\in A$, τέτοιων ώστε να ισχύει $g=ab$.

2-19. Για καθεμιά εκ των κατωτέρω ομάδων να προσδιορισθούν δυο μη τετριμμένες γνήσιες υποομάδες:

(i) $(\mathbb{Z},+)$, (ii) $(\mathbb{Q},+)$, (iii) $(\mathbb{C}\smallsetminus\{0\},\cdot)$,
(iv) $(10\mathbb{Z},+)$, (v) $(\mathbb{Z}_{11}^{\times},\cdot)$, (vi) $(\mathbf{GL}_2(\mathbb{Q}),\cdot)$.

2-20. Να αποδειχθεί ότι μια ομάδα είναι πεπερασμένη εάν και μόνον εάν διαθέτει πεπερασμένου πλήθους υποομάδες. (Ισοδυνάμως, μια ομάδα είναι άπειρη εάν και μόνον εάν το σύνολο των υποομάδων της είναι άπειρο.)

2-21. Έστω $(G,\cdot)$ μια ομάδα. Να αποδειχθεί ότι $\mathrm{card}(\mathbf{Subg}(G)) = 3 \Leftrightarrow$ η G είναι κυκλική τάξεως p^2, όπου p κάποιος πρώτος αριθμός.

2-22. Να σχεδιασθούν τα διαγράμματα τού Hasse για τους συνδέσμους υποομάδων $(\mathbf{Subg}(\mathbb{Z}_{36}),\sqsubseteq)$ και $(\mathbf{Subg}(\mathbb{Z}_{pq}),\sqsubseteq)$, όπου p,q είναι δυο πρώτοι αριθμοί.

2-23. Να αποδειχθεί ότι η $(\mathbb{Z}_{11}^{\times},\cdot)$ είναι κυκλική και να σχεδιασθεί το διάγραμμα τού Hasse για τον σύνδεσμο $(\mathbf{Subg}(\mathbb{Z}_{11}^{\times}),\sqsubseteq)$.

2-24. Να αποδειχθεί ότι για κάθε $m\in\mathbb{N}$ το

$$H_m := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) \;\middle|\; a\equiv d\equiv 1 (\mathrm{mod}\, m) \text{ και } b\equiv c\equiv 0 (\mathrm{mod}\, m) \right\}$$

αποτελεί μια υποομάδα τής $\mathrm{SL}_2(\mathbb{Z})$. Εν συνεχεία, να σχεδιασθεί το διάγραμμα τού Hasse για το μερικώς διατεταγμένο σύνολο $(X,\sqsubseteq)$, όπου

$$\mathfrak{X} := \{\, H_m \mid 2\le m\le 12\} \subsetneqq \mathbf{Subg}(\mathrm{SL}_2(\mathbb{Z})).$$

2-25. Έστω $(G,\cdot)$ μια ομάδα. Να αποδειχθούν τα εξής:

(i) Εάν $H\sqsubset G$ και $K\sqsubset G$, τότε $\exists g\in G$ με $g\notin H$ και $g\notin K$.

(ii) Εάν $H\sqsubset G$, τότε $\langle G\smallsetminus H\rangle = G$ και $\langle H\smallsetminus\{e_G\}\rangle = H$.

2-26. Οι γεννήτορες τής κυκλικής ομάδας $(\mathcal{E}_n, \cdot)$, $n \in \mathbb{N}$, των n-οστών ριζών τής μονάδας καλούνται **πρωταρχικές n-οστές ρίζες τής μονάδας**. Να δειχθεί ότι το σύνολο των πρωταρχικών n-οστών ριζών τής μονάδας είναι το $\left\{ \zeta_n^k \middle| \, 1 \leq k \leq n \text{ και } \mu\kappa\delta(k,n) = 1 \right\}$.

2-27. Να αποδειχθεί ότι κάθε άπειρη κυκλική ομάδα διαθέτει *ακριβώς δύο* γεννήτορες.

2-28. Εάν $\{H_j\}_{j\in J}$ είναι μια οικογένεια υποομάδων μιας ομάδας $(G, \cdot)$, όπου το

$$J = \{j_1, ..., j_n, j_{n+1}, ...\} \subseteq \mathbb{N}_0$$

είναι ένα αριθμήσιμο σύνολο δεικτών και ισχύει $H_{j_k} \subseteq H_{j_{k+1}}$ για κάθε $k \in \mathbb{N}$, να αποδειχθεί

(i) ότι η ένωση $\bigcup_{k\in\mathbb{N}} H_{j_k}$ αποτελεί μια υποομάδα τής G και

(ii) ότι εάν η H_{j_k} είναι αβελιανή για κάθε $k \in \mathbb{N}$, τότε και η $\bigcup_{k\in\mathbb{N}} H_{j_k}$ είναι ωσαύτως αβελιανή.

2-29. Για την ομάδα $(\mathbb{Q}, +)$ να αποδειχθούν τα ακόλουθα:

(i) Κάθε πεπερασμένως παραγόμενη υποομάδα τής $(\mathbb{Q}, +)$ είναι γνήσια και κυκλική.

(ii) $\mathbb{Q} = \bigcup_{n\in\mathbb{N}} \left\langle \frac{1}{n!} \right\rangle$.

(iii) $\mathbf{Max\text{-}Subg}(\mathbb{Q}) = \varnothing = \mathbf{Min\text{-}Subg}(\mathbb{Q})$.

2-30. Εάν $\{H_j\}_{j\in\mathbb{N}}$ είναι μια ακολουθία γνησίων υποομάδων μιας ομάδας $(G, \cdot)$, για την οποία ισχύει $H_j \subseteq H_{j+1}$ για κάθε $j \in \mathbb{N}$ και $G = \bigcup_{j\in\mathbb{N}} H_j$, να αποδειχθεί ότι η $(G, \cdot)$ δεν είναι πεπερασμένως παραγόμενη.

2-31. Έστω $G := \langle f_1, f_2 \rangle$ η υποομάδα τής ομάδας $(\mathbf{Bij}(\mathbb{R}, \mathbb{R}), \circ)$ (των αμφιρρίψεων από το $\mathbb{R}$ επί τού $\mathbb{R}$ ως προς την πράξη τής συνθέσεως) η παραγόμενη από τις αμφιρρίψεις

$$\mathbb{R} \ni x \longmapsto f_1(x) := x + 1 \in \mathbb{R} \text{ και } \mathbb{R} \ni x \longmapsto f_2(x) := 2x \in \mathbb{R}.$$

Να αποδειχθεί η ύπαρξη μιας γνήσιας μη πεπερασμένως παραγόμενης υποομάδας H τής G. [*Υπόδειξη*: Αρκεί για κάθε $j \in \mathbb{N}$ να θεωρηθεί η κυκλική υποομάδα $H_j := \langle \sigma_j \rangle$ η παραγόμενη από την αμφίρριψη

$$\sigma_j := f_2^{-j} \circ f_1 \circ f_2^j \text{ με τύπο } \mathbb{R} \ni x \longmapsto \sigma_j(x) := x + 2^{-j} \in \mathbb{R},$$

να τεθεί $H := \bigcup_{j\in\mathbb{N}} H_j$, να αποδειχθεί ότι $H_j \sqsubset H_{j+1}$ για κάθε $j \in \mathbb{N}$ και να εφαρμοσθεί καταλλήλως η άσκηση **2-30**.]

2-32. Να προσδιορισθεί η τάξη τού στοιχείου g τής ομάδας $(G,*)$ στις 10 περιπτώσεις τις παρατιθέμενες στον κάτωθι κατάλογο:

A/A	$(G,*)$	g	A/A	$(G,*)$	g
(i)	$(\mathbb{C}\setminus\{0\},\cdot)$	$-i$	(vi)	$(\mathbb{Z}_{18},+)$	$[2]_{18}$
(ii)	$(\mathbb{C}\setminus\{0\},\cdot)$	$-1+i\sqrt{3}$	(vii)	$(\mathbb{Z}_{150},+)$	$[55]_{150}$
(iii)	$(\mathbb{C}\setminus\{0\},\cdot)$	$\frac{-1+i\sqrt{3}}{2}$	(viii)	$(\mathbb{Z}_{150},+)$	$[60]_{150}$
(iv)	$(\mathbb{C}\setminus\{0\},\cdot)$	$\exp(\frac{2\pi i}{11})$	(ix)	$(\mathbb{Z}_{23}^{\times},\cdot)$	$[2]_{23}$
(v)	$(\mathbb{C}\setminus\{0\},\cdot)$	$\exp(\frac{\pi i}{12})$	(x)	$(\mathbb{Z}_{21}^{\times},\cdot)$	$[4]_{21}$

2-33. Επί τού συνόλου $G := (\mathbb{R}\setminus\{0\})\times\mathbb{R}$ ορίζεται η εσωτερική πράξη:

$$G\times G\ni((a,b),(c,d))\longmapsto(a,b)\boxdot(c,d):=(ac,bc+d)\in G.$$

(i) Να αποδειχθεί ότι το ζεύγος $(G,\boxdot)$ είναι μια μη αβελιανή ομάδα.

(ii) Ποια εκ των κάτωθι υποσυνόλων αποτελούν υποομάδες αυτής;

$$H_1:=\{(a,k(a-1))|\,a\neq0\},\qquad H_2:=\{(a,0)|\,a>0\},$$
$$H_3:=\{(a,na^n)|\,a\neq0\},\qquad H_4:=\{(1,b))|\,b\in\mathbb{R}\}.$$

(Εν προκειμένω, οι $k\in\mathbb{R}$ και $n\in\mathbb{N}_0$ είναι παγιωμένοι.)

(iii) Να αποδειχθεί ότι το σύνολο των στοιχείων τής $(G,\boxdot)$ που έχουν τάξη 2 είναι άπειρο.

(iv) Διαθέτει η $(G,\boxdot)$ στοιχεία τάξεως 3;

2-34. Έστω $(G,\cdot)$ μια ομάδα τάξεως $2n$, για κάποιον $n\in\mathbb{N}$. Να αποδειχθεί ότι

(i) $\exists m\in\mathbb{N}:\text{card}\big(\{x\in G\mid x^{-1}=x\}\big)=2m$,

(ii) $\exists a\in G:\text{ord}(a)=2$.

2-35. Εάν $(G,\cdot)$ είναι μια αβελιανή ομάδα και $(x,y)\in G\times G$ με $x^n=y^n$ για κάποιον $n\in\mathbb{N}$, να αποδειχθεί ότι $y=xw$ για κάποιο $w\in G$ με $\text{ord}(w)\mid n$.

2-36. Εάν $(G,\cdot)$ είναι μια ομάδα, $(x,y)\in G\times G$ με $xy=yx$ και

$$\text{ord}\,(x)=m\in\mathbb{N},\ \ \text{ord}\,(y)=n\in\mathbb{N},$$

να αποδειχθούν τα ακόλουθα:

(i) Η τάξη $\text{ord}(xy)$ τού xy είναι πεπερασμένη,

$$\frac{\text{εκπ}\,(m,n)}{\text{μκδ}\,(m,n)} \mid \text{ord}\,(xy) \quad \text{και} \quad \text{ord}\,(xy) \mid \text{εκπ}\,(m,n)\,.$$

(ii) Ειδικότερα, $\text{μκδ}(m,n) = 1 \Longleftrightarrow \text{ord}(xy) = mn$.

(iii) Εάν για κάθε πρώτο αριθμό p που διαιρεί το γινόμενο mn, η μέγιστη δύναμη τού p που διαιρεί τον m δεν ισούται με τη μέγιστη δύναμη τού p που διαιρεί τον n, τότε

$$\text{ord}\,(xy) = \text{εκπ}\,(m,n)\,.$$

Εν συνεχεία, να δοθεί παράδειγμα ζεύγους στοιχείων x, y πεπερασμένης τάξεως μιας ομάδας $(G,*)$ με $x*y = y*x \neq e_G$ και

$$\text{ord}(x*y) < \text{εκπ}(\text{ord}(x), \text{ord}(y)).$$

2-37. Εντός τής $\text{SL}_2(\mathbb{Z})$ να υπολογισθούν οι τάξεις των στοιχείων

$$\mathbf{A} := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ \mathbf{B} := \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \text{ και } \mathbf{AB} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Εν συνεχεία, να αποδειχθεί ότι $\text{SL}_2(\mathbb{Z}) = \langle \mathbf{A}, \mathbf{AB} \rangle$.

2-38. Έστω τυχών $n \in \mathbb{N}$, $n \geq 3$. Εντός τής $\text{GL}_2(\mathbb{Z}_n)$ να υπολογισθούν οι τάξεις των

$$\mathbf{A} := \begin{pmatrix} [-1]_n & [1]_n \\ [0]_n & [1]_n \end{pmatrix},\ \mathbf{B} := \begin{pmatrix} [-1]_n & [0]_n \\ [0]_n & [1]_n \end{pmatrix} \text{ και } \mathbf{AB} = \begin{pmatrix} [1]_n & [1]_n \\ [0]_n & [1]_n \end{pmatrix}.$$

2-39. Εάν $(G,\cdot)$ είναι μια αβελιανή ομάδα και $(g,h) \in G \times G$ με

$$\text{ord}\,(g) = m \in \mathbb{N},\ \ \text{ord}\,(h) = n \in \mathbb{N},$$

να αποδειχθούν τα εξής:

(i) $\exists a \in G : \text{ord}(a) = \text{εκπ}(m,n)$.

(ii) Εάν $\text{ord}(x) \leq m, \forall x \in G \setminus \{g\}$, τότε $\text{ord}\,(y) | \, m$ και $y^m = e_G, \forall y \in G$.

2-40. Να αποδειχθεί ότι το $H := \{\exp(\pi i r) | \, r \in \mathbb{Q}\}$ αποτελεί μια άπειρη, περιοδική υποομάδα τής $(\mathbb{C} \setminus \{0\}, \cdot)$, καθώς και ότι για οιονδήποτε $n \in \mathbb{N}$ η H διαθέτει κάποιο στοιχείο, η τάξη τού οποίου ισούται με n.

2-41. Έστω $(R,+,\cdot)$ ένας μη τετριμμένος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και έστω

$$\mathbf{Heis}(R) := \left\{ \begin{pmatrix} 1_R & a & c \\ 0_R & 1_R & b \\ 0_R & 0_R & 1_R \end{pmatrix} \middle| \, a,b,c \in R \right\}$$

η ομάδα τού Heisenberg υπεράνω αυτού. (Βλ. εδ. D.2.24.)

(i) Να αποδειχθεί ότι $|\mathbf{Heis}(R)| = \mathrm{card}(R)^3$.

(ii) Ποιος είναι ο αντίστροφος τυχόντος πίνακα $\mathbf{A} \in \mathbf{Heis}(R)$;

(iii) Να αποδειχθεί ότι η $\mathbf{Heis}(R)$ είναι μη αβελιανή.

(iv) Όταν $R = \mathbb{Z}_2$, να υπολογισθεί η τάξη καθενός εκ των 8 στοιχείων τής ομάδας $\mathbf{Heis}(\mathbb{Z}_2)$.

(v) Όταν ο R είναι το σώμα $\mathbb{R}$ των πραγματικών αριθμών, να αποδειχθεί ότι η $\mathbf{Heis}(\mathbb{R})$ στερείται στρέψεως.

2-42. Έστω $(G, \cdot)$ μια πεπερασμένη αβελιανή ομάδα και έστω $u := \prod_{g\in G} g$ το γινόμενο όλων των στοιχείων της. Να αποδειχθεί ότι:

(i) Εάν η G διαθέτει ακριβώς ένα στοιχείο a τάξεως 2, τότε $u = a$.

(ii) Ένας φυσικός αριθμός $p \geq 2$ είναι πρώτος εάν και μόνον εάν ισχύει η ισοτιμία

$$(p-1)! \equiv -1 \pmod{p}\,.$$

Τούτο είναι γνωστό στη Στοιχειώδη Θεωρία Αριθμών ως *θεώρημα τού Wilson*. (Βλ. Β.4.52.) [*Υπόδειξη*: Να χρησιμοποιηθεί το (i) για την ομάδα $G = \mathbb{Z}_p^\times$.]

2-43. Έστω τυχών $k \in \mathbb{N}$, $k \geq 3$. Να δειχθεί ότι η ομάδα $(\mathbb{Z}_{2^k}^\times, \cdot)$ δεν είναι κυκλική. [*Υπόδειξη*: Αρκεί να δειχθεί ότι $\mathrm{ord}([2^k - 1]_{2^k}) = \mathrm{ord}([2^{k-1} + 1]_{2^k}) = 2$. Μια διαφορετική απόδειξη δίδεται αργότερα στην πρόταση 7.3.12.]

2-44. Να υπολογισθούν οι εκθέτες των ομάδων $(\mathbb{Z}_m, +)$, $m \in \mathbb{N}$, και $(\mathbf{Q}, \cdot)$.

2-45. Να εξετασθεί ποιες εκ των ακολούθων απεικονίσεων είναι ομομορφισμοί ομάδων:

(i) $f : (\mathbb{Z}_{12}, +) \longrightarrow (\mathbb{Z}_{12}, +)$, $f([n]_{12}) := [n+1]_{12}$,

(ii) $f : (G, \cdot) \longrightarrow (G, \cdot)$, $f(x) := x^3$, όπου G μια κυκλική ομάδα τάξεως 12,

(iii) $f : (\mathbb{Z}_8, +) \longrightarrow (\mathbb{Z}_2, +)$, $f([n]_8) := [n]_2$,

(iv) $f : (\mathbb{R}, +) \longrightarrow (\mathbb{C}\setminus\{0\}, \cdot)$, $f(x) := \cos(x) + i \sin x$,

(v) $f : \left(\left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \middle| n \in \mathbb{Z} \right\}, \cdot \right) \longrightarrow (\mathcal{E}_4, \cdot)$, $f \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} := i^n$.

Εν συνεχεία, να προσδιορισθούν οι πυρήνες και οι εικόνες όσων εξ αυτών είναι ομομορφισμοί.

2-46. Εάν $(G, \cdot), (H, *)$ είναι δυο πεπερασμένες κυκλικές ομάδες, g ένας γεννήτορας τής G και h ένας γεννήτορας τής H, να αποδειχθούν τα ακόλουθα:

(i) $\exists f \in \mathrm{Hom}(G, H) : f(g) = h \iff \mathrm{ord}(h) \,|\mathrm{ord}(g)$.

(ii) Εάν $\mathrm{ord}(h) \,|\mathrm{ord}(g)$, τότε υπάρχει μοναδικός $f \in \mathrm{Hom}(G, H) : f(g) = h$. Επιπροσθέτως, γι' αυτόν τον f ισχύουν οι ισότητες $f(g^k) = h^k, \forall k \in \mathbb{Z}$.

2-47. Να αποδειχθεί ότι οι προσθετικές ομάδες $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ και $(\mathbb{R}, +)$ είναι ανά δύο μη ισόμορφες.

2-48. Να αποδειχθεί ότι η ομάδα $\mathbb{Z}[i] := \{\, a+bi \mid (a,b) \in \mathbb{Z}^2\}$ των ακεραίων τού Gauss είναι ισόμορφη με την πολλαπλασιαστική ομάδα

$$G := \{\, 2^a 3^b \;\big|\; (a,b) \in \mathbb{Z}^2\}.$$

2-49. Να αποδειχθεί ότι τα σύνολα 2×2-πινάκων

$$G_1 := \left\{ \begin{pmatrix} 1-n & -n \\ n & 1+n \end{pmatrix} \middle| \, n \in \mathbb{Z} \right\} \;\text{ και }\; G_2 := \left\{ \begin{pmatrix} 1-2n & n \\ -4n & 1+2n \end{pmatrix} \middle| \, n \in \mathbb{Z} \right\}$$

αποτελούν υποκείμενα σύνολα υποομάδων τής ειδικής γραμμικής ομάδας $\mathrm{SL}_2(\mathbb{Z})$, καθώς και ότι $G_1 \cong \mathbb{Z} \cong G_2$.

2-50. Εάν $G := \left\{\, x \in \mathbb{R} \middle|\, x^2 < 1\right\}$, να αποδειχθούν τα ακόλουθα:

(i) $\frac{x+y}{1+xy} \in G,\ \forall\, (x,y) \in G \times G$.

(ii) Το ζεύγος $(G, *)$, όπου $G \times G \ni (x,y) \mapsto x * y := \frac{x+y}{1+xy}$, αποτελεί μια αβελιανή ομάδα.

(iii) Η απεικόνιση $f : (G,*) \longrightarrow (\mathbb{R}, +)\,,\ x \mapsto f(x) := \ln\left(\frac{1+x}{1-x}\right)$, είναι ισομορφισμός ομάδων.

2-51. Να αποδειχθεί ότι η προσθετική ομάδα $(\mathbb{Z}\,[\mathsf{X}]\,, +)$ τού πολυωνυμικού δακτυλίου $(\mathbb{Z}\,[\mathsf{X}]\,, +, \cdot)$ (βλ. C.1.17) είναι ισόμορφη με την πολλαπλασιαστική ομάδα $(\mathbb{Q}_{>0}, \cdot)$.

2-52. Για οιονδήποτε πραγματικό αριθμό $\theta \in \mathbb{R}$ ορίζεται ο πίνακας

$$\mathbf{A}_{[\theta]} := \begin{pmatrix} 0 & 1 & -\sin(\theta) \\ -1 & 0 & \cos(\theta) \\ -\sin(\theta) & \cos(\theta) & 0 \end{pmatrix} \in \mathrm{Mat}_{3\times 3}(\mathbb{R}).$$

Να αποδειχθούν τα ακόλουθα:

(i) $\mathbf{A}_{[\theta]}^3 = \mathbf{0}_{\mathrm{Mat}_{3\times 3}(\mathbb{R})}$.

(ii) Εάν για κάθε $x \in \mathbb{R}$ τεθεί $\mathbf{A}_{[\theta],x} := \mathbf{I}_3 + x\mathbf{A}_{[\theta]} + \frac{1}{2}x\mathbf{A}_{[\theta]}^2$, τότε το σύνολο 3×3-πινάκων $G_{[\theta]} := \{\, \mathbf{A}_{[\theta],x} \;\big|\; x \in \mathbb{R}\}$, εφοδιασμένο με την πράξη τού πολλαπλασιασμού πινάκων, αποτελεί μια αβελιανή ομάδα η οποία είναι ισόμορφη με την $(\mathbb{R}, +)$.

2-53. (i) Από το σύνολο των απεικονίσεων $f : \mathbb{R}\smallsetminus\{0,1\} \longrightarrow \mathbb{R}\smallsetminus\{0,1\}$ επιλέγονται οι ακόλουθες έξι:

$$f_1(x) := x, \qquad f_2(x) := \frac{1}{1-x}, \qquad f_3(x) := \frac{x-1}{x},$$
$$f_4(x) := \frac{1}{x}, \qquad f_5(x) := 1-x, \qquad f_6(x) := \frac{x}{x-1},$$

$\forall x \in \mathbb{R}\smallsetminus\{0,1\}$. Εάν $G_1 := \{f_1, f_2, f_3, f_4, f_5, f_6\}$, να αποδειχθεί ότι το ζεύγος $(G_1, \circ)$ αποτελεί μια μη αβελιανή ομάδα με $e_{G_1} = f_1$ και να δοθεί ο πολλαπλασιαστικός κατάλογος αυτής (όπου ως «πολλαπλασιασμός» νοείται, εν προκειμένω, η σύνθεση απεικονίσεων "$\circ$").

(ii) Να αποδειχθεί ότι το σύνολο των έξι 2×2-πινάκων

$$G_2 := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}, \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \omega^2 \\ \omega & 0 \end{pmatrix}, \begin{pmatrix} 0 & \omega \\ \omega^2 & 0 \end{pmatrix} \right\},$$

όπου $\omega \in \mathbb{C} \setminus \{1\}$, $\omega^3 = 1$ (ήτοι $\omega \in \{\zeta_3, \zeta_3^2\}$), αποτελεί τη μη αβελιανή υποομάδα τής $\mathrm{GL}_2(\mathbb{C})$ την παραγόμενη από τους πίνακες

$$\mathbf{A} := \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix} \text{ και } \mathbf{B} := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

(iii) Να αποδειχθεί ότι $G_1 \cong G_2$.

2-54. (i) Έστω $(G, \cdot)$ μια πεπερασμένη μη αβελιανή ομάδα (έχουσα το $e = e_G$ ως ουδέτερό της στοιχείο) η οποία μπορεί να παραχθεί από το σύνολο $\{s, t\}$ δύο στοιχείων της s και t. Εάν $\mathrm{ord}(s) = 4$ και αυτοί οι γεννήτορες τής $(G, \cdot)$ υπόκεινται στις σχέσεις

$$s^2 = t^2 \text{ και } st = ts^{-1},$$

να αποδειχθεί ότι $G = \{e, s, s^2, s^3, t, ts, ts^2, ts^3\}$ και $(G, \cdot) \cong (\mathbf{Q}, \cdot)$.

(ii) Να αποδειχθεί (μέσω τού (i)) ότι η υποομάδα

$$H := \left\langle \begin{pmatrix} [0]_3 & [-1]_3 \\ [1]_3 & [0]_3 \end{pmatrix}, \begin{pmatrix} [1]_3 & [1]_3 \\ [1]_3 & [-1]_3 \end{pmatrix} \right\rangle$$

τής $\mathrm{SL}_2(\mathbb{Z}_3)$ είναι ισόμορφη με την ομάδα των τετρανίων.

2-55. Εάν $(G, \cdot)$ είναι μια πεπερασμένη αβελιανή ομάδα, να αποδειχθεί ότι η ομάδα $\mathrm{Hom}(G, \mathbb{Z})$ όλων των ομομορφισμών από αυτήν στην $(\mathbb{Z}, +)$ (βλ. εδ. 2.4.13 (ii)) είναι τετριμμένη.

2-56. Να αποδειχθεί ότι για κάθε αβελιανή ομάδα $(G, *)$ υφίσταται ισομορφισμός

$$\mathrm{Hom}(\mathbb{Z}, G) \xrightarrow{\cong} G.$$

2-57. Εάν $(G, \cdot)$ είναι μια κυκλική ομάδα άπειρης τάξεως, να αποδειχθεί ότι η απεικόνιση $f : G \longrightarrow G,\ f(g) := g^2, \forall g \in G$, είναι μονομορφισμός, αλλά όχι και αυτομορφισμός.

2-58. Εάν $(G, \cdot)$ είναι μια πεπερασμένη ομάδα και η $f : G \longrightarrow G$ ένας μονομορφισμός, να αποδειχθεί ότι η f είναι κατ' ανάγκην αυτομορφισμός τής G.

2-59. Έστω $(G, \cdot)$ μια ομάδα. Να αποδειχθεί ότι η G είναι αβελιανή εάν και μόνον εάν η $f : G \longrightarrow G,\ f(g) := g^{-1},\ \forall g \in G$, είναι ένας αυτομορφισμός τής G.

2-60. Έστω $(G, \cdot)$ μια πεπερασμένη αβελιανή ομάδα. Εάν υπάρχει $\vartheta \in \mathrm{Aut}(G)$ με $\vartheta^2 = \mathrm{id}_G$ και εάν η τάξη $|G|$ αυτής τής ομάδας είναι περιττή, να αποδειχθεί ότι κάθε στοιχείο $x \in G$ γράφεται ως γινόμενο $x = yz$ δυο στοιχείων $y, z \in G$ για τα οποία ισχύει $\vartheta(y) = y$ και $\vartheta(z) = z^{-1}$.

ΚΕΦΑΛΑΙΟ 3

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.

3.1 Η ΣΥΜΜΕΤΡΙΚΗ ΟΜΑΔΑ

3.1.1 Ορισμός. (i) Έστω A ένα μη κενό σύνολο και

$$\mathfrak{S}_A := \mathbf{Bij}\,(A, A) := \left\{ \sigma : A \longrightarrow A \;\middle|\; \begin{array}{c} \sigma \text{ αμφιρριπτική απεικόνιση} \\ \text{από το } A \text{ επί τού } A \end{array} \right\}.$$

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

[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 $\mathfrak{S}_n$, $n \geq 3$, είναι μη μεταθετικές ομάδες! Εξάλλου, το ουσιαστικό *αντιμετάθεση* δεσμεύεται για την απόδοση τού όρου transposition.)

εκ των στοιχείων τού A, δηλαδή το απεικονίζει σε ένα άλλο (διαφορετικό) στοιχείο τού A. Εάν το θεωρούμενο A είναι ένα *πεπερασμένο* σύνολο και $n = \text{card}(A)$, 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,...,x_n αποτελούν μια αναδιάταξη των αριθμών $1, 2, ..., n$. 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

$$\begin{bmatrix} 1 & \cdots & n \\ \tau(\sigma(1)) & \cdots & \tau(\sigma(n)) \end{bmatrix} = \begin{bmatrix} 1 & \cdots & n \\ \tau(1) & \cdots & \tau(n) \end{bmatrix} \circ \begin{bmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{bmatrix}.$$

3.1.2 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

$$\begin{bmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(2) \\ 1 & 2 & \cdots & n \end{bmatrix}.$$

(ii) Για λόγους συντομίας, θα συμβολίζουμε το ουδέτερο στοιχείο $\text{id}_{\{1,...,n\}}$ τής $\mathfrak{S}_n$ απλώς ως id.

(iii) Όταν $n \geq 3$, η $\mathfrak{S}_n$ *δεν* είναι αβελιανή. Πράγματι· ορίζοντας τις $\sigma, \tau \in \mathfrak{S}_n$ ως ακολούθως:

$$\begin{array}{llll} \sigma(1) = 1, & \sigma(2) = 3, & \sigma(3) = 2, & \sigma(j) = j, \quad \forall j \in \{4, ..., n\}, \\ \tau(1) = 2, & \tau(2) = 1, & \tau(3) = 3, & \tau(j) = j, \quad \forall j \in \{4, ..., n\}, \end{array}$$

λαμβάνουμε $(\tau \circ \sigma)(1) = 2 \neq 3 = (\sigma \circ \tau)(1)$. Επομένως, $\tau \circ \sigma \neq \sigma \circ \tau$.

3.1.3 Πρόταση. *Η τάξη τής ομάδας $\mathfrak{S}_n$ ισούται με*

$$\boxed{|\mathfrak{S}_n| = n!}$$

ΑΠΟΔΕΙΞΗ. Με τη βοήθεια τής μαθηματικής επαγωγής θα αποδείξουμε γενικότερα τον ακόλουθο ισχυρισμό:

Ισχυρισμός: *Εάν τα* $A = \{x_1,...,x_n\}$ *και* $B = \{y_1,...,y_n\}$ *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*.

Όταν $n = 1$, ο ισχυρισμός είναι προφανής. Ας υποθέσουμε ότι για κάποιον $n > 1$ ισχύει $\text{card}(\mathbf{Bij}\,(A',B')) = (n-1)!$ για οιαδήποτε σύνολα A', B' που διαθέτουν (ακριβώς) $n-1$ στοιχεία. Έστω τώρα ότι τα $A = \{x_1,...,x_n\}$ και $B = \{y_1,...,y_n\}$ είναι δυο σύνολα που περιέχουν (ακριβώς) n στοιχεία. Για κάθε $j \in \{1,...,n\}$ ορίζουμε το $\mathbf{Bij}\,(A,B)_j := \{f \in \mathbf{Bij}\,(A,B) \mid f(x_1) = y_j\}$. 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 $|\mathfrak{S}_n| = n!$. □

3.1.4 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 $j, k \in \{1,...,n\}$ ισχύουν (ταυτοχρόνως) οι συνεπαγωγές

$$\sigma(j) \neq j \Rightarrow \tau(j) = j \quad \text{και} \quad \tau(k) \neq k \Rightarrow \sigma(k) = k.$$

3.1.5 Πρόταση. *Δυο μετατάξεις* $\sigma, \tau \in \mathfrak{S}_n$ *είναι ξένες μεταξύ τους εάν και μόνον εάν* $\text{supp}(\sigma) \cap \text{supp}(\tau) = \varnothing$.

ΑΠΟΔΕΙΞΗ. 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. □

3.1.6 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.

3.1.7 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

$$(\sigma \circ \tau)(j) = (\tau \circ \sigma)(j), \quad \forall j \in \{1,...,n\}. \tag{3.1}$$

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 (3.1) 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 (3.1) είναι αληθής ακόμη και για τους φυσικούς j τους ανήκοντες στον φορέα τής τ. □

3.1.8 Παρατήρηση. Το αντίστροφο τής προτάσεως 3.1.7 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

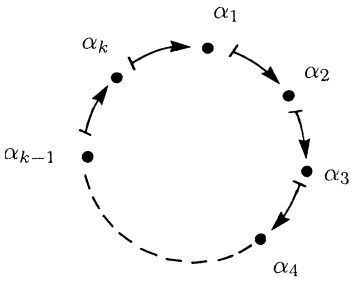
$$\sigma \circ \tau = \tau \circ \sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix},$$

αλλά δεν είναι ξένες μεταξύ τους, διότι $\text{supp}(\sigma) \cap \text{supp}(\tau) = \{1,2,3,4\} \neq \varnothing$.

3.2 ΚΥΚΛΟΙ

3.2.1 Ορισμός. Μια μετάταξη $\sigma \in \mathfrak{S}_n$ λέγεται **κύκλος μήκους** k (όπου $k \in \mathbb{N}$) ή **k-κύκλος** και γράφεται ως $[\alpha_1\ \alpha_2\ ...\ \alpha_k]$ όταν υπάρχουν k σαφώς διακεκριμένοι αριθμοί $\alpha_1, \alpha_2, ..., \alpha_k$ από το σύνολο $\{1, ..., n\}$ $(k \leq n)$, ούτως ώστε να ισχύει

$$\begin{cases} \sigma(\alpha_1) = \alpha_2, \sigma(\alpha_2) = \alpha_3, ..., \sigma(\alpha_{k-1}) = \alpha_k, \sigma(\alpha_k) = \alpha_1 \text{ (για } k \geq 2) \\ (\sigma(\alpha_1) = \alpha_1, \text{ για } k = 1) \text{ και } \sigma(\beta) = \beta, \ \forall \beta \in \{1, .., n\} \setminus \{\alpha_1, .., \alpha_k\}. \end{cases}$$



(Προφανώς, $\text{supp}([\alpha_1\ \alpha_2\ ...\ \alpha_k]) = \{\alpha_1, \alpha_2, ..., \alpha_k\}$ όταν $k \geq 2$ 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 $\mathfrak{S}_n$, $n \geq 3$, έχουμε $[2\ 3] \circ [1\ 2] = [1\ 3\ 2]$, και εντός τής $\mathfrak{S}_n$, $n \geq 8$,

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 6 & 7 & 3 & 5 & 4 & 2 \end{bmatrix} = [1\ 8\ 2] \circ [3\ 6\ 5] \circ [4\ 7]\,.$$

Οι 2-κύκλοι ονομάζονται, ιδιαιτέρως, **αντιμεταθέσεις**.

3.2.2 Παράδειγμα. Τα στοιχεία τής $\mathfrak{S}_3$ είναι τα

$$\text{id},\ [1\,2]\,,\ [1\,3]\,,\ [2\,3]\,,\ [1\,2\,3]\,,\ [1\,3\,2]\,,$$

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 ιδιότητές τους που δίδονται στην επόμενη πρόταση.

3.2.3 Πρόταση. (Ιδιότητες κύκλων) *Για τους k-κύκλους (εντός τής $\mathfrak{S}_n$) ισχύουν τα εξής*:

(i) $[\alpha_1\ \alpha_2 ...\ \alpha_k] = [\alpha_2\ \alpha_3 ...\ \alpha_k\ \alpha_1] = \cdots = [\alpha_k\ \alpha_1 ...\ \alpha_{k-1}]$, *ήτοι όλες οι «κυκλικές εναλλαγές» των k στοιχείων ενός k-κύκλου είναι ίσες μεταξύ τους.*

(ii) *Όταν* $k \geq 3$, *τότε* $[\alpha_1\ \alpha_2 ...\ \alpha_k] = [\alpha_1 ...\ \alpha_j] \circ [\alpha_j\ \alpha_{j+1} ...\ \alpha_k]$, $\forall j \in \{2,...,k-1\}$.

(iii) *Όταν* $k \geq 3$, *τότε*

$$[\alpha_1\ \alpha_2 ...\ \alpha_k] = [\alpha_1\ \alpha_2]\ \circ [\alpha_2\ \alpha_3] \circ \cdots \circ [\alpha_{k-1}\ \alpha_k] \tag{3.2}$$

και

$$[\alpha_1\ \alpha_2 ...\ \alpha_k] = [\alpha_1\ \alpha_k]\ \circ [\alpha_1\ \alpha_{k-1}] \circ \cdots \circ [\alpha_1\ \alpha_2]. \tag{3.3}$$

(iv) *Για κάθε* $m \in \mathbb{N}$ *ισχύει η ισότητα*

$$[\alpha_1\ \alpha_2 ...\ \alpha_k]^m = \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_{m+1} & a_{m+2} & \cdots & a_{m+k} \end{bmatrix},$$

όπου οι (υπο)δείκτες τής κάτω γραμμής οφείλουν να «διαβάζονται κατά μόδιο k», ήτοι $a_{k+1} = a_1$, $a_{k+2} = a_2$,....., $a_{k+t} = a_l$, *όπου* $t \equiv l (\mathrm{mod}\, k)$ $(t, l \in \mathbb{N})$.

(v) $\mathrm{ord}([\alpha_1\ \alpha_2 ...\ \alpha_k]) = k$.

(vi) $[\alpha_1\ \alpha_2 ...\ \alpha_k]^{-1} = [\alpha_k\ \alpha_{k-1} ...\ \alpha_1]$.

(vii) *Για κάθε* $\sigma \in \mathfrak{S}_n$ *ισχύει η ισότητα*

$$\boxed{\sigma \circ [\alpha_1\ \alpha_2 ...\ \alpha_k] \circ \sigma^{-1} = [\sigma(\alpha_1)\ \sigma(\alpha_2) ...\ \sigma(\alpha_k)].} \tag{3.4}$$

ΑΠΟΔΕΙΞΗ. Το (i) είναι εξ ορισμού προφανές. Το (ii) είναι άμεση συνέπεια τού υπολογισμού τού γινομένου (= συνθέσεως).

(iii) Η ισότητα (3.2) 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 (3.3) 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 $k \geq 4$ 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 $m \geq 1$, τότε

$$\begin{aligned} &[\alpha_1\ \alpha_2 ...\ \alpha_k]^{m+1} = [\alpha_1\ \alpha_2 ...\ \alpha_k]^m \circ [\alpha_1\ \alpha_2 ...\ \alpha_k] \\ &= \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_{m+1} & a_{m+2} & \cdots & a_{m+k} \end{bmatrix} \circ \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_2 & a_3 & \cdots & a_1 \end{bmatrix} \\ &= \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_{m+2} & a_{m+3} & \cdots & a_{m+1+k} \end{bmatrix}, \end{aligned}$$

όπου η δεύτερη ισότητα έπεται από την επαγωγική μας υπόθεση.
(v) Εάν $\sigma := [\alpha_1\ \alpha_2 ...\ \alpha_k]$, τότε από το (iv) λαμβάνουμε

$$\begin{aligned}\sigma^k &= [\alpha_1\ \alpha_2 ...\ \alpha_k]^k \\ &= \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_{k+1} & a_{k+2} & \cdots & a_{k+k} \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_1 & a_2 & \cdots & a_k \end{bmatrix} = \text{id}.\end{aligned}$$

Εάν $\varrho \in \{1, ..., k-1\}$, τότε $\sigma^\varrho(a_j) = a_{j+\varrho}, \forall j \in \{1, ..., k\}$, οπότε

$$j + \varrho \not\equiv j (\mathrm{mod}\, k), \forall j \in \{1, ..., k\} \Longrightarrow \sigma^\varrho \neq \text{id} \Longrightarrow \text{ord}\,([\alpha_1\ \alpha_2 ...\ \alpha_k]) = k.$$

(vi) Για $k = 1$ τούτο είναι προφανές. Για $k \geq 2$ έχουμε

$$[\alpha_1\ \alpha_2 ...\ \alpha_k]^{-1} = [\alpha_1\ \alpha_2 ...\ \alpha_k]^{k-1} = \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_k & a_{k+1} & \cdots & a_{2k-1} \end{bmatrix}$$

$$= \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_k & a_1 & \cdots & a_{k-1} \end{bmatrix} = [\alpha_k\ \alpha_{k-1} ...\ \alpha_1]$$

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 (3.4) 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 (3.4) είναι αληθής και *για κάθε* αντιμετάθεση (εντός τής $\mathfrak{S}_n$). Στην περίπτωση θεωρήσεως k-κύκλων $[\alpha_1\ \alpha_2 ...\ \alpha_k]$, όπου $k \geq 3$, χρησιμοποιούμε το (iii): Για κάθε $\sigma \in \mathfrak{S}_n$ έχουμε

$$\sigma \circ [\alpha_1\ \alpha_2 ...\ \alpha_k] \circ \sigma^{-1} = \sigma \circ [\alpha_1\ \alpha_2] \circ [\alpha_2\ \alpha_3] \circ \cdots \circ [\alpha_{k-1}\ \alpha_k] \circ \sigma^{-1}$$

$$= \left(\sigma \circ [\alpha_1\ \alpha_2] \circ \sigma^{-1}\right) \circ \left(\sigma \circ [\alpha_2\ \alpha_3] \circ \sigma^{-1}\right) \circ \cdots \circ \left(\sigma \circ [\alpha_{k-1}\ \alpha_k] \circ \sigma^{-1}\right)$$

$$= [\sigma(\alpha_1)\ \sigma(\alpha_2)] \circ [\sigma(\alpha_2)\ \sigma(\alpha_3)] \circ \cdots \circ [\sigma(\alpha_{k-1})\ \sigma(\alpha_k)] = [\sigma(\alpha_1)\ \sigma(\alpha_2) ...\ \sigma(\alpha_k)],$$

όπου η προτελευταία ισότητα έπεται από ό,τι είχαμε αποδείξει προηγουμένως για τις αντιμεταθέσεις. Ως εκ τούτου, η ισότητα (3.4) είναι αληθής για *οιουσδήποτε* k-κύκλους (εντός τής $\mathfrak{S}_n$). □

3.2.4 Λήμμα. *Εάν δυο κύκλοι $\sigma, \tau \in \mathfrak{S}_n$ είναι ξένοι μεταξύ τους, τότε μετατίθενται αμοιβαίως, δηλαδή $\sigma \circ \tau = \tau \circ \sigma$.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από την πρόταση 3.1.7. □

3.2.5 Λήμμα. *Εάν μια μετάταξη $\sigma \in \mathfrak{S}_n$ γράφεται υπό τη μορφή*

$$\sigma = c_1 \circ c_2 \circ \cdots \circ c_\nu \ \ (\nu \in \mathbb{N})$$

επαλλήλων συνθέσεων ανά δύο ξένων μεταξύ τους κύκλων $c_1, c_2, ..., c_\nu \in \mathfrak{S}_n$, και εάν υπάρχει $j \in \{1, ..., n\}$, ούτως ώστε $j \in \text{supp}(c_s)$ για κάποιον $s \in \{1, ..., \nu\}$, τότε

$$\sigma^\kappa(j) = c_s^\kappa(j), \ \ \forall \kappa \in \mathbb{N}.$$

ΑΠΟΔΕΙΞΗ. Επειδή οι $c_1, c_2, ..., c_\nu$ είναι ανά δύο ξένοι μεταξύ τους κύκλοι, το λήμμα 3.2.4 μας επιτρέπει να γράψουμε την σ ως εξής:

$$\sigma = \check{\sigma} \circ c_s, \ \ \text{όπου} \ \ \check{\sigma} := c_1 \circ \cdots \circ c_{s-1} \circ c_{s+1} \circ \cdots \circ c_\nu.$$

Προφανώς, οι $\check{\sigma}, c_s$ είναι μεταξύ τους ξένες μετατάξεις. Κατά συνέπειαν, $\check{\sigma}(j) = j$ (πρβλ. πρόταση 3.1.5) και

$$\check{\sigma} \circ c_s = c_s \circ \check{\sigma} \tag{3.5}$$

(και πάλι λόγω τού λήμματος 3.2.4). Κάνοντας χρήση τής κλασικής μαθηματικής επαγωγής ως προς τον κ και τής ισότητας (3.5) 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 $\kappa \in \mathbb{N}$. □

3.2.6 Λήμμα. *Εάν οι $\sigma, \tau \in \mathfrak{S}_n$ είναι κύκλοι και εάν υπάρχει $j \in \{1, ..., n\}$, ούτως ώστε $j \in \text{supp}(\sigma) \cap \text{supp}(\tau)$, τότε ισχύει η ακόλουθη συνεπαγωγή* :

$$[\sigma^\kappa(j) = \tau^\kappa(j), \ \forall \kappa \in \mathbb{N}] \Longrightarrow \sigma = \tau.$$

ΑΠΟΔΕΙΞΗ. Λόγω τού (i) τής προτάσεως 3.2.3 μπορούμε δίχως βλάβη τής γενικότητας να υποθέσουμε ότι

$$\sigma = [\alpha_1 \ \alpha_2 ... \ \alpha_\nu], \ \tau = [\beta_1 \ \beta_2 ... \ \beta_\xi], \ \ \text{όπου} \ \ \alpha_1 = \beta_1 = j.$$

Κατά το 3.2.3 (iv), $\alpha_{\kappa+1} = \sigma^\kappa(j)$ για κάθε κ, $1 \leq \kappa < \nu$, και $\beta_{\kappa+1} = \tau^\kappa(j)$ για κάθε κ, $1 \leq \kappa < \xi$. Δίχως βλάβη τής γενικότητας υποθέτουμε ότι $\nu \leq \xi$. 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 $\sigma^\nu = \text{id}$, λόγω τού 3.2.3 (v)), οπότε έχουμε κατ' ανάγκην $\xi = \nu$ και $\sigma = \tau$. □

3.2.7 Θεώρημα. *Κάθε μη ταυτοτική μετάταξη ανήκουσα στην $\mathfrak{S}_n$, $n \geq 2$, είτε είναι αφ' εαυτής ένας κύκλος είτε μπορεί να γραφεί υπό τη μορφή επαλλήλων συνθέσεων (πεπερασμένου πλήθους) ανά δύο ξένων μεταξύ τους κύκλων μήκους ≥ 2. Επιπροσθέτως, μια τέτοια έκφραση είναι μονοσημάντως ορισμένη (ενδεχομένως ύστερα από κάποια αναδιάταξη των μετεχόντων κύκλων).*

ΑΠΟΔΕΙΞΗ. 1) ΕΠΑΛΗΘΕΥΣΗ ΠΡΩΤΟΥ ΙΣΧΥΡΙΣΜΟΥ. Επειδή $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{id}\}$, έχουμε προφανώς $\varnothing \neq \mathrm{supp}(\sigma) \subseteq \{1, 2, ..., n\}$. Θέτουμε[2]

$$j_1 := \min(\mathrm{supp}(\sigma)) \ \text{ και } \ k_1 := \min\{\xi \in \mathbb{N} \,\big|\, \sigma^{\xi}(j_1) = j_1\},$$

και ορίζουμε τον k_1-κύκλο $\tau_1 := [j_1\ \sigma(j_1)\ \sigma^2(j_1)\ ...\ \sigma^{k_1-1}(j_1)]$, όπου $k_1 \geq 2$. Εάν $\mathrm{supp}(\sigma) = \mathrm{supp}(\tau_1)$, τότε $\sigma = \tau_1$. Ειδάλλως, $\mathrm{supp}(\tau_1) \subsetneqq \mathrm{supp}(\sigma)$, θέτουμε

$$j_2 := \min(\mathrm{supp}(\sigma) \setminus \mathrm{supp}(\tau_1)) \ \text{ και } \ k_2 := \min\{\xi \in \mathbb{N} \,\big|\, \sigma^{\xi}(j_2) = j_2\},$$

και ορίζουμε τον k_2-κύκλο $\tau_2 := [j_2\ \sigma(j_2)\ \sigma^2(j_2)\ ...\ \sigma^{k_2-1}(j_2)]$, όπου $k_2 \geq 2$. 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

$$j_3 := \min(\mathrm{supp}(\sigma) \setminus (\mathrm{supp}(\tau_1) \cup \mathrm{supp}(\tau_2))) \ \text{ και } \ k_3 := \min\{\xi \in \mathbb{N} \,\big|\, \sigma^{\xi}(j_3) = j_3\},$$

ορίζουμε τον k_3-κύκλο $\tau_3 := [j_3\ \sigma(j_3)\ \sigma^2(j_3)\ ...\ \sigma^{k_3-1}(j_3)]$, όπου $k_3 \geq 2$, 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 $\nu \leq \left\lfloor \frac{n}{2} \right\rfloor$ 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

$$\sigma^m(j_s) = \tau_s^m(j_s),\ \forall s \in \{1, ..., \nu\} \ \text{ και } \ \forall m \in \mathbb{Z}. \tag{3.6}$$

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 $0 \leq r_s \leq k_s - 1$. (Βλ. θεώρημα Β.1.6.) Επειδή $\mathrm{ord}(\tau_s) = k_s$, έχουμε $\tau_s^m = \tau_s^{r_s}$ και

$$\left.\begin{array}{c} \tau_s^{r_s}(j_s) = \sigma^{1+r_s-1}(j_s) = \sigma^{r_s}(j_s) \ \ (\text{από το 3.2.3 (iv)}) \\ \sigma^m(j_s) = \sigma^{q_s k_s + r_s}(j_s) \\ = \sigma^{r_s}(\underbrace{\sigma^{\mathrm{sign}(q_s)k_s} \circ \cdots \circ \sigma^{\mathrm{sign}(q_s)k_s}}_{|q_s| \text{ φορές}}(j_s)) = \sigma^{r_s}(j_s) \\ \big(\text{καθότι} \ \ \sigma^{k_s}(j_s) = j_s\big) \end{array}\right\} \Rightarrow \sigma^m(j_s) = \tau_s^m(j_s).$$

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,

$$\exists\, (m, m') \in \mathbb{N}_0 \times \mathbb{N}_0 : j = \sigma^m(j_s) = \sigma^{m'}(j_{s'}).$$

[2] 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 $\{\xi \in \mathbb{N} \,\big|\, \sigma^{\xi}(j) = j\}$ είναι ένα μη κενό υποσύνολο τού $\mathbb{N}$ περιέχον (σύμφωνα με την αρχή τής καλής διατάξεως τού $\mathbb{N}$) ελάχιστο στοιχείο.

Η (3.6) δίδει $j_{s'} = \sigma^{-m'}(\sigma^m(j_s)) = \sigma^{m-m'}(j_s) = \tau_s^{m-m'}(j_s) \Rightarrow j_{s'} \in \text{supp}(\tau_s)$. Από την άλλη μεριά, επειδή

$$j_{s'} := \min(\text{supp}(\sigma) \setminus (\text{supp}(\tau_1) \cup \cdots \cup \text{supp}(\tau_s) \cup \cdots \cup \text{supp}(\tau_{s'-1}))),$$

έχουμε $j_{s'} \notin \text{supp}(\tau_s)$. Άρα οι $\tau_1, ..., \tau_\nu$ είναι όντως ανά δύο ξένοι μεταξύ τους.

2) ΕΠΑΛΗΘΕΥΣΗ ΔΕΥΤΕΡΟΥ ΙΣΧΥΡΙΣΜΟΥ. Έστω $\sigma \in \mathfrak{S}_n \setminus \{\text{id}\}$. 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 $\tau_1, \tau_2, ..., \tau_\nu$ (και, αντιστοίχως, οι $\varrho_1, \varrho_2, ..., \varrho_{\nu'}$) είναι κύκλοι ανά δύο ξένοι μεταξύ τους μήκους ≥ 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 $\ell \geq 2$, αρκεί να αποδείξουμε την ορθότητά του και για τον ίδιον τον ℓ. Επειδή $\sigma \neq \text{id}$, $\exists j \in \{1, ..., n\} : \sigma(j) \neq j$ και $\exists s \in \{1, ..., \nu\}$, $s' \in \{1, ..., \nu'\} : j \in \text{supp}(\tau_s) \cap \text{supp}(\varrho_{s'})$. Κατά το λήμμα 3.2.5,

$$\sigma^\kappa(j) = \tau_s^\kappa(j) = \varrho_{s'}^\kappa(j), \ \ \forall \kappa \in \mathbb{N},$$

οπότε το λήμμα 3.2.6 μας πληροφορεί ότι $\tau_s = \varrho_{s'}$. Εξάλλου, δυνάμει τού λήμματος 3.2.4 και τού νόμου τής διαγραφής 2.1.9 (i) συνάγεται ότι

$$\begin{aligned}
&\tau_1 \circ \cdots \circ \tau_{s-1} \circ \tau_s \circ \tau_{s+1} \circ \cdots \circ \tau_\nu = \varrho_1 \circ \cdots \circ \varrho_{s'-1} \circ \varrho_{s'} \circ \varrho_{s'+1} \circ \cdots \circ \varrho_{\nu'} \\
&\Rightarrow (\tau_1 \circ \cdots \circ \tau_{s-1} \circ \tau_{s+1} \circ \cdots \circ \tau_\nu) \circ \tau_s = \left(\varrho_1 \circ \cdots \circ \varrho_{s'-1} \circ \varrho_{s'+1} \circ \cdots \circ \varrho_{\nu'}\right) \circ \varrho_{s'} \\
&\Rightarrow \tau_1 \circ \cdots \circ \tau_{s-1} \circ \tau_{s+1} \circ \cdots \circ \tau_\nu = \varrho_1 \circ \cdots \circ \varrho_{s'-1} \circ \varrho_{s'+1} \circ \cdots \circ \varrho_{\nu'}
\end{aligned}$$

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. □

3.2.8 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 $\text{supp}(\sigma) = \{1,2,3,4,6,7,8,9\}$, $j_1 = 1$, $k_1 = 2$, $\tau_1 = [1\ 6]$ και

$$\text{supp}(\sigma) \setminus \text{supp}(\tau_1) = \{2,3,4,7,8,9\}, \quad j_2 = 2, \quad k_2 = 2, \quad \tau_2 = [2\ 4],$$
$$\text{supp}(\sigma) \setminus \bigcup_{s=1}^{2} \text{supp}(\tau_s) = \{3,7,8,9\}, \quad j_3 = 3, \quad k_3 = 4, \quad \tau_3 = [3\ 7\ 8\ 9],$$

οπότε $\sigma = \tau_1 \circ \tau_2 \circ \tau_3$. (Το 5 δεν εμφανίζεται διότι μένει αμετάβλητο μέσω τής σ.)

3.2.9 Σημείωση. Ο λογισμός με τους κύκλους και τις μετατάξεις αναπτύχθηκε πλήρως από τον Γάλλο μαθηματικό Augustin-Louis Cauchy (1789-1857) περί το[3] 1815. Αυτός είχε κατ' ουσίαν αποδείξει *και* το θεώρημα 3.2.7, αν και πολλά συναφή λήμματα και αποτελέσματα (όπως είναι το πόρισμα 3.2.10) ήταν ήδη γνωστά (τουλάχιστον σε υπολογιστικό επίπεδο) ήδη από τα τέλη τού 18ου αιώνα.

3.2.10 Πόρισμα. (P. Ruffini, 1799) *Εάν μια μετάταξη $\sigma \in \mathfrak{S}_n \setminus \{\text{id}\}$, $n \geq 2$, γραφεί υπό τη μορφή επαλλήλων συνθέσεων $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_\nu$ -ανά δύο ξένων μεταξύ τους- κύκλων $\tau_1,...,\tau_\nu$ με μήκη $k_1,...,k_\nu \geq 2$, αντιστοίχως, τότε*[4]

$$\boxed{\text{ord}\,(\sigma) = \text{εκπ}(k_1,...,k_\nu).}$$

ΑΠΟΔΕΙΞΗ. Από το (v) τής προτάσεως 3.2.3 γνωρίζουμε ότι $k_i = \text{ord}(\tau_i)$ για κάθε $i \in \{1,...,\nu\}$. Θέτουμε[5] $k := \text{εκπ}(k_1,...,k_\nu)$. Επειδή οι $\tau_1,...,\tau_\nu$ είναι ανά δύο ξένοι μεταξύ τους, μετατίθενται αμοιβαίως ανά δύο (βλ. λήμμα 3.2.4). Επομένως,

$$\begin{aligned} \sigma^k &= (\tau_1 \circ \tau_2 \circ \cdots \circ \tau_\nu)^k = {\tau_1}^k \circ {\tau_2}^k \circ \cdots \circ {\tau_\nu}^k \\ &= ({\tau_1}^{k_1})^{\frac{k}{k_1}} \circ ({\tau_2}^{k_2})^{\frac{k}{k_2}} \circ \cdots \circ ({\tau_\nu}^{k_\nu})^{\frac{k}{k_\nu}} = \text{id} \circ\ \text{id} \circ \cdots \circ\ \text{id} =\ \text{id}, \end{aligned}$$

και, ως εκ τούτου,

$$k \geq \text{ord}(\sigma). \tag{3.7}$$

Έστω τώρα *τυχόν* $m \in \mathbb{N}$ με $\sigma^m = \text{id}$. Επειδή οι $\tau_1,...,\tau_\nu$ μετατίθενται αμοιβαίως ανά δύο, έχουμε $\text{id} = \sigma^m = (\tau_1 \circ \tau_2 \circ \cdots \circ \tau_\nu)^m = {\tau_1}^m \circ {\tau_2}^m \circ \cdots \circ {\tau_\nu}^m$. Ας υποθέσουμε ότι $\exists i_0 \in \{1,...,\nu\}$, τέτοιος ώστε να ισχύει ${\tau_{i_0}}^m \neq \text{id}$. Τότε ${\tau_{i_0}}^m(x) \neq x$ για κάποιο $x \in \{1,...,n\}$. 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 $\tau_1,...,\tau_\nu$ είναι ανά δύο ξένοι μεταξύ τους, θα έχουμε

$$\tau_j(x) = x,\ \forall j \in \{1,...,\nu\} \setminus \{i_0\} \Longrightarrow {\tau_j}^m(x) = x,\ \forall j \in \{1,...,\nu\} \setminus \{i_0\},$$

οπότε $({\tau_1}^m \circ {\tau_2}^m \circ \cdots \circ {\tau_\nu}^m)(x) \neq x \Longrightarrow {\tau_1}^m \circ {\tau_2}^m \circ \cdots \circ {\tau_\nu}^m \neq \text{id}$. Άτοπο! Κατά συνέπειαν, ${\tau_1}^m = {\tau_2}^m = \cdots = {\tau_\nu}^m = \text{id}$. Δυνάμει τής προτάσεως 2.3.8, $k_i \mid m$ για κάθε $i \in \{1,...,\nu\}$, οπότε (λόγω τής προτάσεως B.2.25)

$$k \mid m \Longrightarrow k \leq m \Longrightarrow k \leq \text{ord}(\sigma). \tag{3.8}$$

Από τις (3.7) και (3.8) έπεται ότι $k = \text{ord}(\sigma)$. □

[3] 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] Στην ειδική περίπτωση όπου $\nu = 1$, λαμβάνουμε $\text{ord}(\sigma) = k_1$. (Βλ. 3.2.3 (v).)

[5] Εάν $\nu = 1$, τότε θέτουμε απλώς $k := k_1$.

3.2.11 Πόρισμα. *Κάθε μετάταξη εντός τής* $\mathfrak{S}_n$, $n \geq 2$, *μπορεί να γραφεί υπό τη μορφή επαλλήλων συνθέσεων* (*πεπερασμένου πλήθους*) *αντιμεταθέσεων.*

ΑΠΟΔΕΙΞΗ. Εάν $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{id}\}$, τότε αυτό έπεται άμεσα από τον συνδυασμό τού θεωρήματος 3.2.7 με την ισότητα (3.2) (ή, εναλλακτικώς, την ισότητα (3.3)) τού (iii) τής προτάσεως 3.2.3. 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) τής προτάσεως 3.2.3. □

3.2.12 Πόρισμα. *Όταν* $n \in \mathbb{N}$, $n \geq 2$, *τότε η συμμετρική ομάδα* $\mathfrak{S}_n$ *παράγεται από το σύνολο των αντιμεταθέσεών της.*

3.2.13 Πόρισμα. *Έστω* $n \in \mathbb{N}$, $n \geq 2$. *Τότε ισχύουν τα ακόλουθα*:

(i) $\mathfrak{S}_n = \langle \{[1\ \ i] \mid i \in \{2, \ldots, n\}\} \rangle$.

(ii) $\mathfrak{S}_n = \langle \{[j\ \ j+1] \mid j \in \{1, \ldots, n-1\}\} \rangle$.

(iii) $\mathfrak{S}_n = \langle [1\ \ 2], [1\ 2 \ldots\ n] \rangle$, *όταν* $n \geq 3$.

ΑΠΟΔΕΙΞΗ. (i) Λόγω τού πορίσματος 3.2.12 αρκεί να δειχθεί ότι κάθε αντιμετάθεση ανήκουσα στην $\mathfrak{S}_n$ μπορεί να γραφεί ως σύνθεση (πεπερασμένου πλήθους) αντιμεταθέσεων τής μορφής $[1\ \ i]$ (όπου $i \in \{2, \ldots, n\}$). 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. 3.2.3 (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 $i \in \{2, \ldots, n\}$) μπορεί να γραφεί ως σύνθεση (πεπερασμένου πλήθους) αντιμεταθέσεων τής μορφής $[j\ \ j+1]$ (όπου $j \in \{1, \ldots, n-1\}$). Προς τούτο αρκεί να παρατηρήσουμε ότι

$$\begin{aligned}
[1\ \ i] &= [1\ \ i-1] \circ [i-1\ \ i] \circ [1\ \ i-1] \\
&= [1\ \ i-2] \circ [i-2\ \ i-1] \circ [1\ \ i-2] \circ [i-1\ \ i] \circ [1\ \ i-2] \circ [i-2\ \ i-1] \circ [1\ \ i-2] \\
&= [1\ \ i-2] \circ [i-2\ \ i-1] \circ [i-1\ \ i] \circ [1\ \ i-2]^2 \circ [i-2\ \ i-1] \circ [1\ \ i-2] \\
&= [1\ \ i-2] \circ [i-2\ \ i-1] \circ [i-1\ \ i] \circ [i-2\ \ i-1] \circ [1\ \ i-2] \\
&= \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}$$

$$= [1\ 2] \circ [2\ 3] \circ [3\ 4] \circ \cdots \circ [i-2\ \ i-1] \circ [i-1\ \ i] \circ [i-2\ \ i-1] \circ \cdots \circ [3\ 4] \circ [2\ 3] \circ [1\ 2]\,.$$

(iii) Λόγω τού (ii) αρκεί να δειχθεί ότι κάθε αντιμετάθεση τής μορφής $[j\ \ j+1]$ (όπου $j \in \{1, \ldots, n-1\}$) ανήκει στην υποομάδα τής $\mathfrak{S}_n$ που παράγεται από τους κύκλους $\tau := [1\ \ 2]$ και $\sigma := [1\ 2 \ldots\ n]$. Εφαρμόζοντας την (3.4) 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 $[j\ \ j+1]$. □

3.3 ΑΡΤΙΕΣ ΚΑΙ ΠΕΡΙΤΤΕΣ ΜΕΤΑΤΑΞΕΙΣ

Έστω τυχούσα μετάταξη $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{id}\}$ (όπου $n \geq 2$). Αυτή, σύμφωνα με το θεώρημα 3.2.7, μπορεί να γραφεί *μονοσημάντως* υπό τη μορφή επαλλήλων συνθέσεων (πεπερασμένου πλήθους) ανά δύο ξένων μεταξύ τους κύκλων μήκους ≥ 2 (ενδεχομένως ύστερα από κάποια αναδιάταξη των μετεχόντων κύκλων). Όμως η έκφρασή της υπό τη μορφή επαλλήλων συνθέσεων (πεπερασμένου πλήθους) αντιμεταθέσεων (βλ. πόρισμα 3.2.11) *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 $k \geq 3$ εντός τής $\mathfrak{S}_n$ $(k \leq n)$ και να εφαρμόσει την (3.2):

$$[\alpha_1\ \alpha_2 \ldots\ \alpha_k] = [\alpha_1\ \alpha_2] \circ [\alpha_2\ \alpha_3] \circ [\alpha_3\ \alpha_4] \circ \cdots \circ [\alpha_{k-1}\ \alpha_k]. \tag{3.9}$$

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 (3.2) και τη δεύτερη λόγω τής (3.3) για $k = 3$) έχουμε

$$[\alpha_1\ \alpha_2 \ldots\ \alpha_k] = ([\alpha_1\ \alpha_3] \circ [\alpha_1\ \alpha_2]) \circ [\alpha_3\ \alpha_4] \circ \cdots \circ [\alpha_{k-1}\ \alpha_k], \tag{3.10}$$

με τις (3.9) και (3.10) περιέχουσες διαφορετικές αντιμεταθέσεις! Ωστόσο, αξίζει να επισημανθεί ότι σε *οιεσδήποτε* θεωρούμενες εκφράσεις μιας $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{id}\}$, $n \geq 2$, 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. 3.3.5 (iv)).

3.3.1 Ορισμός. (i) Έστω $n \in \mathbb{N}$ και έστω $\sigma \in \mathfrak{S}_n$ μια μετάταξη. Ορίζουμε ως **παραβατικό ζεύγος**[6] (για την σ) κάθε διατεταγμένο ζεύγος $(i, j) \in \{1,...,n\} \times \{1,...,n\}$ 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

$$\mathrm{sgn} : (\mathfrak{S}_n, \circ) \longrightarrow (\{1, -1\}, \cdot) \tag{3.11}$$

[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).

μέσω τού τύπου[7]:

$$\operatorname{sgn}(\sigma) := \begin{cases} 1, & \text{όταν η } \sigma \text{ διαθέτει έναν άρτιο αριθμό παραβατικών ζευγών,} \\ -1, & \text{όταν η } \sigma \text{ διαθέτει έναν περιττό αριθμό παραβατικών ζευγών,} \end{cases}$$

για κάθε[8] $\sigma \in \mathfrak{S}_n$.

(iii) Μια μετάταξη $\sigma \in \mathfrak{S}_n$ ονομάζεται **άρτια** (και αντιστοίχως, **περιττή**) όταν $\operatorname{sgn}(\sigma) = 1$ (και αντιστοίχως, όταν $\operatorname{sgn}(\sigma) = -1$).

3.3.2 Παράδειγμα. Τα παραβατικά ζεύγη τής μετατάξεως

$$\begin{bmatrix} 1\,2\,3\,4 \\ 2\,1\,4\,3 \end{bmatrix}$$

είναι τα $(1,2)$ και $(3,4)$.

3.3.3 Λήμμα. *Κάθε αντιμετάθεση $\tau \in \mathfrak{S}_n$, $n \geq 2$, είναι περιττή μετάταξη, δηλαδή*

$$\boxed{\operatorname{sgn}(\tau) = -1.}$$

ΑΠΟΔΕΙΞΗ. Έστω $\tau = [i\ j]$, όπου $1 \leq i < j \leq n$. Αρκεί να καταμετρήσουμε το πλήθος των παραβατικών ζευγών της. Γράφοντάς την «σε πλήρη έκταση», λαμβάνουμε

$$\begin{bmatrix} 1 & \ldots & i-1 & \boxed{i} & i+1 & \ldots & j-1 & \boxed{j} & j+1 & \ldots & n \\ 1 & \ldots & i-1 & \boxed{j} & i+1 & \ldots & j-1 & \boxed{i} & j+1 & \ldots & n \end{bmatrix}.$$

Προφανώς, τα παραβατικά ζεύγη -πέραν τού ιδίου τού (i,j)- ανήκουν στην ένωση δύο συνόλων:

$$\{(i,k) \mid i+1 \leq k \leq j-1\} \cup \{(l,j) \mid i+1 \leq l \leq j-1\}.$$

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 $\operatorname{sgn}(\tau) = -1$. □

3.3.4 Λήμμα. *Η τιμή που λαμβάνει οιαδήποτε μετάταξη $\sigma \in \mathfrak{S}_n$, $n \geq 1$, μέσω τής απεικονίσεως προσημάνσεως μπορεί να εκφρασθεί με τη βοήθεια τού ακολούθου «κλειστού» τύπου*:

$$\boxed{\operatorname{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j-i}.}$$

[7] Η τιμή $\operatorname{sgn}(\sigma)$ ονομάζεται **προσημασμένος άσος** (ή -πιο σύντομα, αλλά όχι ακριβολογημένα- **πρόσημο**) τής σ.

[8] Σημειωτέον ότι $\operatorname{sgn}(\mathrm{id}) = 1$ (διότι το πλήθος των παραβατικών ζευγών τής id ισούται με το 0).

ΑΠΟΔΕΙΞΗ. 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

$$\prod_{1\le i<j\le n}(\sigma(j)-\sigma(i)) = \left(\prod_{\substack{1\le i<j\le n\\ \sigma(i)<\sigma(j)}}\sigma(j)-\sigma(i)\right)\cdot(-1)^s\prod_{\substack{1\le i<j\le n\\ \sigma(i)>\sigma(j)}}|\sigma(j)-\sigma(i)|$$

$$= (-1)^s\prod_{1\le i<j\le n}|\sigma(j)-\sigma(i)| = (-1)^s\prod_{1\le i<j\le n}(j-i).$$

Σημειωτέον ότι στην τελευταία ισότητα χρησιμοποιήσαμε το γεγονός τού ότι τα δύο γινόμενα περιέχουν *τους ίδιους παράγοντες* (έστω κι αν αυτοί τύχει να είναι παρατεταγμένοι κατά διαφορετικό τρόπο). Τούτο έπεται από την αμφιρριπτικότητα τής σ. □

3.3.5 Θεώρημα. (i) *Για τυχούσες* $\sigma,\tau\in\mathfrak{S}_n$ (*όπου* $n\ge 1$) *έχουμε*

$$\boxed{\operatorname{sgn}(\tau\circ\sigma)=\operatorname{sgn}(\tau)\cdot\operatorname{sgn}(\sigma).}$$

οπότε η απεικόνιση προσημάνσεως (3.11) *είναι ένας ομομορφισμός ομάδων.*

(ii) *Για κάθε* $\sigma\in\mathfrak{S}_n$ (*όπου* $n\ge 1$) *έχουμε*

$$\boxed{\operatorname{sgn}(\sigma)=\operatorname{sgn}\left(\sigma^{-1}\right).}$$

(iii) *Εάν η μετάταξη* $\sigma=\tau_1\circ\tau_2\circ\cdots\circ\tau_k\in\mathfrak{S}_n$, $n\ge 2$, *συντίθεται από* k *αντιμεταθέσεις* $\tau_1,\tau_2,...,\tau_k$, *τότε*

$$\boxed{\operatorname{sgn}(\sigma)=(-1)^k.}$$

Ιδιαιτέρως, αυτή η ισότητα ισχύει για κάθε $(k+1)$*-κύκλο*[9] $\sigma\in\mathfrak{S}_n$ $(0\le k\le n-1)$.

(iv) *Εάν μια μετάταξη* $\sigma\in\mathfrak{S}_n, n\ge 2,$ *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* $\tau_1,...,\tau_k$ *και -ταυτοχρόνως-* l *αντιμεταθέσεων* $\tau_1',...,\tau_l'$, *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.*

[9] Ως εκ τούτου, ένας k-κύκλος εντός τής $\mathfrak{S}_n$ $(1\le k\le n)$ είναι άρτια (και αντιστοίχως, περιττή) μετάταξη εάν και μόνον εάν ο k είναι περιττός (και αντιστοίχως, άρτιος) φυσικός αριθμός.

ΑΠΟΔΕΙΞΗ. (i) Σύμφωνα με το λήμμα 3.3.4 έχουμε

$$\begin{aligned}\operatorname{sgn}(\tau\circ\sigma) &= \prod_{1\le i<j\le n}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{j-i}\\ &= \prod_{1\le i<j\le n}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)}\prod_{1\le i<j\le n}\frac{\sigma(j)-\sigma(i)}{j-i}.\end{aligned}$$

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

$$\prod_{1\le i<j\le n}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)}$$

γράφεται ως ακολούθως:

$$\begin{aligned}&\prod_{\substack{1\le i<j\le n\\ \sigma(i)<\sigma(j)}}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)}\prod_{\substack{1\le i<j\le n\\ \sigma(i)>\sigma(j)}}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)}\\ =&\prod_{\substack{1\le i<j\le n\\ \sigma(i)<\sigma(j)}}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)}\prod_{\substack{1\le j<i\le n\\ \sigma(i)<\sigma(j)}}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)}\\ =&\prod_{\sigma(i)<\sigma(j)}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)}.\end{aligned}$$

Επειδή η σ είναι αμφιρριπτική, θα υπάρχουν *μοναδικοί* $l,m\in\{1,...,n\}$ για *κάθε* i,j, τέτοιοι ώστε $\sigma(j)=l$, $\sigma(i)=m$ (και *ταυτόχρονα*). 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 3.3.3 και το (iii) τής προτάσεως 3.2.3.

(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. □

3.3.6 Πόρισμα. *Για οιεσδήποτε μετατάξεις $\sigma, \tau \in \mathfrak{S}_n$ (όπου $n \geq 2$) 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.*

ΑΠΟΔΕΙΞΗ. Τα (i) και (ii) έπονται άμεσα από το 3.3.5 (ii), και τα (iii), (iv), (v), (vi) από το 3.3.5 (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). □

3.3.7 Πόρισμα. *Έστω $n \in \mathbb{N}$, $n \geq 2$, 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 $k_j \geq 2$ για κάθε $j \in \{1, ..., \nu\}$ (όπως στο θεώρημα 3.2.7), 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 3.3.5 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 $\xi \equiv 0 (\mathrm{mod}\, 2)$. □

3.3.8 Ορισμός. Έστω n ένας φυσικός αριθμός ≥ 2. Ο πυρήνας

$$\boxed{\mathfrak{A}_n := \mathrm{Ker}\,(\mathrm{sgn}) = \{\, \sigma \in \mathfrak{S}_n \mid \mathrm{sgn}\,(\sigma) = 1\}}$$

τού ομομορφισμού (3.11) είναι μια υποομάδα τής συμμετρικής ομάδας $\mathfrak{S}_n$ (κατά το (ii) τού λήμματος 2.4.4), απαρτίζεται από όλες τις άρτιες μετατάξεις τής $\mathfrak{S}_n$ και καλείται **εναλλάσσουσα ομάδα** (σε n σύμβολα). Σημειωτέον ότι το σύνολο $\{\sigma \in \mathfrak{S}_n \mid \operatorname{sgn}(\sigma) = -1\}$ *δεν* είναι υποομάδα τής $\mathfrak{S}_n$, διότι δεν περιέχει το ουδέτερο στοιχείο id τής $\mathfrak{S}_n$.

3.3.9 Πρόταση. *Η τάξη τής* $\mathfrak{A}_n$, $n \geq 2$, *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 $\operatorname{sgn}(\tau) = 1$, τότε $\mathfrak{A}_n \circ \tau = \mathfrak{A}_n$. Ας παγιώσουμε τώρα μια $\tau \in \mathfrak{S}_n$ για την οποία ισχύει $\operatorname{sgn}(\tau) = -1$. Για κάθε $\sigma \in \mathfrak{S}_n$ με $\operatorname{sgn}(\sigma) = -1$ έχουμε $\operatorname{sgn}\left(\sigma \circ \tau^{-1}\right) = 1$ (βάσει τού (i) τού θεωρήματος 3.3.5), οπότε $\sigma \in \mathfrak{A}_n \circ \tau$, διότι $\sigma = \left(\sigma \circ \tau^{-1}\right) \circ \tau$. Τούτο σημαίνει ότι $\{\sigma \in \mathfrak{S}_n \mid \operatorname{sgn}(\sigma) = -1\} \subseteq \mathfrak{A}_n \circ \tau$, οπότε τελικώς

$$\{\sigma \in \mathfrak{S}_n \mid \operatorname{sgn}(\sigma) = -1\} = \mathfrak{A}_n \circ \tau$$

(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 3.1.3)

$$\mathfrak{S}_n = \mathfrak{A}_n \coprod (\mathfrak{A}_n \circ \tau) \Rightarrow n! = |\mathfrak{S}_n| = |\mathfrak{A}_n| + \operatorname{card}(\mathfrak{A}_n \circ \tau) = 2\,|\mathfrak{A}_n|\,,$$

οπότε $|\mathfrak{A}_n| = \frac{n!}{2}$. □

3.3.10 Παρατήρηση. Από το (i) τού θεωρήματος 3.3.5 και την απόδειξη τής προτάσεως 3.3.9 έπεται άμεσα ότι για $n \geq 2$ η απεικόνιση προσημάνσεως (3.11) είναι *επιμορφισμός* ομάδων.

3.3.11 Παραδείγματα. Προφανώς,

$$\mathfrak{A}_2 = \{\mathrm{id}\},\ \ \mathfrak{A}_3 = \{\mathrm{id}, [1\ 2\ 3], [1\ 3\ 2]\} = \langle [1\ 2\ 3] \rangle\,.$$

Για την εύρεση των στοιχείων τής $\mathfrak{A}_4$ επιχειρηματολογούμε ως εξής: Κατά το θεώρημα 3.2.7 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 ≥ 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 3.3.9) 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)

$$2\nu \leq \sum_{\kappa=1}^{\nu} (\text{μήκος τού } \tau_\kappa) \leq 4 \Longrightarrow \nu \leq 2.$$

Λαμβάνοντας υπ' όψιν ότι οι 2-κύκλοι (= αντιμεταθέσεις) είναι περιττές μετατάξεις (βλ. λήμμα 3.3.3), συμπεραίνουμε (από το (iii) τού θεωρήματος 3.3.5) ότι η μετάταξη 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 $1 \leq i < j \leq 4$, $1 \leq k < l \leq 4$ και $\{i,j\} \cap \{k,l\} = \varnothing$. Επειδή, εν προκειμένω, ισχύει $[i\ j] \circ [k\ l] = [k\ l] \circ [i\ j]$ (βλ. λήμμα 3.2.4), 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 $[i\ j\ k]$, $1 \leq i < j < k \leq 4$ 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 $3 + 4 + 4 = 11 = \mathrm{card}(\mathfrak{A}_4 \smallsetminus \{\mathrm{Id}\})$, έχουμε τελικώς (λόγω των (vi) και (i) τής προτάσεως 3.2.3)

$$\mathfrak{A}_4 = \left\{ \begin{array}{cccc} \mathrm{id}, & [1\ 2] \circ [3\ 4], & [1\ 3] \circ [2\ 4], & [1\ 4] \circ [2\ 3], \\ [1\ 2\ 3], & [1\ 2\ 4], & [1\ 3\ 4], & [2\ 3\ 4], \\ [1\ 3\ 2], & [1\ 4\ 2], & [1\ 4\ 3], & [2\ 4\ 3] \end{array} \right\}.$$

3.3.12 Σημείωση. Η εναλλάσσουσα ομάδα $\mathfrak{A}_n$ *δεν είναι αβελιανή για* $n \geq 4$. 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, $\tau \circ \sigma \neq \sigma \circ \tau$.

3.3.13 Πρόταση. *Έστω* $n \in \mathbb{N}$, $n \geq 3$. *Τότε ισχύουν τα ακόλουθα:*

(i) $\mathfrak{A}_n = \langle \{[i\ j] \circ [k\ l] \mid 1 \leq i < j \leq n,\ 1 \leq k < l \leq n\} \rangle$.

(ii) *Η* $\mathfrak{A}_n$ *παράγεται από το σύνολο των* 3*-κύκλων*[10].

(iii) $\mathfrak{A}_n = \langle \{[\alpha\ \beta\ i] \mid i \in \{1,...,n\} \smallsetminus \{\alpha, \beta\}\} \rangle$, *όπου τα* α, β *είναι δύο παγιωμένα στοιχεία τού* $\{1,...,n\}$ *και* $\alpha \neq \beta$.

(iv) $\mathfrak{A}_n = \langle \{[1\ 2\ i] \mid 3 \leq i \leq n\} \rangle$.

ΑΠΟΔΕΙΞΗ. (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. 3.2.11 και 3.3.5 (iv)). Άρα το $\{[i\ j] \circ [k\ l] \mid 1 \leq i < j \leq n,\ 1 \leq k < l \leq n\}$ είναι όντως ένα σύνολο γεννητόρων τής $\mathfrak{A}_n$.

[10] Κατά το (iii) τού θεωρήματος 3.3.5 κάθε 3-κύκλος είναι άρτια μετάταξη, οπότε ανήκει στην $\mathfrak{A}_n$.

(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

$$[i\ j] \circ [k\ l] \in \mathfrak{A}_n,\ 1 \leq i < j \leq n,\ 1 \leq k < l \leq n,$$

και εξετάζουμε τέσσερεις περιπτώσεις χωριστά.
Περίπτωση πρώτη. Εάν $i = k$ και $j = l$, τότε, σύμφωνα με το 3.2.3 (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 3.2.3, 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 3.2.3 και τής γενικευμένης προσεταιριστικής ιδιότητας (βλ. πρόταση 1.2.19) 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) 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 $\langle \{[\alpha\ \beta\ i] \mid i \in \{1,...,n\} \setminus \{\alpha, \beta\}\} \rangle$. 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 $\alpha = 1, \beta = 2$. □

3.4 ΠΑΡΑΔΕΙΓΜΑΤΑ ΟΜΑΔΩΝ ΜΕΤΑΤΑΞΕΩΝ

3.4.1 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**.

3.4.2 Παραδείγματα. (i) Η εναλλάσσουσα ομάδα $\mathfrak{A}_n$ είναι μια ομάδα μετατάξεων.
(ii) Έστω $\mathbf{V}$ 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 $\mathbf{V}$ 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[11] $(\mathbf{V},\circ)$ 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. 2.3.7.)

(iii) Έστω $n\in\mathbb{N}$, $n\geq 3$. Ορίζουμε τις ακόλουθες μετατάξεις $\sigma,\tau\in\mathfrak{S}_n$:

$$\sigma:=\begin{bmatrix}1 & 2 & 3 & \cdots & n-1 & n\\ 1 & n & n-1 & \cdots & 3 & 2\end{bmatrix},\ \ \tau:=[1\,2\ldots\,n]. \tag{3.12}$$

Σημειωτέον ότι

$$\sigma^2=\ \mathrm{id}=\tau^n,\quad \tau\circ\sigma=\sigma\circ\tau^{-1}\ \left(=\sigma\circ\tau^{n-1}\right). \tag{3.13}$$

Η τρίτη ισότητα έπεται από τα (vi) και (vii) τής προτάσεως 3.2.3, 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

$$\boxed{\bar{\mathbf{D}}_n:=\langle\sigma,\tau\rangle} \tag{3.14}$$

τής $\mathfrak{S}_n$ η παραγόμενη από τις σ και τ είναι μια (μη αβελιανή[12]) ομάδα μετατάξεων. Επειδή $\mathrm{ord}(\sigma)=2$ (καθότι $\sigma\neq\mathrm{id}$, $\sigma^2=\mathrm{id}$) και $\mathrm{ord}(\tau)=n$ (βλ. 3.2.3 (v)), μέσω των ισοτήτων (3.13) διαπιστώνουμε εύκολα ότι

$$\bar{\mathbf{D}}_n=\left\{\sigma^j\circ\tau^k\,|j\in\{0,1\}\ ,\ k\in\{0,1,\ldots,n-1\}\right\}.$$

Τα αναγραφόμενα $2n$ στοιχεία είναι σαφώς διακεκριμένα. Πράγματι· εάν

$$j_1,j_2\in\{0,1\},\ k_1,k_2\in\{0,1,\ldots,n-1\}:\sigma^{j_1}\circ\tau^{k_1}=\sigma^{j_2}\circ\tau^{k_2},$$

[11] Το γράμμα $\mathbf{V}$ 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.

[12] Προφανώς, $\tau\circ\sigma=\sigma\circ\tau^{-1}\neq\sigma\circ\tau$.

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

$$\left.\begin{array}{r} \mathrm{ord}(\tau) = n \underset{(\text{βλ. } 2.3.8)}{\Longrightarrow} n \mid k_2 - k_1 \\ |k_2 - k_1| < n \end{array}\right\} \Rightarrow k_2 - k_1 = 0 \Rightarrow k_1 = k_2$$

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

$$\sigma^{j_1} \circ \tau^{k_1} = \sigma^{j_2} \circ \tau^{k_2} \Longleftrightarrow [j_1 = j_2 \ \text{και} \ \ k_1 = k_2],$$

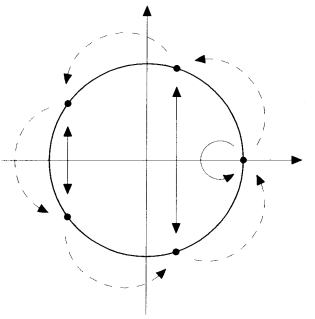
και $\left|\bar{\mathbf{D}}_n\right| = 2n$. Στο εδάφιο 3.4.4 θα ορισθεί άλλη μία σημαντική ομάδα μετατάξεων, η οποία, όπως θα δούμε, είναι ισόμορφη με την $\bar{\mathbf{D}}_n$ και διαθέτει στοιχεία που επιδέχονται μια ειδική *γεωμετρική ερμηνεία*.

3.4.3 Σημείωση. Όταν $n = 3$, τότε $\bar{\mathbf{D}}_3 = \mathfrak{S}_3$ (πρβλ. 3.2.2).

3.4.4 Παράδειγμα. (Διεδρική ομάδα) Έστω $n \in \mathbb{N}$, $n \geq 3$, και έστω $(\mathcal{E}_n, \cdot)$ η ομάδα των n-οστών ριζών τής μονάδας (βλ. 2.1.21 (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. 2.2.16.) Θεωρούμε τα στοιχεία α και β τής $\mathfrak{S}_{\mathcal{E}_n}$ τα οριζόμενα μέσω των τύπων

$$\alpha(z) := z^{-1} = \frac{\overline{z}}{z\overline{z}} = \frac{\overline{z}}{|z|^2} = \overline{z}, \ \ \beta(z) := \zeta_n z, \ \ \forall z \in \mathcal{E}_n. \tag{3.15}$$

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:

$$\alpha^2 = \beta^n = \mathrm{id}_{\mathcal{E}_n}, \quad \beta \circ \alpha = \alpha \circ \beta^{-1} \ \left(= \alpha \circ \beta^{n-1}\right). \tag{3.16}$$

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 3.4.2 διαπιστώνουμε μέσω των ισοτήτων (3.16) 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[13] $|\mathbf{D}_n| = 2n$. Επιπροσθέτως, η απεικόνιση

$$\mathbf{D}_n \ni \alpha^j \circ \beta^k \longmapsto \sigma^j \circ \tau^k \in \bar{\mathbf{D}}_n, \ \ j \in \{0,1\}, \ k \in \{0,1,...,n-1\},$$

(όπου σ, τ όπως στην (3.12)) είναι ισομορφισμός ομάδων, οπότε

$$\boxed{\mathbf{D}_n \cong \bar{\mathbf{D}}_n.} \tag{3.17}$$

Η $(\mathbf{D}_n, \circ)$ καλείται n-**οστή διεδρική ομάδα**. Στην ειδική περίπτωση όπου $n = 3$ έχουμε[14] (λόγω των (3.17) και 3.4.3)

$$\boxed{\mathbf{D}_3 \cong \mathfrak{S}_3.}$$

3.4.5 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. 2.1.21 (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

$$\mathbf{M}P_n := \left\{ \mathbf{M}\begin{pmatrix} x \\ y \end{pmatrix} \middle| \begin{pmatrix} x \\ y \end{pmatrix} \in P_n \right\}, \ \forall \mathbf{M} \in \mathrm{Mat}_{2\times 2}(\mathbb{R}),$$

[13] 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).

[14] Όταν $n > 3$, τότε $|\mathbf{D}_n| = 2n < n! = |\mathfrak{S}_n|$, οπότε $\mathbf{D}_n \ncong \mathfrak{S}_n$ (βλ. 3.1.3 και 2.4.19 (i)).

και ορίζοντας ως **ομάδα των (πλήρων, επιπέδων) συμμετριών τού** P_n την

$$\boxed{\mathbf{\Sigma υμμ}(P_n) := \{\mathbf{M} \in \mathbf{O}_2(\mathbb{R}) | \, \mathbf{M}P_n = P_n\} \sqsubset \mathbf{O}_2(\mathbb{R}),}$$

ήτοι την ομάδα την απαρτιζόμενη από τους ορθογώνιους πίνακες που στέλνουν το P_n να απεικονισθεί στο εαυτό του, αποδεικνύεται ότι

$$\begin{aligned}\mathbf{\Sigma υμμ}(P_n) = \langle \mathbf{A}, \mathbf{B} \rangle &= \left\{ \mathbf{A}^j \mathbf{B}^k \, | j \in \{0,1\} \, , \; k \in \{0,1,...,n-1\} \right\} \\ &= \left\{ \mathbf{I}_2, \mathbf{B}, \mathbf{B}^2, ..., \mathbf{B}^{n-1}, \mathbf{A}, \mathbf{AB}, \mathbf{AB}^2, ..., \mathbf{AB}^{n-1} \right\},\end{aligned}$$

όπου

$$\mathbf{A} := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \; \mathbf{B} := \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}, \tag{3.18}$$

με

$$\mathbf{A}^2 = \mathbf{B}^n = \mathbf{I}_2, \quad \mathbf{BA} = \mathbf{AB}^{-1} \; \left(= \mathbf{AB}^{n-1} \right). \tag{3.19}$$

Επιπροσθέτως, $|\mathbf{\Sigma υμμ}(P_n)| = 2n$. Για κάθε $k \in \{0,1,...,n-1\}$ ο ορθογώνιος μετασχηματισμός

$$\mathbb{R}^2 \ni \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \mathbf{B}^k \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2,$$

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* [15] 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

$$\mathbb{R}^2 \ni \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \mathbf{AB}^k \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2, \;\; k \in \{0,1,...,n-1\},$$

[15] 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* [16] 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 $m \geq 1$, 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 $\mathbf{v}_{n-\frac{k}{2}}$ 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 $k \in \{2, 4, ..., 2m-2, 2m\}$, 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 $k \in \{1, 3, 5, ..., 2m-3, 2m-1\}$.

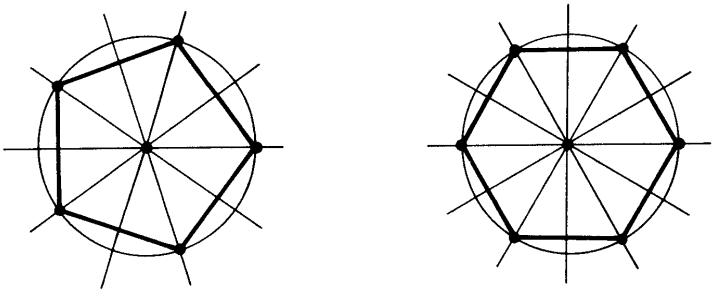
• Εάν $n = 2m$, για κάποιον φυσικό αριθμό $m \geq 2$, τότε η εν λόγω ευθεία η καθορίζεται (κατά περίπτωση)

(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 $k \in \{2, 4, ..., 2m-4, 2m-2\}$, 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 $k \in \{1, 3, 5, ..., 2m-3, 2m-1\}$.

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

$$\mathbf{D}_n \ni \alpha^j \circ \beta^k \longmapsto \mathbf{A}^j\mathbf{B}^k \in \Sigma\upsilon\mu\mu(P_n), \;\; j \in \{0, 1\}, \; k \in \{0, 1, ..., n-1\},$$

[16] Ένας 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.)

(όπου α, β όπως στην (3.15)) είναι ισομορφισμός ομάδων, οπότε

$$\boxed{\mathbf{D}_n \cong \Sigma\upsilon\mu\mu(P_n).}$$

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

$$\boxed{\Pi\epsilon\rho.\Sigma\upsilon\mu\mu(\widehat{P}_n) := \left\{ \mathbf{M} \in \mathrm{SO}_3(\mathbb{R}) |\, \mathbf{M}\widehat{P}_n = \widehat{P}_n \right\} \sqsubset \mathrm{SO}_3(\mathbb{R}),}$$

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

$$\begin{aligned} \Pi\epsilon\rho.\Sigma\upsilon\mu\mu(\widehat{P}_n) &= \left\langle \widehat{\mathbf{A}}, \widehat{\mathbf{B}} \right\rangle = \left\{ \widehat{\mathbf{A}}^j \widehat{\mathbf{B}}^k \,|\, j \in \{0,1\}\ ,\ k \in \{0,1,...,n-1\} \right\} \\ &= \left\{ \mathbf{I}_3, \widehat{\mathbf{B}}, \widehat{\mathbf{B}}^2, ..., \widehat{\mathbf{B}}^{n-1}, \widehat{\mathbf{A}}, \widehat{\mathbf{A}}\widehat{\mathbf{B}}, \widehat{\mathbf{A}}\widehat{\mathbf{B}}^2, ..., \widehat{\mathbf{A}}\widehat{\mathbf{B}}^{n-1} \right\}, \end{aligned}$$

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

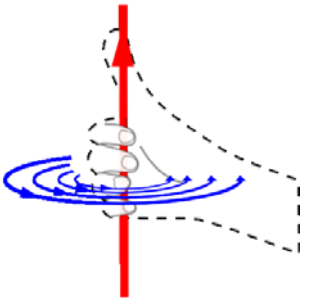
$$\widehat{\mathbf{A}}^2 = \widehat{\mathbf{B}}^n = \mathbf{I}_3, \quad \widehat{\mathbf{B}}\widehat{\mathbf{A}} = \widehat{\mathbf{A}}\widehat{\mathbf{B}}^{-1}\ (= \widehat{\mathbf{A}}\widehat{\mathbf{B}}^{n-1}). \tag{3.20}$$

Επιπροσθέτως, $\left|\Pi\epsilon\rho.\Sigma\upsilon\mu\mu(\widehat{P}_n)\right| = 2n$. 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

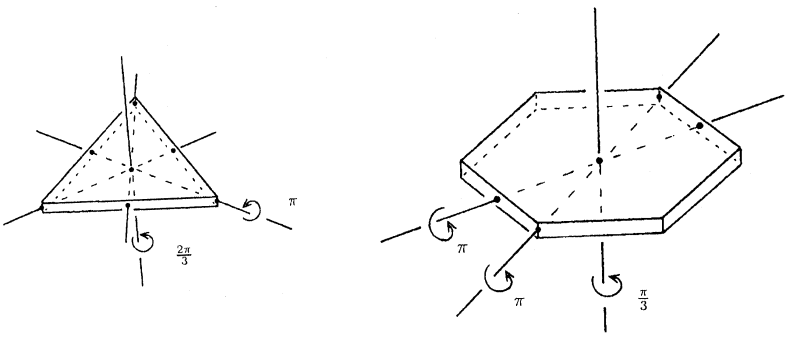
$$\mathbb{R}^3 \ni \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \widehat{\mathbf{A}}\,\widehat{\mathbf{B}}^k \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3, \quad k \in \{0,1,...,n-1\},$$

όπου

$$\widehat{\mathbf{A}}\,\widehat{\mathbf{B}}^k = \begin{pmatrix} \cos(\frac{2(n-k)\pi}{n}) & \sin(\frac{2(n-k)\pi}{n}) & 0 \\ \sin(\frac{2(n-k)\pi}{n}) & -\cos(\frac{2(n-k)\pi}{n}) & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

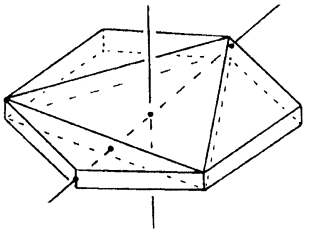
παριστούν *στροφές* τού $\mathbb{R}^3$ κατά π ακτίνια περί τις ευθείες, ως προς τις οποίες εκτελούνται οι n κατοπτρισμοί τού P_n (και τις οποίες έχουμε ήδη περιγράψει διεξοδικώς σε ό,τι προηγήθηκε). Στα κάτωθι σχήματα υποδηλούνται οι στροφές τού $\mathbb{R}^3$ οι επαγόμενες μέσω των πινάκων $\widehat{\mathbf{A}}, \widehat{\mathbf{B}}$ 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 αυτά τα σχήματα είναι δυνατόν να «συνδυασθούν» προκειμένου να δοθεί μια *γεωμετρική* απόδειξη για το ότι[17]

$$\text{Περ.Συμμ}(\widehat{P}_3) \sqsubset \text{Περ.Συμμ}(\widehat{P}_6).$$



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 (3.18)) είναι ισομορφισμός ομάδων, οπότε

$$\boxed{\mathbf{D}_n \cong \text{Συμμ}(P_n) \cong \text{Περ.Συμμ}(\widehat{P}_n).}$$

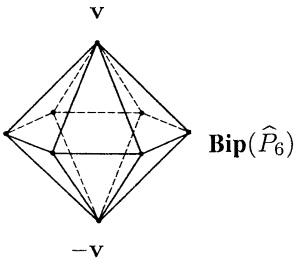
Τέλος, εάν κανείς επιθυμεί να αποκτήσει ένα «καθαρόαιμο» πολύεδρο, οι περιστροφικές συμμετρίες τού οποίου δομούν μια ομάδα ισόμορφη με την $\mathbf{D}_n$, αρκεί να θεωρήσει τη *διπλή πυραμίδα* $\textbf{Bip}(\widehat{P}_n)$ που σχηματίζεται ενώνοντας ένα σημείο $\mathbf{v} = (0,0,\lambda)$, $\lambda \in \mathbb{R}_{>0} \setminus \{1\}$, 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

[17] Γενικότερα, $\text{Περ.Συμμ}(\widehat{P}_n) \sqsubset \text{Περ.Συμμ}(\widehat{P}_{2n})$ *για κάθε* $n \geq 3$.

περίπτωση όπου $\lambda = 1$ και $n = 4$, η διπλή πυραμίδα $\mathbf{Bip}(\widehat{P}_4)$ είναι ένα *κανονικό οκτάεδρο*, η ομάδα περιστροφικών συμμετριών τού οποίου είναι ισόμορφη με την ομάδα $\mathfrak{S}_4 \ncong \mathbf{D}_4$.]



3.4.6 Παρατήρηση. Η πρόταση 3.4.7 και το πόρισμα 3.4.8 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.

3.4.7 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 $n \geq 3$ και $(G, \cdot) \cong (\mathbf{D}_n, \circ)$.

ΑΠΟΔΕΙΞΗ. 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. 2.2.17.) Σύμφωνα με την πρόταση 2.2.3,

$$G = \{x_1^{\varepsilon_1} \cdots x_\nu^{\varepsilon_\nu} \mid (x_1, .., x_\nu) \in \{s, t\}^\nu \text{ και } \varepsilon_\varrho \in \mathbb{Z},\ \forall \varrho \in \{1, .., \nu\}, \nu \in \mathbb{N}\}\,.$$

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 $k \geq 1$. 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 $(q, r) \in \mathbb{Z}^2 : k = nq + r$, $0 \leq r < n$ (βλ.

θεώρημα Β.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

$$G = \left\{ s^j t^k \,|j \in \{0,1\}\ ,\ k \in \{0,1,...,n-1\} \right\}. \tag{3.21}$$

Δεύτερος ισχυρισμός: $n \geq 3$. 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 (3.21) *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 $t^{k_2} = s^{-j_2} s^{j_2} t^{k_2} = s^{-j_2} s^{j_1} t^{k_1} \Rightarrow s^{j_1 - j_2} = t^{k_2 - k_1} \Rightarrow t^{k_2-k_1} \in \{e_G, s\}$. Στην περίπτωση κατά την οποία $t^{k_2-k_1} = e_G$, έχουμε

$$\left.\begin{array}{r} \mathrm{ord}(t) = n \underset{2.3.8}{\Longrightarrow} n \mid k_2 - k_1 \\ |k_2 - k_1| < n \end{array}\right\} \Rightarrow k_2 - k_1 = 0 \Rightarrow k_1 = k_2$$

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

$$(s^{j_1} t^{k_1})(s^{j_2} t^{k_2}) = \begin{cases} t^{k_1+k_2}, & \text{όταν} \ \ j_1 = j_2 = 0, \\ s t^{k_1+k_2}, & \text{όταν} \ \ j_1 = 1,\ j_2 = 0, \\ t^{k_1} s t^{k_2} = s t^{k_2-k_1}, & \text{όταν} \ \ j_1 = 0,\ j_2 = 1, \\ s\left(t^{k_1} s\right) t^{k_2} = t^{k_2-k_1}, & \text{όταν} \ \ j_1 = j_2 = 1, \end{cases}$$

οπότε η εικόνα τού γινομένου δυο στοιχείων τής G μέσω αυτής ισούται με τη σύνθεση των εικόνων τους. Κατά συνέπειαν, $(G, \cdot) \cong (\mathbf{D}_n, \circ)$. □

3.4.8 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 $n \geq 3$ και $(G, \cdot) \cong (\mathbf{D}_n, \circ)$.

ΑΠΟΔΕΙΞΗ. 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. 2.2.17.) 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 3.4.7 για τους γεννήτορες s, t τής ομάδας G. □

► **Από την πεπερασμένη στην άπειρη διεδρική ομάδα**. Αντικαθιστώντας τόν γεννήτορα t που παρατίθεται στην πρόταση 3.4.7 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.

3.4.9 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. 2.1.16 (iii).)

3.4.10 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 $a \in \mathbb{R}$.

3.4.11 Λήμμα. *Το σύνολο*

$$\boxed{\mathrm{Trans}(\mathbb{R}) := \{T_a \,|a \in \mathbb{R}\} \subseteq \mathrm{Isom}(\mathbb{R}),}$$

όλων των μεταφορών τού $\mathbb{R}$ συγκροτεί μια άπειρη αβελιανή υποομάδα τής $\mathrm{Isom}(\mathbb{R})$. *Επιπροσθέτως,* $(\mathrm{Trans}(\mathbb{R}), \circ) \cong (\mathbb{R}, +)$.

ΑΠΟΔΕΙΞΗ. 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 απεικόνιση $\mathbb{R} \ni a \mapsto T_a \in \mathrm{Trans}(\mathbb{R})$ αποτελεί ισομορφισμό ομάδων. □

3.4.12 Συμβολισμός. Με το γράμμα S θα συμβολίσουμε τον *κατοπτρισμό*

$$S : \mathbb{R} \longrightarrow \mathbb{R}, \;\; x \longmapsto S(x) := -x,$$

τού $\mathbb{R}$ ως προς το 0.

3.4.13 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,

$$\begin{aligned} \mathrm{Isom}(\mathbb{R}) &= \mathrm{Trans}(\mathbb{R}) \cup \{T_a \circ S \,|a \in \mathbb{R}\} = \{T_a \,|a \in \mathbb{R} \cup \{T_a \circ S \,|a \in \mathbb{R}\} \\ &= \{\sigma \in \mathfrak{S}_{\mathbb{R}} | \, \exists a \in \mathbb{R} \text{ και } \exists \varepsilon \in \{\pm 1\} : \sigma(x) = \varepsilon x + a, \forall x \in \mathbb{R}\} \\ &= \{S^j \circ T_{-a} \big| \, a \in \mathbb{R} \text{ και } j \in \{0, 1\}\}. \end{aligned}$$

ΑΠΟΔΕΙΞΗ. 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 για κάθε $x \in \mathbb{R} \setminus \{0\}$,

$$|(T_{-a} \circ \sigma)(x)| = |(T_{-a} \circ \sigma)(x) - (T_{-a} \circ \sigma)(0)| = |x - 0| = |x|.$$

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 $\mathbb{R}$. □

3.4.14 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 3.4.15, 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.)

3.4.15 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 $T_{-1} \circ S = S \circ {T_{-1}}^{-1}\ (= S \circ T_1)$.

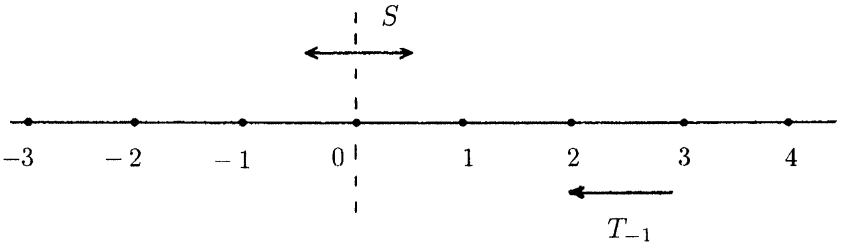
ΑΠΟΔΕΙΞΗ. Έστω τυχούσα ισομετρία $\sigma \in \mathbf{D}_\infty$. Προφανώς, $\sigma\,(0) =: k \in \mathbb{Z}$. Κατά την πρόταση 3.4.13, $\exists j \in \{0,1\} : \sigma = S^j \circ T_{-k}$, όπου

$$T_{-k} = \begin{cases} T_{-1}^k, & \text{όταν} \quad k \geq 0, \\ T_1^{-k}, & \text{όταν} \quad k < 0. \end{cases}$$

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. □



3.4.16 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[18], 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:

[18] 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 $S(T_{-1}^k(x)) = x \Leftrightarrow x = \frac{k}{2}$.

3.4.17 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 $(G,\cdot) \cong (\mathbf{D}_\infty, \circ)$.

ΑΠΟΔΕΙΞΗ. 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. 2.2.17.) Σύμφωνα με την πρόταση 2.2.3,

$$G = \{x_1^{\varepsilon_1} \cdots x_\nu^{\varepsilon_\nu} \mid (x_1,..,x_\nu) \in \{s,t\}^\nu \text{ και } \varepsilon_\varrho \in \mathbb{Z},\ \forall \varrho \in \{1,..,\nu\}, \nu \in \mathbb{N}\}\,.$$

Στηριζόμενοι στην ισότητα $ts = st^{-1}$ αποδεικνύουμε επαγωγικώς ότι

$$t^k s = st^{-k},\ \forall k \in \mathbb{Z}.$$

Επειδή $s \neq e_G, s^2 = e_G \Rightarrow \text{ord}(s) = 2$, συμπεραίνουμε τελικώς ότι

$$G = \left\{t^k \ | k \in \mathbb{Z}\right\} \cup \left\{st^k \,| k \in \mathbb{Z}\right\}.$$

(Η άπειρη κυκλική ομάδα $\langle t\rangle$ είναι υποομάδα τής G). Είναι εύκολο να ελεγχθεί ότι η απεικόνιση $G \ni s^j t^k \longmapsto S^j \circ T_{-1}^k \in \mathbf{D}_\infty,\ j \in \{0,1\},\ k \in \mathbb{Z}$, αποτελεί ισομορφισμό ομάδων. □

3.5 ΤΟ ΘΕΩΡΗΜΑ ΤΟΥ CAYLEY

Η σημασία των ομάδων μετατάξεων στη Θεωρία Ομάδων παρεμφαίνεται στο ακόλουθο:

3.5.1 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. 2.4.14 και 2.4.17).

ΑΠΟΔΕΙΞΗ. 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 2.1.16. Η απεικόνιση

$$G \longrightarrow L(G), \quad g \longmapsto L_g,$$

είναι προφανώς επιρριπτική 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 $\mathfrak{S}_G$. □

3.5.2 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,

$$\boxed{L(G) \cong G \cong R(G).}$$

3.5.3 Πόρισμα. *Εάν η G είναι μια πεπερασμένη ομάδα τάξεως n, τότε η G είναι εμφυτεύσιμη*

(i) *στη συμμετρική ομάδα $\mathfrak{S}_n$ και*

(ii) *στις γενικές γραμμικές ομάδες $\mathrm{GL}_n(\mathbb{Z})$ και $\mathrm{GL}_n(F)$, όπου F τυχόν σώμα.*

ΑΠΟΔΕΙΞΗ. (i) Εάν, κατά κάποιον τρόπο, αριθμήσουμε τα στοιχεία τής G ως $1, 2, ..., n$, δηλαδή εάν ορίσουμε μια αμφίριψη $f : G \longrightarrow \{1, 2, ..., n\}$, τότε κάθε μετάταξη τής G επάγει μια μετάταξη των $1, 2, ..., n$ 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. 2.4.12 (ii)), η G είναι ισόμορφη με την $\Phi_f(L(G))$.

(ii) Η ομάδα $\Phi_f(L(G))$ είναι ισόμορφη με την εικόνα της μέσω τού μονομορφισμού $\tau \longmapsto \mathbf{P}_\tau$ (όπου $\mathbf{P}_\tau$ είναι ο μετατακτικός πίνακας ο οριζόμενος μέσω τής τ, ο ανήκων στην $\mathrm{GL}_n(\mathbb{Z})$ και, αντιστοιχώς, στην $\mathrm{GL}_n(F)$). Βλ. D.2.27 και D.2.28 (i). □

3.5.4 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 3.5.1 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, $\Phi_f(L_g) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} = [1\,2\,3\,4]$. Κατ' αναλογίαν,

$$\Phi_f(L_{g^2}) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} = [1\,3] \circ [2\,4]\,, \;\; \Phi_f(L_{g^3}) = [1\,4\,3\,2].$$

Άρα η G είναι ισόμορφη με την υποομάδα

$$\Phi_f(L(G)) = \{\mathrm{id}, [1\,2\,3\,4], [1\,3] \circ [2\,4]\,, [1\,4\,3\,2]\}$$

τής $\mathfrak{S}_4$ (και φυσικά και με την ομάδα $(\mathbb{Z}_4, +)$ επί τη βάσει τού (ii) τού θεωρήματος 2.4.23). Επίσης, η $G \cong \Phi_f(L(G))$ (κατά το 3.5.3 (ii)) είναι ισόμορφη με την υποομάδα

$$\left\{ \mathbf{I}_4, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right\}$$

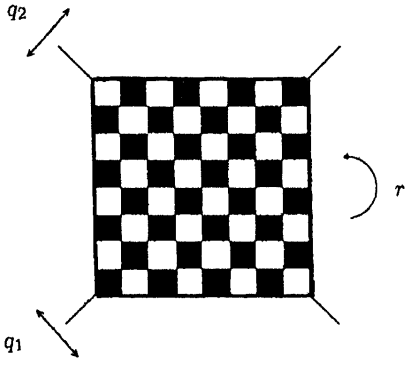
τής $\mathrm{GL}_4(\mathbb{Z})$ και με την υποομάδα

$$\left\{ \mathbf{I}_4, \begin{pmatrix} 0_F & 0_F & 0_F & 1_F \\ 1_F & 0_F & 0_F & 0_F \\ 0_F & 1_F & 0_F & 0_F \\ 0_F & 0_F & 1_F & 0_F \end{pmatrix}, \begin{pmatrix} 0_F & 0_F & 1_F & 0_F \\ 0_F & 0_F & 0_F & 1_F \\ 1_F & 0_F & 0_F & 0_F \\ 0_F & 1_F & 0_F & 0_F \end{pmatrix}, \begin{pmatrix} 0_F & 1_F & 0_F & 0_F \\ 0_F & 0_F & 1_F & 0_F \\ 0_F & 0_F & 0_F & 1_F \\ 1_F & 0_F & 0_F & 0_F \end{pmatrix} \right\}$$

τής $\mathrm{GL}_4(F)$ για κάθε σώμα F. Τέλος, αξίζει να επισημανθεί ότι, ορίζοντας ως f μια *άλλη* αμφίρριψη μεταξύ τής G και τού $\{1,2,3,4\}$, λαμβάνουμε μια *άλλη* εμφύτευση τής G εντός τής $\mathfrak{S}_4$. Επί παραδείγματι, εάν ορισθεί ως $f : G \longrightarrow \{1,2,3,4\}$ η αμφίρριψη με $f(e) := 1$, $f(g) := 3$, $f(g^2) := 2$ και $f(g^3) := 4$, τότε

$$\Phi_f(L(G)) = \{\mathrm{id}, [1\,3\,2\,4], [1\,2] \circ [3\,4]\,, [1\,4\,3\,2]\}.$$

3.5.5 Παράδειγμα. (Επίπεδες συμμετρίες μιας σκακιέρας) Μια σκακιέρα διαθέτει τέσσερεις επίπεδες συμμετρίες[19]: 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 σύν-

[19] 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.

θεση 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

Σύμφωνα με το θεώρημα 3.5.1 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 3.4.2 (ii) των τεσσάρων στοιχείων τού Klein και $G \cong \mathbf{V}$. Επίσης, η G (κατά το 3.5.3 (ii)) είναι ισόμορφη με την υποομάδα

$$\left\{ \mathbf{I}_4, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right\}$$

τής $\mathrm{GL}_4(\mathbb{Z})$ και με την υποομάδα

$$\left\{ \mathbf{I}_4, \begin{pmatrix} 0_F & 1_F & 0_F & 0_F \\ 1_F & 0_F & 0_F & 0_F \\ 0_F & 0_F & 0_F & 1_F \\ 0_F & 0_F & 1_F & 0_F \end{pmatrix}, \begin{pmatrix} 0_F & 0_F & 1_F & 0_F \\ 0_F & 0_F & 0_F & 1_F \\ 1_F & 0_F & 0_F & 0_F \\ 0_F & 1_F & 0_F & 0_F \end{pmatrix}, \begin{pmatrix} 0_F & 0_F & 0_F & 1_F \\ 0_F & 0_F & 1_F & 0_F \\ 0_F & 1_F & 0_F & 0_F \\ 1_F & 0_F & 0_F & 0_F \end{pmatrix} \right\}$$

τής $\mathrm{GL}_4(F)$ για κάθε σώμα F.

Το θεώρημα 3.5.6 μας πληροφορεί ότι *κάθε* ομάδα *τάξεως* 4 οφείλει να είναι ισόμορφη με μία εκ των ομάδων μετατάξεων που παρουσιάσθηκαν στα παραδείγματα 3.5.4 και 3.5.5.

3.5.6 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.*

ΑΠΟΔΕΙΞΗ. (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 2.3.7 και 2.2.17).

(β) Εάν η G έχει δεν έχει κανένα στοιχείο τάξεως 4, τότε η G δεν είναι κυκλική (βλ. πρόταση 2.3.7). 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 2.1.9 (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, $\text{ord}(a) = 2$. Εναλλάσσοντας τώρα τους ρόλους των a και b, και επιχειρηματολογώντας αναλόγως, αποδεικνύουμε την ισότητα $\text{ord}(b) = 2$.

Εξέταση τού γινομένου ab. Είτε $ab = e$ είτε $ab = c$. Εάν $ab = e$, τότε $b = a^{-1} = a$ (αφού $\text{ord}(a) = 2$, 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 2.4.23.

(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 $\text{ord}(a) = \text{ord}(b) = 2$ (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[20]:

$\cdot$	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 3.5.5 (με τα a, b, ab στη θέση των r, q_1 και q_2, αντιστοίχως) είτε ορίζουμε απευθείας την απεικόνιση

$$e \longmapsto \text{id},\ \ a \longmapsto [1\,2] \circ [3\,4]\,,\ \ b \longmapsto [1\,3] \circ [2\,4]\,,\ \ ab \longmapsto [1\,4] \circ [2\,3]$$

και διαπιστώνουμε ότι είναι ισομορφισμός ομάδων. □

3.5.7 Παρατήρηση. Προφανώς, $(\mathbf{V}, \circ) \ncong (\mathbb{Z}_4, +)$ (βλ. 2.4.19 (iii)).

[20] Εξ αυτού έπεται, ιδιαιτέρως, ότι $G = \langle a, b\rangle = \langle a, ab\rangle = \langle b, ab\rangle$.

3.5.8 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* $(\mathrm{Aut}(G),\circ)\cong(\mathfrak{S}_3,\circ)$.

ΑΠΟΔΕΙΞΗ. (i) Η ύπαρξη τού πρώτου ισομορφισμού διασφαλίζεται μέσω τού (ii) τού θεωρήματος 2.4.32. 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 2.4.23 (ii).
(ii) Εάν η ομάδα $(G,\cdot)$ δεν είναι κυκλική, τότε $(G,\cdot)\cong(\mathbf{V},\circ)$ (σύμφωνα με το θεώρημα 3.5.6), όπου $\mathbf{V}:=\{\mathrm{id},\sigma_1,\sigma_2,\sigma_3\}$ με

$$\sigma_1:=[1\,2]\circ[3\,4]\,,\ \ \sigma_2:=[1\,3]\circ[2\,4]\,,\ \ \sigma_3:=[1\,4]\circ[2\,3]\,.$$

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. 2.4.3 (i)) και, ως εκ τούτου,

$$\{\vartheta(\sigma_1),\vartheta(\sigma_2),\vartheta(\sigma_3)\}=\{\sigma_1,\sigma_2,\sigma_3\}$$

με

$$\vartheta(\sigma_j\circ\sigma_k)=\vartheta(\sigma_j)\circ\vartheta(\sigma_k)\,,\ \forall(j,k)\in\{1,2,3\}\times\{1,2,3\}.\tag{3.22}$$

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 αυτομορφισμού $\vartheta\in\mathrm{Aut}(\mathbf{V})$ είναι η $\vartheta(\mathrm{id})=\mathrm{id}$, αφού η (3.22) πληρούται *αυτομάτως* για οιαδήποτε $(j,k)\in\{1,2,3\}\times\{1,2,3\}$. 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 $j\in\{1,2,3,4,5\}$,

$$\begin{array}{c}\vartheta_1(\sigma_1):=\sigma_1,\ \vartheta_1(\sigma_2):=\sigma_3,\ \vartheta_1(\sigma_3):=\sigma_2,\\ \vartheta_2(\sigma_1):=\sigma_2,\ \vartheta_2(\sigma_2):=\sigma_1,\ \vartheta_2(\sigma_3):=\sigma_3,\\ \vartheta_3(\sigma_1):=\sigma_2,\ \vartheta_3(\sigma_2):=\sigma_3,\ \vartheta_3(\sigma_3):=\sigma_1,\\ \vartheta_4(\sigma_1):=\sigma_3,\ \vartheta_4(\sigma_2):=\sigma_1,\ \vartheta_4(\sigma_3):=\sigma_2\end{array}$$

και $\vartheta_5(\sigma_1):=\sigma_3,\ \vartheta_5(\sigma_2):=\sigma_2,\ \vartheta_5(\sigma_3):=\sigma_1$. □

Ασκήσεις

3-1. Για οιοδήποτε μη κενό σύνολο A και για οιοδήποτε στοιχείο $a \in A$ να αποδειχθεί ότι το $\{\sigma \in \mathfrak{S}_A | \, \sigma(a) = a\}$ αποτελεί μια υποομάδα τής $(\mathfrak{S}_A, \circ)$.

3-2. Εάν $m \in \mathbb{N}, k \in \mathbb{Z}$ και $\sigma : \mathbb{Z}_m \longrightarrow \mathbb{Z}_m$ η απεικόνιση $[l]_m \longmapsto \sigma([l]_m) := [kl]_m$, να αποδειχθεί ότι $\sigma \in \mathfrak{S}_{\mathbb{Z}_m} \iff \text{μκδ}(k, m) = 1$.

3-3. (i) Εάν $(G, \cdot)$ είναι μια αβελιανή ομάδα, a, b στοιχεία τής G,και $l, m, n \in \mathbb{N}$, για τους οποίους ισχύει $\text{μκδ}(l, m) = \text{μκδ}(m, n) = \text{μκδ}(n, l) = 1$, να αποδειχθεί η συνεπαγωγή $\left[a^l = b^m = (ab)^n = e_G\right] \Longrightarrow a = b = e_G$.

(ii) Παραμένει αυτό το συμπέρασμα εν ισχύ ακόμη και όταν η G είναι μη αβελιανή;

3-4. (i) Να υπολογισθούν οι συνθέσεις των ακολούθων μετατάξεων εντός τής $\mathfrak{S}_6$

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 5 & 6 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 6 & 5 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 2 & 1 & 6 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \end{bmatrix}^3, \quad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 1 & 2 & 3 \end{bmatrix}^5,$$

καθώς και τα αντίστροφα αυτών.

(ii) Να εκφρασθεί η μετάταξη

$$\sigma := \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 9 & 8 & 4 & 5 & 7 & 11 & 1 & 2 & 6 & 10 \end{bmatrix} \in \mathfrak{S}_{11}$$

υπό τη μορφή επαλλήλων συνθέσεων ανά δύο ξένων μεταξύ τους κύκλων μήκους ≥ 2 και να υπολογισθεί η τάξη της.

3-5. Να αποδειχθεί ότι εντός τής συμμετρικής ομάδας $\mathfrak{S}_6$ οι συνθέσεις κύκλων

$$[1\ 4\ 5\ 6] \circ [2\ 1\ 5]\,, \ [2\ 1\ 5] \circ [1\ 4\ 5\ 6]$$

είναι δύο (άνισες) μετατάξεις που δεν είναι κύκλοι.

3-6. Εάν $n \in \mathbb{N}$, $n \geq 2$, και $\sigma \in \mathfrak{S}_n$ με $\sigma(i) \neq i$ για κάποιον $i \in \{1, ..., n\}$, να αποδειχθεί ότι $\sigma^2(i) \neq \sigma(i)$.

3-7. Εάν $\tau := [1\ 2\ 3\ 4] \in \mathfrak{S}_4$, να προσδιορισθούν όλες οι μετατάξεις $\sigma \in \mathfrak{S}_4$ για τις οποίες ισχύει η ισότητα $\sigma \circ \tau \circ \sigma^{-1} = \tau^3$.

3-8. Να προσδιορισθούν οι μετατάξεις σ_1, σ_2 εντός τής συμμετρικής ομάδας $\mathfrak{S}_7$ για τις οποίες οι ισότητες $\sigma_1 \circ \varrho = \tau = \varrho \circ \sigma_2$, όπου

$$\varrho := \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 3 & 4 & 7 & 6 & 1 \end{bmatrix}, \ \tau := \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 7 & 6 & 3 & 5 \end{bmatrix}.$$

3-9. Δίδονται οι μετατάξεις

$$\sigma := \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 9 & 2 & 1 & 4 & 3 & 6 & 7 \end{bmatrix} \in \mathfrak{S}_9$$

και

$$\tau := \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & ... & 3n-2 & 3n-1 & 3n \\ 2 & 3 & 1 & 5 & 6 & 4 & ... & 3n-1 & 3n & 3n-2 \end{bmatrix} \in \mathfrak{S}_{3n},\ n \in \mathbb{N}.$$

Να εκφρασθούν οι σ και τ υπό τη μορφή επαλλήλων συνθέσεων (πεπερασμένου πλήθους) ανά δύο ξένων μεταξύ τους κύκλων μήκους ≥ 2. Εν συνεχεία, να εξετασθεί εάν οι σ και τ είναι άρτιες ή περιττές.

3-10. Να προσδιορισθεί η $\sigma^{1000} = \underbrace{\sigma \circ \sigma \circ \cdots \circ \sigma}_{1000 \text{ φορές}}$ όταν

$$\sigma := \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 8 & 9 & 4 & 5 & 2 & 1 & 6 \end{bmatrix} \in \mathfrak{S}_9.$$

3-11. Εάν $n \in \mathbb{N}$, $n \geq 3$, και $\sigma_1, \sigma_2 \in \mathfrak{S}_n$ είναι δυο αντιμεταθέσεις, να αποδειχθεί ότι η μετάταξη $\sigma_1 \circ \sigma_2$ μπορεί να γραφεί ως σύνθεση (όχι κατ' ανάγκην ανά δύο ξένων μεταξύ τους) κύκλων μήκους 3.

3-12. Έστω $n \in \mathbb{N}$, $n \geq 4$, και έστω p ένας πρώτος αριθμός. Να αποδειχθούν τα ακόλουθα:

(i) Η τάξη μιας μετατάξεως $\sigma \in \mathfrak{S}_n$ είναι ίση με p εάν και μόνον η σ γράφεται ως σύνθεση επαλλήλων ανά δύο ξένων μεταξύ τους p-κύκλων.

(ii) Το (i) δεν είναι εν γένει αληθές εάν σε αυτό ο πρώτος αριθμός p αντικατασταθεί με έναν σύνθετο αριθμό.

3-13. Εάν $m, n \in \mathbb{N}$ με $m \mid n$ και $\sigma \in \mathfrak{S}_n$ είναι ένας n-κύκλος, να αποδειχθεί ότι η μετάταξη $\sigma^m = \underbrace{\sigma \circ \cdots \circ \sigma}_{m \text{ φορές}}$ γράφεται ως σύνθεση m επαλλήλων ανά δύο ξένων μεταξύ τους $\frac{n}{m}$-κύκλων.

3-14. Εάν $n \in \mathbb{N}$, $n \geq 3$, και $\sigma \in \mathfrak{S}_n$, να αποδειχθεί ότι

$$\mathfrak{S}_n = \langle [\sigma(1)\ \ \sigma(2)], [\sigma(1)\, \sigma(2) ... \, \sigma(n)] \rangle\,.$$

3-15. Να αποδειχθεί ότι για κάθε $\sigma \in \mathfrak{S}_5 \setminus \{\mathrm{id}\}$ υπάρχει κάποια μετάταξη $\tau \in \mathfrak{S}_5$, τέτοια ώστε να ισχύει $\mathfrak{S}_5 = \langle \sigma, \tau \rangle$.

3-16. Εάν $n \in \mathbb{N}$ και $\tau := [1\, 2 ... \, n] \in \mathfrak{S}_n$, να αποδειχθεί ότι για κάθε $\sigma \in \mathfrak{S}_n$ ισχύει

$$\sigma \circ \tau = \tau \circ \sigma \iff \sigma \in \langle \tau \rangle\,.$$

3-17. Στο γνωστό «παιχνίδι[21] των 15 (τετράγωνων) πλακιδίων», καθένα εκ των 15 πλακιδίων είναι τοποθετημένο σε ένα τετράγωνο πλαίσιο με πλευρά που είναι τετραπλάσια τής πλευράς του. Τα πλακίδια εφάπτονται μεταξύ τους κατά τέτοιον τρόπο, ώστε εντός τού τετραγώνου πλαισίου να αφήνεται κενό το κάτω-δεξιά τετραγωνίδιο, αριθμούνται δε από το 1 έως το 15 όπως στο σχήμα:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

(Στο κενό τετραγωνίδιο θα αντιστοιχεί *νοερώς* ο αριθμός 16.) Τα πλακίδια μπορούν να μετακινούνται οριζοντίως ή κατακορύφως (κάνοντας χρήση τού εκάστοτε εμφανιζόμενου κενού τετραγωνιδίου) χωρίς, όμως, να μπορούν να «ξεκαρφιτσωθούν» από το τετράγωνο πλαίσιο. (Μια **απλή μετακίνηση** είναι εξ ορισμού το αποτέλεσμα τού να συρθεί κάποιο πλακίδιο σε κενό τετραγωνίδιο, απ' όπου προκύπτει η αλλαγή τής αρχικής θέσεως τού κενού τετραγωνιδίου οριζοντίως ή κατακορύφως σε μια γειτονική θέση.) Συγκεκριμένα, εκκινώντας από το ανωτέρω σχήμα, ως **επιτρεπτές μετακινήσεις** (τού παιχνιδιού) χαρακτηρίζονται όλες οι δυνατές επίπεδες μετακινήσεις (ήτοι αναδιατάξεις) των πλακιδίων, οι οποίες προκύπτουν ύστερα από εφαρμογή πεπερασμένου πλήθους απλών μετακινήσεων, υπό την προϋπόθεση ότι το κάτω-δεξιά τετραγωνίδιο παραμένει (στο τέλος) κενό. Το αποτέλεσμα κάθε επιτρεπτής μετακινήσεως είναι οι τοποθετήσεις των αριθμών $1, 2, ..., 15$ σε νέες θέσεις $\sigma(1), \sigma(2), ..., \sigma(15)$, για κάποια μετάταξη $\sigma \in \mathfrak{S}_{16}$, για την οποία ισχύει $\sigma(16) = 16$, όπως στο σχήμα:

σ(1)	σ(2)	σ(3)	σ(4)
σ(5)	σ(6)	σ(7)	σ(8)
σ(9)	σ(10)	σ(11)	σ(12)
σ(13)	σ(14)	σ(15)	

Για το σύνολο H όλων των επιτρεπτών μετακινήσεων να αποδειχθούν τα εξής:

(i) $H \sqsubseteq \mathfrak{S}_{16}$, (ii) $\exists K \sqsubseteq \mathfrak{A}_{15} : K \cong H$ και (iii) $K = \mathfrak{A}_{15}$.

[21] Παρά το γεγονός ότι αυτό το παιχνίδι έχει συνδεθεί με το όνομα τού Αμερικανού (σκακιστή και συλλέκτη puzzles) Sam Loyd (1841-1911), είχε επινοηθεί (με κάποιους περιορισμούς ως προς τους αριθμούς) το 1874 από τον Noyes Palmer Chapman, έναν νεοϋορκέζο διευθυντή ταχυδρομείου και μετεξελιχθεί από τον γιο του Frank. Το τετράγωνο πλαίσιο με τους αριθμούς 1 έως το 15 άρχισε να παράγεται και να πωλείται στο Connecticut και στη Βοστώνη το 1879. Οι πωλήσεις του (και η υστερία για το παίξιμό του) αυξήθηκαν εκθετικώς έναν χρόνο αργότερα, το 1880, τόσο στις Η.Π.Α. όσο και στην Ευρώπη. Για περισσότερα ιστορικά στοιχεία και όμορφες εικόνες, βλ. J. Slocum & D. Sonneveld: *The 15-Puzzle. How It Drove The World Crazy*, Beverly Hills, CA, Slocum Puzzle Foundation, 2006.

(Ως εκ τούτου, είθισται να «ταυτίζει» κανείς την ομάδα H με την εναλλάσσουσα ομάδα[22] $\mathfrak{A}_{15}$ που έχει τάξη[23] $|\mathfrak{A}_{15}| = \frac{15!}{2} = 65383718400$.)

3-18. Να αποδειχθούν τα ακόλουθα:

(i) Οι ομάδες G_1, G_2 τής ασκήσεως **2-53** είναι ισόμορφες με την $\mathbf{D}_3 (\cong \mathfrak{S}_3)$.

(ii) Οι ομάδες $\mathbf{D}_4$ και $\mathbf{Heis}(\mathbb{Z}_2)$ είναι ισόμορφες.

3-19. Έστω $n \in \mathbb{N}$, $n \geq 3$. Να αποδειχθεί ότι $G_n \cong \mathbf{D}_n \cong H_n$, όπου

$$G_n := \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \zeta_n & 0 \\ 0 & \zeta_n^{-1} \end{pmatrix} \right\rangle \sqsubseteq \mathbf{GL}_2(\mathbb{C})$$

(με $\zeta_n := \exp\left(\frac{2\pi i}{n}\right)$) και

$$H_n := \left\{ \begin{pmatrix} [\varepsilon]_n & [\lambda]_n \\ [0]_n & [1]_n \end{pmatrix} \middle| \, \varepsilon \in \{\pm 1\}\,,\ \lambda \in \mathbb{Z} \right\} \sqsubseteq \mathbf{GL}_2(\mathbb{Z}_n).$$

3-20. Να αποδειχθεί ότι η $\mathbf{D}_\infty$ είναι ισόμορφη με την ομάδα

$$G := \left\{ \begin{pmatrix} \varepsilon & \lambda \\ 0 & 1 \end{pmatrix} \middle| \, \varepsilon \in \{\pm 1\}\,,\ \lambda \in \mathbb{Z} \right\} \sqsubseteq \mathbf{GL}_2(\mathbb{Z}).$$

---

[22] Μέσω αυτού τού συμπεράσματος είναι πλέον εμφανές γιατί η εικασία τού Sam Loyd (ότι υπάρχουν επιτρεπτές μετακινήσεις, το αποτέλεσμα των οποίων εναλλάσσει τις θέσεις των αριθμών 14 και 15 και αφήνει τους υπολοίπους στις αρχικές τους θέσεις) είναι εσφαλμένη. (Για γενικεύσεις τού παιχνιδιού των 15 πλακιδίων μέσω τής Θεωρίας Γραφημάτων πρβλ. R.M. Wilson: *Graph puzzles, homotopy, and the alternating group*, J. Combin. Theory Ser. B, **16** (1974), 86-96, και C.Yang: *Sliding puzzles and rotating puzzles on graphs*, Discrete Mathematics **311**, Issue **14** (2011), 1290-1294.)

[23] Πρόκειται για έναν *τεράστιο αριθμό*. (Σημειωτέον, ότι όλα τα πιθανά αποτελέσματα μιας κληρώσεως τού «Τζόκερ» είναι «μόλις» 13983816.) Από την άλλη μεριά, εάν ως σκοπός τού παιχνιδιού ορισθεί *η επαναφορά των πλακιδίων στην αρχική τους θέση* (με την αρχική αρίθμηση) ύστερα από τη μεσολάβηση οιασδήποτε *επιτρεπτής αναδιατάξεως* αυτών (ήτοι ύστερα από τη μεσολάβηση τής εφαρμογής τυχούσας μετατάξεως $\sigma \in H$ στους $1, 2, \ldots, 15, 16$), τότε αποδεικνύεται (αλγοριθμικώς) ότι υφίστανται πάντοτε *αρκούντως σύντομες επαναφορές* που απαιτούν την εκτέλεση *το πολύ* 80 απλών μετακινήσεων. (Βλ. A. Bruengger, A. Marzetta, K. Fukuda and J. Nievergelt, *The parallel search bench ZRAM and its applications*, Annals of Operations Research **90** (1999), 45-63.)

ΚΕΦΑΛΑΙΟ 4

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* 4.1.22, μέσω ενός γενικότερου θεωρήματος που συνδέει την τάξη *οιασδήποτε* ομάδας με την τάξη μιας υποομάδας της (βλ. θεώρημα 4.1.20). Προς τούτο προαπαιτείται η παράθεση των ορισμών των *πλευρικών κλάσεων* και τού *δείκτη* υποομάδων. Εν συνεχεία, αποδεικνύεται η *απλότητα* τής $\mathfrak{A}_n$ για $n \geq 5$, ορίζονται *πηλικοομάδες* και αποδεικνύονται τα τρία χαρακτηριστικά *θεωρήματα ισομορφισμών ομάδων*, καθώς και το *θεώρημα τής αντιστοιχίσεως ορθόθετων υποομάδων*.

4.1 ΠΛΕΥΡΙΚΕΣ ΚΛΑΣΕΙΣ ΚΑΙ ΔΕΙΚΤΕΣ ΥΠΟΟΜΑΔΩΝ

4.1.1 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]

$$\boxed{AB := \{\, xy \mid x \in A \ \text{ και } \ y \in B\}.} \tag{4.1}$$

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.)

[1] Όταν χρησιμοποιείται *προσθετικός συμβολισμός* για την ομάδα G, τότε αντί τού συνόλου AB θεωρούμε το σύνολο $A + B := \{\, x + y \mid x \in A \ \text{ και } \ y \in B\}$.

4.1.2 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.*

(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,

$$\exists y\in B\ \ \text{και}\ \ \exists z\in C:g=xy=xz\underset{\text{2.1.9 (i)}}{\Longrightarrow}y=z\in B\cap C,$$

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 "$\cdot$". □

4.1.3 Σημείωση. Το σύνολο $\mathfrak{P}\,(G)\smallsetminus\{\varnothing\}$ των μη κενών υποσυνόλων τού υποκειμένου συνόλου G μιας ομάδας $(G,\cdot)$, εφοδιαζόμενο με την εσωτερική πράξη

$$(\mathfrak{P}\,(G)\smallsetminus\{\varnothing\})\times(\mathfrak{P}\,(G)\smallsetminus\{\varnothing\})\ni(A,B)\longmapsto AB\in\mathfrak{P}\,(G)\smallsetminus\{\varnothing\}$$

την ορισθείσα στην (4.1), καθίσταται μονοειδές έχον το μονοσύνολο $\{e_G\}$ ως ουδέτερό του στοιχείο.

4.1.4 Πρόταση. *Έστω ότι τα H και K είναι δυο υποομάδες μιας ομάδας $(G,\cdot)$. Τότε*[2]

$$\boxed{HK\sqsubseteq G\Longleftrightarrow HK=KH.}$$

[2]Προσοχή! Η ισότητα $HK=KH$ δεν σημαίνει ότι κάθε στοιχείο τής H μετατίθεται 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. "⇒": 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 2.1.16). Άρα $x^{-1} = a'b'$ για κάποια $a' \in H$ και $b' \in K$, και

$$\left.\begin{array}{r} x = \left(x^{-1}\right)^{-1} \Rightarrow x = (a'b')^{-1} = (b')^{-1}(a')^{-1} \\ b' \in K \Rightarrow (b')^{-1} \in K \ \text{ και } \ a' \in H \Rightarrow (a')^{-1} \in H \end{array}\right\} \Rightarrow x = (b')^{-1}(a')^{-1} \in KH.$$

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

$$\left.\begin{array}{r} a \in H \Rightarrow a^{-1} \in H \ \text{ και } \ b \in K \Rightarrow b^{-1} \in K \\ y^{-1} = (ba)^{-1} = a^{-1}b^{-1} \end{array}\right\} \Rightarrow y^{-1} \in HK.$$

Επειδή το HK υπετέθη ότι είναι υποομάδα τής G, έχουμε $\left(y^{-1}\right)^{-1} = y \in HK$. Άρα ισχύει και αντίστροφος εγκλεισμός $HK \supseteq KH$.

"⇐": 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 να ισχύουν οι ισότητες $x_1 = a_1 b_1$ 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,

$$\begin{aligned} x_1 x_2 &= (a_1 b_1)(a_2 b_2) \underset{1.2.19}{=} a_1 (b_1 a_2) b_2 \\ &= a_1 (a_3 b_3) b_2 \underset{1.2.19}{=} (\underbrace{a_1 a_3}_{\in H})(\underbrace{b_3 b_2}_{\in K}) \in HK. \end{aligned}$$

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 2.1.16, $HK \sqsubseteq G$. □

4.1.5 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 $\mathfrak{S}_3$.

4.1.6 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) $f^{-1}(f(K) * L) = K f^{-1}(L)$.

(ii) $f^{-1}(L * f(K)) = f^{-1}(L)K$.

(iii) $f^{-1}(f(K)) = K(\mathrm{Ker}(f)) = (\mathrm{Ker}(f))K$, *οπότε* $K(\mathrm{Ker}(f)) \sqsubseteq G$.

ΑΠΟΔΕΙΞΗ. (i) Από το (ii) τής προτάσεως 2.4.8 γνωρίζουμε ότι

$$f(f^{-1}(L)) = \mathrm{Im}(f) \cap L. \tag{4.2}$$

Επειδή η απεικόνιση f είναι εξ υποθέσεως ομομορφισμός, ισχύει η ισότητα

$$f(Kf^{-1}(L)) = f(K) * f(f^{-1}(L)). \tag{4.3}$$

Ως εκ τούτου,

$$\begin{aligned} Kf^{-1}(L) \subseteq f^{-1}\left(f(Kf^{-1}(L))\right) &\underset{(4.3)}{=} f^{-1}\left(f(K) * f(f^{-1}(L))\right) \\ &\underset{(4.2)}{=} f^{-1}\left(f(K) * (\mathrm{Im}(f) \cap L)\right). \end{aligned} \tag{4.4}$$

Επιπροσθέτως,

$$f(K) * (\mathrm{Im}(f) \cap L) \underset{4.1.2\,\text{(ii)}}{\subseteq} (f(K) * \mathrm{Im}(f)) \cap (f(K) * L) \subseteq f(K) * L, \tag{4.5}$$

οπότε από τις (4.4) και (4.5) 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 4.1.4. □

4.1.7 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**[3] **τής** H **εντός τής** G.

[3] 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).

4.1.8 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

$$\boxed{(x,y)\in\mathcal{R}_H \underset{\text{ορσ}}{\Longleftrightarrow} xy^{-1}\in H} \tag{4.6}$$

και

$$\boxed{(x,y)\in {}_H\mathcal{R} \underset{\text{ορσ}}{\Longleftrightarrow} x^{-1}y\in H.} \tag{4.7}$$

4.1.9 Πρόταση. *Οι* (4.6) *και* (4.7) *αποτελούν σχέσεις ισοδυναμίας επί τού* G.

ΑΠΟΔΕΙΞΗ. Η (4.6) 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 (4.7). □

4.1.10 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* (4.6)) *ισούται με τη δεξιά πλευρική κλάση*

$$[g]_{\mathcal{R}_H} = Hg$$

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* (4.7)) *ισούται με την αριστερή πλευρική κλάση*

$$[g]_{{}_H\mathcal{R}} = gH$$

τής H *εντός τής* G *την οριζόμενη μέσω τού* g.

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. □

4.1.11 Πόρισμα. *Εάν η H είναι μια υποομάδα μιας ομάδας $(G,\cdot)$, τότε*

$$\boxed{G=\bigcup_{Hg\in(G/\mathcal{R}_H)}Hg=\bigcup_{gH\in(G/{}_H\mathcal{R})}gH} \tag{4.8}$$

και ισχύουν οι αμφίπλευρες συνεπαγωγές

$$Hg_1\cap Hg_2\neq\varnothing\Leftrightarrow Hg_1=Hg_2\Leftrightarrow g_1\in Hg_2\Leftrightarrow g_1g_2^{-1}\in H,\ \forall(g_1,g_2)\in G\times G,$$

καθώς και οι

$$g_1H\cap g_2H\neq\varnothing\Leftrightarrow g_1H=g_2H\Leftrightarrow g_1\in g_2H\Leftrightarrow g_1^{-1}g_2\in H,\ \forall(g_1,g_2)\in G\times G.$$

Ιδιαιτέρως δε, για ένα $g\in G$, $g\in H\Leftrightarrow Hg=H\Leftrightarrow H=gH$.

ΑΠΟΔΕΙΞΗ. Αυτή έπεται άμεσα από το γεγονός ότι τα σύνολα

$$G/\mathcal{R}_H=\{\,Hg\mid g\in G\}\quad\text{και}\quad G/{}_H\mathcal{R}=\{\,gH\mid g\in G\}$$

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

$$Hg_1=Hg_2\Leftrightarrow g_1\in Hg_2\Leftrightarrow g_1g_2^{-1}\in H$$

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 $g_1g_2^{-1}=h\in H$. Τέλος, εάν υποθέσουμε ότι $g_1g_2^{-1}\in H$, τότε $g_1g_2^{-1}=h$ 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. □

4.1.12 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,

$$|H|=\operatorname{card}(Hg)=\operatorname{card}(gH),\ \ \forall g\in G. \tag{4.9}$$

ΑΠΟΔΕΙΞΗ. Θεωρούμε την απεικόνιση

$$\psi_g^{[\delta]}:Hg\longrightarrow H,\quad \psi_g^{[\delta]}(x):=xg^{-1},\ \forall x\in Hg.$$

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

$$\psi_g^{[\alpha]}:gH\longrightarrow H,\quad \psi_g^{[\alpha]}(x):=g^{-1}x,\ \forall x\in gH.$$

ως αντίστροφό της. □

4.1.13 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*

$$\left|f^{-1}(L)\right| = |\mathrm{Ker}(f)|\,|L|\,. \tag{4.10}$$

ΑΠΟΔΕΙΞΗ. (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 4.1.11) $g_{y_1}\mathrm{Ker}(f) \cap g_{y_2}\mathrm{Ker}(f) = \varnothing$. Τούτο σημαίνει ότι

$$f^{-1}(L) = \coprod_{y\in L} g_y\mathrm{Ker}(f) \Rightarrow \left|f^{-1}(L)\right| = \sum_{y\in L} \mathrm{card}(g_y\mathrm{Ker}(f)).$$

Κατά την (4.9), $\mathrm{card}(g_y\mathrm{Ker}(f)) = |\mathrm{Ker}(f)|$ για κάθε $g_y \in G$ και $y \in L$, οπότε η (4.10) είναι αληθής. □

4.1.14 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[4] για οιαδήποτε $x, y \in \Delta$ να ισχύει η συνεπαγωγή

$$x \neq y \Longrightarrow Hx \neq Hy \tag{4.11}$$

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.

[4] Προφανώς, η συνθήκη (4.11) ισοδυναμεί με την: $\mathrm{card}(\Delta \cap Hg) = 1, \forall g \in G$.

4.1.15 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.)

4.1.16 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*

$$\mathrm{card}\,(\{Hg\,|g \in \Delta\}) = \mathrm{card}\,(\Delta) = \mathrm{card}\,(\mathrm{A}) = \mathrm{card}\,(\{gH\,|g \in \mathrm{A}\}). \tag{4.12}$$

ΑΠΟΔΕΙΞΗ. 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. □

4.1.17 Ορισμός. Εάν η H είναι μια υποομάδα μιας ομάδας $(G, \cdot)$, τότε ο πληθικός αριθμός (4.12) 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, $|G : H| = \infty$).

4.1.18 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. 4.4.7.)

4.1.19 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[5].)

4.1.20 Θεώρημα. *Εάν η H είναι μια υποομάδα μιας ομάδας $(G, \cdot)$, τότε*

$$\boxed{|G| = |G : H|\ |H|\,.} \tag{4.13}$$

ΑΠΟΔΕΙΞΗ. Έστω Δ ένα σύστημα δεξιών εκπροσώπων τής H εντός τής G. Τότε

$$|G| := \mathrm{card}(G) = \mathrm{card}(\coprod_{g \in \Delta} Hg). \tag{4.14}$$

[5] Κάθε υποομάδα μιας *αβελιανής* ομάδας είναι ορθόθετη (βλ. 4.2.6). 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. 4.1.36, 4.1.37).

Η απεικόνιση

$$f : H \times \Delta \longrightarrow \coprod_{g\in\Delta} Hg, \quad f(h,g) := hg \in Hg,\ \forall (h,g) \in H \times \Delta, \tag{4.15}$$

είναι αμφίρριψη. Ως εκ τούτου, μέσω των (4.14) και (4.15) ή, εναλλακτικώς, μέσω των (4.14) και (4.9) συνάγεται ότι

$$|G| = \text{card}\,(H \times \Delta) = |H| \cdot \text{card}(\Delta) = \text{card}(\Delta) \cdot |H| = |G : H|\ |H|\,,$$

οπότε η (4.13) είναι αληθής. □

4.1.21 Σημείωση. Εάν δύο εκ των πληθικών αριθμών $|G|\,,\ |H|\,,\ |G : H|$ είναι πεπερασμένοι, τότε και ο τρίτος είναι πεπερασμένος.

4.1.22 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 $|G : H| = \frac{|G|}{|H|}$.*

ΑΠΟΔΕΙΞΗ[6]. Εάν η G είναι μια πεπερασμένη ομάδα τάξεως $|G| = n \in \mathbb{N}$ και η H τυχούσα υποομάδα της τάξεως $|H| = m \leq n$, τότε $|G : H| < \infty$ και δυνάμει τής (4.13) έχουμε $m\,|n$ και $|G : H| = \frac{n}{m}$. □

4.1.23 Παράδειγμα. Έστω H η κυκλική υποομάδα τής $(\mathbb{Z}_{12}, +)$ η 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 4.1.22, 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.

4.1.24 Πόρισμα. *Εάν $(G, \cdot)$ είναι μια πεπερασμένη ομάδα και H μια γνήσια υποομάδα της, τότε $|H| \leq \frac{1}{2}\,|G|$.*

ΑΠΟΔΕΙΞΗ. $H \sqsubset G \underset{\text{4.1.18 (i)}}{\Longrightarrow} |G : H| \geq 2 \underset{\text{4.1.22}}{\Longrightarrow} \frac{|G|}{|H|} \geq 2 \Rightarrow |H| \leq \frac{1}{2}\,|G|$. □

[6] Ο Joseph-Louis Lagrange (1736-1813) ήταν ο πρώτος που διετύπωσε ένα θεώρημα ισοδύναμο τού 4.1.22 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 4.1.22 για *οιεσδήποτε πεπερασμένες ομάδες* οφείλεται στον Evariste Galois (1811-1832).

4.1.25 Πόρισμα. *Εάν οι H, K είναι δυο υποομάδες μιας πεπερασμένης ομάδας $(G, \cdot)$, τότε ισχύουν τα εξής:*

(i) $|H \cap K| \mid |H|, |H \cap K| \mid |K|$ *και* $|H \cap K| \mid$ μκδ$(|H|, |K|)$.

(ii) *Εάν* μκδ$(|H|, |K|) = 1$, *τότε* $H \cap K = \{e_G\}$.

(iii) *Εάν* $|H| = |K| = p$, *όπου πρώτος αριθμός, τότε είτε* $H = K$ *είτε* $H \cap K = \{e_G\}$.

ΑΠΟΔΕΙΞΗ. (i) Επειδή $H \cap K \sqsubseteq H$ και $H \cap K \sqsubseteq K$, οι δύο πρώτες σχέσεις διαιρετότητας έπονται άμεσα από το θεώρημα 4.1.22 τού Lagrange. Προφανώς (λόγω τού πορίσματος Β.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) $|H \cap K| \mid$ μκδ$(|H|, |K|) = 1 \Rightarrow |H \cap K| = 1 \Rightarrow H \cap K = \{e_G\}$.

(iii) Εάν $|H| = |K| = p$, όπου πρώτος αριθμός, τότε μκδ$(|H|, |K|) = p$, οπότε (λόγω τής τρίτης σχέσεως διαιρετότητας στο (i))

$$\text{είτε } \ |H \cap K| = 1 \ \text{ είτε } \ |H \cap K| = p.$$

Στην πρώτη περίπτωση έχουμε $H \cap K = \{e_G\}$. Στη δεύτερη περίπτωση έχουμε $|H| = |H \cap K| = |K| = p$, οπότε $H = H \cap K = K$. □

4.1.26 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*

$$k := \text{card}(\{H \in \mathbf{Subg}(G) \mid H \text{ κυκλική τάξεως } |H| = p\}).$$

ΑΠΟΔΕΙΞΗ. Εάν ένα στοιχείο $x \in G$ έχει τάξη p, τότε $|\langle x \rangle| = p$ (βλ. (2.9)) και η πρόταση 2.3.10 μας πληροφορεί ότι *κάθε* στοιχείο $g \in \langle x \rangle \setminus \{e_G\}$ έχει τάξη p και, ως εκ τούτου, $\langle g \rangle = \langle x \rangle$ (λόγω τού πορίσματος 2.3.17). Δυνάμει τού (iii) τού πορίσματος 4.1.25 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 $G \setminus \{e_G\}$ 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 $\text{card}(\{g \in G \,|\text{ord}(g) = p\}) = (p-1)k$. □

4.1.27 Πόρισμα. *Εάν $(G, \cdot)$ είναι μια πεπερασμένη ομάδα, τότε η τάξη οιουδήποτε στοιχείου της είναι διαιρέτης τής $|G|$. (Ιδιαιτέρως, $\exp(G) \mid |G|$.)*

ΑΠΟΔΕΙΞΗ. Εάν $g \in G$, τότε $\text{ord}(g) = |\langle g \rangle|$ (βλ. (2.9)), οπότε η τάξη $\text{ord}(g)$ τού g είναι διαιρέτης τής $|G|$ επί τη βάσει τού θεωρήματος 4.1.22 τού Lagrange. Σημειωτέον ότι $[\text{ord}(g) \mid |G|, \ \forall g \in G] \Longrightarrow \exp(G) = \text{εκπ}(\{\text{ord}(g) | \, g \in G\}) \mid |G|$. (Βλ. το (i) τής προτάσεως 2.3.25 και την πρόταση Β.2.25.) □

4.1.28 Πόρισμα. *Εάν $(G, \cdot)$ είναι μια πεπερασμένη ομάδα, τότε*

$$\boxed{g^{|G|} = e_G, \quad \forall g \in G.} \tag{4.16}$$

ΑΠΟΔΕΙΞΗ. Έστω τυχόν $g \in G$. Εάν $m := \text{ord}(g)$, τότε $g^m = e_G$ και, σύμφωνα με το πόρισμα 4.1.27, η τάξη $\text{ord}(g)$ τού g είναι διαιρέτης τής $|G|$, οπότε

$$g^{|G|} = g^{m(\frac{|G|}{m})} = (g^m)^{\frac{|G|}{m}} = e_G^{\frac{|G|}{m}} = e_G,$$

και η (4.16) είναι αληθής. □

4.1.29 Πόρισμα. *Εάν $(G, \cdot)$ είναι μια πεπερασμένη κυκλική ομάδα, τότε ισχύει η ισότητα* $\exp(G) = |G|$.

ΑΠΟΔΕΙΞΗ. Σύμφωνα με την πρόταση 2.3.7, $\exists x \in G$: $\text{ord}(x) = |G|$, οπότε

$$\text{ord}(x) = |G| \mid \text{εκπ}(\{\text{ord}(g) | \, g \in G\}) = \exp(G) \Rightarrow |G| \leq \exp(G).$$

Από την άλλη μεριά, από την (4.16) και από τον ορισμό 2.3.24 τού εκθέτη λαμβάνουμε $\exp(G) \leq |G|$. Επομένως, $\exp(G) = |G|$. □

4.1.30 Πόρισμα. (Θεώρημα τού Euler περί ισοτιμιών, 1760) *Έστω m ένας φυσικός αριθμός ≥ 2 και έστω a ένας ακέραιος με* $\text{μκδ}(a, m) = 1$. *Τότε*

$$\boxed{a^{\phi(m)} \equiv 1 (\text{mod}\, m),} \tag{4.17}$$

όπου ϕ η συνάρτηση φι τού Euler. (Βλ. Β.4.15 και 2.1.7 (iii)).

ΑΠΟΔΕΙΞΗ. Θεωρούμε την πολλαπλασιαστική ομάδα $(\mathbb{Z}_m^\times, \cdot)$,

$$\mathbb{Z}_m^\times = \{[k]_m \in \mathbb{Z}_m \mid k \in \mathbb{N}, \;\; k \leq m, \;\; \text{μκδ}\,(k, m) = 1\},$$

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 4.1.28 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 (4.17). □

4.1.31 Πόρισμα. («Μικρό» Θεώρημα τού Fermat, 1640) *Εάν ο p είναι ένας πρώτος αριθμός και ο a ένας ακέραιος, τέτοιος ώστε*[7] $p \nmid a$, *τότε*

$$\boxed{a^{p-1} \equiv 1 (\text{mod}\, p).} \tag{4.18}$$

ΑΠΟΔΕΙΞΗ. Άμεση από το πόρισμα 4.1.30 και το γεγονός ότι $\phi(p) = p - 1$. (Βλ. λήμμα Β.4.19.) □

4.1.32 Πόρισμα. *Εάν ο p είναι ένας πρώτος αριθμός, τότε*

$$\boxed{a^p \equiv a (\text{mod}\, p), \;\; \forall a \in \mathbb{Z}.} \tag{4.19}$$

[7] Εξ αυτής τής συνθήκης έπεται, ιδιαιτέρως, ότι $a \neq 0$.

ΑΠΟΔΕΙΞΗ. Έστω a τυχών ακέραιος αριθμός. Εάν $p \nmid a$, τότε η (4.19) έπεται άμεσα από την (4.18). 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 (4.19) είναι αληθής. □

4.1.33 Πόρισμα. *Εάν μια ομάδα $(G, \cdot)$ έχει ως τάξη της έναν πρώτο αριθμό p, τότε αυτή είναι κυκλική.*

ΑΠΟΔΕΙΞΗ. Επειδή $p = |G| \geq 2$, υπάρχει κάποιο $g \in G$ με $g \neq e_G$. Συνεπώς, $\mathrm{ord}(g) \geq 2$ και $\mathrm{ord}(g) \,|p$ (δυνάμει τού πορίσματος 4.1.27). Και επειδή ο p είναι εξ υποθέσεως πρώτος, έχουμε $\mathrm{ord}(g) = p$. Αυτό όμως σημαίνει ότι η G είναι κυκλική δυνάμει τής προτάσεως 2.3.7. □

4.1.34 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.*

(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 2.2.18). 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 2.2.18), 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 2.2.18). Κατά συνέπειαν, η G είναι *πεπερασμένη* και *κυκλική* με $|G| > 1$. Κατά το πόρισμα 2.3.17,

$$\mathrm{card}(\{\text{γεννήτορες τής } G\}) = \phi(|G|),$$

όπου ϕ η συνάρτηση φι τού Euler (βλ. B.4.15). Εξ υποθέσεως, η G διαθέτει ακριβώς $|G| - 1$ γεννήτορες. Κατά συνέπειαν, $\phi(|G|) = |G| - 1$. Εάν η τάξη $|G|$ τής 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

$$\phi\left(|G|\right) = \mathrm{card}\left\{\, k \in \mathbb{N} \mid \; k \leq |G| \;\text{ και }\; \mu\kappa\delta\left(k, |G|\right) = 1\right\} < |G| - 2.$$

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 4.1.22 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 $|H| = |G| \Rightarrow H = G$. □

4.1.35 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.*

4.1.36 Πόρισμα. *Κάθε πεπερασμένη ομάδα τάξεως* ≤ 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. 3.1.2, 3.4.4).

ΑΠΟΔΕΙΞΗ. Κάθε ομάδα τάξεως $1, 2, 3$ ή 5 είναι κυκλική και, ως εκ τούτου, αβελιανή (βλ. 2.4.24, 2.3.19, 4.1.33 και 2.2.17). Επίσης, σύμφωνα με το (i) τού θεωρήματος 3.5.6 κάθε ομάδα τάξεως 4 είναι αβελιανή. □

4.1.37 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* $(\mathfrak{S}_3, \circ)$).

ΑΠΟΔΕΙΞΗ. 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. 2.3.7 και 2.4.23 (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 4.1.27 κάθε στοιχείο διαφορετικό τού ουδετέρου οφείλει να έχει τάξη είτε 2 είτε 3. Εάν όλα τα $g \in G \setminus \{e_G\}$ είχαν τάξη 2, τότε η G θα ήταν αβελιανή (βλ. 2.3.9 (iv)). Εν τοιαύτη περιπτώσει, για οιαδήποτε $a, b \in G \setminus \{e_G\}$, $a \neq b$, το σύνολο $\{e_G, a, b, ab\}$ θα ήταν κλειστό ως προς την πράξη τής ομάδας G, οπότε (σύμφωνα με την πρόταση 2.1.19) θα αποτελούσε *υποομάδα* τής G τάξεως 4, πράγμα που θα μας οδηγούσε σε άτοπο λόγω τού θεωρήματος 4.1.22 τού Lagrange (καθότι $4 \nmid 6$). *Άρα η* G *διαθέτει κατ' ανάγκην κάποιο στοιχείο*, ας πούμε x, *τάξεως* 3. Έστω τυχόν στοιχείο $y \in G \setminus \langle x \rangle$. 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

$$y^2 \in \langle x \rangle \underset{4.1.27}{\Longrightarrow} \mathrm{ord}(y^2) \mid |\langle x \rangle| \Rightarrow \text{ είτε } \mathrm{ord}(y^2) = 1 \text{ είτε } \mathrm{ord}(y^2) = 3.$$

Εάν ίσχυε $\text{ord}(y^2) = \left|\langle y^2\rangle\right| = 3$, τότε θα είχαμε

$$\{e_G, y^2, y^4\} = \langle y^2\rangle = \langle x\rangle = \{e_G, x, x^2\},$$

οπότε είτε $[y^2 = x \text{ και } y^4 = x^2]$ είτε $[y^2 = x^2 \text{ και } y^4 = x]$. 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 $\text{ord}(y) = 6$ (βλ. 2.3.7). Άτοπο! Κατ' ανάγκην, λοιπόν,

$$\text{ord}(y^2) = 1 \Rightarrow y^2 = e_G \underset{y\neq e_G}{\Longrightarrow} \text{ord}(y) = 2.$$

Ως εκ τούτου, *κάθε στοιχείο* $y \in G\setminus\langle x\rangle$ *έχει τάξη* 2. Για οιοδήποτε $y \in G\setminus\langle x\rangle$ έχουμε $xy \notin \langle x\rangle$, οπότε μέσω τού ανωτέρω επιχειρήματος (αλλά αυτήν τη φορά με το xy στη θέση τού y) συνάγεται ότι

$$\text{ord}(xy) = 2 \Rightarrow xyxy = e_G \Rightarrow xy = y^{-1}x^{-1} = yx^{-1}.$$

Αυτές οι σχέσεις καθορίζουν πλήρως τον πολλαπλασιαστικό κατάλογο τής ομάδας G. Η G είναι μη αβελιανή (αφού[8] $xy \neq yx$) και

$$\left.\begin{array}{r} \langle x\rangle \sqsubset \langle x, y\rangle \sqsubseteq G \Rightarrow 3 = |\langle x\rangle| < |\langle x, y\rangle| \leq |G| = 6 \\ 4.1.22 \Longrightarrow |\langle x\rangle| \mid |\langle x, y\rangle| \Rightarrow |\langle x, y\rangle| = 6 \end{array}\right\} \Rightarrow G = \langle x, y\rangle.$$

Εφαρμόζοντας την πρόταση 3.4.7 (ή ελέγχοντας απευθείας ότι η απεικόνιση

$$G \ni y^j x^k \longmapsto \alpha^j \circ \beta^k \in \mathbf{D}_3,\ \ j \in \{0, 1\},\ k \in \{0, 1, 2\},$$

είναι ισομορφισμός) συμπεραίνουμε ότι $(G, \cdot) \cong (\mathbf{D}_3, \circ)$. □

4.1.38 Θεώρημα. (Ταξινόμηση ομάδων τάξεως ≤ 7.) *Η ταξινόμηση των ομάδων G με $|G| \leq 7$ 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	$\mathbb{Z}_7$

[8] 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 $\text{ord}(x) < 3$.

ΑΠΟΔΕΙΞΗ. Αυτή έπεται ύστερα από συνδυασμό τού (ii) τού θεωρήματος 2.4.23, τού θεωρήματος 2.3.19, τού θεωρήματος 3.5.6, τού πορίσματος 4.1.33 και τού θεωρήματος 4.1.37. □

4.1.39 Θεώρημα. *Κάθε μη αβελιανή ομάδα τάξεως* 8 *είναι ισόμορφη είτε με την* $(\mathbf{Q}, \cdot)$ *είτε με την* $(\mathbf{D}_4, \circ)$.

ΑΠΟΔΕΙΞΗ. Έστω $(G, \cdot)$ μια μη αβελιανή ομάδα τάξεως 8 και έστω $g \in G$. Από το πόρισμα 4.1.27 έπεται ότι

$$\text{ord}(g) = |\langle g \rangle| \in \{1, 2, 4, 8\}.$$

Το ενδεχόμενο να ισχύει $\text{ord}(g) = 8$ αποκλείεται (διότι τότε η $G = \langle g \rangle$, ως κυκλική, θα ήταν αβελιανή, βλ. προτάσεις 2.3.7 και 2.2.17). Άρα οι τάξεις *όλων* των στοιχείων τής G είναι ≤ 4. Από την άλλη μεριά, αποκλείεται ωσαύτως το να έχουν *όλα* τα στοιχεία τής G τάξεις ≤ 2 (διότι εν τοιαύτη περιπτώσει η G θα ήταν αβελιανή επί τη βάσει τού (iv) τής προτάσεως 2.3.9). Επομένως υπάρχει τουλάχιστον ένα στοιχείο, ας πούμε το x, τής G με $\text{ord}(x) = 4$. Κατά το θεώρημα 4.1.22 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 $y \in G \smallsetminus \langle x \rangle$. Προφανώς,

$$G = \langle x \rangle \coprod \langle x \rangle y = \{e_G, x, x^2, x^3\} \coprod \{y, xy, x^2y, x^3y\},$$

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 $\text{ord}(yxy^{-1}) = \text{ord}(x) = 4$ (βλ. 2.3.9 (ii)). Επειδή $\text{ord}(e_G) = 1$, $\text{ord}(x^2) = 2$ και $\text{ord}(x^3) = 4$ (βλ. 2.3.10 (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 $x^i y^j = y^j x^i$ 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

$$\left.\begin{array}{r} y^2 \in \langle x \rangle = \{e_G, x, x^2, x^3\} \\ \text{ord}(y) \in \{2, 4\} \underset{\text{2.3.10 (i)}}{\Longrightarrow} \text{ord}(y^2) \in \{1, 2\} \end{array}\right\} \Rightarrow y^2 \in \{e_G, x^2\}.$$

Επιπροσθέτως,

$$\left.\begin{array}{r} \langle x\rangle \sqsubset \langle x,y\rangle \sqsubseteq G \Rightarrow 4 = |\langle x\rangle| < |\langle x,y\rangle| \leq |G| = 8 \\ 4.1.22 \Longrightarrow |\langle x\rangle| \,|\, |\langle x,y\rangle| \Rightarrow |\langle x,y\rangle| = 8 \end{array}\right\} \Rightarrow G = \langle x,y\rangle\,.$$

Εν κατακλείδι, υπάρχουν μόνον δύο ενδεχόμενα:
(i) $G = \langle x,y\rangle$, *όπου* $y^2 = e_G$ *και* $xy = yx^{-1}$. Εφαρμόζοντας την πρόταση 3.4.7 (ή ελέγχοντας απευθείας ότι η απεικόνιση

$$G \ni y^j x^k \longmapsto \alpha^j \circ \beta^k \in \mathbf{D}_4,\ \ j \in \{0,1\},\ k \in \{0,1,2,3\},$$

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. 2.2.11) παρατηρούμε ότι η απεικόνιση[9]

$$G \ni y^\mu x^\nu \longmapsto \mathbf{k}^\mu \mathbf{i}^\nu = \mathbf{k}^\mu (\mathbf{jk})^\nu \in \mathbf{Q},\ \ \mu \in \{0,1\},\ \nu \in \{0,1,2,3\},$$

είναι ισομορφισμός, οπότε $(G,\cdot) \cong (\mathbf{Q},\cdot)$. □

4.1.40 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. 3.4.4) 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. 2.4.19 (iv)).

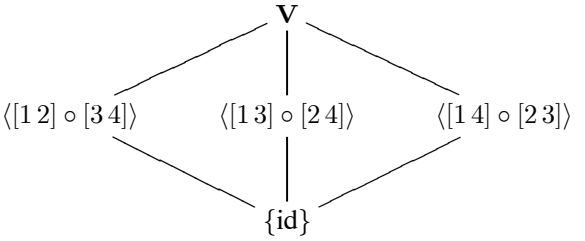
► **Εφαρμογές τού θεωρήματος τού Lagrange κατά τον προσδιορισμό υποομάδων.** Δοθείσας μιας πεπερασμένης ομάδας G *σχετικώς μικρής τάξεως* $m := |G|$, το θεώρημα 4.1.22 τού Lagrange περιορίζει την αναζήτηση των τάξεων των πιθανών υποομάδων τής G στους διαιρέτες τού m, διευκολύνοντάς μας, ως εκ τούτου, 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 2.4.26, 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.

[9] Σημειωτέον ότι $\mathbf{i}^0 = \mathbf{I}_2, \mathbf{i}^1 = \mathbf{i}, \mathbf{i}^2 = -\mathbf{I}_2, \mathbf{i}^3 = -\mathbf{i}, \mathbf{ki}^0 = \mathbf{k}, \mathbf{ki} = \mathbf{j}, \mathbf{ki}^2 = -\mathbf{k}, \mathbf{ki}^3 = -\mathbf{j}$.

4.1.41 Εφαρμογή. *Το σύνολο των υποομάδων τής ομάδας* $\mathbf{V}$ *των τεσσάρων στοιχείων τού Klein* (*βλ.* 3.4.2 (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*



ΑΠΟΔΕΙΞΗ. Έστω H μια υποομάδα τής $\mathbf{V}$. Κατά το θεώρημα 4.1.22, $|H| \in \{1, 2, 4\}$. Εάν $|H| = 1$, τότε $H = \{\mathrm{id}\}$. Εάν $|H| = 4$, τότε $H = \mathbf{V}$. Εάν $|H| = 2$, τότε η H είναι κυκλική (βλ. 2.3.19). Επειδή

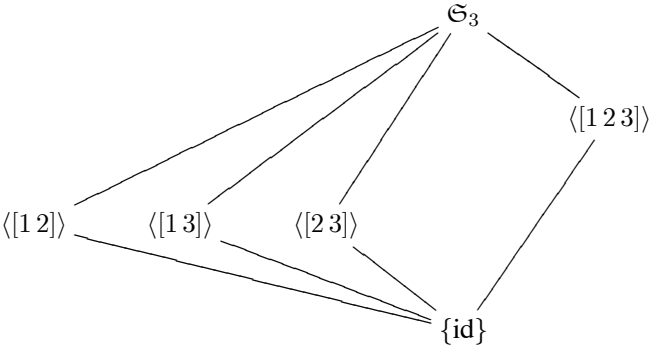
$$\mathrm{ord}([1\,2] \circ [3\,4]) = \mathrm{ord}([1\,3] \circ [2\,4]) = \mathrm{ord}([1\,4] \circ [2\,3]) = 2,$$

έχουμε κατ' ανάγκην $H \in \{\langle [1\,2] \circ [3\,4]\rangle\,, \langle [1\,3] \circ [2\,4]\rangle\,, \langle [1\,4] \circ [2\,3]\rangle\}$. □

4.1.42 Εφαρμογή. *Το σύνολο των υποομάδων τής συμμετρικής 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*



ΑΠΟΔΕΙΞΗ. Έστω ότι $H \sqsubseteq \mathfrak{S}_3$. Κατά το θεώρημα 4.1.22, $|H| \in \{1, 2, 3, 6\}$. 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. 2.3.19). Επειδή

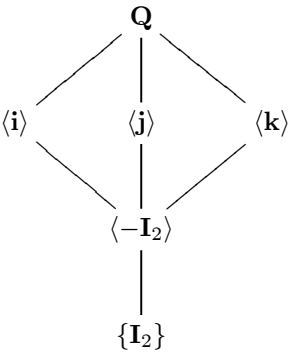
$$\mathrm{ord}([1\,2]) = \mathrm{ord}([1\,3]) = \mathrm{ord}([2\,3]) = 2,\ \mathrm{ord}([1\,2\,3]) = 3,$$

(βλ. 3.2.2) και $[1\,2\,3] = [1\,3\,2]^{-1}$, έχουμε $H \in \{\langle [1\,2]\rangle\,, \langle [1\,3]\rangle\,, \langle [2\,3]\rangle\,, \langle [1\,2\,3]\rangle\}$. □

4.1.43 Εφαρμογή. *Το σύνολο των υποομάδων τής ομάδας* $\mathbf{Q} := \langle \mathbf{j}, \mathbf{k} \rangle$ *των τετρανίων* (*τής ορισθείσας στο εδάφιο* 2.2.11) *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*



ΑΠΟΔΕΙΞΗ. Έστω H μια υποομάδα τής $\mathbf{Q} = \{\pm\mathbf{I}_2, \pm\mathbf{i} \pm \mathbf{j}, \pm\mathbf{k}\}$. Σύμφωνα με το θεώρημα 4.1.22, $|H| \in \{1, 2, 4, 8\}$. 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

στο οποίο καταχωρίζουμε τα 8 στοιχεία τής $\mathbf{Q}$ στην πρώτη του γραμμή, τα αντίστροφά τους στη δεύτερη και τις τάξεις τους στην τρίτη (πρβλ. 2.3.9 (i)). Εάν $|H| = 2$, τότε η H είναι κυκλική (βλ. 2.3.19), 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 3.5.6). Επειδή η $\mathbf{V}$ περιέχει *τρία* στοιχεία τάξεως 2, συμπεραίνουμε ότι $H \ncong \mathbf{V}$ (διότι η $\mathbf{Q}$ περιέχει *μόνον ένα* στοιχείο τάξεως 2, πρβλ. 2.4.19 (iv)). Άρα

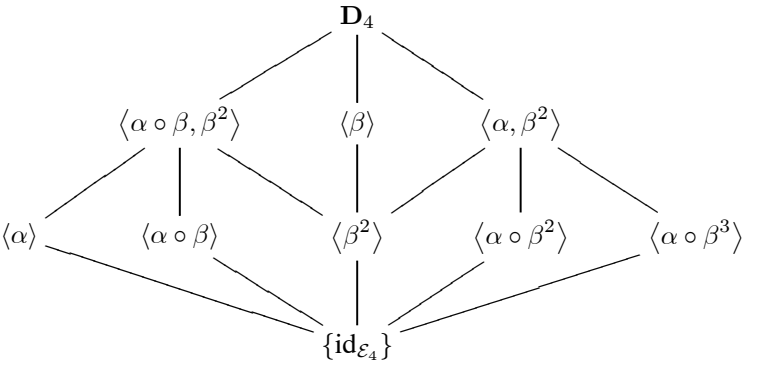
$$|H| = 4 \Rightarrow H \in \{\langle \mathbf{i} \rangle, \langle \mathbf{j} \rangle, \langle \mathbf{k} \rangle\},$$

αφού $\langle \mathbf{i} \rangle = \langle -\mathbf{i} \rangle$, $\langle \mathbf{j} \rangle = \langle -\mathbf{j} \rangle$ και $\langle \mathbf{k} \rangle = \langle -\mathbf{k} \rangle$. □

4.1.44 Εφαρμογή. *Το σύνολο των υποομάδων τής διεδρικής ομάδας* $\mathbf{D}_4 := \langle \alpha, \beta \rangle$ (*τής ορισθείσας στο εδάφιο* 3.4.4) *είναι το*

$$\boxed{\mathbf{Subg}(\mathbf{D}_4) = \left\{ \begin{array}{c} \{\mathrm{id}_{\mathcal{E}_4}\}, \langle \alpha \rangle, \langle \beta \rangle, \left\langle \beta^2 \right\rangle, \langle \alpha \circ \beta \rangle, \left\langle \alpha \circ \beta^2 \right\rangle, \\ \left\langle \alpha \circ \beta^3 \right\rangle, \left\langle \alpha, \beta^2 \right\rangle, \left\langle \alpha \circ \beta, \beta^2 \right\rangle, \mathbf{D}_4 \end{array} \right\}}$$

και το διάγραμμα τού Hasse για τον σύνδεσμο $(\mathbf{Subg}(\mathbf{D}_4), \sqsubseteq)$ *το*



ΑΠΟΔΕΙΞΗ. Η $\mathbf{D}_4$ παράγεται από τις αμφιρρίψεις

$$\mathcal{E}_4 \ni z \overset{\alpha}{\longmapsto} \overline{z} \in \mathcal{E}_4, \;\; \mathcal{E}_4 \ni z \overset{\beta}{\longmapsto} \zeta_4 z = iz \in \mathcal{E}_4,$$

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. 3.4.4), 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 4.1.22, $|H| \in \{1,2,4,8\}$. 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

στο 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. 2.3.9 (i)). Εάν $|H| = 2$, τότε η H είναι κυκλική (βλ. 2.3.19), οπότε

$$H \in \left\{\langle\alpha\rangle, \left\langle\beta^2\right\rangle, \langle\alpha\circ\beta\rangle, \left\langle\alpha\circ\beta^2\right\rangle, \left\langle\alpha\circ\beta^3\right\rangle\right\}.$$

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 3.5.6). 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 $H = \{\mathrm{id}_{\mathcal{E}_4}, x, y, z\}$,

$$x \neq y,\ x \neq z,\ y \neq z,\ \{x, y, z\} \subsetneqq \{\alpha, \beta^2, \alpha\circ\beta, \alpha\circ\beta^2, \alpha\circ\beta^3\},$$

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, $H \in \left\{\langle\alpha, \beta^2\rangle,\ \langle\alpha\circ\beta, \beta^2\rangle\right\}$. □

4.1.45 Παρατήρηση. Κάθε *γνήσια* υποομάδα των ομάδων $\mathbf{V}, \mathfrak{S}_3$ και $\mathbf{Q}$ 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 4.1.22 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. 2.3.21 (i)) και, γενικότερα, για τις πεπερασμένες αβελιανές ομάδες (βλ. 4.4.22), για τις προηγουμένως εξετασθείσες (μη αβελιανές) ομάδες $\mathfrak{S}_3, \mathbf{Q}$ και $\mathbf{D}_4$, καθώς και για τις ομάδες τάξεως p^ν (p πρώτος, $\nu \in \mathbb{N}$, βλ. 5.6.6), η απάντηση είναι *εν γένει αρνητική*. Η ομάδα με τη μικρότερη δυνατή τάξη, η οποία μπορεί, όπως θα δούμε στην πρόταση 4.1.47, 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 (όπως είναι το *θεώρημα τού Cauchy* 5.7.1 και το γενικότερο 1ο *θεώρημα τού Sylow* 11.1.2 που παρατίθενται σε κατοπινά κεφάλαια) τα οποία είναι δυνατόν να ιδωθούν ως *μερικά αντίστροφα* τού θεωρήματος 4.1.22 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 4.1.47 στηρίζεται στο ακόλουθο:

4.1.46 Λήμμα. *Έστω H μια υποομάδα μιας ομάδας $(G, \cdot)$ με $|G : H| = 2$. Τότε*

$$g^2 \in H,\ \ \forall g \in G.$$

ΑΠΟΔΕΙΞΗ. Επειδή $|G : H| = 2$, έχουμε $G = H \coprod aH$, για κάποιο $a \notin H$. Επομένως, $aH = G \smallsetminus H$. Έστω τυχόν $g \in G$.

Περίπτωση πρώτη. Εάν $g \in H$, τότε $g^2 \in H$ (λόγω τής κλειστότητας τής πράξεως).
Περίπτωση δεύτερη. Εάν $g \in G \smallsetminus H$, 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 $g \in G \smallsetminus H$). Άρα όντως (και σε αυτήν την περίπτωση) $g^2 \in H$. □

4.1.47 Πρόταση. *Η εναλλάσσουσα ομάδα $\mathfrak{A}_4$ δεν διαθέτει υποομάδες τάξεως 6.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι υπάρχει υποομάδα H τής $\mathfrak{A}_4$ τάξεως 6. Τότε από το θεώρημα 4.1.22 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 3.2.3, ισχύει $\mathrm{ord}(\sigma) = 3$, έχουμε

$$\left.\begin{array}{c} \sigma = \sigma^3 \circ \sigma = \sigma^4 = (\sigma^2)^2 \\ \sigma^2 \in \mathfrak{A}_4 \underset{4.1.46}{\Longrightarrow} (\sigma^2)^2 \in H \end{array}\right\} \Longrightarrow \sigma \in H.$$

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 3.3.11), ενώ $|H| = 6$. Άτοπο! Άρα η εναλλάσσουσα ομάδα $\mathfrak{A}_4$ δεν διαθέτει υποομάδες τάξεως 6. □

4.1.48 Σημείωση. Μια διαφορετική απόδειξη τής προτάσεως 4.1.47 (που δεν χρησιμοποιεί το λήμμα 4.1.46) είναι η εξής: Ας υποθέσουμε εκ νέου ότι υπάρχει υποομάδα H τής $\mathfrak{A}_4$ τάξεως 6. Τότε, σύμφωνα με το θεώρημα 4.1.37, 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. 2.4.19 (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 2.4.19 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

$$\begin{aligned} u_1 \circ u_2 &= [1\,3\,2] \neq [1\,2\,3] = u_2 \circ u_1, \\ u_1 \circ u_3 &= [1\,2\,3] \neq [1\,3\,2] = u_3 \circ u_1, \\ u_2 \circ u_3 &= [1\,3\,2] \neq [1\,2\,3] = u_3 \circ u_2, \end{aligned}$$

για οιαδήποτε $j,k\in\{1,2,3\}$ με $j\neq k$ συμπεραίνουμε ότι

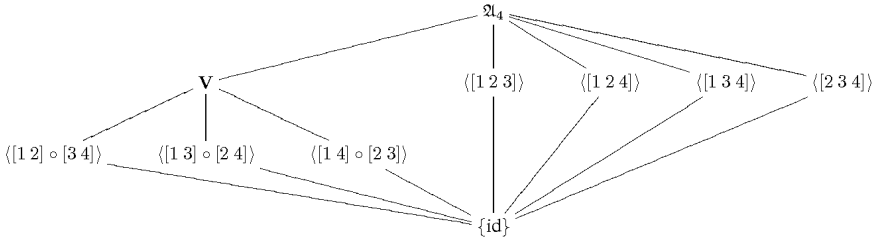
$$u_j\circ u_k\neq u_k\circ u_j \underset{f\text{ ένριψη}}{\Longrightarrow} f(u_j)\circ f(u_k)=f(u_j\circ u_k)\neq f(u_k\circ u_j)=f(u_k)\circ f(u_j),$$

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. (Μια επιπρόσθετη, *τρίτη* απόδειξη τής προτάσεως 4.1.47 δίδεται στο εδάφιο 5.3.24.)

4.1.49 Πόρισμα. *Το σύνολο των υποομάδων τής εναλλάσσουσας ομάδας* $\mathfrak{A}_4$ *είναι το*

$$\mathbf{Subg}(\mathfrak{A}_4)=\left\{\begin{array}{c}\{\mathrm{id}\},\langle[1\,2]\circ[3\,4]\rangle,\langle[1\,3]\circ[2\,4]\rangle,\langle[1\,4]\circ[2\,3]\rangle\\ \langle[1\,2\,3]\rangle,\ \langle[1\,2\,4]\rangle,\ \langle[1\,3\,4]\rangle,\ \langle[2\,3\,4]\rangle,\ \mathbf{V},\ \mathfrak{A}_4\end{array}\right\}$$

και το διάγραμμα τού Hasse για τον σύνδεσμο $(\mathbf{Subg}(\mathfrak{A}_4),\sqsubseteq)$ *το*



ΑΠΟΔΕΙΞΗ. Έστω H μια υποομάδα τής $\mathfrak{A}_4$. Σύμφωνα με το θεώρημα 4.1.22 και την πρόταση 4.1.47 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 $|H|\in\{2,3,4\}$. 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. 2.3.19), 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. 2.3.19), 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

$$\begin{array}{ll} \langle [1\ 2\ 3] \rangle = \langle [1\ 3\ 2] \rangle, & \langle [1\ 2\ 4] \rangle = \langle [1\ 4\ 2] \rangle, \\ \langle [1\ 3\ 4] \rangle = \langle [1\ 4\ 3] \rangle, & \langle [2\ 3\ 4] \rangle = \langle [2\ 4\ 3] \rangle. \end{array}$$

Τέλος, στην περίπτωση κατά την οποία $|H| = 4$, έχουμε κατ' ανάγκην[10] $H = \mathbf{V}$.□

► **Βασικές ιδιότητες υποομάδων πεπερασμένου δείκτη.** Το θεώρημα 4.1.20 γενικεύεται ως ακολούθως:

4.1.50 Θεώρημα. *Έστω $(G, \cdot)$ μια ομάδα. Εάν οι H και K είναι δυο υποομάδες της με $K \sqsubseteq H$, τότε*

$$\boxed{|G : K| = |G : H|\ |H : K|} \tag{4.20}$$

Ιδιαιτέρως, ισχύει η συνεπαγωγή :

$$K \sqsubset H \Longrightarrow |G : H| < |G : K|.$$

ΑΠΟΔΕΙΞΗ. Έστω A ένα σύστημα αριστερών εκπροσώπων *της H εντός της G* και έστω A′ ένα σύστημα αριστερών εκπροσώπων *της K εντός της H*. Τότε

$$\text{card}(\mathrm{A}) = |G : H| \quad \text{και} \quad \text{card}(\mathrm{A}') = |H : K|. \tag{4.21}$$

Θα αποδείξουμε ότι το $\mathrm{AA}' \subseteq G$ αποτελεί ένα σύστημα αριστερών εκπροσώπων *της K εντός της 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) της προτάσεως 4.1.2. 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 $(g_1 h_1)\, K = (g_2 h_2)\, K$, τότε

$$\left.\begin{array}{r} (g_1 h_1)\, KH = (g_2 h_2)\, KH \\ K \subseteq H \Rightarrow KH = H \end{array}\right\} \Rightarrow \left.\begin{array}{r} g_1 h_1 H = g_2 h_2 H \\ h_j \in H \Rightarrow h_j H = H, \forall j \in \{1, 2\} \end{array}\right\} \Rightarrow g_1 H = g_2 H,$$

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 $\text{card}(\mathrm{AA}') = |G : K|$. 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

$$g_1 h_1 = g_2 h_2 \Rightarrow (g_1 h_1)\, KH = (g_2 h_2)\, KH \Rightarrow g_1 = g_2 \Rightarrow h_1 = h_2,$$

[10] 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 3.5.6). 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).

όπου η πρώτη είναι προφανής, η δεύτερη απόρροια των όσων έχουμε ήδη προαναφέρει και η τρίτη έπεται από τον νόμο τής διαγραφής 2.1.9 (i). Από το γεγονός τού ότι τελικώς ισχύει $g_1h_1 = g_2h_2 \Rightarrow [g_1 = g_2 \ \text{ και } \ h_1 = h_2]$ συμπεραίνουμε ότι

$$|G : K| = \text{card}(\text{AA}') = \text{card}(\text{A} \times \text{A}') = \text{card}(\text{A}) \cdot \text{card}(\text{A}'). \tag{4.22}$$

Ο συνδυασμός των (4.21) και (4.22) δίδει την (4.20). □

4.1.51 Παρατήρηση. Η ισότητα (4.13) έπεται άμεσα από την (4.20) εάν ως K θεωρήσουμε την τετριμμένη υποομάδα τής G (βλ. 4.1.18 (i)).

4.1.52 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. 2.2.11 και 4.1.43), η (4.20) είναι άμεσα επαληθεύσιμη, καθόσον

$$|\mathbf{Q} : \langle -\mathbf{I}_2 \rangle| = 4 = 2 \cdot 2 = |\mathbf{Q} : \langle \mathbf{i} \rangle| \, |\langle \mathbf{i} \rangle : \langle -\mathbf{I}_2 \rangle| \, .$$

4.1.53 Ορισμός. Κάθε υποομάδα H μιας ομάδας $(G, \cdot)$ με $|G : H| < \infty$ καλείται **υποομάδα πεπερασμένου δείκτη** (εντός τής G).

4.1.54 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*:

$$\boxed{|G : H \cap K| \leq |G : H| \, |G : K| \, .} \tag{4.23}$$

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*:

$$\boxed{\text{εκπ}\left(|G : H| \, , |G : K|\right) \leq |G : H \cap K|} \tag{4.24}$$

και ισχύει, ιδιαιτέρως, η συνεπαγωγή

$$\text{μκδ}\left(|G : H| \, , |G : K|\right) = 1 \Longrightarrow |G : H \cap K| = |G : H| \, |G : K| \, .$$

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 4.1.11). Από το (ii) τής προτάσεως 4.1.2 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

$$\begin{aligned} \mathrm{card}\left(\{ (xH) \cap (yK) \,|x \in \mathrm{A},\ y \in \mathrm{A}' \} \right) &= \mathrm{card}(\mathrm{A}) \cdot \mathrm{card}(\mathrm{A}') \\ &= |G : H|\ |G : K| \end{aligned}$$

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 (4.23).

ΔΕΥΤΕΡΗ ΑΠΟΔΕΙΞΗ ΤΟΥ (i). Εφαρμόζοντας το θεώρημα 4.1.50 (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 $|H : H \cap K| \leq |G : K|$. 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 $f : \{ h (H \cap K) \,| h \in \mathrm{A} \} \longrightarrow \{ gK \,| g \in \mathrm{A}' \}$ με τύπο $f(h (H \cap K)) := hK$ είναι μια καλώς ορισμένη *ενριπτική* απεικόνιση, πράγμα που σημαίνει ότι

$$|H : H \cap K| = \mathrm{card}(\mathrm{A}) \leq \mathrm{card}(\mathrm{A}') = |G : K| \,.$$

ΑΠΟΔΕΙΞΗ ΤΟΥ (ii). Θέτοντας $m := |G : H|$ και $n := |G : K|$, η (4.23) μας πληροφορεί ότι

$$|G : H \cap K| \leq mn < \infty. \tag{4.25}$$

Θέτοντας $k := |G : H \cap K|$, διπλή εφαρμογή τού θεωρήματος 4.1.50 μας δίδει[11]

$$[k = m \,|H : H \cap K| \Rightarrow m \mid k] \text{ και } [k = n \,|K : H \cap K| \Longrightarrow n \mid k] \,.$$

Άρα $\mathrm{εκπ}(m, n) \mid k$ (βλ. Β.2.25), οπότε $\mathrm{εκπ}(m, n) \leq k$. Στην ειδική περίπτωση όπου $\mathrm{μκδ}(m, n) = 1$ συμπεραίνουμε (μέσω τής προτάσεως Β.2.29) ότι $\mathrm{εκπ}(m, n) = mn$, οπότε από τις (4.24) και (4.25) προκύπτει ότι $k = mn$. □

[11] Από την υπόθεσή μας και από το θεώρημα 4.1.50 έπεται ότι $|H : H \cap K| < \infty$ και $|K : H \cap K| < \infty$.

4.1.55 Πόρισμα. *Εάν $H_1,...,H_k$ είναι υποομάδες μιας ομάδας $(G,\cdot)$ (όπου k κάποιος φυσικός αριθμός ≥ 2), τότε*

$$|G : \bigcap_{j=1}^{k} H_j| \leq \prod_{j=1}^{k} |G : H_j| .$$

Ως εκ τούτου, εάν $H_1,...,H_k$ είναι υποομάδες πεπερασμένου δείκτη, τότε και η τομή $\bigcap_{j=1}^{k} H_j$ είναι υποομάδα πεπερασμένου δείκτη. Εν τοιαύτη περιπτώσει,

$$\text{εκπ}\left(|G : H_1| ,..., |G : H_k|\right) \leq |G : \bigcap_{j=1}^{k} H_j|$$

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 4.1.54, τής προτάσεως Β.2.27 και τού πορίσματος Β.3.19. □

4.1.56 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. 4.1.15.) Θα δείξουμε ότι ο ισχυρισμός είναι αληθής αποδεικνύοντας ότι

$$H = \left\langle \Delta X \Delta^{-1} \cap H \right\rangle , \text{ όπου } \Delta X \Delta^{-1} := \left\{ yxz^{-1} \middle| \, x \in X,\ y,z \in \Delta \right\} .$$

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 $\varepsilon_j \in \{\pm 1\}$ για κάθε $j \in \{1,..,k\}$, για κάποιον $k \in \mathbb{N}$. (Βλ. (2.6).) 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 $\exists h_1 \in H : x_1^{\varepsilon_1} = h_1 g_1$. Ως εκ τούτου,

$$h_1 = x_1^{\varepsilon_1} g_1^{-1} = \left\{ \begin{array}{ll} e_G x_1 g_1^{-1}, & \text{όταν } \varepsilon_1 = 1, \\ \left(g_1 x_1 e_G^{-1}\right)^{-1}, & \text{όταν } \varepsilon_1 = -1. \end{array} \right.$$

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 $k \geq 2$, τότε συνεχίζουμε ως εξής: Προφανώς, υπάρχει

κάποιο $g_2 \in \Delta$, τέτοιο ώστε να ισχύει $g_1 x_2^{\varepsilon_2} \in H g_2$. Άρα $\exists h_2 \in H : g_1 x_2^{\varepsilon_2} = h_2 g_2$. Ως εκ τούτου,

$$h_2 = g_1 x_2^{\varepsilon_2} g_2^{-1} = \begin{cases} g_1 x_2 g_2^{-1}, & \text{όταν } \varepsilon_2 = 1, \\ \left(g_2 x_2 g_1^{-1}\right)^{-1}, & \text{όταν } \varepsilon_2 = -1. \end{cases}$$

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 $k \geq 4$), ορίζουμε αναλόγως στοιχεία $h_3, ..., h_{k-1}$ καταλήγουμε στις ισότητες

$$\begin{aligned} h &= x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k} = x_1^{\varepsilon_1} \left(g_1^{-1} g_1\right) x_2^{\varepsilon_2} \left(g_2^{-1} g_2\right) x_3^{\varepsilon_3} \cdots x_{k-1}^{\varepsilon_{k-1}} \left(g_{k-1}^{-1} g_{k-1}\right) x_k^{\varepsilon_k} \\ &= \left(x_1^{\varepsilon_1} g_1^{-1}\right) \left(g_1 x_2^{\varepsilon_2} g_2^{-1}\right) \left(g_2 x_3^{\varepsilon_3} g_3^{-1}\right) \cdots \left(g_{k-2} x_{k-1}^{\varepsilon_{k-1}} g_{k-1}^{-1}\right) g_{k-1} x_k^{\varepsilon_k} \\ &= h_1 h_2 \cdots h_{k-1} g_{k-1} x_k^{\varepsilon_k}, \end{aligned}$$

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

$$g_{k-1} x_k^{\varepsilon_k} = \begin{cases} g_{k-1} x_k e_G^{-1}, & \text{όταν } \varepsilon_k = 1, \\ \left(e_G x_k g_{k-1}^{-1}\right)^{-1}, & \text{όταν } \varepsilon_k = -1, \end{cases}$$

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 θεώρημα αντιστοιχίσεως υποομάδων 2.4.7, ορίζεται η αμφίριψη

$$\mathbf{Subg}(G; \mathrm{Ker}(f)) \ni K \overset{\Psi_f}{\longmapsto} f(K) \in \mathbf{Subg}(\mathrm{Im}(f))$$

που καθορίζει έναν ισομορφισμό μεταξύ των αντιστοίχων συνδέσμων. Λόγω τής «ισοτονίας» τής Ψ_f έχουμε για οιεσδήποτε $K_1, K_2 \in \mathbf{Subg}(G; \mathrm{Ker}(f))$,

$$K_1 \sqsubseteq K_2 \Longleftrightarrow \Psi_f(K_1) \sqsubseteq \Psi_f(K_2).$$

Φυσικό ερώτημα: Πώς σχετίζονται οι *δείκτες* $|K_2 : K_1|$ και $|\Psi_f(K_2) : \Psi_f(K_1)|$; 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 Ψ_f *διατηρεί και τους δείκτες*.

4.1.57 Πρόταση. (Θεώρημα αντιστοιχίσεως πλευρικών κλάσεων) *Εάν η*

$$f : (G, \cdot) \longrightarrow (H, *)$$

είναι ένας 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*

$$\boxed{|K_2 : K_1| = |\Psi_f(K_2) : \Psi_f(K_1)\,|\,(= |f(K_2) : f(K_1)\,|).}$$

ΑΠΟΔΕΙΞΗ. 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

$$(\Psi_f(K_2) =)\ f(K_2) = \bigcup_{x\in \mathrm{A}} f(x) * f(K_1). \tag{4.26}$$

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 (4.26) είναι αληθής. Θα αποδείξουμε ότι το $f(\mathrm{A}) = \{f(x)\,|x \in \mathrm{A}\}$ είναι ένα σύστημα αριστερών εκπροσώπων τής $\Psi_f(K_1) = f(K_1)$ εντός τής $\Psi_f(K_2) = f(K_2)$. Προς τούτο αρκεί να αποδειχθεί ότι η ένωση στο δεξιό μέλος τής (4.26) 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

$$x_1^{-1}x_2 \in f^{-1}(f(K_1)) = \Upsilon_f(\Psi_f(K_1)) = \mathrm{id}_{\mathbf{Subg}(G;\mathrm{Ker}(f))}(K_1) = K_1,$$

(όπου Υ_f η αντίστροφος τής Ψ_f, βλ. 2.4.7) 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,

$$\mathrm{card}(f(\mathrm{A})) = |f(K_2) : f(K_1)\,|\,(= |\Psi_f(K_2) : \Psi_f(K_1)\,|).$$

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 $\mathfrak{y}$. □

4.1.58 Πόρισμα. *Εάν η* $f : (G, \cdot) \longrightarrow (H, *)$ *είναι ένας ομομορφισμός ομάδων, τότε για οιεσδήποτε* $L_1, L_2 \in \mathbf{Subg}(\mathrm{Im}(f))$ *με* $L_1 \sqsubseteq L_2$ *ισχύει η ισότητα*

$$\boxed{|L_2 : L_1| = |\Upsilon_f(L_2) : \Upsilon_f(L_1)| \,(= |f^{-1}(L_2) : f^{-1}(L_1)|).}$$

ΑΠΟΔΕΙΞΗ. Αρκεί κανείς να επαναλάβει κατά γράμμα την επιχειρηματολογία που χρησιμοποιήθηκε προηγουμένως στην απόδειξη τής προτάσεως 4.1.57 με την Υ_f στη θέση τής Ψ_f. □

4.2 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 και τανάπαλιν.

4.2.1 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*[12] *με την πράξη* "$\cdot$".

ΑΠΟΔΕΙΞΗ. 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. 4.1.11). 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 $gHg^{-1} = H,\ \forall g \in G$.

[12] 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 "${}_H\mathcal{R}$").

(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 "$\mathcal{R}_H$".) □

4.2.2 Ορισμός. Έστω $(G, \cdot)$ μια ομάδα. Μια υποομάδα H τής G ονομάζεται **ορθόθετη**[13] (σημειούμενη συνήθως ως[14] $H \trianglelefteq G$) όταν πληρούται μία (και, κατ' επέκταση, και οιαδήποτε άλλη) εκ των συνθηκών (i)-(vi) τής προτάσεως 4.2.1. (Όταν επιθυμούμε να δώσουμε *έμφαση* στο ότι μια υποομάδα H τής G είναι *γνήσια* ορθόθετη υποομάδα της, γράφουμε "$H \lhd G$".)

4.2.3 Παρατήρηση. Θα πρέπει να δοθεί ιδιαίτερη προσοχή στο ότι οι συνθήκες (iv) και (v) τής προτάσεως 4.2.1 είναι ισοδύναμες μόνον όταν ισχύουν *για κάθε* $g \in G$. Θεωρώντας, επί παραδείγματι, την υποομάδα

$$H := \left\{ \left(\begin{array}{cc} 1 & n \\ 0 & 1 \end{array} \right) \middle| \, n \in \mathbb{Z} \right\}$$

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

$$g \left(\begin{array}{cc} 1 & n \\ 0 & 1 \end{array} \right) g^{-1} = \left(\begin{array}{cc} 1 & 5n \\ 0 & 1 \end{array} \right) \in H,\ \forall n \in \mathbb{Z},$$

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 $H \not\trianglelefteq G$ -κάνοντας χρήση *τού συγκεκριμένου* g- *μόνον μέσω τής* (iv)!)

4.2.4 Παράδειγμα. Στο εδάφιο 4.1.19 έχουμε δείξει ότι η υποομάδα $\langle [1\,2] \rangle$ τής συμμετρικής ομάδας $\mathfrak{S}_3$ δεν είναι ορθόθετη. Κατ' αναλογίαν, $\langle [1\,3] \rangle \not\trianglelefteq \mathfrak{S}_3$ και $\langle [2\,3] \rangle \not\trianglelefteq \mathfrak{S}_3$. Εντούτοις, οι $\{\mathrm{id}\}$, $\langle [1\,2\,3] \rangle$ και $\mathfrak{S}_3$ *είναι* ορθόθετες υποομάδες τής $\mathfrak{S}_3$.

[13] 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.

[14] Κατ' αντιστοιχίαν, ο συμβολισμός "$H \not\trianglelefteq G$" θα σημαίνει ότι η H *δεν είναι ορθόθετη υποομάδα* τής ομάδας G.

4.2.5 Πρόταση. *Η τετριμμένη υποομάδα μιας ομάδας G και η ίδια η G αποτελούν πάντοτε ορθόθετες υποομάδες τής G.*

ΑΠΟΔΕΙΞΗ. Προφανώς, $G \trianglelefteq G$. Εξάλλου, $\forall g \in G$ έχουμε $ge_G = g = e_G g$, οπότε $\{e_G\} \trianglelefteq G$. □

4.2.6 Πρόταση. *Κάθε υποομάδα μιας αβελιανής ομάδας είναι ορθόθετη.*

ΑΠΟΔΕΙΞΗ. Έστω H μια υποομάδα μιας αβελιανής ομάδας $(G, \cdot)$. Τότε για κάθε $g \in G$ έχουμε $gHg^{-1} = \{ghg^{-1} \,|h \in H\} = \{gg^{-1}h \,|h \in H\} = H$, οπότε $H \trianglelefteq G$. □

4.2.7 Παραδείγματα. (i) Κάθε υποομάδα μιας κυκλικής ομάδας είναι ορθόθετη.

(ii) Κάθε υποομάδα τής ομάδας **V** των τεσσάρων στοιχείων τού Klein είναι ορθόθετη (βλ. 3.4.2 (ii) και 4.1.41).

4.2.8 Πρόταση. *Η τομή των μελών οιασδήποτε οικογενείας ορθόθετων υποομάδων $(H_j)_{j\in J}$ μιας ομάδας $(G, \cdot)$ αποτελεί μια ορθόθετη υποομάδα τής $(G, \cdot)$.*

ΑΠΟΔΕΙΞΗ. Σύμφωνα με την πρόταση 2.1.23 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, $g(\bigcap\limits_{j\in J} H_j)g^{-1} \subseteq \bigcap\limits_{j\in J} H_j \Rightarrow \bigcap\limits_{j\in J} H_j \trianglelefteq G$. □

4.2.9 Πρόταση. *Εάν $(H_j)_{j\in J}$ είναι μια οικογένεια ορθόθετων υποομάδων μιας ομάδας $(G, \cdot)$, τότε $\langle\{H_j \,| j \in J\}\rangle \trianglelefteq G$.*

ΑΠΟΔΕΙΞΗ. Έστω τυχόν $h \in \langle\{H_j \,| j \in J\}\rangle$. Σύμφωνα με το πόρισμα 2.2.6, το h γράφεται υπό τη μορφή

$$h = h_{j_1} h_{j_2} \cdots h_{j_k},\ \text{όπου } h_{j_\rho} \in H_{j_\rho},\ \forall \rho \in \{1, ..., k\},\ k \in \mathbb{N}.$$

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, $\langle\{H_j \,| j \in J\}\rangle \trianglelefteq G$. □

4.2.10 Ορισμός. Για *οιοδήποτε υποσύνολο* X τού υποκειμένου συνόλου G μιας ομάδας $(G,\cdot)$, χαρακτηρίζουμε την τομή

$$\boxed{\mathrm{NCL}_G(X) := \bigcap \{K \in \mathbf{Subg}(G) \mid K \trianglelefteq G \text{ και } X \subseteq K\},} \tag{4.27}$$

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. 2.2.1).

4.2.11 Πρόταση. *Έστω* H *μια υποομάδα μιας ομάδας* $(G,\cdot)$. *Τότε ισχύει η αμφίπλευρη συνεπαγωγή*

$$\mathrm{NCL}_G(H) = H \Longleftrightarrow H \trianglelefteq G.$$

ΑΠΟΔΕΙΞΗ. Επειδή $\mathrm{NCL}_G(H) \trianglelefteq G$, η συνεπαγωγή " $\Rightarrow$ " είναι προφανής. Εάν $H \trianglelefteq G$, τότε έχουμε $\mathrm{NCL}_G(H) \trianglelefteq G$ από τον ορισμό (4.27), διότι η H είναι η ελάχιστη ορθόθετη υποομάδα τής G που περιέχει τον εαυτό της, οπότε η " $\Leftarrow$ " είναι ωσαύτως αληθής. □

4.2.12 Πρόταση. *Για οιοδήποτε μη κενό*[15] *υποσύνολο* X *τού υποκειμένου συνόλου* G *μιας ομάδας* $(G,\cdot)$ *έχουμε*

$$\mathrm{NCL}_G(X) = \left\langle \left\{ gxg^{-1} \mid g \in G \text{ και } x \in X \right\} \right\rangle.$$

ΑΠΟΔΕΙΞΗ. 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 2.2.3, $\exists k \in \mathbb{N}$ και

$$(g_1,...,g_k) \in G^k,\ (x_1,...,x_k) \in X^k,\ (\varepsilon_1,...,\varepsilon_k) \in \mathbb{Z}^k,$$

ούτως ώστε να ισχύει

$$h = \left(g_1 x_1 g_1^{-1}\right)^{\varepsilon_1} \cdots \left(g_k x_k g_k^{-1}\right)^{\varepsilon_k} = \left(g_1 x_1^{\varepsilon_1} g_1^{-1}\right) \cdots \left(g_k x_k^{\varepsilon_k} g_k^{-1}\right). \tag{4.28}$$

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 $H \trianglelefteq G$. 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 (4.28) 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

$$\left.\begin{array}{r} g_j \in G \\ x_j^{\varepsilon_j} \in B \trianglelefteq G \end{array}\right\} \Rightarrow g_j x_j^{\varepsilon_j} g_j^{-1} \in B,$$

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 $\mathrm{NCL}_G(X) = H$. □

[15] Εάν $X = \varnothing$, τότε $\mathrm{NCL}_G(X) = \{e_G\}$.

4.2.13 Πρόταση. *Έστω H μια υποομάδα μιας ομάδας $(G,\cdot)$. Εάν ο δείκτης τής H εντός τής G είναι $|G:H|=2$, τότε $H \lhd G$.*

ΑΠΟΔΕΙΞΗ. 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, $H \lhd G$. □

4.2.14 Παράδειγμα. Έστω n ένας φυσικός αριθμός ≥ 2. Επειδή, σύμφωνα με τις προτάσεις 3.1.3 και 3.3.9, $|\mathfrak{S}_n| = n!$ και $|\mathfrak{A}_n| = \frac{n!}{2}$, το θεώρημα 4.1.22 τού Lagrange μας πληροφορεί ότι $|\mathfrak{S}_n : \mathfrak{A}_n| = \frac{|\mathfrak{S}_n|}{|\mathfrak{A}_n|} = 2$. Άρα $\mathfrak{A}_n \lhd \mathfrak{S}_n$.

4.2.15 Παράδειγμα. Έστω n ένας φυσικός αριθμός ≥ 3 και έστω $\mathbf{D}_n = \langle \alpha, \beta \rangle$ η n-οστή διεδρική ομάδα (βλ. 3.4.4). Η κυκλική ομάδα $\langle \beta \rangle$ έχει τάξη n, οπότε από το θεώρημα 4.1.22 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 $\mathbf{D}_n$, διότι $\beta \circ \alpha \circ \beta^{-1} = \alpha \circ \beta^{n-2} \notin \langle \alpha \rangle$. (Όπως θα δούμε στο εδάφιο 4.2.18, υπάρχουν και *μη αβελιανές* ομάδες, *κάθε* υποομάδα των οποίων είναι ορθόθετη.)

4.2.16 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 $\left|gHg^{-1}\right| = |H|$.*

ΑΠΟΔΕΙΞΗ. Επειδή $e_G \in H$, έχουμε $g e_G g^{-1} = e_G \in gHg^{-1}$. Εν συνεχεία θεωρούμε τυχόντα στοιχεία gh_1g^{-1} και gh_2g^{-1} τού gHg^{-1}. Προφανώς,

$$\left(gh_1g^{-1}\right)\left(gh_2g^{-1}\right)^{-1} = \left(gh_1g^{-1}\right)\left(gh_2^{-1}g^{-1}\right) = g(\underbrace{h_1 h_2^{-1}}_{\in H})g^{-1} \in gHg^{-1},$$

οπότε το gHg^{-1} είναι πράγματι μια υποομάδα τής G δυνάμει τού (iii) τής προτάσεως 2.1.16. Επιπροσθέτως, η απεικόνιση $H \ni h \longmapsto ghg^{-1} \in gHg^{-1}$ είναι αμφιρριπτική. Άρα $\left|gHg^{-1}\right| = |H|$. □

4.2.17 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 $H \trianglelefteq G$.*

ΑΠΟΔΕΙΞΗ. Έστω τυχόν στοιχείο $g \in G$. Σύμφωνα με το λήμμα 4.2.16 το σύνολο gHg^{-1} αποτελεί μια υποομάδα τής G τάξεως $\left|gHg^{-1}\right| = |H| = m$. Εξ υποθέσεως, $gHg^{-1} = H \Rightarrow H \trianglelefteq G$. □

4.2.18 Παράδειγμα. Ως παράδειγμα μιας οικείας μας μη αβελιανής ομάδας, κάθε υποομάδα τής οποίας είναι ορθόθετη[16], αναφέρουμε την ομάδα $\mathbf{Q}$ των τετρανίων (βλ. 2.2.11 και 4.1.43). Οι υποομάδες της $\{\mathbf{I}_2\}$ και $\mathbf{Q}$ είναι ορθόθετες λόγω τής προτάσεως 4.2.5, οι υποομάδες $\langle\mathbf{i}\rangle$, $\langle\mathbf{j}\rangle$ και $\langle\mathbf{k}\rangle$ είναι ορθόθετες λόγω τής προτάσεως 4.2.13 (αφού ο δείκτης τους εντός τής $\mathbf{Q}$ ισούται με 2), και η υποομάδα $\langle-\mathbf{I}_2\rangle$ είναι ορθόθετη λόγω τής προτάσεως 4.2.17 (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. 4.2.8).

4.2.19 Πρόταση. *Εάν H και K είναι δυο υποομάδες μιας ομάδας $(G,\cdot)$, τέτοιες ώστε $K \sqsubseteq H$ και $K \trianglelefteq G$, τότε $K \trianglelefteq H$.*

ΑΠΟΔΕΙΞΗ. Θεωρούμε τυχόντα στοιχεία $x \in H$ και $y \in K$. Προφανώς,

$$x \in G,\ K \trianglelefteq G \Rightarrow xyx^{-1} \in K,$$

οπότε $xKx^{-1} \subseteq K \Rightarrow K \trianglelefteq H$. □

4.2.20 Παρατήρηση. Με τα δεδομένα τής προτάσεως 4.2.19 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. 4.1.19).

4.2.21 Παράδειγμα. Η ομάδα $\mathbf{V}$ των τεσσάρων στοιχείων τού Klein (βλ. 3.4.2 (ii)) είναι ορθόθετη υποομάδα τής $\mathfrak{S}_4$. Πράγματι· για οιαδήποτε μετάταξη $\sigma \in \mathfrak{S}_4$ έχουμε (λόγω τού (vii) τής προτάσεως 3.2.3)

$$\begin{aligned}\sigma\circ([1\,2]\circ[3\,4])\circ\sigma^{-1} &= \big(\sigma\circ[1\,2]\circ\sigma^{-1}\big)\circ\big(\sigma\circ[3\,4]\circ\sigma^{-1}\big)\\ &= [\sigma(1)\,\sigma(2)]\circ[\sigma(3)\,\sigma(4)]\end{aligned}$$

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. 4.1.49 και 4.2.14), η πρόταση 4.2.19 μας πληροφορεί ότι $\mathbf{V} \lhd \mathfrak{A}_4$.

4.2.22 Πρόταση. *Εάν H και K είναι δυο υποομάδες μιας ομάδας $(G,\cdot)$, τότε ισχύει η συνεπαγωγή : $K \trianglelefteq G \Longrightarrow K \cap H \trianglelefteq H$.*

ΑΠΟΔΕΙΞΗ. Έστω $h \in H$ και έστω $x \in K \cap H$. Τότε

$$\left.\begin{array}{r} x \in K \\ h \in H \Rightarrow h \in G \end{array}\right\} \underset{K\trianglelefteq G}{\Longrightarrow} hxh^{-1} \in K$$

[16] Μια περιγραφή *όλων* των μη αβελιανών ομάδων, κάθε υποομάδα των οποίων είναι ορθόθετη, δίδεται αργότερα στο θεώρημα 7.5.3.

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, $K \cap H \trianglelefteq H$. □

4.2.23 Πρόταση. *Έστω $(G, \cdot)$ μια ομάδα. Υποθέτουμε ότι $H, K \in \mathbf{Subg}(G)$. Εάν $H \cap K \trianglelefteq H$ και $H \cap K \trianglelefteq K$, τότε $H \cap K \trianglelefteq \langle H, K\rangle$.*

ΑΠΟΔΕΙΞΗ. Έστω $g \in \langle H, K\rangle$. Σύμφωνα με το πόρισμα 2.2.6, 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, $H \cap K \trianglelefteq \langle H, K\rangle$. □

4.2.24 Πρόταση. *Έστω $(G, \cdot)$ μια ομάδα. Υποθέτουμε ότι $H, K \in \mathbf{Subg}(G)$. 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 $HK \trianglelefteq G$.*

ΑΠΟΔΕΙΞΗ. 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. 2.1.16 (iii)) και $HK = KH$ (βλ. πρόταση 4.1.4). (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 $HK \trianglelefteq G$. □

4.2.25 Συμβολισμός. Έστω $(G, \cdot)$ μια ομάδα. Ως

$$\boxed{\mathbf{NSubg}(G) := \{H \in \mathbf{Subg}(G) \mid H \trianglelefteq G\}}$$

συμβολίζουμε το σύνολο όλων των ορθόθετων υποομάδων της. Το ζεύγος $(\mathbf{NSubg}(G), \sqsubseteq)$ αποτελεί ένα μερικώς διατεταγμένο σύνολο (ως προς τη μερική

διάταξη "$\sqsubseteq$" -ή, ακριβέστερα, ως προς την "$\sqsubseteq|_{\mathbf{NSubg}(G)}$"- την επαγομένη επ' αυτού υπό την έννοια τού ορισμού A.2.6.) Επίσης, θέτουμε

$$\mathbf{Min\text{-}NSubg}(G) := \mathbf{Min\text{-}Subg}(G) \cap \mathbf{NSubg}(G) \tag{4.29}$$

και

$$\mathbf{Max\text{-}NSubg}(G) := \mathbf{Max\text{-}Subg}(G) \cap \mathbf{NSubg}(G) \tag{4.30}$$

καλώντας τά στοιχεία τού (4.29) (και αντιστοίχως, τού (4.30)) **ελαχιστικές** (και αντιστοίχως, **μεγιστικές) ορθόθετες υποομάδες τής** G. (Πρβλ. (2.2) και (2.3). Εν προκειμένω, θεωρούνται υποομάδες με την ιδιότητα ΙΔ «τού να είναι ορθόθετες».)

4.2.26 Πρόταση. *Το μερικώς διατεταγμένο σύνολο* $(\mathbf{NSubg}(G), \sqsubseteq)$ *αποτελεί έναν υποσύνδεσμο τού συνδέσμου* $(\mathbf{Subg}(G), \sqsubseteq)$. (Βλ. A.2.25 και 2.1.30.)

ΑΠΟΔΕΙΞΗ. Θεωρούμε τυχούσες $H, K \in \mathbf{NSubg}(G)$. Κατά την πρόταση 4.2.8, $H \wedge K = H \cap K \in \mathbf{NSubg}(G)$. Εξάλλου, σύμφωνα με την πρόταση 4.2.24 έχουμε

$$H \vee K = \langle H, K\rangle = HK \trianglelefteq G \Rightarrow H \vee K \in \mathbf{NSubg}(G).$$

Άρα το μερικώς διατεταγμένο σύνολο $(\mathbf{NSubg}(G), \sqsubseteq)$ είναι όντως υποσύνδεσμος τού $(\mathbf{Subg}(G), \sqsubseteq)$. □

4.2.27 Σημείωση. (Η "$\trianglelefteq$" δεν είναι μεταβατική επί τού $\mathbf{Subg}(G)$.) Εν αντιθέσει προς την "$\sqsubseteq$", η διμελής σχέση "$\trianglelefteq$" *δεν είναι* μερική διάταξη επί τού συνόλου $\mathbf{Subg}(G)$ διότι ναι μεν είναι (προφανώς) αυτοπαθής και αντισυμμετρική αλλά *δεν είναι* μεταβατική: Εάν $K \trianglelefteq H$ και $H \trianglelefteq G$, τότε ενδέχεται να έχουμε $K \ntrianglelefteq G$. 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 $K \lhd \mathbf{V}$ (επί τη βάσει τής προτάσεως 4.2.6) και $\mathbf{V} \lhd \mathfrak{A}_4$ (βλ. 4.2.21). Μολαταύτα, χρησιμοποιώντας τόν 3-κύκλο $\sigma = [1\,2\,3] \in \mathfrak{A}_4$ συμπεραίνουμε ότι $K \ntrianglelefteq \mathfrak{A}_4$, καθόσον

$$\begin{aligned}\sigma \circ ([1\,2] \circ [3\,4]) \circ \sigma^{-1} &= \big(\sigma \circ [1\,2] \circ \sigma^{-1}\big) \circ \big(\sigma \circ [3\,4] \circ \sigma^{-1}\big)\\ &= [\sigma(1)\,\sigma(2)] \circ [\sigma(3)\,\sigma(4)] = [2\,3] \circ [1\,4] = [1\,4] \circ [2\,3] \notin K.\end{aligned}$$

4.2.28 Πρόταση. *Έστω* $(G, \cdot)$ *μια ομάδα. Η "*$\trianglelefteq$*" είναι μεταβατική (και, ως εκ τούτου, μερική διάταξη) επί τού συνόλου* $\mathbf{NSubg}(G)$. *Επιπροσθέτως, το ζεύγος* $(\mathbf{NSubg}(G), \trianglelefteq)$ *είναι σύνδεσμος. Μάλιστα, εν προκειμένω, για τυχούσες ομάδες* $H, K \in \mathbf{NSubg}(G)$ *έχουμε*

$$H \wedge K = H \cap K, \quad H \vee K = \mathrm{NCL}_G(H, K) := \mathrm{NCL}_G(H \cup K).$$

ΑΠΟΔΕΙΞΗ. Εάν $H_1, H_2, H_3 \in \mathbf{NSubg}(G)$ με $H_1 \trianglelefteq H_2$ και $H_2 \trianglelefteq H_3$, τότε

$$\left.\begin{array}{r} H_1 \sqsubseteq H_2,\ H_2 \sqsubseteq H_3 \Rightarrow H_1 \sqsubseteq H_3 \\ H_1 \trianglelefteq G \end{array}\right\} \underset{4.2.19}{\Longrightarrow} H_1 \trianglelefteq H_3.$$

Οι λοιποί ισχυρισμοί είναι προδήλως αληθείς. □

4.2.29 Πόρισμα. *Έστω* $(G,\cdot)$ *μια ομάδα. Εάν* $L \sqsubseteq G$ *και*

$$\boxed{\mathbf{NSubg}(G;L) := \{H \in \mathbf{NSubg}(G) \mid L \sqsubseteq H\} = \mathbf{NSubg}(G) \cap \mathbf{Subg}(G;L)}$$

(βλ. 2.1.32), *τότε το μερικώς διατεταγμένο σύνολο* $(\mathbf{NSubg}(G;L), \trianglelefteq)$ *είναι υποσύνδεσμος τού* $(\mathbf{NSubg}(G), \trianglelefteq)$.

ΑΠΟΔΕΙΞΗ. Για οιεσδήποτε $H, K \in \mathbf{NSubg}(G;L)$, έχουμε

$$H \cap K \in \mathbf{NSubg}(G;L) \ \text{ και } \ \mathrm{NCL}_G(H,K) \in \mathbf{NSubg}(G;L),$$

οπότε το $(\mathbf{NSubg}(G;L), \trianglelefteq)$ είναι όντως υποσύνδεσμος τού $(\mathbf{NSubg}(G), \trianglelefteq)$. □

4.2.30 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* $f^{-1}(L) = \{g \in G \mid f(g) \in L\} \in \mathbf{NSubg}(G; \mathrm{Ker}(f))$.

ΑΠΟΔΕΙΞΗ. (i) Κατά το 2.4.6 (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 2.4.6 (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, $f^{-1}(L) \trianglelefteq G$. □

4.2.31 Πόρισμα. *Ο πυρήνας οιουδήποτε ομομορφισμού ομάδων* $f : (G,\cdot) \to (H,*)$ *είναι ορθόθετη υποομάδα τής* G.

ΑΠΟΔΕΙΞΗ. Άμεση από τα 2.4.4 (ii), 4.2.5 και 4.2.30 (ii), καθόσον ο πυρήνας $\mathrm{Ker}(f)$ είναι εξ ορισμού η αντίστροφη εικόνα τής τετριμμένης υποομάδας τής H μέσω τής απεικονίσεως f. □

4.2.32 Παραδείγματα. (i) Έστω $n \in \mathbb{N}$, $n \geq 2$. Εξ ορισμού, $\mathfrak{A}_n := \mathrm{Ker}(\mathrm{sgn})$, όπου $\mathrm{sgn}: (\mathfrak{S}_n, \circ) \longrightarrow (\{1,-1\},\cdot)$ η απεικόνιση προσημάνσεως (3.11). Κατά το (i) τού

θεωρήματος 3.3.5 και την παρατήρηση 3.3.10 η sgn είναι ένας επιμορφισμός ομάδων. Εάν εφαρμόσουμε το πόρισμα 4.2.31, τότε διαπιστώνουμε εκ νέου ότι $\mathfrak{A}_n \lhd \mathfrak{S}_n$ (πρβλ. 4.2.14).

(ii) Έστω $(R, +, \cdot)$ ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο $1_R \neq 0_R$ και έστω $n \in \mathbb{N}$. 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. 2.1.21 (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 $\mathrm{SU}_n(\mathbb{C}) \lhd \mathrm{U}_n(\mathbb{C})$.

4.3 ΑΠΛΕΣ ΟΜΑΔΕΣ

Ένα σημαντικό τμήμα τής Θεωρίας Ομάδων συναρτάται με τη μελέτη εκείνων των ομάδων που διαθέτουν *τον ελάχιστο δυνατό αριθμό* ορθόθετων υποομάδων.

4.3.1 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*.

4.3.2 Πρόταση. *Κάθε αβελιανή απλή ομάδα είναι κυκλική και έχει ως τάξη της έναν πρώτο αριθμό.*

ΑΠΟΔΕΙΞΗ. Έστω G μια αβελιανή ομάδα. Εάν η G είναι απλή, τότε, σύμφωνα με την πρόταση 4.2.6, οι μόνες υποομάδες της είναι η τετριμμένη και ο εαυτός της. Αρκεί λοιπόν η εφαρμογή τού πορίσματος 4.1.35. □

4.3.3 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[17]. Ο πλήρης κατάλογος των μη αβελιανών απλών πεπερασμένων ομάδων υποδιαιρείται σε τρεις κλάσεις ομάδων. Αυτές είναι οι εξής:

(i) Οι *εναλλάσσουσες ομάδες* $\mathfrak{A}_n$, $n \geq 5$ (βλ. θεώρημα 4.3.6).

(ii) 16 απειροπληθείς οικογένειες ομάδων *τύπου Lie*[18]. (Ο κατάλογός τους με τους συμβολισμούς τους και τις τάξεις τους θα δοθεί στην ενότητα ??.)

(iii) Οι *σποραδικές ομάδες*[19], ήτοι 26 ειδικές απλές ομάδες που δεν εντάσσονται στις (i)-(ii). (Βλ. τον κατάλογο IV τής ενότητας ??.)

► **Απλότητα των $\mathfrak{A}_n$, $n \geq 5$, 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. 4.2.21). Για να αποδείξουμε την απλότητα τής $\mathfrak{A}_n$ όταν $n \geq 5$ θα προτάξουμε δύο βοηθητικά λήμματα.

4.3.4 Λήμμα. *Έστω $n \in \mathbb{N}$, $n \geq 5$. Εάν η H είναι μια ορθόθετη υποομάδα τής $\mathfrak{A}_n$ περιέχουσα (τουλάχιστον) έναν 3-κύκλο, τότε $H = \mathfrak{A}_n$.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι $H \trianglelefteq \mathfrak{A}_n$ και ότι η H περιέχει τον 3-κύκλο $[\alpha\ \beta\ \gamma]$. Θεωρούμε *τυχόν* στοιχείο $i \in \{1,...,n\} \setminus \{\alpha, \beta, \gamma\}$. Τότε

$$\begin{aligned}
[\alpha\ \beta\ i] &= [i\,\alpha\,\beta] = [i\ \alpha] \circ [\alpha\ \beta] = [\alpha\ \beta] \circ [\alpha\ i\ \beta] \circ [\alpha\ \beta] \\
&= [\alpha\ \beta] \circ [i\ \gamma\ \alpha\ \beta] \circ [\alpha\ \beta\ \gamma\ i] \circ [\alpha\ \beta] \\
&= [\alpha\ \beta] \circ [i\ \gamma] \circ [\gamma\ \alpha\ \beta] \circ [\alpha\ \beta\ \gamma\ i] \circ [\alpha\ \beta] \\
&= [\alpha\ \beta] \circ [\gamma\ i] \circ [\alpha\ \beta\ \gamma]^2 \circ [\gamma\ i] \circ [\alpha\ \beta] \\
&= \underbrace{([\alpha\ \beta] \circ [\gamma\ i])}_{\in \mathfrak{A}_n} \circ \underbrace{[\alpha\ \beta\ \gamma]^2}_{\in H} \circ \underbrace{([\alpha\ \beta] \circ [\gamma\ i])^{-1}}_{\in \mathfrak{A}_n},
\end{aligned}$$

[17] Για περισσότερες πληροφορίες ο αναγνώστης παραπέμπεται στα συγγράμματα των

D. Gorenstein: *Finite Simple Groups: An Introduction to their Classification*, Plenum Press, (1982); *The Classification of Finite Simple Groups* I, Plenum Press, (1983), και

M. Aschbacher: *Finite Group Theory*, Cambridge St. in Adv. Math., Vol. **10**, Cambridge Un. Press, (1994). [Κεφ. 16],

καθώς και στον «ΑΤΛΑΝΤΑ των πεπερασμένων ομάδων»

J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson: ATLAS *of finite groups*, Clarendon Press, (1985).

Πιο πρόσφατα κυκλοφόρησε το δίτομο έργο των D. Gorenstein, R. Lyons και R. Solomon: *The Classification of Finite Simple Groups*, American Math. Soc. (Vol. I, 1994; Vol. II, 1996) με στόχο την αναθεώρηση και συντόμευση των αποδείξεων των θεωρημάτων που οδηγούν στην εν λόγω ταξινόμηση.

[18] Βλ. R.W. Carter: *Simple Groups of Lie Type*, Wiley, (1972).

[19] Βλ. M. Aschbacher: *Sporadic Groups*, Cambridge Tracts in Math., Vol. **104**, Cambridge University Press, (1994).

οπότε $[\alpha\ \beta\ i] \in H$. Κατά συνέπειαν, $\{[\alpha\ \beta\ i]\ \mid i \in \{1,...,n\}\setminus\{\alpha,\beta\}\} \subseteq H$. Όμως αυτό το υποσύνολο παράγει την εναλλάσσουσα ομάδα $\mathfrak{A}_n$ (επί τη βάσει τού (iii) τής προτάσεως 3.3.13). Ως εκ τούτου, $H = \mathfrak{A}_n$. □

4.3.5 Λήμμα. *Έστω $n \in \mathbb{N}$, $n \geq 5$. Εάν η H είναι μια ορθόθετη υποομάδα τής $\mathfrak{A}_n$ περιέχουσα τη σύνθεση δύο ξένων μεταξύ τους αντιμεταθέσεων, τότε $H = \mathfrak{A}_n$.*

ΑΠΟΔΕΙΞΗ. 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 $\beta \in \{1,...,n\}\setminus\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$, 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 3.2.3 (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 4.3.4 συμπεραίνουμε ότι $H = \mathfrak{A}_n$. □

4.3.6 Θεώρημα. *Οι εναλλάσσουσες ομάδες $\mathfrak{A}_n$ είναι απλές για κάθε $n \geq 5$.*

ΑΠΟΔΕΙΞΗ[20]. Έστω H μια μη τετριμμένη ορθόθετη υποομάδα τής $\mathfrak{A}_n$, $n \geq 5$, και έστω $\sigma \in H\setminus\{\mathrm{id}\}$. Σύμφωνα με το θεμελιώδες θεώρημα 3.2.7 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 ≥ 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

$$(\text{μήκος τού } \tau_j) \geq (\text{μήκος τού } \tau_{j+1}),\ \forall j \in \{1,2,...,\nu-1\}$$

(όταν $\nu \geq 2$) και ότι $\tau_1 = [\alpha_1\ \alpha_2 ...\ \alpha_k]$. Εξετάζουμε τα πέντε ενδεχόμενα χωριστά:
Περίπτωση πρώτη. Υποθέτουμε ότι $k \geq 4$, $\nu \geq 1$. Θέτοντας $c := [\alpha_1\ \alpha_2\ \alpha_3] \in \mathfrak{A}_n$ παρατηρούμε ότι

$$c \in \mathfrak{A}_n,\ \sigma \in H \Rightarrow c \circ \sigma \circ c^{-1} \in H,$$

[20] 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).

οπότε $\sigma^{-1} \in H \Rightarrow \left(c \circ \sigma \circ c^{-1}\right) \circ \sigma^{-1} \in H$. Επειδή (κατά το 3.2.3 (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 4.3.4.

Περίπτωση δεύτερη. Εάν $k = 3, \nu = 1$, τότε $H = \mathfrak{A}_n$ (με απευθείας εφαρμογή τού λήμματος 4.3.4).

Περίπτωση τρίτη. Υποθέτουμε ότι $k = 3$, $\nu \geq 2$, 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 3.2.3 (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. 3.2.3 (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 $k = 3$, $\nu \geq 2$, και ότι όλοι οι κύκλοι $\tau_2,...,\tau_\nu$ 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. 3.2.3 (iv), (v), και 3.2.4). Επειδή η H περιέχει τον 3-κύκλο $[\alpha_1\ \alpha_3\ \alpha_2]$, $H = \mathfrak{A}_n$ δυνάμει τού λήμματος 4.3.4.

Περίπτωση πέμπτη. Υποθέτουμε ότι $k = 2$, $\nu \geq 2$, και ότι όλοι οι κύκλοι $\tau_1,...,\tau_\nu$ είναι αντιμεταθέσεις, με τον φυσικό αριθμό ν κατ' ανάγκην *άρτιο* (αφού $\sigma \in \mathfrak{A}_n$). Εάν $\tau_2 = [\beta_1\ \beta_2]$, 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 3.2.3 (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. 3.2.3 (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 4.3.5. □

4.3.7 Σημείωση. Παρά το γεγονός ότι η ανωτέρω παρατεθείσα *κλασική* απόδειξη τού θεωρήματος 4.3.6 είναι διαυγής, η διάκριση και μελέτη τόσο πολλών περιπτώσεων είναι ομολογουμένως κατά τι κοπιαστική. Στη σελίδα 251 δίδεται μια δεύτερη, *επαγωγική* απόδειξη (προϋποθέτουσα την απλότητα τής $\mathfrak{A}_5$ που μπορεί να δειχθεί στοιχειωδώς) στην οποία υπεισέρχεται μόνον το αρχικό λήμμα 4.3.4 και στο (ii) τής ασκήσεως **5-27** μια τρίτη.

4.3.8 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[21] μήκους 3, καλείται **άπειρη εναλλάσσουσα ομάδα επί τού $\mathbb{N}$** (και αποτελεί άμεση γενίκευση τής $\mathfrak{A}_n$, πρβλ. 3.3.13 (ii)). Ακολουθώντας κατά γράμμα την αποδεικτική μέθοδο που εφαρμόσθηκε στο θεώρημα 4.3.6 καταλήγουμε στη διαπίστωση τού ότι η $\mathfrak{A}_\infty$ είναι ωσαύτως απλή. Ως εκ τούτου, η $\mathfrak{A}_\infty$ αποτελεί *παράδειγμα άπειρης απλής ομάδας*. (Γενικότερα, για την κατασκευή μιας άπειρης απλής ομάδας *για κάθε* άπειρο πληθάριθμο βλ. άσκηση **4-65**. Εν προκειμένω, $\mathfrak{A}_\infty = \mathfrak{A}_{(\mathbb{N})}$.)

4.3.9 Θεώρημα. *Κάθε πεπερασμένη ομάδα εμφυτεύεται σε μια πεπερασμένη απλή ομάδα* (βλ. 2.4.14 και 2.4.17).

ΑΠΟΔΕΙΞΗ. Έστω G τυχούσα πεπερασμένη ομάδα τάξεως $n = |G| \geq 1$. 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 $n \geq 4$, τότε (σύμφωνα με το πόρισμα 3.5.3) 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 $k \in \{2,...,n\}$ αντιστοιχίζουμε τον 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 3.3.5). Εκφράζοντας κάθε μετάταξη $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{id}\}$ υπό τη μορφή επαλλήλων συνθέσεων (πεπερασμένου πλήθους) ανά δύο ξένων μεταξύ τους κύκλων μήκους ≥ 2, ας πούμε $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_\nu$, κατά το θεμελιώδες θεώρημα 3.2.7, 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 3.2.4). Κατά συνέπειαν, η ίδια η G είναι εμφυτεύσιμη εντός τής $\mathfrak{A}_{2n}$ (βάσει τού (ii) τής προτάσεως 2.4.12). Όμως η $\mathfrak{A}_{2n}$ είναι *απλή ομάδα*, αφού εξ υποθέσεως $2n \geq 8$ (βλ. θεώρημα 4.3.6). □

[21] 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. 3.2.1), με μόνη διαφορά ότι $\sigma(\beta) = \beta$ *για κάθε* $\beta \in \mathbb{N} \setminus \{a_1, a_2, ..., a_k\}$.

4.3.10 Πόρισμα. *Έστω R ένας μη τετριμμένος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Κάθε πεπερασμένη ομάδα τάξεως $n \geq 4$ εμφυτεύεται στην ειδική γραμμική ομάδα* $\mathrm{SL}_{2n}(R)$.

ΑΠΟΔΕΙΞΗ. Έστω G τυχούσα πεπερασμένη ομάδα τάξεως $n \geq 4$. Τότε υφίστανται τρεις μονομορφισμοί ομάδων

$$G \hookrightarrow \mathfrak{S}_n \hookrightarrow \mathfrak{A}_{2n} \hookrightarrow \mathrm{SL}_{2n}(R).$$

(Ο πρώτος λόγω τού πορίσματος 3.5.3, ο δεύτερος βάσει των προαναφερθέντων στην απόδειξη τού θεωρήματος 4.3.9 και ο τρίτος βάσει των προαναφερθέντων στο εδάφιο D.2.28 (ii).) Οι συνθέσεις αυτών δίδουν μια εμφύτευση τής G στην $\mathrm{SL}_{2n}(R)$. □

► **Ορθόθετες υποομάδες τής** $\mathfrak{S}_n$, $n \geq 5$. Το θεώρημα 4.3.12 μας πληροφορεί ότι για φυσικούς αριθμούς $n \geq 5$ ακόμη και η ίδια η συμμετρική ομάδα $\mathfrak{S}_n$ δεν διαθέτει άλλες ορθόθετες υποομάδες πέραν των (τριων) προφανών. Για την απόδειξή του θα χρησιμοποιήσουμε το ακόλουθο:

4.3.11 Λήμμα. *Εάν $n \in \mathbb{N}, n \geq 3$, 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, $\sigma \circ \varrho = \varrho \circ \sigma$), $\forall \varrho \in \mathfrak{S}_n$.

ΑΠΟΔΕΙΞΗ. 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 3.2.7) γράφεται υπό τη μορφή επαλλήλων συνθέσεων (πεπερασμένου πλήθους) ανά δύο ξένων μεταξύ τους κύκλων μήκους ≥ 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 $k \in \mathbb{N}, 2 \leq k \leq n$. Εξετάζουμε δύο περιπτώσεις χωριστά:

Περίπτωση πρώτη. Εάν $k \geq 3$, τότε θεωρώντας ως ϱ τον 2-κύκλο $[a_1\ a_2]$ καταλήγουμε σε άτοπο, καθόσον (κατά το 3.2.3 (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 $a_3 \in \{1, ..., n\} \smallsetminus \{a_1, a_2\}$, καταλήγουμε εκ νέου σε άτοπο, καθόσον (κατά το 3.2.3 (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 $\left(\sigma \circ \varrho \circ \sigma^{-1}\right)(a_2) = a_1 \neq a_3 = \varrho(a_2)$. □

4.3.12 Θεώρημα. *Εάν $n \in \mathbb{N}, n \geq 5$, τότε οι $\{\mathrm{id}\}, \mathfrak{A}_n$ και $\mathfrak{S}_n$ είναι οι μόνες ορθόθετες υποομάδες τής $\mathfrak{S}_n$.*

ΑΠΟΔΕΙΞΗ. Έστω H τυχούσα ορθόθετη υποομάδα τής $\mathfrak{S}_n$. Τότε

$$\left.\begin{array}{r} H \trianglelefteq \mathfrak{S}_n \text{ (εξ υποθέσεως)} \\ \mathfrak{A}_n \lhd \mathfrak{S}_n \ \text{(βλ. 4.2.14)} \end{array}\right\} \underset{\text{(βλ. 4.2.8)}}{\Longrightarrow} H \cap \mathfrak{A}_n \lhd \mathfrak{S}_n$$

και

$$\left.\begin{array}{r} H \sqsubseteq \mathfrak{S}_n,\ \mathfrak{A}_n \sqsubseteq \mathfrak{S}_n \underset{2.1.23}{\Longrightarrow} H \cap \mathfrak{A}_n \sqsubseteq \mathfrak{S}_n \\ H \cap \mathfrak{A}_n \subseteq \mathfrak{A}_n \sqsubseteq \mathfrak{S}_n \underset{2.1.20}{\Longrightarrow} H \cap \mathfrak{A}_n \sqsubseteq \mathfrak{A}_n \\ H \cap \mathfrak{A}_n \lhd \mathfrak{S}_n \text{ (λόγω των προαναφερθέντων)} \end{array}\right\} \underset{4.2.19}{\Longrightarrow} H \cap \mathfrak{A}_n \trianglelefteq \mathfrak{A}_n$$

$$\underset{4.3.6}{\Longrightarrow} H \cap \mathfrak{A}_n \in \{\{\mathrm{id}\}, \mathfrak{A}_n\}.$$

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 4.1.50) 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 3.3.6) 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. 3.3.6 (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 4.3.11, κάποιο στοιχείο $\varrho \in \mathfrak{S}_n$, τέτοιο ώστε να ισχύει $\sigma \circ \varrho \circ \sigma^{-1} \neq \varrho$. Ως εκ τούτου,

$$\left.\begin{array}{c} H \trianglelefteq \mathfrak{S}_n \Rightarrow \varrho \circ \sigma \circ \varrho^{-1} \in \{\mathrm{id}, \sigma\} = H \\ \sigma \circ \varrho \circ \sigma^{-1} \neq \varrho \Rightarrow \varrho \circ \sigma \circ \varrho^{-1} \neq \sigma \end{array}\right\} \Rightarrow \varrho \circ \sigma \circ \varrho^{-1} = \mathrm{id} \Rightarrow \varrho \circ \sigma = \varrho \Rightarrow \sigma = \mathrm{id}.$$

Άτοπο! Επομένως, $H = \{\mathrm{id}\}$. □

4.4 ΠΗΛΙΚΟΟΜΑΔΕΣ: ΚΑΤΑΣΚΕΥΗ-ΙΔΙΟΤΗΤΕΣ

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.

4.4.1 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 $\pi_H^G(g) := gH, \forall g \in G$).

4.4.2 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

$$\begin{array}{ccc} G\times G & \xrightarrow{\ \cdot\ } & G \\ {\scriptstyle \pi_H^G\times\pi_H^G}\downarrow & & \downarrow{\scriptstyle \pi_H^G} \\ (G/H)\times(G/H) & \xrightarrow[\ \odot\ ]{} & G/H \end{array}$$

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 $|G/H|=\frac{|G|}{|H|}$.*

ΑΠΟΔΕΙΞΗ. Εάν $g_1,g_2,g_3\in G$, τότε

$$\begin{aligned}(g_1H\odot g_2H)\odot g_3H &= ((g_1\cdot g_2)\,H)\odot g_3H=((g_1\cdot g_2)\cdot g_3)\,H\\ &= (g_1\cdot(g_2\cdot g_3))\,H=g_1H\odot((g_2\cdot g_3)\,H)\\ &= g_1H\odot(g_2H\odot g_3H)\,,\end{aligned}$$

οπότε η "$\odot$" είναι προσεταιριστική. Επίσης, για κάθε $g\in G$,

$$(e_GH\odot gH)=(e_G\cdot g)\,H=gH=(g\cdot e_G)\,H=(gH\odot e_GH)\,,$$

πράγμα που σημαίνει ότι το G/H έχει το $e_GH\,(=H)$ ως ουδέτερο στοιχείο του ως προς την "$\odot$". Τέλος, για κάθε $g\in G$,

$$\left(g^{-1}H\odot gH\right)=\left(g^{-1}\cdot g\right)H=e_GH=\left(g\cdot g^{-1}\right)H=\left(g^{-1}H\odot gH\right),$$

οπότε το (μονοσημάντως ορισμένο) συμμετρικό (= αντίστροφο) στοιχείο οιουδήποτε $gH\in G/H$ ως προς την "$\odot$" είναι το $g^{-1}H$, το (i) είναι αληθές και το ζεύγος $(G/H,\odot)$ αποτελεί μια ομάδα τάξεως $|G/H|=|G:H|$ με $e_{G/H}=e_GH=H$. Μάλιστα, εάν η G είναι αβελιανή, τότε για οιαδήποτε στοιχεία $g_1,g_2\in G$ ισχύουν οι ισότητες

$$g_1H\odot g_2H=(g_1\cdot g_2)\,H=(g_2\cdot g_1)\,H=g_2H\odot g_1H,$$

απ' όπου έπεται ότι η $(G/H,\odot)$ είναι ωσαύτως αβελιανή. Άρα και το (ii) είναι αληθές. Το (iii) έπεται άμεσα από το θεώρημα 4.1.22 τού Lagrange. □

4.4.3 Ορισμός. Η ομάδα $(G/H, \odot)$ η ορισθείσα μέσω τής προτάσεως 4.4.2 καλείται **πηλικοομάδα** (ή **ομάδα πηλίκων**) τής 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».)

4.4.4 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[22] $(gH)\,(g'H)$ 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 4.4.2 (και που απλώς *επάγεται* μέσω τού «πολλαπλασιασμού» τού ορισμένου επί τού G).

4.4.5 Παραδείγματα. Έστω $(G,\cdot)$ τυχούσα ομάδα. Τότε $\{e_G\} \trianglelefteq G$ και $G \trianglelefteq G$ (βλ. 4.2.5). Προφανώς,

$$G/\{e_G\} = \{\, g\{e_G\} \,|\, g \in G\} \cong G \quad \text{και} \quad G/G \cong \{e_G\},$$

διότι οι απεικονίσεις

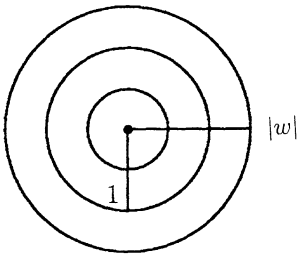
$$G/\{e_G\} \ni g\{e_G\} \longmapsto g \in G \quad \text{και} \quad G/G \ni gG \longmapsto e_G \in \{e_G\}$$

είναι ισομορφισμοί ομάδων.

4.4.6 Παράδειγμα. Η ομάδα $(\mathbb{S}^1,\cdot)$ είναι ορθόθετη υποομάδα τής πολλαπλασιαστικής ομάδας $(\mathbb{C}\smallsetminus\{0\},\cdot)$ (βλ. 2.1.21 (vi) και 4.2.5). 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

$$\begin{aligned} w\mathbb{S}^1 &= [w]_{{}_{\mathbb{S}^1}\mathcal{R}} = \{\, z \in \mathbb{C}\smallsetminus\{0\} \mid (z,w) \in {}_{\mathbb{S}^1}\mathcal{R}\} = \{\, z \in \mathbb{C}\smallsetminus\{0\} \mid z^{-1}w \in \mathbb{S}^1\} \\ &= \{\, z \in \mathbb{C}\smallsetminus\{0\} \mid |z^{-1}w| = 1\} = \{\, z \in \mathbb{C}\smallsetminus\{0\} \mid |z| = |w|\} \end{aligned}$$

είναι η περιφέρεια κύκλου κέντρου $0 \in \mathbb{C}$ και ακτίνας $|w|$.



Επομένως, τα στοιχεία τής $(\mathbb{C}\smallsetminus\{0\})/\mathbb{S}^1$ είναι οι ομόκεντροι κύκλοι κέντρου $0 \in \mathbb{C}$ και θετικής ακτίνας.

[22] Όταν χρησιμοποιούμε *προσθετικό συμβολισμό*, γράφουμε αντ' αυτού $(g+H)+(g'+H)$.

4.4.7 Παράδειγμα. Η ομάδα $(\mathbb{Z},+)$ είναι ορθόθετη υποομάδα τής ομάδας $(\mathbb{Q},+)$ (βλ. 4.2.6). Το υποκείμενο σύνολο τής πηλικοομάδας $(\mathbb{Q}/\mathbb{Z},+)$ γράφεται ως εξής:

$$\mathbb{Q}/\mathbb{Z} = \coprod \{\, \lambda + \mathbb{Z} \mid \lambda \in \mathbb{Q} \cap [0,1) \}\,,$$

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 $0 \leq r < b$, 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 $|\lambda_1 - \lambda_2| = |c| \geq 1$ (πράγμα αδύνατο, καθόσον $0 \leq \lambda_1, \lambda_2 < 1$).

4.4.8 Παράδειγμα. Έστω n ένας φυσικός αριθμός ≥ 3 και έστω $\mathbf{D}_n = \langle \alpha, \beta \rangle$ η n-οστή διεδρική ομάδα (βλ. 3.4.4). Ως γνωστόν, $\langle\beta\rangle \lhd \mathbf{D}_n$ (βλ. 4.2.15). 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. 2.2.17). Κατά συνέπειαν, το αντίστροφο τού (ii) τής προτάσεως 4.4.2 δεν είναι πάντοτε ορθό (διότι η ίδια η $\mathbf{D}_n$ δεν είναι αβελιανή).

4.4.9 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \trianglelefteq G$. Τότε για τις δυνάμεις των στοιχείων τής πηλικοομάδας G/H ισχύει η ισότητα*

$$(gH)^n = g^n H,\ \forall g \in G \text{ και } \forall n \in \mathbb{Z}.$$

ΑΠΟΔΕΙΞΗ. 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 $n \geq 1$. Τότε

$$(gH)^{n+1} = \ (gH)^n\,(gH) = (g^nH)\,(gH) = (g^n gH) = g^{n+1}H.$$

Εάν $n \in \mathbb{Z}\smallsetminus\mathbb{N}_0$, τότε $-n > 0$, οπότε εφαρμόζοντας το ανωτέρω αποδειχθέν για τον $-n$, το (i) τής προτάσεως 4.4.2, καθώς και το (iii) τής προτάσεως 2.1.11, 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 $\forall n \in \mathbb{Z}$. □

4.4.10 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \trianglelefteq G$. Για οιοδήποτε $g \in G$ η τάξη τού στοιχείου gH τής G/H ισούται με*

$$\operatorname{ord}(gH) = \begin{cases} \infty, & \text{όταν } g^k \notin H,\ \forall k \in \mathbb{N}, \\ \min\left\{ k \in \mathbb{N} \mid\ g^k \in H \right\}, & \text{στην αντίθετη περίπτωση.} \end{cases}$$

ΑΠΟΔΕΙΞΗ. Έστω τυχόν στοιχείο $g \in G$. Εάν $g^k \notin H$ για κάθε $k \in \mathbb{N}$, τότε έχουμε $g^k H = (gH)^k \neq H$, $\forall k \in \mathbb{N}$, οπότε $\operatorname{ord}(gH) = \infty$. 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 $m = \min\{ k \in \mathbb{N} \mid\ (gH)^k = H\} = \operatorname{ord}(gH)$. □

4.4.11 Παράδειγμα. Η πηλικοομάδα $(\mathbb{Q}/\mathbb{Z},+)$ (βλ. 4.4.7) 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 4.4.9 και 4.4.10 έπεται ότι

$$b\,(\xi + \mathbb{Z}) = b\xi + \mathbb{Z} = a + \mathbb{Z} = \mathbb{Z} \Rightarrow b\xi \in \mathbb{Z} \Rightarrow\ \operatorname{ord}(\xi + \mathbb{Z}) \leq b < \infty.$$

4.4.12 Πρόταση. *Εάν $(G,\cdot)$ είναι μια πεπερασμένη ομάδα, τότε*

$$\exp(G/H) \mid \exp(G),\ \forall H \in \mathbf{NSubg}(G).$$

ΑΠΟΔΕΙΞΗ. Εάν $H \trianglelefteq G$ και $g \in H$, τότε για την πλευρική κλάση gH έχουμε

$$(gH)^{\operatorname{ord}(g)} = g^{\operatorname{ord}(g)} H = e_G H = H = e_{G/H} \Longrightarrow \operatorname{ord}(gH) \mid \operatorname{ord}(g).$$

Εξ αυτού έπεται ότι

$$\exp(G/H) = \text{εκπ}(\{\operatorname{ord}(gH) \mid g \in G\}) \mid \text{εκπ}(\{\operatorname{ord}(g) \mid g \in G\}) = \exp(G).$$

(Βλ. το (i) τής προτάσεως 2.3.25.) □

► **Ιδιότητες τού φυσικού επιμορφισμού**. Τα στοιχεία δοθείσας πηλικοομάδας G/H είναι οι εικόνες των στοιχείων τής G μέσω τού επιμορφισμού (4.31). Η μελέτη των ιδιοτήτων του είναι, ως εκ τούτου, απαραίτητη για την ομαδοθεωρητική περιγραφή τής ίδιας τής G/H.

4.4.13 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \trianglelefteq G$. Η φυσική επίρριψη*

$$\boxed{\pi_H^G : G \longrightarrow G/H,\ \ g \longmapsto \pi_H^G(g) := gH,} \tag{4.31}$$

(βλ. 4.4.1) *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.*

ΑΠΟΔΕΙΞΗ. Αρκεί να αποδείξουμε ότι η π_H^G είναι ομομορφισμός ομάδων και ότι $\operatorname{Ker}(\pi_H^G) = H$. 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, $\operatorname{Ker}(\pi_H^G) = \{g \in G \,|\, \pi_H^G(g) = H\} = \{g \in G \,|\, gH = H\} = H$. □

4.4.14 Πόρισμα. *Έστω υποομάδα H μιας ομάδας $(G,\cdot)$. Τότε $H \trianglelefteq G$ εάν και μόνον εάν η H αποτελεί τον πυρήνα ενός ομομορφισμού ομάδων $f : (G,\cdot) \longrightarrow (K,*)$.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από την πρόταση 4.4.13 και το πόρισμα 4.2.31. □

4.4.15 Πόρισμα. (Θεώρημα αντιστοιχίσεως υποομάδων μέσω τού π_H^G.) *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \trianglelefteq G$. Τότε ορίζεται η αμφιρριπτική απεικόνιση*

$$\boxed{\mathbf{Subg}(G;H) \ni K \overset{\Psi_{\pi_H^G}}{\longmapsto} \pi_H^G(K) \in \mathbf{Subg}(G/H)}$$

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[23] *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*

$$K_1 \sqsubseteq K_2 \iff K_1/H \sqsubseteq K_2/H.$$

(ii) *H $\Psi_{\pi_H^G}$ καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων*

$$(\mathbf{Subg}(G;H), \sqsubseteq) \quad \textit{και} \quad (\mathbf{Subg}(G/H), \sqsubseteq)$$

(βλ. 2.1.30, 2.1.32, και A.2.26).

(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*

$$|L_2 : L_1| = |(\pi_H^G)^{-1}(L_2) : (\pi_H^G)^{-1}(L_1)|.$$

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα ύστερα από εφαρμογή τού θεωρήματος αντιστοιχίας υποομάδων 2.4.7, τής προτάσεως 4.1.57 και τού πορίσματος 4.1.58 για τον φυσικό επιμορφισμό (4.31). □

4.4.16 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 $m \mid n$.*

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμοσθεί το (iv) τής προτάσεως 2.4.3 για τον φυσικό επιμορφισμό (4.31). □

[23] Σημειωτέον ότι για κάθε υποομάδα K τής G που περιέχει την H έχουμε $H \trianglelefteq K$ (λόγω τής προτάσεως 4.2.19, ύστερα από εναλλαγή των ρόλων των σε αυτήν παρατεθεισών υποομάδων H και K), οπότε η εικόνα $\pi_H^G(K)$ τής K μέσω τού φυσικού επιμορφισμού (4.31) είναι αφ' εαυτής *πηλικοομάδα*.

4.4.17 Παράδειγμα. Εάν θεωρήσουμε την υποομάδα $H := \langle \mathbf{i} \rangle$ τής ομάδας $\mathbf{Q}$ των τετρανίων (βλ. 2.2.11), 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.

4.4.18 Πρόταση. *Έστω X ένα σύστημα γεννητόρων μιας ομάδας $(G, \cdot)$ και έστω $H \trianglelefteq G$. Τότε*

$$\boxed{G/H = \langle \{ xH \mid x \in X \} \rangle .}$$

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το (i) τής προτάσεως 2.4.9,

$$G/H = \pi_H^G(G) = \pi_H^G(\langle X \rangle) = \left\langle \pi_H^G(X) \right\rangle ,$$

όπου $\pi_H^G(X) = \left\{ \pi_H^G(x) \;\middle|\; x \in X \right\} = \{ xH \mid x \in X \}$. □

4.4.19 Πόρισμα. *Έστω H μια υποομάδα μιας κυκλικής ομάδας $(G, \cdot)$. Τότε η G/H είναι κυκλική. Ειδικότερα, για κάθε γεννήτορα g τής G έχουμε $G/H = \langle gH \rangle$.*

ΑΠΟΔΕΙΞΗ. Η G ως κυκλική είναι αβελιανή (βλ. 2.2.17), οπότε η H είναι ορθόθετη (βλ. 4.2.6). Ως εκ τούτου, ορίζεται η πηλικομάδα G/H. Αρκεί λοιπόν να εφαρμοσθεί η πρόταση 4.4.18 για το $X = \{g\}$, όπου g οιοσδήποτε γεννήτορας τής G. □

4.4.20 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. 3.5.6).

► **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 4.4.2, σε συνδυασμό με το θεώρημα 4.4.21, μας δίδουν τη δυνατότητα επαγωγικής αποδείξεως τής υπάρξεως μιας υποομάδας H τής G τάξεως $|H| = k$ *για κάθε* διαιρέτη k τής $|G|$.

4.4.21 Θεώρημα. («Θεώρημα τού Cauchy για αβελιανές ομάδες».) *Έστω $(G,\cdot)$ μια πεπερασμένη αβελιανή ομάδα. Εάν $p \mid |G|$, όπου p κάποιος πρώτος αριθμός, τότε $\exists g \in G\setminus\{e_G\} : \mathrm{ord}(g) = p$, ήτοι η κυκλική ομάδα $\langle g\rangle$ είναι μια υποομάδα τής G τάξεως p* (βλ. (2.9)).

ΑΠΟΔΕΙΞΗ. 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. 4.1.27), οπότε $\mathrm{ord}(g) = p$ για κάθε $g \in G\setminus\{e_G\}$. 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. 4.1.35). 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

$$\left.\begin{aligned} |G| = pn = |G:L|\cdot|L| \\ p \nmid |L| \underset{\text{B.3.16}}{\Longrightarrow} \mu\kappa\delta(p,|L|) = 1 \end{aligned}\right\} \underset{\text{B.2.9}}{\Longrightarrow} p \mid |G:L| \Rightarrow \exists k \in \mathbb{N} : |G:L| = pk.$$

Επειδή η G είναι αβελιανή, $L \lhd G$ (βλ. 4.2.6). Επομένως ορίζεται η πηλικοομάδα G/L, η δε τάξη της ισούται με $|G/L| = |G:L| = pk$ (βλ. 4.4.2), όπου $k < n$, διότι (εξ υποθέσεως) $|L| > 1$. Σύμφωνα με το (ii) τής προτάσεως 4.4.2 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

$$g^pL = (gL)^p = e_{G/L} = L \Rightarrow g^p \in L \underset{\text{4.1.28}}{\Longrightarrow} (g^p)^{|L|} = e_G = (g^{|L|})^p \underset{\text{2.3.8}}{\Longrightarrow} \mathrm{ord}(g^{|L|}) \mid p,$$

απ' όπου έπεται ότι $\mathrm{ord}(g^{|L|}) \in \{1,p\}$. Το ενδεχόμενο να ισχύει $\mathrm{ord}(g^{|L|}) = 1$ ($\Leftrightarrow g^{|L|} = e_G$) αποκλείεται, διότι εν τοιαύτη περιπτώσει θα καταλήγαμε στην ακόλουθη αντίφαση:

$$(gL)^{|L|} = g^{|L|}L = e_GL = L = e_{G/L} \underset{\text{4.1.27}}{\Longrightarrow} p \mid |L|.$$

Επομένως, $g^{|L|} \in G$ με $\mathrm{ord}(g^{|L|}) = p$. □

4.4.22 Θεώρημα. («Το αντίστροφο τού θεωρήματος 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 $|H| = k$.*

ΑΠΟΔΕΙΞΗ. 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 4.4.21 υπάρχει $g \in G \setminus \{e_G\} : \mathrm{ord}(g) = |\langle g\rangle| = p$. Επειδή η G είναι αβελιανή, $\langle g\rangle \trianglelefteq G$ (βλ. 4.2.6). Επομένως ορίζεται η πηλικοομάδα $G/\langle g\rangle$, η δε τάξη της ισούται με $|G/\langle g\rangle| = \frac{m}{p}$ (βλ. 4.4.2 (iii)). Σύμφωνα με το (ii) τής προτάσεως 4.4.2 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 2.4.6, $(\pi^G_{\langle g\rangle})^{-1}(K) \sqsubseteq G$, 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 4.1.13 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 $(\pi^G_{\langle g\rangle})^{-1}(K)$). □

► **Ένα χρήσιμο κριτήριο μη απλότητας**. Το θεώρημα 4.4.23 μπορεί να ιδωθεί ως μια γενίκευση τού θεωρήματος 3.5.1 τού Cayley (στην περίπτωση που περιοριζόμαστε σε *πεπερασμένες* ομάδες αναφοράς) και μας παρέχει μια εύχρηστη ικανή συνθήκη για *να μην είναι* μια εξεταζόμενη πεπερασμένη ομάδα $(G, \cdot)$ *απλή*.

4.4.23 Θεώρημα. («Τέχνασμα τού Poincaré».) *Έστω $(G, \cdot)$ μια ομάδα. Υποθέτουμε ότι υπάρχει μια γνήσια (όχι κατ' ανάγκην ορθόθετη) υποομάδα H τής G πεπερασμένου δείκτη, ας πούμε $|G : H| =: n$, όπου $n \geq 2$. Επιλέγοντας ένα σύστημα αριστερών εκπροσώπων* A *τής H εντός τής G ορίζουμε την απεικόνιση*

$$\boxed{\Theta_H : G \longrightarrow \mathfrak{S}_{\{gH \mid g \in \mathrm{A}\}},\ \ x \longmapsto \Theta_H(x) := \sigma_x,}$$

όπου $\sigma_x(gH) := xgH$, $\forall g \in$ A. Η Θ_H είναι ομομορφισμός ομάδων. Επιπροσθέτως, ισχύουν τα ακόλουθα[24]:

(i) $\mathrm{Ker}(\Theta_H) \sqsubseteq H$.

(ii) *Εάν $K \sqsubseteq H$ και $K \trianglelefteq G$, τότε $K \sqsubseteq \mathrm{Ker}(\Theta_H)$.*

(iii) $\exists K \trianglelefteq G : K \sqsubseteq H$ *με* $|G : K| = m < \infty$, $n \mid m$ *και* $m \mid n!$.

(iv) *Εάν η G είναι πεπερασμένη και $|G| \nmid n!$, τότε* $\mathrm{Ker}(\Theta_H) \neq \{e_G\}$, *οπότε η G δεν είναι απλή.*

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς θα αποδείξουμε ότι η Θ_H είναι ομομορφισμός. Εάν $x_1, x_2 \in G$, τότε $\Theta_H(x_1x_2) = \sigma_{x_1x_2} = \sigma_{x_1} \circ \sigma_{x_2} = \Theta_H(x_1) \circ \Theta_H(x_2)$, διότι για κάθε $g \in$ A,

$$\sigma_{x_1x_2}(gH) = (x_1x_2)\,gH = x_1(x_2g)\,H = \sigma_{x_1}(\sigma_{x_2}(gH)).$$

[24] Το θεώρημα 3.5.1 τού Cayley (για πεπερασμένες ομάδες) έπεται από το (i) τού παρόντος θεωρήματος όταν η H είναι η τετριμμένη υποομάδα τής G.

(i) Ο πυρήνας τού ομομορφισμού Θ_H είναι ο

$$\begin{aligned}\mathrm{Ker}(\Theta_H) &= \left\{x \in G \,\middle|\, \sigma_x = \mathrm{id}_{\{gH|g\in \mathrm{A}\}}\right\} = \{x \in G \,|\, \sigma_x(gH) = gH,\ \ \forall g \in \mathrm{A}\}\\ &= \{x \in G \,|\, xgH = gH,\ \ \forall g \in \mathrm{A}\} = \left\{x \in G \,\middle|\, g^{-1}xg \in H,\ \ \forall g \in \mathrm{A}\right\}\\ &= \left\{x \in G \,\middle|\, x \in gHg^{-1},\ \ \forall g \in \mathrm{A}\right\} = \bigcap_{g\in \mathrm{A}} gHg^{-1}.\end{aligned}$$

Επειδή $\mathrm{Ker}(\Theta_H) \subseteq gHg^{-1}, \forall g \in \mathrm{A}$ και (δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι) $e_G \in \mathrm{A}$ (βλ. 4.1.15), έχουμε

$$\mathrm{Ker}(\Theta_H) \subseteq e_G H e_G^{-1} = H \sqsubseteq G \underset{2.1.20}{\Longrightarrow} \mathrm{Ker}(\Theta_H) \sqsubseteq H.$$

(ii) Εάν $K \sqsubseteq H$ και $K \trianglelefteq G$,τότε για κάθε $g \in \mathrm{A}$ έχουμε

$$y \in gKg^{-1} \subseteq gHg^{-1}, \forall y \in K \Longrightarrow y \in \bigcap_{g\in \mathrm{A}} gHg^{-1}, \forall y \in K,$$

οπότε $K \subseteq \mathrm{Ker}(\Theta_H) \sqsubseteq G \underset{2.1.20}{\Longrightarrow} K \sqsubseteq \mathrm{Ker}(\Theta_H)$.

(iii) Αρκεί να θέσουμε $K := \mathrm{Ker}(\Theta_H)$. Τότε $K \trianglelefteq G$ (λόγω τού πορίσματος 4.2.31), $K \sqsubseteq H$ (λόγω τού (i)), $K \trianglelefteq H$ (λόγω τής προτάσεως 4.2.19), $H/K \sqsubseteq G/K$ (λόγω τού (i) τού πορίσματος 4.4.15) και

$$|G/K| = |G/K : H/K|\ |H/K| = |G : H|\ |H/K| = n\ |H/K|\,,$$

όπου η πρώτη ισότητα έπεται από το θεώρημα 4.1.20 και η δεύτερη από το (v) τού πορίσματος 4.4.15. Εν συνεχεία, λαμβάνοντας υπ' όψιν ότι η εικόνα $\mathrm{Im}(\Theta_{\mathrm{H}})$ τού ομομορφισμού Θ_{H} είναι μια υποομάδα τής $\mathfrak{S}_{\{gH|g\in \mathrm{A}\}}$ (βλ. 2.4.6 (i)), παρατηρούμε ότι η *επιρριπτική* απεικόνιση $G/K \ni xK \longmapsto \Theta_{_H}(x) = \sigma_x \in \mathrm{Im}(\Theta_H)$ είναι ισομορφισμός, διότι είναι ομομορφισμός (αφού $\sigma_{x_1x_2} = \sigma_{x_1} \circ \sigma_{x_2}$ για οιαδήποτε στοιχεία $x_1, x_2 \in G$) έχων ως πυρήνα του την ομάδα

$$\{xK \in G/K |\, \sigma_x = e_{\mathfrak{S}_{\{gH|g\in \mathrm{A}\}}}\} = \{xK \in G/K |\, x = e_{_G}\} = \{e_{_G}K\} = \{K\} = \{e_{G/K}\}.$$

(Βλ. πρόταση 2.4.15.) Αυτό σημαίνει ότι

$$|G/K| = |\mathrm{Im}(\Theta_H)| \leq \left|\mathfrak{S}_{\{gH|g\in \mathrm{A}\}}\right| = \left|\mathfrak{S}_{\mathrm{card(A)}}\right| = |\mathrm{card(A)}|! = n!.$$

Κατά συνέπειαν, $|G/K| = m < \infty$ και $n \mid m = |G : K|$. Από την άλλη μεριά,

$$\mathrm{Im}(\Theta_H) \sqsubseteq \mathfrak{S}_{\{gH|g\in \mathrm{A}\}} \underset{4.1.22}{\Longrightarrow} |G : K| = |\mathrm{Im}(\Theta_H)| = m \mid n!.$$

(iv) Εάν η G είναι πεπερασμένη και $|G| \nmid n!$, τότε, σύμφωνα με το (iii),

$$|G : \mathrm{Ker}(\Theta_H)| = \frac{|G|}{|\mathrm{Ker}(\Theta_H)|} \mid n! \Longrightarrow \mathrm{Ker}(\Theta_H) \neq \{e_G\}.$$

Επειδή $\mathrm{Ker}(\Theta_H) \trianglelefteq G$ και $\mathrm{Ker}(\Theta_H) \sqsubseteq H \sqsubset G$, έχουμε $\mathrm{Ker}(\Theta_H) \lhd G$, οπότε η G δεν είναι απλή. □

4.4.24 Πόρισμα. *Έστω $(G,\cdot)$ μια πεπερασμένη μη τετριμμένη ομάδα και έστω*

$$p := \min\{q \in \mathbb{N} \,|\, q \text{ πρώτος και } q \mid |G|\}.$$

Τότε κάθε υποομάδα H της G έχουσα δείκτη $|G:H| = p$ είναι ορθόθετη.

ΑΠΟΔΕΙΞΗ. Εάν $|G| \mid p!$, τότε από τον ορισμό τού p λαμβάνουμε $|G| = p$, οπότε $H = \{e_G\} \lhd G$. Εάν $|G| \nmid p!$, τότε, βάσει των (iii) και (iv) τού θεωρήματος 4.4.23, $\exists K \trianglelefteq G : K \sqsubseteq H$ με $1 < |G:K| = m < \infty$, $p \mid m$ και $m \mid p!$. Επειδή $p \mid m$, $p \mid |G|$ και

$$\left.\begin{matrix} m \mid p! \\ 4.1.22 \Rightarrow m \mid |G| \end{matrix}\right\} \underset{\text{B.2.6}}{\Longrightarrow} m \mid \text{μκδ}(p!, |G|) = p,$$

έχουμε $|G:K| = m = p = |G:H|$, $K \sqsubseteq H \Rightarrow H = K \lhd G$. □

4.4.25 Πόρισμα. *Έστω $(G,\cdot)$ μια πεπερασμένη ομάδα τάξεως $|G| = p^\nu$, όπου p πρώτος αριθμός και $\nu \in \mathbb{N}$. Τότε κάθε υποομάδα H της G τάξεως $|H| = p^{\nu-1}$ είναι ορθόθετη.*

ΑΠΟΔΕΙΞΗ. Επειδή $\text{Ker}(\Theta_H) \sqsubseteq H \underset{4.1.22}{\Longrightarrow} |\text{Ker}(\Theta_H)| \mid p^{\nu-1}$, έχουμε $|\text{Ker}(\Theta_H)| = p^j$, για κάποιον $j \in \{0,1,...,\nu-1\}$ (βλ. λήμμα Β.3.14) και

$$|\text{Im}(\Theta_H)| = \frac{|G|}{|\text{Ker}(\Theta_H)|} = p^{\nu-j}.$$

Επειδή $\text{Im}(\Theta_H) \sqsubseteq \mathfrak{S}_p \underset{4.1.22}{\Longrightarrow} |\text{Im}(\Theta_H)| \mid p!$ και $p^{\nu-j} \nmid p!$ για κάθε $j \in \{0,1,...,\nu-2\}$, έχουμε κατ' ανάγκην $|\text{Im}(\Theta_H)| = p$ (για $j = \nu-1$). Άρα

$$|\text{Ker}(\Theta_H)| = p^{\nu-1} = |H|,$$

απ' όπου έπεται ότι $H = \text{Ker}(\Theta_H) \lhd G$. □

4.4.26 Πόρισμα. *Εάν μια απλή ομάδα $(G,\cdot)$ διαθέτει κάποια γνήσια υποομάδα H πεπερασμένου δείκτη, ας πούμε $|G:H| =: n$, όπου $n \geq 2$, τότε αυτή είναι ισόμορφη με μια υποομάδα τής συμμετρικής ομάδας $\mathfrak{S}_n$.*

ΑΠΟΔΕΙΞΗ. Επειδή $\text{Ker}(\Theta_H) \trianglelefteq G$ και η G είναι εξ υποθέσεως απλή, έχουμε κατ' ανάγκην είτε $\text{Ker}(\Theta_H) = \{e_G\}$ είτε $\text{Ker}(\Theta_H) = G$. Η δεύτερη περίπτωση αποκλείεται, καθότι $H \sqsubset G$. Επομένως, $\text{Ker}(\Theta_H) = \{e_G\}$, οπότε ο ομομορφισμός Θ_H είναι μονομορφισμός και η ομάδα G εμφυτεύεται στην $\mathfrak{S}_n$ και είναι, ως εκ τούτου, ισόμορφη με μια υποομάδα τής $\mathfrak{S}_n$ (βλ. προτάσεις 2.4.15 και 2.4.17). □

4.4.27 Εφαρμογή. *Έστω $n \in \mathbb{N}$, $n \geq 5$. Εάν ο k είναι ένας φυσικός αριθμός που ικανοποιεί (ταυτοχρόνως) τις συνθήκες*

$$1 < k < \frac{n!}{2}, \quad k \mid \frac{n!}{2}, \quad \left(\frac{n!/2}{k}\right)! < \frac{n!}{2},$$

τότε η εναλλάσσουσα ομάδα $\mathfrak{A}_n$ δεν διαθέτει καμία υποομάδα τάξεως k.

ΑΠΟΔΕΙΞΗ. Εάν $n \in \mathbb{N}$, $n \geq 5$, τότε, σύμφωνα με το θεώρημα 4.3.6, η $\mathfrak{A}_n$ είναι απλή. Εάν αυτή διέθετε μια υποομάδα H τάξεως k, όπου ο k ικανοποιεί τις ανωτέρω συνθήκες, τότε θα έπρεπε να ισχύει $|\mathfrak{A}_n : H| = \frac{n!/2}{k}$ και (λόγω τού πορίσματος 4.4.26)

$$|\mathfrak{A}_n| = \frac{n!}{2} \leq \left|\mathfrak{S}_{\frac{n!/2}{k}}\right| = \left(\frac{n!/2}{k}\right)!,$$

ήτοι κάτι εξ υποθέσεως αποκλεισθέν. □

4.4.28 Παράδειγμα. Η εναλλάσσουσα ομάδα $\mathfrak{A}_5$ δεν διαθέτει υποομάδες τάξεως $15, 20$ ή 30. Ως εκ τούτου, η[25] $\mathfrak{A}_5$ αποτελεί ένα επιπλέον παράδειγμα μη αβελιανής ομάδας, για την οποία το «αντίστροφο» τού θεωρήματος τού Lagrange δεν είναι αληθές (πρβλ. 4.1.47).

4.4.29 Πόρισμα. *Δεν υφίστανται άπειρες απλές ομάδες έχουσες κάποια γνήσια υποομάδα πεπερασμένου δείκτη.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το πόρισμα 4.4.26. □

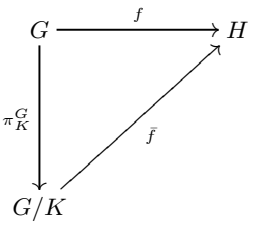
4.5 ΘΕΩΡΗΜΑΤΑ ΙΣΟΜΟΡΦΙΣΜΩΝ ΟΜΑΔΩΝ

Αυτά είναι ορισμένα χαρακτηριστικά θεωρήματα που περιγράφουν τον τρόπο διασυνδέσεως των ομομορφισμών ομάδων, των ορθόθετων υποομάδων και των πηλικοομάδων.

4.5.1 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



(4.32)

[25] *Σημείωση.* Η εναλλάσσουσα ομάδα $\mathfrak{A}_5$ διαθέτει ακριβώς 59 (διαφορετικές) υποομάδες: Την τετριμμένη και την ίδια την $\mathfrak{A}_5$ (που είναι οι μόνες ορθόθετες υποομάδες της), 15 υποομάδες ισόμορφες με την $(\mathbb{Z}_2, +)$, 10 υποομάδες ισόμορφες με την $(\mathbb{Z}_3, +)$, 5 υποομάδες ισόμορφες με την $(\mathbf{V}, \circ)$, 6 υποομάδες ισόμορφες με την $(\mathbb{Z}_5, +)$, 10 υποομάδες ισόμορφες με την $(\mathfrak{S}_3, \circ)$, 6 υποομάδες ισόμορφες με την $(\mathbf{D}_5, \circ)$ και 5 υποομάδες ισόμορφες με την $(\mathfrak{A}_4, \circ)$.

να καθίσταται μεταθετικό, εάν και μόνον εάν $K \subseteq \mathrm{Ker}(f)$. *Ο εν λόγω ομομορφισμός ορίζεται μέσω τού τύπου*

$$\boxed{\bar{f}(gK) := f(g),\ \ \forall g \in G.} \tag{4.33}$$

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 (4.33). 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 $\bar{f}(g_1K) = \bar{f}(g_2K)$. Η $\bar{f}$ 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 (4.32) μεταθετικό. Και αντιστρόφως· εάν ο $\bar{f} : G/K \longrightarrow H$ είναι ο μόνος ομομορφισμός που καθιστά το διάγραμμα (4.32) 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

$$\left.\begin{array}{l}\mathrm{Ker}(f) \sqsubseteq G\\ K \subseteq \mathrm{Ker}(f)\end{array}\right\} \underset{2.1.20}{\Longrightarrow} K \sqsubseteq \mathrm{Ker}(f).$$

Επειδή εξ υποθέσεως $K \trianglelefteq G$ και $K \sqsubseteq \mathrm{Ker}(f)$, η πρόταση 4.2.19 μας πληροφορεί ότι $K \trianglelefteq \mathrm{Ker}(f)$. Κατά συνέπειαν, ορίζεται η πηλικομάδα $\mathrm{Ker}(f)/K$. Προφανώς,

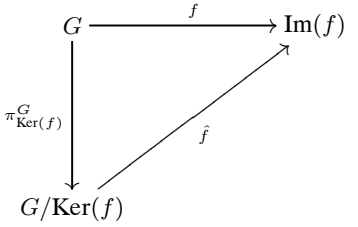
$$\begin{aligned}\mathrm{Ker}(f)/K &= \{gK \,|g \in \mathrm{Ker}(f)\} = \{gK \,|f(g) = e_H\} \\ &= \left\{gK \,\middle|\, \bar{f}(\pi_K^G(g)) = e_H\right\} = \left\{gK \,\middle|\, \bar{f}(gK) = e_H\right\} = \mathrm{Ker}(\bar{f}).\end{aligned}$$

(iii) Το ότι ο $\bar{f}$ είναι μονομορφισμός $\Leftrightarrow K = \mathrm{Ker}(f)$ είναι άμεση συνέπεια τού (ii) και τής προτάσεως 2.4.15. □

4.5.2 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,

$$\boxed{G/\mathrm{Ker}(f) \cong \mathrm{Im}\,(f)\,.}$$

ΑΠΟΔΕΙΞΗ. Εφαρμόζοντας το θεώρημα 4.5.1 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* $\mathrm{Im}(f) \subseteq H$. □

4.5.3 Παραδείγματα. (i) Εάν $n \in \mathbb{N}$, τότε η απεικόνιση

$$(\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_n, +), \;\; k \longmapsto [k]_n$$

είναι ένας επιμορφισμός ομάδων με πυρήνα του την υποομάδα $n\mathbb{Z}$ τής ομάδας $\mathbb{Z}$ (βλ. 2.1.21 (iii)). Συνεπώς,

$$\boxed{\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.}$$

Και, γενικότερα, εάν $m, n \in \mathbb{N}$ και $m \mid n$, τότε $n\mathbb{Z} \trianglelefteq m\mathbb{Z}$ (βλ. 2.2.20 (i) και 4.2.6) και ορίζεται η πηλικοομάδα $m\mathbb{Z}/n\mathbb{Z}$. Η απεικόνιση

$$(m\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_{\frac{n}{m}}, +), \;\; mk \longmapsto [k]_{\frac{n}{m}},$$

είναι ένας επιμορφισμός ομάδων με πυρήνα του την υποομάδα

$$\{\, mk |\, k \in \mathbb{Z} : [k]_{\frac{n}{m}} = [0]_{\frac{n}{m}}\} = \{\, mk |\, k \in \mathbb{Z} :\; k \mid \tfrac{n}{m}\} = \{\, mk |\, k \in \tfrac{n}{m}\mathbb{Z}\} = n\mathbb{Z}$$

τής ομάδας $m\mathbb{Z}$. Συνεπώς,

$$\boxed{m\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_{\frac{n}{m}}.} \tag{4.34}$$

(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

$$(\mathbb{C}\smallsetminus\{0\}, \cdot) \longrightarrow (\mathbb{S}^1, \cdot), \;\; z \longmapsto \frac{z}{|z|},$$

έχει ως πυρήνα του την $(\mathbb{R}_{>0}, \cdot)$. Άρα

$$\boxed{(\mathbb{C}\smallsetminus\{0\})/\mathbb{R}_{>0} \cong \mathbb{S}^1.}$$

(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 4.2.32 (i) κατασκευάζεται ισομορφισμός

$$\boxed{\mathfrak{S}_n/\mathfrak{A}_n \xrightarrow{\cong} \{\pm 1\}.}$$

(vi) Μέσω τού επιμορφισμού 4.2.32 (ii) κατασκευάζεται ισομορφισμός

$$\boxed{\mathbf{GL}_n(R)/\mathbf{SL}_n(R) \xrightarrow{\cong} R^\times.}$$

(vii) Μέσω τού επιμορφισμού 4.2.32 (iii) κατασκευάζεται ισομορφισμός

$$\boxed{\mathbf{O}_n(\mathbb{R})/\mathbf{SO}_n(\mathbb{R}) \xrightarrow{\cong} \{\pm 1\}.}$$

(viii) Μέσω τού επιμορφισμού 4.2.32 (iv) κατασκευάζεται ισομορφισμός

$$\boxed{\mathbf{U}_n(\mathbb{C})/\mathbf{SU}_n(\mathbb{C}) \xrightarrow{\cong} \mathbb{S}^1.}$$

4.5.4 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) $|G : K| = |\mathrm{Im}(f) : f(K)|\ |\mathrm{Ker}(f) : \mathrm{Ker}(f|_K)|$.

ΑΠΟΔΕΙΞΗ. (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 4.5.2,

$$K/\mathrm{Ker}(f|_K) = K/\mathrm{Ker}\,(f|_K)^\wedge \cong \mathrm{Im}\,(f|_K)^\wedge = f(K),$$

όπου $\mathrm{Ker}(f|_K) = \mathrm{Ker}(f) \cap K$, οπότε ο ισχυρισμός είναι αληθής επί τη βάσει τού θεωρήματος 4.1.22 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

$$\left.\begin{array}{r} |G| = |f(G)|\ |\mathrm{Ker}(f)| \\ |K| = |f(K)|\ |\mathrm{Ker}(f|_K)| \end{array}\right\} \Rightarrow |G : K| = |f(G) : f(K)|\ \left|\mathrm{Ker}(f) : \mathrm{Ker}(f|_K)\right|,$$

κατόπιν εφαρμογής τού θεωρήματος 4.1.22 τού Lagrange. □

4.5.5 Θεώρημα. (Μεταφορά ομομορφισμού σε «επίπεδο πηλικοομάδων») *Έστω $f : (G_1, \cdot) \longrightarrow (G_2, *)$ ένας ομομορφισμός ομάδων. Εάν $K_1 \trianglelefteq G_1$ και $K_2 \trianglelefteq G_2$, 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*

$$\begin{array}{ccc} G_1 & \xrightarrow{\ f\ } & G_2 \\ {\scriptstyle \pi_{K_1}^{G_1}}\downarrow & \circlearrowleft & \downarrow{\scriptstyle \pi_{K_2}^{G_2}} \\ G_1/K_1 & \xrightarrow[f^{\pi\eta\lambda.}]{} & G_2/K_2 \end{array}$$

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* $\Longleftrightarrow \mathrm{Im}(f) * K_2 = G_2$.

ΑΠΟΔΕΙΞΗ. Εφαρμόζουμε το θεώρημα 4.5.1 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 4.5.1. 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

$$\mathrm{Ker}(f^{\pi\eta\lambda.}) = \{gK_1 \in G_1/K_1 \,|f(g) * K_2 = K_2\} = \{gK_1 \in G_1/K_1 \,|f(g) \in K_2\}$$
$$= \left\{gK_1 \in G_1/K_1 \,\middle|g \in f^{-1}(K_2)\right\} = f^{-1}(K_2)/K_1$$

ο $f^{\pi\eta\lambda.}$ (λόγω τής προτάσεως 2.4.15) 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 $\mathrm{Im}(f) * K_2 = G_2$. □

4.5.6 Παρατήρηση. Ακόμη και εάν, υποτιθεμένου ότι ικανοποιούνται οι συνθήκες (i), (ii) τού θεωρήματος 4.5.5, 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[26]. Αλλά *ούτε* ο επιμορφισμός[27]

$$(f|_{K_1})^{\wedge} : K_1 \longrightarrow f(K_1) = f(f^{-1}(K_2)),\ x \longmapsto (f|_{K_1})^{\wedge}(x) := f|_{K_1}(x) = f(x),$$

ο δημιουργούμενος ύστερα από περιορισμό τού πεδίου τιμών τής απεικονίσεως $f|_{K_1}$ στο $f(K_1)$ είναι κατ' ανάγκην ισομορφισμός[28].

4.5.7 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* $G_1 \cong G_2$.

[26] Ο f είναι επιμορφισμός $\Leftrightarrow K_2 \sqsubseteq \mathrm{Im}(f) \Leftrightarrow \mathrm{Im}(f) = G_2$ και μονομορφισμός $\Leftrightarrow \mathrm{Ker}(f) = \{e_{G_1}\}$.

[27] Σημειωτέον ότι $f(f^{-1}(K_2)) \subseteq K_2$.

[28] Ο $(f|_{K_1})^{\wedge}$ είναι μονομορφισμός $\Leftrightarrow \{e_{G_1}\} = \mathrm{Ker}(f) \cap K_1 (= \mathrm{Ker}(f|_{K_1}) = \mathrm{Ker}((f|_{K_1})^{\wedge}))$.

Επί παραδείγματι, $\langle [2]_4 \rangle \lhd \mathbb{Z}_4$ και $\langle [1\,2] \circ [3\,4] \rangle \lhd \mathbf{V}$ (βλ. 4.2.6) με

$$|\langle [2]_4 \rangle| = |\langle [1\,2] \circ [3\,4] \rangle| = 2,$$

και (λόγω τής προτάσεως 2.3.19, τού (ii) τού θεωρήματος 2.4.23 και των όσων προαναφέρθησαν στο (ii) τού εδαφίου 3.4.2)

$$\left\{ \begin{array}{c} \mathbb{Z}_4 / \langle [2]_4 \rangle \cong \mathbb{Z}_2 \cong \mathbf{V} / \langle [1\,2] \circ [3\,4] \rangle\,, \\ \langle [2]_4 \rangle \cong \mathbb{Z}_2 \cong \langle [1\,2] \circ [3\,4] \rangle \end{array} \right\} \text{ αλλά } \mathbb{Z}_4 \ncong \mathbf{V}.$$

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 4.5.5) 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 4.1.22 τού Lagrange και των προαναφερθέντων στο εδάφιο 4.1.44 (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 $\langle \beta \rangle \lhd \mathbf{D}_4$ και $\left\langle \alpha, \beta^2 \right\rangle \lhd \mathbf{D}_4$ (βλ. 4.2.13), και ότι -ως εκ τούτου- ορίζονται οι πηλικοομάδες $\mathbf{D}_4 / \langle \beta \rangle$ και $\mathbf{D}_4 / \left\langle \alpha, \beta^2 \right\rangle$. Παρατηρούμε ότι

$$\mathbf{D}_4 / \langle \beta \rangle \cong \mathbb{Z}_2 \cong \mathbf{D}_4 / \left\langle \alpha, \beta^2 \right\rangle \text{ αλλά } \langle \beta \rangle \cong \mathbb{Z}_4 \ncong \mathbf{V} \cong \left\langle \alpha, \beta^2 \right\rangle.$$

(Βλ. πρόταση 2.3.19 και το (ii) τού θεωρήματος 2.4.23.) Μάλιστα, ο υποδηλούμενος ισομορφισμός $\mathbf{D}_4 / \langle \beta \rangle \xrightarrow{\cong} \mathbf{D}_4 / \left\langle \alpha, \beta^2 \right\rangle$ *δεν μπορεί να είναι* «κανονιστικός» (υπό την έννοια τού θεωρήματος 4.5.5) εάν αξιώσουμε από αυτόν να επάγεται από κάποιον *αυτομορφισμό* τής $\mathbf{D}_4$. (Όπως θα δούμε αργότερα στο εδ. 6.1.4, $\vartheta(\langle \beta \rangle) = \langle \beta \rangle \not\subseteq \left\langle \alpha, \beta^2 \right\rangle$ για κάθε $\vartheta \in \mathrm{Aut}(\mathbf{D}_4)$.) Μολαταύτα, υπάρχει ισομορφισμός $\mathbf{D}_4 / \langle \beta \rangle \xrightarrow{\cong} \mathbf{D}_4 / \left\langle \alpha, \beta^2 \right\rangle$ ο οποίος *είναι* «κανονιστικός» αλλά επαγόμενος από τον (μη ενριπτικό, μη επιρριπτικό) *ενδομορφισμό* [29] 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* $G_1/K_1 \cong G_2/K_2$. (Βλ. εδάφιο 7.1.7.)

[29] 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.

4.5.8 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*

$$\boxed{G_1/K_1 \cong G_2/f(K_1).}$$

ΑΠΟΔΕΙΞΗ. (i) Αρκεί να εφαρμοσθεί το θεώρημα 4.5.5. (Εν προκειμένω, ο κατασκευαζόμενος «κανονιστικός» ομομορφισμός $f^{\pi\eta\lambda.}$ είναι ισομορφισμός.)

(ii) Αρκεί να εφαρμοσθεί εκ νέου το θεώρημα 4.5.5. Προφανώς, ο κατασκευαζόμενος «κανονιστικός» ομομορφισμός $f^{\pi\eta\lambda.}$ είναι επιμορφισμός. Από την άλλη μεριά, επειδή

$$\left.\begin{array}{r} f^{-1}\left(f(K_1)\right) = \mathrm{Ker}(f)K_1 \ \text{(βλ. 4.1.6 (iii))} \\ \mathrm{Ker}(f) \subseteq K_1 \ \text{(εξ υποθέσεως)} \end{array}\right\} \Rightarrow K_1 = f^{-1}\left(f(K_1)\right),$$

ο $f^{\pi\eta\lambda.}$ είναι *και* μονομορφισμός. □

4.5.9 Θεώρημα. (Τύπος γινομένου) *Εάν οι* H, K *είναι πεπερασμένες υποομάδες μιας ομάδας* $(G, \cdot)$, *τότε*

$$\boxed{\mathrm{card}(HK) = \frac{|H|\ |K|}{|H \cap K|} = \mathrm{card}(KH).} \tag{4.35}$$

ΑΠΟΔΕΙΞΗ. Ορίζουμε την επιρριπτική απεικόνιση

$$f : H \times K \longrightarrow HK, \ \ (x, y) \longmapsto f(x, y) := xy.$$

Αρκεί να αποδείξουμε ότι

$$\mathrm{card}(f^{-1}(\{z\})) = |H \cap K|, \ \ \forall z \in HK,$$

διότι[30] $H \times K = \coprod_{z \in HK} f^{-1}(\{z\})$ και $\mathrm{card}(H \times K) = |H|\ |K|$. Έστω τυχόν $z \in HK$. Τότε $\exists x \in H, y \in K$: $z = xy$ και

$$f^{-1}(\{z\}) = \{(xr, r^{-1}y) \,|r \in H \cap K\}. \tag{4.36}$$

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

$$f(xr, r^{-1}y) = (xr)(r^{-1}y) = x(rr^{-1})y = xe_G y = xy = z.$$

[30] 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 $z = f(w) = z'$.

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 (4.36) είναι αληθής. Επομένως,

$$\text{card}(f^{-1}(\{z\})) = \text{card}(\{(xr, r^{-1}y)\,|r \in H \cap K\}) = |H \cap K|\,,$$

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 (4.35) αποδεικνύεται παρομοίως.) □

4.5.10 Σημείωση. Στο θεώρημα 4.5.9 *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 (4.35) δίδει $\text{card}(H \circ K) = 4$. Προφανώς,

$$4 \nmid 6 \underset{4.1.22}{\Longrightarrow} H \circ K \not\sqsubseteq \mathfrak{S}_3.$$

(Πρβλ. 4.1.5.) Επιπροσθέτως, $[1\,2\,3] = [1\,2\,] \circ [2\,3]$ και

$$\left.\begin{array}{r} H \circ K = \{\text{id},\ [1\,2]\,,\ [2\,3]\,,\ [1\,2\,3]\} \subseteq \langle H, K\rangle \sqsubseteq \mathfrak{S}_3 \\ |\langle H, K\rangle| \geq 4 > 3 \end{array}\right\} \underset{4.1.24}{\Longrightarrow} \langle H, K\rangle = \mathfrak{S}_3,$$

οπότε $\mathfrak{S}_3 = \langle[1\,2]\,, [2\,3]\rangle$. (Πρβλ. 3.2.13 (ii).)

4.5.11 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 (4.35) έπεται άμεσα ότι

$$|G| \geq \text{card}(HK) = \frac{|H|\ |K|}{|H \cap K|} > \frac{\sqrt{|G|}\,\sqrt{|G|}}{|H \cap K|} = \frac{|G|}{|H \cap K|},$$

ήτοι ότι $|H \cap K| > 1$. □

4.5.12 Λήμμα. *Εάν 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. 2.2.2)*, τότε ισχύουν τα εξής*:

(i) $HK = \langle H, K\rangle = KH$.

(ii) $H \cap K \trianglelefteq K$.

ΑΠΟΔΕΙΞΗ. (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 4.1.4) 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 $\langle H, K\rangle \subseteq HK$, οπότε $HK = \langle H, K\rangle$.

(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

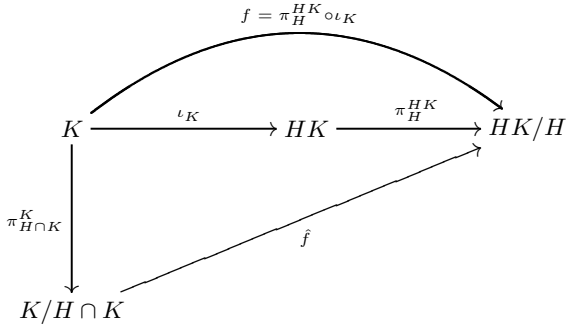
$$f(y) := \pi_H^{HK}(\iota_K(y)) = \pi_H^{HK}(y) = yH, \;\; \forall y \in K,$$

και (ούσα σύνθεση δύο ομομορφισμών ομάδων) είναι ομομορφισμός ομάδων 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 4.2.31). □

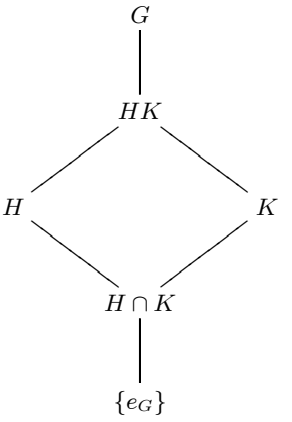
4.5.13 Δεύτερο Θεώρημα Ισομορφισμών. *Έστω ότι οι H, K είναι δυο υποομάδες μιας ομάδας $(G, \cdot)$ ικανοποιούσες τη συνθήκη $H \trianglelefteq \langle H, K\rangle$. Εάν $f := \pi_H^{HK} \circ \iota_K$ είναι η σύνθεση τής ενθέσεως $\iota_K : K \to HK$, $y \mapsto \iota_K(y) := y$ και τού φυσικού επιμορφισμού $\pi_H^{HK} : HK \to HK/H$, 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,

$$\boxed{K/\,H\cap K\cong HK/\,H\,(=\langle H,K\rangle\,/\,H),} \tag{4.37}$$

το δε διάγραμμα τού Hasse για το σύνολο των υποομάδων τής G που υπεισέρχονται στον ισομορφισμό (4.37) *(συμπεριλαμβανομένης τής τετριμμένης και τής ιδίας τής G) είναι το εξής*:



ΠΡΩΤΗ ΑΠΟΔΕΙΞΗ. Σύμφωνα με το λήμμα 4.5.12, $HK=\langle H,K\rangle=KH$ 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

$$(xy)H=(xH)(yH)=H(yH)=(e_GH)(yH)=(e_Gy)H=yH=f(y),$$

οπότε ο f είναι *επιμορφισμός* ομάδων. Εφαρμόζοντας γι' αυτόν το 1ο θεώρημα ισομορφισμών 4.5.2 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 ΑΠΟΔΕΙΞΗ. Επειδή

$$\begin{aligned}&\iota_K(H\cap K)=H\cap K\subseteq H,\\ &{\iota_K}^{-1}(K)=\{y\in K\,|\iota_K(y)=y\in H\}=H\cap K,\\ &\mathrm{Im}(\iota_K)H=KH=\langle H,K\rangle=HK.\end{aligned}$$

ο ισχυρισμός είναι αληθής, προκύπτων άμεσα ύστερα από εφαρμογή τού θεωρήματος 4.5.5 για τις ορθόθετες υποομάδες $H\cap K$ και H των K και HK, αντιστοίχως, και τον ομομορφισμό ι_K. □

4.5.14 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 4.2.19 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 (4.35) έπεται άμεσα από τον ισομορφισμό (4.37), τη σημείωση 4.1.21 και το θεώρημα 4.1.22 τού Lagrange. Ωστόσο, το θεώρημα 4.5.9 μας πληροφορεί ότι ο εν λόγω τύπος εξακολουθεί να ισχύει *ακόμη και όταν το σύνολο HK δεν είναι υποομάδα τής G.* (Βλ. εδ. 4.5.10.)

4.5.15 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 2.2.20, έχουμε

$$H \cap K = \text{εκπ}(m, n)\mathbb{Z} \text{ και } H + K = \langle H, K\rangle = \text{μκδ}(m, n)\mathbb{Z}.$$

Επειδή $H := m\mathbb{Z} \trianglelefteq \langle H, K\rangle = \text{μκδ}(m, n)\mathbb{Z}$ (βλ. 2.2.20 (i) και 4.2.6), από το 2ο θεώρημα ισομορφισμών 4.5.13 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 (4.34) 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

$$\tfrac{\text{εκπ}(m,n)}{n} = \left|\mathbb{Z}_{\frac{\text{εκπ}(m,n)}{n}}\right| = \left|\mathbb{Z}_{\frac{m}{\text{μκδ}(m,n)}}\right| = \tfrac{m}{\text{μκδ}(m,n)}$$

ή, ισοδυνάμως, ότι $\text{μκδ}(m, n)\text{εκπ}(m, n) = mn$. (Πρβλ. πρόταση[31] Β.2.29.)

4.5.16 Παράδειγμα. Έστω $\mathbf{V}$ η ομάδα των τεσσάρων στοιχείων τού Klein (βλ. εδάφιο 3.4.2 (ii)). Ως γνωστόν, $\mathbf{V} \lhd \mathfrak{S}_4$ (βλ. 4.2.21). 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 μετάταξη $\sigma \in \mathfrak{S}_4$. 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 $\{l, m\} = \{1, 2, 3\} \setminus \{j\}$, $l \neq m$, συμπεραίνουμε (μέσω των (i), (v) και (vi) τής προτάσεως 3.2.3) ότι

$$\sigma = [j\ 4]^{-1} \circ \tau = [j\ 4] \circ \tau = (\underbrace{[j\ 4] \circ [l\ m]}_{\in \mathbf{V}}) \circ (\underbrace{[l\ m] \circ \tau}_{\in K}) \in \mathbf{V} \circ K.$$

[31] Η ισότητα $\text{μκδ}(m, n)\text{εκπ}(m, n) = |mn|$ ισχύει για *οιουσδήποτε* $m, n \in \mathbb{Z} \setminus \{0\}$. Επειδή όμως $m\mathbb{Z} = |m|\,\mathbb{Z}$ και $n\mathbb{Z} = |n|\,\mathbb{Z}$ για *οιουσδήποτε* $m, n \in \mathbb{Z} \setminus \{0\}$, *και αυτή* έπεται από τα προαναφερθέντα, αρκεί κανείς, όταν $m, n \in \mathbb{Z} \setminus \{0\}$,να εργασθεί με τους $|m|$ και $|n|$ στη θέση των m και n.

Άρα όντως $\mathbf{V} \circ K = \mathfrak{S}_4$. Σημειωτέον ότι $\mathbf{V} \cap K = \{\mathrm{id}\}$, διότι κανένα από τα στοιχεία τού $\mathbf{V} \smallsetminus \{\mathrm{id}\}$ δεν αφήνει το 4 αμετάβλητο. Ως εκ τούτου, μέσω τού 2ου θεωρήματος ισομορφισμών 4.5.13 καταλήγουμε στο ότι

$$\boxed{\mathfrak{S}_3 \cong K \cong K/\{\mathrm{id}\} \cong \mathfrak{S}_4/\,\mathbf{V}.}$$

4.5.17 Πόρισμα. *Έστω $(G, \cdot)$ μια πεπερασμένη ομάδα και έστω $H \trianglelefteq G$ τάξεως $|H| = m$. Εάν* μκδ$(m, |G/H|) = 1$, *τότε η H είναι η μοναδική υποομάδα τής G που έχει τάξη m.*

ΑΠΟΔΕΙΞΗ. Έστω K τυχούσα υποομάδα τής G τάξεως $|K| = m$. Κατά το 2ο θεώρημα ισομορφισμών 4.5.13,

$$K/\,H \cap K \cong HK/\,H \Longrightarrow |HK/\,H| = |K/\,H \cap K| = \frac{m}{|H \cap K|}. \tag{4.38}$$

Επειδή

$$\left.\begin{array}{c} |HK/\,H| \mid |G/H| \\ \text{μκδ}(m, |G/H|) = 1 \end{array}\right\} \Longrightarrow \text{μκδ}(m, |HK/\,H|) = 1 \underset{(4.38)}{\Longrightarrow} \text{μκδ}(m, \tfrac{m}{|H\cap K|}) = 1,$$

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 $K = H$. □

4.5.18 Θεώρημα. («Θεώρημα αντιστοιχίσεως ορθόθετων υποομάδων») *Εάν*

$$f : (G, \cdot) \longrightarrow (H, *)$$

είναι ένας ομομορφισμός ομάδων και

$$\mathbf{Subg}(G; \mathrm{Ker}(f)) \ni K \overset{\Psi_f}{\longmapsto} f(K) \in \mathbf{Subg}(\mathrm{Im}(f)) \tag{4.39}$$

η αμφίρριψη η ορισθείσα στο πόρισμα 2.4.7, *τότε ισχύουν τα ακόλουθα*:
(i) *Για $K_1, K_2 \in \mathbf{Subg}(G; \mathrm{Ker}(f))$ αληθεύει η κάτωθι αμφίπλευρη συνεπαγωγή*

$$\boxed{K_1 \trianglelefteq K_2 \Longleftrightarrow \Psi_f(K_1) \trianglelefteq \Psi_f(K_2).}$$

(ii) *Για $K_1, K_2 \in \mathbf{Subg}(G; \mathrm{Ker}(f))$ με $K_1 \trianglelefteq K_2$ υφίσταται ισομορφισμός*

$$\boxed{K_2/K_1 \overset{\cong}{\longrightarrow} \Psi_f(K_2)/\Psi_f(K_1).}$$

(iii) *Περιορίζοντας την αμφίρριψη* (4.39) *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. 4.2.29), *λαμβάνουμε μια αμφίριψη*

$$\boxed{\mathbf{NSubg}(G;\mathrm{Ker}(f)) \ni K \longmapsto f(K) \in \mathbf{NSubg}(\mathrm{Im}(f))}$$

η οποία καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων[32]

$$(\mathbf{NSubg}(G;\mathrm{Ker}(f)), \trianglelefteq) \quad \textit{και} \quad (\mathbf{NSubg}(\mathrm{Im}(f)), \trianglelefteq)\,.$$

(iv) $\Psi_f(\mathrm{NCL}_G(K_1,K_2)) = \mathrm{NCL}_G(\Psi_f(K_1), \Psi_f(K_2)), \forall\,(K_1,K_2) \in \mathbf{NSubg}(G;\mathrm{Ker}(f))^2$.

ΑΠΟΔΕΙΞΗ. (i) Αυτό προκύπτει από την αμφιρριπτικότητα τής Ψ_f (βλ. 2.4.7) και την εφαρμογή τής προτάσεως 4.2.30 για τον επιμορφισμό

$$f|_{K_2} : K_2 \longrightarrow f(K_2)\ (= \Psi_f(K_2)).$$

(ii) Επειδή (κατά το (i)) $K_1 \trianglelefteq K_2 \Rightarrow \Psi_f(K_1) \trianglelefteq \Psi_f(K_2)$, ορίζεται η πηλικοομάδα $\Psi_f(K_2)/\Psi_f(K_1)$ και η απεικόνιση

$$\rho := \pi^{f(K_2)}_{f(K_1)} \circ f|_{K_2} : K_2 \longrightarrow f(K_2)/f(K_1)\ (= \Psi_f(K_2)/\Psi_f(K_1))$$

αποτελεί επιμορφισμό ομάδων (ως σύνθεση δύο επιμορφισμών) με πυρήνα του την ομάδα

$$\begin{aligned}\mathrm{Ker}(\rho) &= \{x \in K_2 \,|\rho(x) = f(K_1)\} = \{x \in K_2 \,|f(x) * f(K_1) = f(K_1)\}\\ &= \{x \in K_2 \,|f(x) \in f(K_1)\} = \left\{x \in K_2 \,\middle|x \in f^{-1}(f(K_1))\right\}\\ &= \{x \in K_2 \,|x \in K_1\} = K_1 \ \ (\text{διότι } f^{-1}(f(K_1)) = K_1).\end{aligned}$$

Επομένως, είναι δυνατόν να εφαρμόσουμε το 1ο θεώρημα ισομορφισμών 4.5.2 (για τον επιμορφισμό ρ) και να κατασκευάσουμε τον ισομορφισμό

$$\hat{\rho} : K_2/K_1 \longrightarrow \Psi_f(K_2)/\Psi_f(K_1)\,,\ \ xK_1 \longmapsto \hat{\rho}(xK_1) = \rho(x) = f(x) * \Psi_f(K_1)\,.$$

(iii) Τούτο είναι άμεσο επακόλουθο τού (i).

(iv) Επειδή η αμφίριψη $\Psi_f|_{\mathbf{NSubg}(G;\mathrm{Ker}(f))}$ καθορίζει έναν ισομορφισμό μεταξύ των συνδέσμων

$$(\mathbf{NSubg}(G;\mathrm{Ker}(f)), \trianglelefteq) \ \ \text{και} \ \ (\mathbf{NSubg}(\mathrm{Im}(f)), \trianglelefteq)\,,$$

αρκεί να χρησιμοποιηθεί η ισοδυναμία των συνθηκών (i) και (iii) τής προτάσεως[33] Α.2.27, σε συνδυασμό με την πρόταση 4.2.28 και το πόρισμα 4.2.29. □

[32] Βλ. πρόταση 4.2.28 και πόρισμα 4.2.29.

[33] Στη διατύπωση τού θεωρήματος δεν θεωρήθηκε σκόπιμο να συμπεριληφθεί και η ιδιότητα

$$\Psi_f(K_1 \cap K_2) = \Psi_f(K_1) \cap \Psi_f(K_2)\,,\ \forall\,(K_1,K_2) \in \mathbf{NSubg}(G;\mathrm{Ker}(f))^2$$

(η οποία απορρέει από την ισοδυναμία των συνθηκών (i) και (ii) τής προτάσεως Α.2.27), καθότι αυτή (όπως είδαμε στο (iii) τού πορίσματος 2.4.7) 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 $(\mathbf{Subg}(G;\mathrm{Ker}(f)), \sqsubseteq)$.)

4.5.19 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*[34]

$$\boxed{f^{-1}(L)/\mathrm{Ker}(f) \xrightarrow{\cong} L.}$$

ΑΠΟΔΕΙΞΗ. (i) Η ισότητα αυτή έχει ήδη αποδειχθεί στο (iii) τής προτάσεως 4.1.6. Σημειωτέον ότι $f(K) \in \mathbf{Subg}(\mathrm{Im}(f))$, οπότε

$$\Upsilon_f(f(K)) = \Psi_f^{-1}(f(K)) = f^{-1}(f(K)) = K(\mathrm{Ker}(f)) \in \mathbf{Subg}(G; \mathrm{Ker}(f)).$$

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 Ψ_f στην $f(K)$ κατά τα ειωθότα.

(ii) Επειδή $K(\mathrm{Ker}(f)) \in \mathbf{Subg}(G; \mathrm{Ker}(f))$, έχουμε

$$\left.\begin{array}{r} \mathrm{Ker}(f) \sqsubseteq K(\mathrm{Ker}(f)) \\ \mathrm{Ker}(f) \trianglelefteq G \end{array}\right\} \underset{4.2.19}{\Longrightarrow} \mathrm{Ker}(f) \trianglelefteq K(\mathrm{Ker}(f))$$

και το (ii) τού θεωρήματος 4.5.18 για τις $K_1 = \mathrm{Ker}(f)$ και $K_2 = K(\mathrm{Ker}(f))$ δίδει τον ισομορφισμό

$$(K(\mathrm{Ker}(f)))/\mathrm{Ker}(f) \cong \Psi_f\left((K(\mathrm{Ker}(f)))\right)/\Psi_f\left(\mathrm{Ker}(f)\right) = f(K)/\{e_H\} \cong f(K).$$

(iii) Για κάθε $L \in \mathbf{Subg}(\mathrm{Im}(f))$ ισχύουν οι ισότητες

$$L = \left(\Psi_f \circ \Upsilon_f\right)(L) = \Psi_f(f^{-1}(L)) = f(f^{-1}(L))$$

και το (ii) τού θεωρήματος 4.5.18 για τις $K_1 = \mathrm{Ker}(f)$ και $K_2 = f^{-1}(L)$ δίδει τον ισομορφισμό

$$f^{-1}(L)/\mathrm{Ker}(f) \cong \Psi_f(f^{-1}(L))/\Psi_f(\mathrm{Ker}(f)) = L/\{e_H\} \cong L,$$

απ' όπου έπεται το ζητούμενο. □

[34] Εάν $|\mathrm{Ker}(f)| < \infty$ και $|L| < \infty$, τότε από αυτόν και από το θεώρημα 4.1.22 τού Lagrange έπεται η ισότητα (4.10) τού (ii) τού πορίσματος 4.1.13.

4.5.20 Πόρισμα. (Θεώρημα αντιστοιχίσεως ορθόθετων υποομάδων για τον π_H^G.) *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \trianglelefteq G$. Τότε για την αμφίρριψη*

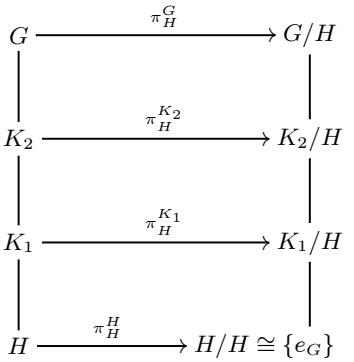
$$\mathbf{Subg}(G;H) \ni K \overset{\Psi_{\pi_H^G}}{\longmapsto} \pi_H^G(K) = \pi_H^K(K) = K/H \in \mathbf{Subg}(G/H) \tag{4.40}$$

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:



(ii) *Για $K_1, K_2 \in \mathbf{Subg}(G;H)$ με $K_1 \trianglelefteq K_2$ υφίσταται ισομορφισμός*

$$\boxed{K_2/K_1 \overset{\cong}{\longrightarrow} (K_2/H)\,/\,(K_1/H)\,.}$$

(iii) *Περιορίζοντας την αμφίρριψη* (4.40) *στο σύνολο*

$$\mathbf{NSubg}(G;H) = \mathbf{NSubg}(G) \cap \mathbf{Subg}(G;H)$$

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

$$(\mathbf{NSubg}(G;H), \trianglelefteq) \quad \textit{και} \quad (\mathbf{NSubg}(G/H), \trianglelefteq)\,.$$

(iv) $\mathrm{NCL}_G(K_1,K_2)/H = \mathrm{NCL}_G(K_1/H, K_2/H),\ \forall\,(K_1,K_2) \in \mathbf{NSubg}(G;H)^2$.

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμοσθεί το θεώρημα 4.5.18 για τον φυσικό επιμορφισμό $\pi_H^G : G \longrightarrow G/H$. □

4.5.21 Τρίτο Θεώρημα Ισομορφισμών. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \trianglelefteq G$. Τότε*

$$\boxed{G/K \cong (G/H)\,/\,(K/H)} \tag{4.41}$$

για κάθε $K \in \mathbf{NSubg}(G;H)$.

ΑΠΟΔΕΙΞΗ. Λαμβανομένου υπ' όψιν τού ότι $H \sqsubseteq K, H \trianglelefteq G \underset{4.2.19}{\Longrightarrow} H \trianglelefteq K$, αυτή έπεται άμεσα ύστερα από εφαρμογή τού (ii) τού πορίσματος 4.5.20 για τις ομάδες $K_1 = K$ και $K_2 = G$. □

4.5.22 Παράδειγμα. Εάν $m,n \in \mathbb{N}$, τότε (σύμφωνα με την πρόταση 4.2.6) 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. 2.2.20 (i)), το θεώρημα 4.5.21 μας παρέχει ισομορφισμό

$$\boxed{\mathbb{Z}/m\mathbb{Z} \xrightarrow{\cong} (\mathbb{Z}/n\mathbb{Z})\ /\ (m\mathbb{Z}/n\mathbb{Z})\,.}$$

4.5.23 Πόρισμα. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \trianglelefteq G$. Εάν $K_1, K_2 \in \mathbf{Subg}(G)$ με $K_1 \trianglelefteq K_2$, τότε*

$$\boxed{HK_2/HK_1 \cong K_2/(K_1(K_2 \cap H)).}$$

ΑΠΟΔΕΙΞΗ. 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 4.5.13). 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 4.5.19 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 4.5.18 λαμβάνουμε

$$\begin{aligned} K_2/K_1(K_2 \cap H) &\cong \Psi_f\,(K_2)\,/\Psi_f\,(K_1(K_2 \cap H)) = f(K_2)/f(K_1(K_2 \cap H)) \\ &= (HK_2/H)\,/f(K_1(K_2 \cap H)). \end{aligned}$$

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 4.5.21. □

Ασκήσεις

4-1. Εάν $(G, \cdot)$ είναι μια ομάδα, να αποδειχθούν τα εξής:

(i) $HH = H,\ \forall H \in \mathbf{Subg}(G)$.

(ii) Έστω $A \in \mathfrak{P}(G) \setminus \{\varnothing\}$ με $AA = A$. Εάν το A είναι πεπερασμένο σύνολο, τότε $A \sqsubseteq G$.

(iii) Το (ii) δεν είναι πάντοτε αληθές εάν αφαιρεθεί η προϋπόθεση ότι το A είναι πεπερασμένο.

4-2. Έστω $(G, \cdot)$ μια ομάδα. Εάν $A \in \mathfrak{P}(G) \setminus \{\varnothing\}$, τότε θέτουμε

$$A^{-1} := \left\{ a^{-1} \middle|\, a \in A \right\}.$$

Να αποδειχθεί ότι τα ακόλουθα είναι ισοδύναμα:

(i) $A \sqsubseteq G$.

(ii) Εάν $a, b \in A$, τότε $ab \in A$ και $a^{-1} \in A$.

(iii) $AA \subseteqq A$ και $A^{-1} \subseteqq A$.

(iv) $AA = A$ και $A^{-1} = A$.

(v) Εάν $a, b \in A$, τότε $ab^{-1} \in A$.

(vi) $AA^{-1} \subseteqq A$.

(vii) $AA^{-1} = A$.

4-3. Έστω $(G, \cdot)$ μια ομάδα. Εάν $K_1, K_2, H \in \mathbf{Subg}(G)$ και $K_1 \sqsubseteq K_2$, να αποδειχθούν τα ακόλουθα:

(i) $K_1H \cap K_2 = K_1(H \cap K_2)$.

(ii) $[K_1 \cap H = K_2 \cap H \ \text{ και } \ K_1H = K_2H] \Longrightarrow K_1 = K_2$.

4-4. Να δοθεί ένα σύστημα αριστερών εκπροσώπων (i) τής $H := 4\mathbb{Z}$ εντός τής $2\mathbb{Z}$ και (ii) τής $K := \langle [18]_{36} \rangle$ εντός τής $\mathbb{Z}_{36}$.

4-5. Να γραφεί η πολλαπλασιαστική ομάδα $\mathbb{Z}_{15}^{\times}$ ως αποσυνδετή ένωση αριστερών πλευρικών κλάσεων τής $H = \langle [7]_{15} \rangle$ (εντός τής $\mathbb{Z}_{15}^{\times}$).

4-6. Να δοθεί ένα σύστημα αριστερών εκπροσώπων τής $H := \langle \alpha \circ \beta \rangle$ εντός τής διεδρικής ομάδας $\mathbf{D}_4 = \langle \alpha, \beta \rangle$ (τής ορισθείσας στο εδ. 3.4.4).

4-7. Να δοθεί ένα σύστημα αριστερών εκπροσώπων τής $H := \langle [1\ 2\ 3] \rangle$ εντός τής εναλλάσσουσας ομάδας $\mathfrak{A}_4$.

4-8. Να δοθούν παραδείγματα ομάδων G και υποομάδων $\{e_G\} \neq H \sqsubset G$, ούτως ώστε:

(i) $|H| < \infty$ και $|G : H| < \infty$, (iii) $|H| = \infty$ και $|G : H| < \infty$,

(ii) $|H| < \infty$ και $|G : H| = \infty$, (iv) $|H| = \infty$ και $|G : H| = \infty$.

4-9. (i) Εάν $q \in \mathbb{Q}$, να δειχθεί ότι το $q\mathbb{Z} := \{\, qk |\, k \in \mathbb{Z}\}$ αποτελεί μια υποομάδα τής $(\mathbb{Q}, +)$.

(ii) Εάν $q, q' \in \mathbb{Q}$, να δειχθεί ότι $q\mathbb{Z} \sqsubseteq q'\mathbb{Z} \iff q = q'm$, για κάποιον $m \in \mathbb{Z}$.

(iii) Εάν $n, m \in \mathbb{Z}$, να προσδιορισθούν οι δείκτες $\left|\mathbb{Q} : \frac{1}{n}\mathbb{Z}\right|, \left|\frac{1}{n}\mathbb{Z} : \mathbb{Z}\right|$ και $\left|\frac{1}{n}\mathbb{Z} : m\mathbb{Z}\right|$.

4-10. Να αποδειχθεί ότι η $(\mathbb{Q}, +)$ δεν διαθέτει καμία γνήσια υποομάδα πεπερασμένου δείκτη και ότι δεν είναι ισόμορφη με την $(\mathbb{Q}_{>0}, \cdot)$. [*Υπόδειξη*: Εάν $n \in \mathbb{N}, n \geq 2,$ η γνήσια υποομάδα $H := \langle \{2^n, 3, 5, 7, 11, 13, ...\} \rangle$ τής $(\mathbb{Q}_{>0}, \cdot)$ έχει δείκτη n. Πρβλ. 2.2.5 (iv).]

4-11. Να αποδειχθούν τα εξής:

(i) Ο δείκτης τής $(\mathbb{R}_{>0}, \cdot)$ εντός τής $(\mathbb{R}\smallsetminus\{0\}, \cdot)$ (βλ. 2.4.2 (iii)) ισούται με 2.

(ii) Η μόνη γνήσια υποομάδα τής $(\mathbb{R}\smallsetminus\{0\}, \cdot)$ πεπερασμένου δείκτη είναι η $(\mathbb{R}_{>0}, \cdot)$.

4-12. Εάν $K \sqsubseteq G$ και $H \sqsubseteq G$, και εάν η H είναι υποομάδα πεπερασμένου δείκτη εντός τής G, να αποδειχθεί ότι και η $K \cap H$ είναι υποομάδα πεπερασμένου δείκτη εντός τής K, και ότι -επιπροσθέτως- ισχύει η ανισοϊσότητα:

$$|K : H \cap K| \leq |G : H|.$$

4-13. Εάν H και K είναι δυο υποομάδες μιας πεπερασμένης ομάδας $(G, \cdot)$, να δειχθεί ότι ισχύει η συνεπαγωγή $\mu\kappa\delta(|G : H|, |G : K|) = 1 \Rightarrow HK = G$.

4-14. Εάν H και K είναι δυο υποομάδες μιας πεπερασμένης ομάδας $(G, \cdot)$, να αποδειχθούν τα ακόλουθα:

(i) $|\langle H, K \rangle : K| \geq |H : H \cap K|$.

(ii) Εάν $|H : H \cap K| > \frac{1}{2}|G : K|$, τότε $\langle H, K \rangle = G$.

(iii) $|H : H \cap K| = |G : K| \Leftrightarrow HK = G\ (= KH = \langle H, K \rangle)$.

4-15. Να υπολογισθούν: (i) Η τάξη τού στοιχείου $[5]_{12} + \langle [4]_{12} \rangle$ τής πηλικοομάδας $\mathbb{Z}_{12}/\langle [4]_{12} \rangle$ και (ii) η τάξη τού στοιχείου $[26]_{60} + \langle [12]_{60} \rangle$ τής πηλικοομάδας $\mathbb{Z}_{60}/\langle [12]_{60} \rangle$.

4-16. Έστω $H := \langle [12]_{24} \rangle \sqsubset \mathbb{Z}_{24}$. Να προσδιορισθούν τα στοιχεία τής πηλικοομάδας $\mathbb{Z}_{24}/H$ και να υπολογισθεί η τάξη καθενός εξ αυτών. Εν συνεχεία, να δειχθεί ότι $\mathbb{Z}_{24}/H \cong \mathbb{Z}_{12}$.

4-17. Έστω $H := \langle [13]_{28} \rangle \sqsubset \mathbb{Z}_{28}^{\times}$. Να προσδιορισθούν τα στοιχεία τής πηλικοομάδας $\mathbb{Z}_{28}^{\times}/H$ και να υπολογισθεί η τάξη καθενός εξ αυτών. Εν συνεχεία, να δειχθεί ότι $\mathbb{Z}_{28}^{\times}/H \cong \mathbb{Z}_6$.

4-18. Να προσδιορισθεί το σύνολο $\mathbf{NSubg}(\mathfrak{A}_4)$ των ορθόθετων υποομάδων τής εναλλάσσουσας ομάδας $(\mathfrak{A}_4, \circ)$.

4-19. Έστω $n \in \mathbb{N}$, $n \geq 3$. Εάν $G \sqsubseteq \mathfrak{S}_n$ και $H := G \cap \mathfrak{A}_n$, να αποδειχθεί ότι είτε $H = G$ είτε $|H| = \frac{1}{2}|G|$.

4-20. Έστω $n \in \mathbb{N}$, $n \geq 3$. Εάν $G \sqsubseteq \mathfrak{S}_n$ και $G \not\sqsubseteq \mathfrak{A}_n$, να αποδειχθεί ότι είτε $G \cong \mathbb{Z}_2$ είτε η G είναι μη απλή.

4-21. Να αποδειχθεί ότι η $\mathfrak{A}_4$ είναι η μοναδική υποομάδα τής $\mathfrak{S}_4$ που έχει τάξη 12.

4-22. Έστω $(G, \cdot)$ μια ομάδα. Εάν $K \sqsubseteq H \sqsubseteq G$, να αποδειχθούν τα εξής:

(i) Εάν $L \sqsubseteq G$, τότε ισχύει η συνεπαγωγή $K \trianglelefteq H \Rightarrow K \cap L \trianglelefteq H \cap L$.

(ii) Εάν $L \trianglelefteq G$, τότε ισχύει η συνεπαγωγή $K \trianglelefteq H \Rightarrow KL \trianglelefteq HL$.

4-23. Έστω ότι $\{G_j\}_{j\in\mathbb{N}}$ είναι μια ακολουθία γνησίων υποομάδων μιας ομάδας $(G, \cdot)$, για την οποία ισχύει $G_j \subseteq G_{j+1}$ για κάθε $j \in \mathbb{N}$ και $G = \bigcup\limits_{j\in\mathbb{N}} G_j$. Εάν $H_j \trianglelefteq G_j$ με $H_j \subseteq H_{j+1}$ για κάθε $j \in \mathbb{N}$ και $H := \bigcup\limits_{j\in\mathbb{N}} H_j$, να αποδειχθεί ότι $H \trianglelefteq G$.

4-24. Έστω $(G, \cdot)$ μια πεπερασμένη κυκλική ομάδα και έστω p ένας πρώτος αριθμός που διαιρεί την τάξη της. Να αποδειχθεί ότι το $H := \{\, g^p \,|\, g \in G\}$ αποτελεί μια υποομάδα τής G τάξεως $\frac{|G|}{p}$.

4-25. Έστω $(G, \cdot)$ μια πεπερασμένη κυκλική ομάδα, όπου $G = \langle g \rangle$ και $|G| = n$. Εάν ο $m \in \mathbb{N}$ είναι ένας διαιρέτης τού n, να αποδειχθεί ότι:

(i) $|G/\langle g^m \rangle| = m$, και

(ii) $G/\langle g^m \rangle = \langle g \langle g^m \rangle \rangle$.

4-26. Εάν H είναι μια ορθόθετη υποομάδα μιας πεπερασμένης ομάδας $(G, \cdot)$ με μκδ$(|G/H|, |H|) = 1$ και $g \in G$ τέτοιο, ώστε να ισχύει $g^{|H|} = e_G$, να αποδειχθεί ότι $g \in H$.

4-27. Εάν H είναι μια ορθόθετη υποομάδα μιας πεπερασμένης ομάδας $(G, \cdot)$ και $K \sqsubseteq G$ με μκδ$(|G/H|, |K|) = 1$, να αποδειχθεί ότι $K \sqsubseteq H$.

4-28. Έστω $(G,\cdot)$ μια ομάδα. Εάν $H \trianglelefteq G$ και $|G/H| = n \in \mathbb{N}$, να αποδειχθούν τα ακόλουθα:

(i) $g^n \in H,\ \forall g \in G$.

(ii) Εάν $g \in G$ είναι ένα στοιχείο για το οποίο ισχύει $g^m \in H$ για κάποιον $m \in \mathbb{N}$ με μκδ$(m,n) = 1$, τότε $g \in H$.

4-29. Έστω $(G,\cdot)$ μια ομάδα. Υποθέτοντας ότι $H \trianglelefteq G$ με $|H| = m \in \mathbb{N}$ και $n \in \mathbb{N}$ είναι τέτοιος, ώστε μκδ$(m,n) = 1$, να αποδειχθεί ότι για ένα στοιχείο $g \in G$ ισχύουν τα ακόλουθα:

(i) Εάν $\mathrm{ord}(g) = n$, τότε $\mathrm{ord}(gH) = n$ (εντός τής G/H).

(ii) Εάν $\mathrm{ord}(gH) = n$, τότε $\exists g' \in G : [\mathrm{ord}(g') = n$ και $gH = g'H]$.

4-30. Έστω $(G,\cdot)$ μια πεπερασμένη ομάδα τάξεως n. Να αποδειχθεί ότι

$$\exists X \in \mathfrak{P}(G) : [\langle X\rangle = G \ \text{ με } \ \mathrm{card}(X) \leq \log_2(n)].$$

[*Υπόδειξη*: Εάν $H \in \mathbf{Max\text{-}Subg}(G)$ και $g \in G \smallsetminus H$, τότε $\langle H, g\rangle = G$. Επειδή $H \sqsubset G$, είναι δυνατόν να χρησιμοποιηθεί μαθηματική επαγωγή ως προς την τάξη n τής G. Υποθέτοντας ότι η H μπορεί να παραχθεί το πολύ από $\log_2(m)$ στοιχεία, όπου $m := |H|$, η G μπορεί να παραχθεί το πολύ από $\log_2(m)+1$ στοιχεία. Απομένει να ληφθεί υπ' όψιν το θεώρημα 4.1.22 τού Lagrange.]

4-31. Έστω $(G,\cdot)$ μια ομάδα τάξεως 105. Εάν $H \sqsubseteq G$ με $|H| \geq 36$, να αποδειχθεί ότι $H = G$.

4-32. Έστω $H \sqsubset \mathfrak{S}_4$. Εάν $|H| > 8$, να αποδειχθεί ότι $|H| = 12$.

4-33. Εάν $H := \langle\sigma\rangle \sqsubset \mathfrak{S}_7$ και $K := \langle\tau\rangle \sqsubset \mathfrak{S}_7$, όπου

$$\sigma := [1\ 2\ 3\ 4\ 5] \ \text{ και } \ \tau := [1\ 3] \circ [2\ 4\ 5] \circ [6\ 7]\,,$$

να αποδειχθεί ότι $H \cap K = \{\mathrm{id}\}$.

4-34. Έστω $(G,\cdot)$ μια ομάδα. Εάν $H \sqsubseteq G$ και $K \sqsubseteq G$ με $|H| = 175$ και $|K| = 133$, να αποδειχθεί ότι η ομάδα $H \cap K$ είναι κυκλική.

4-35. Έστω $(G,\cdot)$ μια ομάδα τάξεως 21. Να αποδειχθούν τα εξής:

(i) Κάθε γνήσια υποομάδα τής G είναι κυκλική.

(ii) Η G διαθέτει κάποιο στοιχείο τάξεως 3.

4-36. Εάν $m,n \in \mathbb{N}$ και μκδ$(m,n) = 1$,να αποδειχθεί ότι

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 (\mathrm{mod}\, mn).$$

όπου ϕ η συνάρτηση φι τού Euler. (Βλ. Β.4.15.) [*Υπόδειξη*: Να εφαρμοσθεί καταλλήλως το πόρισμα 4.1.30, σε συνδυασμό με το πόρισμα Β.2.10.]

4-37. Εάν $m, n \in \mathbb{N}$ και $m \geq 2$, να αποδειχθεί ότι $n \mid \phi(m^n - 1)$, όπου ϕ η συνάρτηση φι τού Euler. (Βλ. Β.4.15.) [*Υπόδειξη*: Να εφαρμοσθεί το θεώρημα 4.1 .22 τού Lagrange για μια υποομάδα τάξεως n μιας ομάδας τάξεως $\phi(m^n - 1)$.]

4-38. Έστω $(G, \cdot)$ μια ομάδα. Εάν οι $H \sqsubseteq G$ και $K \sqsubseteq G$ είναι πεπερασμένες και $HK \sqsubseteq G$, να αποδειχθούν τα ακόλουθα:

(i) Εάν $x \in H$ και $y \in K$, τότε $\text{ord}(xy) \mid |H|\,|K|$. (Ιδιαιτέρως, εάν το $\langle x\rangle\langle y\rangle$ είναι πεπερασμένη υποομάδα τής G, τότε $\text{ord}(xy) \mid \text{ord}(x)\text{ord}(y)$.)

(ii) Εάν L είναι μια πεπερασμένη υποομάδα τής G, τότε ισχύει η συνεπαγωγή

$$\left.\begin{array}{c} HL = KL \\ \text{μκδ}(|H|, |L|) = \text{μκδ}(|K|, |L|) = 1 \end{array}\right\} \Longrightarrow H = K.$$

4-39. Έστω $(G, \cdot)$ τυχούσα πεπερασμένη ομάδα άρτιας τάξεως και έστω K μια υποομάδα αυτής με $|K| = \frac{1}{2}|G|$. Να αποδειχθεί ότι για κάθε $H \in \mathbf{Subg}(G)$ ισχύουν τα εξής:

(i) Είτε $H \sqsubseteq K$ είτε $|H \cap K| = \frac{1}{2}|H|$.

(ii) $H = (H \cap K) \coprod h\,(H \cap K)\,,\ \forall h \in H \smallsetminus K$.

4-40. Έστω n ένας φυσικός αριθμός ≥ 3 και έστω $\mathfrak{D}_n$ το σύνολο των θετικών ακεραίων διαιρετών τού n. (Βλ. Β.2.34). Να αποδειχθεί ότι για την n-οστή διεδρική ομάδα $\mathbf{D}_n = \langle \alpha, \beta\rangle$ (την ορισθείσα στο εδάφιο 3.4.4) ισχύουν τα ακόλουθα:

(i) Ο εκθέτης 2.3.24 τής $\mathbf{D}_n$ είναι ο

$$\exp(\mathbf{D}_n) = \text{εκπ}(n, 2) = \begin{cases} 2n, & \text{όταν } n \equiv 1 (\text{mod}\, 2), \\ n, & \text{όταν } n \equiv 0 (\text{mod}\, 2). \end{cases}$$

(ii) Κάθε υποομάδα τής $\mathbf{D}_n$ είναι είτε κυκλική είτε ισόμορφη με την $\mathbf{V}$ είτε ισόμορφη με κάποια διεδρική ομάδα. Συγκεκριμένα,

$$\boxed{\mathbf{Subg}(\mathbf{D}_n) = \{\, H_d \mid d \in \mathfrak{D}_n\} \coprod \{\, H_{d,j} \mid d \in \mathfrak{D}_n, j \in \{0, 1, ..., d-1\}\}\,,}$$

όπου $H_d := \left\langle \beta^d \right\rangle \cong \mathbb{Z}_{\frac{n}{d}}$ και

$$H_{d,j} := \left\langle \alpha \circ \beta^{d-j}, \beta^d \right\rangle \cong \begin{cases} \mathbf{D}_{\frac{n}{d}}, & \text{όταν } d \notin \{\frac{n}{2}, n\}, \\ \mathbf{V}, & \text{όταν } n \equiv 0 (\text{mod}\, 2) \text{ και } d = \frac{n}{2}, \\ \left\langle \alpha \circ \beta^{n-j} \right\rangle \cong \mathbb{Z}_2, & \text{όταν } d = n. \end{cases}$$

(iii) $H_d \sqsubset H_{d'} \Leftrightarrow [d' \mid d \text{ και } d \neq d']$, για οιουσδήποτε $d, d' \in \mathfrak{D}_n$, $H_d \sqsubset H_{d,j}$ για κάθε $j \in \{0, 1, ..., d-1\}$ και $H_{d,j} \cong H_{d,j'}$ για οιουσδήποτε υποδείκτες $j, j' \in \{0, 1, ..., d-1\}$.

(iv) $\mathbf{Max\text{-}Subg}(\mathbf{D}_n) = \{H_1\} \coprod \{\, H_{p,j} \mid p \in \mathfrak{D}_n, p \text{ πρώτος},\ j \in \{0, 1, ..., p-1\}\}$.

(v) $\mathbf{Min\text{-}Subg}(\mathbf{D}_n) = \{\, H_p \mid p \in \mathfrak{D}_n, p \text{ πρώτος}\} \coprod \{\, H_{n,j} \mid j \in \{0, 1, ..., n-1\}\}$,
όταν ο n δεν είναι πρώτος, και $= \{H_1\} \coprod \{\, H_{n,j} \mid j \in \{0, 1, ..., n-1\}\}$ όταν ο n είναι

πρώτος.

(vi) Το σύνολο των ορθόθετων υποομάδων τής $\mathbf{D}_n$ είναι το

$$\mathbf{NSubg}(\mathbf{D}_n) = \begin{cases} \{H_d \,|\, d \in \mathfrak{D}_n\} \coprod \{\mathbf{D}_n\}, & \text{όταν } n \equiv 1 (\mathrm{mod}\, 2), \\ \{H_d \,|\, d \in \mathfrak{D}_n\} \coprod \{\langle \alpha, \beta^2 \rangle, \langle \alpha \circ \beta, \beta^2 \rangle, \mathbf{D}_n\}, & \text{όταν } n \equiv 0 (\mathrm{mod}\, 2). \end{cases}$$

(vii) Εάν $n = p_1^{\nu_1} p_2^{\nu_2} \cdots p_k^{\nu_k}$, $k \in \mathbb{N}$, $\nu_1, ..., \nu_k \in \mathbb{N}$, είναι η κανονική παράσταση (B.19) τού n ως γινομένου πρώτων αριθμών $p_1, ..., p_k$, τότε

$$\mathrm{card}\,(\mathbf{Subg}(\mathbf{D}_n)) = \mathrm{card}(\mathfrak{D}_n) + \sum_{d \in \mathfrak{D}_n} d = \prod_{i=1}^{k} (\nu_i + 1) + \prod_{i=1}^{k} \left(\tfrac{p_i^{\nu_i + 1} - 1}{p_i - 1} \right),$$

$\mathrm{card}(\mathbf{Max\text{-}Subg}(\mathbf{D}_n)) = p_1 + \cdots + p_k + 1$, $\mathrm{card}(\mathbf{Min\text{-}Subg}(\mathbf{D}_n)) = k + n$ και

$$\mathrm{card}\,(\mathbf{NSubg}(\mathbf{D}_n)) = \begin{cases} 1 + \prod_{i=1}^{k} (\nu_i + 1), & \text{όταν } n \equiv 1 (\mathrm{mod}\, 2), \\ 3 + \prod_{i=1}^{k} (\nu_i + 1), & \text{όταν } n \equiv 0 (\mathrm{mod}\, 2). \end{cases}$$

(viii) $\mathbf{D}_n / H_1 \cong \mathbb{Z}_2$, $\mathbf{D}_n / H_d \cong \mathbf{D}_d$, $\forall d \in \mathfrak{D}_n \smallsetminus \{1, 2\}$, ενώ για άρτιους n,

$$\mathbf{D}_n / H_2 \cong \mathbf{V},\ \mathbf{D}_n / \langle \alpha, \beta^2 \rangle \cong \mathbb{Z}_2 \cong \mathbf{D}_n / \langle \alpha \circ \beta, \beta^2 \rangle .$$

(ix) Να σχεδιασθούν τα διαγράμματα τού Hasse για τους εξής συνδέσμους: $(\mathbf{Subg}(\mathbf{D}_5), \sqsubseteq)$, $(\mathbf{Subg}(\mathbf{D}_6), \sqsubseteq)$, $(\mathbf{Subg}(\mathbf{D}_7), \sqsubseteq)$, $(\mathbf{Subg}(\mathbf{D}_8), \sqsubseteq)$ και $(\mathbf{Subg}(\mathbf{D}_9), \sqsubseteq)$.

4-41. Έστω p ένας πρώτος αριθμός. Μέσω τής υποομάδας

$$\mathbb{Z}[\tfrac{1}{p}] := \left\{ \tfrac{a}{p^i} \,\middle|\, a \in \mathbb{Z}, i \in \mathbb{N}_0 \right\}$$

τής $(\mathbb{Q}, +)$ ορίζουμε την υποομάδα

$$\boxed{\mathbb{Z}(p^\infty) := \mathbb{Z}[\tfrac{1}{p}]/\mathbb{Z} = \left\{ \tfrac{a}{p^i} + \mathbb{Z} \,\middle|\, a \in \mathbb{Z}, i \in \mathbb{N}_0 \right\}}$$

τής (προσθετικής) πηλικοομάδας $(\mathbb{Q}/\mathbb{Z}, +)$. Να αποδειχθούν τα ακόλουθα:

(i) Η $\mathbb{Z}(p^\infty)$ είναι μια άπειρη, γνήσια υποομάδα τής $\mathbb{Q}/\mathbb{Z}$.

(ii) $\mathbb{Z}(p^\infty) = \langle \{ p^{-n} + \mathbb{Z} \,|\, n \in \mathbb{N}_0 \} \rangle = \bigcup_{n \in \mathbb{N}_0} H_n$, όπου $H_n := \langle p^{-n} + \mathbb{Z} \rangle$.

(iii) $\mathrm{ord}(\frac{a}{p^i} + \mathbb{Z}) = p^\nu$ για κάποιον $\nu \in \mathbb{N}_0$, $\nu \leq i$.

(iv) Εάν $m, n \in \mathbb{N}_0$, τότε $H_m \sqsubset H_n \Leftrightarrow m < n$.

(v) $\mathbf{Subg}(\mathbb{Z}(p^\infty)) \smallsetminus \{\mathbb{Z}(p^\infty)\} = \{ H_n \,|\, n \in \mathbb{N}_0 \}$. (Επομένως, κάθε γνήσια υποομάδα τής $\mathbb{Z}(p^\infty)$ είναι πεπερασμένη και κυκλική, έχουσα ως τάξη της μια δύναμη τού p.)

(vi) Το σύνολο $\mathbf{Subg}(\mathbb{Z}(p^\infty))$ αποτελεί μια αλυσίδα τού συνδέσμου $(\mathbf{Subg}(\mathbb{Z}(p^\infty)), \sqsubseteq)$ υπό την έννοια τού ορισμού A.2.18 (i). (Με άλλα λόγια,

για οιεσδήποτε $H, K \in \mathbf{Subg}(\mathbb{Z}(p^\infty))$ ισχύει είτε $H \sqsubseteq K$ είτε $K \sqsubseteq H$.)

(vii) $\mathbf{Max\text{-}Subg}(\mathbb{Z}(p^\infty)) = \varnothing$.

(viii) Η $\mathbb{Z}(p^\infty)$ δεν είναι πεπερασμένως παραγόμενη.

(ix) Για οιαδήποτε $H \sqsubset \mathbb{Z}(p^\infty)$ ισχύει $\mathbb{Z}(p^\infty)/H \cong \mathbb{Z}(p^\infty)$.

(Η $(\mathbb{Z}(p^\infty), +)$ καλείται, ιδιαιτέρως, p-**σχεδόν κυκλική ομάδα** ή p-**ομάδα τού Prüfer**[35].)

4-42. Να δειχθεί ότι η προσθετική πηλικοομάδα $(\mathbb{Q}/\mathbb{Z}, +)$ είναι ισόμορφη με την $(\mathcal{E}_\infty, \cdot)$. (Βλ. 2.3.6 (i).) [*Υπόδειξη*: Να χρησιμοποιηθεί το 1ο θεώρημα ισομορφισμών 4.5.2 για τον ομομορφισμό $\mathbb{Q}/\mathbb{Z} \ni q+\mathbb{Z} \longmapsto \exp(2\pi i q) \in \mathbb{C}\setminus\{0\}$.]

4-43. Να αποδειχθεί ότι η πολλαπλασιαστική πηλικοομάδα $(\mathbb{S}^1/\mathcal{E}_\infty, \cdot)$ είναι ισόμορφη με την προσθετική πηλικοομάδα $(\mathbb{R}/\mathbb{Q}, +)$. [*Υπόδειξη*: Να χρησιμοποιηθεί το εδ. 4.5.3 (ii) και η άσκηση **4-42**, σε συνδυασμό με το 3ο θεώρημα ισομορφισμών 4.5.21.]

4-44. Έστω p ένας πρώτος αριθμός. Να αποδειχθούν τα ακόλουθα:

(i) $\mathbb{Z}(p^\infty) \cong \mathcal{E}_{p^\infty}$. (Βλ. εδ. 2.3.6.)

(ii) Εάν $(G, \cdot)$ είναι μια ομάδα με $G = \bigcup_{n\in\mathbb{N}_0} H_n$, όπου $H_n \in \mathbf{CSubg}(G)$,

$$\{e_G\} = H_0 \sqsubset H_1 \sqsubset \cdots \sqsubset H_j \sqsubset H_{j+1} \sqsubset \cdots$$

και $|H_n| = p^n$, $\forall n \in \mathbb{N}_0$, τότε $G \cong \mathbb{Z}(p^\infty)$.

4-45. Εάν p είναι ένας πρώτος αριθμός και $n \in \mathbb{N}$, να αποδειχθεί ότι

$$\mathcal{E}_{p^\infty}/\mathcal{E}_{p^n} \cong \mathcal{E}_{p^\infty}.$$

(Βλ. 2.3.6 (ii).) [*Υπόδειξη*: Αρκεί να δειχθεί ότι η απεικόνιση

$$\mathcal{E}_{p^\infty} \ni z \longmapsto z^{p^n} \in \mathcal{E}_{p^\infty}$$

είναι επιμορφισμός και να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών 4.5.2.]

4-46. (i) Να δοθεί ο κατάλογος τού Cayley για την εναλλάσσουσα ομάδα $(\mathfrak{A}_4, \circ)$.

(ii) Να προσδιορισθούν όλοι οι επιμορφισμοί $f : \mathfrak{A}_4 \longrightarrow \mathbb{Z}_3$.

4-47. Να προσδιορισθεί το σύνολο $\mathrm{Hom}(\mathbf{Q}, \mathfrak{S}_3)$ των ομομορφισμών από την ομάδα $\mathbf{Q}$ των τετρανίων στη συμμετρική ομάδα $\mathfrak{S}_3$.

4-48. Για οιουσδήποτε $m, n \in \mathbb{N}$ να αποδειχθεί ότι

$$\mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_n) \cong \mathbb{Z}_{\text{μκδ}(m,n)}.$$

[*Υπόδειξη*: Θέτοντας $d := \text{μκδ}(m, n)$, να ορισθεί η

$$f : \mathbb{Z}_d \longrightarrow \mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_n),\ [k]_d \longmapsto f([k]_d) := \eta_k,\ \forall k \in \mathbb{Z},$$

[35] Προς τιμήν τού Γερμανού μαθηματικού Heinz Prüfer (1896-1934) που την εισήγαγε και μελέτησε τις ιδιότητές της στο άρθρο του *Untersuchungen über die Zerlegbarkeit der abzählbaren primären Abelschen Gruppen,* Math. Zeitschrift **17** (1923), 35-61.

όπου $\eta_k\left([l]_m\right) := \frac{kn}{d}[l]_n,\ \forall l \in \mathbb{Z}$, να δειχθεί ότι είναι (i) μια καλώς ορισμένη επιρριπτική απεικόνιση και (ii) επιμορφισμός (προσθετικών) ομάδων, και -εν συνεχεία- να υπολογισθεί ο πυρήνας $\mathrm{Ker}(f)$.]

4-49. Να αποδειχθεί ότι το σύνολο

$$G := \left\{ \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix} \right) \in \mathrm{Mat}_{2\times 2}(\mathbb{R}) \,\middle|\, (a,b) \neq (0,0) \right\},$$

εφοδιασμένο με τον πολλαπλασιασμό πινάκων, αποτελεί μια υποομάδα τής $\mathrm{GL}_2(\mathbb{R})$ και είναι ισόμορφη με την $(\mathbb{C}\smallsetminus\{0\}, \cdot)$.

4-50. Εάν $G := \mathrm{UT}_2\left(\mathbb{R}\right)^{\times}$ (βλ. D.2.21) και

$$H := \left\{ \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix} \right) \in G \,\middle|\, x \in \mathbb{R} \right\},$$

να αποδειχθούν τα εξής:

(i) $H \lhd G$.

(ii) Η H είναι ισόμορφη με την $(\mathbb{R}, +)$.

(iii) Η G/H είναι αβελιανή (παρότι η ίδια η G δεν είναι αβελιανή).

4-51. Θεωρούνται οι ακόλουθες υποομάδες τής $\mathrm{UT}_3\left(\mathbb{R}\right)^{\times}$ (βλ. D.2.21):

$$G := \left\{ \left(\begin{smallmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & c \end{smallmatrix} \right) \,\middle|\, a,b,c \in \mathbb{R}, c > 0 \right\},\ H := \left\{ \left(\begin{smallmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{smallmatrix} \right) \,\middle|\, a,b \in \mathbb{R} \right\}.$$

Να αποδειχθούν τα εξής:

(i) $H \lhd G$.

(ii) Η πηλικοομάδα G/H είναι ισόμορφη με την $(\mathbb{R}_{>0}, \cdot)$.

4-52. Να αποδειχθεί ότι για κάθε $n \in \mathbb{N}$, $n \geq 2$, και για κάθε μη τετριμμένο μεταθετικό δακτύλιο R με μοναδιαίο στοιχείο υφίστανται ισομορφισμοί (πολλαπλασιαστικών) ομάδων:

$$\mathrm{UT}_n\left(R\right)^{\times}/\mathrm{UT}_n^{[1]}\left(R\right) \cong \mathrm{Diag}_n(R) \cong \mathrm{LT}_n\left(R\right)^{\times}/\mathrm{LT}_n^{[1]}\left(R\right).$$

(Βλ. D.1.6 (i), D.2.21 και D.2.23.)

4-53. Έστω $(F, +, \cdot)$ ένα σώμα και έστω τυχών $n \in \mathbb{N}$. Επί τού (συνήθους) F-διανυσματικού χώρου F^n (τα στοιχεία τού οποίου ταυτίζονται με $(1 \times n)$-πίνακες με εγγραφές ειλημμένες από το F) ορίζεται, δοθέντος ενός πίνακα $\mathbf{A} \in \mathrm{GL}_n(F)$ και ενός $\mathbf{b} \in F^n$, η απεικόνιση:

$$T_{\mathbf{A},\mathbf{b}} : F^n \longrightarrow F^n,\ \ \mathbf{x} \longmapsto T_{\mathbf{A},\mathbf{b}}(\mathbf{x}) := \mathbf{x}\mathbf{A}^{\intercal} + \mathbf{b}.$$

Θέτοντας $\mathrm{Trans}(F^n) := \{T_{\mathbf{I}_n,\mathbf{b}} |\, \mathbf{b} \in F^n\}$ και

$$\boxed{\mathrm{AGL}_n(F) := \{T_{\mathbf{A},\mathbf{b}} |\, \mathbf{A} \in \mathrm{GL}_n(F), \mathbf{b} \in F^n\},}$$

να αποδειχθούν τα ακόλουθα:

(i) $\mathrm{AGL}_n(F) \sqsubseteq \mathfrak{S}_{F^n}$. (Η $\mathrm{AGL}_n(F)$ καλείται, ιδιαιτέρως, **συσχετική (γενική γραμμική) ομάδα βαθμού** n **υπεράνω τού** F.)

(ii) $\mathrm{Trans}(F^n) \trianglelefteq \mathrm{AGL}_n(F)$ και $\mathrm{AGL}_n(F)/\mathrm{Trans}(F^n) \cong \mathrm{GL}_n(F)$.

(iii) Η $\mathrm{AGL}_n(F)$ είναι ισόμορφη με την (πολλαπλασιαστική) ομάδα πινάκων

$$\left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{n1} & \cdots & a_{nn} & b_n \\ 0_F & \cdots & 0_F & 1_F \end{pmatrix} \;\middle|\; \begin{array}{c} \mathbf{A} = (a_{ij})_{1 \le i,j \le n} \in \mathbf{GL}_n(F), \\ \mathbf{b} = (b_1, ..., b_n) \in F^n \end{array} \right\} \sqsubset \mathbf{GL}_{n+1}(F).$$

(iv) Η $\mathrm{AGL}_1(\mathbb{Z}_3)$ είναι ισόμορφη με την $\mathfrak{S}_3$.

4-54. Έστω $(G, \cdot)$ μια μη τετριμμένη ομάδα. Εάν $K \sqsubseteq H \sqsubseteq G$ με $K \trianglelefteq G$, να αποδειχθεί ότι $H \in \mathbf{Max\text{-}Subg}(G) \Leftrightarrow H/K \in \mathbf{Max\text{-}Subg}(G/K)$.

4-55. Έστω $(G, \cdot)$ μια μη τετριμμένη ομάδα και έστω $H \sqsubseteq G$. Εάν $|G : H| = p$, για κάποιον πρώτο αριθμό p, να αποδειχθεί ότι $H \in \mathbf{Max\text{-}Subg}(G)$.

4-56. Έστω $(G, \cdot)$ μια μη τετριμμένη ομάδα. Εάν H, K είναι δυο μη τετριμμένες ορθόθετες υποομάδες της με $H \cap K = \{e_G\}$ και εάν $|G : H| = |G : K| = p$, όπου p ένας πρώτος αριθμός, να δειχθεί ότι η G είναι μια μη κυκλική ομάδα τάξεως p^2.

4-57. Έστω $(G, \cdot)$ μια ομάδα τάξεως $|G| = pq$, όπου p, q είναι δυο πρώτοι αριθμοί με $p < q$. Να αποδειχθεί ότι υπάρχει *το πολύ μία* $H \in \mathbf{Subg}(G)$ τάξεως $|H| = q$ και ότι αυτή (εάν υπάρχει) οφείλει να είναι ορθόθετη. [*Υπόδειξη*: Να χρησιμοποιηθεί το πόρισμα 4.5.11, το θεώρημα 4.1.22 τού Lagrange και το πόρισμα 4.4.24. *Σημείωση*. Αργότερα (στο λήμμα 5.7.9) θα δούμε ότι υπάρχει *πάντοτε* ακριβώς μία υποομάδα τής G με αυτήν την ιδιότητα.]

4-58. Έστω $f : (G, \cdot) \longrightarrow (H, *)$ ένας επιμορφισμός ομάδων, όπου η H είναι αβελιανή τάξεως $|H| = 105$. Να δειχθεί ότι η G διαθέτει ορθόθετες υποομάδες έχουσες δείκτες $3, 5, 7, 15, 21, 35$ και 105 εντός αυτής. [*Υπόδειξη*: Να χρησιμοποιηθεί το 1ο θεώρημα ισομορφισμών 4.5.2, το θεώρημα 4.4.22 και το πόρισμα 4.4.15.]

4-59. Έστω $(G, \cdot)$ μια μη τετριμμένη ομάδα. Να αποδειχθούν τα εξής:

(i) Εάν η G είναι πεπερασμένως παραγόμενη, τότε κάθε γνήσια υποομάδα της περιέχεται σε κάποια μεγιστική υποομάδα της.

(ii) Εάν υποτεθεί ότι η G είναι πεπερασμένη, τότε διαθέτει μία και μόνον μεγιστική υποομάδα εάν και μόνον εάν είναι κυκλική τάξεως $|G| = p^n$, όπου p είναι ένας πρώτος αριθμός και $n \in \mathbb{N}$.

4-60. Έστω $n \in \mathbb{N}$, $n \ge 3$, και έστω $H := \langle \sigma \rangle \sqsubset \mathfrak{S}_n$ η υποομάδα η παραγόμενη από έναν k-κύκλο σ, όπου $2 \le k \le n$ και $k \equiv 0 (\mathrm{mod}\, 2)$. Να δειχθεί ότι η πηλικοομάδα $H\mathfrak{A}_n/\mathfrak{A}_n$ είναι κυκλική τάξεως k.

4-61. Έστω $(G,\cdot)$ μια ομάδα. Εάν $K \sqsubseteq H \sqsubseteq G$ με $K \trianglelefteq G$ να αποδειχθεί ότι για κάθε $L \sqsubseteq G$ ισχύουν τα εξής:

(i) $K \trianglelefteq H$ και $K \cap L \trianglelefteq H \cap L$.

(ii) Η πηλικοομάδα $H \cap L/K \cap L$ είναι εμφυτεύσιμη εντός τής H/K.

4-62. Μια ομάδα $(G,\cdot)$ καλείται **μετακυκλική** όταν υπάρχει $H \in \mathbf{NSubg}(G)$, τέτοια ώστε αμφότερες οι H και G/H να είναι κυκλικές. Για μια μετακυκλική ομάδα $(G,\cdot)$ να αποδειχθούν τα εξής:

(i) Κάθε $K \in \mathbf{Subg}(G)$ είναι μετακυκλική.

(ii) Εάν $L \in \mathbf{NSubg}(G)$, τότε η πηλικοομάδα G/L είναι μετακυκλική.

4-63. Έστω $(G,\cdot)$ μια ομάδα. Υποθέτοντας ότι

$$H \sqsubseteq G,\ K \sqsubseteq G,\ L \trianglelefteq G,\ L \sqsubseteq H \cap K \ \text{ και } \ (H/L)(K/L) \sqsubseteq G,$$

να αποδειχθεί ότι $HK \sqsubseteq G$ και $(H/L)(K/L) = HK/L$.

4-64. Έστω A τυχόν μη κενό σύνολο και έστω $\sigma \in \mathfrak{S}_A$. (Βλ. 3.1.1.) Ως **φορέας** τής σ ορίζεται (γενικεύοντας τα προαναφερθέντα στο εδ. 3.1.4 (i)) το σύνολο

$$\boxed{\text{supp}(\sigma) := \{\, a \in A |\, \sigma\,(a) \neq a\}\,.}$$

(a) Εάν $\sigma, \tau \in \mathfrak{S}_A$, να αποδειχθούν τα εξής:

(i) $\text{supp}(\sigma^{-1}) = \text{supp}(\sigma)$ και $\text{supp}(\sigma \circ \tau) \subseteq \text{supp}(\sigma) \cup \text{supp}(\tau)$.

(ii) $\text{supp}(\sigma \circ \tau \circ \sigma^{-1}) = \{\, \sigma\,(a) \in A |\, a \in \text{supp}(\tau)\}\,.$

(iii) Εάν $\text{supp}(\sigma) \cap \text{supp}(\tau) = \varnothing$, τότε $\sigma \circ \tau = \tau \circ \sigma$.

(b) Θέτοντας

$$\boxed{\mathfrak{S}_{(A)} := \{\, \sigma \in \mathfrak{S}_A |\, \text{supp}(\sigma) \text{ πεπερασμένο}\}}$$

να αποδειχθούν τα εξής:

(i) $\mathfrak{S}_{(A)} \trianglelefteq \mathfrak{S}_A$. (Η $\mathfrak{S}_{(A)}$ καλείται, ιδιαιτέρως, **περιορισμένη συμμετρική ομάδα** επί τού A.)

(ii) $\mathfrak{S}_{(A)} = \mathfrak{S}_A \Leftrightarrow$ το A είναι πεπερασμένο σύνολο.

(iii) Εάν το A είναι απειροσύνολο, τότε η $\mathfrak{S}_{(A)}$ είναι μια άπειρη περιοδική ομάδα και η $\mathfrak{S}_A/\mathfrak{S}_{(A)}$ άπειρη πηλικοομάδα.

(iv) Κάθε πεπερασμένη ομάδα είναι εμφυτεύσιμη εντός τής $\mathfrak{S}_{(\mathbb{N})}$.

4-65. Έστω A τυχόν *απειροσύνολο* και έστω τυχούσα $\sigma \in \mathfrak{S}_{(A)}$. Εξ ορισμού, $\text{card}(\text{supp}(\sigma)) = n$ για κάποιον $n \in \mathbb{N}$. Εάν $\text{supp}(\sigma) = \{a_1, ..., a_n\}$ είναι η αναγραφή των στοιχείων τού φορέα τής σ (ύστερα από κατάλληλη αρίθμηση αυτών) και $f_\sigma : \text{supp}(\sigma) \longrightarrow \{1, ..., n\}$ η αμφίρριψη $f_\sigma(a_j) := j$, $\forall j \in \{1, ..., n\}$, τότε η απεικόνιση

$$\mathfrak{S}_{\text{supp}(\sigma)} \xrightarrow{\eta_\sigma} \mathfrak{S}_n,\ \ \tau \longmapsto \eta_\sigma(\tau) := f_\sigma \circ \tau \circ f_\sigma^{-1},$$

αποτελεί ισομορφισμό ομάδων. Έστω $\widetilde{\sigma} : \text{supp}(\sigma) \longrightarrow \text{supp}(\sigma)$ ο περιορισμός τής σ επί τού φορέα της (ήτοι $\widetilde{\sigma}(a_j) := \sigma(a_j), \forall j \in \{1, ..., n\}$). Προφανώς, $\widetilde{\sigma} \in \mathfrak{S}_{\text{supp}(\sigma)}$ και $\eta_\sigma(\widetilde{\sigma}) \in \mathfrak{S}_n$. Η σ καλείται **άρτια** (και αντιστοίχως, **περιττή) μετάταξη** τής $\mathfrak{S}_{(A)}$ όταν $\eta_\sigma(\widetilde{\sigma}) \in \mathfrak{A}_n$ (και αντιστοίχως, όταν $\eta_\sigma(\widetilde{\sigma}) \in \mathfrak{S}_n \setminus \mathfrak{A}_n$). Θέτοντας

$$\boxed{\mathfrak{A}_{(A)} := \left\{ \sigma \in \mathfrak{S}_{(A)} \middle| \, \sigma \text{ άρτια μετάταξη} \right\}}$$

να αποδειχθούν τα ακόλουθα:

(i) $\mathfrak{A}_{(A)} \lhd \mathfrak{S}_{(A)}$ με δείκτη $\left|\mathfrak{S}_{(A)} : \mathfrak{A}_{(A)}\right| = 2$. (Η $\mathfrak{A}_{(A)}$ καλείται, ιδιαιτέρως, **περιορισμένη εναλλάσσουσα ομάδα** επί τού A.)

(ii) Η $\mathfrak{A}_{(A)}$ είναι μια *άπειρη απλή ομάδα*.

4-66. Έστω $f : (G, \cdot) \longrightarrow (H, *)$ ένας ομομορφισμός πεπερασμένων ομάδων και έστω $K \sqsubseteq G$. Να αποδειχθούν τα εξής:

(i) $|f(K)| \mid \text{μκδ}(|K|, |\text{Im}(f)|)$.

(ii) $|\text{Im}(f) : f(K)| \mid \text{μκδ}(|G : K|, |\text{Im}(f)|)$.

(iii) Εάν $\text{μκδ}(|K|, |\text{Im}(f)|) = 1$, τότε $K \sqsubseteq \text{Ker}(f)$.

[*Υπόδειξη*: Να χρησιμοποιηθεί το πόρισμα 4.5.4 και το θεώρημα 4.1.22 τού Lagrange.]

4-67. Έστω $f : (G, \cdot) \longrightarrow (H, *)$ ένας ομομορφισμός ομάδων και έστω $K \sqsubseteq G$. Να αποδειχθεί ότι

$$\boxed{|G : K| = |\text{Im}(f) : f(K)| \; |\text{Ker}(f) : \text{Ker}(f|_K)| \, .}$$

Σημείωση. Πρόκειται για τη γενίκευση τού (iii) τού πορίσματος 4.5.4 ακόμη και στην περίπτωση κατά την οποία οι G και H δεν είναι κατ' ανάγκην πεπερασμένες. [*Υπόδειξη*: Να χρησιμοποιηθεί το (iii) τής προτάσεως 4.1.6 και η πρόταση 4.4.2, σε συνδυασμό με τα θεωρήματα 4.5.5 και 4.5.13.]

4-68. Έστω $(G, \cdot)$ μια ομάδα. Εάν $f \in \text{End}(G)$ και $H \in \mathbf{Subg}(G)$ με $f(H) \sqsubseteq H$ και $|G : H| < \infty$, να αποδειχθεί ότι

$$\boxed{|G : \text{Im}(f)| = |H : f(H)| \; |\text{Ker}(f) : \text{Ker}(f|_K)| \, .}$$

4-69. Έστω $(G, \cdot)$ μια αβελιανή ομάδα. Εάν $f_1, f_2 \in \text{End}(G)$ είναι τέτοιοι, ώστε να ικανοποιούνται οι συνθήκες:

(a) $\text{Im}(f_2) \sqsubseteq \text{Ker}(f_1)$ $(\Longleftrightarrow f_1(f_2(G)) = \{e_G\})$,

(b) $\text{Im}(f_1) \sqsubseteq \text{Ker}(f_2)$ $(\Longleftrightarrow f_2(f_1(G)) = \{e_G\})$ και

(c) $|\text{Ker}(f_1) : \text{Im}(f_2)| < \infty$, $|\text{Ker}(f_2) : \text{Im}(f_1)| < \infty$,

τότε ορίζεται το λεγόμενο **πηλίκο τού Herbrand**[36]

$$\boxed{\mathcal{HQ}(G; f_1, f_2) := \frac{|\text{Ker}(f_1) : \text{Im}(f_2)|}{|\text{Ker}(f_2) : \text{Im}(f_1)|}}$$

[36] Προς τιμήν τού Γάλλου μαθηματικού Jacques Herbrand (1908-1931) που το εισήγαγε.

για την G ως προς τους f_1, f_2. Υποθέτοντας ότι $H \sqsubseteq G$ με

$$f_1|_H\,,\, f_2|_H \in \mathrm{End}(H),$$

να αποδειχθούν τα ακόλουθα:

(i) Εάν ορίζεται το $\mathcal{HQ}(G; f_1, f_2)$ και $|G:H| < \infty$, τότε ορίζεται και το $\mathcal{HQ}(H;\, f_1|_H\,,\, f_2|_H)$ και ισχύει η ισότητα

$$\mathcal{HQ}(G; f_1, f_2) = \mathcal{HQ}(H;\, f_1|_H\,,\, f_2|_H).$$

(Ως εκ τούτου, το πηλίκο τού Herbrand για την G δεν μεταβάλλεται αντικαθιστάμενο με εκείνο τής H, υπό την προϋπόθεση ότι $|G:H| < \infty$.)

(ii) Στην περίπτωση κατά την οποία $|G:H| = \infty$, εάν δύο εκ των πηλίκων

$$\mathcal{HQ}(G; f_1, f_2),\ \mathcal{HQ}(H;\, f_1|_H\,,\, f_2|_H)\ \text{ και }\ \mathcal{HQ}(G/H; f_1^{\pi\eta\lambda.}, f_2^{\pi\eta\lambda.})$$

τού Herbrand ορίζονται, τότε ορίζεται και το τρίτο και ισχύει η ισότητα

$$\mathcal{HQ}(G; f_1, f_2) = \mathcal{HQ}(H;\, f_1|_H\,,\, f_2|_H)\,\mathcal{HQ}(G/H; f_1^{\pi\eta\lambda.}, f_2^{\pi\eta\lambda.}).$$

(Εν προκειμένω, $f_j^{\pi\eta\lambda.} \in \mathrm{End}(G/H)$ με $f_j^{\pi\eta\lambda.}(gH) := f_j(g)H$, $\forall g \in G$ και $j = 1, 2$. Βλ. 4.5.5.)

4-70. Έστω $(G, \cdot)$ μια ομάδα. Εάν $H, K \in \mathbf{Subg}(G)$, να αποδειχθούν τα εξής:

(i) Το σύνολο $\mathcal{R}_{\delta.\pi.\kappa.} := \{\,(a,b) \in G \times G |\, \exists (h,k) \in H \times K : a = hbk\}$ αποτελεί μια σχέση ισοδυναμίας επί τού υποκειμένου συνόλου G τής ομάδας αναφοράς. (Η κλάση ισοδυναμίας $[g]_{\mathcal{R}_{\delta.\pi.\kappa.}} := \{\,x \in G |\, (x,g) \in \mathcal{R}_{\delta.\pi.\kappa.}\}$ οιουδήποτε $g \in G$ ως προς την $\mathcal{R}_{\delta.\pi.\kappa.}$ ισούται εμφανώς με το σύνολο

$$\boxed{HgK := \{\,hgk |\, (h,k) \in H \times K\}\,.}$$

Κάθε σύνολο τής μορφής HgK, όπου $g \in G$, καλείται, ιδιαιτέρως, **διπλή πλευρική κλάση τής** $(G, \cdot)$ **ως προς τις** H **και** K. Σύμφωνα με το θεώρημα Α.1.14, το σύνολο όλων των διπλών πλευρικών κλάσεων τής $(G, \cdot)$ ως προς τις H και K αποτελεί έναν *διαμελισμό* τού συνόλου G.)

(ii) Οιαδήποτε διπλή πλευρική κλάση τής $(G, \cdot)$ ως προς τις H και K ισούται με μια ένωση αριστερών πλευρικών κλάσεων τής K και με μια ένωση δεξιών πλευρικών κλάσεων τής H εντός τής $(G, \cdot)$.

(iii) $\mathrm{card}(HgKg^{-1}) = \mathrm{card}(HgK), \forall g \in G$.

(iv) Εάν $|H| < \infty$ και $|K| < \infty$, τότε

$$\mathrm{card}(HgK) = \frac{|H|\ |K|}{|H \cap gKg^{-1}|},\ \forall g \in G.$$

(v) Εάν $|G| < \infty$, ο $\mathrm{card}(HgK)$ δεν είναι απαραιτήτως διαιρέτης τής $|G|$.

(vi) Εάν $|G| < \infty$ και εάν $\{g_1, ..., g_k\}$ είναι ένα πλήρες σύστημα εκπροσώπων τού συνόλου G ως προς την $\mathcal{R}_{\delta.\pi.\kappa.}$ (βλ. εδ. Α.1.12), τότε

$$\boxed{|G| = \sum_{j=1}^{k} \frac{|H|\ |K|}{\left|H \cap g_j K g_j^{-1}\right|}.}$$