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**

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

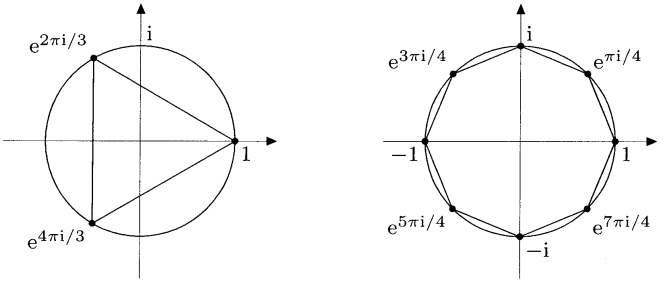
εφοδιασμένος με τον συνήθη πολλαπλασιασμό μιγαδικών αριθμών, αποτελεί υποομάδα τής $(\mathbb{C}\setminus\{0\}, \cdot)$. Επίσης, το σύνολο των n-**οστών ριζών τής μονάδας**[10]

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

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. □

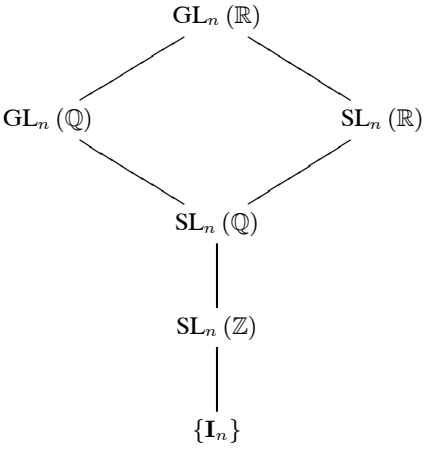
2.1.27 Παραδείγματα. Τα διαγράμματα τού Hasse για τα μερικώς διατεταγμένα σύνολα $(\mathbf{Subg}(\mathbb{Z}_2),\sqsubseteq)$ και $(\mathbf{Subg}(\mathbb{Z}_4),\sqsubseteq)$ των ομάδων $(\mathbb{Z}_2,+)$ και $(\mathbb{Z}_4,+)$ είναι τα εξής:

(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

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

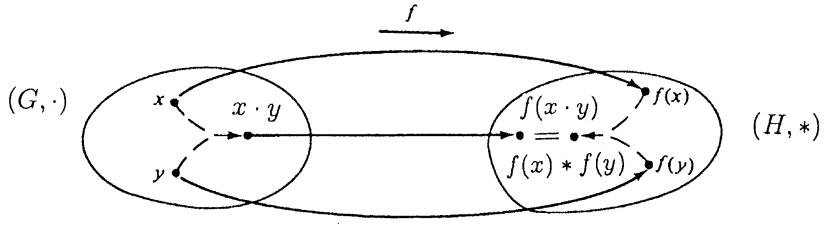
κάτι που αντίκειται στον ορισμό τού l. Άρα $\exp(G) \mid l \Rightarrow \exp(G) = l$. □

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

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

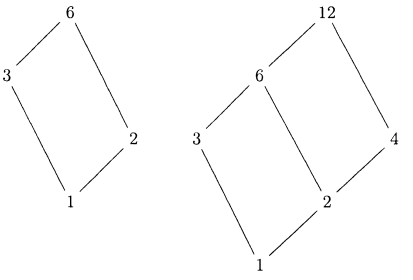
είναι η τετριμμένη $\{[0]_{12}\}$, ολόκληρη η $\mathbb{Z}_{12}$, καθώς και οι

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

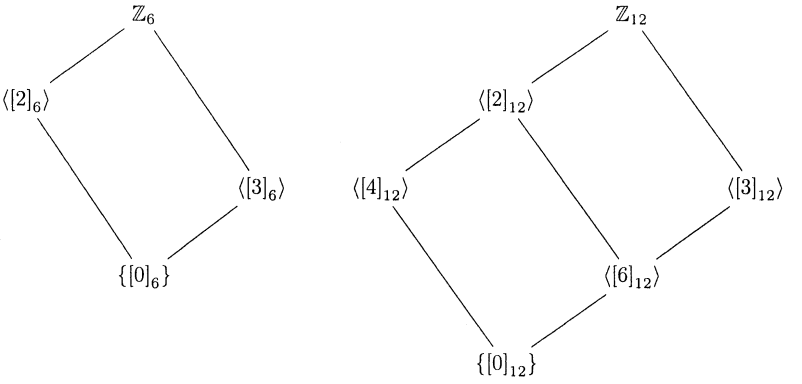
Η αμφίρριψη $\mathfrak{D}_{12} \longrightarrow \mathbf{Subg}(\mathbb{Z}_{12})$ είναι η εξής:

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

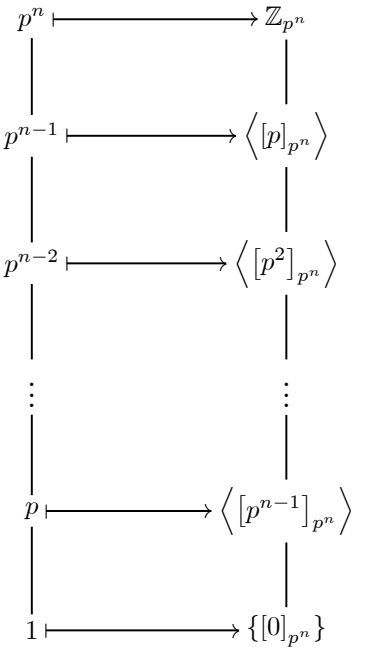
Τα διαγράμματα τού Hasse για τους συνδέσμους των διαιρετών στα (i) και (ii) είναι τα



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

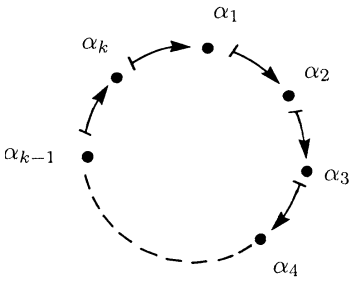
$$\sigma \circ \tau = \tau \circ \sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix},$$

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

$$\sigma^{j_1} \circ \tau^{k_1} = \sigma^{j_2} \circ \tau^{k_2} \Longleftrightarrow [j_1 = j_2 \ \text{και} \ \ k_1 = k_2],$$

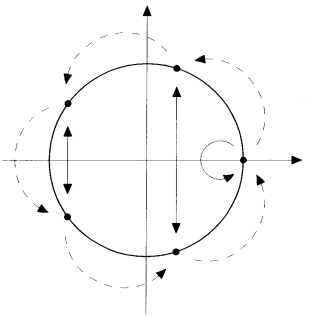
και $\left|\bar{\mathbf{D}}_n\right| = 2n$. Στο εδάφιο 3.4.4 θα ορισθεί άλλη μία σημαντική ομάδα μετατάξεων, η οποία, όπως θα δούμε, είναι ισόμορφη με την $\bar{\mathbf{D}}_n$ και διαθέτει στοιχεία που επιδέχονται μια ειδική *γεωμετρική ερμηνεία*.

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 $k \in \{1, 3, 5, ..., 2m-3, 2m-1\}$.

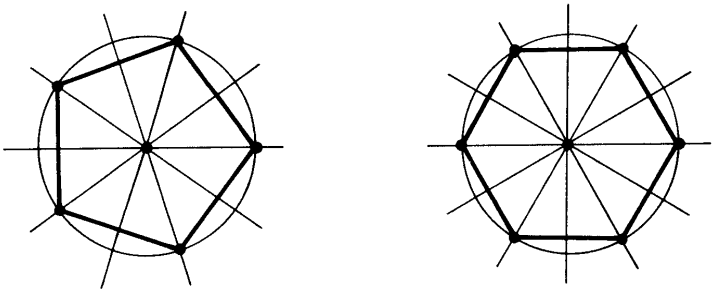
• Εάν $n = 2m$, για κάποιον φυσικό αριθμό $m \geq 2$, τότε η εν λόγω ευθεία η καθορίζεται (κατά περίπτωση)

(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

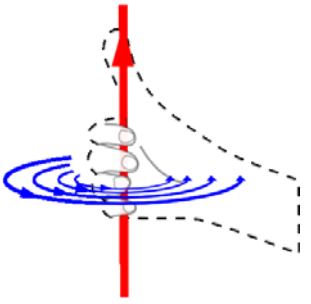
$$\widehat{\mathbf{A}}^2 = \widehat{\mathbf{B}}^n = \mathbf{I}_3, \quad \widehat{\mathbf{B}}\widehat{\mathbf{A}} = \widehat{\mathbf{A}}\widehat{\mathbf{B}}^{-1}\ (= \widehat{\mathbf{A}}\widehat{\mathbf{B}}^{n-1}). \tag{3.20}$$

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

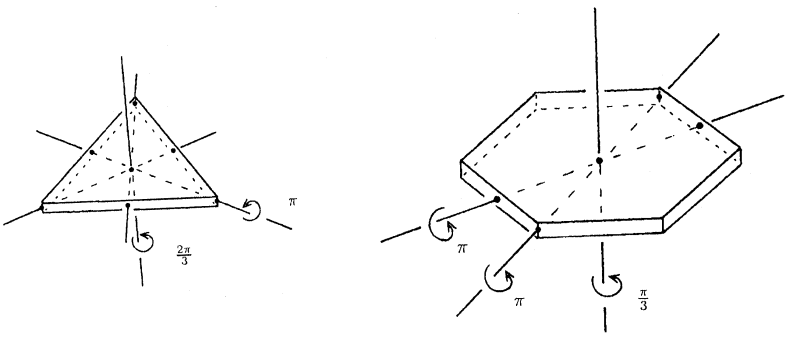
$$\mathbb{R}^3 \ni \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \widehat{\mathbf{A}}\,\widehat{\mathbf{B}}^k \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3, \quad k \in \{0,1,...,n-1\},$$

όπου

$$\widehat{\mathbf{A}}\,\widehat{\mathbf{B}}^k = \begin{pmatrix} \cos(\frac{2(n-k)\pi}{n}) & \sin(\frac{2(n-k)\pi}{n}) & 0 \\ \sin(\frac{2(n-k)\pi}{n}) & -\cos(\frac{2(n-k)\pi}{n}) & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

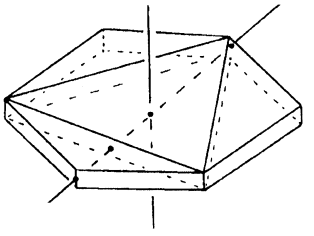
παριστούν *στροφές* τού $\mathbb{R}^3$ κατά π ακτίνια περί τις ευθείες, ως προς τις οποίες εκτελούνται οι n κατοπτρισμοί τού P_n (και τις οποίες έχουμε ήδη περιγράψει διεξοδικώς σε ό,τι προηγήθηκε). Στα κάτωθι σχήματα υποδηλούνται οι στροφές τού $\mathbb{R}^3$ οι επαγόμενες μέσω των πινάκων $\widehat{\mathbf{A}}, \widehat{\mathbf{B}}$ 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

$$\boxed{\mathbf{D}_n \cong \text{Συμμ}(P_n) \cong \text{Περ.Συμμ}(\widehat{P}_n).}$$

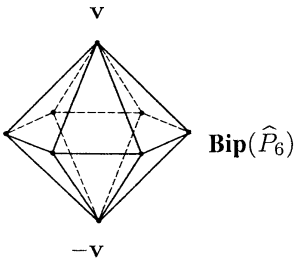
Τέλος, εάν κανείς επιθυμεί να αποκτήσει ένα «καθαρόαιμο» πολύεδρο, οι περιστροφικές συμμετρίες τού οποίου δομούν μια ομάδα ισόμορφη με την $\mathbf{D}_n$, αρκεί να θεωρήσει τη *διπλή πυραμίδα* $\textbf{Bip}(\widehat{P}_n)$ που σχηματίζεται ενώνοντας ένα σημείο $\mathbf{v} = (0,0,\lambda)$, $\lambda \in \mathbb{R}_{>0} \setminus \{1\}$, 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 $T_{-1} \circ S = S \circ {T_{-1}}^{-1}\ (= S \circ T_1)$.

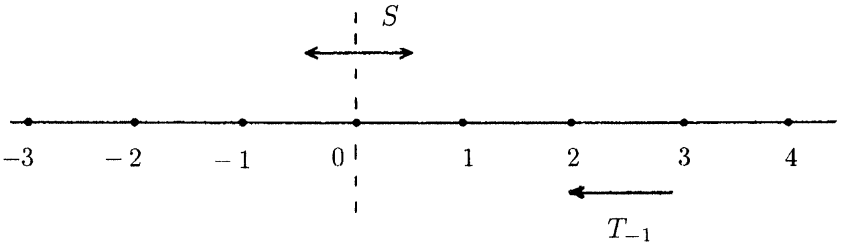
ΑΠΟΔΕΙΞΗ. Έστω τυχούσα ισομετρία $\sigma \in \mathbf{D}_\infty$. Προφανώς, $\sigma\,(0) =: k \in \mathbb{Z}$. Κατά την πρόταση 3.4.13, $\exists j \in \{0,1\} : \sigma = S^j \circ T_{-k}$, όπου

$$T_{-k} = \begin{cases} T_{-1}^k, & \text{όταν} \quad k \geq 0, \\ T_1^{-k}, & \text{όταν} \quad k < 0. \end{cases}$$

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

$$\left\{ \mathbf{I}_4, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right\}$$

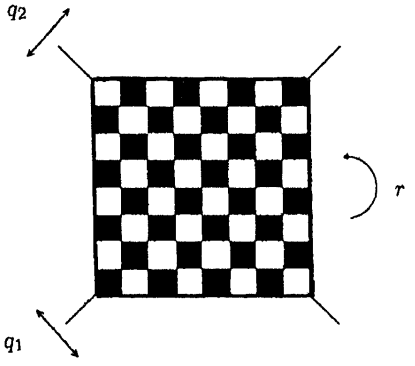
τής $\mathrm{GL}_4(\mathbb{Z})$ και με την υποομάδα

$$\left\{ \mathbf{I}_4, \begin{pmatrix} 0_F & 0_F & 0_F & 1_F \\ 1_F & 0_F & 0_F & 0_F \\ 0_F & 1_F & 0_F & 0_F \\ 0_F & 0_F & 1_F & 0_F \end{pmatrix}, \begin{pmatrix} 0_F & 0_F & 1_F & 0_F \\ 0_F & 0_F & 0_F & 1_F \\ 1_F & 0_F & 0_F & 0_F \\ 0_F & 1_F & 0_F & 0_F \end{pmatrix}, \begin{pmatrix} 0_F & 1_F & 0_F & 0_F \\ 0_F & 0_F & 1_F & 0_F \\ 0_F & 0_F & 0_F & 1_F \\ 1_F & 0_F & 0_F & 0_F \end{pmatrix} \right\}$$

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 $x_1 = a_1b_1$ και $x_2 = a_2b_2$. Επιπροσθέτως,

$$b_1a_2 \in KH = HK \Rightarrow \exists a_3 \in H \ \text{ και } \ \exists b_3 \in K : b_1a_2 = a_3b_3.$$

Κατά συνέπειαν,

$$\begin{aligned} x_1x_2 &= (a_1b_1)(a_2b_2) \underset{1.2.19}{=} a_1(b_1a_2)b_2 \\ &= a_1(a_3b_3)b_2 \underset{1.2.19}{=} \underbrace{(a_1a_3)}_{\in H}\underbrace{(b_3b_2)}_{\in K} \in HK. \end{aligned}$$

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) $f^{-1}(f(K) * L) = Kf^{-1}(L)$.

(ii) $f^{-1}(L * f(K)) = f^{-1}(L)K$.

(iii) $f^{-1}(f(K)) = K(\mathrm{Ker}(f)) = (\mathrm{Ker}(f))K$, *οπότε* $K(\mathrm{Ker}(f)) \sqsubseteq G$.

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)).

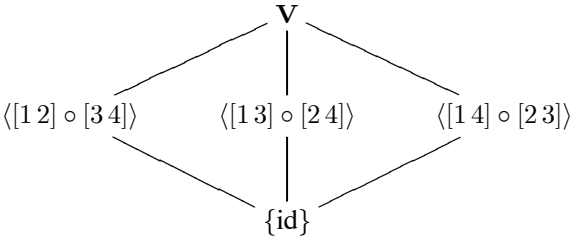
► **Εφαρμογές τού θεωρήματος τού Lagrange κατά τον προσδιορισμό υποομάδων.** Δοθείσας μιας πεπερασμένης ομάδας G *σχετικώς μικρής τάξεως* $m := |G|$, το θεώρημα 4.1.22 τού Lagrange περιορίζει την αναζήτηση των τάξεων των πιθανών υποομάδων τής G στους διαιρέτες τού m, διευκολύνοντάς μας, ως εκ τούτου, 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

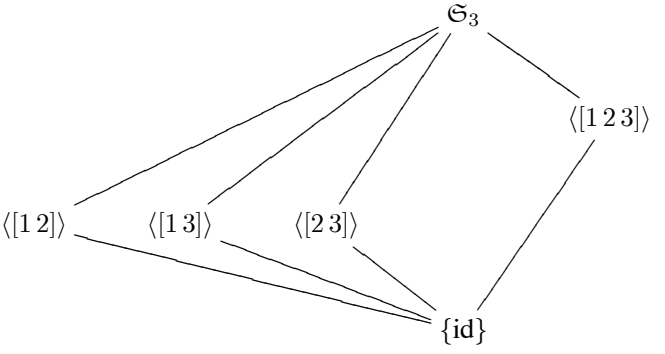
$$\mathrm{ord}([1\,2] \circ [3\,4]) = \mathrm{ord}([1\,3] \circ [2\,4]) = \mathrm{ord}([1\,4] \circ [2\,3]) = 2,$$

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

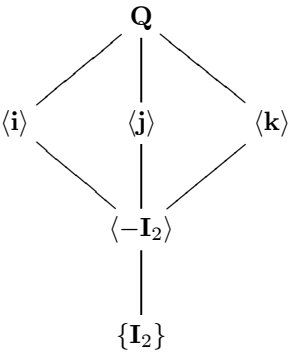
$$\mathrm{ord}([1\,2]) = \mathrm{ord}([1\,3]) = \mathrm{ord}([2\,3]) = 2,\ \mathrm{ord}([1\,2\,3]) = 3,$$

(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

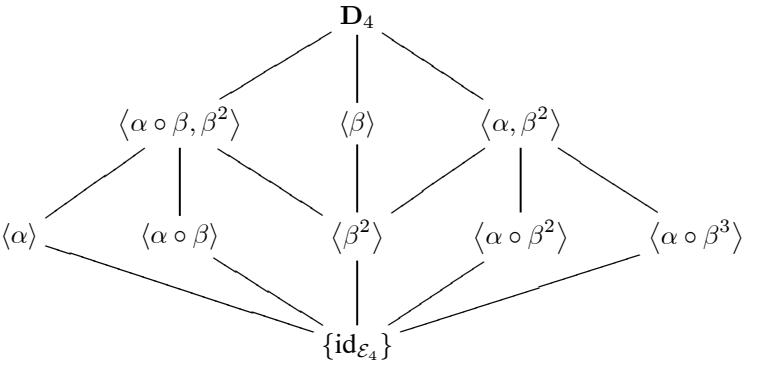
$$|H| = 4 \Rightarrow H \in \{\langle \mathbf{i} \rangle, \langle \mathbf{j} \rangle, \langle \mathbf{k} \rangle\},$$

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

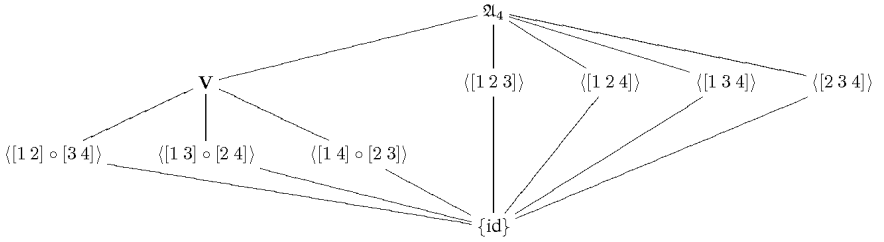
$$u_j\circ u_k\neq u_k\circ u_j \underset{f\text{ ένριψη}}{\Longrightarrow} f(u_j)\circ f(u_k)=f(u_j\circ u_k)\neq f(u_k\circ u_j)=f(u_k)\circ f(u_j),$$

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

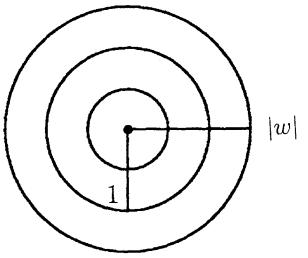
$$G/\{e_G\} \ni g\{e_G\} \longmapsto g \in G \quad \text{και} \quad G/G \ni gG \longmapsto e_G \in \{e_G\}$$

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. □

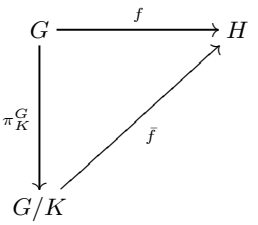
4.5 ΘΕΩΡΗΜΑΤΑ ΙΣΟΜΟΡΦΙΣΜΩΝ ΟΜΑΔΩΝ

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,

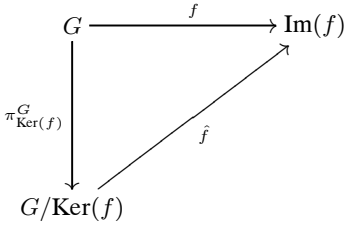
$$\begin{aligned}\mathrm{Ker}(f)/K &= \{gK \,|g \in \mathrm{Ker}(f)\} = \{gK \,|f(g) = e_H\} \\ &= \left\{gK \,\middle|\, \bar{f}(\pi_K^G(g)) = e_H\right\} = \left\{gK \,\middle|\, \bar{f}(gK) = e_H\right\} = \mathrm{Ker}(\bar{f}).\end{aligned}$$

(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

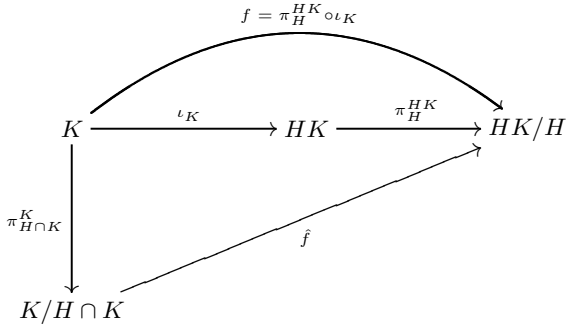
$$f(y) := \pi_H^{HK}(\iota_K(y)) = \pi_H^{HK}(y) = yH, \;\; \forall y \in K,$$

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). □

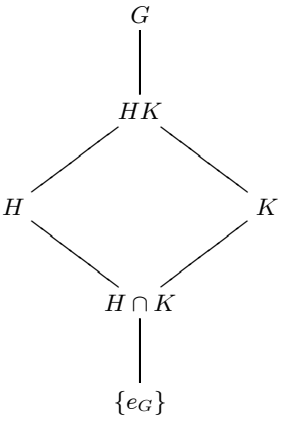
4.5.13 Δεύτερο Θεώρημα Ισομορφισμών. *Έστω ότι οι H, K είναι δυο υποομάδες μιας ομάδας $(G, \cdot)$ ικανοποιούσες τη συνθήκη $H \trianglelefteq \langle H, K\rangle$. Εάν $f := \pi_H^{HK} \circ \iota_K$ είναι η σύνθεση τής ενθέσεως $\iota_K : K \to HK$, $y \mapsto \iota_K(y) := y$ και τού φυσικού επιμορφισμού $\pi_H^{HK} : HK \to HK/H$, 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*

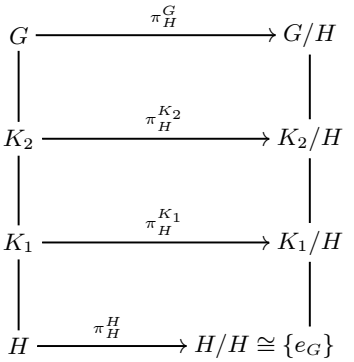
$$\mathbf{Subg}(G;H) \ni K \overset{\Psi_{\pi_H^G}}{\longmapsto} \pi_H^G(K) = \pi_H^K(K) = K/H \in \mathbf{Subg}(G/H) \tag{4.40}$$

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

$$\boxed{|G| = \sum_{j=1}^{k} \frac{|H|\ |K|}{\left|H \cap g_j K g_j^{-1}\right|}.}$$

ΚΕΦΑΛΑΙΟ 5

Συζυγία

Όπως έχουμε ήδη δει στο κεφάλαιο 4, μια από τις πιο θεμελιώδεις έννοιες τής Θεωρίας Ομάδων είναι αυτή τού *δείκτη* μιας υποομάδας H δοθείσας ομάδας $(G,\cdot)$. Ο ορισμός τού δείκτη $|G:H|$ στηρίζεται στον διαμελισμό τού υποκειμένου συνόλου G τής ομάδας αναφοράς σε πλευρικές κλάσεις. Ο διαμελισμός τού G υπαγορεύεται από τη σχέση ισοδυναμίας ${}_H\mathcal{R}$ (ή $\mathcal{R}_H$). Ένας επιπρόσθετος διαμελισμός τού G (σε *διπλές πλευρικές κλάσεις*) εδόθη στην άσκηση **4-70**. Ένας εξίσου σημαντικός διαμελισμός τού συνόλου G επιτυγχάνεται μέσω μιας *άλλης* σχέσεως ισοδυναμίας, τής λεγομένης *συζυγίας*. Π.χ., η H είναι ορθόθετη υποομάδα εάν και μόνον εάν μπορεί να γραφεί ως ένωση κάποιων κλάσεων συζυγίας (βλ. 5.1.15). Η συζυγία (η οποία μπορεί να ορισθεί καταλλήλως τόσον επί τού G όσον και επί τού συνόλου $\mathbf{Subg}(G)$ ή ακόμη και επί ολοκλήρου τού συνόλου $\mathfrak{P}(G)\setminus\{\varnothing\}$) διευκολύνει ποικιλοτρόπως τη μελέτη τής $(G,\cdot)$, ιδίως όταν αυτή είναι *μη αβελιανή*. Εξάλλου, ο υπολογισμός τού πληθικού αριθμού τής κλάσεως συζυγίας ενός στοιχείου $x\in G$ ανάγεται στον υπολογισμό τού δείκτη $|G:\mathrm{C}_G(x)|$ τού λεγομένου *κεντροποιητή* $\mathrm{C}_G(x)$ τού x (βλ. 5.2.10). Οι *κεντροποιητές* $\mathrm{C}_G(X)$ και οι *ορθοθέτες* $\mathrm{N}_G(X)$ οιωνδήποτε υποσυνόλων $\varnothing\neq X\subseteq G$, καθώς και το *κέντρο* $Z(G):=\mathrm{C}_G(G)$ και η *μεταθέτρια υποομάδα* G' τής $(G,\cdot)$ αποτελούν *ειδικές υποομάδες*, οι ιδιότητες των οποίων μας παρέχουν χρήσιμες πληροφορίες για την εσωτερική δόμηση τής ίδιας τής $(G,\cdot)$. (Συγκεκριμένα, η $\mathrm{C}_G(X)$ είναι η υποομάδα η απαρτιζόμενη από τα στοιχεία τής $(G,\cdot)$ που μετατίθενται αμοιβαίως με κάθε στοιχείο τού X, η $\mathrm{N}_G(X)$ είναι η μέγιστη υποομάδα τής $(G,\cdot)$ εντός τής οποίας το σύνολο X είναι ορθόθετο, το κέντρο $Z(G)$ αποτελεί το «αβελιανό μέρος» τής $(G,\cdot)$ και, τέλος, η μεταθέτρια υποομάδα G' είναι η ελάχιστη ορθόθετη υποομάδα τής $(G,\cdot)$, ούτως ώστε η αντίστοιχη πηλικοομάδα να είναι αβελιανή.)

Στο παρόν κεφάλαιο, εκτός τού ορισμού τής εννοίας τής συζυγίας και των κύριων ιδιοτήτων των προαναφερθεισών υποομάδων, περιέχονται και εφαρμογές τής σχετικής θεωρίας για συγκεκριμένες ομάδες, όπως π.χ. συμβαίνει με την παράθεση

των κλάσεων συζυγίας των διεδρικών ομάδων $\mathbf{D}_n$, την περιγραφή των κλάσεων συζυγίας των συμμετρικών και εναλλασσουσών ομάδων $\mathfrak{S}_n$ και $\mathfrak{A}_n$ (που δεσμεύει μια ολόκληρη ενότητα), την περιγραφή των κέντρων διαφόρων ομάδων πινάκων κ.ά. Επίσης, επισημαίνονται ορισμένα επακόλουθα τής *εξισώσεως κλάσεων συζυγίας*, δίδεται η απόδειξη τού *θεωρήματος τού Cauchy* και παρατίθενται αρκετά πορίσματα που προκύπτουν από αυτό.

5.1 Η ΕΝΝΟΙΑ ΤΗΣ ΣΥΖΥΓΙΑΣ

Έστω $(G,\cdot)$ μια ομάδα και έστω $H \sqsubseteq G$. Τότε $H \trianglelefteq G \Leftrightarrow gHg^{-1} = H$ *για κάθε* $g \in G$ (βλ. 4.2.1 και 4.2.2). Η γενικότερη θεώρηση υποσυνόλων τής μορφής

$$gXg^{-1} := \{g\}X\{g^{-1}\} := \left\{gxg^{-1}\,|x \in X\right\} \subseteq G$$

για *οιαδήποτε μη κενά υποσύνολα* $X \subseteq G$ και *για κάποιο* $g \in G$ μας υποδεικνύει τον τρόπο καθορισμού μιας διμελούς σχέσεως που είναι γνωστή ως *συζυγία*.

5.1.1 Ορισμός. Έστω $(G,\cdot)$ μια ομάδα. Ως

$$\mathcal{R}^G_{\text{συζ.}} \subseteq (\mathfrak{P}(G) \smallsetminus \{\varnothing\}) \times (\mathfrak{P}(G) \smallsetminus \{\varnothing\})$$

συμβολίζουμε τη διμελή σχέση επί τού $\mathfrak{P}(G) \smallsetminus \{\varnothing\}$ την οριζόμενη ως εξής:

$$\boxed{(X,Y) \in \mathcal{R}^G_{\text{συζ.}} \underset{\text{ορσ}}{\Longleftrightarrow} \exists g \in G : Y = gXg^{-1}.}$$

Όταν $(X,Y) \in \mathcal{R}^G_{\text{συζ.}}$, τότε λέμε ότι τα σύνολα X και Y είναι **συζυγή εντός τής** G.

5.1.2 Πρόταση. *Η* $\mathcal{R}^G_{\text{συζ.}}$ *αποτελεί μια σχέση ισοδυναμίας επί τού* $\mathfrak{P}(G) \smallsetminus \{\varnothing\}$.

ΑΠΟΔΕΙΞΗ. Η $\mathcal{R}^G_{\text{συζ.}}$ είναι *αυτοπαθής*, διότι $X = e_G X e_G^{-1}$ για κάθε $\varnothing \neq X \subseteq G$, *συμμετρική*, διότι για οιαδήποτε $\varnothing \neq X \subseteq G$ και $\varnothing \neq Y \subseteq G$ με $Y = gXg^{-1}$, για κάποιο $g \in G$, έχουμε

$$X = g^{-1}Yg = g^{-1}Y(g^{-1})^{-1},$$

και, τέλος, *μεταβατική*, διότι για μη κενά υποσύνολα $X_1, X_2, X_3 \subseteq G$ για τα οποία ισχύει $(X_1,X_2) \in \mathcal{R}^G_{\text{συζ.}}$ και $(X_2,X_3) \in \mathcal{R}^G_{\text{συζ.}}$,

$$\left.\begin{array}{l}\exists g_1 \in G : X_2 = g_1 X_1 g_1^{-1} \\ \exists g_2 \in G : X_3 = g_2 X_2 g_2^{-1}\end{array}\right\} \Longrightarrow X_3 = (g_2 g_1) X_1 (g_2 g_1)^{-1},$$

οπότε $(X_1,X_3) \in \mathcal{R}^G_{\text{συζ.}}$ □

5.1.3 Σημείωση. Είθισται (γενικεύοντας τον ορισμό 4.2.2) να καλούμε οιοδήποτε $\varnothing \neq X \subseteq G$ το οποίο πληροί τη συνθήκη

$$X = gXg^{-1},\ \forall g \in G,$$

ορθόθετο υποσύνολο τής G.

5.1.4 Ορισμός. Έστω $(G,\cdot)$ μια ομάδα. Ως

$$\mathcal{R}^G_{\sigma\upsilon\zeta.}\big|_{\mathbf{Subg}(G)\times\mathbf{Subg}(G)} := \mathcal{R}^G_{\sigma\upsilon\zeta.} \cap (\mathbf{Subg}(G)\times\mathbf{Subg}(G))$$

συμβολίζουμε τη σχέση ισοδυναμίας την επαγομένη επί τού συνόλου $\mathbf{Subg}(G)$ των υποομάδων τής G. Όταν

$$(H,K) \in \mathcal{R}^G_{\sigma\upsilon\zeta.}\big|_{\mathbf{Subg}(G)\times\mathbf{Subg}(G)} \ (\Leftrightarrow \exists g\in G : K = gHg^{-1}),$$

τότε λέμε ότι οι υποομάδες H και K είναι **συζυγείς εντός τής** G. (Υπενθυμίζεται ότι, σύμφωνα με το λήμμα 4.2.16, για οιαδήποτε $H\in\mathbf{Subg}(G)$ και οιοδήποτε $g\in G$ το σύνολο gHg^{-1} αποτελεί μια υποομάδα τής G και $\left|gHg^{-1}\right| = |H|$.) Η κλάση ισοδυναμίας μιας $H\in\mathbf{Subg}(G)$ ως προς την $\mathcal{R}^G_{\sigma\upsilon\zeta.}\Big|_{\mathbf{Subg}(G)\times\mathbf{Subg}(G)}$ καλείται **κλάση συζυγίας τής** H (εντός τής G) και συμβολίζεται ως εξής:

$$\boxed{\text{ΚΛΣ}_G(H) := \left\{K\in\mathbf{Subg}(G)\,\middle|\,(H,K)\in\mathcal{R}^G_{\sigma\upsilon\zeta.}\big|_{\mathbf{Subg}(G)\times\mathbf{Subg}(G)}\right\}.}$$

5.1.5 Ορισμός. Έστω $(G,\cdot)$ μια ομάδα και έστω

$$\mathcal{R}^G_{\sigma\upsilon\zeta.}\big|_{\mathbf{Mov}(G)\times\mathbf{Mov}(G)} := \mathcal{R}^G_{\sigma\upsilon\zeta.} \cap (\mathbf{Mov}(G)\times\mathbf{Mov}(G))$$

η σχέση ισοδυναμίας η επαγομένη επί τού συνόλου $\mathbf{Mov}(G)$ των *μονοσυνόλων* των ανηκόντων στο $\mathfrak{P}(G)$. Προφανώς, επί τού υποκειμένου συνόλου G τής ομάδας $(G,\cdot)$ ορίζεται μια σχέση ισοδυναμίας "$\underset{\sigma\upsilon\zeta.}{\overset{G}{\sim}}$" ως ακολούθως:

$$\boxed{x \underset{\sigma\upsilon\zeta.}{\overset{G}{\sim}} y \underset{\text{ορσ}}{\Longleftrightarrow} (\{x\},\{y\})\in\mathcal{R}^G_{\sigma\upsilon\zeta.}\big|_{\mathbf{Mov}(G)\times\mathbf{Mov}(G)} \ (\Leftrightarrow\exists g\in G : y = gxg^{-1}).}$$

Όταν $x \underset{\sigma\upsilon\zeta.}{\overset{G}{\sim}} y$, τότε λέμε ότι **τα στοιχεία** $x,y\in G$ είναι **συζυγή** (εντός τής G). (Επίσης, ενίοτε, όταν η ομάδα αναφοράς υπονοείται από τα συμφραζόμενα, απλουστεύουμε τον συμβολισμό γράφοντας "$\underset{\sigma\upsilon\zeta.}{\sim}$" αντί τού "$\underset{\sigma\upsilon\zeta.}{\overset{G}{\sim}}$".) Η κλάση ισοδυναμίας ενός στοιχείου $x\in G$ ως προς την "$\underset{\sigma\upsilon\zeta.}{\overset{G}{\sim}}$" καλείται **κλάση συζυγίας τού** x (εντός τής G) και συμβολίζεται ως εξής:

$$\boxed{\text{ΚΛΣ}_G(x) := \left\{y\in G\,\middle|\,y \underset{\sigma\upsilon\zeta.}{\overset{G}{\sim}} x\right\}.}$$

Όταν αναφερόμαστε (εν συντομία) στις **κλάσεις συζυγίας τής** $(G,\cdot)$, εννοούμε τα στοιχεία τού $G/\underset{\sigma\upsilon\zeta.}{\sim}$ και χρησιμοποιούμε τον συμβολισμό

$$\boxed{\mathfrak{K}(G) := \text{card}(G/\underset{\sigma\upsilon\zeta.}{\overset{G}{\sim}}).}$$

5.1.6 Πρόταση. *Δυο στοιχεία μιας ομάδας $(G,\cdot)$ που είναι συζυγή εντός αυτής έχουν την ίδια τάξη*[1].

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το (ii) τής προτάσεως 2.3.9. □

5.1.7 Παρατήρηση. Για *κάθε* ομάδα $(G,\cdot)$ η κλάση συζυγίας $\text{ΚΛΣ}_G(e_G)$ τού ουδετέρου στοιχείου της e_G είναι το μονοσύνολο $\{e_G\}$, διότι το μόνο στοιχείο τής G τάξεως 1 είναι το e_G.

5.1.8 Πρόταση. *Κάθε αυτομορφισμός $\vartheta \in \text{Aut}(G)$ μιας ομάδας $(G,\cdot)$ απεικονίζει κάθε κλάση συζυγίας της σε μια κλάση συζυγίας της.*

ΑΠΟΔΕΙΞΗ. Αρκεί να αποδειχθεί ότι για οιαδήποτε $x,y\in G$ ισχύει η αμφίπλευρη συνεπαγωγή $x \underset{\text{συζ.}}{\sim} y \iff \vartheta(x) \underset{\text{συζ.}}{\sim} \vartheta(y)$. Εάν $\exists g\in G : y = gxg^{-1}$, τότε

$$\vartheta(y) = \vartheta(gxg^{-1}) = \vartheta(g)\vartheta(x)\vartheta(g^{-1}) = \vartheta(g)\vartheta(x)\vartheta(g)^{-1}.$$

Και αντιστρόφως· εάν $\exists g\in G : \vartheta(y) = g\vartheta(x)g^{-1}$, τότε υπάρχει (μονοσημάντως ορισμένο) στοιχείο $h\in G : g = \vartheta(h)$, οπότε

$$\vartheta(y) = \vartheta(h)\vartheta(x)\vartheta(h)^{-1} = \vartheta(h)\vartheta(x)\vartheta(h^{-1}) = \vartheta(hxh^{-1}) \Rightarrow y = hxh^{-1}.$$

(Η τελευταία συνεπαγωγή είναι πρόδηλη λόγω τής ενριπτικότητας τού ϑ.) □

5.1.9 Σημείωση. Έστω $(G,\cdot)$ μια ομάδα. Προφανώς,

$$\text{ℜ}(G) = \text{card}(\Xi),\ \ G = \coprod_{x\in\Xi} \text{ΚΛΣ}_G(x),$$

όπου Ξ ένα πλήρες σύστημα εκπροσώπων τής G ως προς την "$\underset{\text{συζ.}}{\sim}$". Όταν η G είναι *πεπερασμένη* ομάδα τάξεως $|G| = n$, τότε για την περιγραφή τού $G/\underset{\text{συζ.}}{\sim}$ είθισται να εργαζόμαστε με ένα *συγκεκριμένο* πλήρες σύστημα εκπροσώπων τής G ως προς την "$\underset{\text{συζ.}}{\sim}$", ας πούμε το

$$\Xi = \{x_1, x_2, ..., x_\nu\} \ \text{με}\ \ \kappa_j := \text{card}(\text{ΚΛΣ}_G(x_j)),\ \forall j\in\{1,...,\nu\},$$

και να συντάσσουμε τον αντίστοιχο *κατάλογο εκπροσώπων των κλάσεων συζυγίας τής G*:

εκπρ.	x_1	x_2	$\cdots$	x_ν
τάξη	$\text{ord}(x_1)$	$\text{ord}(x_2)$	$\cdots$	$\text{ord}(x_\nu)$
♯	κ_1	κ_2	$\cdots$	κ_ν

όπου $\kappa_1+\kappa_2+\cdots+\kappa_\nu = n$.

[1] Το αντίστροφο δεν είναι εν γένει αληθές. Ενδέχεται να υπάρχουν μη συζυγή στοιχεία ιδίας τάξεως. Βλ., π.χ., παραδείγματα 5.2.12 και 5.1.10.

5.1.10 Πρόταση. (Κλάσεις συζυγίας διεδρικών ομάδων.) *Έστω $n \in \mathbb{N}, n \geq 3$, και έστω $\mathbf{D}_n = \langle \alpha, \beta \rangle$ η n-οστή διεδρική ομάδα η παραγόμενη (εντός τής $(\mathfrak{S}_{\mathcal{E}_n}, \circ)$) από τα στοιχεία*

$$\mathcal{E}_n \ni z \overset{\alpha}{\longmapsto} \overline{z} \in \mathcal{E}_n \ \textit{και} \ \ \mathcal{E}_n \ni z \overset{\beta}{\longmapsto} \zeta_n z \in \mathcal{E}_n$$

(βλ. 3.4.4). *Τότε ισχύουν τα ακόλουθα*:

(i) *Εάν ο n είναι περιττός, τότε η $\mathbf{D}_n$ διαθέτει $\frac{n-1}{2} + 2$ κλάσεις συζυγίας που είναι οι εξής*:

$$\{\mathrm{id}_{\mathcal{E}_n}\}, \{\beta, \beta^{n-1}\}, \{\beta^2, \beta^{n-2}\}, ..., \{\beta^{\frac{n-1}{2}}, \beta^{\frac{n+1}{2}}\}, \left\{\alpha \circ \beta^j \,|j \in \{0, 1, ..., n-1\}\right\},$$

ο δε κατάλογος εκπροσώπων των κλάσεων συζυγίας τής $\mathbf{D}_n$ που αντιστοιχίζεται στο σύστημα $\Xi_n := \{\mathrm{id}_{\mathcal{E}_n}, \beta, \beta^2, ..., \beta^{\frac{n-1}{2}}, \alpha\}$ είναι ο

εκπρ.	$\mathrm{id}_{\mathcal{E}_n}$	β	β^2	$\cdots$	β^j	$\cdots$	$\beta^{\frac{n-1}{2}}$	α
τάξη	1	n	n	$\cdots$	$\frac{n}{\mu\kappa\delta(j,n)}$	$\cdots$	n	2
♯	1	2	2	$\cdots$	2	$\cdots$	2	n

(ii) *Εάν ο n είναι άρτιος, τότε η $\mathbf{D}_n$ διαθέτει $\frac{n}{2} + 3$ κλάσεις συζυγίας που είναι οι εξής*:

$$\{\mathrm{id}_{\mathcal{E}_n}\}, \{\beta, \beta^{n-1}\}, \{\beta^2, \beta^{n-2}\}, ..., \{\beta^{\frac{n}{2}-1}, \beta^{\frac{n}{2}+1}\}, \{\beta^{\frac{n}{2}}\},$$
$$\left\{\alpha \circ \beta^{2j} \,\middle|\, j \in \{0, 1, ..., \tfrac{n}{2} - 1\}\right\}, \left\{\alpha \circ \beta^{2j+1} \,\middle|\, j \in \{0, 1, ..., \tfrac{n}{2} - 1\}\right\},$$

ο δε κατάλογος εκπροσώπων των κλάσεων συζυγίας τής $\mathbf{D}_n$ που αντιστοιχίζεται στο σύστημα $\Xi_n := \{\mathrm{id}_{\mathcal{E}_n}, \beta, \beta^2, ..., \beta^{\frac{n}{2}-1}, \beta^{\frac{n}{2}}, \alpha, \alpha \circ \beta\}$ είναι ο

εκπρ.	$\mathrm{id}_{\mathcal{E}_n}$	β	β^2	$\cdots$	β^j	$\cdots$	$\beta^{\frac{n}{2}-1}$	$\beta^{\frac{n}{2}}$	α	$\alpha \circ \beta$
τάξη	1	n	$\frac{n}{2}$	$\cdots$	$\frac{n}{\mu\kappa\delta(j,n)}$	$\cdots$	$\frac{n}{\mu\kappa\delta(2,\frac{n}{2}-1)}$	2	2	2
♯	1	2	2	$\cdots$	2	$\cdots$	2	1	$\frac{n}{2}$	$\frac{n}{2}$

ΑΠΟΔΕΙΞΗ. Κάθε στροφή β^j είναι συζυγής προς την αντίστροφό της β^{-j}, διότι[2]

$$\beta^j = \alpha \circ \beta^{-j} \circ \alpha^{-1}, \ \forall j \in \mathbb{Z}.$$

Μάλιστα, μέσω των ισοτήτων

$$\beta^i \circ \beta^j \circ \beta^{-i} = \beta^j, \ \ \left(\alpha \circ \beta^i\right) \circ \beta^j \circ \left(\alpha \circ \beta^i\right)^{-1} = \beta^{-j}, \ \forall (i, j) \in \mathbb{Z} \times \mathbb{Z},$$

[2] Αυτού τού είδους οι ισότητες αποδεικνύονται με τη βοήθεια τής μαθηματικής επαγωγής, εκκινώντας από τις σχέσεις (3.16) στις οποίες υπόκεινται οι γεννήτορες. Πρβλ. με την απόδειξη τής προτάσεως 3.4.7.

διαπιστώνουμε ότι τα μόνα στοιχεία τής $\mathbf{D}_n$ που είναι συζυγή προς τη στροφή β^j (για οιονδήποτε παγιωμένον $j \in \{0, 1, ..., n-1\}$) είναι τα β^j και $\beta^{-j} = \beta^{n-j}$. Για τον προσδιορισμό τής κλάσεως συζυγίας τού κατοπτρισμού α χρησιμοποιούμε τις ισότητες

$$\beta^i \circ \alpha \circ \beta^{-i} = \alpha \circ \beta^{2i}, \ \ \left(\alpha \circ \beta^i\right) \circ \alpha \circ \left(\alpha \circ \beta^i\right)^{-1} = \alpha \circ \beta^{2i}, \ \forall i \in \mathbb{Z}.$$

Καθώς το i διατρέχει όλους τους ακεραίους, το $\alpha \circ \beta^{2i}$ ταυτίζεται με κάθε δυνατό κατοπτρισμό στον οποίο το β εμφανίζεται υψωμένο σε μια δύναμη διαιρούμενη διά τού 2. Εάν ο n είναι *περιττός*, τότε κάθε ακέραιος mod n είναι ένα πολλαπλάσιο τού 2. (Επειδή το 2 είναι αντιστρέψιμο mod n, δοθέντος ενός $\kappa \in \mathbb{Z}$ μπορούμε να επιλύσουμε την ισοτιμία $\kappa \equiv 2x (\mathrm{mod}\, n)$.) Επομένως,

$$\left\{\alpha \circ \beta^{2i} \,|i \in \mathbb{Z}\right\} = \left\{\alpha \circ \beta^i \,|i \in \mathbb{Z}\right\},$$

και καθένας εκ των n κατοπτρισμών των ανηκόντων στην $\mathbf{D}_n$ είναι συζυγής προς τον κατοπτρισμό α. Επίσης, λόγω τού πορίσματος 2.3.11,

$$\mathrm{ord}(\beta^j) = \left|\left\langle \beta^j \right\rangle\right| = \frac{n}{\mu\kappa\delta(j,n)}, \ \forall j \in \{0, 1, ..., \tfrac{n-1}{2}\}.$$

Από την άλλη μεριά, εάν ο n είναι *άρτιος*, τότε μόνον οι μισοί από τους διαθέσιμους κατοπτρισμούς είναι συζυγείς προς τον α. Οι άλλοι μισοί κατοπτρισμοί είναι συζυγείς προς τον $\alpha \circ \beta$, καθόσον

$$\beta^i \circ (\alpha \circ \beta) \circ \beta^{-i} = \alpha \circ \beta^{2i+1}, \ \ \left(\alpha \circ \beta^i\right) \circ (\alpha \circ \beta) \circ \left(\alpha \circ \beta^i\right)^{-1} = \alpha \circ \beta^{2i-1}, \ \forall i \in \mathbb{Z}.$$

Αυτοί συνιστούν το σύνολο $\left\{\alpha \circ \beta^{2j+1} \,\middle|\, j \in \{0, 1, ..., \tfrac{n}{2} - 1\}\right\}$. Λόγω τού πορίσματος 2.3.11,

$$\mathrm{ord}(\beta^j) = \left|\left\langle \beta^j \right\rangle\right| = \frac{n}{\mu\kappa\delta(j,n)}, \ \forall j \in \{0, 1, ..., \tfrac{n}{2}\}.$$

Τέλος, $\mathrm{ord}(\alpha \circ \beta) = 2$, διότι $(\alpha \circ \beta)^2 = \left(\alpha \circ \beta \circ \alpha^{-1}\right) \circ \beta = \beta^{-1} \circ \beta = \mathrm{id}_{\mathcal{E}_n}$. □

5.1.11 Σημείωση. Αξίζει, στο σημείο αυτό, να επισημανθεί ότι η σχέση τής συζυγίας είναι εξίσου σημαντική και για τη μελέτη *άπειρων* ομάδων. Ας θεωρήσουμε, επί παραδείγματι, τη γενική γραμμική ομάδα $\mathbf{GL}_n(\mathbb{C})$ υπεράνω τού $\mathbb{C}$. Δοθέντος ενός $\mathbf{A} \in \mathbf{GL}_n(\mathbb{C})$, είναι δυνατόν να περιγραφεί κάποιος «χαρακτηριστικός» εκπρόσωπος τής κλάσεως συζυγίας $\mathrm{ΚΛΣ}_{\mathbf{GL}_n(\mathbb{C})}(\mathbf{A})$; Η απάντηση αυτού τού ερωτήματος είναι γνωστή από το μάθημα τής Γραμμικής Άλγεβρας. Αρκεί η υπόμνηση τού ότι το να είναι δυο στοιχεία $\mathbf{A}$ και $\mathbf{B}$ τής $\mathbf{GL}_n(\mathbb{C})$ *συζυγή* ισοδυναμεί με την *ομοιότητα* των πινάκων $\mathbf{A}$ και $\mathbf{B}$. (Εν προκειμένω, *συζυγία* και *ομοιότητα* συμπίπτουν!) Επομένως,

$$\mathbf{A} \overset{\substack{\mathbf{GL}_n(\mathbb{C}) \\ \sim \\ \text{συζ.}}}{} \begin{pmatrix} \mathbf{M}_1 & & & \\ & \mathbf{M}_2 & & \mathbf{0} \\ & & \ddots & \\ \mathbf{0} & & & \mathbf{M}_n \end{pmatrix} \tag{5.1}$$

όπου για κάθε $j \in \{1, ..., n\}$ ο πίνακας

$$\mathbf{M}_j = \begin{pmatrix} z_j & 1 & 0 & 0 & \cdots & 0 \\ 0 & z_j & 1 & & \cdots & 0 \\ 0 & 0 & z_j & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & z_j & 1 \\ 0 & 0 & 0 & \cdots & 0 & z_j \end{pmatrix} \tag{5.2}$$

περιέχει μια ιδιοτιμή z_j τού $\mathbb{C}^n \ni \mathbf{z} \longmapsto \mathbf{Az} \in \mathbb{C}^n$ ως εγγραφή του σε κάθε διαγώνια θέση. Πρόκειται λοιπόν για τη «μέχρις συζυγίας» γραφή τού $\mathbf{A}$ υπό τη μορφή ενός *πίνακα τού Jordan*. Ο εν λόγω πίνακας (5.1) καθορίζεται μονοσημάντως από τον $\mathbf{A}$, με εξαίρεση κάποια πιθανή μετάταξη των *στοιχειωδών πινάκων τού Jordan* (5.2), ο δε προσδιορισμός του είναι προϊόν μιας απολύτως αυτοματοποιημένης αλγοριθμικής[3] διαδικασίας.

5.1.12 Σημείωση. Θα πρέπει να γίνεται πάντοτε σαφής διάκριση μεταξύ των εννοιών *συζυγία στοιχείων* και *συζυγία υποομάδων* δοθείσας ομάδας. Επί παραδείγματι, η πρόταση 5.1.10 μας πληροφορεί ότι η διεδρική ομάδα $\mathbf{D}_4$ διαθέτει 5 κλάσεις συζυγίας (ήτοι 5 κλάσεις ισοδυναμίας ως προς την "$\underset{\text{συζ.}}{\sim}$" υπό την έννοια τού ορισμού 5.1.5) που είναι οι εξής:

$$\{\mathrm{id}_{\mathcal{E}_4}\},\ \{\beta, \beta^3\},\ \{\beta^2\},\ \left\{\alpha, \alpha \circ \beta^2\right\},\ \left\{\alpha \circ \beta, \alpha \circ \beta^3\right\}.$$

Από την άλλη μεριά, σύμφωνα με τους υπολογισμούς τού εδαφίου 4.1.44,

$$\mathbf{Subg}(\mathbf{D}_4) = \left\{ \begin{array}{c} \{\mathrm{id}_{\mathcal{E}_4}\}, \langle\alpha\rangle, \langle\beta\rangle, \left\langle\beta^2\right\rangle, \langle\alpha \circ \beta\rangle, \left\langle\alpha \circ \beta^2\right\rangle, \\ \left\langle\alpha \circ \beta^3\right\rangle,\ \left\langle\alpha, \beta^2\right\rangle,\ \left\langle\alpha \circ \beta, \beta^2\right\rangle,\ \mathbf{D}_4 \end{array} \right\}. \tag{5.3}$$

Εν προκειμένω, το σύνολο $\mathbf{Subg}(\mathbf{D}_4)$ (έχον ως στοιχεία του τις 10 υποομάδες τής $\mathbf{D}_4$) διαμελίζεται σε 8 κλάσεις ισοδυναμίας ως προς την[4] $\mathcal{R}^{\mathbf{D}_4}_{\text{συζ.}}\Big|_{\mathbf{Subg}(\mathbf{D}_4)\times\mathbf{Subg}(\mathbf{D}_4)}$ (βλ. 5.1.5) που είναι οι εξής[5]:

$$\{\{\mathrm{id}_{\mathcal{E}_4}\}\},\ \{\langle\beta\rangle\},\ \left\{\langle\alpha\rangle, \left\langle\beta^2\right\rangle\right\},\ \left\{\left\langle\alpha \circ \beta^2\right\rangle\right\},$$

$$\left\{\langle\alpha \circ \beta\rangle, \left\langle\alpha \circ \beta^3\right\rangle\right\},\ \left\{\left\langle\alpha, \beta^2\right\rangle\right\},\ \left\{\left\langle\alpha \circ \beta, \beta^2\right\rangle\right\},\ \{\mathbf{D}_4\}.$$

[3] Είναι π.χ. αρκετό (για συγκεκριμένα παραδείγματα) να γίνει χρήση τής εντολής *Jordan form* τού «πακέτου» *linear algebra* τού προγράμματος Maple.

[4] Ορισμένοι συγγραφείς χρησιμοποιούν τους όρους *κλάσεις συζυγίας στοιχείων* και *κλάσεις συζυγίας υποομάδων*, αντιστοίχως, για σαφέστερη διάκριση. Ωστόσο εδώ, για την αποφυγή μακρόσυρτων εκφράσεων, ο «σκέτος» όρος *κλάση συζυγίας* θα σημαίνει πάντοτε *κλάση ισοδυναμίας ως προς την* "$\underset{\text{συζ.}}{\sim}$". Από την άλλη μεριά, αναφέροντας ότι οι $H_1, H_2 \sqsubseteq G$ είναι *συζυγείς*, θα εννοούμε τη συζυγία υποομάδων υπό την έννοια τού 5.1.5.

[5] Γενικότερα, αποδεικνύεται ότι για κάθε $n \in \mathbb{N}$, $n \geq 3$, ο αριθμός των κλάσεων ισοδυναμίας στις οποίες διαμελίζεται το $\mathbf{Subg}(\mathbf{D}_n)$ ως προς τη σχέση συζυγίας υποομάδων ισούται με

$$\mathrm{card}(\mathbf{Subg}(\mathbf{D}_n)/\ \mathcal{R}^{\mathbf{D}_n}_{\text{συζ.}}\Big|_{\mathbf{Subg}(\mathbf{D}_n)\times\mathbf{Subg}(\mathbf{D}_n)}) = 3\mathrm{card}(\mathfrak{D}_n) - \ \mathrm{card}(\mathfrak{D}_m),$$

(βλ. B.2.34, B.3.15 (i)), όπου $m := \max\{\, d \in \mathfrak{D}_n \,|\, d \equiv 1 (\mathrm{mod}\, 2)\}$. Ιδιαιτέρως, για $n = 4$ έχουμε $m = 1$, οπότε αυτός ο αριθμός είναι ίσος με $3 \cdot 3 - 1 = 8$.

5.1.13 Παρατήρηση. Αξιοσημείωτη είναι η συνεπαγωγή

$$(H,K) \in \mathcal{R}^{G}_{\text{συζ.}}\big|_{\mathbf{Subg}(G)\times\mathbf{Subg}(G)} \Rightarrow H \cong K,$$

δηλαδή το ότι *δυο συζυγείς υποομάδες* H, K μιας ομάδας G *είναι πάντοτε ισόμορφες*, καθόσον $\exists g \in G : K = gHg^{-1}$ και η απεικόνιση

$$H \longrightarrow gHg^{-1},\ h \longmapsto ghg^{-1},$$

αποτελεί ισομορφισμό ομάδων. Εντούτοις, το αντίστροφο δεν είναι πάντοτε αληθές. Επί παραδείγματι, το σύνολο (5.3) των 10 υποομάδων τής $\mathbf{D}_4$ διαμελίζεται σε 5 κλάσεις ισομορφίας:

$$\{\mathrm{id}_{\mathcal{E}_4}\},\ \langle\alpha\rangle \cong \langle\alpha\circ\beta\rangle \cong \left\langle\beta^2\right\rangle \cong \left\langle\alpha\circ\beta^2\right\rangle \cong \left\langle\alpha\circ\beta^3\right\rangle \cong \mathbb{Z}_2,$$
$$\langle\beta\rangle \cong \mathbb{Z}_4,\ \left\langle\alpha,\beta^2\right\rangle \cong \left\langle\alpha\circ\beta,\beta^2\right\rangle \cong \mathbf{V},\ \mathbf{D}_4$$

και σε 8 κλάσεις ισοδυναμίας ως προς την $\mathcal{R}^{\mathbf{D}_4}_{\text{συζ.}}\Big|_{\mathbf{Subg}(\mathbf{D}_4)\times\mathbf{Subg}(\mathbf{D}_4)}$ (βλ. 4.1.44 και 5.1.12). Π.χ.,

$$\langle\alpha\rangle \cong \langle\alpha\circ\beta\rangle \text{ αλλά } (\langle\alpha\rangle, \langle\alpha\circ\beta\rangle) \notin \mathcal{R}^{\mathbf{D}_4}_{\text{συζ.}}\Big|_{\mathbf{Subg}(\mathbf{D}_4)\times\mathbf{Subg}(\mathbf{D}_4)}.$$

Ως εκ τούτου, *η σχέση ισομορφίας* $\cong|_{\mathbf{Subg}(G)\times\mathbf{Subg}(G)}$ *είναι αδρότερη τής σχέσεως συζυγίας υποομάδων* $\mathcal{R}^{G}_{\text{συζ.}}\Big|_{\mathbf{Subg}(G)\times\mathbf{Subg}(G)}$ επί τού $\mathbf{Subg}(G)$. (Πρβλ. Α.1.3.)

5.1.14 Πρόταση. *Έστω* $(G,\cdot)$ *μια ομάδα και έστω* $\varnothing \neq X \subseteq G$. *Τότε τα ακόλουθα είναι ισοδύναμα*:

(i) *Το* X *είναι ένα ορθόθετο υποσύνολο τής* G (*υπό την έννοια τού ορισμού* 5.1.3).

(ii) *Το* X *είναι η ένωση κάποιων κλάσεων συζυγίας τής* G (*ήτοι κάποιων κλάσεων ισοδυναμίας ως προς την* "$\overset{G}{\underset{\text{συζ}}{\sim}}$").

(iii) $gXg^{-1} \subseteq X, \forall g \in G$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν $x \in X$, τότε $gxg^{-1} \in X$ για κάθε $g \in G$, οπότε έχουμε $\text{ΚΛΣ}_G(x) \subseteq X$, πράγμα που σημαίνει ότι

$$X = \bigcup_{x\in X} \text{ΚΛΣ}_G(x).$$

(ii)⇒(iii) Επειδή το X είναι η ένωση κάποιων κλάσεων συζυγίας τής G, θα περιέχει μαζί με κάθε στοιχείο του και όλα τα συζυγή του, οπότε $gXg^{-1} \subseteq X, \forall g \in G$.

(iii)⇒(i) Επειδή $gXg^{-1} \subseteq X$ *για κάθε* $g \in G$, έχουμε

$$g^{-1}Xg = g^{-1}X(g^{-1})^{-1} \subseteq X \Longrightarrow X \subseteq gXg^{-1},$$

οπότε $gXg^{-1} = X$ *για κάθε* $g \in G$ και το X είναι, ως εκ τούτου, ορθόθετο υποσύνολο τής G. □

5.1.15 Πόρισμα. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \sqsubseteq G$. Τότε τα ακόλουθα είναι ισοδύναμα*:

(i) $H \trianglelefteq G$.

(ii) *Η υποομάδα H είναι η ένωση κάποιων κλάσεων συζυγίας τής G (ήτοι κάποιων κλάσεων ισοδυναμίας ως προς την "$\overset{G}{\underset{\text{συζ.}}{\sim}}$").*

5.1.16 Πόρισμα. *Έστω $(G,\cdot)$ μια πεπερασμένη ομάδα. Εάν $H \trianglelefteq G$, τότε για οιοδήποτε πλήρες σύστημα εκπροσώπων $\Xi = \{x_1 = e_G, x_2,...,x_\nu\}$ τής G ως προς την "$\underset{\text{συζ.}}{\sim}$" με $\kappa_j := \text{card}(\text{ΚΛΣ}_G(x_j))$, $\forall j \in \{1,...,\nu\}$, υπάρχουν $\lambda_j \in \{0,1\}$, $j \in \{1,...,\nu-1\}$, τέτοιοι ώστε να ισχύει*

$$1 + \sum_{j=1}^{\nu-1} \kappa_{j+1}\lambda_j = |H|\,. \tag{5.4}$$

ΑΠΟΔΕΙΞΗ. Υποθέτουμε ότι $H \trianglelefteq G$. Σύμφωνα με το πόρισμα 5.1.15 η H είναι η ένωση κάποιων κλάσεων συζυγίας τής G. Εάν λοιπόν θεωρήσουμε ένα πλήρες σύστημα εκπροσώπων $\Xi = \{x_1 = e_G, x_2,...,x_\nu\}$ τής G ως προς τη σχέση "$\underset{\text{συζ.}}{\sim}$" με $\kappa_j := \text{card}(\text{ΚΛΣ}_G(x_j))$, $\forall j \in \{1,...,\nu\}$, τότε $e_G = e_H \in H$, $\kappa_1 = 1$ (βλ. 5.1.7) και υπάρχει κάποιο υποσύνολο δεικτών $\{i_1,...,i_\mu\} \subseteq \{2,...,\nu\}$, $\mu \in \{1,...,\nu-1\}$, τέτοιο ώστε να ισχύει

$$H = \{e_G\} \coprod \text{ΚΛΣ}_G(x_{i_1}) \coprod \cdots \coprod \text{ΚΛΣ}_G(x_{i_\mu}) \tag{5.5}$$

(διότι $\text{ΚΛΣ}_G(x_j) \cap \text{ΚΛΣ}_G(x_{j'}) = \varnothing$ για οιουσδήποτε $j, j' \in \{1,...,\nu\}$, $j \neq j'$). Θέτοντας

$$\lambda_j := \begin{cases} 1, & \text{όταν } j+1 \in \{i_1,...,i_\mu\}, \\ 0, & \text{όταν } j+1 \in \{2,...,\nu\} \setminus \{i_1,...,i_\mu\}, \end{cases}$$

η ισότητα (5.4) έπεται άμεσα από την (5.5). □

5.1.17 Παράδειγμα. Εάν $n \in \mathbb{N}$, $n \geq 3$, τότε η κυκλική υποομάδα $H := \langle \alpha \circ \beta \rangle$ τής $\mathbf{D}_n := \langle \alpha, \beta \rangle$ τάξεως 2 *δεν είναι* ορθόθετη. Πράγματι· εάν ίσχυε $H \trianglelefteq \mathbf{D}_n$, τότε για το πλήρες σύστημα εκπροσώπων

$$\Xi_n := \begin{cases} \{\text{id}_{\mathcal{E}_n}, \beta, \beta^2,..., \beta^{\frac{n-1}{2}}, \alpha\}, & \text{όταν ο } n \text{ είναι περιττός}, \\ \{\text{id}_{\mathcal{E}_n}, \beta, \beta^2,..., \beta^{\frac{n}{2}-1}, \beta^{\frac{n}{2}}, \alpha, \alpha\circ\beta\}, & \text{όταν ο } n \text{ είναι άρτιος}, \end{cases}$$

(τής $\mathbf{D}_n$ ως προς την "$\underset{\text{συζ.}}{\sim}$") με $\text{card}(\text{ΚΛΣ}_{\mathbf{D}_n}(\text{id}_{\mathcal{E}_n})) = 1$ και

$$\text{card}(\text{ΚΛΣ}_{\mathbf{D}_n}(\beta^j)) = 2,\ \forall j \in \{1,...,\tfrac{n-1}{2}\},\ \text{card}(\text{ΚΛΣ}_{\mathbf{D}_n}(\alpha)) = n,$$

όταν ο n είναι περιττός και, αντιστοίχως,

$$\left\{ \begin{array}{l} \text{card}(\text{ΚΛΣ}_{\mathbf{D}_n}(\beta^j)) = 2,\ \forall j \in \{1,...,\frac{n}{2}-1\}, \\ \text{card}(\text{ΚΛΣ}_{\mathbf{D}_n}(\beta^{\frac{n}{2}})) = 1, \\ \text{card}(\text{ΚΛΣ}_{\mathbf{D}_n}(\alpha)) = \text{card}(\text{ΚΛΣ}_{\mathbf{D}_n}(\alpha\circ\beta)) = \frac{n}{2} \end{array} \right\},$$

όταν ο n είναι άρτιος (βλ. 5.1.10), θα έπρεπε (σύμφωνα με το πόρισμα 5.1.16) να υπάρχουν $\lambda_1, \lambda_2,..., \lambda_{\frac{n-1}{2}+1} \in \{0,1\}$, τέτοιοι ώστε να ισχύει η ισότητα

$$\begin{aligned} &1 + 2 \cdot \lambda_1 + \cdots + 2 \cdot \lambda_{\frac{n-1}{2}} + n \cdot \lambda_{\frac{n-1}{2}+1} = 2 \\ &\Rightarrow 2(\lambda_1 + \cdots \lambda_{\frac{n-1}{2}}) + n \cdot \lambda_{\frac{n-1}{2}+1} = 1 \end{aligned} \tag{5.6}$$

όταν ο n είναι περιττός και, αντιστοίχως, να υπάρχουν $\lambda_1, \lambda_2,...\lambda_{\frac{n}{2}+2} \in \{0,1\}$, τέτοιοι ώστε να ισχύει η ισότητα

$$\begin{aligned} &1 + 2 \cdot \lambda_1 + \cdots + 2 \cdot \lambda_{\frac{n}{2}-1} + 1 \cdot \lambda_{\frac{n}{2}} + \tfrac{n}{2} \cdot \lambda_{\frac{n}{2}+1} + \tfrac{n}{2} \cdot \lambda_{\frac{n}{2}+2} = 2 \\ &\Rightarrow 2(\lambda_1 + \cdots + \lambda_{\frac{n}{2}-1}) + \lambda_{\frac{n}{2}} + \tfrac{n}{2}(\lambda_{\frac{n}{2}+1} + \lambda_{\frac{n}{2}+2}) = 1. \end{aligned} \tag{5.7}$$

όταν ο n είναι άρτιος. Είναι προφανές ότι η (5.6) δεν διαθέτει λύσεις (διότι $n > 2$ και το 1 είναι περιττός). Εάν η (5.7) διέθετε λύσεις, τότε θα έπρεπε να ικανοποιείται η συνθήκη

$$\lambda_1 = \cdots = \lambda_{\frac{n}{2}-1} = \lambda_{\frac{n}{2}+1} = \lambda_{\frac{n}{2}+2} = 0 \text{ και } \lambda_{\frac{n}{2}} = 1.$$

Όμως ούτε αυτή μπορεί να ικανοποιείται, καθότι

$$\{\mathrm{id}_{\mathcal{E}_n}\} \coprod \text{ΚΛΣ}_{\mathbf{D}_n}(\beta^{\frac{n}{2}}) = \{\mathrm{id}_{\mathcal{E}_n}, \beta^{\frac{n}{2}}\} \neq H.$$

Άρα *και* η (5.7) δεν διαθέτει λύσεις και, ως εκ τούτου, $H \not\trianglelefteq \mathbf{D}_n$.

5.2 ΚΕΝΤΡΟΠΟΙΗΤΕΣ ΚΑΙ ΟΡΘΟΘΕΤΕΣ

5.2.1 Ορισμός. Έστω $(G, \cdot)$ μια ομάδα και έστω $\varnothing \neq X \subseteq G$. Ως **κεντροποιητής τού** X (εντός τής G) ορίζεται το σύνολο

$$\boxed{\mathrm{C}_G(X) := \{g \in G \,|\, gx = xg, \forall x \in X\}}$$

όλων των στοιχείων τής G που μετατίθενται αμοιβαίως με κάθε στοιχείο τού X. Εάν $\varnothing \neq Y \subseteq G$ είναι τέτοιο, ώστε να ισχύει η εγκλειστική σχέση $Y \subseteq \mathrm{C}_G(X)$, τότε λέμε ότι **το** Y **κεντροποιεί το** X (εντός τής G).

5.2.2 Πρόταση. *Για μια ομάδα* $(G, \cdot)$ *ισχύουν τα εξής*:

(i) *Εάν* $\varnothing \neq X \subseteq G$, *τότε*[6] $\mathrm{C}_G(X) \sqsubseteq G$.

(ii) *Εάν* $H \sqsubseteq G$, *τότε* $H \sqsubseteq \mathrm{C}_G(H) \Longleftrightarrow$ *η* H *είναι αβελιανή υποομάδα.*

(iii) *Εάν* $H \trianglelefteq G$, *τότε* $\mathrm{C}_G(H) \trianglelefteq G$.

(iv) *Εάν* $\varnothing \neq X \subseteq H \sqsubseteq G$, *τότε* $\mathrm{C}_H(X) = H \cap \mathrm{C}_G(X)$.

(v) *Εάν* $K \sqsubseteq H \sqsubseteq G$, *τότε* $\mathrm{C}_G(H) \sqsubseteq \mathrm{C}_G(K)$.

[6] Επειδή $\mathrm{C}_G(X) \sqsubseteq G$, ο κεντροποιητής $\mathrm{C}_G(X)$ τού X καλείται ενίοτε και **κεντροποιούσα υποομάδα τού** X.

ΑΠΟΔΕΙΞΗ. (i) Προφανώς, $e_G \in \mathrm{C}_G(X)$. Επίσης, για οιαδήποτε $g_1, g_2 \in \mathrm{C}_G(X)$,

$$g_1 x = x g_1, \forall x \in X \ \text{ και } \ g_2 x = x g_2, \forall x \in X,$$

οπότε

$$[(g_1 g_2)\, x = g_1(g_2 x) = (g_1 x) g_2 = (x g_1) g_2 = x(g_1 g_2),\ \forall x \in X] \Rightarrow g_1 g_2 \in \mathrm{C}_G(X)$$

και για οιοδήποτε $g \in \mathrm{C}_G(X)$, $gx = xg, \forall x \in X$, οπότε

$$[g^{-1}(xg)g^{-1} = g^{-1}(gx)g^{-1} \Rightarrow g^{-1}x = xg^{-1}, \forall x \in X] \Rightarrow g^{-1} \in \mathrm{C}_G(X).$$

Δυνάμει τού 2.1.16 (ii) συνάγεται ότι $\mathrm{C}_G(X) \sqsubseteq G$.
(ii) Έστω ότι $H \sqsubseteq G$. Εάν $H \sqsubseteq \mathrm{C}_G(H)$, τότε $hh' = h'h, \forall (h, h') \in H \times H$, οπότε η H είναι αβελιανή. Το αντίστροφο αποδεικνύεται παρομοίως.
(iii) Για τυχόντα $g_1 \in G$, $g_2 \in \mathrm{C}_G(H)$ και $h \in H$,

$$\left(g_1 g_2 g_1^{-1}\right) h \left(g_1 g_2 g_1^{-1}\right)^{-1} = g_1 (g_2 \left(g_1^{-1} h g_1\right) g_2^{-1}) g_1^{-1},$$

κι επειδή $H \trianglelefteq G \Rightarrow g_1^{-1} h g_1 = g_1^{-1} h (g_1^{-1})^{-1} \in H$ και $g_2 \in \mathrm{C}_G(H)$, λαμβάνουμε

$$\begin{aligned} g_2 \left(g_1^{-1} h g_1\right) &= \left(g_1^{-1} h g_1\right) g_2 \Rightarrow g_2 \left(g_1^{-1} h g_1\right) g_2^{-1} = g_1^{-1} h g_1 \\ &\Rightarrow \left(g_1 g_2 g_1^{-1}\right) h \left(g_1 g_2 g_1^{-1}\right)^{-1} = g_1 \left(g_1^{-1} h g_1\right) g_1^{-1} = h \end{aligned}$$

και

$$\left(g_1 g_2 g_1^{-1}\right) h \left(g_1 g_2 g_1^{-1}\right)^{-1} = h \Rightarrow \left(g_1 g_2 g_1^{-1}\right) h = h \left(g_1 g_2 g_1^{-1}\right),$$

ήτοι $g_1 g_2 g_1^{-1} \in \mathrm{C}_G(H)$, απ' όπου έπεται ότι $g_1 \mathrm{C}_G(H) g_1^{-1} \subseteq \mathrm{C}_G(X) \Rightarrow \mathrm{C}_G(H) \trianglelefteq G$.
(iv) Προφανώς, $\mathrm{C}_H(X) \sqsubseteq H$ και $\mathrm{C}_H(X) \sqsubseteq \mathrm{C}_G(X) \Rightarrow \mathrm{C}_H(X) \sqsubseteq H \cap \mathrm{C}_G(X)$. Και αντιστρόφως· εάν $h \in H \cap \mathrm{C}_G(X)$, τότε $hx = xh$ για κάθε $x \in X$, οπότε $h \in \mathrm{C}_H(X)$ και ισχύει και ο αντίστροφος εγκλεισμός $H \cap \mathrm{C}_G(X) \sqsubseteq \mathrm{C}_H(X)$.
(v) Εάν $K \sqsubseteq H \sqsubseteq G$ και $y \in \mathrm{C}_G(H)$, τότε

$$[yh = hy,\ \forall h \in H] \Longrightarrow [yx = xy,\ \forall x \in K] \Longrightarrow y \in \mathrm{C}_G(K),$$

οπότε $\mathrm{C}_G(H) \subseteq \mathrm{C}_G(K)$ και $\mathrm{C}_G(K) \sqsubseteq G \underset{2.1.20}{\Longrightarrow} \mathrm{C}_G(H) \sqsubseteq \mathrm{C}_G(K)$. □

5.2.3 Ορισμός. Έστω $(G, \cdot)$ μια ομάδα και έστω $\varnothing \neq X \subseteq G$. Ως **ορθοθέτης τού** X (εντός τής G) ορίζεται το σύνολο[7]

$$\boxed{\mathrm{N}_G(X) := \left\{ g \in G \,\middle|\, gXg^{-1} = X \right\}.}$$

Εάν $\varnothing \neq Y \subseteq G$ είναι τέτοιο, ώστε να ισχύει η εγκλειστική σχέση $Y \subseteq \mathrm{N}_G(X)$, τότε λέμε ότι **το** Y **ορθοθετεί το** X (εντός τής G).

[7] Προσοχή! Εάν $\varnothing \neq X \subseteq G$ και $x \in X$, τότε για ένα στοιχείο $g \in G$ που ανήκει στον κεντροποιητή $\mathrm{C}_G(X)$ ισχύει $gx = xg$, ενώ για ένα στοιχείο $g \in G$ που ανήκει στον ορθοθέτη $\mathrm{N}_G(X)$ ισχύει $gx = yg$, για κάποιο $y \in X$ το οποίο ενδέχεται (όταν το X δεν είναι μονοσύνολο) να είναι διάφορο τού x.

5.2.4 Πρόταση. *Για μια ομάδα* $(G,\cdot)$ *ισχύουν τα εξής*:

(i) *Εάν* $\varnothing \neq X \subseteq G$, *τότε*[8] $\mathrm{N}_G(X) \sqsubseteq G$.

(ii) *Εάν* $\varnothing \neq X \subseteq G$, *τότε το* X *είναι ορθόθετο υποσύνολο τής υποομάδας* $\mathrm{N}_G(X)$.

(iii) *Εάν* $\varnothing \neq X \subseteq G$, *τότε* $\mathrm{N}_G(X) = G \Leftrightarrow$ *το* X *είναι ορθόθετο υποσύνολο τής* G.

(iv) *Εάν* $H \sqsubseteq G$ *και* $H \trianglelefteq K \sqsubseteq G$, *τότε* $K \sqsubseteq \mathrm{N}_G(H)$.

(v) *Εάν* $\varnothing \neq X \subseteq H \sqsubseteq G$, *τότε* $\mathrm{N}_H(X) = H \cap \mathrm{N}_G(X)$.

(vi) *Εάν* $\varnothing \neq X \subseteq G$, *τότε* $\mathrm{C}_G(X) \sqsubseteq \mathrm{N}_G(X)$.

(vii) *Εάν* $H \sqsubseteq G$, *τότε* $\mathrm{C}_G(H) \trianglelefteq \mathrm{N}_G(H)$.

ΑΠΟΔΕΙΞΗ. (i) Προφανώς, $e_G \in \mathrm{N}_G(X)$. Επίσης, για οιαδήποτε $g_1, g_2 \in \mathrm{N}_G(X)$,

$$g_1 X g_1^{-1} = X \ \text{ και } \ g_2 X g_2^{-1} = X \Rightarrow g_2^{-1} X g_2 = X,$$

οπότε $X = g_1 X g_1^{-1} = g_1(g_2^{-1} X g_2) g_1^{-1} = \left(g_1 g_2^{-1}\right) X \left(g_1 g_2^{-1}\right)^{-1} \Rightarrow g_1 g_2^{-1} \in \mathrm{N}_G(X)$. Δυνάμει τού 2.1.16 (iii) συνάγεται ότι $\mathrm{N}_G(X) \sqsubseteq G$.

(ii) Εξ ορισμού τού ορθοθέτη $\mathrm{N}_G(X)$, $gXg^{-1} = X$ για κάθε $g \in \mathrm{N}_G(X)$, οπότε το X είναι ορθόθετο υποσύνολο τής υποομάδας $\mathrm{N}_G(X)$.

(iii) Εάν $\mathrm{N}_G(X) = G$, τότε για κάθε $g \in G$ έχουμε $gXg^{-1} = X$, οπότε το X είναι ορθόθετο υποσύνολο τής υποομάδας $\mathrm{N}_G(X)$. Και αντιστρόφως· εάν το X είναι ορθόθετο υποσύνολο τής υποομάδας $\mathrm{N}_G(X)$, τότε $gXg^{-1} = X$ για κάθε $g \in G$, απ' όπου έπεται ότι $\mathrm{N}_G(X) = G$.

(iv) Επειδή $H \trianglelefteq K$, έχουμε

$$\left.\begin{array}{r} [aHa^{-1} \in H,\ \forall a \in K] \Rightarrow K \subseteq \mathrm{N}_G(H) \\ \mathrm{N}_G(H) \sqsubseteq G \end{array}\right\} \underset{2.1.20}{\Longrightarrow} K \sqsubseteq \mathrm{N}_G(H).$$

(v) Προφανώς, $\mathrm{N}_H(X) \sqsubseteq H$ και $\mathrm{N}_H(X) \sqsubseteq \mathrm{N}_G(X) \Rightarrow \mathrm{N}_H(X) \sqsubseteq H \cap \mathrm{N}_G(X)$. Και αντιστρόφως· εάν $h \in H \cap \mathrm{N}_G(X)$, τότε $hXh^{-1} = X$, οπότε $h \in \mathrm{N}_H(X)$ και ισχύει και ο αντίστροφος εγκλεισμός $H \cap \mathrm{N}_G(X) \sqsubseteq \mathrm{N}_H(X)$.

(vi) Έστω τυχόν $g \in \mathrm{C}_G(X)$. Τότε

$$[gx = xg, \forall x \in X] \Rightarrow gX = Xg \Rightarrow gXg^{-1} = X \Rightarrow g \in \mathrm{N}_G(X),$$

οπότε $\mathrm{C}_G(X) \subseteq \mathrm{N}_G(X) \underset{2.1.20}{\Longrightarrow} \mathrm{C}_G(X) \sqsubseteq \mathrm{N}_G(X)$.

(vii) Για τυχόντα $g_1 \in \mathrm{N}_G(H)$, $g_2 \in \mathrm{C}_G(H)$ και $h \in H$,

$$\left(g_1 g_2 g_1^{-1}\right) h \left(g_1 g_2 g_1^{-1}\right)^{-1} = g_1(g_2 \left(g_1^{-1} h g_1\right) g_2^{-1}) g_1^{-1},$$

κι επειδή $g_1 \in \mathrm{N}_G(H) \Rightarrow g_1^{-1} h g_1 \in H$, έχουμε

$$g_2 \in \mathrm{C}_G(H) \Rightarrow g_2 \left(g_1^{-1} h g_1\right) = \left(g_1^{-1} h g_1\right) g_2 \Rightarrow g_2 \left(g_1^{-1} h g_1\right) g_2^{-1} = g_1^{-1} h g_1,$$

[8] Επειδή $\mathrm{N}_G(X) \sqsubseteq G$, ο ορθοθέτης $\mathrm{N}_G(X)$ τού X καλείται ενίοτε και **ορθοθετούσα υποομάδα τού** X (εντός τής ομάδας G).

απ' όπου έπεται ότι

$$\left(g_1 g_2 g_1^{-1}\right) h \left(g_1 g_2 g_1^{-1}\right)^{-1} = g_1 \left(g_1^{-1} h g_1\right) g_1^{-1} = h,$$

δηλαδή $g_1 g_2 g_1^{-1} \in \mathrm{C}_G(H)$. Επειδή $\mathrm{C}_G(H) \sqsubseteq \mathrm{N}_G(H)$, συμπεραίνουμε τελικώς ότι $\mathrm{C}_G(H) \trianglelefteq \mathrm{N}_G(H)$. □

5.2.5 Παράδειγμα. Οι ορθοθέτες των υποομάδων τής συμμετρικής ομάδας $\mathfrak{S}_3$ είναι οι

$$\mathrm{N}_{\mathfrak{S}_3}(\langle [1\,2] \rangle) = \langle [1\,2] \rangle\,,\ \mathrm{N}_{\mathfrak{S}_3}(\langle [1\,3] \rangle) = \langle [1\,3] \rangle\,,\ \mathrm{N}_{\mathfrak{S}_3}(\langle [2\,3] \rangle) = \langle [2\,3] \rangle\,,$$

και $\mathrm{N}_{\mathfrak{S}_3}(\{\mathrm{id}\}) = \mathrm{N}_{\mathfrak{S}_3}(\langle [1\,2\,3] \rangle) = \mathrm{N}_{\mathfrak{S}_3}(\mathfrak{S}_3) = \mathfrak{S}_3$ (όπως έπεται άμεσα από τον ορισμό 5.2.3 και τα προαναφερθέντα στα εδάφια 3.2.2, 4.1.19 και 4.1.42).

5.2.6 Παράδειγμα. Εάν $G := \mathfrak{A}_4$ και $H := \langle [1\,2] \circ [3\,4] \rangle$, τότε $H \lhd \mathrm{N}_G(H) = \mathbf{V}$.

5.2.7 Σημείωση. (i) Λόγω των (ii) και (iii) τής προτάσεως 5.2.4 ο ορθοθέτης $\mathrm{N}_G(H)$ μιας υποομάδας H τής G (και, αντιστοίχως, ο ορθοθέτης $\mathrm{N}_G(X)$ οιουδήποτε υποσυνόλου $\varnothing \neq X \subseteq G$) είναι η *μέγιστη υποομάδα* τής G εντός τής οποίας η υποομάδα H είναι ορθόθετη[9] (και, αντιστοίχως, η *μέγιστη υποομάδα*[10] τής G εντός τής οποίας το σύνολο X είναι ορθόθετο υπό την έννοια τού ορισμού 5.1.3). Βεβαίως, ο ορθοθέτης $\mathrm{N}_G(H)$ μιας υποομάδας H τής G (και, αντιστοίχως, ο ορθοθέτης $\mathrm{N}_G(X)$ οιουδήποτε υποσυνόλου $\varnothing \neq X \subseteq G$) δεν θα πρέπει να συγχέεται με την ορθόθετη θήκη $\mathrm{NCL}_G(H)$ τής H (και, αντιστοίχως, με την ορθόθετη θήκη $\mathrm{NCL}_G(X)$ τού X) που είναι η *ελάχιστη ορθόθετη* υποομάδα *τής* G που περιέχει την υποομάδα H (και, αντιστοίχως, το σύνολο X).

(ii) Για τα μονοσύνολα $\{x\} \in \mathfrak{P}(G)$ έχουμε προφανώς $\mathrm{N}_G(\{x\}) = \mathrm{C}_G(\{x\})$. Τούτη η υποομάδα τής G (ο **κεντροποιητής τού** x) *θα συμβολίζεται εφεξής* απλώς ως $\mathrm{C}_G(x)$. Εάν $\varnothing \neq Y \subseteq G$ είναι τέτοιο, ώστε να ισχύει $Y \subseteq \mathrm{C}_G(x)$, τότε λέμε ότι **το** Y **κεντροποιεί το** x (εντός τής G). Εξάλλου, για οιοδήποτε $\varnothing \neq X \subseteq G$ ισχύει $\mathrm{C}_G(X) = \bigcap\limits_{x \in X} \mathrm{C}_G(x)$.

(iii) Για $x \in G$ οι υποομάδες $\mathrm{N}_G(\langle x \rangle)$ και $\mathrm{C}_G(x)$ τής ομάδας G είναι ίσες όταν[11] $\mathrm{ord}(x) \in \{1, 2\}$. Ωστόσο, όταν $\mathrm{ord}(x) \geq 3$, ισχύει εν γένει μόνον ο εγκλεισμός $\mathrm{C}_G(x) \subseteq \mathrm{N}_G(\langle x \rangle)$. Επί παραδείγματι, εάν $G := \mathfrak{S}_4$ και $\sigma := [1\,2\,3]$, τότε

$$\mathrm{C}_{\mathfrak{S}_4}(\sigma) \subsetneqq \mathrm{N}_{\mathfrak{S}_4}(\langle \sigma \rangle) = \{\tau \in \mathfrak{S}_4 \,|\, \tau(4) = 4\} \cong \mathfrak{S}_3,$$

διότι $[2\,3] \in \mathrm{N}_{\mathfrak{S}_4}(\langle \sigma \rangle) \smallsetminus \mathrm{C}_{\mathfrak{S}_4}(\sigma)$.

[9] Υπ' αυτήν την έννοια, ο ορθοθέτης $\mathrm{N}_G(H)$ μιας υποομάδας H τής G μπορεί να εκληφθεί ως εκείνη η υποομάδα που εκφράζει το πόσο «απέχει» η H από το να είναι *ορθόθετη*. Προσοχή! Ο ορθοθέτης $\mathrm{N}_G(H)$ τής H είναι υποομάδα αλλά *όχι κατ' ανάγκην ορθόθετη* υποομάδα τής G!

[10] Έστω $K \sqsubseteq G$, τέτοια ώστε το X να είναι ορθόθετο υποσύνολό της. Τότε για οιοδήποτε στοιχείο $g \in K$ θα έχουμε $gxg^{-1} \in X$, για κάθε $x \in X$, οπότε $K \sqsubseteq \mathrm{N}_G(X)$.

[11] Όταν $\mathrm{ord}(x) = 1$, τούτο είναι προφανές. Όταν $\mathrm{ord}(x) = 2$, έχουμε $g \langle x \rangle g^{-1} = \langle x \rangle = \{e_G, x\}$ για κάθε στοιχείο $g \in \mathrm{N}_G(\langle x \rangle)$, οπότε $gxg^{-1} = x \Rightarrow g \in \mathrm{C}_G(x)$.

5.2.8 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω $\varnothing \neq X \subseteq G$. Τότε*

$$\boxed{\text{card}(\left\{ Y \in \mathfrak{P}(G) \smallsetminus \{\varnothing\} \,\middle|\, (X,Y) \in \mathcal{R}^{G}_{\text{συζ.}} \right\}) = |G : \mathrm{N}_G(X)|,}$$

δηλαδή ο πληθικός αριθμός των μη κενών υποσυνόλων τού υποκειμένου συνόλου G τής $(G,\cdot)$ που είναι συζυγή με το X ισούται με τον δείκτη τού ορθοθέτη $\mathrm{N}_G(X)$ τού X εντός τής G. Επιπροσθέτως, όταν η G είναι πεπερασμένη, αυτός ο πληθικός αριθμός είναι διαιρέτης τής τάξεως $|G|$ τής G.

ΑΠΟΔΕΙΞΗ. Έστω A ένα σύστημα αριστερών εκπροσώπων τού ορθοθέτη $\mathrm{N}_G(X)$ τού X εντός τής G. Ορίζουμε την f μέσω τού τύπου

$$\{ g\mathrm{N}_G(X) \,|\, g \in \mathrm{A} \} \ni g\mathrm{N}_G(X) \overset{f}{\longmapsto} gXg^{-1} \in \left\{ Y \in \mathfrak{P}(G) \smallsetminus \{\varnothing\} \,\middle|\, (X,Y) \in \mathcal{R}^{G}_{\text{συζ.}} \right\}.$$

Αυτή είναι καλώς ορισμένη απεικόνιση, διότι για δυο στοιχεία $g_1, g_2 \in \mathrm{A}$ για τα οποία ισχύει η ισότητα $g_1\mathrm{N}_G(X) = g_2\mathrm{N}_G(X)$ έχουμε

$$g_1^{-1}g_2 \in \mathrm{N}_G(X) \Rightarrow \left(g_1^{-1}g_2\right) X \left(g_1^{-1}g_2\right)^{-1} = X \Rightarrow g_1 X g_1^{-1} = g_2 X g_2^{-1}.$$

Η f είναι ενριπτική, καθότι ισχύουν οι συνεπαγωγές

$$\begin{aligned} f\left(g_1\mathrm{N}_G(X)\right) &= f\left(g_2\mathrm{N}_G(X)\right) \Rightarrow g_1 X g_1^{-1} = g_2 X g_2^{-1} \\ &\Rightarrow g_1^{-1}g_2 \in \mathrm{N}_G(X) \Rightarrow g_1\mathrm{N}_G(X) = g_2\mathrm{N}_G(X). \end{aligned}$$

Επιπροσθέτως, η f είναι και επιρριπτική, αφού για κάθε σύνολο Y ανήκον στο $\left\{ Y \in \mathfrak{P}(G) \smallsetminus \{\varnothing\} \,\middle|\, (X,Y) \in \mathcal{R}^{G}_{\text{συζ.}} \right\}$ υπάρχει κάποιο στοιχείο $g \in G : Y = gXg^{-1}$, οπότε $f\left(g\mathrm{N}_G(X)\right) = Y$. Τέλος, το ότι $|G : \mathrm{N}_G(X)| \mid |G|$, όταν $|G| < \infty$, έπεται από το θεώρημα 4.1.22 τού Lagrange. □

5.2.9 Πόρισμα. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \sqsubseteq G$. Τότε*

$$\boxed{\text{card}\left(\left\{ K \in \mathbf{Subg}(G) \,\middle|\, (H,K) \in \mathcal{R}^{G}_{\text{συζ.}\mathbf{Subg}(G)\times\mathbf{Subg}(G)} \right\}\right) = |G : \mathrm{N}_G(H)|,}$$

δηλαδή ο πληθικός αριθμός τής υποομάδων τής G που είναι συζυγείς με την H ισούται με τον δείκτη τού ορθοθέτη $\mathrm{N}_G(H)$ τής υποομάδας H εντός τής G. Επιπροσθέτως, όταν η G είναι πεπερασμένη, αυτός ο πληθικός αριθμός είναι διαιρέτης τής τάξεως $|G|$ τής G.

ΑΠΟΔΕΙΞΗ. Η ανωτέρω ισότητα αποδεικνύεται ακολουθώντας κατά γράμμα την απόδειξη τής προτάσεως 5.2.8 και αντικαθιστώντας -εκ παραλλήλου- σε αυτήν τα μη κενά υποσύνολα τού υποκειμένου συνόλου G τής ομάδας $(G,\cdot)$ με *υποομάδες* αυτής. □

5.2.10 Πόρισμα. *Έστω $(G,\cdot)$ μια ομάδα και έστω $x \in G$. Τότε*

$$\boxed{\text{card}(\text{ΚΛΣ}_G(x)) = \text{card}\left(\left\{ y \in G \,\middle|\, x \underset{\text{συζ.}}{\overset{G}{\sim}} y \right\}\right) = |G : \mathrm{C}_G(x)|,}$$

δηλαδή ο πληθικός αριθμός τής κλάσεως συζυγίας τού x εντός τής G ισούται με τον δείκτη τού κεντροποιητή $\mathrm{C}_G(x)$ τού x εντός τής G. Επιπροσθέτως, όταν η G είναι πεπερασμένη, αυτός ο πληθικός αριθμός είναι διαιρέτης τής τάξεως $|G|$ τής G.

ΑΠΟΔΕΙΞΗ. Λαμβανομένου υπ' όψιν τού 5.2.7 (ii), η ανωτέρω ισότητα αποδεικνύεται ακολουθώντας κατά γράμμα την απόδειξη τής προτάσεως 5.2.8 και αντικαθιστώντας -εκ παραλλήλου- σε αυτήν τα μη κενά υποσύνολα τού υποκειμένου συνόλου G τής $(G,\cdot)$ με *μονοσύνολα*. □

5.2.11 Παράδειγμα. (Κλάσεις συζυγίας αβελιανών ομάδων) Εάν η $(G,\cdot)$ είναι μια *αβελιανή* ομάδα, τότε *κάθε κλάση συζυγίας της* είναι ένα μονοσύνολο. Πράγματι· για κάθε $x\in G$ έχουμε

$$\mathrm{C}_G(x)=\{g\in G\,|gx=xg\}=G\Longrightarrow \mathrm{card}(\kappa\lambda\Sigma_G(x))=1\Rightarrow \kappa\lambda\Sigma_G(x)=\{x\}.$$

Άρα οι κλάσεις συζυγίας τής G είναι τα μονοσύνολα $\{x\}$, $x\in G$.

5.2.12 Παράδειγμα. (Κλάσεις συζυγίας τής $\mathbf{Q}$.) Μέσω τού πολλαπλασιαστικού καταλόγου τής ομάδας $\mathbf{Q}=\{\pm\mathbf{I}_2,\pm\mathbf{i},\pm\mathbf{j},\pm\mathbf{k}\}$ των τετρανίων (βλ. 2.2.11) διαπιστώνουμε αφ' ενός μεν ότι το $-\mathbf{I}_2$ μετατίθεται αμοιβαίως με κάθε στοιχείο τής $\mathbf{Q}$, οπότε $\kappa\lambda\Sigma_{\mathbf{Q}}(\mathbf{I}_2)=\{\mathbf{I}_2\}$,$\kappa\lambda\Sigma_{\mathbf{Q}}(-\mathbf{I}_2)=\{-\mathbf{I}_2\}$, αφ' ετέρου δε ότι

$$\mathbf{iji}^{-1}=\mathbf{j}^{-1}=-\mathbf{j},\ \mathbf{jkj}^{-1}=\mathbf{k}^{-1}=-\mathbf{k},\ \mathbf{kik}^{-1}=\mathbf{i}^{-1}=-\mathbf{i},$$

οπότε $\{\mathbf{i},-\mathbf{i}\}\subseteq\kappa\lambda\Sigma_{\mathbf{Q}}(\mathbf{i})$, $\{\mathbf{j},-\mathbf{j}\}\subseteq\kappa\lambda\Sigma_{\mathbf{Q}}(\mathbf{j})$ και $\{\mathbf{k},-\mathbf{k}\}\subseteq\kappa\lambda\Sigma_{\mathbf{Q}}(\mathbf{k})$. Επειδή η $\langle\mathbf{i}\rangle$ (ως κυκλική) είναι αβελιανή ομάδα, έχουμε $\langle\mathbf{i}\rangle\sqsubseteq\mathrm{C}_{\mathbf{Q}}(\langle\mathbf{i}\rangle)$, $\langle\mathbf{i}\rangle\trianglelefteq\mathbf{Q}\Rightarrow\mathrm{C}_{\mathbf{Q}}(\langle\mathbf{i}\rangle)\trianglelefteq\mathbf{Q}$ (βλ. 5.2.2 (ii)-(iii) και 4.2.18) και το θεώρημα 4.1.50 δίδει

$$|\mathbf{Q}:\mathrm{C}_{\mathbf{Q}}(\langle\mathbf{i}\rangle)|\,|\mathrm{C}_{\mathbf{Q}}(\langle\mathbf{i}\rangle):\langle\mathbf{i}\rangle|=|\mathbf{Q}:\langle\mathbf{i}\rangle|=|\mathbf{Q}/\langle\mathbf{i}\rangle|=\tfrac{|\mathbf{Q}|}{|\langle\mathbf{i}\rangle|}=2. \tag{5.8}$$

Επειδή $\mathbf{j}\in\mathbf{Q}\smallsetminus\mathrm{C}_{\mathbf{Q}}(\langle\mathbf{i}\rangle)\Rightarrow\mathrm{C}_{\mathbf{Q}}(\langle\mathbf{i}\rangle)\sqsubset\mathbf{Q}$, από την (5.8) και το πόρισμα 5.2.10 προκύπτει ότι

$$\mathrm{C}_{\mathbf{Q}}(\langle\mathbf{i}\rangle)=\langle\mathbf{i}\rangle\,,\ \mathrm{card}(\kappa\lambda\Sigma_{\mathbf{Q}}(\mathbf{i}))=|\mathbf{Q}:\mathrm{C}_{\mathbf{Q}}(\langle\mathbf{i}\rangle)|=2$$

και, κατ' επέκταση, ότι $\kappa\lambda\Sigma_{\mathbf{Q}}(\mathbf{i})=\{\mathbf{i},-\mathbf{i}\}$. Χρησιμοποιώντας τά ίδια επιχειρήματα (κατόπιν κυκλικής εναλλαγής των $\mathbf{i},\mathbf{j}$ και $\mathbf{k}$) καταλήγουμε στο συμπέρασμα ότι $\kappa\lambda\Sigma_{\mathbf{Q}}(\mathbf{j})=\{\mathbf{j},-\mathbf{j}\}$ και $\kappa\lambda\Sigma_{\mathbf{Q}}(\mathbf{k})=\{\mathbf{k},-\mathbf{k}\}$. Άρα η $\mathbf{Q}$ διαθέτει εν συνόλω πέντε κλάσεις συζυγίας:

$$\{\mathbf{I}_2\},\ \{-\mathbf{I}_2\},\ \{\mathbf{i},-\mathbf{i}\},\ \{\mathbf{j},-\mathbf{j}\},\ \{\mathbf{k},-\mathbf{k}\}.$$

Το $\Xi:=\{\mathbf{I}_2,-\mathbf{I}_2,\mathbf{i},\mathbf{j},\mathbf{k}\}$ αποτελεί ένα πλήρες σύστημα εκπροσώπων τής $\mathbf{Q}$ ως προς την "$\underset{\text{συζ.}}{\sim}$", ενώ ο αντίστοιχος κατάλογος εκπροσώπων των κλάσεων συζυγίας τής $\mathbf{Q}$ είναι ο εξής:

εκπρ.	$\mathbf{I}_2$	$-\mathbf{I}_2$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
τάξη	1	2	4	4	4
♯	1	1	2	2	2

Εν συνεχεία, για να αναδείξουμε την ιδιαίτερη σημασία τού πορίσματος 5.2.9, θα αποδείξουμε μέσω αυτού (σε συνδυασμό με τα λήμματα 5.2.14 και 5.2.17 που ακολουθούν) ότι εάν μια ομάδα έχει μια γνήσια υποομάδα πεπερασμένου δείκτη, τότε έχει κατ' ανάγκην και μια γνήσια *ορθόθετη* υποομάδα πεπερασμένου δείκτη (βλ. θεώρημα 5.2.18).

5.2.13 Ορισμός. Έστω $(G,\cdot)$ μια ομάδα και έστω $H \sqsubseteq G$. Για κάθε $g \in G$ έχουμε $gHg^{-1} \sqsubseteq G$ (βλ. 4.2.16). Κατ' επέκταση, $\bigcap\limits_{g\in G} gHg^{-1} \sqsubseteq G$ (βλ. 2.1.23). Αυτή η υποομάδα

$$\boxed{\mathrm{Core}_G(H) := \bigcap_{g\in G} gHg^{-1}}$$

(οριζόμενη ως η τομή *όλων* των συζυγών υποομάδων τής H εντός τής G) καλείται **ορθόθετο εσωτερικό** (ή ο **μυχός**) **τής** H **εντός τής** G (και αποτελεί, όπως θα δούμε στο λήμμα 5.2.14 που ακολουθεί, τη *μέγιστη ορθόθετη υποομάδα τής* G *που περιέχεται στην* H).

5.2.14 Λήμμα. *Έστω* $(G,\cdot)$ *μια ομάδα και έστω* $H \sqsubseteq G$. *Τότε ισχύουν τα εξής*:
(i) $\mathrm{Core}_G(H) \trianglelefteq G$.
(ii) *Εάν* $L \sqsubseteq H$ *και* $L \trianglelefteq G$, *τότε* $L \sqsubseteq \mathrm{Core}_G(H)$.

ΑΠΟΔΕΙΞΗ. (i) Θεωρούμε τυχόντα στοιχεία $x \in G$ και $y \in \mathrm{core}_G(H)$. Προφανώς, $y \in gHg^{-1},\ \forall g \in G$, οπότε $xyx^{-1} \in x\left(gHg^{-1}\right)x^{-1} = (xg)\,H\,(xg)^{-1},\ \forall g \in G$. Εν συνεχεία παρατηρούμε ότι για *οιοδήποτε* στοιχείο $a \in G$ υπάρχει (μονοσημάντως ορισμένο) $g \in G$, τέτοιο ώστε να ισχύει η ισότητα $a = xg$ (ήτοι το $g := x^{-1}a$, βλ. 2.1.9 (iv)). Κατά συνέπειαν,

$$xyx^{-1} \in aHa^{-1},\ \forall a \in G \Rightarrow xyx^{-1} \in \bigcap_{g\in G} gHg^{-1} := \mathrm{Core}_G(H),$$

οπότε $\mathrm{core}_G(H) \trianglelefteq G$.
(ii) Έστω g *τυχόν* στοιχείο τής G. Επειδή $L \trianglelefteq G$, έχουμε $gLg^{-1} = L$. Επομένως,

$$L \subseteq H \Rightarrow [gLg^{-1} \subseteq gHg^{-1}, \forall g \in G] \Rightarrow \bigcap_{g\in G} gLg^{-1} = L \subseteq \mathrm{Core}_G(H),$$

απ' όπου έπεται ότι $L \sqsubseteq \mathrm{Core}_G(H)$ (καθόσον $L \sqsubseteq G$, βλ. 2.1.20). □

5.2.15 Παράδειγμα. Για τη μη ορθόθετη υποομάδα $H := \langle[1\,2]\rangle = \{\mathrm{id},\ [1\,2]\}$ τής

$$\mathfrak{S}_3 = \{\mathrm{id},\ [1\,2]\,,\ [1\,3]\,,\ [2\,3]\,,\ [1\,2\,3]\,,\ [1\,3\,2]\}$$

ισχύουν τα εξής:

$$\mathrm{id} \circ H \circ \mathrm{id}^{-1} = H, \qquad [1\,2] \circ H \circ [1\,2]^{-1} = H,$$
$$[1\,3] \circ H \circ [1\,3]^{-1} = \langle[2\,3]\rangle\,, \qquad [2\,3] \circ H \circ [2\,3]^{-1} = \langle[1\,3]\rangle\,,$$
$$[1\,2\,3] \circ H \circ [1\,2\,3]^{-1} = \langle[2\,3]\rangle\,, \qquad [1\,3\,2] \circ H \circ [1\,3\,2]^{-1} = \langle[1\,3]\rangle\,.$$

(Πρβλ. 3.2.2 και 4.1.19.) Άρα $\mathrm{Core}_{\mathfrak{S}_3}(H) = \langle[1\,2]\rangle \cap \langle[1\,3]\rangle \cap \langle[2\,3]\rangle = \{\mathrm{id}\}$.

5.2.16 Παράδειγμα. Θεωρούμε την υποομάδα

$$H := \left\{ \begin{pmatrix} r & 0 \\ 0 & s \end{pmatrix} \middle| \, r, s \in \mathbb{Q},\ rs \neq 0 \right\}$$

τής $\mathrm{GL}_2(\mathbb{Q})$. Αυτή δεν είναι ορθόθετη, διότι π.χ.

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ -2 & 3 \end{pmatrix} \notin H.$$

Αντιθέτως, η ομάδα

$$L := \left\{ \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \middle| \, r \in \mathbb{Q} \smallsetminus \{0\} \right\} \sqsubseteq H.$$

αποτελεί ορθόθετη υποομάδα τής $\mathrm{GL}_2(\mathbb{Q})$, καθόσον για οιουσδήποτε $r \in \mathbb{Q} \smallsetminus \{0\}$ και $a, b, c, d \in \mathbb{Q}$ με $ad - bc \neq 0$ έχουμε

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}.$$

Σύμφωνα με το (ii) τού λήμματος 5.2.14, $L \sqsubseteq \mathrm{Core}_{\mathrm{GL}_2(\mathbb{Q})}(H)$. Έστω $\mathbf{A}$ τυχών πίνακας ανήκων στην $\mathrm{Core}_{\mathrm{GL}_2(\mathbb{Q})}(H)$. Ο $\mathbf{A}$ ανήκει στην τομή *όλων* των συζυγών υποομάδων τής H εντός τής $\mathrm{GL}_2(\mathbb{Q})$. Επειδή μεταξύ αυτών των συζυγών ανήκει και η ίδια η H $(= \mathbf{I}_2 H \mathbf{I}_2^{-1})$,

$$\exists r_1, s_1 \in \mathbb{Q},\ r_1 s_1 \neq 0 : \mathbf{A} = \begin{pmatrix} r_1 & 0 \\ 0 & s_1 \end{pmatrix}.$$

Η ομάδα $\mathbf{B}H\mathbf{B}^{-1}$, όπου $\mathbf{B} := \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$, είναι άλλη μία συζυγής υποομάδα τής H εντός τής $\mathrm{GL}_2(\mathbb{Q})$. Προφανώς,

$$\mathbf{A} \in H \cap \mathbf{B}H\mathbf{B}^{-1} \Rightarrow \exists \mathbf{C} \in H,\ \mathbf{C} = \begin{pmatrix} r_2 & 0 \\ 0 & s_2 \end{pmatrix} : \mathbf{A} = \mathbf{B}\mathbf{C}\mathbf{B}^{-1}$$

(για κατάλληλους $r_2, s_2 \in \mathbb{Q}$ με $r_2 s_2 \neq 0$). Κατά συνέπειαν,

$$\begin{pmatrix} r_1 & 0 \\ 0 & s_1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r_2 & 0 \\ 0 & s_2 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} r_2 & r_2 - s_2 \\ 0 & s_2 \end{pmatrix},$$

απ' όπου έπεται ότι $r_1 = r_2 = s_1 = s_2$, ήτοι ότι $\mathbf{A} \in L$. Άρα $\mathrm{Core}_{\mathrm{GL}_2(\mathbb{Q})}(H) = L$.

5.2.17 Λήμμα. *Έστω $(G, \cdot)$ μια ομάδα για την οποία $\exists H \sqsubseteq G$ με $|G : H| < \infty$. Τότε*

$$|G : H| = \left|G : gHg^{-1}\right|,\ \forall g \in G.$$

ΑΠΟΔΕΙΞΗ. Έστω τυχόν $g \in G$. Υποθέτουμε ότι το A είναι ένα σύστημα αριστερών εκπροσώπων τής H εντός τής G με $\mathrm{card}(\mathbf{A}) = n \in \mathbb{N}$ και

$$\{aH \,|a \in \mathbf{A}\} = \{a_1 H,\ a_2 H, ...,\ a_n H\}.$$

Θα αποδείξουμε ότι το

$$\left\{g(aH)g^{-1} \,|a \in \mathbf{A}\right\} = \{g(a_1 H)g^{-1}, g(a_2 H)g^{-1}, ...,\ g(a_n H)g^{-1}\}$$

αποτελεί ένα σύστημα αριστερών εκπροσώπων τής gHg^{-1} εντός τής G. Προφανώς,

$$\bigcup_{j=1}^{n} g(a_nH)g^{-1} = g\left(\bigcup_{j=1}^{n} a_nH\right)g^{-1} = gGg^{-1} = G.$$

Επιπροσθέτως, εάν $j, j' \in \{1, 2, ..., n\}$ με $g(a_jH)g^{-1} = g(a_{j'}H)g^{-1}$, τότε

$$g^{-1}(g(a_jH)g^{-1}) = g^{-1}(g(a_{j'}H)g^{-1}) \Rightarrow (a_jH)\,g^{-1} = (a_{j'}H)\,g^{-1},$$

οπότε

$$((a_jH)\,g^{-1})g = ((a_{j'}H)\,g^{-1})g \Rightarrow a_jH = a_{j'}H \Rightarrow j = j'.$$

Συνεπώς, $\left|G : gHg^{-1}\right| = \text{card(A)} = n$. □

5.2.18 Θεώρημα. *Έστω $(G, \cdot)$ μια ομάδα για την οποία $\exists H \sqsubset G$ με $|G : H| < \infty$. Τότε $\exists K \lhd G$ με*

$$\boxed{|G : H| \leq |G : K| \leq |G : H|^{|G:\mathrm{N}_G(H)|} < \infty.}$$

ΑΠΟΔΕΙΞΗ. Εάν μια ομάδα $(G, \cdot)$ διαθέτει μια *γνήσια* υποομάδα H πεπερασμένου δείκτη $|G : H| = n \geq 2$, τότε $|G : \mathrm{N}_G(H)| \leq n$, διότι $H \sqsubseteq \mathrm{N}_G(H)$ (βλ. 5.2.4 (iv)). Άρα και ο ορθοθέτης $\mathrm{N}_G(H)$ τής H είναι μια υποομάδα τής G πεπερασμένου δείκτη. Ας θέσουμε $l := |G : \mathrm{N}_G(H)|$. Κατά το πόρισμα 5.2.9 υφίστανται ακριβώς l υποομάδες τής G που είναι συζυγείς προς την H. Αυτές είναι τής μορφής

$$g_1Hg_1^{-1},\ g_2Hg_2^{-1}, \ldots,\ g_lHg_l^{-1},$$

για κάποια στοιχεία $g_1, g_2, ..., g_l \in G$. Κατά το λήμμα 5.2.17,

$$\left|G : g_jHg_j^{-1}\right| = n,\ \forall j \in \{1, 2, ..., l\}.$$

Θέτοντας $K := \bigcap_{j=1}^{l} g_jHg_j^{-1}$, παρατηρούμε αφ' ενός μεν ότι

$$n \leq |G : K| \leq \prod_{j=1}^{l} \left|G : g_jHg_j^{-1}\right| = n^l \tag{5.9}$$

(κάνοντας χρήση τού πορίσματος 4.1.55), αφ' ετέρου δε ότι

$$K = \bigcap_{g\in G} gHg^{-1} =: \mathrm{Core}_G(H), \tag{5.10}$$

καθόσον για *οιοδήποτε* στοιχείο $g \in G$ υπάρχει κάποιος δείκτης $j \in \{1, 2, ..., l\}$ με $gHg^{-1} = g_jHg_j^{-1}$. (Οι gHg^{-1} και H είναι συζυγείς για *οιοδήποτε* $g \in G$.) Από την (5.10) και το (i) τού λήμματος 5.2.14 έπεται ότι $K \lhd G$. □

5.2.19 Παρατήρηση. Η ύπαρξη μιας $K \lhd G$ με $|G:K| < \infty$ είχε ήδη αποδειχθεί (με άλλον τρόπο) στο (iii) τού θεωρήματος 4.4.23. Ως K επελέγη -και σε εκείνο το θεώρημα- το ορθόθετο εσωτερικό τής H εντός τής G. Ωστόσο εκεί, ως άνω φράγμα τού δείκτη $|G:K|$ είχε προκύψει το παραγοντικό $n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$ τού $n := |G:H|$ και όχι η δύναμη n^l (βλ. (5.9)).

5.2.20 Σημείωση. Εάν $(G,\cdot)$ είναι μια πεπερασμένη ομάδα, τότε *υπό συγκεκριμένες προϋποθέσεις* υφίσταται κάποια χαρακτηριστική *σχέση ισοτιμίας* μεταξύ τής τάξεώς της $|G|$ και τού πλήθους $\mathfrak{K}(G)$ των κλάσεων συζυγίας της. Επί παραδείγματι, στο κλασικό σύγγραμμα **[3]** τού G. Burnside αποδεικνύεται η συνεπαγωγή

$$\boxed{|G| \equiv 1(\mathrm{mod}\ 2) \Longrightarrow |G| \equiv \mathfrak{K}(G)\,(\mathrm{mod}\ 16)}$$

και προτείνεται ως άσκηση (στη σελ. 320 τής δεύτερης εκδόσεώς του) η απόδειξη τής συνεπαγωγής

$$\boxed{|G| \equiv 1(\mathrm{mod}\ 4) \Longrightarrow |G| \equiv \mathfrak{K}(G)\,(\mathrm{mod}\ 32)\,.}$$

Κλείνουμε την παρούσα ενότητα παραθέτοντας την απόδειξη τής ισχύος μιας παρόμοιας σχέσεως ισοτιμίας, την οφειλόμενη στον B. Poonen[12], η οποία κάνει χρήση μόνον τού πορίσματος 5.2.10 και στοιχειωδών αριθμοθεωρητικών επιχειρημάτων.

5.2.21 Θεώρημα. (B. Poonen, 1995) *Έστω $m \in \mathbb{N}$, $m \geq 2$, και έστω $(G,\cdot)$ μια πεπερασμένη μη τετριμμένη ομάδα. Εάν υποθέσουμε ότι $|G| = p_1^{\nu_1}\cdots p_k^{\nu_k}$ είναι η παράσταση τής τάξεώς της ως γινομένου (καταλλήλων δυνάμεων) σαφώς διακεκριμένων πρώτων αριθμών $p_1,...,p_k$, όπου $k \in \mathbb{N}$ και $\nu_1,...,\nu_k \in \mathbb{N}$* (βλ. (B.19)), *τότε ισχύει η συνεπαγωγή*

$$\boxed{\left.\begin{array}{c} p_j \equiv 1(\mathrm{mod}\, m), \\ \forall j \in \{1,...,k\} \end{array}\right\} \Longrightarrow |G| \equiv \mathfrak{K}(G)\,\left(\mathrm{mod}\ 2m^2\right).}$$

ΑΠΟΔΕΙΞΗ. Θέτοντας $\mathcal{A} := \{\,(g,h) \in G\times G |\, gh \neq hg\}$ μπορούμε *για κάθε* μη διατεταγμένο ζεύγος $\{K_1,K_2\}$ δύο κυκλικών υποομάδων K_1 και K_2 τής G να θεωρήσουμε το σύνολο των $(g,h) \in G\times G$ για τα οποία ισχύει *είτε* $\langle g\rangle = K_1$ και $\langle h\rangle = K_2$ *είτε* $\langle g\rangle = K_2$ και $\langle h\rangle = K_1$ (δηλαδή για τα οποία οι υποομάδες $\langle g\rangle$ και $\langle h\rangle$ είναι οι K_1 και K_2 ως προς κάποια διάταξή τους). Προφανώς, αυτού τού είδους τα υποσύνολα διαμελίζουν το καρτεσιανό γινόμενο $G\times G$.

Βήμα 1ο. *Το $\mathcal{A}$ αποτελεί αποσυνδετή ένωση υποσυνόλων αυτού τού είδους*. Πράγματι·

$$(g,h) \notin \mathcal{A} \Longleftrightarrow [xy = yx, \forall x \in \langle g\rangle \ \text{ και } \ \forall y \in \langle h\rangle],$$

όπου το δεξιό μέλος εξαρτάται μόνον από το μη διατεταγμένο ζεύγος $\{\langle g\rangle, \langle h\rangle\}$.

[12] B. Poonen: *Congruences relating the order of a group to the number of conjugacy classes*, The American Mathematical Monthly, Vol. **102**, No. 5 (1995), 440-442.

Βήμα 2ο. *Για κάθε υποσύνολο* $\mathcal{B}$ *τού* $\mathcal{A}$ *αυτού τού είδους ισχύει* $2m^2 \mid \text{card}(\mathcal{B})$. Πράγματι· εάν $\{K_1, K_2\}$ είναι τυχόν (μη διατεταγμένο) ζεύγος κυκλικών υποομάδων K_1 και K_2 τής G που αντιστοιχεί στο $\mathcal{B}$, τότε

$$\begin{aligned}\mathcal{B} &= \{(g_1,g_2)\in K_1\times K_2 \mid \langle g_1\rangle = K_1 \text{ και } \langle g_2\rangle = K_2\} \\ &\quad \bigcup \{(g_1,g_2)\in K_1\times K_2 \mid \langle g_1\rangle = K_2 \text{ και } \langle g_2\rangle = K_1\}. \end{aligned} \tag{5.11}$$

Επειδή για $i = 1,2$ η K_i έχει $\phi(|K_i|)$ γεννήτορες (όπου ϕ η συνάρτηση φι τού Euler, βλ. πόρισμα 2.3.17), καθένα εκ των συνόλων τής ανωτέρω ενώσεως διαθέτει $\phi(|K_1|)\,\phi(|K_2|)$ στοιχεία. Επιπροσθέτως, επειδή

$$\mathcal{B}\subseteq\mathcal{A} \Rightarrow K_1 \neq K_2,$$

η ένωση (5.11) είναι αποσυνδετή και, ως εκ τούτου, ισχύει

$$\text{card}(\mathcal{B}) = 2\phi(|K_1|)\,\phi(|K_2|). \tag{5.12}$$

Από τον εγκλεισμό $\mathcal{B}\subseteq\mathcal{A}$ συνάγεται ότι αμφότερες οι K_1 και K_2 είναι μη τετριμμένες. Κατά συνέπειαν, για $i = 1,2$ έχουμε

$$1 \neq |K_i| \mid |G| \underset{\text{B.3.14}}{\Longrightarrow} [\exists \xi_i \in \{1,...,k\} : p_{\xi_i} \mid |K_i|] \Longrightarrow p_{\xi_i} \mid |G|,$$

οπότε $m \mid p_{\xi_i} - 1 = \phi\left(p_{\xi_i}\right)$ (βλ. λήμμα Β.4.19) και

$$\phi\left(p_{\xi_i}\right) \mid \phi(|K_i|) \Rightarrow m \mid \phi(|K_i|) \underset{(5.12)}{\Longrightarrow} 2m^2 \mid \text{card}(\mathcal{B}).$$

Βήμα 3ο. Εάν $s := \text{card}(G/\underset{\text{συζ.}}{\sim})$ και $\mathcal{C}_1,...,\mathcal{C}_s$ είναι οι σαφώς διακεκριμένες κλάσεις συζυγίας τής G, τότε το πόρισμα 5.2.10 δίδει

$$\begin{aligned}&\text{card}\left((G\times G)\smallsetminus\mathcal{A}\right) = \sum_{g\in G}\text{card}(\{h\in G \mid gh = hg\}) \\ &= \sum_{g\in G}|\mathrm{C}_G(g)| = |G|\sum_{g\in G}\tfrac{1}{\text{card}(\kappa\lambda\Sigma_G(g))} = |G|\sum_{\varrho=1}^{s}\sum_{g\in\mathcal{C}_\varrho}\tfrac{1}{\text{card}(\kappa\lambda\Sigma_G(g))} \\ &= |G|\sum_{\varrho=1}^{s}(\underbrace{\frac{1}{\text{card}(\mathcal{C}_\varrho)}+\cdots+\frac{1}{\text{card}(\mathcal{C}_\varrho)}}_{\text{card}(\mathcal{C}_\varrho)\ \text{φορές}}) = |G|\sum_{\varrho=1}^{s}1 = |G|\,s,\end{aligned}$$

καθόσον $G = \mathcal{C}_1 \coprod \cdots \coprod \mathcal{C}_s$ και

$$\text{card}(\kappa\lambda\Sigma_G(g)) = \text{card}(\mathcal{C}_\varrho),\ \forall\varrho\in\{1,...,s\} \text{ και } \forall g\in\mathcal{C}_\varrho.$$

Επομένως, $\text{card}(\mathcal{A}) = |G|\,(|G|-s)$. Από τα προηγηθέντα βήματα **1** και **2** έπεται ότι $2m^2 \mid \text{card}(\mathcal{A})$. Επειδή

$$\left.\begin{array}{c} p_j \equiv 1 (\mathrm{mod}\, m) \Rightarrow p_j > m, \\ \forall j\in\{1,...,k\} \text{ και } m\geq 2 \end{array}\right\} \underset{\text{B.3.16}}{\Longrightarrow} \mu\kappa\delta(|G|, 2m^2) = 1,$$

έχουμε

$$\left.\begin{array}{c} 2m^2 \mid \text{card}(\mathcal{A}) = |G|\,(|G|-s) \\ \mu\kappa\delta(|G|, 2m^2) = 1 \end{array}\right\} \underset{\text{B.2.9}}{\Longrightarrow} 2m^2 \mid |G| - s,$$

ήτοι $|G| \equiv s (\mathrm{mod}\, 2m^2)$. □

5.3 ΚΛΑΣΕΙΣ ΣΥΖΥΓΙΑΣ ΤΩΝ ΣΥΜΜΕΤΡΙΚΩΝ ΚΑΙ ΤΩΝ ΕΝΑΛΛΑΣΣΟΥΣΩΝ ΟΜΑΔΩΝ

Η συστηματική μελέτη των κλάσεων συζυγίας των $\mathfrak{S}_n$ και $\mathfrak{A}_n$ προαπαιτεί την υπόμνηση αρκετών θεμελιωδών εννοιών και αποτελεσμάτων τής Θεωρίας Διαμερίσεων Αριθμών και τής Συνδυαστικής.

5.3.1 Συμβολισμός. Έστω $n \in \mathbb{N}$. Για κάθε $\nu \in \{1,...,n\}$ συμβολίζουμε ως

$$\Pi_\nu(n) := \left\{ (k_1, k_2,..., k_\nu) \in \mathbb{N}^\nu \;\middle|\; k_1 \leq k_2 \leq \cdots \leq k_\nu, \text{ με } \sum_{j=1}^{\nu} k_j = n \right\}$$

το σύνολο *όλων των διαμερίσεων τού* n (ως προς την πρόσθεση τού $\mathbb{N}$) *σε* ν *φυσικούς αριθμούς*. (Προφανώς, $\Pi_1(n) = \{n\}$ και $\Pi_n(n) = \{(1,1,...,1)\}$.) Επίσης, συμβολίζουμε ως

$$\boxed{\Pi(n) := \bigcup_{\nu=1}^{n} \Pi_\nu(n)}$$

το σύνολο *όλων των δυνατών διαμερίσεων* τού n και θέτουμε

$$\boxed{\varpi(n) := \text{card}(\Pi(n)).}$$

5.3.2 Σημείωση. (Περί τού $\varpi(n)$.) (i) Ο τρόπος προσδιορισμού τού πλήθους $\varpi(n)$ όλων των δυνατών διαμερίσεων ενός $n \in \mathbb{N}$ περιεγράφη διεξοδικώς από τον L. Euler (1707-1783) το έτος[13] 1741. Η *γεννήτρια συνάρτηση* τού $\varpi(n)$ είναι η[14]

$$\boxed{\sum_{n=0}^{\infty} \varpi(n)\, t^n = \prod_{\kappa=1}^{\infty} \left(\frac{1}{1-t^\kappa} \right) \left(= \prod_{\kappa=1}^{\infty} \left(\sum_{j=0}^{\infty} t^{\kappa j} \right) \right).} \tag{5.13}$$

(ii) Η *ασυμπτωτική συμπεριφορά* τού $\varpi(n)$ είναι η εξής:

$$\boxed{\varpi(n) \approx \tfrac{1}{4n\sqrt{3}} \exp(2\pi\sqrt{\tfrac{n}{6}}), \text{ καθώς το } n \longrightarrow \infty.} \tag{5.14}$$

Η ανακάλυψη τής εκφράσεως (5.14) έγινε από τους G.H. Hardy (1877-1947) και S. Ramanujan (1887-1920) το έτος[15] 1918 και (ανεξαρτήτως αυτών) από τον J.V. Uspensky (1883-1947) το έτος 1920. Ένα επιπρόσθετο ασυμπτωτικό αποτέλεσμα εδόθη από τον H. Rademacher (1892-1969) το[16] 1937.

[13] Το πρόβλημα τού προσδιορισμού τού $\varpi(n)$ είχε τεθεί ήδη από το έτος 1699 σε μια επιστολή τού G. Leibnitz (1646-1716) προς τον J. Bernoulli (1667-1748). Το 1740 (και συγκεκριμένα, την 4η Σεπτεμβρίου 1740) ετέθη εκ νέου ως ερώτημα από τον Ph. Naudé (1684-1747) στον L. Euler. Ο τελευταίος παρουσίασε τη λύση τού προβλήματος στην Ακαδημία Επιστημών τής Αγίας Πετρουπόλεως την 6η Απριλίου τού 1741. Ωστόσο, αυτή δημοσιεύθηκε έπειτα από μία δεκαετία. (Βλ. L. Euler: *Observationes analyticae variae decomtinationibus*, Commentarii academiae scientiarum Petropolitanae **13** (1741/43) 1751, pp. 64-93, reprinted in Opera Omnia Series I, Vol. **2,** pp. 163-193.)

[14] Εδώ χρησιμοποιείται η συνήθης σύμβαση: $\varpi(0) := 1$.

[15] Βλ. G.H. Hardy & S. Ramanujan: *Asymptotic formulae in combinatory analysis*, Proc. London Math. Soc. (2) **17** (1918), 75-115.

[16] Βλ. H. Rademacher: *On the partition function* $p(n)$, Proc. London Math. Soc. (2) **43** (1937), 75-115.

5.3.3 Λήμμα. *Έστω* $n \in \mathbb{N}$. *Τότε κάθε μετάταξη* $\sigma \in \mathfrak{S}_n$ *γράφεται ως σύνθεση*

$$\sigma = c_1 \circ c_2 \circ \cdots \circ c_\nu \tag{5.15}$$

ν *ανά δύο ξένων μεταξύ τους κύκλων* $c_1, c_2,..., c_\nu$ *τής μορφής*

$$c_j = \left[\alpha_{j1}\ \alpha_{j2} ... \ \alpha_{jk_j}\right],\ \forall j \in \{1,..., \nu\},$$

για κάποιον $\nu \in \{1,..., n\}$, *ούτως ώστε να ισχύει*[17]

$$\bigcup_{j=1}^{\nu} \{\alpha_{j1}, \alpha_{j2},..., \alpha_{jk_j}\} = \{1, 2,..., n\},$$

όπου $(k_1, k_2,..., k_\nu) \in \Pi_\nu(n)$. (Προσοχή! Η έκφραση (5.15) δεν είναι (εν γένει) μονοσημάντως ορισμένη παρά μόνον ύστερα από κάποια αναδιάταξη των μετεχόντων κύκλων *ιδίου μήκους*. Αντιθέτως, η ν-άδα $(k_1, k_2,..., k_\nu) \in \Pi_\nu(n)$ είναι *πάντοτε* μονοσημάντως ορισμένη!)

ΑΠΟΔΕΙΞΗ. Έστω τυχούσα μετάταξη $\sigma \in \mathfrak{S}_n$. Εάν $\sigma = \mathrm{id}$, τότε αυτή γράφεται υπό τη μορφή (5.15), καθότι $\mathrm{id} = [1] \circ [2] \circ \cdots \circ [n]$ (με $k_1 = k_2 = \cdots = k_\nu = 1$). Εάν $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{id}\}$, τότε, σύμφωνα με το θεώρημα 3.2.7, η σ μπορεί να γραφεί υπό τη μορφή επαλλήλων συνθέσεων $\sigma = d_1 \circ d_2 \circ \cdots \circ d_m$ ανά δύο ξένων μεταξύ τους κύκλων $d_1, d_2,..., d_m$ μήκους ≥ 2 (με $m \geq 1$ και $2m \leq n$). Επιλέγουμε μια αναδιάταξη[18] $\hat{d}_1, \hat{d}_2,..., \hat{d}_m$ των κύκλων $d_1, d_2,..., d_m$, ούτως ώστε να ισχύει

$$(\text{μήκος τού } \hat{d}_i) \leq (\text{μήκος τού } \hat{d}_{i+1}),\ \forall i \in \{1,..., m-1\}.$$

Τότε $\sigma = \hat{d}_1 \circ \hat{d}_2 \circ \cdots \circ \hat{d}_m$ (διότι οι $d_1, d_2,..., d_m$ είναι ανά δύο ξένοι μεταξύ τους, βλ. λήμμα 3.2.4). Στην περίπτωση όπου $\mathrm{supp}(\sigma) = \{1,..., n\}$, αρκεί να θέσουμε

$$c_j := \hat{d}_j,\ \forall j \in \{1,..., m\ (=: \nu)\}.$$

Στην περίπτωση όπου $\mathrm{supp}(\sigma) \subsetneqq \{1,..., n\}$, θεωρούμε το σύνολο

$$\{1,..., n\} \setminus \mathrm{supp}(\sigma) = \{\beta_1,..., \beta_\mu\}\ (\text{με } \mathrm{card}(\mathrm{supp}(\sigma)) = n - \mu)$$

και θέτουμε

$$c_j := \begin{cases} \left[\beta_j\right], & \text{όταν } j \in \{1,..., \mu\}, \\ \hat{d}_{j-\mu}, & \text{όταν } j \in \{\mu + 1,..., \mu + m\ (=: \nu)\}. \end{cases}$$

Σε αμφότερες τις περιπτώσεις θέτουμε $k_j := (\text{μήκος τού } c_j),\ \forall j \in \{1,..., \nu\}$. □

5.3.4 Ορισμός. (Ο «τύπος» μιας μετατάξεως.) Έστω $n \in \mathbb{N}$ και έστω $\sigma \in \mathfrak{S}_n$. Η μονοσημάντως ορισμένη ν-άδα

$$\boxed{\mathbf{tp}(\sigma) := (k_1, k_2,..., k_\nu) \in \ \Pi_\nu(n)}$$

που αντιστοιχίζεται στην σ μέσω τού λήμματος 5.3.3 ονομάζεται **τύπος τής** σ.

[17] Ενίοτε μια έκφραση τής σ αυτής τής μορφής καλείται **πλήρης παραγοντοποίηση** τής σ.

[18] Η επιλεγόμενη αναδιάταξη (που θα πληροί την επιθυμητή συνθήκη) δεν είναι κατ' ανάγκην μονοσημάντως ορισμένη!

5.3.5 Ορισμός. Έστω $n \in \mathbb{N}$. Εάν $\sigma, \tau \in \mathfrak{S}_n$, τότε λέμε ότι οι σ και τ **έχουν την ίδια δομή κύκλων** όταν $\exists \nu \in \{1,...,n\} : \mathbf{tp}(\sigma) \in \Pi_\nu(n), \mathbf{tp}(\tau) \in \Pi_\nu(n)$ και

$$\mathbf{tp}(\sigma) = \mathbf{tp}(\tau),$$

όπου η ισότητα αυτή νοείται «κατά συντεταγμένες».

5.3.6 Θεώρημα. *Έστω $n \in \mathbb{N}$. Για δυο μετατάξεις $\sigma, \tau \in \mathfrak{S}_n$ τα ακόλουθα είναι ισοδύναμα*:

(i) *Οι σ και τ είναι συζυγείς εντός τής $\mathfrak{S}_n$.*

(ii) *Οι σ και τ έχουν την ίδια δομή κύκλων.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν οι σ και τ είναι συζυγείς εντός τής $\mathfrak{S}_n$, τότε $\exists \vartheta \in \mathfrak{S}_n$, ούτως ώστε να ισχύει $\tau = \vartheta \circ \sigma \circ \vartheta^{-1}$. Γράφοντας την $\sigma \in \mathfrak{S}_n$ ως σύνθεση

$$\sigma = c_1 \circ c_2 \circ \cdots \circ c_\nu,\ c_j = \left[\alpha_{j1}\ \alpha_{j2} ... \ \alpha_{jk_j}\right],\ \forall j \in \{1,...,\nu\},$$

ν ανά δύο ξένων μεταξύ τους κύκλων $c_1, c_2, ..., c_\nu$ (όπως στην (5.15)) έχουσα τύπο

$$\mathbf{tp}(\sigma) = (k_1, k_2, ..., k_\nu) \in \quad \Pi_\nu(n),$$

για κάποιον (παγιωμένον) $\nu \in \{1,...,n\}$, παρατηρούμε ότι

$$\tau = \vartheta \circ c_1 \circ \cdots \circ c_\nu \circ \vartheta^{-1} = \left(\vartheta \circ c_1 \circ \vartheta^{-1}\right) \circ \cdots \circ \left(\vartheta \circ c_\nu \circ \vartheta^{-1}\right),$$

όπου για κάθε $j \in \{1,...,\nu\}$,

$$\vartheta \circ c_j \circ \vartheta^{-1} = \vartheta \circ \left[\alpha_{j1}\ \alpha_{j2} ... \ \alpha_{jk_j}\right] \circ \vartheta^{-1} = \left[\vartheta(\alpha_{j1})\ \vartheta(\alpha_{j2}) ... \ \vartheta(\alpha_{jk_j})\right]$$

(λόγω τού 3.2.3 (vii)), οπότε

$$\tau = [\vartheta(\alpha_{11}) ... \ \vartheta(\alpha_{1k_1})] \circ \cdots \circ [\vartheta(\alpha_{\nu 1}) ... \ \vartheta(\alpha_{\nu k_\nu})] \Rightarrow \mathbf{tp}(\tau) = \mathbf{tp}(\sigma).$$

(ii)⇒(i) Εάν οι μετατάξεις σ και τ έχουν την ίδια δομή κύκλων, τότε

$$\exists \nu \in \{1,...,n\} : \mathbf{tp}(\sigma), \mathbf{tp}(\tau) \in \Pi_\nu(n) \text{ και } \mathbf{tp}(\sigma) = \mathbf{tp}(\tau).$$

Γράφοντάς τες υπό τη μορφή συνθέσεων

$$\begin{cases} \sigma = c_1 \circ \cdots \circ c_\nu,\ c_j = [\alpha_{j1} ... \ \alpha_{jk_j}],\ \forall j \in \{1,...,\nu\}, \\ \tau = c'_1 \circ \cdots \circ c'_\nu,\ c'_j = [\beta_{j1} ... \ \beta_{jk_j}],\ \forall j \in \{1,...,\nu\}, \end{cases}$$

(όπως στην (5.15)) με $\bigcup_{j=1}^{\nu} \{\alpha_{j1}, \alpha_{j2}, ..., \alpha_{jk_j}\} = \bigcup_{j=1}^{\nu} \{\beta_{j1}, \beta_{j2}, ..., \beta_{jk_j}\} = \{1, 2, ..., n\}$, κατασκευάζουμε μια $\vartheta \in \mathfrak{S}_n$ μέσω τού τύπου $\vartheta(\alpha_{jl}) := \beta_{jl}$ για κάθε $j \in \{1,...,\nu\}$ και κάθε $l \in \{1,...,k_j\}$. Εκ κατασκευής, $\tau = \vartheta \circ \sigma \circ \vartheta^{-1}$. □

5.3.7 Πόρισμα. *Το πλήθος των κλάσεων συζυγίας τής συμμετρικής ομάδας $\mathfrak{S}_n$ ισούται με*

$$\boxed{\mathfrak{K}(\mathfrak{S}_n) = \varpi(n).}$$

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το θεώρημα 5.3.6 η κλάση συζυγίας (εντός τής $\mathfrak{S}_n$) οιασδήποτε μετατάξεως $\sigma \in \mathfrak{S}_n$ που έχει τύπο $\mathbf{tp}(\sigma) \in \Pi_\nu(n)$, για κάποιον $\nu \in \{1,...,n\}$, είναι η

$$\text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma) = \left\{ \tau \in \mathfrak{S}_n \,\middle|\, \tau \underset{\text{συζ.}}{\overset{\mathfrak{S}_n}{\sim}} \sigma \right\} = \{ \tau \in \mathfrak{S}_n \,|\mathbf{tp}(\tau) \in \Pi_\nu(n) \text{ και } \mathbf{tp}(\tau) = \mathbf{tp}(\sigma) \}.$$

Θέτοντας $\mathfrak{S}_{n,\nu} := \{ \sigma \in \mathfrak{S}_n \,|\mathbf{tp}(\sigma) \in \Pi_\nu(n) \}$, αποκτούμε μια αμφίρριψη

$$\{ \text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma) \,|\sigma \in \mathfrak{S}_{n,\nu} \} \ni \text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma) \longmapsto \mathbf{tp}(\sigma) \in \Pi_\nu(n)$$

για κάθε $\nu \in \{1,...,n\}$. Επειδή $\mathfrak{S}_n / \underset{\text{συζ.}}{\sim} = \bigcup_{\nu=1}^{n} \{ \text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma) \,|\sigma \in \mathfrak{S}_{n,\nu} \}$, προκύπτει τελικώς μια αμφίρριψη $\mathfrak{S}_n / \underset{\text{συζ.}}{\sim} \longrightarrow \Pi(n)$. □

5.3.8 Σημείωση. Εάν $n \in \mathbb{N}$, $n \geq 3$, και $G \sqsubseteq \mathfrak{S}_n$, τότε, σύμφωνα με ένα αποτέλεσμα τού A. Maróti (δημοσιευθέν το έτος[19] 2005), το πλήθος των κλάσεων συζυγίας τής G έχει το εξής άνω φράγμα:

$$\boxed{\mathfrak{K}(G) \leq 3^{\frac{n-1}{2}}.}$$

5.3.9 Παρατήρηση. Χρησιμοποιώντας τή γεννήτρια συνάρτηση (5.13) τού $\varpi(n)$ προσδιορίζουμε απευθείας το πλήθος των κλάσεων συζυγίας τής $\mathfrak{S}_n$. Επί παραδείγματι, για

$$n \in \{2,...,20\} \cup \{10\lambda \,|\lambda \in \{3,...,10\}\} \cup \{200\}$$

λαμβάνουμε

n	$\mathfrak{K}(\mathfrak{S}_n)$	n	$\mathfrak{K}(\mathfrak{S}_n)$
2	2	16	231
3	3	17	297
4	5	18	385
5	7	19	490
6	11	20	627
7	15	30	5604
8	22	40	37338
9	30	50	204226
10	42	60	966467
11	56	70	4087968
12	77	80	15796476
13	101	90	56634173
14	135	100	190569292
15	176	200	3972999029388

Ο πληθικός αριθμός τής κλάσεως συζυγίας $\text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma)$ και η τάξη τού κεντροποιητή $\mathrm{C}_{\mathfrak{S}_n}(\sigma)$ μιας μετατάξεως $\sigma \in \mathfrak{S}_n$ υπολογίζονται λεπτομερώς στο θεώρημα 5.3.16. Προτάσσονται τέσσερα απαραίτητα λήμματα καθαρώς *συνδυαστικής φύσεως*.

[19] Βλ. A. Maróti: *Bounding the number of conjugacy classes of a permutation group,* Journal of Group Th. **8** (2005), 273-289.

5.3.10 Ορισμός. Έστω $n \in \mathbb{N}$ και έστω $k \in \mathbb{N}$, $k \leq n$. Εάν το X είναι ένα σύνολο με n στοιχεία, τότε κάθε ενριπτική απεικόνιση $f : \{1, ..., k\} \longrightarrow X$ καλείται **διάταξη των n στοιχείων τού X ανά k**. (Είθισται να ταυτίζουμε κάθε διάταξη f των n στοιχείων τού X ανά k με τη *διατεταγμένη* k-άδα $(f(1), f(2),..., f(k)) \in X^k$.)

5.3.11 Λήμμα. *Έστω $n \in \mathbb{N}$ και έστω X ένα σύνολο με n στοιχεία. Εάν $k \in \mathbb{N}$, $k \leq n$, τότε το πλήθος των διατάξεων των n στοιχείων τού X ανά k ισούται με*

$$n(n-1)(n-2)\cdots(n-k+1).$$

ΑΠΟΔΕΙΞΗ. Έστω $\mathbf{Inj}(k; X) := \{f : \{1, ..., k\} \longrightarrow X \,|\, f \text{ ένριψη}\}$ το σύνολο των ενριπτικών απεικονίσεων από το $\{1, ..., k\}$ στο X. Προφανώς,

$$\text{card}(\mathbf{Inj}(k; X)) = \begin{cases} n, & \text{όταν } k = 1, \\ (n-k+1)\,\text{card}(\mathbf{Inj}(k-1; X)), & \text{όταν } k \geq 2. \end{cases}$$

Η απόδειξη τής ισότητας $\text{card}(\mathbf{Inj}(k; X)) = n(n-1)(n-2)\cdots(n-k+1)$ έπεται άμεσα κάνοντας χρήση μαθηματικής επαγωγής ως προς τον k. □

5.3.12 Ορισμός. Έστω $n \in \mathbb{N}$ και έστω $k \in \mathbb{N}$, $k \leq n$. Εάν το X είναι ένα σύνολο με n στοιχεία, τότε κάθε μη *διατεταγμένη* συλλογή $\{x_1,..., x_k\}$ k στοιχείων τού X καλείται **συνδυασμός των n στοιχείων τού X ανά k**.

5.3.13 Λήμμα. *Έστω $n \in \mathbb{N}$ και έστω X ένα σύνολο με n στοιχεία. Εάν $k \in \mathbb{N}$, $k \leq n$, τότε το πλήθος των συνδυασμών των n στοιχείων τού X ανά k ισούται με τον διωνυμικό συντελεστή* [20]

$$\tbinom{n}{k} := \frac{n!}{k!\,(n-k)!}.$$

ΑΠΟΔΕΙΞΗ. Ας συμβολίσουμε ως $\Sigma_k(X)$ το σύνολο των συνδυασμών n στοιχείων τού X ανά k. Ορίζουμε την απεικόνιση

$$\eta : \mathbf{Inj}(k; X) \longrightarrow \Sigma_k(X), \quad f \longmapsto \eta(f) := \{f(1), f(2),..., f(k)\}.$$

Προφανώς,

$$\mathbf{Inj}(k; X) = \coprod_{\{x_1,...,x_k\} \in \Sigma_k(X)} \eta^{-1}(\{x_1,..., x_k\})$$

και

$$\text{card}(\eta^{-1}(\{x_1,..., x_k\})) = |\mathfrak{S}_k|\,,$$

για κάθε $\{x_1,..., x_k\} \in \Sigma_k(X)$, διότι οι μετατάξεις

$$\begin{bmatrix} 1 & 2 & \cdots & k \\ \sigma(1) & \sigma(2) & \cdots & \sigma(k) \end{bmatrix} \in \mathfrak{S}_k$$

[20] Οι διωνυμικοί συντελεστές $\binom{n}{k}$ ορίζονται ακόμη και για *οιονδήποτε* $k \in \mathbb{Z}$, θέτοντας $\binom{n}{k} := 0$ όταν $k < 0$ ή $k > n$, και $\binom{n}{0} := 1$ (καθόσον $0! := 1$).

για τις οποίες ισχύει η (συνολοθεωρητική!) ισότητα

$$\{\sigma(1), \sigma(2), ..., \sigma(k)\} = \{x_1, ..., x_k\},$$

απεικονίζονται στη *μη διατεταγμένη* συλλογή $\{x_1, ..., x_k\}$. Δυνάμει τού λήμματος 5.3.11 και τής προτάσεως 3.1.3 ισχύουν οι ισότητες

$$\begin{aligned} & n(n-1)(n-2)\cdots(n-k+1) = \text{card}(\mathbf{Inj}(k; X)) \\ &= \sum_{\{x_1,..,x_k\}\in\Sigma_k(X)} \text{card}(\eta^{-1}(\{x_1, ..., x_k\})) = \text{card}(\Sigma_k(X)) \cdot |\mathfrak{S}_k| \\ &= \text{card}(\Sigma_k(X)) \cdot (k!), \end{aligned}$$

απ' όπου έπεται ότι $\text{card}(\Sigma_k(X)) = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \binom{n}{k}$. □

5.3.14 Λήμμα. *Έστω $n \in \mathbb{N}$ και έστω $k \in \{1, ..., n\}$. Για κάθε k-κύκλο $c \in \mathfrak{S}_n$ ο πληθικός αριθμός τής κλάσεως συζυγίας* $\text{ΚΛΣ}_{\mathfrak{S}_n}(c)$ *(ο οποίος, λόγω τού θεωρήματος* 5.3.6, *ισούται με το πλήθος όλων των k-κύκλων εντός τής $\mathfrak{S}_n$) είναι ο*

$$\boxed{\text{card}(\text{ΚΛΣ}_{\mathfrak{S}_n}(c)) = \binom{n}{k}(k-1)! = \frac{n!}{k\cdot((n-k)!)}.} \tag{5.16}$$

Ως εκ τούτου,

$$\boxed{|\mathbf{C}_{\mathfrak{S}_n}(c)| = k\cdot((n-k)!).} \tag{5.17}$$

ΑΠΟΔΕΙΞΗ. Για $n = 1$ οι (5.16) και (5.17) είναι προφανείς. Ας υποθέσουμε λοιπόν ότι $n \geq 2$.

Περίπτωση πρώτη. Υποθέτουμε ότι $k = n$. Σύμφωνα με το 3.2.3 (i) όλες οι «κυκλικές εναλλαγές» των n στοιχείων ενός n-κύκλου μάς δίδουν τον *ίδιον κύκλο*. Επομένως, για να προβούμε στην καταμέτρηση όλων των n-κύκλων εντός τής $\mathfrak{S}_n$ οφείλουμε να παγιώσουμε τη θέση *ενός* εκ των στοιχείων $1, 2, ..., n$ σε *κάθε έναν εξ αυτών* (ούτως ώστε να αποφευχθούν επαναλήψεις). Επί παραδείγματι, τοποθετώντας τόν n πάντοτε στην n-οστή θέση *καθενός εξ αυτών* λαμβάνουμε μονοσημάντως ορισμένες εκφράσεις τους. Κάθε n-κύκλος $[\alpha_1\ \alpha_2 ...\ \alpha_{n-1}\ n]$ δημιουργείται μέσω μιας μετατάξεως

$$\begin{bmatrix} 1 & 2 & \cdots & n-1 \\ a_1 & a_2 & \cdots & a_{n-1} \end{bmatrix}$$

των στοιχείων $1, 2, ..., n-1$. Επειδή υπάρχουν ακριβώς $(n-1)!$ μετατάξεις των στοιχείων $1, 2, ..., n-1$, το πλήθος όλων των n-κύκλων εντός τής $\mathfrak{S}_n$ (και, κατ' επέκταση, και ο πληθικός αριθμός τής κλάσεως συζυγίας καθενός εξ αυτών) ισούται με $(n-1)!$.

Περίπτωση δεύτερη. Εάν $k < n$, τότε, σύμφωνα με το λήμμα 5.3.13, υφίστανται $\binom{n}{k}$ υποσύνολα τού $\{1, ..., n\}$ με k στοιχεία. Από καθένα εξ αυτών των υποσυνόλων προκύπτουν $(k-1)!$ διαφορετικοί k-κύκλοι (όπως στην πρώτη περίπτωση), οπότε

το πλήθος όλων των k-κύκλων εντός τής $\mathfrak{S}_n$ (και, κατ' επέκταση, και ο πληθικός αριθμός τής κλάσεως συζυγίας καθενός εξ αυτών) ισούται με $\binom{n}{k}(k-1)!$.
Τέλος, η ισότητα (5.17) έπεται από την (5.16), το πόρισμα 5.2.10, το (iii) τής προτάσεως 4.4.2 και την πρόταση 3.1.3. □

5.3.15 Λήμμα. *Έστω $n \in \mathbb{N}$. Εάν $k, m \in \{1, ..., n\}$ είναι τέτοιοι, ώστε $km \leq n$, τότε υφίστανται ακριβώς*

$$\frac{n!}{k^m \cdot (m!) \cdot ((n-km)!)} \tag{5.18}$$

μετατάξεις $\sigma \in \mathfrak{S}_n$ οι οποίες γράφονται υπό τη μορφή επαλλήλων συνθέσεων

$$\sigma = c_1 \circ c_2 \circ \cdots \circ c_m$$

m ανά δύο ξένων μεταξύ τους κύκλων, καθένας εκ των οποίων έχει μήκος k.

ΑΠΟΔΕΙΞΗ. Θα εφαρμόσουμε μαθηματική επαγωγή ως προς τον m. Για $m = 1$ ο ισχυρισμός είναι αληθής επί τη βάσει τού λήμματος 5.3.14. Ας υποθέσουμε ότι είναι αληθής για κάποιον $m \in \mathbb{N}$ με $1 \leq m \leq \frac{n-k}{k}$. Τότε υπάρχουν

$$\frac{n!}{k^m \cdot (m!) \cdot ((n-km)!)}$$

στοιχεία τής $\mathfrak{S}_n$ που γράφονται υπό τη μορφή επαλλήλων συνθέσεων m ανά δύο ξένων μεταξύ τους κύκλων, καθένας εκ των οποίων έχει μήκος k. Ως εκ τούτου, το πλήθος των στοιχείων τής $\mathfrak{S}_n$ που γράφονται υπό τη μορφή επαλλήλων συνθέσεων $m+1$ ανά δύο ξένων μεταξύ τους κύκλων μήκους k ισούται με

$$\left(\tfrac{n!}{k^m \cdot (m!) \cdot ((n-km)!)}\right) \cdot \left(\tfrac{1}{m+1}\binom{n-km}{k}(k-1)!\right) = \tfrac{n!}{k^{m+1} \cdot ((m+1)!) \cdot ((n-k(m+1))!)},$$

με τον πρώτο παράγοντα τού αριστερού μέλους τής ανωτέρω ισότητας προερχόμενο από την επαγωγική μας υπόθεση και τον δεύτερο παράγοντα εκφράζοντα το πλήθος των k-κύκλων που σχηματίζονται από τα εναπομένοντα $n - km$ στοιχεία τού $\{1,...,n\}$, *διαιρούμενο διά τού* $m+1$, διότι συνθέτοντας κάθε μία εκ των $\frac{n!}{k^m \cdot (m!) \cdot ((n-km)!)}$ αρχικώς θεωρηθεισών μετατάξεων τής μορφής $c_1 \circ c_2 \circ \cdots \circ c_m$ με έναν επιπρόσθετο κύκλο c_{m+1} μήκους k με

$$\operatorname{supp}(c_1 \circ c_2 \circ \cdots \circ c_m) \cap \operatorname{supp}(c_{m+1}) = \varnothing,$$

οφείλουμε να λάβουμε υπ' όψιν ότι

$$\begin{aligned}
(c_1 \circ c_2 \circ \cdots \circ c_{m-1} \circ c_m) \circ c_{m+1} &= (c_1 \circ c_2 \circ \cdots \circ c_{m-1}) \circ c_{m+1} \circ c_m \\
&= (c_1 \circ c_2 \circ \cdots \circ c_{m-2}) \circ c_{m+1} \circ (c_{m-1} \circ c_m) \\
&= \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&= c_1 \circ c_{m+1} \circ (c_2 \circ \cdots \circ c_{m-1} \circ c_m) \\
&= c_{m+1} \circ (c_1 \circ c_2 \circ \cdots \circ c_{m-1} \circ c_m),
\end{aligned}$$

ήτοι ότι εμφανίζονται ακριβώς $m+1$ μετατάξεις που είναι ίσες μεταξύ τους. Άρα ο ισχυρισμός είναι αληθής και για τον $m+1$. □

5.3.16 Θεώρημα. *Έστω $n \in \mathbb{N}$ και έστω τυχούσα μετάταξη $\sigma \in \mathfrak{S}_n$. Εάν*

$$\mathbf{tp}(\sigma) = (k_1, k_2, ..., k_\nu) \in \quad \Pi_\nu(n)\,,$$

τότε ο πληθικός αριθμός τής κλάσεως συζυγίας $\text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma)$ και η τάξη τού κεντροποιητή $\mathrm{C}_{\mathfrak{S}_n}(\sigma)$ τής σ υπολογίζονται ως ακολούθως:

(i) *Εάν $k_1 = k_2 = \cdots = k_\nu =: k$, τότε*

$$\boxed{\text{card}(\text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma)) = \frac{n!}{k^\nu \cdot (\nu!)}.} \tag{5.19}$$

Ως εκ τούτου,

$$\boxed{|\mathrm{C}_{\mathfrak{S}_n}(\sigma)| = k^\nu \cdot (\nu!)\,.} \tag{5.20}$$

(ii) *Εάν $\nu \geq 2$ και εάν τουλάχιστον δύο εκ των μηκών $k_1, ..., k_\nu$ είναι διαφορετικά, τότε θεωρώντας εκείνο το (μονοσημάντως καθοριζόμενο) υποσύνολο δεικτών $\{\varrho_1, ..., \varrho_s\} \subseteq \{1, ..., \nu\}$ (με $s \geq 2$ και $\varrho_1 \geq 1$, $\varrho_s = \nu$) για το οποίο ισχύει*

$$k_1 = \cdots = k_{\varrho_1} < k_{\varrho_1+1} = \cdots = k_{\varrho_2} < \cdots\cdots < k_{\varrho_{s-1}+1} = \cdots = k_{\varrho_s} = k_\nu$$

και ορίζοντας τους αριθμούς $\varrho_0 := 0$ και $\lambda_j := \varrho_j - \varrho_{j-1}$, $\forall j \in \{1, ..., s\}$, καταλήγουμε στις

$$\boxed{\text{card}(\text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma)) = \frac{n!}{k_{\varrho_1}^{\lambda_1}(\lambda_1!)\, k_{\varrho_2}^{\lambda_2}(\lambda_2!)\ \cdots\ k_{\varrho_s}^{\lambda_s}(\lambda_s!)}.} \tag{5.21}$$

και

$$\boxed{|\mathrm{C}_{\mathfrak{S}_n}(\sigma)| = k_{\varrho_1}^{\lambda_1}(\lambda_1!)\, k_{\varrho_2}^{\lambda_2}(\lambda_2!)\ \cdots\ k_{\varrho_s}^{\lambda_s}(\lambda_s!)\,.} \tag{5.22}$$

ΑΠΟΔΕΙΞΗ. Στην περίπτωση (i) ο πληθικός αριθμός τής κλάσεως συζυγίας $\text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma)$ ισούται, λόγω τού θεωρήματος 5.3.6, με το πλήθος των στοιχείων τής $\mathfrak{S}_n$ που γράφονται υπό τη μορφή επαλλήλων συνθέσεων ν ανά δύο ξένων μεταξύ τους κύκλων μήκους k, όπου $k\nu = n$, οπότε το δεξιό μέλος τής (5.19) δεν είναι τίποτα άλλο παρά ο αριθμός (5.18) για $\nu = m$. Η (5.20) έπεται από την (5.19), το πόρισμα 5.2.10, το (iii) τής προτάσεως 4.4.2 και την πρόταση 3.1.3. Στην περίπτωση (ii) έχουμε

$$k_{\varrho_1}\lambda_1 + k_{\varrho_2}\lambda_2 + \ \cdots + \ k_{\varrho_s}\lambda_s = n$$

και η μετάταξη σ είναι εξ ορισμού τής μορφής

$$\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_s,$$

όπου οι $\sigma_1, ..., \sigma_s \in \mathfrak{S}_n$ είναι ανά δύο ξένες μεταξύ τους μετατάξεις και για κάθε δείκτη $j \in \{1, ..., s\}$ η σ_j είναι η σύνθεση

$$\sigma_j = c_{j1} \circ c_{j2} \circ \cdots \circ c_{j\lambda_j}$$

λ_j ανά δύο ξένων μεταξύ τους κύκλων $c_{j1}, ..., c_{j\lambda_j} \in \mathfrak{S}_n$ με

$$\text{μήκος}(c_{j\mu}) = k_{\varrho_j}, \ \ \forall \mu \in \{1,..., \lambda_j\}.$$

Έστω $A_j := \text{supp}(\sigma_j), \forall j \in \{1,..., s\}$. Για κάθε $\vartheta \in \mathrm{C}_{\mathfrak{S}_n}(\sigma)$ έχουμε

$$\vartheta \circ \sigma = \sigma \circ \vartheta \Rightarrow \sigma = \vartheta \circ \sigma \circ \vartheta^{-1}$$
$$\Rightarrow \sigma = \left(\vartheta \circ \sigma_1 \circ \vartheta^{-1}\right) \circ \left(\vartheta \circ \sigma_2 \circ \vartheta^{-1}\right) \circ \cdots \circ \left(\vartheta \circ \sigma_\nu \circ \vartheta^{-1}\right),$$

όπου

$$\vartheta \circ \sigma_j \circ \vartheta^{-1} = \left(\vartheta \circ c_{j1} \circ \vartheta^{-1}\right) \circ \left(\vartheta \circ c_{j2} \circ \vartheta^{-1}\right) \circ \cdots \circ \left(\vartheta \circ c_{j\lambda_j} \circ \vartheta^{-1}\right),$$

για κάθε $j \in \{1,..., s\}$ και όπου η $\vartheta \circ c_{j\mu} \circ \vartheta^{-1}$ είναι ένας k_{ϱ_j}-κύκλος με

$$\text{supp}(\vartheta \circ c_{j\mu} \circ \vartheta^{-1}) = \text{supp}(c_{j\mu}), \ \ \forall \mu \in \{1,..., \lambda_j\}.$$

Κατά συνέπειαν, για κάθε $j \in \{1,..., s\}$ ο περιορισμός $\vartheta|_{A_j}$ τής ϑ επί τού A_j είναι μια αμφίρριψη από το A_j επί τού ιδίου τού A_j, οπότε $\vartheta|_{A_j} \in \mathfrak{S}_{A_j}$ (με $\mathfrak{S}_{A_j} \cong \mathfrak{S}_{k_{\varrho_j}\lambda_j}$) και, επιπροσθέτως, $\vartheta|_{A_j} \in \mathrm{C}_{\mathfrak{S}_{A_j}}(\sigma|_{A_j})$. Μέσω τού θεωρήματος 5.3.6 συνάγεται ότι η απεικόνιση

$$\mathrm{C}_{\mathfrak{S}_n}(\sigma) \longrightarrow \mathrm{C}_{\mathfrak{S}_{A_1}}(\sigma|_{A_1}) \times \mathrm{C}_{\mathfrak{S}_{A_2}}(\sigma|_{A_2}) \times \cdots \times \mathrm{C}_{\mathfrak{S}_{A_s}}(\sigma|_{A_s})$$
$$\vartheta \longmapsto \left(\vartheta|_{A_1}, \vartheta|_{A_2}, ..., \vartheta|_{A_s}\right)$$

είναι αμφιρριπτική. Ως εκ τούτου,

$$|\mathrm{C}_{\mathfrak{S}_n}(\sigma)| = \prod_{j=1}^{s} \left|\mathrm{C}_{\mathfrak{S}_{A_j}}(\sigma|_{A_j})\right|. \tag{5.23}$$

Επειδή $\sigma|_{A_j} = \text{id}_{\{1,..,n\}}\big|_{A_j} \circ \sigma_j \circ \iota \in \mathfrak{S}_{A_j}$ ($\cong \mathfrak{S}_{k_{\varrho_j}\lambda_j}$), όπου $\iota : A_j \hookrightarrow \{1, ..., n\}$ η συνήθης ένθεση, η $\sigma|_{A_j}$ γράφεται υπό τη μορφή επαλλήλων συνθέσεων λ_j ανά δύο ξένων μεταξύ τους κύκλων μήκους k_{ϱ_j} *εντός τής* $\mathfrak{S}_{A_j}$. Άρα η τάξη τού κεντροποιητή $\mathrm{C}_{\mathfrak{S}_{A_j}}(\sigma|_{A_j})$ υπολογίζεται όπως στην περίπτωση (i) (με τον $k_{\varrho_j}\lambda_j$ στη θέση τού n και με την $\sigma|_{A_j}$ στη θέση τής σ):

$$\left|\mathrm{C}_{\mathfrak{S}_{A_j}}(\sigma|_{A_j})\right| = k_{\varrho_j}^{\lambda_j}(\lambda_j!), \ \forall j \in \{1,..., s\}. \tag{5.24}$$

Η (5.22) έπεται άμεσα από τις (5.23) και (5.24). Τέλος, η (5.21) έπεται από την (5.22), το πόρισμα 5.2.10, το (iii) τής προτάσεως 4.4.2 και την πρόταση 3.1.3. □

5.3.17 Παραδείγματα. Για τη σύνταξη τού καταλόγου των κλάσεων συζυγίας τής $\mathfrak{S}_n$ (για κάποιον αρκούντως μικρό n) εκκινούμε από τις διαμερίσεις τού n. Σε κάθε διαμέριση τού n αντιστοιχίζεται μία και μόνον κλάση συζυγίας (βλ. 5.3.7). Η τάξη καθενός στοιχείου ανήκοντος σε μία κλάση συζυγίας προσδιορίζεται από το πόρισμα 3.2.10, ο δε πληθικός αριθμός τής εκάστοτε θεωρούμενης κλάσεως συζυγίας (στη στήλη υπό το "♯") από τις (5.16), (5.19) και (5.21). Για τον προσδιορισμό *ενός*

εκπροσώπου καθεμιάς εκ των κλάσεων συζυγίας, ήτοι για την εύρεση ενός (ομοιογενώς συγκροτούμενου) πλήρους συστήματος εκπροσώπων Ξ_n τής $\mathfrak{S}_n$ ως προς την "$\underset{\text{συζ.}}{\sim}$", χρησιμοποιούμε την εξής μέθοδο: Για κάθε $\nu \in \{1,...,n\}$ εφοδιάζουμε το σύνολο $\Pi_\nu\,(n)$ (και, κατ' επέκταση, και τους τύπους των αντιστοίχων μετατάξεων) με τη *λεξικογραφική διάταξη* "$\preccurlyeq_{\text{λεξ.}}$":

$$(k_1,...,k_\nu) \preccurlyeq_{\text{λεξ.}} (k'_1,...,k'_\nu) \underset{\text{ορσ}}{\Longleftrightarrow} \left\{ \begin{array}{c} \text{είτε } k_1 \leq k'_1 \text{ είτε } \exists i \in \{2,..,\nu\}\text{:} \\ k_1 = k'_1,...,k_{i-1} = k'_{i-1}, k_i \leq k'_i \end{array} \right\}$$

Αυτή είναι σχέση *ολικής* διατάξεως. Για $n \geq 2$, $\nu \in \{1,...,n-1\}$, συμβολίζουμε ως

$$(\kappa_1,...,\kappa_\nu) := \min{}_{\preccurlyeq_{\text{λεξ.}}} \{\mathbf{tp}(\sigma)\,|\sigma \in \mathfrak{S}_{n,\nu}\}$$

το ελάχιστο στοιχείο τού $\{\mathbf{tp}(\sigma)\,|\sigma \in \mathfrak{S}_{n,\nu}\}$ ως προς την "$\preccurlyeq_{\text{λεξ.}}$" (βλ. A.2.14 (ii)). Εάν $\kappa_1 \geq 2$, τότε εντάσσουμε τον n-κύκλο $[1\ 2...\ n]$, όταν $\nu = 1$, και τη μετάταξη

$$[1\ 2...\ \kappa_1] \circ [\kappa_1+1\ \kappa_1+2...\ \kappa_1+\kappa_2] \circ \cdots \circ \left[(\sum_{j=1}^{\nu-1} \kappa_j)+1...\ \sum_{j=1}^{\nu} \kappa_j\right],$$

όταν $\nu \geq 2$, στο (υπό κατασκευήν ευρισκόμενο) σύνολο Ξ_n. Εάν $\kappa_1 = 1$, τότε θεωρούμε τον δείκτη $\varrho := \min\{j \in \{1,...,\nu\}\,|\kappa_j \geq 2\}$ και εντάσσουμε (κατ' αναλογίαν) τον ν-κύκλο $[1\ 2...\ \kappa_\nu]$, όταν $\varrho = \nu$, και τη μετάταξη

$$[1\ 2...\ \kappa_\varrho] \circ [\kappa_\varrho+1\ \kappa_\varrho+2...\ \kappa_\varrho+\kappa_{\varrho+1}] \circ \cdots \circ \left[(\sum_{j=\varrho}^{\nu-1} \kappa_j)+1...\ \sum_{j=\varrho}^{\nu} \kappa_j\right],$$

όταν $\varrho < \nu$, στο σύνολο Ξ_n. Κατόπιν τούτου επιλέγουμε το ελάχιστο στοιχείο

$$\min{}_{\preccurlyeq_{\text{λεξ.}}} (\{\mathbf{tp}(\sigma)\,|\sigma \in \mathfrak{S}_{n,\nu}\} \setminus \{(\kappa_1,...,\kappa_\nu)\})$$

και επαναλαμβάνουμε την ανωτέρω διαδικασία με αυτήν τη νέα ν-άδα στη θέση τής ν-άδας $(\kappa_1,...,\kappa_\nu)$. Ύστερα από πεπερασμένου πλήθους βήματα (και την προσάρτηση τής ταυτοτικής σε αυτό) κατασκευάζουμε με την ίδια επιχειρηματολογία ολόκληρο το Ξ_n. Ως παραδείγματα παραθέτουμε τους καταλόγους των κατ' αυτόν τον τρόπο επιλεχθέντων εκπροσώπων των κλάσεων συζυγίας τής συμμετρικής ομάδας $\mathfrak{S}_n$ για $n \in \{3,4,5,6\}$. (Στην τελευταία στήλη αναφέρεται και το *είδος* των καταχωριζόμενων μετατάξεων, ήτοι το ποιες εξ αυτών είναι *άρτιες* και ποιες *περιττές*.)

► **Κατάλογος εκπροσώπων των κλάσεων συζυγίας τής** $\mathfrak{S}_3$:

Διαμερίσεις τού 3
$1+1+1$
$1+2$
3

εκπρ.	**τάξη**	♯	**είδος**
id	1	1	άρτια
[1 2]	2	3	περιττή
[1 2 3]	3	2	άρτια

► **Κατάλογος εκπροσώπων των κλάσεων συζυγίας τής** $\mathfrak{S}_4$:

Διαμερίσεις τού 4
$1+1+1+1$
$1+1+2$
$1+3$
$2+2$
4

εκπρ.	**τάξη**	♯	**είδος**
id	1	1	άρτια
[1 2]	2	6	περιττή
[1 2 3]	3	8	άρτια
[1 2] ∘ [3 4]	2	3	άρτια
[1 2 3 4]	4	6	περιττή

► **Κατάλογος εκπροσώπων των κλάσεων συζυγίας τής** $\mathfrak{S}_5$:

Διαμερίσεις τού 5
$1+1+1+1+1$
$1+1+1+2$
$1+1+3$
$1+2+2$
$1+4$
$2+3$
5

εκπρ.	**τάξη**	♯	**είδος**
id	1	1	άρτια
[1 2]	2	10	περιττή
[1 2 3]	3	20	άρτια
[1 2] ∘ [3 4]	2	15	άρτια
[1 2 3 4]	4	30	περιττή
[1 2] ∘ [3 4 5]	6	20	περιττή
[1 2 3 4 5]	5	24	άρτια

► **Κατάλογος εκπροσώπων των κλάσεων συζυγίας τής** $\mathfrak{S}_6$: Υπάρχουν εν συνόλω 11 διαμερίσεις τού αριθμού 6,

Διαμερίσεις τού 6 [I]	**Διαμερίσεις τού 6 [II]**
$1+1+1+1+1+1$	$1+5$
$1+1+1+1+2$	$2+2+2$
$1+1+1+3$	$2+4$
$1+1+2+2$	$3+3$
$1+1+4$	6
$1+2+3$	

οπότε ο ζητούμενος κατάλογος είναι ο εξής:

εκπρ.	**τάξη**	♯	**είδος**
id	1	1	άρτια
[1 2]	2	15	περιττή
[1 2 3]	3	40	άρτια
[1 2] ∘ [3 4]	2	45	άρτια
[1 2 3 4]	4	90	περιττή
[1 2] ∘ [3 4 5]	6	120	περιττή
[1 2 3 4 5]	5	144	άρτια
[1 2] ∘ [3 4] ∘ [5 6]	2	15	περιττή
[1 2] ∘ [3 4 5 6]	4	90	άρτια
[1 2 3] ∘ [4 5 6]	3	40	άρτια
[1 2 3 4 5 6]	6	120	περιττή

► **Τρόπος προσδιορισμού των κλάσεων συζυγίας τής $\mathfrak{A}_n$.** Έστω $n \in \mathbb{N}$, $n \geq 2$. Τότε οι κλάσεις συζυγίας τής εναλλάσσουσας ομάδας $\mathfrak{A}_n$ (και η επιλογή ενός εκπροσώπου καθεμιάς εξ αυτών) μελετώνται με τη βοήθεια των κλάσεων συζυγίας τής $\mathfrak{S}_n$. Συγκεκριμένα, το θεώρημα 5.3.19 μας δίδει ικανές και αναγκές συνθήκες υπό τις οποίες η κλάση ισοδυναμίας μιας μετατάξεως $\sigma \in \mathfrak{A}_n$ *εντός τής* $\mathfrak{S}_n$ ισούται με την κλάση ισοδυναμίας τής σ *εντός τής* $\mathfrak{A}_n$ και μας πληροφορεί, στην περίπτωση κατά την οποία ισχύει ο γνήσιος εγκλεισμός $\text{ΚΛΣ}_{\mathfrak{A}_n}(\sigma) \subsetneqq \text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma)$, ότι η $\text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma)$ διασπάται σε δύο ισοπληθείς κλάσεις συζυγίας τής $\mathfrak{A}_n$. Για την απόδειξή του απαιτείται το ακόλουθο:

5.3.18 Λήμμα. *Έστω $n \in \mathbb{N}$, $n \geq 2$, και έστω $\sigma \in \mathfrak{A}_n$. Τότε ισχύουν τα εξής*:
(i) $\mathrm{C}_{\mathfrak{A}_n}(\sigma) = \mathrm{C}_{\mathfrak{S}_n}(\sigma) \cap \mathfrak{A}_n \sqsubseteq \mathrm{C}_{\mathfrak{S}_n}(\sigma)$.
(ii) $|\mathrm{C}_{\mathfrak{S}_n}(\sigma) : \mathrm{C}_{\mathfrak{A}_n}(\sigma)| \in \{1, 2\}$ *και*

$$|\mathrm{C}_{\mathfrak{S}_n}(\sigma) : \mathrm{C}_{\mathfrak{A}_n}(\sigma)| = 1 \Leftrightarrow \mathrm{C}_{\mathfrak{S}_n}(\sigma) = \mathrm{C}_{\mathfrak{A}_n}(\sigma) \Leftrightarrow \mathrm{C}_{\mathfrak{S}_n}(\sigma) \sqsubseteq \mathfrak{A}_n. \tag{5.25}$$

(iii) $\text{ΚΛΣ}_{\mathfrak{A}_n}(\sigma) = \text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma) \Leftrightarrow |\mathrm{C}_{\mathfrak{A}_n}(\sigma)| = \frac{1}{2}\,|\mathrm{C}_{\mathfrak{S}_n}(\sigma)| \Leftrightarrow \mathrm{C}_{\mathfrak{S}_n}(\sigma) \nsubseteq \mathfrak{A}_n$.

ΑΠΟΔΕΙΞΗ. (i) Τούτο έπεται άμεσα από το 5.2.2 (iv).
(ii) Από το (i), το 4.4.2 (iii), το θεώρημα 4.5.9, την πρόταση 3.1.3 και την πρόταση 3.3.9 συνάγεται ότι

$$\begin{aligned} |\mathrm{C}_{\mathfrak{S}_n}(\sigma) : \mathrm{C}_{\mathfrak{A}_n}(\sigma)| &= |\mathrm{C}_{\mathfrak{S}_n}(\sigma) : \mathrm{C}_{\mathfrak{S}_n}(\sigma) \cap \mathfrak{A}_n| = \frac{|\mathrm{C}_{\mathfrak{S}_n}(\sigma)|}{|\mathrm{C}_{\mathfrak{S}_n}(\sigma) \cap \mathfrak{A}_n|} \\ &= \frac{\mathrm{card}(\mathrm{C}_{\mathfrak{S}_n}(\sigma)\mathfrak{A}_n)}{|\mathfrak{A}_n|} \leq \frac{|\mathfrak{S}_n|}{|\mathfrak{A}_n|} = |\mathfrak{S}_n : \mathfrak{A}_n| = 2, \end{aligned}$$

οπότε $|\mathrm{C}_{\mathfrak{S}_n}(\sigma) : \mathrm{C}_{\mathfrak{A}_n}(\sigma)| \in \{1, 2\}$. Οι αμφίπλευρες συνεπαγωγές (5.25) είναι προφανείς.
(iii) Από το πόρισμα 5.2.10, το 4.4.2 (iii), την πρόταση 3.1.3 και την πρόταση 3.3.9 έπονται οι ισότητες

$$\mathrm{card}(\text{ΚΛΣ}_{\mathfrak{A}_n}(\sigma)) = \frac{|\mathfrak{A}_n|}{|\mathrm{C}_{\mathfrak{A}_n}(\sigma)|} = \frac{n!}{2\,|\mathrm{C}_{\mathfrak{A}_n}(\sigma)|},\ \mathrm{card}(\text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma)) = \frac{|\mathfrak{S}_n|}{|\mathrm{C}_{\mathfrak{S}_n}(\sigma)|} = \frac{n!}{|\mathrm{C}_{\mathfrak{S}_n}(\sigma)|},$$

οπότε

$$\mathrm{card}(\text{ΚΛΣ}_{\mathfrak{A}_n}(\sigma))\,|\mathrm{C}_{\mathfrak{A}_n}(\sigma)| = \frac{1}{2}\mathrm{card}(\text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma))\,|\mathrm{C}_{\mathfrak{S}_n}(\sigma)|\,. \tag{5.26}$$

Εάν $\text{ΚΛΣ}_{\mathfrak{A}_n}(\sigma) = \text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma)$, τότε η (5.26) δίδει

$$|\mathrm{C}_{\mathfrak{A}_n}(\sigma)| = \frac{1}{2}\,|\mathrm{C}_{\mathfrak{S}_n}(\sigma)| \Rightarrow |\mathrm{C}_{\mathfrak{S}_n}(\sigma) : \mathrm{C}_{\mathfrak{A}_n}(\sigma)| = 2 \underset{(5.25)}{\Longrightarrow} \mathrm{C}_{\mathfrak{S}_n}(\sigma) \nsubseteq \mathfrak{A}_n.$$

Και αντιστρόφως· εάν $\mathrm{C}_{\mathfrak{S}_n}(\sigma) \nsubseteq \mathfrak{A}_n$, τότε (μέσω τού (ii)) συνάγεται ότι

$$|\mathrm{C}_{\mathfrak{A}_n}(\sigma)| = \frac{1}{2}\,|\mathrm{C}_{\mathfrak{S}_n}(\sigma)| \underset{(5.26)}{\Longrightarrow} \mathrm{card}(\text{ΚΛΣ}_{\mathfrak{A}_n}(\sigma)) = \mathrm{card}(\text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma)),$$

Επειδή $\text{ΚΛΣ}_{\mathfrak{A}_n}(\sigma) \subseteq \text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma)$, έχουμε $\text{ΚΛΣ}_{\mathfrak{A}_n}(\sigma) = \text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma)$. □

5.3.19 Θεώρημα. (Περί των κλάσεων συζυγίας τής $\mathfrak{A}_n$.) *Έστω $n \in \mathbb{N}, n \geq 2$, και έστω $\sigma \in \mathfrak{A}_n$. Εάν*

$$\mathbf{tp}(\sigma) = (k_1, k_2, ..., k_\nu) \in \Pi_\nu(n),$$

τότε ισχύουν τα ακόλουθα:
(i) *Εάν $k_1 = k_2 = \cdots = k_\nu =: k$, τότε*

$$\boxed{\text{ΚΛΣ}_{\mathfrak{A}_n}(\sigma) = \text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma) \Leftrightarrow \left\{ \begin{array}{c} \text{είτε } [\nu = 1 \text{ και } k = n \equiv 0(\mathrm{mod}\, 2)] \\ \text{είτε } \nu \geq 2 \end{array} \right\}.}$$

(ii) *Εάν $\nu \geq 2$ και εάν τουλάχιστον δύο εκ των μηκών $k_1, ..., k_\nu$ είναι διαφορετικά, τότε θεωρώντας εκείνο το (μονοσημάντως καθοριζόμενο) υποσύνολο δεικτών $\{\varrho_1, ..., \varrho_s\} \subseteq \{1, ..., \nu\}$ (με $s \geq 2$ και $\varrho_1 \geq 1$, $\varrho_s = \nu$) για το οποίο ισχύει*

$$k_1 = \cdots = k_{\varrho_1} < k_{\varrho_1+1} = \cdots = k_{\varrho_2} < \cdots\cdots < k_{\varrho_{s-1}+1} = \cdots = k_{\varrho_s} = k_\nu$$

και ορίζοντας τους αριθμούς $\varrho_0 := 0$ και $\lambda_j := \varrho_j - \varrho_{j-1}$, $\forall j \in \{1, ..., s\}$, καταλήγουμε στην αμφίπλευρη συνεπαγωγή

$$\boxed{\text{ΚΛΣ}_{\mathfrak{A}_n}(\sigma) = \text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma) \Leftrightarrow \left\{ \begin{array}{c} \text{είτε } \mathrm{card}(\{ j \in \{1, ..., s\} \,|\, k_{\varrho_j} \equiv 0(\mathrm{mod}\, 2) \}) \geq 1 \\ \text{είτε } \exists j \in \{1, ..., s\} : \lambda_j \geq 2 \end{array} \right\},}$$

δηλαδή στο ότι η κλάση συζυγίας τής σ εντός τής $\mathfrak{A}_n$ ταυτίζεται με την κλάση συζυγίας της εντός τής $\mathfrak{S}_n$ εάν και μόνον εάν στην έκφραση (5.15) *τής σ ως συνθέσεως ν ανά δύο ξένων μεταξύ τους κύκλων εμφανίζεται είτε τουλάχιστον ένας κύκλος αρτίου μήκους είτε τουλάχιστον δύο κύκλοι ιδίου μήκους.*
(iii) *Εάν $\text{ΚΛΣ}_{\mathfrak{A}_n}(\sigma) \subsetneqq \text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma)$, τότε για κάθε $\tau \in \text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma) \setminus \text{ΚΛΣ}_{\mathfrak{A}_n}(\sigma)$ έχουμε*

$$\boxed{\text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma) = \text{ΚΛΣ}_{\mathfrak{A}_n}(\sigma) \coprod \text{ΚΛΣ}_{\mathfrak{A}_n}(\tau),} \tag{5.27}$$

όπου

$$\boxed{\mathrm{card}(\text{ΚΛΣ}_{\mathfrak{A}_n}(\sigma)) = \mathrm{card}(\text{ΚΛΣ}_{\mathfrak{A}_n}(\tau)) = \frac{\mathrm{card}(\text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma))}{2},} \tag{5.28}$$

δηλαδή η κλάση συζυγίας τής σ εντός τής $\mathfrak{S}_n$ διασπάται σε δύο ισοπληθείς κλάσεις συζυγίας τής $\mathfrak{A}_n$.

ΑΠΟΔΕΙΞΗ. (i) Εάν $\text{ΚΛΣ}_{\mathfrak{A}_n}(\sigma) = \text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma)$, τότε κατά το 5.3.18 (iii),

$$|\mathrm{C}_{\mathfrak{A}_n}(\sigma)| = \frac{1}{2} |\mathrm{C}_{\mathfrak{S}_n}(\sigma)| \underset{(5.20)}{\Longrightarrow} k^\nu \cdot (\nu!) = |\mathrm{C}_{\mathfrak{S}_n}(\sigma)| \equiv 0(\mathrm{mod}\, 2),$$

απ' όπου έπεται ότι είτε [$\nu = 1$ και $k = n$ άρτιος] είτε $\nu \geq 2$. Και αντιστρόφως· εάν $\nu = 1$ και ο $k = n$ είναι άρτιος, τότε η $\sigma \in \mathrm{C}_{\mathfrak{S}_n}(\sigma)$ είναι ένας n-κύκλος. Όμως κάθε κύκλος αρτίου μήκους είναι μια περιττή μετάταξη (βλ. 3.3.5 (iii)). Ως εκ τούτου, $\sigma \in \mathfrak{S}_n \setminus \mathfrak{A}_n$ και

$$\mathrm{C}_{\mathfrak{S}_n}(\sigma) \nsubseteqq \mathfrak{A}_n \underset{5.3.18\,\text{(iii)}}{\Longrightarrow} \text{ΚΛΣ}_{\mathfrak{A}_n}(\sigma) = \text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma).$$

Εν συνεχεία υποθέτουμε ότι $\nu \geq 2$ και $k\nu = n$. Προφανώς,

$$\text{sgn}\,(\sigma) = (-1)^{(k-1)\nu} = (-1)^{n-\nu}\,.$$

Στην περίπτωση όπου ο k είναι *άρτιος* και ο ν *περιττός* χρησιμοποιούμε εκ νέου την προηγηθείσα επιχειρηματολογία. Στην περίπτωση όπου ο k είναι *περιττός* και ο ν *οιοσδήποτε* φυσικός αριθμός ≥ 2 γράφουμε την σ υπό τη μορφή επαλλήλων συνθέσεων $\sigma = c_1 \circ c_2 \circ \cdots \circ c_\nu$ ανά δύο ξένων μεταξύ τους κύκλων $c_1,...,c_\nu$ μήκους k. Εάν

$$c_1 = [\alpha_1 \ldots \alpha_k]\,,\ c_2 = [\beta_1 \ldots \beta_k]\,,$$

θέτουμε $d := [\alpha_1\ \beta_1] \circ [\alpha_2\ \beta_2] \circ \cdots \circ [\alpha_k\ \beta_k]$ και παρατηρούμε ότι

$$(c_1 \circ c_2) \circ d = d \circ (c_1 \circ c_2)\,. \tag{5.29}$$

Επιπροσθέτως, επειδή $\text{supp}(d) \cap \text{supp}(c_3 \circ \cdots \circ c_\nu) = \varnothing$ (όταν $\nu \geq 3$), έχουμε

$$(c_3 \circ \cdots \circ c_\nu) \circ d = d \circ (c_3 \circ \cdots \circ c_\nu). \tag{5.30}$$

Από τις (5.29) και (5.30) λαμβάνουμε

$$\begin{aligned} \sigma \circ d &= (c_1 \circ c_2) \circ (c_3 \circ \cdots \circ c_\nu) \circ d \\ &= (c_1 \circ c_2) \circ d \circ (c_3 \circ \cdots \circ c_\nu) \\ &= d \circ (c_1 \circ c_2 \circ \cdots \circ c_\nu) = d \circ \sigma, \end{aligned}$$

οπότε $d \in \mathrm{C}_{\mathfrak{S}_n}(\sigma)$ με $\text{sgn}(d) = (-1)^k = -1$ (βλ. 3.3.5 (iii)). Κατά συνέπειαν,

$$d \in \mathfrak{S}_n \setminus \mathfrak{A}_n \Rightarrow \mathrm{C}_{\mathfrak{S}_n}(\sigma) \nsubseteq \mathfrak{A}_n \underset{\text{5.3.18 (iii)}}{\Longrightarrow} \text{ΚΛΣ}_{\mathfrak{A}_n}(\sigma) = \text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma).$$

(ii) Εάν $\text{ΚΛΣ}_{\mathfrak{A}_n}(\sigma) = \text{ΚΛΣ}_{\mathfrak{S}_n}(\sigma)$, τότε κατά το 5.3.18 (iii),

$$|\mathrm{C}_{\mathfrak{A}_n}(\sigma)| = \frac{1}{2}\,|\mathrm{C}_{\mathfrak{S}_n}(\sigma)| \underset{(5.22)}{\Longrightarrow} k_{\varrho_1}^{\lambda_1}\,(\lambda_1!) \cdots k_{\varrho_s}^{\lambda_s}\,(\lambda_s!) = |\mathrm{C}_{\mathfrak{S}_n}(\sigma)| \equiv 0 (\mathrm{mod}\,2),$$

απ' όπου έπεται ότι είτε

$$\text{card}(\left\{ j \in \{1,..,s\} \,\middle|\, k_{\varrho_j} \equiv 0(\mathrm{mod}\,2) \right\}) \geq 1 \ \text{ είτε } \exists j \in \{1,..,s\} : \lambda_j \geq 2. \tag{5.31}$$

Αντιστρόφως τώρα, υποθέτουμε ότι οι συνθήκες (5.31) ικανοποιούνται. Η μετάταξη σ είναι εξ ορισμού τής μορφής

$$\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_s,$$

όπου οι $\sigma_1,...,\sigma_s \in \mathfrak{S}_n$ είναι ανά δύο ξένες μεταξύ τους μετατάξεις και για κάθε δείκτη $j \in \{1,...,s\}$ η σ_j είναι η σύνθεση $\sigma_j = c_{j1} \circ c_{j2} \circ \cdots \circ c_{j\lambda_j}$ ανά δύο ξένων μεταξύ τους κύκλων $c_{j1}, ..., c_{j\lambda_j} \in \mathfrak{S}_n$ με

$$\text{μήκος}(c_{j\mu}) = k_{\varrho_j},\ \ \forall \mu \in \{1,...,\lambda_j\}.$$

Εάν $\exists j = j_\bullet \in \{1,...,s\} : k_{\varrho_{j_\bullet}} \equiv 0(\mathrm{mod}\, 2)$, τότε θέτοντας

$$\tau_{j_\bullet} := \sigma_1 \circ \cdots \circ \sigma_{j_\bullet - 1} \circ \sigma_{j_\bullet + 1} \circ \cdots \circ \sigma_s$$

λαμβάνουμε

$$\sigma = \sigma_{j_\bullet} \circ \tau_{j_\bullet} = \tau_{j_\bullet} \circ \sigma_{j_\bullet},$$

οπότε $\sigma_{j_\bullet} \circ \sigma = \sigma_{j_\bullet} \circ (\sigma_{j_\bullet} \circ \tau_{j_\bullet}) = \sigma_{j_\bullet} \circ (\tau_{j_\bullet} \circ \sigma_{j_\bullet}) = \sigma \circ \sigma_{j_\bullet}$. Τούτο σημαίνει ότι $\sigma_{j_\bullet} \in \mathrm{C}_{\mathfrak{S}_n}(\sigma)$. Όμως κάθε κύκλος αρτίου μήκους είναι μια περιττή μετάταξη (βλ. 3.3.5 (iii)). Άρα $\sigma_{j_\bullet} \in \mathfrak{S}_n \setminus \mathfrak{A}_n$ και, ως εκ τούτου,

$$\mathrm{C}_{\mathfrak{S}_n}(\sigma) \nsubseteqq \mathfrak{A}_n \underset{\text{5.3.18 (iii)}}{\Longrightarrow} \mathrm{K\Lambda\Sigma}_{\mathfrak{A}_n}(\sigma) = \mathrm{K\Lambda\Sigma}_{\mathfrak{S}_n}(\sigma).$$

Εάν $\exists j = j_\bullet \in \{1,...,s\} : \lambda_{j_\bullet} \geq 2$, τότε διακρίνουμε δύο περιπτώσεις. Στην περίπτωση όπου ο $k_{\varrho_{j_\bullet}}$ είναι *άρτιος* και ο $\lambda_{j_\bullet}$ *περιττός*, τότε $\mathrm{sgn}(\sigma_{j_\bullet}) = -1$ και χρησιμοποιούμε εκ νέου την προηγηθείσα επιχειρηματολογία. Στην περίπτωση όπου ο $k_{\varrho_{j_\bullet}}$ είναι *περιττός* και ο $\lambda_{j_\bullet}$ *οιοσδήποτε* φυσικός αριθμός ≥ 2 γράφουμε τους κύκλους $c_{j_\bullet 1}, c_{j_\bullet 2}$ αναλυτικώς ως

$$c_{j_\bullet 1} = [\alpha_{j_\bullet 1} ... \, \alpha_{j_\bullet k_{\varrho_{j_\bullet}}}],\ c_{j_\bullet 2} = [\beta_{j_\bullet 1} ... \, \beta_{j_\bullet k_{\varrho_{j_\bullet}}}],$$

θέτουμε $d_{j_\bullet} := [\alpha_{j_\bullet 1}\ \beta_{j_\bullet 1}] \circ \cdots \circ [\alpha_{j_\bullet k_{\varrho_{j_\bullet}}}\ \beta_{j_\bullet k_{\varrho_{j_\bullet}}}]$ και παρατηρούμε ότι

$$(c_{j_\bullet 1} \circ c_{j_\bullet 2}) \circ d_{j_\bullet} = d_{j_\bullet} \circ (c_{j_\bullet 1} \circ c_{j_\bullet 2})\,. \tag{5.32}$$

Επιπροσθέτως, θέτοντας

$$\hat{d}_{j_\bullet} := \sigma_1 \circ \cdots \circ \sigma_{j_\bullet - 1} \circ \left(c_{j_\bullet 3} \circ \cdots \circ c_{j_\bullet \lambda_{j_\bullet}}\right) \circ \sigma_{j_\bullet + 1} \circ \cdots \circ \sigma_s$$

(όταν $\lambda_{j_\bullet} \geq 3$) και λαμβάνοντας υπ' όψιν ότι $\mathrm{supp}(d_{j_\bullet}) \cap \mathrm{supp}(\hat{d}_{j_\bullet}) = \varnothing$, συμπεραίνουμε ότι

$$\hat{d}_{j_\bullet} \circ d_{j_\bullet} = d_{j_\bullet} \circ \hat{d}_{j_\bullet}. \tag{5.33}$$

Από τις (5.32) και (5.33) λαμβάνουμε

$$\sigma \circ d_{j_\bullet} = (c_{j_\bullet 1} \circ c_{j_\bullet 2}) \circ (\hat{d}_{j_\bullet} \circ d_{j_\bullet})$$

$$= (c_{j_\bullet 1} \circ c_{j_\bullet 2}) \circ (d_{j_\bullet} \circ \hat{d}_{j_\bullet}) = d_{j_\bullet} \circ (c_{j_\bullet 1} \circ c_{j_\bullet 2}) \circ \hat{d}_{j_\bullet} = d_{j_\bullet} \circ \sigma,$$

οπότε $d_{j_\bullet} \in \mathrm{C}_{\mathfrak{S}_n}(\sigma)$ με $\mathrm{sgn}(d_{j_\bullet}) = (-1)^{k_{\varrho_{j_\bullet}}} = -1$ (βλ. 3.3.5 (iii)). Κατά συνέπειαν,

$$d_{j_\bullet} \in \mathfrak{S}_n \setminus \mathfrak{A}_n \Rightarrow \mathrm{C}_{\mathfrak{S}_n}(\sigma) \nsubseteqq \mathfrak{A}_n \underset{\text{5.3.18 (iii)}}{\Longrightarrow} \mathrm{K\Lambda\Sigma}_{\mathfrak{A}_n}(\sigma) = \mathrm{K\Lambda\Sigma}_{\mathfrak{S}_n}(\sigma).$$

(iii) Εάν $\mathrm{K\Lambda\Sigma}_{\mathfrak{A}_n}(\sigma) \subsetneqq \mathrm{K\Lambda\Sigma}_{\mathfrak{S}_n}(\sigma)$, τότε από τα (ii) και (iii) τού λήμματος 5.3.18 έπεται ότι

$$\mathrm{C}_{\mathfrak{S}_n}(\sigma) \sqsubseteq \mathfrak{A}_n \Rightarrow |\mathrm{C}_{\mathfrak{A}_n}(\sigma)| = |\mathrm{C}_{\mathfrak{S}_n}(\sigma)| \underset{(5.26)}{\Longrightarrow} \mathrm{card}(\mathrm{K\Lambda\Sigma}_{\mathfrak{A}_n}(\sigma)) = \frac{1}{2}\mathrm{card}(\mathrm{K\Lambda\Sigma}_{\mathfrak{S}_n}(\sigma)).$$

Επειδή για κάθε $\tau \in \mathrm{K\Lambda\Sigma}_{\mathfrak{S}_n}(\sigma) \setminus \mathrm{K\Lambda\Sigma}_{\mathfrak{A}_n}(\sigma)$ έχουμε $\mathrm{K\Lambda\Sigma}_{\mathfrak{A}_n}(\sigma) \cap \mathrm{K\Lambda\Sigma}_{\mathfrak{A}_n}(\tau) = \varnothing$ και $\mathrm{K\Lambda\Sigma}_{\mathfrak{A}_n}(\tau) \subseteq \mathrm{K\Lambda\Sigma}_{\mathfrak{S}_n}(\tau) = \mathrm{K\Lambda\Sigma}_{\mathfrak{S}_n}(\sigma)$, συμπεραίνουμε τελικώς ότι οι (5.27) και (5.28) είναι αληθείς. □

5.3.20 Παραδείγματα. Λαμβάνοντας υπ' όψιν το θεώρημα 5.3.19 και ό,τι προαναφέραμε στο εδάφιο 5.3.17 συντάσσουμε τους καταλόγους των εκπροσώπων των κλάσεων συζυγίας τής εναλλάσσουσας ομάδας $\mathfrak{A}_n$ για $n \in \{4, 5, 6\}$.

► **Κατάλογος εκπροσώπων των κλάσεων συζυγίας τής** $\mathfrak{A}_4$:

εκπρ.	**τάξη**	$\sharp$	**είδος**
id	1	1	άρτια
$[1\,2\,3]$	3	4	άρτια
$[1\,3\,2]$	3	4	άρτια
$[1\,2] \circ [3\,4]$	2	3	άρτια

► **Κατάλογος εκπροσώπων των κλάσεων συζυγίας τής** $\mathfrak{A}_5$:

εκπρ.	**τάξη**	$\sharp$	**είδος**
id	1	1	άρτια
$[1\,2\,3]$	3	20	άρτια
$[1\,2] \circ [3\,4]$	2	15	άρτια
$[1\,2\,3\,4\,5]$	5	12	άρτια
$[1\,2\,3\,5\,4]$	5	12	άρτια

► **Κατάλογος εκπροσώπων των κλάσεων συζυγίας τής** $\mathfrak{A}_6$:

εκπρ.	**τάξη**	$\sharp$	**είδος**
id	1	1	άρτια
$[1\,2\,3]$	3	40	άρτια
$[1\,2] \circ [3\,4]$	2	45	άρτια
$[1\,2\,3\,4\,5]$	5	72	άρτια
$[1\,2\,3\,5\,4]$	5	72	άρτια
$[1\,2] \circ [3\,4\,5\,6]$	4	90	άρτια
$[1\,2\,3] \circ [4\,5\,6]$	3	40	άρτια

5.3.21 Σημείωση. (Περί τού πλήθους των κλάσεων συζυγίας τής $\mathfrak{A}_n$**.)** Μεταξύ των αποτελεσμάτων των περιεχομένων σε ένα άρθρο των J. Dénes, P. Erdös και P. Turán (δημοσιευθέν το έτος[21] 1969) περί τού αριθμού $\mathfrak{K}(\mathfrak{A}_n)$ συγκαταλέγεται η περιγραφή τής *ασυμπτωτικής συμπεριφοράς του,* βάσει τής οποίας

$$\boxed{\mathfrak{K}(\mathfrak{A}_n) \approx \tfrac{1}{8n\sqrt{3}} \exp(2\pi\sqrt{\tfrac{n}{6}}),\ \text{καθώς το}\ n \longrightarrow \infty.} \qquad (5.34)$$

Συγκρίνοντας τις (5.14) και (5.34) διαπιστώνουμε ότι ο αριθμός $\mathfrak{K}(\mathfrak{S}_n)$ *για μεγάλους* n είναι *περίπου διπλάσιος* τού $\mathfrak{K}(\mathfrak{A}_n)$. Στο εν λόγω άρθρο δίδεται και ένας κλειστός (αλλά σχετικώς περίπλοκος) τύπος εκφράσεως τού αριθμού $\mathfrak{K}(\mathfrak{A}_n)$ συναρτήσει τού $\varpi\,(n)$. Ο τύπος αυτός απλουστεύθηκε (μέσω χρήσεως τής ταυτότητας τού Jacobi) το 1980 από τον R.D. Girse[22], ο οποίος κατέληξε στην «κομψή» έκφραση (5.35).

[21] Βλ. J. Dénes, P. Erdös και P. Turán: *On some statistical properties of the alternating group of degree* n, Enseignement Math., Ser. 2, Vol. **15** (1969), 89-99.

[22] Βλ. R.D. Girse: *The number of conjugacy classes of the alternating group*, B.I.T., Vol. **20** (1980), 515-517.

5.3.22 Θεώρημα. (Τύπος τού Girse, 1980) *Για κάθε $n \in \mathbb{N}$, $n \geq 2$, το πλήθος των κλάσεων συζυγίας τής εναλλάσσουσας ομάδας $\mathfrak{A}_n$ μπορεί να εκφρασθεί μέσω τού τύπου*

$$\boxed{\mathfrak{K}(\mathfrak{A}_n) = 2\varpi(n) + 3\sum_{j=1}^{\left\lfloor\sqrt{\frac{n}{2}}\right\rfloor} (-1)^j \varpi\left(n - 2j^2\right),} \tag{5.35}$$

(*όπου* $\varpi(0) := 1$).

5.3.23 Παραδείγματα. Για $n \in \{2,...,20\} \cup \{10\lambda \,|\lambda \in \{3,...,10\}\} \cup \{200\}$ ο τύπος (5.35) τού Girse δίδει

n	$\mathfrak{K}(\mathfrak{A}_n)$	n	$\mathfrak{K}(\mathfrak{A}_n)$
2	1	16	123
3	3	17	156
4	4	18	200
5	5	19	254
6	7	20	324
7	9	30	2829
8	14	40	18738
9	18	50	102260
10	24	60	483547
11	31	70	2044596
12	43	80	7899414
13	55	90	28319236
14	72	100	95288507
15	94	200	1986499984086

Συγκρίνοντας (επί τη βάσει τού ανωτέρω καταλόγου και τού καταλόγου τού παρατεθέντος στο εδάφιο 5.3.9) τον λόγο $\mathfrak{K}(\mathfrak{S}_n) \,/\, \mathfrak{K}(\mathfrak{A}_n)$ π.χ. για τις τιμές

n	5	10	15	20	50	100	200
λόγος	1,4	1,75	1,8723..	1,9352..	1,9971..	1,9999..	2

παρατηρούμε ότι αυτός τείνει ταχέως προς το 2. Μάλιστα, είναι αξιοσημείωτο ότι ο αριθμός των κλάσεων συζυγίας τής εναλλάσσουσας ομάδας $\mathfrak{A}_{200}$ είναι ίσος *ακριβώς με το ήμισυ* τού αριθμού των κλάσεων συζυγίας τής $\mathfrak{S}_{200}$!

► **Ενδιαφέρουσες εφαρμογές.** Οι κατάλογοι οι συνταχθέντες στο εδάφιο 5.3.20 είναι λίαν χρήσιμοι και ικανοί να μας οδηγήσουν ακόμη και σε *διαφορετικές* αντιμετωπίσεις ήδη τεθέντων προβλημάτων.

5.3.24 Σημείωση. Στα εδάφια 4.1.47 και 4.1.48 είχαν δοθεί δύο αποδείξεις για το ότι *η εναλλάσσουσα ομάδα* $\mathfrak{A}_4$ *δεν διαθέτει υποομάδες τάξεως* 6. Μια *τρίτη* απόδειξη (εκ νέου με «εις άτοπον απαγωγή») είναι η εξής: Ας υποθέσουμε ότι υπάρχει υποομάδα H τής $\mathfrak{A}_4$ τάξεως 6. Τότε $|\mathfrak{A}_4 : H| = 2 \underset{4.2.13}{\Longrightarrow} H \trianglelefteq \mathfrak{A}_4$. Επειδή τα στοιχεία id, $[1\,2\,3]$, $[1\,3\,2]$ και $[1\,2] \circ [3\,4]$ τής $\mathfrak{A}_4$ απαρτίζουν (βάσει των προαναφερθέντων

στο εδάφιο 5.3.20) ένα πλήρες σύστημα εκπροσώπων αυτής ως προς την "$\underset{\text{συζ.}}{\sim}$" και οι πληθικοί αριθμοί των κλάσεων συζυγίας τους είναι ίσοι με $1, 4, 4$ και 3, αντιστοίχως, υπάρχουν (λόγω τού πορίσματος 5.1.16) $\lambda_1, \lambda_2, \lambda_3 \in \{0, 1\}$, τέτοιοι ώστε να ισχύει η ισότητα

$$1 + 4\lambda_1 + 4\lambda_2 + 3\lambda_3 = 6\,(= |H|). \tag{5.36}$$

Από τον κατάλογο των δυνατών τιμών τού αριστερού μέλους («Α.Μ.») τής (5.36):

λ_1	0	1	0	1	0	1	0	1
λ_2	0	0	1	1	0	0	1	1
λ_3	0	0	0	0	1	1	1	1
Α.Μ.	**1**	**5**	**5**	**9**	**4**	**8**	**8**	**12**

που προκύπτει από όλες τις δυνατές τιμές των συντελεστών $\lambda_1, \lambda_2, \lambda_3$, συμπεραίνουμε ότι η (5.36) δεν διαθέτει καμία λύση. Άτοπο! Άρα η $\mathfrak{A}_4$ δεν διαθέτει υποομάδες τάξεως 6.

Άλλη μία ενδιαφέρουσα εφαρμογή (τού δευτέρου καταλόγου) τού εδαφίου 5.3.20 είναι αυτή που (σε συνδυασμό με το πόρισμα 5.1.16) οδηγεί στην εύρεση μιας εύκολης αποδείξεως τής απλότητας τής $\mathfrak{A}_5$, και, κατ' επέκταση, στη δημιουργία των απαραίτητων προϋποθέσεων για μια *επαγωγική* απόδειξη τής απλότητας των εναλλασσουσών ομάδων $\mathfrak{A}_n$ *για κάθε* $n \geq 5$.

5.3.25 Λήμμα. *Η* $\mathfrak{A}_5$ *είναι απλή ομάδα.*

ΑΠΟΔΕΙΞΗ. Έστω τυχούσα $H \trianglelefteq \mathfrak{A}_5$. Επειδή $|\mathfrak{A}_5| = \frac{5!}{2} = 60$, το θεώρημα 4.1.22 τού Lagrange μας πληροφορεί ότι $|H| \in \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$. Εξάλλου, επειδή τα στοιχεία id, $[1\,2\,3]$, $[1\,2] \circ [3\,4]$, $[1\,2\,3\,4\,5]$, $[1\,2\,3\,5\,4]$ τής $\mathfrak{A}_5$ απαρτίζουν (βάσει των προαναφερθέντων στο εδάφιο 5.3.20) ένα πλήρες σύστημα εκπροσώπων αυτής ως προς την "$\underset{\text{συζ.}}{\sim}$" και οι πληθικοί αριθμοί των κλάσεων συζυγίας τους είναι ίσοι με $1, 20, 15, 12$ και 12, αντιστοίχως, υπάρχουν (σύμφωνα με το πόρισμα 5.1.16) $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \{0, 1\}$, τέτοιοι ώστε να ισχύει η ισότητα

$$1 + 20\lambda_1 + 15\lambda_2 + 12\lambda_3 + 12\lambda_4 = |H|\,. \tag{5.37}$$

Από τον κατάλογο των δυνατών τιμών τού αριστερού μέλους («Α.Μ.») τής (5.37):

λ_1	0	1	0	1	0	1	0	1
λ_2	0	0	1	1	0	0	0	0
λ_3	0	0	0	0	1	1	0	0
λ_4	0	0	0	0	0	0	1	1
Α.Μ.	**1**	**21**	**16**	**36**	**13**	**33**	**13**	**33**
λ_1	0	1	0	1	0	1	0	1
λ_2	1	1	1	1	0	0	1	1
λ_3	1	1	0	0	1	1	1	1
λ_4	0	0	1	1	1	1	1	1
Α.Μ.	**28**	**48**	**28**	**48**	**25**	**45**	**40**	**60**

που προκύπτει από όλες τις δυνατές τιμές των $\lambda_1, \lambda_2, \lambda_3, \lambda_4$, συμπεραίνουμε ότι $|H| \in \{1, 60\} \Rightarrow$ [είτε $H = \{\mathrm{id}\}$ είτε $H = \mathfrak{A}_5$]. Άρα η $\mathfrak{A}_5$ είναι απλή ομάδα. □

• ΔΕΥΤΕΡΗ ΑΠΟΔΕΙΞΗ ΤΟΥ ΘΕΩΡΗΜΑΤΟΣ 4.3.6: Δυνάμει τού λήμματος 5.3.25 η $\mathfrak{A}_5$ είναι απλή ομάδα. Θεωρώντας τυχόντα φυσικό αριθμό $n \geq 6$ και υποθέτοντας ότι η $\mathfrak{A}_{n-1}$ είναι απλή, θα αποδείξουμε (επαγωγικώς) ότι η $\mathfrak{A}_n$ είναι ωσαύτως απλή ομάδα. Έστω $\{\mathrm{id}\} \neq H \trianglelefteq \mathfrak{A}_n$.

Ισχυρισμός πρώτος: $\exists \tau \in H \setminus \{\mathrm{id}\}$: $\tau(i) = i$ *για κάποιον* $i \in \{1, ..., n\}$.

Αυτός θα επαληθευθεί μέσω τής «εις άτοπον απαγωγής». Υποθέτουμε ότι $\sigma(j) \neq j$ *για κάθε* $j \in \{1, ..., n\}$ και *για οιαδήποτε μετάταξη* $\sigma \in H \setminus \{\mathrm{id}\}$. Έστω τυχούσα μετάταξη $\pi \in H \setminus \{\mathrm{id}\}$. Θέτοντας $k := \pi(1)$, η π γράφεται υπό τη μορφή

$$\begin{bmatrix} 1 & \cdots & l & \cdots & n \\ k & \cdots & m & \cdots & \pi(n) \end{bmatrix},\ l \in \{2, ..., n\},$$

όπου $m := \pi(l) \neq k$ και (λόγω τής υποθέσεώς μας) $l \neq m$. Επειδή $n \geq 6$, υπάρχουν $r, s \in \{1, ..., n\} \setminus \{1, k, l, m\}$ με $r \neq s$. Η σύνθεση $\rho := [1\ k] \circ [l\ m\ r\ s]$ είναι μια *άρτια* μετάταξη, διότι (κατά το λήμμα 3.3.4 και τα (i) και (iii) τού θεωρήματος 3.3.5)

$$\mathrm{sgn}\,(\tau \circ \sigma) = \mathrm{sgn}([1\ k])\,\mathrm{sgn}([l\ m\ r\ s]) = (-1)(-1)^3 = 1.$$

Επομένως, $\rho \in \mathfrak{A}_n \underset{H \trianglelefteq \mathfrak{A}_n}{\Longrightarrow} \rho \circ \pi \circ \rho^{-1} \in H$, $\rho^{-1} = [l\ m\ r\ s]^{-1} \circ [1\ k]^{-1} = [s\ r\ m\ l] \circ [1\ k]$ και

$$\left(\rho \circ \pi \circ \rho^{-1}\right)(k) = \rho(\pi(\rho^{-1}(k))) = \rho(\pi(1)) = \rho(k) = 1,$$
$$\left(\rho \circ \pi \circ \rho^{-1}\right)(m) = \rho(\pi(\rho^{-1}(m))) = \rho(\pi(l)) = \rho(m) = r,$$

οπότε για τη σύνθεση $\left(\rho \circ \pi \circ \rho^{-1}\right) \circ \pi \in H$ ισχύει $\left(\rho \circ \pi \circ \rho^{-1}\right)(\pi(1)) = 1$ και

$$\left(\rho \circ \pi \circ \rho^{-1}\right)(\pi(l)) = \left(\rho \circ \pi \circ \rho^{-1}\right)(m) = r \neq l \Rightarrow \left(\rho \circ \pi \circ \rho^{-1}\right) \circ \pi \neq \mathrm{id}.$$

Άτοπο! Άρα *υπάρχει πράγματι* (τουλάχιστον μία) μετάταξη $\tau \in H \setminus \{\mathrm{id}\}$: $\tau(i) = i$ για κάποιον $i \in \{1, ..., n\}$.

Ισχυρισμός δεύτερος: $H = \mathfrak{A}_n$. Η υποομάδα $\mathfrak{A}(i) := \{\sigma \in \mathfrak{A}_n | \, \sigma(i) = i\}$ τής $\mathfrak{A}_n$ είναι ισόμορφη με την $\mathfrak{A}_{n-1}$ και για την τομή $H(i) := H \cap \mathfrak{A}(i)$ έχουμε

$$H \trianglelefteq \mathfrak{A}_n \underset{4.2.22}{\Longrightarrow} H(i) \trianglelefteq \mathfrak{A}(i).$$

Σύμφωνα με την επαγωγική μας υπόθεση, η $\mathfrak{A}(i)$ είναι απλή ομάδα. Κατά συνέπειαν, είτε η $H(i)$ είναι τετριμμένη είτε ισχύει $H(i) = \mathfrak{A}(i)$. Το πρώτο ενδεχόμενο αποκλείεται, διότι $\tau \in H(i)$ και $\tau \neq \mathrm{id}$. Αυτό σημαίνει ότι

$$H(i) = \mathfrak{A}(i) \Rightarrow \mathfrak{A}(i) \subseteq H \underset{2.1.20}{\Longrightarrow} \mathfrak{A}(i) \sqsubseteq H.$$

Επειδή $n \geq 6$, η $\mathfrak{A}(i)$ *περιέχει* 3-κύκλους. Επομένως *και* η H περιέχει 3-κύκλους. Σύμφωνα με το λήμμα 4.3.4, $H = \mathfrak{A}_n$. Άρα η $\mathfrak{A}_n$ είναι όντως απλή ομάδα. □

5.4 ΤΟ ΚΕΝΤΡΟ ΜΙΑΣ ΟΜΑΔΑΣ

Το *κέντρο* μιας ομάδας αποτελεί το «αβελιανό μέρος» αυτής.

5.4.1 Ορισμός. Έστω $(G, \cdot)$ μια ομάδα. Το σύνολο

$$\boxed{Z(G) := \mathrm{C}_G(G) = \{\, g \in G \mid \ gx = xg,\ \forall x \in G\}}$$

όλων των στοιχείων τής G που μετατίθενται αμοιβαίως με κάθε στοιχείο τής G καλείται **κέντρο τής** G. Προφανώς,

$$\boxed{Z(G) = \bigcap_{x \in G} \mathrm{C}_G(x).}$$

5.4.2 Πρόταση. *Έστω $(G, \cdot)$ μια ομάδα. Τότε $Z(G) \trianglelefteq G$ και*

$$G = Z(G) \iff \textit{η } G \textit{ είναι αβελιανή.}$$

ΑΠΟΔΕΙΞΗ. Το ότι $Z(G) \trianglelefteq G$ έπεται ύστερα από εφαρμογή τού (iii) τής προτάσεως 5.2.2 (για $H = G$). Εάν $g_1, g_2 \in Z(G)$, τότε προφανώς (εξ ορισμού) $g_1 g_2 = g_2 g_1$, οπότε η ομάδα $Z(G)$ είναι αβελιανή. Εξ αυτού έπεται η κατεύθυνση "$\Rightarrow$" τής αποδεικτέας αμφίπλευρης συνεπαγωγής. Η "$\Leftarrow$" έπεται από το 5.2.2 (ii) (εφαρμοζόμενο για την $H = G$). □

5.4.3 Πρόταση. *Έστω $(G, \cdot)$ μια ομάδα και έστω $H \sqsubseteq G$. Τότε ισχύουν τα εξής*:

(i) $Z(G) \cap H \sqsubseteq Z(H)$.

(ii) $\mathrm{C}_G(H) = G \iff H \sqsubseteq Z(G)$.

ΑΠΟΔΕΙΞΗ. (i) Κατά το 5.2.2 (v), $Z(G) := \mathrm{C}_G(G) \sqsubseteq \mathrm{C}_G(H)$, οπότε

$$Z(G) \cap H \sqsubseteq \mathrm{C}_G(H) \cap H = \mathrm{C}_H(H) = Z(H),$$

όπου η προτελευταία ισότητα έπεται από το 5.2.2 (iv).

(ii) "$\Rightarrow$" Εάν $\mathrm{C}_G(H) = G$ και $h \in H$, τότε $h \in \mathrm{C}_G(H) \Rightarrow h \in Z(G)$. Κατά συνέπειαν, $H \subseteq Z(G) \sqsubseteq G \underset{2.1.20}{\Longrightarrow} H \sqsubseteq Z(G)$.

"$\Leftarrow$" Εάν $H \sqsubseteq Z(G)$, τότε $\mathrm{C}_G(Z(G)) \sqsubseteq \mathrm{C}_G(H)$ (βλ. 5.2.2 (v)). Εξάλλου, επειδή $\mathrm{C}_G(Z(G)) = G$, λαμβάνουμε $\mathrm{C}_G(H) = G$. □

5.4.4 Σημείωση. Εάν η G είναι αβελιανή, τότε προφανώς

$$G \cap H = Z(G) \cap H = Z(H) = H.$$

Υπάρχουν και αρκετά παραδείγματα *ειδικών* υποομάδων H *μη αβελιανών* ομάδων G στα οποία το κέντρο $Z(H)$ *ισούται* με την τομή $Z(G) \cap H$. Βλ., π.χ., τους υπολογισμούς των κέντρων ορισμένων υποομάδων ομάδων πινάκων που περιέχονται στις προτάσεις 5.4.12, 5.4.14 και 5.4.15. Ωστόσο, απλούστερα παραδείγματα

(όπως αυτό τής κυκλικής υποομάδας $\langle\beta\rangle$ των στροφών τής $\mathbf{D}_n$, βλ. 5.4.8) δείχνουν ότι τα κέντρα $Z(H)$ μπορούν να είναι «ευρύτερα» των τομών[23] $Z(G)\cap H$.

5.4.5 Πρόταση. *Έστω $f:(G,\cdot)\longrightarrow(H,*)$ ένας ομομορφισμός ομάδων. Τότε*

$$K\sqsubseteq G\Longrightarrow f(Z(K))\sqsubseteq Z(f(K)).$$

Επιπροσθέτως, εάν ο f είναι ισομορφισμός, τότε $f(Z(K))=Z(f(K))$.

ΑΠΟΔΕΙΞΗ. Εάν $K\sqsubseteq G$ και $y\in Z(K)$, τότε

$$yx=xy,\ \forall x\in K\Rightarrow f(yx)=f(y)*f(x)=f(x)*f(y),\ \forall x\in K,$$

οπότε $f(Z(K))\subseteq Z(f(K))$ και $Z(f(K))\sqsubseteq f(K)\underset{2.1.20}{\Longrightarrow} f(Z(K))\sqsubseteq Z(f(K))$. Εάν ο f είναι ισομορφισμός, τότε χρησιμοποιώντας το ίδιο είδος επιχειρημάτων για τον f^{-1} συμπεραίνουμε ότι $f(Z(K))=Z(f(K))$. □

5.4.6 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω $g\in G$. Τότε τα ακόλουθα είναι ισοδύναμα*:

(i) $\text{ΚΛΣ}_G(g)=\{g\}$.

(ii) $g\in Z(G)$.

(iii) $\mathrm{C}_G(g)=G$.

(iv) $|G:\mathrm{C}_G(g)|=1$.

ΑΠΟΔΕΙΞΗ. Επειδή

$$\text{ΚΛΣ}_G(g)=\{g\}\Leftrightarrow xgx^{-1}=g,\forall x\in G\Leftrightarrow gx=xg,\forall x\in G\Leftrightarrow g\in Z(G),$$

η αμφίπλευρη συνεπαγωγή (i)⇔(ii) είναι αληθής. Οι (i)⇔(iii)⇔(iv) έπονται άμεσα από το πόρισμα 5.2.10. □

Λόγω τής προτάσεως 5.4.2 «ενδιαφέροντα» παραδείγματα κέντρων εμφανίζονται μόνον στην κλάση των *μη αβελιανών* ομάδων.

5.4.7 Παράδειγμα. (Κέντρο τής Q.) Από την πρόταση 5.4.6 και από τον κατάλογο εκπροσώπων των κλάσεων συζυγίας τής ομάδας $\mathbf{Q}$ των τετρανίων (που δίδεται στο εδάφιο 5.2.12) συνάγεται ότι $Z(\mathbf{Q})=\{\mathbf{I}_2,-\mathbf{I}_2\}$.

5.4.8 Παράδειγμα. (Κέντρο τής $\mathbf{D}_n$.) Έστω $n\in\mathbb{N}$, $n\geq 3$, και έστω $\mathbf{D}_n=\langle\alpha,\beta\rangle$ η n-οστή διεδρική ομάδα (βλ. 3.4.4). Από την πρόταση 5.4.6 και από τους δύο καταλόγους εκπροσώπων των κλάσεων συζυγίας τής ομάδας $\mathbf{D}_n$ που δίδονται στην πρόταση 5.1.10 (για n περιττό και n άρτιο, αντιστοίχως) συνάγεται ότι

$$Z(\mathbf{D}_n)=\begin{cases}\{\mathrm{id}_{\mathcal{E}_n}\}, & \text{όταν ο } n \text{ είναι περιττός,}\\ \{\mathrm{id}_{\mathcal{E}_n},\beta^{\frac{n}{2}}\}=\left\langle\beta^{\frac{n}{2}}\right\rangle, & \text{όταν ο } n \text{ είναι άρτιος.}\end{cases}$$

Σημειωτέον ότι $Z(\mathbf{D}_n)=Z(\mathbf{D}_n)\cap\langle\beta\rangle\sqsubset Z(\langle\beta\rangle)=\langle\beta\rangle$.

[23] Επί παραδείγματι, εάν η G είναι μια μη αβελιανή ομάδα και $H\sqsubset G$ με $Z(G)\sqsubset H$, τότε $Z(G)=Z(G)\cap H\sqsubset H$.

5.4.9 Παράδειγμα. (Κέντρο τής $\mathfrak{S}_n$.) Η συμμετρική ομάδα $\mathfrak{S}_n$ σε n σύμβολα είναι αβελιανή για $n \leq 2$, ενώ για $n \geq 3$ έχει *τετριμμένο κέντρο* $Z(\mathfrak{S}_n) = \{\mathrm{id}\}$, κάτι το οποίο έπεται άμεσα από το λήμμα 4.3.11.

5.4.10 Παράδειγμα. Κάθε μη αβελιανή απλή ομάδα G έχει *τετριμμένο κέντρο* (καθότι $Z(G) \trianglelefteq G$).

5.4.11 Παράδειγμα. (Κέντρο τής $\mathfrak{A}_n$.) Η εναλλάσσουσα ομάδα $\mathfrak{A}_n$ σε n σύμβολα είναι αβελιανή για $n \leq 3$, ενώ για $n \geq 4$ έχει *τετριμμένο κέντρο* $Z(\mathfrak{A}_n) = \{\mathrm{id}\}$. Πράγματι· για $n \geq 5$ τούτο είναι προφανές (λόγω των 4.3.6 και 5.4.10). Εξάλλου, εάν το $Z(\mathfrak{A}_4)$ ήταν μια μη τετριμμένη υποομάδα τής (μη αβελιανής ομάδας) $\mathfrak{A}_4$, τότε θα είχαμε $|Z(\mathfrak{A}_4)| \in \{2, 3, 4\}$ (λόγω τού θεωρήματος 4.1.22 τού Lagrange και τής προτάσεως 4.1.47). Το ενδεχόμενο να έχουμε $|Z(\mathfrak{A}_4)| = 4$ αποκλείεται, διότι τότε η πηλικοομάδα $\mathfrak{A}_4/Z(\mathfrak{A}_4)$ θα είχε τάξη 3 και θα ήταν κατ' ανάγκην κυκλική ομάδα (βλ. 2.3.19), κάτι που (όπως θα δούμε στην πρόταση 5.4.17) είναι αδύνατο. Εάν ίσχυε $|Z(\mathfrak{A}_4)| \in \{2, 3\}$, τότε το κέντρο $Z(\mathfrak{A}_4)$ τής $\mathfrak{A}_4$ θα έπρεπε να είναι είτε μία εκ των τριών κυκλικών υποομάδων τής $\mathfrak{A}_4$ τάξεως 2 είτε μία εκ των τεσσάρων κυκλικών υποομάδων τής $\mathfrak{A}_4$ τάξεως 3 που περιεγράφησαν στο πόρισμα 4.1.49. Όμως καμία[24] εξ αυτών των επτά κυκλικών υποομάδων τής ομάδας $\mathfrak{A}_4$ δεν είναι ορθόθετη, ενώ $Z(\mathfrak{A}_4) \lhd \mathfrak{A}_4$! Επομένως, $Z(\mathfrak{A}_4) = \{\mathrm{id}\}$.

«Ενδιαφέροντα» κέντρα διαθέτουν και κάποιες *ομάδες πινάκων*.

5.4.12 Πρόταση. (Κέντρο τής $\mathbf{GL}_n(F)$.) *Έστω F ένα σώμα και έστω $n \in \mathbb{N}$. Τότε*

$$Z(\mathbf{GL}_n(F)) = \left\{ \lambda \mathbf{I}_n \,|\, \lambda \in F^\times \right\}$$

και $Z(\mathbf{SL}_n(F)) = Z(\mathbf{GL}_n(F)) \cap \mathbf{SL}_n(F) = \left\{ \lambda \mathbf{I}_n \,|\, \lambda \in F^\times,\ \lambda^n = 1_F \right\}$.

ΑΠΟΔΕΙΞΗ. Για $n = 1$ ο ισχυρισμός είναι προδήλως αληθής. Έστω ότι $n \geq 2$. Προφανώς,

$$\left\{ \lambda \mathbf{I}_n \,|\, \lambda \in F^\times \right\} \subseteq Z(\mathbf{GL}_n(F)),\ \left\{ \lambda \mathbf{I}_n \,|\, \lambda \in F^\times,\ \lambda^n = 1_F \right\} \subseteq Z(\mathbf{SL}_n(F)).$$

Για κάθε $\lambda \in F$ και για κάθε ζεύγος $(j, k) \in \{1, .., n\} \times \{1, .., n\}$, $j \neq k$, θεωρούμε τους πίνακες[25]

$$\mathbf{R}_{jk}(\lambda) := \mathbf{I}_n + \lambda \mathbf{E}_{jk} \in \mathbf{GL}_n(F),$$

(όπου $\mathbf{E}_{jk}$ οι ορισθέντες στο εδάφιο D.1.4 (i)), οι εγγραφές των οποίων είναι ίσες με 1_F στην κύρια διαγώνιό τους και ίσες με 0_F σε κάθε άλλη θέση, μέ μόνη εξαίρεση τη θέση την ευρισκόμενη στην j-οστή γραμμή και στην k-οστή στήλη, όπου η εγγραφή τους ορίζεται να είναι ίση με λ. (Σημειωτέον ότι $\mathbf{R}_{jk}(\lambda)^{-1} = \mathbf{R}_{jk}(-\lambda)$.) Έστω τώρα τυχών πίνακας $\mathbf{A} = (a_{jk})_{1 \leq j,k \leq n} \in Z(\mathbf{GL}_n(F))$. Προφανώς,

$$\mathbf{R}_{jk}(1_F)\, \mathbf{A} = \mathbf{A}\, \mathbf{R}_{jk}(1_F) \Rightarrow \mathbf{R}_{jk}(1_F)\, \mathbf{A}\, \mathbf{R}_{jk}(1_F)^{-1} = \mathbf{R}_{jk}(1_F)\, \mathbf{A}\, \mathbf{R}_{jk}(-1_F) = \mathbf{A},$$

[24] Στο εδάφιο 4.2.27 αποδείξαμε ότι $\langle [1\,2] \circ [3\,4] \rangle \not\trianglelefteq \mathfrak{A}_4$. Παρομοίως αποδεικνύεται ότι και οι άλλες έξι κυκλικές υποομάδες τής $\mathfrak{A}_4$ δεν είναι ορθόθετες. (Οι λεπτομέρειες αφήνονται ως άσκηση για τον αναγνώστη.) Ως εκ τούτου, $\mathbf{NSubg}(\mathfrak{A}_4) = \{\{\mathrm{id}\}, \mathbf{V}, \mathfrak{A}_4\}$.

[25] Αυτοί καλούνται, ιδιαιτέρως, **στοιχειώδεις διατμήσεις**.

απ' όπου έπεται ότι

$$\left.\begin{array}{r} a_{jk}+a_{kk}=a_{jk}+a_{jj} \\ a_{jj}=a_{jj}+a_{kj} \end{array}\right\} \Rightarrow a_{kj}=\left\{\begin{array}{ll} 0_F, & \text{όταν } (j,k)\in\{1,..,n\}\times\{1,..,n\}, j\neq k, \\ a_{jj} & \text{όταν } (j,k)\in\{1,..,n\}\times\{1,..,n\}, j=k, \end{array}\right.$$

(με τον $\mathbf{A}$ διάφορο τού μηδενικού πίνακα, διότι $\det(\mathbf{A})\neq 0_F$), οπότε

$$\mathbf{A}\in\left\{\lambda\mathbf{I}_n|\,\lambda\in F^\times\right\}\Rightarrow Z(\mathrm{GL}_n(F))\subseteq\left\{\lambda\mathbf{I}_n|\,\lambda\in F^\times\right\}.$$

Επειδή $\det(\mathbf{R}_{jk}(\lambda))=1_F$ για κάθε $\lambda\in F$, επαναλαμβάνοντας την ίδια επιχειρηματολογία για τυχόντα πίνακα $\mathbf{A}\in Z(\mathrm{SL}_n(F))$ συμπεραίνουμε ότι

$$\left.\begin{array}{r} \exists\lambda\in F^\times(=F\smallsetminus\{0_F\}):\mathbf{A}=\lambda\mathbf{I}_n \\ \det(\mathbf{A})=\lambda^n \end{array}\right\}\Rightarrow\mathbf{A}\in\left\{\lambda\mathbf{I}_n|\,\lambda\in F^\times,\ \lambda^n=1_F\right\},$$

οπότε $Z(\mathrm{SL}_n(F))\subseteq\left\{\lambda\mathbf{I}_n|\,\lambda\in F^\times,\ \lambda^n=1_F\right\}$. □

5.4.13 Σημείωση. (Περί των $\mathrm{PGL}_n(F)$ και $\mathrm{PSL}_n(F)$.) (i) Οι πηλικοομάδες

$$\boxed{\mathrm{PGL}_n(F):=\mathrm{GL}_n(F)/Z(\mathrm{GL}_n(F))}\ \text{και}\ \boxed{\mathrm{PSL}_n(F):=\mathrm{SL}_n(F)/Z(\mathrm{SL}_n(F))}$$

καλούνται **προβολική γενική γραμμική ομάδα** και **προβολική ειδική γραμμική ομάδα** (βαθμού n), αντιστοίχως, **υπεράνω τού** F και παίζουν σημαίνοντα ρόλο στην Προβολική Γεωμετρία. Επί παραδείγματι, η ομάδα $\mathrm{PGL}_{n+1}(\mathbb{R})$ (και αντιστοίχως, η ομάδα $\mathrm{PGL}_{n+1}(\mathbb{C})$) αποτελεί την ομάδα των αυτομορφισμών[26] τού n-διάστατου *πραγματικού προβολικού χώρου* $\mathbb{P}^n_{\mathbb{R}}$ (και αντιστοίχως, τού n-διάστατου *μιγαδικού προβολικού χώρου* $\mathbb{P}^n_{\mathbb{C}}$) ιδωμένου ως *πραγματικού πολυπτύγματος* (και αντιστοίχως, ως *μιγαδικού πολυπτύγματος*).

(ii) Τοπολογικώς, η **μιγαδική προβολική ευθεία** $\mathbb{P}^1_{\mathbb{C}}$ μπορεί να εκληφθεί ως το *επεκτεταμένο μιγαδικό επίπεδο* $\mathbb{C}\cup\{\infty\}$ (ήτοι ως *μονοσημειακή συμπαγοποίηση*[27] τού $\mathbb{C}$ ως προς ένα επισυναπτόμενο *επάπειρον σημείο* "∞"). Ταυτίζοντας το $\mathbb{C}$ με το επίπεδο $\left\{(x_1,x_2,x_3)\in\mathbb{R}^3\ |\ x_3=0\right\}$ τού $\mathbb{R}^3$ μέσω τής

$$\mathbb{C}\ni x_1+ix_2\longleftrightarrow(x_1,x_2,0)\in\mathbb{R}^2\times\{0\},$$

όπου το i συμβολίζει τη φανταστική μονάδα, είναι δυνατόν να ταυτίσουμε τη μιγαδική προβολική ευθεία $\mathbb{P}^1_{\mathbb{C}}$ με τη διδιάστατη μοναδιαία σφαίρα

$$\mathbb{S}^2=\left\{(x_1,x_2,x_3)\in\mathbb{R}^3\ \middle|\ x_1^2+x_2^2+x_3^2=1\right\}$$

[26] Εδώ η λέξη *αυτομορφισμός* αφορά στην τοπολογική-αναλυτική δομή τού $\mathbb{P}^n_{\mathbb{R}}$ (και αντιστοίχως, τού $\mathbb{P}^n_{\mathbb{C}}$). Ένας **αυτομορφισμός** τού $\mathbb{P}^n_{\mathbb{R}}$ (και αντιστοίχως, τού $\mathbb{P}^n_{\mathbb{C}}$) είναι μια αμφιρριπτική απεικόνιση από τον εν λόγω χώρο επί τού εαυτού του που είναι αμφισυνεχής (ως προς τη συνήθη τοπολογία) και μάλιστα αμφιδιαφορίσιμη (και αντιστοίχως, αμφιολόμορφη). Το σύνολο όλων των αυτομορφισμών τού $\mathbb{P}^n_{\mathbb{R}}$ (και αντιστοίχως, τού $\mathbb{P}^n_{\mathbb{C}}$), εφοδιασμένο με την πράξη τής συνθέσεως απεικονίσεων, καθίσταται ομάδα. Αυτή η ομάδα καλείται **ομάδα αυτομορφισμών** τού $\mathbb{P}^n_{\mathbb{R}}$ (και αντιστοίχως, τού $\mathbb{P}^n_{\mathbb{C}}$).

[27] Αυτό σημαίνει ότι η υποβάση τής τοπολογίας με την οποία εφοδιάζεται το $\mathbb{C}\cup\{\infty\}$ συνίσταται (i) από όλα τα ανοικτά υποσύνολα τού $\mathbb{C}$, (ii) από όλα τα σύνολα τής μορφής $\mathbb{C}\smallsetminus A$, όπου A κάποιο συμπαγές τού $\mathbb{C}$, και (iii) από το ίδιο το $\mathbb{C}\cup\{\infty\}$.

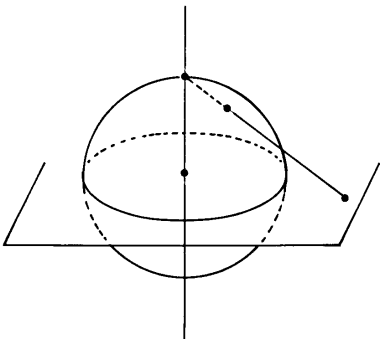
μέσω τής **στερεογραφικής προβολής** $\mathrm{pr}^{[\mathrm{st}]} : \mathbb{S}^2 \to \mathbb{P}^1_{\mathbb{C}}$ (τού $\mathbb{S}^2 \setminus \{(0,0,1)\}$ από τον βόρειο πόλο $(0,0,1)$ τής $\mathbb{S}^2$ επί τού $\mathbb{C}$):

$$\mathbb{S}^2 \ni (x_1,x_2,x_3) \mapsto \mathrm{pr}^{[\mathrm{st}]}(x_1,x_2,x_3) := \begin{cases} \frac{x_1+i\,x_2}{1-x_3}, & \text{όταν } (x_1,x_2,x_3) \neq (0,0,1) \\ \infty, & \text{όταν } (x_1,x_2,x_3) = (0,0,1)\,, \end{cases}$$

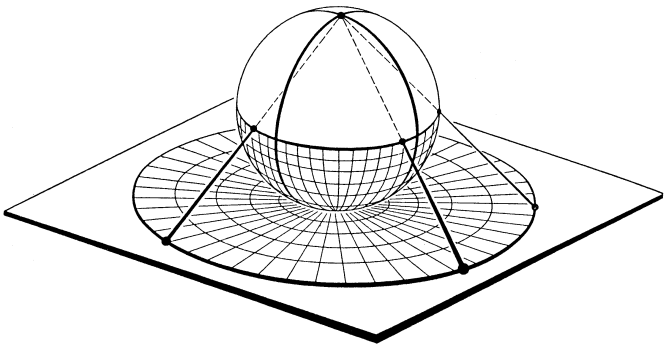
που έχει την

$$\mathbb{P}^1_{\mathbb{C}} \ni z \longmapsto \begin{cases} \frac{\left(2\,\mathrm{Re}(z), 2\,\mathrm{Im}(z), |z|^2-1\right)}{1+|z|^2}, & \text{όταν } z \in \mathbb{C} \\ \infty, & \text{όταν } z = \infty. \end{cases}$$

ως αντίστροφό της (βλ. το ακόλουθο σχήμα).



Σημειωτέον ότι ορισμένοι συγγραφείς, όταν μελετούν τον συσχετισμό τού μοντέλου των E. Beltrami (1835-1900) και F. Klein (1849-1925) για τη *διδιάστατη Υπερβολική Γεωμετρία* με εκείνο τού H. Poincaré (1854-1912), προτιμούν να προβάλουν στερεογραφικώς την $\mathbb{S}^2$ επί τού επιπέδου $\left\{(x_1,x_2,x_3) \in \mathbb{R}^3 \mid x_3 = -1\right\}$ που τέμνει καθέτως τον άξονα των κατηγμένων στον νότιο πόλο της[28] $(0,0,-1)$. Ωστόσο, ακόμη και αν κανείς ταυτίσει *αυτό* το επίπεδο με το $\mathbb{C}$, τοπολογικώς δεν επέρχεται καμία αλλαγή, διότι απλώς μεταβαίνουμε σε έναν διαφορετικό ομοιομορφισμό μεταξύ των $\mathbb{C} \cup \{\infty\}$ και $\mathbb{S}^2$.



[28] Βλ. D. Hilbert, S. Cohn-Vossen: *Anschauliche Geometrie*, Springer-Verlag, 1932 (εν. 36) και M.J. Greenberg: *Euclidean and Non-Euclidean Geometries*, Second Ed., W.H. Freeman & Co., 1974, σελ. 190.

Κάθε πίνακας $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$ γίνεται ο αίτιος για τον ορισμό ενός **μετασχηματισμού τού Möbius**[29] $\sigma_{\mathbf{A}} \in \mathfrak{S}_{\mathbb{P}^1_{\mathbb{C}}}$ μέσω τού τύπου

$$\mathbb{P}^1_{\mathbb{C}} \ni z \longmapsto \sigma_{\mathbf{A}}(z) := \begin{cases} \frac{az+b}{cz+d}, & \text{όταν } c \neq 0 \text{ και } z \in \mathbb{C} \smallsetminus \{-\frac{d}{c}\}, \\ \frac{az+b}{d} & \text{όταν } c = 0\,(\Rightarrow d \neq 0) \text{ και } z \in \mathbb{C}, \\ \frac{a}{c}, & \text{όταν } c \neq 0 \text{ και } z = \infty, \\ \infty, & \text{όταν } c \neq 0 \text{ και } z = -\frac{d}{c}, \\ \infty, & \text{όταν } c = 0 \text{ και } z = \infty, \end{cases}$$

(Προφανώς, για $c \neq 0$ έχουμε $\frac{a}{c} = \lim\limits_{z \longrightarrow \infty} \left(\frac{az+b}{cz+d}\right)$ και $\infty = \lim\limits_{z \longrightarrow -\frac{d}{c}} \left(\frac{az+b}{cz+d}\right)$.) Επειδή $\sigma_{\mathbf{I}_2} = \mathrm{id}_{\mathbb{P}^1_{\mathbb{C}}}$ και $\sigma_{\mathbf{A}} \circ \sigma_{\mathbf{B}}^{-1} = \sigma_{\mathbf{A}} \circ \sigma_{\mathbf{B}^{-1}} = \sigma_{\mathbf{AB}^{-1}} \in \mathfrak{S}_{\mathbb{P}^1_{\mathbb{C}}}$, δημιουργείται κατ' αυτόν τον τρόπο μια υποομάδα

$$\boxed{\mathbf{Möb} := \{\sigma_{\mathbf{A}} \,|\mathbf{A} \in \mathrm{GL}_2(\mathbb{C})\,\} \sqsubseteq \quad \mathfrak{S}_{\mathbb{P}^1_{\mathbb{C}}}}$$

η οποία καλείται, ιδιαιτέρως, **ομάδα τού Möbius**. Η απεικόνιση

$$\mathrm{GL}_2(\mathbb{C}) \ni \mathbf{A} \longmapsto \sigma_{\mathbf{A}} \in \mathbf{Möb}$$

είναι επιμορφισμός ομάδων έχων ως πυρήνα του την ομάδα

$$\left\{\mathbf{A} \in \mathrm{GL}_2(\mathbb{C}) \,|\sigma_{\mathbf{A}} = \ \mathrm{id}_{\mathbb{P}^1_{\mathbb{C}}}\right\} \ = \ \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C}) \,\middle|\, b = c = 0 \text{ και } a = d \right\}$$

$$= \ \{\,\lambda \mathbf{I}_2 |\, \lambda \in \mathbb{C} \smallsetminus \{0\}\} = Z(\mathrm{GL}_2(\mathbb{C})).$$

Δυνάμει τού 1ου θεωρήματος ισομορφισμών 4.5.2,

$$\boxed{\mathrm{PGL}_2(\mathbb{C}) \cong \mathbf{Möb},}$$

δηλαδή η ομάδα αυτομορφισμών τής μιγαδικής προβολικής ευθείας $\mathbb{P}^1_{\mathbb{C}}$ είναι ισόμορφη με την ομάδα τού Möbius.

(iii) Οι προβολικές ειδικές γραμμικές ομάδες $\mathrm{PSL}_n(F)$ είναι ιδιαίτερα «δημοφιλείς» όταν το F είναι ένα *πεπερασμένο σώμα*. Π.χ., είναι εύκολο να αποδειχθεί ότι $\mathrm{PSL}_2(\mathbb{Z}_2) \cong \mathfrak{S}_3$, $\mathrm{PSL}_2(\mathbb{Z}_3) \cong \mathfrak{A}_4$ και $\mathrm{PSL}_2(\mathbb{Z}_5) \cong \mathfrak{A}_5$. Αντιθέτως, είναι αρκετά μακροσκελής η απόδειξη τού ότι *για ένα (πεπερασμένο ή άπειρο) σώμα F οι προβολικές ειδικές γραμμικές ομάδες $\mathrm{PSL}_n(F)$ είναι απλές*[30] όταν ισχύει *είτε* $n \geq 3$ *είτε* $(n, \chi\alpha\rho(F)) \notin \{(2,2),(2,3)\}$.

[29] Οι μετασχηματισμοί αυτοί ονομάσθηκαν έτσι προς τιμήν τού Γερμανού μαθηματικού August Ferdinand Möbius (1790-1868), ο οποίος κατέδειξε τη σημαντικότητά τους μέσω ποικίλων εφαρμογών τους στη Γεωμετρία, στη Μιγαδική Ανάλυση και στη Μαθηματική Φυσική.

[30] Η πρώτη απόδειξη (για πεπερασμένα σώματα, η οποία μπορεί να τροποποιηθεί καταλλήλως και για άπειρα σώματα) οφείλεται στον L.E. Dickson (1874-1954) και παρουσιάσθηκε στις ενότητες 104-105 τού συγγράμματός του: *Linear groups with an exposition of the Galois field theory*, Leipzig, 1901 (reprinted by Dover Publ., NY, 1958). Η σκιαγράφηση μιας «μοντέρνας» αποδείξεως εντοπίζεται σε ένα βιβλίο τού J. Dieudonné (1906-1992) που φέρει τον τίτλο *La géométrie des groupes classiques*, Springer-Verlag, 1955 (βλ. κεφ. II, εν. 1), καθώς και σε ένα βιβλίο τού E. Artin (1898-1962) υπό τον τίτλο *Geometric Algebra*, J. Wiley, Inc., 1957 (βλ. θεώρημα 4.10, σελ. 169). Για μια διεξοδική απόδειξη ο αναγνώστης παραπέμπεται στο θεώρημα 9.46, σελ. 279, τού βιβλίου τού J.J. Rotman: *An Introduction to the Theory of Groups*, GTM, Vol. **148**, Springer-Verlag, fourth ed., 1995.

(iv) Επανερχόμενοι, τέλος, στην Κλασική Γεωμετρία, συναντούμε την πασίγνωστη απλή ομάδα

$$\boxed{\mathrm{GL}_3(\mathbb{Z}_2) \cong \mathrm{PSL}_2(\mathbb{Z}_7) \cong \mathrm{PSL}_3(\mathbb{Z}_2)}$$

με 168 στοιχεία (που είναι η δεύτερη κατά σειράν ομάδα στους καταλόγους II και III τής σελίδας 660), καθόσον είναι ισόμορφη με την ομάδα των αυτομορφισμών $\mathrm{Aut}(C)$ τής μιγαδικής (μη ιδιάζουσας) **τεταρτοβάθμιας καμπύλης τού Klein** (Klein's quartic)

$$C := \left\{ [z_0 : z_1 : z_2] \in \mathbb{P}^2_{\mathbb{C}} \middle| \, z_0^3 z_1 + z_1^3 z_2 + z_2^3 z_0 = 0 \right\}$$

γένους[31] 3 (εξ ου και οι τρεις οπές[32] στη σχηματική αναπαράσταση τής $C \cap \mathbb{R}^3$).

5.4.14 Πρόταση. (Τα κέντρα των $\mathbf{O}_n(\mathbb{R})$ και $\mathbf{SO}_n(\mathbb{R})$.) *Το κέντρο τής ορθογώνιας ομάδας* $\mathrm{O}_n(\mathbb{R})$ *είναι το* $Z(\mathrm{O}_n(\mathbb{R})) = Z(\mathrm{GL}_n(\mathbb{R})) \cap \mathrm{O}_n(\mathbb{R}) = \{\mathbf{I}_n, -\mathbf{I}_n\}$, *τής δε ειδικής ορθογώνιας ομάδας* $\mathrm{SO}_n(\mathbb{R})$ *το*

$$Z(\mathrm{SO}_n(\mathbb{R})) = Z(\mathrm{O}_n(\mathbb{R})) \cap \mathrm{SO}_n(\mathbb{R}) = \begin{cases} \{\mathbf{I}_n\}, & \text{όταν ο } n \text{ είναι περιττός,} \\ \{\mathbf{I}_n, -\mathbf{I}_n\}, & \text{όταν ο } n \text{ είναι άρτιος.} \end{cases}$$

ΑΠΟΔΕΙΞΗ. Οι εγκλεισμοί " $\supseteq$ " είναι προφανείς. Γι' αυτό θεωρούμε τυχόντα πίνακα $\mathbf{A} \in Z(\mathrm{O}_n(\mathbb{R}))$, εφαρμόζουμε εκ νέου το τέχνασμα (με τους βοηθητικούς πίνακες $\mathbf{E}_{jk}(\lambda)$) που υπεισέρχεται στην απόδειξη τής προτάσεως 5.4.12 και καταλήγουμε στο ότι

$$\mathbf{A} \in \{ \lambda \mathbf{I}_n \,|\, \lambda \in \mathbb{R} \smallsetminus \{0\} \} = Z(\mathrm{GL}_n(\mathbb{R})).$$

[31] Σύμφωνα με ένα αποτέλεσμα τού A. Hurwitz (1859-1919), η τάξη τής ομάδας αυτομορφισμών μιας επιφάνειας Riemann γένους $g \geq 2$ είναι $\leq 84(g-1)$. (Βλ. A. Hurwitz: *Über algebraische Gebilde mit eindeutigen Transformationen in sich,* Math. Ann., Bd. **41** (1893), 403-442, για την πρωτότυπη εργασία και R. Miranda: *Algebraic Curves and Riemann Surfaces*, Graduate Studies in Math., Vol. **5**, A.M.S., 1997, Thm. 3.9, σελ. 82, για μια απλή σύγχρονη απόδειξη.) Δεν υφίσταται επιφάνεια Riemann γένους $g = 2$, η ομάδα αυτομορφισμών τής οποίας να έχει τάξη ίση με 84. Όμως η ανωτέρω μιγαδική (μη ιδιάζουσα) καμπύλη C (ιδωθείσα ως επιφάνεια Riemann γένους $g = 3$) διαθέτει ομάδα αυτομορφισμών τάξεως $|\mathrm{Aut}(C)| = 84 \cdot 2 = 168$, ήτοι ακριβώς ίσης με το μέγιστο άνω φράγμα. Κατά τον Hurwitz, για όσες επιφάνειες Riemann S έχουν αυτήν την ιδιότητα, ο πηλικόχωρος $S/\mathrm{Aut}(S)$ είναι μια νέα επιφάνεια Riemann γένους 0 (τοπολογικώς η $\mathbb{S}^2$), η δε φυσική επίρριψη $S \longrightarrow \widetilde{S} = S/\mathrm{Aut}(S)$ είναι μια κανονική επικάλυψη διακλαδιζόμενη υπεράνω ακριβώς τριών σημείων τής $\widetilde{S}$, με τάξεις διακλαδώσεως 2, 3 και 7, αντιστοίχως.

[32] Ο αναγνώστης που βλέπει 4 οπές, παραπέμπεται στην πλήρη τριδιάστατη φιλμική αναπαράσταση (για να κανονήσει σε τι οφείλεται η οφθαλμαπάτη) στη διαδικτυακή διεύθυνση:
http://gregegan.customer.netspace.net.au/SCIENCE/KleinQuartic/KleinQuartic.html

Επειδή $\mathbf{A} \in \mathrm{O}_n(\mathbb{R}) \Rightarrow \mathbf{A}^{\intercal} = \mathbf{A}^{-1}$, έχουμε

$$(\det(\mathbf{A}))^2 = \det(\mathbf{A})\det(\mathbf{A}^{\intercal}) = \det(\mathbf{A})\det(\mathbf{A}^{-1}) = \det(\mathbf{A}\mathbf{A}^{-1}) = \det(\mathbf{I}_n) = 1,$$

ήτοι $\det(\mathbf{A}) \in \{\pm 1\}$. Κατά συνέπειαν,

$$\left.\begin{array}{r} \exists \lambda \in \mathbb{R}\smallsetminus\{0\} : \mathbf{A} = \lambda \mathbf{I}_n \\ \det(\mathbf{A}\,) = \lambda^n \in \{\pm 1\} \end{array}\right\} \Rightarrow \lambda \in \{\pm 1\},$$

οπότε $Z(\mathrm{O}_n(\mathbb{R})) = Z(\mathbf{GL}_n(\mathbb{R})) \cap \mathrm{O}_n(\mathbb{R}) = \{\mathbf{I}_n, -\mathbf{I}_n\}$. Κατ' αναλογίαν, εκκινώντας από τυχόντα πίνακα $\mathbf{A} \in Z(\mathbf{SO}_n(\mathbb{R}))$ και επαναλαμβάνοντας την ίδια διαδικασία συμπεραίνουμε ότι

$$\left.\begin{array}{r} \exists \lambda \in \mathbb{R}\smallsetminus\{0\} : \mathbf{A} = \lambda \mathbf{I}_n \\ \det(\mathbf{A}\,) = \lambda^n = 1 \end{array}\right\} \Rightarrow \lambda = \left\{\begin{array}{ll} 1, & \text{όταν ο } n \text{ είναι περιττός,} \\ 1 \text{ ή } -1, & \text{όταν ο } n \text{ είναι άρτιος,} \end{array}\right.$$

απ' όπου έπεται το ζητούμενο. □

5.4.15 Πρόταση. (Τα κέντρα των $\mathbf{U}_n(\mathbb{C})$ και $\mathbf{SU}_n(\mathbb{C})$.) *Το κέντρο τής μοναδιακής ομάδας* $\mathrm{U}_n(\mathbb{C})$ *είναι το*

$$Z(\mathrm{U}_n(\mathbb{C})) = Z(\mathbf{GL}_n(\mathbb{C})) \cap \mathrm{U}_n(\mathbb{C}) = \{\, z\mathbf{I}_n |\, z \in \mathbb{C},\ |z| = 1\} \cong \mathbb{S}^1,$$

τής δε ειδικής μοναδιακής ομάδας $\mathrm{SU}_n(\mathbb{C})$ *το*

$$Z(\mathrm{SU}_n(\mathbb{C})) = Z(\mathrm{U}_n(\mathbb{C})) \cap \mathrm{SU}_n(\mathbb{C}) = \{\, z\mathbf{I}_n |\, z \in \mathbb{C},\ z^n = 1\} \cong \mathcal{E}_n.$$

ΑΠΟΔΕΙΞΗ. Οι εγκλεισμοί " $\supseteq$ " είναι προφανείς. Γι' αυτό θεωρούμε τυχόντα πίνακα $\mathbf{A} \in Z(\mathrm{U}_n(\mathbb{C}))$, εφαρμόζουμε εκ νέου το τέχνασμα (με τους βοηθητικούς πίνακες) που υπεισέρχεται στην απόδειξη τής προτάσεως 5.4.12 και καταλήγουμε στο ότι $\mathbf{A} \in \{\, z\mathbf{I}_n |\, z \in \mathbb{C}\smallsetminus\{0\}\} = Z(\mathbf{GL}_n(\mathbb{C}))$. Επειδή $\mathbf{A} \in \mathrm{U}_n(\mathbb{C}) \Rightarrow \overline{\mathbf{A}}^{\intercal} = \mathbf{A}^{-1}$, έχουμε

$$\mathbf{A}\overline{\mathbf{A}}^{\intercal} = \mathbf{I}_n \Rightarrow 1 = \det(\mathbf{I}_n) = \det(\mathbf{A})\det(\overline{\mathbf{A}}^{\intercal}) = \det(\mathbf{A})\det(\overline{\mathbf{A}}) = \det(\mathbf{A})\,\overline{\det(\mathbf{A})},$$

ήτοι $\det(\mathbf{A})\,\overline{\det(\mathbf{A})} = |\det(\mathbf{A})|^2 = 1 \Rightarrow |\det(\mathbf{A})| = 1$. Κατά συνέπειαν,

$$\left.\begin{array}{r} \exists z \in \mathbb{C}\smallsetminus\{0\} : \mathbf{A} = z\mathbf{I}_n \\ |\det(\mathbf{A}\,)| = |z^n| = |z|^n = 1 \end{array}\right\} \Rightarrow |z| = 1,$$

οπότε $Z(\mathrm{U}_n(\mathbb{C})) = \{\, z\mathbf{I}_n |\, z \in \mathbb{C},\ |z| = 1\} \cong \mathbb{S}^1$. Κατ' αναλογίαν, εκκινώντας από τυχόντα πίνακα $\mathbf{A} \in Z(\mathrm{SU}_n(\mathbb{C}))$ και επαναλαμβάνοντας την ίδια διαδικασία συμπεραίνουμε ότι

$$\left.\begin{array}{r} \exists z \in \mathbb{C}\smallsetminus\{0\} : \mathbf{A} = z\mathbf{I}_n \\ \det(\mathbf{A}\,) = 1 \end{array}\right\} \Rightarrow z^n = 1,$$

απ' όπου έπεται το ζητούμενο. □

5.4.16 Σημείωση. Κατ' αναλογίαν προς τις $\mathrm{PGL}_n(F)$ και $\mathrm{PSL}_n(F)$ ορίζονται και οι **προβολικές ορθογώνιες** και **προβολικές ειδικές ορθογώνιες ομάδες**

$$\boxed{\mathrm{PO}_n(\mathbb{R}) := \mathrm{O}_n(\mathbb{R})/Z(\mathrm{O}_n(\mathbb{R}))} \text{ και } \boxed{\mathrm{PSO}_n(\mathbb{R}) := \mathrm{SO}_n(\mathbb{R})/Z(\mathrm{SO}_n(\mathbb{R})),}$$

καθώς και οι **προβολικές μοναδιακές** και **προβολικές ειδικές μοναδιακές ομάδες**

$$\boxed{\mathrm{PU}_n(\mathbb{C}) := \mathrm{U}_n(\mathbb{C})/Z(\mathrm{U}_n(\mathbb{C}))} \text{ και } \boxed{\mathrm{PSU}_n(\mathbb{C}) := \mathrm{SU}_n(\mathbb{C})/Z(\mathrm{SU}_n(\mathbb{C})),}$$

αντιστοίχως.

Η παρούσα ενότητα θα κλείσει με την παράθεση προτάσεων οι οποίες περιγράφουν ορισμένες βασικές ιδιότητες τού κέντρου μιας ομάδας.

5.4.17 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Η πηλικοομάδα $G/Z(G)$ δεν είναι κυκλική, εκτός και εάν η ίδια η G είναι αβελιανή (οπότε η $G/Z(G)$ είναι η τετριμμένη ομάδα).*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι η $G/Z(G)$ είναι κυκλική. Τότε υπάρχει κάποιο στοιχείο $g \in G$, τέτοιο ώστε να ισχύει $G/Z(G) = \langle gZ(G)\rangle$. Εάν $x, y \in G$, τότε

$$xZ(G), yZ(G) \in G/Z(G) \Rightarrow \begin{cases} \exists m \in \mathbb{Z} : xZ(G) = (gZ(G))^m = g^m Z(G) \text{ και} \\ \exists n \in \mathbb{Z} : yZ(G) = (gZ(G))^n = g^n Z(G). \end{cases}$$

Επομένως έχουμε[33] $xZ(G) = g^m Z(G) \Rightarrow \exists z \in Z(G) : x = g^m z$. Κατ' αναλογίαν, $\exists w \in Z(G) : y = g^n w$. Ως εκ τούτου,

$$\begin{aligned} xy &= (g^m z)\,(g^n w) = g^m (z g^n) w = g^m (g^n z) w = g^{m+n} z w \\ &= g^{n+m} w z = g^n (g^m w) z = g^n (w g^m) z = (g^n w)\,(g^m z) = yx, \end{aligned}$$

οπότε η G είναι αβελιανή. □

5.4.18 Παραδείγματα. (i) Υπάρχουν *μη αβελιανές* ομάδες G, τέτοιες ώστε οι πηλικοομάδες $G/Z(G)$ να είναι *αβελιανές*, *μη κυκλικές*! Επί παραδείγματι, η απεικόνιση

$$\pm\mathbf{I}_2 \longmapsto \mathrm{id},\ \pm\mathbf{i} \longmapsto [1\,2] \circ [3\,4]\,,\ \pm\mathbf{j} \longmapsto [1\,3] \circ [2\,4]\,,\ \pm\mathbf{k} \longmapsto [1\,4] \circ [2\,3]\,,$$

είναι ένας επιμορφισμός από την ομάδα $\mathbf{Q}$ των τετρανίων επί τής ομάδας $\mathbf{V}$ των τεσσάρων στοιχείων τού Klein έχων το κέντρο $Z(\mathbf{Q}) = \{\mathbf{I}_2, -\mathbf{I}_2\}$ ως πυρήνα του. Σύμφωνα με το 1ο θεώρημα ισομορφισμών 4.5.2 υφίσταται ένας ισομορφισμός

$$\mathbf{Q}/Z(\mathbf{Q}) \xrightarrow{\cong} \mathbf{V}.$$

(ii) Έστω $n \in \mathbb{N}$, $n \geq 3$. Για την n-οστή διεδρική ομάδα $\mathbf{D}_n = \langle \alpha, \beta\rangle$ έχουμε $\mathbf{D}_n/Z(\mathbf{D}_n) \cong \mathbf{D}_n$ όταν ο n είναι *περιττός*, καθότι σε αυτήν την περίπτωση το

[33] Εξ ορισμού, $xZ(G) = g^m Z(G)$ σημαίνει ότι $x^{-1}g^m = t \in Z(G)$, οπότε αρκεί κανείς να θέσει $z := t^{-1}$.

κέντρο της είναι τετριμμένο (βλ. 5.4.8). Από την άλλη μεριά, όταν ο n είναι *άρτιος*, είναι εύκολο να διαπιστωθεί ότι η απεικόνιση

$$\mathbf{D}_n/Z(\mathbf{D}_n) \ni (\alpha^j \circ \beta^k) \circ Z(\mathbf{D}_n) \longmapsto \alpha^j \circ \beta^{2k} \in \left\langle \alpha, \beta^2 \right\rangle,$$

$j \in \{0,1\},\ k \in \{0,1,...,n-1\}$, είναι ισομορφισμός ομάδων και, ως εκ τούτου,

$$\mathbf{D}_n/Z(\mathbf{D}_n) \cong \left\langle \alpha, \beta^2 \right\rangle \cong \begin{cases} \mathbf{V}, & \text{όταν } n = 4, \\ \mathbf{D}_{\frac{n}{2}}, & \text{όταν ο } n \text{ είναι άρτιος } \geq 6. \end{cases}$$

5.4.19 Πρόταση. *Για οιαδήποτε ομάδα $(G, \cdot)$ ισχύουν τα ακόλουθα*:

(i) *Εάν $H \sqsubseteq Z(G)$, τότε $H \trianglelefteq G$.*

(ii) *Εάν $H \sqsubseteq Z(G)$ και $K \sqsubseteq G$, τότε $HK \sqsubseteq G$.*

(iii) *Εάν $K \sqsubseteq G$ και εάν η πηλικοομάδα $G/Z(G)$ είναι αβελιανή, τότε και η πηλικοομάδα $K/Z(K)$ είναι αβελιανή.*

ΑΠΟΔΕΙΞΗ. (i) Έστω $H \sqsubseteq Z(G)$. Εάν $h \in H$ και $g \in G$, τότε $h \in Z(G)$, οπότε

$$ghg^{-1} = hgg^{-1} = he = h \in H \Rightarrow gHg^{-1} \subseteq H \Rightarrow H \trianglelefteq G.$$

(ii) Εάν $x \in H \subseteq Z(G)$, τότε $xg = gx$ για κάθε $g \in G$, και -ιδιαιτέρως- $xy = yx$ για κάθε $y \in K$, οπότε $HK = KH$. Άρα το γινόμενο HK των H και K αποτελεί μια υποομάδα τής G επί τη βάσει τής προτάσεως 4.1.4.

(iii) Λόγω των ανωτέρω (i) και (ii) έχουμε $Z(G) \trianglelefteq G$ και $Z(G)K \sqsubseteq G$. Παρατηρούμε ότι $Z(G) \trianglelefteq G,\ Z(G) \sqsubseteq Z(G)K \underset{4.2.19}{\Longrightarrow} Z(G) \trianglelefteq Z(G)K$. Άρα ορίζεται η πηλικοομάδα $Z(G)K/Z(G)$. Αυτή, λόγω τού 4.4.15 (i), είναι μια υποομάδα τής πηλικοομάδας $G/Z(G)$. Εξ υποθέσεως, η $G/Z(G)$ είναι αβελιανή, οπότε και η $Z(G)K/Z(G)$ είναι αβελιανή. Επιπροσθέτως, από το 2ο θεώρημα ισομορφισμών ομάδων 4.5.13 έπεται ότι

$$Z(G)K/Z(G) \cong K/(K \cap Z(G)).$$

Άρα και η $K/(K \cap Z(G))$ είναι αβελιανή ομάδα. Η τομή $K \cap Z(G)$ των ομάδων K και $Z(G)$ είναι μια υποομάδα τού κέντρου $Z(K)$. (Πράγματι· για οιαδήποτε στοιχεία $a \in K \cap Z(G)$ και $b \in K$ έχουμε $ab = ba$, διότι $a \in Z(G)$, οπότε $a \in Z(K)$. Συνεπώς, $K \cap Z(G) \subseteq Z(K)$ και $Z(K) \sqsubseteq G \underset{2.1.20}{\Longrightarrow} K \cap Z(G) \sqsubseteq Z(K)$.) Ως εκ τούτου, βάσει τής προτάσεως 5.4.2 (εφαρμοζόμενης για $G = K$) και τού (i) έχουμε

$$Z(K) \trianglelefteq K \ \text{ και } \ K \cap Z(G) \trianglelefteq K.$$

Τούτο σημαίνει ότι έχουμε τη δυνατότητα εφαρμογής τού 3ου θεωρήματος ισομορφισμών ομάδων 4.5.21, από το οποίο λαμβάνουμε

$$K/Z(K) \cong (K/(K \cap Z(G)))/(Z(K)/(K \cap Z(G))).$$

Επειδή η $K/(K \cap Z(G))$ είναι αβελιανή και η $K/Z(K)$ είναι ισόμορφη με την $(K/(K \cap Z(G)))/N$ (όπου $N := Z(K)/(K \cap Z(G))$), *και η ίδια* η $K/Z(K)$ ειναι *αβελιανή* λόγω τού (ii) τής προτάσεως 2.4.19 και τού (ii) τής προτάσεως 4.4.2. □

5.4.20 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Εάν $H \sqsubseteq Z(G)$ και εάν η πηλικοομάδα G/H είναι κυκλική, τότε η G είναι αβελιανή.*

ΑΠΟΔΕΙΞΗ. Επειδή $H \sqsubseteq Z(G) \underset{5.4.19\,(i)}{\Longrightarrow} H \trianglelefteq G$, ορίζεται η πηλικοομάδα G/H. Εάν η G/H είναι κυκλική, αρκεί να επαναληφθεί ό,τι προαναφέρθηκε στην απόδειξη τής προτάσεως 5.4.17 αλλά με την H στη θέση τού κέντρου $Z(G)$ τής G. □

5.4.21 Συμβολισμός. Έστω $(G,\cdot)$ μια ομάδα και έστω $g \in G$. Ως γ_g συμβολίζουμε την απεικόνιση

$$\boxed{\gamma_g : G \longrightarrow G, \quad \gamma_g(x) = gxg^{-1}, \ \ \forall x \in G,}$$

που στέλνει κάθε στοιχείο $x \in G$ να απεικονισθεί στο συζυγές του gxg^{-1} το δημιουργούμενο μέσω τού g.

5.4.22 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Τότε $\gamma_g \in \mathrm{Aut}(G)$ για κάθε $g \in G$.*

ΑΠΟΔΕΙΞΗ. Έστω τυχόν $g \in G$. Κατ' αρχάς, $\gamma_g \in \mathrm{End}(G)$, διότι για οιαδήποτε $x, y \in G$ έχουμε $\gamma_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \gamma_g(x)\gamma_g(y)$. Η γ_g είναι επιμορφισμός, διότι για οιοδήποτε $z \in G$ ισχύει $\gamma_g(g^{-1}zg) = z$. Επιπροσθέτως, $\mathrm{Ker}(\gamma_g) = \{\, x \in G |\, gxg^{-1} = e_G\} = \{e_G\}$. Άρα η γ_g είναι *και* μονομορφισμός επί τη βάσει τής προτάσεως 2.4.15. Επομένως, $\gamma_g \in \mathrm{Aut}(G)$. □

5.4.23 Ορισμός. Έστω $(G,\cdot)$ μια ομάδα. Τότε κάθε αυτομορφισμός τής G που είναι τής μορφής γ_g, για κάποιο στοιχείο $g \in G$, καλείται **εσωτερικός αυτομορφισμός** τής G. Το σύνολο των εσωτερικών αυτομορφισμών τής G συμβολίζεται ως ακολούθως:

$$\boxed{\mathrm{Inn}(G) := \big\{\, \gamma_g \big|\, g \in G\big\} \subseteq \mathrm{Aut}(G).}$$

5.4.24 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \sqsubseteq G$. Οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) $H \trianglelefteq G$.

(ii) $\gamma_g(H) \subseteq H, \ \forall g \in G$.

(iii) $\gamma_g(H) \sqsubseteq H, \ \forall g \in G$.

(iv) $\gamma_g(H) = H, \ \forall g \in G$.

ΑΠΟΔΕΙΞΗ. Επειδή $\gamma_g(H) = gHg^{-1}, \ \forall g \in G$, η αμφίπλευρη συνεπαγωγή (i)⇔(ii) προκύπτει από τα εδάφια 4.2.1 (v) και 4.2.2, η (ii)⇒(iii) είναι προφανής και η (iii)⇒(ii) έπεται από το πόρισμα 2.1.20. Τέλος, η (i)⇔(iv) προκύπτει από τα εδάφια 4.2.1 (iv) και 4.2.2. □

5.4.25 Πρόταση. *Για κάθε ομάδα $(G,\cdot)$ ισχύει* $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

ΑΠΟΔΕΙΞΗ. Για οιαδήποτε $g_1, g_2, g \in G$ έχουμε

$$\boldsymbol{\gamma}_{g_1} \circ \boldsymbol{\gamma}_{g_2} = \boldsymbol{\gamma}_{g_1 g_2} \ \text{ και } \ \boldsymbol{\gamma}_g^{-1} = \boldsymbol{\gamma}_{g^{-1}}, \tag{5.38}$$

διότι για κάθε $x \in G$ ισχύουν οι ισότητες

$$\boldsymbol{\gamma}_{g_1}(\boldsymbol{\gamma}_{g_2}(x)) = g_1 \left(g_2 x g_2^{-1}\right) g_1^{-1} = (g_1 g_2)\, x\, (g_1 g_2)^{-1} = \boldsymbol{\gamma}_{g_1 g_2}(x)$$

και $\boldsymbol{\gamma}_{g^{-1}}(\boldsymbol{\gamma}_g(x)) = g^{-1}\left(g x g^{-1}\right) g = x = g\left(g^{-1} x g\right) g^{-1} = \boldsymbol{\gamma}_g(\boldsymbol{\gamma}_{g^{-1}}(x))$. Άρα $\mathrm{Inn}(G) \sqsubseteq \mathrm{Aut}(G)$ (σύμφωνα με το (ii) της προτάσεως 2.1.16). Εξάλλου, για κάθε $\vartheta \in \mathrm{Aut}(G)$ και κάθε $g \in G$ έχουμε

$$\begin{aligned} (\vartheta \circ \boldsymbol{\gamma}_g \circ \vartheta^{-1})(x) &= \vartheta\left(g \vartheta^{-1}(x) g^{-1}\right) = \vartheta(g) x \vartheta(g^{-1}) \\ &= \vartheta(g) x \vartheta(g)^{-1} = \boldsymbol{\gamma}_{\vartheta(g)}(x),\ \forall x \in G, \end{aligned} \tag{5.39}$$

οπότε $\vartheta \circ \boldsymbol{\gamma}_g \circ \vartheta^{-1} = \boldsymbol{\gamma}_{\vartheta(g)} \in \mathrm{Inn}(G) \Longrightarrow \mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. □

5.4.26 Θεώρημα. *Έστω $(G, \cdot)$ μια ομάδα και έστω $H \sqsubseteq G$. Τότε η πηλικοομάδα $\mathrm{N}_G(H)/\mathrm{C}_G(H)$ είναι εμφυτεύσιμη στην $\mathrm{Aut}(H)$.* (Βλ. 2.4.14 και 2.4.17.)

ΑΠΟΔΕΙΞΗ. Ως γνωστόν, $\mathrm{C}_G(H) \trianglelefteq \mathrm{N}_G(H)$ (βλ. 5.2.4 (vii)). Ορίζουμε την απεικόνιση

$$f_H : \mathrm{N}_G(H) \longrightarrow \mathrm{Aut}(H),\ \ g \longmapsto f_H(g) := \boldsymbol{\gamma}_g\big|_H .$$

Η f είναι ένας ομομορφισμός ομάδων, διότι για οιαδήποτε $g_1, g_2 \in \mathrm{N}_G(H)$ έχουμε

$$f_H(g_1 g_2) = \boldsymbol{\gamma}_{g_1 g_2}\big|_H = \left(\boldsymbol{\gamma}_{g_1}\big|_H\right) \circ \left(\boldsymbol{\gamma}_{g_2}\big|_H\right) = f_H(g_1) \circ f_H(g_2),$$

καθόσον $\boldsymbol{\gamma}_{g_1 g_2}(x) = (g_1 g_2)\, x\, (g_1 g_2)^{-1} = g_1\left(g_2 x g_2^{-1}\right) g_1^{-1} = \boldsymbol{\gamma}_{g_1}(\boldsymbol{\gamma}_{g_2}(x)), \forall x \in H$. Ο πυρήνας του είναι ο

$$\begin{aligned} \mathrm{Ker}\,(f) &= \{\, g \in \mathrm{N}_G(H) |\, f_H(g) = \mathrm{id}_H \} = \left\{ g \in \mathrm{N}_G(H) \,\middle|\, \boldsymbol{\gamma}_g\big|_H = \mathrm{id}_H \right\} \\ &= \{ g \in \mathrm{N}_G(H)\, | gh = hg, \forall h \in H \} = \mathrm{C}_G(H). \end{aligned}$$

Σύμφωνα με το θεώρημα 4.5.2 υπάρχει ισομορφισμός

$$\mathrm{N}_G(H)/\mathrm{C}_G(H) \xrightarrow{\ \cong\ } \mathrm{Im}(f_H). \tag{5.40}$$

Άρα η πηλικοομάδα $\mathrm{N}_G(H)/\mathrm{C}_G(H)$ είναι ισόμορφη με την υποομάδα $\mathrm{Im}(f_H)$ της ομάδας αυτομορφισμών $\mathrm{Aut}(H)$ της H. □

5.4.27 Εφαρμογή. *Έστω $(G, \cdot)$ μια πεπερασμένη μη τετριμμένη ομάδα και έστω*

$$p := \min \{ q \in \mathbb{N} \,|\, q \text{ πρώτος και } \ q \mid |G| \}.$$

Εάν $H \trianglelefteq G$ με $|H| = p$, τότε $H \sqsubseteq Z(G)$.

ΑΠΟΔΕΙΞΗ. Επειδή $H \trianglelefteq G$, έχουμε $\mathrm{N}_G(H) = G$ (βλ. 5.2.4 (iii)). Επειδή $|H| = p$, η H είναι κατ' ανάγκην κυκλική (βλ. πόρισμα 4.1.33). Επομένως, σύμφωνα με (ii) τού θεωρήματος 2.4.32, $\mathrm{Aut}(H) \cong \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^\times \Longrightarrow |\mathrm{Aut}(H)| = p-1$. Ας υποθέσουμε ότι

$$|G| = q_1^{\nu_1} \cdots q_k^{\nu_k},\ k \in \mathbb{N},\ \nu_1,...,\nu_k \in \mathbb{N},\ q_1 < \cdots < q_k,$$

είναι η κανονική παράσταση (B.19) τής τάξεως $|G|$ ως γινομένου πρώτων αριθμών $q_1,...,q_k$. Εξ υποθέσεως, $p = q_1$. Εξάλλου, επειδή $|\mathrm{C}_G(H)| \mid |G|$, υπάρχουν (βάσει τού λήμματος B.3.14) $\mu_1,...,\mu_k \in \mathbb{N}_0$, τέτοιοι ώστε να ισχύει

$$|\mathrm{C}_G(H)| = q_1^{\mu_1} \cdots q_k^{\mu_k},\ \mu_j \leq \nu_j,\ \forall j \in \{1,...,k\}.$$

Σύμφωνα με το θεώρημα 5.4.26,

$$|\mathrm{N}_G(H)/\mathrm{C}_G(H)| = \frac{|\mathrm{N}_G(H)|}{|\mathrm{C}_G(H)|} = \frac{|G|}{|\mathrm{C}_G(H)|} = q_1^{\nu_1-\mu_1} \cdots q_k^{\nu_k-\mu_k}$$

$$= |\mathrm{Im}(f_H)| \leq |\mathrm{Aut}(H)| = p-1 < p = q_1,$$

οπότε $[\mu_j = \nu_j, \forall j \in \{1,...,k\}] \Rightarrow |\mathrm{C}_G(H)| = |G| \Rightarrow \mathrm{C}_G(H) = G$, απ' όπου έπεται ότι $H \sqsubseteq Z(G)$ (βλ. 5.4.3 (ii)). □

5.4.28 Πόρισμα. *Για κάθε ομάδα $(G,\cdot)$ υφίσταται ισομορφισμός*

$$\boxed{G/Z\,(G) \xrightarrow{\cong} \mathrm{Inn}(G).} \tag{5.41}$$

ΑΠΟΔΕΙΞΗ. Εφαρμόζοντας το θεώρημα 5.4.26 για $H = G$ λαμβάνουμε

$$\mathrm{N}_G(G) = G,\ \mathrm{C}_G(G) =: Z(G) \text{ και } \mathrm{Im}(f_G) = \mathrm{Inn}(G),$$

οπότε ο ισομορφισμός (5.40) δίδει τον (5.41). □

5.4.29 Πόρισμα. *Εάν η $(G,\cdot)$ είναι μια αβελιανή ομάδα, τότε αυτή διαθέτει έναν και μόνον εσωτερικό αυτομορφισμό, ήτοι την ταυτοτική απεικόνιση* id_G.

5.4.30 Παραδείγματα. (i) Κατά το 5.4.18 (i) η ομάδα των εσωτερικών αυτομορφισμών τής ομάδας $\mathbf{Q}$ των τετρανίων είναι ισόμορφη με την ομάδα $\mathbf{V}$ των τεσσάρων στοιχείων τού Klein.

(ii) Έστω $n \in \mathbb{N}$, $n \geq 3$. Τότε, κατά το 5.4.18 (ii),

$$\boxed{\mathrm{Inn}(\mathbf{D}_n) \cong \begin{cases} \mathbf{D}_n, & \text{όταν ο } n \text{ είναι περιττός,} \\ \mathbf{V}, & \text{όταν } n = 4, \\ \mathbf{D}_{\frac{n}{2}}, & \text{όταν ο } n \text{ είναι άρτιος } \geq 6. \end{cases}}$$

(iii) Έστω $n \in \mathbb{N}$. Τότε, κατά το 5.4.9,

$$\boxed{\mathrm{Inn}(\mathfrak{S}_n) \cong \begin{cases} \{\mathrm{id}\}, & \text{όταν } n \leq 2, \\ \mathfrak{S}_n, & \text{όταν } n \geq 3. \end{cases}}$$

(iv) Έστω $n \in \mathbb{N}$, $n \geq 2$. Τότε, κατά το 5.4.11,

$$\boxed{\mathrm{Inn}(\mathfrak{A}_n) \cong \begin{cases} \{\mathrm{id}\}, & \text{όταν } n \leq 3, \\ \mathfrak{A}_n, & \text{όταν } n \geq 4. \end{cases}}$$

(v) Η ομάδα των εσωτερικών αυτομορφισμών καθεμιάς εκ των ομάδων πινάκων $\mathrm{GL}_n(F)$, $\mathrm{SL}_n(F)$, $\mathrm{O}_n(\mathbb{R})$, $\mathrm{SO}_n(\mathbb{R})$, $\mathrm{U}_n(\mathbb{C})$ και $\mathrm{SU}_n(\mathbb{C})$ είναι ισόμορφη με την αντίστοιχη *προβολική* ομάδα την ορισθείσα στα εδάφια 5.4.13 (i) και 5.4.16.

5.4.31 Ορισμός. Έστω $(G, \cdot)$ μια ομάδα. Επειδή $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$ (βλ. 5.4.25) ορίζεται η πηλικοομάδα

$$\boxed{\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)}$$

που καλείται **ομάδα των εξωτερικών αυτομορφισμών τής** G, τα δε στοιχεία της **εξωτερικοί αυτομορφισμοί**[34] **τής** G.

5.4.32 Παραδείγματα. (i) Για κάθε *αβελιανή* ομάδα G ισχύει $\mathrm{Out}(G) \cong \mathrm{Aut}(G)$ (βλ. 5.4.29 και 4.4.5).

(ii) Μια ομάδα έχουσα *τετριμμένη* ομάδα εξωτερικών αυτομορφισμών είναι η συμμετρική ομάδα $\mathfrak{S}_3 = \{\mathrm{id}, u_1, u_2, u_3, v_1, v_2\}$, όπου $u_1 := [1\,2]$, $u_2 := [1\,3]$, $u_3 := [2\,3]$ και[35]

$$v_1 := u_1 \circ u_3 = u_2 \circ u_1 = u_3 \circ u_2 = [1\,2\,3]\,,\ v_2 := u_1 \circ u_2 = u_2 \circ u_3 = u_3 \circ u_1 = [1\,3\,2]\,.$$

Πράγματι· για κάθε $\vartheta \in \mathrm{Aut}(\mathfrak{S}_3)$ έχουμε $\vartheta(\mathrm{id}) = \mathrm{id}$ και για κάθε $j \in \{1,2,3\}$ υπάρχει *ακριβώς ένα* $i \in \{1,2,3\}$ με

$$\vartheta(u_i) = u_j \ \text{ και } \ \vartheta(v_1) = \vartheta(u_1) \circ \vartheta(u_3),\ \vartheta(v_2) = \vartheta(u_1) \circ \vartheta(u_2).$$

(Βλ. 2.4.3 (i) και 2.4.19 (iv).) Επειδή (κατά το πόρισμα 3.2.12) $\mathfrak{S}_3 = \langle u_1, u_2, u_3 \rangle$, κάθε αυτομορφισμός τής $\mathfrak{S}_3$ καθορίζεται πλήρως από τις εικόνες των u_1, u_2 και u_3 μέσω αυτού. Επομένως,

$$|\mathrm{Aut}(\mathfrak{S}_3)| \leq \left|\mathfrak{S}_{\{u_1,u_2,u_3\}}\right| = |\mathfrak{S}_3| = 6.$$

Από την άλλη μεριά έχουμε $|\mathrm{Aut}(\mathfrak{S}_3)| \geq 6$, καθώς υπάρχουν *τουλάχιστον* 6 σαφώς διακεκριμένοι αυτομορφισμοί $\vartheta_0, \vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5$ τής $\mathfrak{S}_3$, όπου $\vartheta_0 := e_{\mathrm{Aut}(\mathfrak{S}_3)}$, $\vartheta_j(\mathrm{id}) = \mathrm{id}$ για κάθε $j \in \{1,2,3,4,5\}$ και

$$\begin{array}{l} \vartheta_1\,(u_1) := u_1,\ \vartheta_1\,(u_2) := u_3,\ \vartheta_1\,(u_3) := u_2,\ \vartheta_1\,(v_1) := v_2,\ \vartheta_1\,(v_2) := v_1, \\ \vartheta_2\,(u_1) := u_2,\ \vartheta_2\,(u_2) := u_1,\ \vartheta_2\,(u_3) := u_3,\ \vartheta_1\,(v_1) := v_2,\ \vartheta_1\,(v_2) := v_1, \\ \vartheta_3\,(u_1) := u_2,\ \vartheta_3\,(u_2) := u_3,\ \vartheta_3\,(u_3) := u_1,\ \vartheta_1\,(v_1) := v_1,\ \vartheta_1\,(v_2) := v_2, \\ \vartheta_4\,(u_1) := u_3,\ \vartheta_4\,(u_2) := u_2,\ \vartheta_4\,(u_3) := u_1,\ \vartheta_1\,(v_1) := v_2,\ \vartheta_1\,(v_2) := v_1, \\ \vartheta_5\,(u_1) := u_3,\ \vartheta_5\,(u_2) := u_1,\ \vartheta_5\,(u_3) := u_2,\ \vartheta_5\,(v_1) := v_1,\ \vartheta_5\,(v_2) := v_2. \end{array}$$

[34] Προσοχή! Στην παλαιότερη βιβλιογραφία, ορισμένοι συγγραφείς καλούν *εξωτερικό αυτομορφισμό* τής G κάθε μη εσωτερικό αυτομορφισμό τής G.

[35] Προφανώς, $\mathrm{ord}(u_i) = 2$ και $\mathrm{ord}(v_j) = 3, \forall (i,j) \in \{1,2,3\} \times \{1,2\}$.

Άρα $|\mathrm{Aut}(\mathfrak{S}_3)| = 6$. Επιπροσθέτως,

$$\left.\begin{array}{r} Z(\mathfrak{S}_3) = \{\mathrm{id}\} \underset{(5.41)}{\Longrightarrow} \mathfrak{S}_3 \cong \mathfrak{S}_3/Z(\mathfrak{S}_3) \cong \mathrm{Inn}(\mathfrak{S}_3) \\ \mathrm{Inn}(\mathfrak{S}_3) \trianglelefteq \mathrm{Aut}(\mathfrak{S}_3) \Rightarrow 6 = |\mathrm{Inn}(\mathfrak{S}_3)| \leq |\mathrm{Aut}(\mathfrak{S}_3)| \end{array}\right\} \Rightarrow \mathrm{Aut}(\mathfrak{S}_3) = \mathrm{Inn}(\mathfrak{S}_3)$$

και, ως εκ τούτου, $\mathrm{Aut}(\mathfrak{S}_3) = \{\vartheta_0, ..., \vartheta_5\} = \mathrm{Inn}(\mathfrak{S}_3) \cong \mathfrak{S}_3 \underset{4.4.5}{\Longrightarrow} \mathrm{Out}(G) \cong \{\mathrm{id}_{\mathfrak{S}_3}\}$.

(iii) Οι ομάδες των εξωτερικών αυτομορφισμών των λοιπών συμμετρικών, των εναλλασσουσών και των διεδρικών ομάδων δίδονται στα εδάφια 6.3.9, 6.3.20 και 7.6.37, αντιστοίχως.

5.4.33 Ορισμός. Έστω $(G, \cdot)$ μια ομάδα. Ο κεντροποιητής

$$\boxed{\mathrm{Aut_c}(G) := \mathrm{C}_{\mathrm{Aut}(G)}(\mathrm{Inn}(G))}$$

τής $\mathrm{Inn}(G)$ εντός τής $\mathrm{Aut}(G)$ καλείται **ομάδα των κεντρικών αυτομορφισμών τής** G, τα δε στοιχεία της **κεντρικοί αυτομορφισμοί τής** G.

5.4.34 Παρατήρηση. $\mathrm{Aut_c}(G) \trianglelefteq \mathrm{Aut}(G)$ (βλ. 5.4.25 και 5.2.2 (iii)).

5.4.35 Πρόταση. *Για οιαδήποτε ομάδα $(G, \cdot)$ οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) $\vartheta \in \mathrm{Aut_c}(G)$.

(ii) *Για κάθε $g \in G$ υπάρχει ένα $z_g \in Z(G)$, τέτοιο ώστε να ισχύει $\vartheta(g) = z_g g$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν $\vartheta \in \mathrm{Aut_c}(G)$, τότε για κάθε $g \in G$

$$\vartheta \circ \boldsymbol{\gamma}_g = \boldsymbol{\gamma}_g \circ \vartheta \underset{(5.39)}{\Longrightarrow} \boldsymbol{\gamma}_g = \vartheta \circ \boldsymbol{\gamma}_g \circ \vartheta^{-1} = \boldsymbol{\gamma}_{\vartheta(g)} \Rightarrow \boldsymbol{\gamma}_{\vartheta(g)} \circ \boldsymbol{\gamma}_g^{-1} = \mathrm{id}_G$$
$$\underset{(5.38)}{\Longrightarrow} \boldsymbol{\gamma}_{\vartheta(g)g^{-1}} = \mathrm{id}_G \Rightarrow \vartheta(g)g^{-1} \in Z(G) \Rightarrow \exists z_g \in Z(G) : \vartheta(g) = z_g g.$$

Επειδή οι ανωτέρω συνεπαγωγές είναι αντιστρεπτές, η (ii)⇒(i) είναι πρόδηλη. □

5.4.36 Πόρισμα. *Εάν $(G, \cdot)$ είναι οιαδήποτε ομάδα με $Z(G) = \{e_G\}$, τότε έχουμε $Z(\mathrm{Aut}(G)) = \{\mathrm{id}_G\}$.*

ΑΠΟΔΕΙΞΗ. Εάν $Z(G) = \{e_G\}$, τότε για κάθε $\vartheta \in Z(\mathrm{Aut}(G))$ έχουμε $\vartheta \in \mathrm{Aut_c}(G)$, διότι κατά το (v) τής προτάσεως 5.2.2 ισχύει

$$\mathrm{Inn}(G) \sqsubseteq \mathrm{Aut}(G) \Rightarrow Z(\mathrm{Aut}(G)) = \mathrm{C}_{\mathrm{Aut}(G)}(\mathrm{Aut}(G)) \sqsubseteq \mathrm{Aut_c}(G),$$

δηλαδή ο ϑ είναι ένας κεντρικός αυτομορφισμός τής G, οπότε $\vartheta(g) = e_G g = g$ για κάθε $g \in G$ (επί τη βάσει τής προτάσεως 5.4.35), απ' όπου έπεται ότι $\vartheta = \mathrm{id}_G$. □

5.4.37 Σημείωση. (i) Ένας τρόπος υπολογισμού *τής τάξεως* τής ομάδας των κεντρικών αυτομορφισμών μιας πεπερασμένης ομάδας έχει περιγραφεί ήδη από το

1969 σε ένα άρθρο[36] τού P.R. Sanders.

(ii) Στην αρθρογραφία συναντώνται αρκετές κατασκευές πεπερασμένων p-**ομάδων** G (ήτοι ομάδων, η τάξη των οποίων ισούται με κάποια δύναμη ενός πρώτου αριθμού p, πρβλ. 5.7.3) με $\mathrm{Aut}(G) = \mathrm{Aut_c}(G)$. Επί παραδείγματι, ο G.A. Miller[37] απέδειξε ότι υφίσταται μια μη αβελιανή ομάδα G τάξεως 2^6 που διαθέτει μόνον κεντρικούς αυτομορφισμούς, με την $\mathrm{Aut}(G) = \mathrm{Aut_c}(G)$ *αβελιανή* τάξεως 2^7. Άλλες ομάδες τέτοιου είδους παρήχθησαν από τους D. Johah, M. Konvisser[38], B.E. Earnley[39] και R.R. Struik[40]. Επιπροσθέτως, ο M.J. Curran[41] έδωσε το πρώτο παράδειγμα μη αβελιανής ομάδας G (τάξεως 2^7) για την οποία η $\mathrm{Aut}(G) = \mathrm{Aut_c}(G)$ είναι *μη αβελιανή* (τάξεως 2^{12}).

(iii) Από την άλλη μεριά, κινούμενοι -τρόπον τινά- προς «το άλλο άκρο», οι M.J. Curran και D.J. McGaughan[42] ανακάλυψαν συνοπτικές ικανές και αναγκαίες συνθήκες υπο τις οποίες κάθε κεντρικός αυτομορφισμός μιας πεπερασμένης μη αβελιανής p-ομάδας είναι εσωτερικός (ή τουλάχιστον βρίσκεται «πλησίον» τού να είναι εσωτερικός). Εν συνεχεία, ο πρώτος εξ αυτών[43] προσέθεσε ανάλογες συνθήκες, ούτως ώστε να ισχύει $\mathrm{Aut_c}(G) = Z(\mathrm{Inn}(G))$. (Βλ. 5.4.38 και 5.4.39, όπου ως G' συμβολίζεται η μεταθέτρια υποομάδα 5.5.4 τής G). Περαιτέρω εφαρμογές τής σχετικής θεωρίας παρουσιάσθηκαν αργότερα από τους M. Sharma και D. Gumber[44].

5.4.38 Θεώρημα. (M.J. Curran & D.J. McGaughan, 2001) *Εάν* $(G, \cdot)$ *είναι μια πεπερασμένη μη αβελιανή* p*-ομάδα με* $\mathrm{Inn}(G) \sqsubseteq \mathrm{Aut_c}(G)$, *τότε ισχύουν τα εξής*:

(i) $\mathrm{Aut_c}(G) = \mathrm{Inn}(G) \Leftrightarrow G' = Z(G)$ *και το* $Z(G)$ *είναι κυκλική υποομάδα τής* G.

(ii) $|\mathrm{Aut_c}(G) : \mathrm{Inn}(G)| = p \Leftrightarrow$ *το* $Z(G)$ *είναι κυκλική υποομάδα τής* G *και ισχύει* $|Z(G) : G'| = p$.

5.4.39 Θεώρημα. (M.J. Curran, 2004) *Εάν* $(G, \cdot)$ *είναι μια πεπερασμένη μη αβελιανή* p*-ομάδα, τότε ισχύουν τα εξής*:

(i) *Εάν* $\mathrm{Aut_c}(G) = Z(\mathrm{Inn}(G))$, *τότε* $Z(G) \sqsubseteq G'$.

(ii) $\mathrm{Aut_c}(G) = Z(\mathrm{Inn}(G)) \Leftrightarrow \mathrm{Hom}(G/G', Z(G)) \cong Z(G/Z(G))$.

---

[36] Βλ. P.R. Sanders: *The central automorphisms of a finite group*, Journal of the London Mathematical Society **44** (1969), 225-228.

[37] G.A. Miller: *A non-abelian group whose group of isomorphisms is abelian*, Messenger Math. **43** (1913/1914), 124-125.

[38] D. Johah & M. Konvisser: *Some non-abelian p-groups with abelian automorphism groups*, Archiv der Math. **26** (1975), 131-133.

[39] B.E. Earnley: *On finite groups whose group of automorphisms is abelian*, PhD thesis, Wayne State University, Detroit, Michigan, 1975.

[40] R.R. Struik: *Some non-abelian 2-groups with abelian automorphism groups*, Archiv der Math. **39** (1982), 299-302.

[41] M.J. Curran: *A non-abelian automorphism group with all automorphisms central*, Bull. Australian Math. Soc. **26** (1982), 393-397.

[42] M.J. Curran & D.J. McGaughan: *Central automorphisms that are almost inner*, Communications in Algebra **29**, No. 5 (2001), 2081-2087.

[43] M.J. Curran: *Finite groups with central automorphism group of minimal order*, Math. Proc. of the Royal Irish Academy, **104** A (2), (2004), 223-229.

[44] M. Sharma & D. Gumber: *On central automorphisms of finite p-groups*, Communications in Algebra **41** (2013), 1117-1122.

5.5 ΜΕΤΑΘΕΤΡΙΑ ΥΠΟΟΜΑΔΑ ΚΑΙ ΑΒΕΛΙΑΝΟΠΟΙΗΣΗ ΜΙΑΣ ΟΜΑΔΑΣ

Έστω $(G,\cdot)$ μια ομάδα και έστω $y\in G$. Το συζυγές του στοιχείο xyx^{-1} το δημιουργούμενο μέσω ενός στοιχείου $x\in G$ μπορεί να ιδωθεί ως το γινόμενο $[x,y]\,y$ τού λεγομένου *μεταθέτη* $[x,y]$ των x και y και τού y. Οι μεταθέτες ζευγών στοιχείων τής ομάδας $(G,\cdot)$ παράγουν μια υποομάδα $G'\trianglelefteq G$, τη λεγομένη *μεταθέτρια υποομάδα* τής G, το «μέγεθος» τής οποίας μπορεί να εκληφθεί *ως ένα μέτρο ενδείξεως τού πόσον απέχει η G από το να είναι αβελιανή*. (Η G είναι αβελιανή και μόνον εάν η G' είναι τετριμμένη.) Τόσον η μεταθέτρια υποομάδα G' όσον και η μετάβαση στην πηλικοομάδα $G^{\text{ab}}:=G/G'$ (που καλείται *αβελιανοποίηση* τής G) υπεισέρχονται *ουσιωδώς* στη μελέτη μη αβελιανών ομάδων $(G,\cdot)$.

5.5.1 Ορισμός. Έστω $(G,\cdot)$ μια ομάδα. Εάν $x,y\in G$, τότε το στοιχείο

$$\boxed{[x,y]:=xyx^{-1}y^{-1}}$$

καλείται **μεταθέτης των x και y**. Η ονομασία αυτή εδόθη στο $[x,y]$, διότι αποτελεί εκείνο το στοιχείο με το οποίο πολλαπλασιαζόμενο το yx μας δίδει το xy:

$$xy=[x,y]\,yx \quad\text{και}\quad xy=yx\Leftrightarrow[x,y]=e_G.$$

5.5.2 Πρόταση. (Ιδιότητες μεταθετών.) *Έστω $(G,\cdot)$ μια ομάδα. Εάν $x,y,z\in G$, τότε ισχύουν τα εξής*:

(i) $[x,y]^{-1}=[y,x]$.

(ii) $yxy^{-1}=x^{-1}[x,y]$, $y[x,y]y^{-1}=\left[yxy^{-1},y\right]$, $z[x,y]z^{-1}=[zxz^{-1},zyz^{-1}]$.

(iii) $[x,yz]=[x,y]\,(y[x,z]y^{-1})$.

(iv) $[xy,z]=(x[y,z]x^{-1})[x,z]$.

(v) $[x,yz]=[x,y][x,z][[z,x],y]$.

(vi) $\left[x^{-1},y\right]=x^{-1}[x,y]^{-1}x$.

(vii) $\left[x,y^{-1}\right]=y^{-1}[x,y]^{-1}y$.

(viii) *Για τα x,y,z ισχύει η* ταυτότητα τού Witt:

$$\left(y\left[x,\left[y^{-1},z\right]\right]y^{-1}\right)\left(z\left[y,\left[z^{-1},x\right]\right]z^{-1}\right)\left(x\left[z,\left[x^{-1},y\right]\right]x^{-1}\right)=e_G. \tag{5.42}$$

(ix) *Εάν* $[x,y]\in \mathrm{C}_G(x)\cap\mathrm{C}_G(y)$, *τότε*

$$[x^m,y^n]=[x,y]^{mn},\ \ \forall(m,n)\in\mathbb{Z}\times\mathbb{Z}. \tag{5.43}$$

(x) *Εάν* $[x,y]\in \mathrm{C}_G(x)\cap\mathrm{C}_G(y)$, *τότε*

$$(xy)^n=[y,x]^{\frac{n(n-1)}{2}}x^ny^n,\ \ \forall n\in\mathbb{Z}. \tag{5.44}$$

ΑΠΟΔΕΙΞΗ. (i) $[x,y]\,[y,x] = \left(xyx^{-1}y^{-1}\right)\left(yxy^{-1}x^{-1}\right) = e_G \Rightarrow [x,y]^{-1} = [y,x]\,.$
(ii) $yxy^{-1} = x^{-1}(xyx^{-1}y^{-1}) = x^{-1}\,[x,y]\,,$

$$y\,[x,y]\,y^{-1} = y\left(xyx^{-1}y^{-1}\right)y^{-1} = \left(yxy^{-1}\right)y\left(yxy^{-1}\right)^{-1}y^{-1} = \left[yxy^{-1},y\right]$$

και

$$[zxz^{-1},zyz^{-1}] = zxz^{-1}zyz^{-1}zx^{-1}z^{-1}zy^{-1}z^{-1} = z[x,y]z^{-1}.$$

(iii) Προφανώς, λόγω τής γενικευμένης προσεταιριστικής ιδιότητας (βλ. 1.2.19),

$$[x,y]\,(y\,[x,z]\,y^{-1}) = \left(xyx^{-1}y^{-1}\right)\left(y\left(xzx^{-1}z^{-1}\right)y^{-1}\right) = x(yz)x^{-1}(yz)^{-1} = [x,yz]\,.$$

(iv) Παρομοίως,

$$(x\,[y,z]\,x^{-1})\,[x,z] = \left(x\left(yzy^{-1}z^{-1}\right)x^{-1}\right)\left(xzx^{-1}z^{-1}\right) = (xy)\,z(xy)^{-1}z^{-1} = [xy,z]\,.$$

(v) Επειδή $[x,yz] = x\,(yz)\,x^{-1}(yz)^{-1} = (xyz)\left(x^{-1}z^{-1}y^{-1}\right)$ και

$$\begin{aligned}
&[x,y]\,[x,z]\,[[z,x]\,,y] = \left(xyx^{-1}y^{-1}\right)\left(xzx^{-1}z^{-1}\right)\left([z,x]\,y\,[z,x]^{-1}\,y^{-1}\right)\\
&= \left(xyx^{-1}y^{-1}\right)\left(xzx^{-1}z^{-1}\right)\left(\left(zxz^{-1}x^{-1}\right)y\left(xzx^{-1}z^{-1}\right)y^{-1}\right)\\
&= (xy)\left(x^{-1}\left(y^{-1}\left(x\left(z\left(x^{-1}\left(z^{-1}z\right)x\right)z^{-1}\right)x^{-1}\right)y\right)x\right)\left(zx^{-1}z^{-1}y^{-1}\right)\\
&= (xyz)\left(x^{-1}z^{-1}y^{-1}\right),
\end{aligned}$$

έχουμε $[x,yz] = [x,y]\,[x,z]\,[[z,x]\,,y]\,.$
(vi) Προφανώς,

$$x^{-1}\,[x,y]^{-1}\,x = x^{-1}\,[y,x]\,x = x^{-1}(yxy^{-1}x^{-1})x = x^{-1}y(x^{-1})^{-1}y^{-1} = \left[x^{-1},y\right].$$

(vii) Παρομοίως,

$$y^{-1}\,[x,y]^{-1}\,y = y^{-1}\,[y,x]\,y = y^{-1}(yxy^{-1}x^{-1})y = xy^{-1}x^{-1}(y^{-1})^{-1} = \left[x,y^{-1}\right].$$

(viii) Θέτοντας $a := y^{-1}z^{-1}yx^{-1}y^{-1}$,

$$b := z^{-1}x^{-1}zy^{-1}z^{-1} \quad \text{και} \quad c := x^{-1}y^{-1}xz^{-1}x^{-1}$$

έχουμε

$$y\left[x,\left[y^{-1},z\right]\right]y^{-1} = a^{-1}b,\ z\left[y,\left[z^{-1},x\right]\right]z^{-1} = b^{-1}c,\ x\left[z,\left[x^{-1},y\right]\right]x^{-1} = c^{-1}a.$$

Κατόπιν πολλαπλασιασμού αυτών των τριών όρων λαμβάνουμε το ουδέτερο στοιχείο τής G, οπότε η (5.42) είναι αληθής.
(ix) Εάν τουλάχιστον ένας εκ των m,n είναι $=0$, τότε η (5.43) είναι προφανής. Εάν $m\geq 1$ και $n=1$, τότε εργαζόμαστε επαγωγικώς ως προς τον m. Για $m=1$ η (5.43) είναι αληθής. Υποθέτουμε ότι είναι αληθής για κάποιον $m\geq 1$. Τότε

$$\begin{aligned}
[x,y]^{m+1} &= [x,y]^m\,[x,y] = [x,y]^m\,xyx^{-1}y^{-1}\\
&= x\,[x,y]^m\,yx^{-1}y^{-1} \ \text{(επειδή } [x,y]\in \mathrm{C}_G(x) \Rightarrow [x,y]^m\in \mathrm{C}_G(x))\\
&= x\,[x^m,y]\,yx^{-1}y^{-1} \ \text{(λόγω τής επαγωγικής υποθέσεως)}\\
&= x(x^myx^{-m}y^{-1})yx^{-1}y^{-1} = x^{m+1}y(x^{m+1})^{-1}y^{-1} = \left[x^{m+1},y\right],
\end{aligned}$$

οπότε η (5.43) είναι αληθής και για τον $m+1$. Ως εκ τούτου,

$$[x^m, y] = [x, y]^m\,, \quad \forall m \in \mathbb{N}. \tag{5.45}$$

Κατ' αναλογίαν, επειδή $[x, y] \in \mathrm{C}_G(x) \Rightarrow [x, y]^n \in \mathrm{C}_G(y)$, αποδεικνύεται επαγωγικώς ότι

$$[x, y^n] = [x, y]^n\,, \quad \forall n \in \mathbb{N}, \tag{5.46}$$

δηλαδή ότι η (5.43) αληθεύει και για $m = 1$ και $n \geq 1$. Όμως η (5.43) ισχύει και για *οιοδήποτε ζεύγος* $(m, n) \in \mathbb{N} \times \mathbb{N}$, διότι $[x, y]^m \in \mathrm{C}_G(x)$ και (λόγω τής (5.45))

$$[x^m, y]\, y = [x, y]^m\, y = y\, [x, y]^m = y\, [x^m, y] \Rightarrow [x^m, y] \in \mathrm{C}_G(y),$$

για κάθε $m \in \mathbb{N}$, οπότε από την (5.45) και την (5.46) (εφαρμοζόμενη για τα x^m και y) έπεται ότι

$$[x, y]^{mn} = ([x, y]^m)^n = [x^m, y]^n = [x^m, y^n]\,, \ \forall (m, n) \in \mathbb{N} \times \mathbb{N}. \tag{5.47}$$

Σημειωτέον ότι για $x, y \in G$ με $[x, y] \in \mathrm{C}_G(x) \cap \mathrm{C}_G(y)$ έχουμε $x\,[x, y] = [x, y]\, x$, οπότε

$$[x, y] = \left[y, x^{-1}\right] \Rightarrow [x, y]^{-1} = \left[y, x^{-1}\right]^{-1} = \left[x^{-1}, y\right], \tag{5.48}$$

και $y\,[x, y] = [x, y]\, y$, οπότε

$$[x, y]^{-1} = \left[x, y^{-1}\right]. \tag{5.49}$$

Εφαρμόζοντας την (5.49) για τα x^{-1} και y, και την (5.48) για τα x και y λαμβάνουμε

$$\left[x^{-1}, y^{-1}\right] = \left[x^{-1}, y\right]^{-1} = [x, y]\,. \tag{5.50}$$

Εν συνεχεία, θα εξετάσουμε τις εναπομείνασες περιπτώσεις για την (ολοκληρωτική) επαλήθευση τής (5.43). Εάν $m < 0$ και $n \geq 1$, τότε η (5.47) (εφαρμοζόμενη για τους $-m$ και n), σε συνδυασμό με την (5.48), δίδει

$$[x^m, y^n] = \left[\left(x^{-1}\right)^{-m}, y^n\right] = \left[x^{-1}, y\right]^{-mn} = \left([x, y]^{-1}\right)^{-mn} = [x, y]^{mn}\,.$$

Εάν $m \geq 1$ και $n < 0$, τότε η (5.47) (εφαρμοζόμενη για τους m και $-n$), σε συνδυασμό με την (5.49), δίδει

$$[x^m, y^n] = \left[x^m, \left(y^{-1}\right)^{-n}\right] = \left[x, y^{-1}\right]^{-mn} = \left([x, y]^{-1}\right)^{-mn} = [x, y]^{mn}\,.$$

Τέλος, εάν $m < 0$ και $n < 0$, τότε η (5.47) (εφαρμοζόμενη για τους $-m$ και $-n$), σε συνδυασμό με την (5.50), δίδει

$$[x^m, y^n] = \left[\left(x^{-1}\right)^{-m}, \left(y^{-1}\right)^{-n}\right] = \left[x^{-1}, y^{-1}\right]^{mn} = [x, y]^{mn}\,.$$

Άρα η (5.43) είναι όντως αληθής *για κάθε* $(m, n) \in \mathbb{Z} \times \mathbb{Z}$.

(x) Για $n = 0$ η (5.44) είναι προφανής. Για $n \in \mathbb{N}$ εργαζόμαστε επαγωγικώς ως προς τον n. Για $n = 1$ η (5.44) είναι αληθής. Υποθέτουμε ότι είναι αληθής για κάποιον $n \geq 1$. Τότε

$$\begin{aligned}
(xy)^{n+1} &= [y,x]^{\frac{n(n-1)}{2}}\, x^n y^n\, (xy) \quad \text{(λόγω τής επαγωγικής υποθέσεως)} \\
&= [y,x]^{\frac{n(n-1)}{2}}\, x^{n+1}(x^{-1}y^n)(xy^{-n})y^{n+1} \\
&= [y,x]^{\frac{n(n-1)}{2}}\, x^{n+1}\left[x^{-1},y^n\right] y^{n+1} \\
&= [y,x]^{\frac{n(n-1)}{2}}\, x^{n+1}\,[x,y]^{-n}\, y^{n+1} \quad \text{(λόγω τής (5.43))} \\
&= [y,x]^{\frac{n(n-1)}{2}}\, x^{n+1}\,[y,x]^{n}\, y^{n+1} \quad \text{(λόγω τού (i))} \\
&= [y,x]^{\frac{n(n-1)}{2}}\,[y,x]^n\, x^{n+1}y^{n+1} = [y,x]^{\frac{(n+1)n}{2}}\, x^{n+1}y^{n+1},
\end{aligned}$$

όπου η προτελευταία ισότητα έπεται από το ότι[45]

$$[x,y] \in \mathrm{C}_G(x) \Rightarrow [x,y]^{-1} = [y,x] \in \mathrm{C}_G(x) \Rightarrow [y,x]^n \in \mathrm{C}_G(x),$$

οπότε η (5.44) είναι αληθής και για τον $n+1$. Ως εκ τούτου,

$$(xy)^n = [y,x]^{\frac{n(n-1)}{2}}\, x^n y^n, \ \ \forall n \in \mathbb{N}. \tag{5.51}$$

Εάν $n < 0$, τότε εφαρμόζοντας την (5.51) για τα y^{-1} και x^{-1} λαμβάνουμε

$$\begin{aligned}
(xy)^n &= \left(y^{-1}x^{-1}\right)^{-n} = \left[x^{-1},y^{-1}\right]^{\frac{(-n)(-n-1)}{2}} \left(y^{-1}\right)^{-n} \left(x^{-1}\right)^{-n} \\
&= [x,y]^{\frac{(-n)(-n-1)}{2}}\, y^n x^n \quad \text{(λόγω τής (5.50))} \\
&= \left([y,x]^{-1}\right)^{\frac{(-n)(-n-1)}{2}}\, y^n x^n \quad \text{(λόγω τού (i))} \\
&= [y,x]^{\frac{n(-n-1)}{2}}\,[y^n,x^n]\, x^n y^n \quad \text{(εξ ορισμού)} \\
&= [y,x]^{\frac{-n(n+1)}{2}}\,[y,x]^{n^2}\, x^n y^n \quad \text{(λόγω τής (5.43))} \\
&= [y,x]^{\frac{n(n-1)}{2}}\, x^n y^n
\end{aligned}$$

Άρα η (5.44) είναι όντως αληθής *για κάθε* $n \in \mathbb{Z}$. □

5.5.3 Παρατήρηση. Εάν $H \trianglelefteq G$, τότε για $x, y \in G$ λαμβάνουμε $[xH, yH] = [x,y]H$ εντός τής πηλικοομάδας G/H.

5.5.4 Ορισμός. Έστω $(G,\cdot)$ μια ομάδα. Η υποομάδα

$$\boxed{G' := \langle \{ [x,y] \mid (x,y) \in G \times G \} \rangle \sqsubseteq G}$$

η παραγόμενη από τους μεταθέτες όλων των ζευγών στοιχείων αυτής καλείται **μεταθέτρια υποομάδα** (ή **παράγωγη υποομάδα**) **τής** G. (Όταν συμβαίνει να ισχύει $G' = G$, τότε λέμε ότι η $(G,\cdot)$ είναι μια **τέλεια ομάδα.**)

[45] Προφανώς, $x^n(x\,[y,x]^n) = x^n\,[y,x]^n\,x = x^{n-1}(x\,[y,x]^n)x = x^{n-1}\,[y,x]^n\,x^2 = \cdots = [y,x]^n\,x^{n+1}$.

5.5.5 Σημείωση. Προφανώς,

$$\boxed{\{[x,y] \mid (x,y) \in G \times G\} \subseteq G'.} \tag{5.52}$$

Σε ορισμένες περιπτώσεις η (5.52) ισχύει ως *ισότητα* (όπως, π.χ., όταν η G είναι διεδρική ή συμμετρική ομάδα ή η ομάδα των τετρανίων), ενώ σε άλλες περιπτώσεις η (5.52) ισχύει ως *αυστηρός εγκλεισμός* (ήτοι υπάρχουν στοιχεία τής G' που δεν είναι αφ' εαυτά μεταθέτες δύο στοιχείων τής G). Ένα απλό παράδειγμα, το οποίο δείχνει ότι η (5.52) μπορεί να ισχύει ως αυστηρός εγκλεισμός, οφείλεται στον P.J. Cassidy[46] και παρατίθεται στην άσκηση **5-53**. Κάποιες γενικές ικανές συνθήκες για να ισχύει η (5.52) ως ισότητα (και αντιστοίχως, ως αυστηρός εγκλεισμός) δίδονται στα θεωρήματα 5.5.17 και 5.5.19 (και αντιστοίχως, στο πόρισμα 5.5.22).

5.5.6 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Τότε $G' \trianglelefteq G$ και*

$$G' = \{e_G\} \iff \textit{η } G \textit{ είναι αβελιανή.}$$

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς παρατηρούμε ότι για τον μεταθέτη $[x,y]$ οιωνδήποτε στοιχείων $x, y \in G$ ισχύει

$$g\left(xyx^{-1}y^{-1}\right)g^{-1} = \left(gxg^{-1}\right)\left(gyg^{-1}\right)\left(gxg^{-1}\right)^{-1}\left(gyg^{-1}\right)^{-1} \in G',$$

για κάθε $g \in G$. Ένα τυχόν στοιχείο τής G' ενδέχεται να *μην* είναι μεταθέτης· ωστόσο, γράφεται ως γινόμενο μεταθετών υπό τη μορφή

$$[x_1,y_1]^{\varepsilon_1} \cdots [x_k,y_k]^{\varepsilon_k},\ (x_j,y_j) \in G \times G \text{ και } \varepsilon_j \in \mathbb{Z},\ \forall j \in \{1,..,k\},\ k \in \mathbb{N}.$$

Για κάθε $g \in G$ έχουμε

$$\begin{aligned} g\left([x_1,y_1]^{\varepsilon_1} \cdots [x_k,y_k]^{\varepsilon_k}\right)g^{-1} &= \left(g\,[x_1,y_1]^{\varepsilon_1}\,g^{-1}\right) \cdots \left(g\,[x_k,y_k]^{\varepsilon_k}\,g^{-1}\right) \\ &= \underbrace{\left(g\,[x_1,y_1]\,g^{-1}\right)}_{\in G'}{}^{\varepsilon_1} \cdots \underbrace{\left(g\,[x_k,y_k]\,g^{-1}\right)}_{\in G'}{}^{\varepsilon_k}, \end{aligned}$$

οπότε $g\left([x_1,y_1]^{\varepsilon_1} \cdots [x_k,y_k]^{\varepsilon_k}\right)g^{-1} \in G' \implies gG'g^{-1} \subseteq G' \implies G' \trianglelefteq G$. Εάν $G' = \{e_G\}$, τότε

$$\begin{aligned} [x,y] = e_G,\ \forall (x,y) \in G \times G &\Rightarrow xyx^{-1}y^{-1} = e_G,\ \forall (x,y) \in G \times G \\ &\Rightarrow xy = yx,\ \forall (x,y) \in G \times G, \end{aligned}$$

οπότε η G είναι αβελιανή. Το αντίστροφο αποδεικνύεται παρομοίως. □

5.5.7 Πόρισμα. *Έστω $(G,\cdot)$ μια ομάδα. Τότε*

$$G' = \{e_G\} \iff \textit{η } G \textit{ είναι αβελιανή} \iff G = Z(G). \tag{5.53}$$

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από τις προτάσεις 5.4.2 και 5.5.6. □

[46] P.J. Cassidy: *Products of commutators are not always commutators: An example*, The American Mathematical Monthly **86** (1979), p. 772.

5.5.8 Σημείωση. Λόγω τής ισχύος των αμφιπλεύρων συνεπαγωγών (5.53) θα ανέμενε κανείς την ύπαρξη μιας πιο διευρυμένης σχέσεως «δυϊσμού» μεταξύ τής μεταθέτριας υποομάδας G' και τού κέντρου $Z(G)$. Ωστόσο, εν γένει τούτο δεν συμβαίνει: Υπάρχουν, επί παραδείγματι, ομάδες $(G,\cdot)$ με $Z(G)=\{e_G\}$ και $G'\sqsubset G$ (όπως η $G=\mathfrak{S}_3$, βλ. 5.4.9 και 5.5.9), καθώς και ομάδες $(G,\cdot)$ με μη τετριμμένο κέντρο και $G'=Z(G)$ (όπως η $\mathbf{Q}$ ή οποιαδήποτε άλλη ομάδα τάξεως p^3, όπου p πρώτος αριθμός, βλ. 5.5.13 και 5.6.8, ή ακόμη και άπειρες ομάδες, όπως η $\mathrm{SL}_n(\mathbb{C})$ για κάθε $n\geq 2$). Η μόνη γενικώς ισχύουσα συνεπαγωγή είναι η ακόλουθη:

$$\boxed{|G:Z(G)|<\infty \Longrightarrow |G'|<\infty,}$$

βάσει τής οποίας η μεταθέτρια υποομάδα G' είναι πεπερασμένη υπό την προϋπόθεση ότι το $Z(G)$ είναι υποομάδα πεπερασμένου δείκτη. (Βλ. θεώρημα 5.5.20).

5.5.9 Παράδειγμα. (Μεταθέτρια υποομάδα τής $\mathfrak{S}_n$.) Κάθε μεταθέτης εντός τής $\mathfrak{S}_n$ είναι προφανώς μια άρτια μετάταξη. Επομένως, $\mathfrak{S}_n'\sqsubseteq\mathfrak{A}_n$. Από την άλλη μεριά, κάθε 3-κύκλος $[\alpha_1\ \alpha_2\ \alpha_3]$ αποτελεί έναν μεταθέτη, διότι

$$[\alpha_1\ \alpha_2\ \alpha_3]=[\alpha_1\ \alpha_2]\circ[\alpha_1\ \alpha_3]\circ[\alpha_1\ \alpha_2]\circ[\alpha_1\ \alpha_3]=[[\alpha_1\ \alpha_2],[\alpha_1\ \alpha_3]].$$

Επιπροσθέτως, οι 3-κύκλοι παράγουν την $\mathfrak{A}_n$ όταν $n\geq 3$ (βλ. 3.3.13 (ii)). Εξ αυτού συνάγεται ότι

$$\boxed{\mathfrak{S}_n'=\begin{cases}\{\mathrm{id}\}, & \text{όταν } n\leq 2,\\ \mathfrak{A}_n, & \text{όταν } n\geq 3.\end{cases}}$$

5.5.10 Πρόταση. *Εάν η απεικόνιση $f:(G,\cdot)\longrightarrow(K,*)$ είναι ένας ομομορφισμός ομάδων, τότε $f(G')\sqsubseteq f(G)'\sqsubseteq K'$. Επιπροσθέτως, εάν η f είναι ισομορφισμός, τότε $f(G')=K'$.*

ΑΠΟΔΕΙΞΗ. Για κάθε ζεύγος $(x,y)\in G\times G$ έχουμε

$$\begin{aligned} f([x,y]) &= f(xyx^{-1}y^{-1})=f(x)*f(y)*f(x^{-1})*f(y^{-1})\\ &= f(x)*f(y)*f\,(x)^{-1}*f(y)^{-1}=[f(x),f(y)]\in f(G)'. \end{aligned}$$

Κάθε στοιχείο τής ομάδας G' γράφεται ως γινόμενο μεταθετών υπό τη μορφή

$$[x_1,y_1]^{\varepsilon_1}\cdots[x_k,y_k]^{\varepsilon_k},\ (x_j,y_j)\in G\times G \text{ και } \varepsilon_j\in\mathbb{Z},\ \forall j\in\{1,..,k\},\ k\in\mathbb{N}.$$

Επομένως,

$$\begin{aligned} f\left([x_1,y_1]^{\varepsilon_1}\cdots[x_k,y_k]^{\varepsilon_k}\right) &= f([x_1,y_1])^{\varepsilon_1}\cdots f([x_k,y_k])^{\varepsilon_k}\\ &= [f(x_1),f(y_1)]^{\varepsilon_1}\cdots[f(x_k),f(y_k)]^{\varepsilon_k}\in f(G)', \end{aligned}$$

απ' όπου έπεται ότι $f(G')\sqsubseteq f(G)'$, $f(G)'\sqsubseteq K'\underset{2.1.20}{\Longrightarrow} f(G')\sqsubseteq f(G)'$. Εάν η f είναι ισομορφισμός, τότε χρησιμοποιώντας το ίδιο είδος επιχειρημάτων για την αντίστροφό της f^{-1} συμπεραίνουμε τελικώς ότι $f(G')=K'$. □

5.5.11 Πρόταση. (R. Dedekind, 1880.) *Έστω $(G,\cdot)$ μια ομάδα. Εάν $H \sqsubseteq G$, τότε*

$$[H \trianglelefteq G \text{ και η πηλικοομάδα } G/H \text{ είναι αβελιανή}] \iff G' \sqsubseteq H.$$

ΑΠΟΔΕΙΞΗ. "$\Rightarrow$" Εάν η H είναι ορθόθετη υποομάδα τής G και η πηλικοομάδα G/H αβελιανή, τότε για κάθε ζεύγος $(x,y) \in G \times G$ έχουμε

$$\begin{gathered} H(xy) = (Hx)(Hy) = (Hy)(Hx) = H(yx) \\ \Rightarrow [x,y] = xyx^{-1}y^{-1} = xy(yx)^{-1} \in H \Rightarrow G' \sqsubseteq H. \end{gathered}$$

"$\Leftarrow$" Ας υποθέσουμε ότι $G' \sqsubseteq H$. Θεωρούμε τυχόντα στοιχεία $x \in G$ και $y \in H$. Τότε

$$\left.\begin{aligned} [x,y] = xyx^{-1}y^{-1} \in G' \subseteq H \\ y \in H \Rightarrow y^{-1} \in H \end{aligned}\right\} \Rightarrow xyx^{-1} \in H,$$

οπότε $H \trianglelefteq G$. Εξάλλου, επειδή $xyx^{-1}y^{-1} = xy(yx)^{-1} \in H$, έχουμε

$$H(xy) = H(yx) \Rightarrow (Hx)(Hy) = (Hy)(Hx),$$

οπότε η πηλικοομάδα G/H είναι όντως αβελιανή. □

5.5.12 Σημείωση. Σύμφωνα με την πρόταση 5.5.11 η μεταθέτρια υποομάδα G' τής G είναι το *ελάχιστο στοιχείο* τού συνόλου $\{\, H \in \mathbf{NSubg}(G) \mid G/H \text{ αβελιανή}\}$ ως προς τη διάταξη " $\sqsubseteq$ ".

5.5.13 Παράδειγμα. (Μεταθέτρια υποομάδα τής Q.) Το κέντρο $Z(\mathbf{Q}) = \{\pm\mathbf{I}_2\}$ τής ομάδας $\mathbf{Q}$ των τετρανίων είναι ορθόθετη υποομάδα τής $\mathbf{Q}$ και η πηλικοομάδα $\mathbf{Q}/Z(\mathbf{Q})$ είναι ισόμορφη με την ομάδα $\mathbf{V}$ των τεσσάρων στοιχείων τού Klein (βλ. 5.4.18 (i)). Επομένως, σύμφωνα με την πρόταση 5.5.11 η μεταθέτρια υποομάδα $\mathbf{Q}'$ τής $\mathbf{Q}$ είναι υποομάδα τού κέντρου $Z(\mathbf{Q}) = \{\pm\mathbf{I}_2\}$ (διότι η $\mathbf{V}$ είναι αβελιανή). Επειδή η $\mathbf{Q}$ δεν είναι αβελιανή, η πρόταση 5.5.6 μας πληροφορεί ότι $\mathbf{Q}' \neq \{\mathbf{I}_2\}$. Κατά συνέπειαν, $\mathbf{Q}' = Z(\mathbf{Q})$. Η $\mathbf{Q}$ ανήκει σε μια ευρεία οικογένεια μη αβελιανών ομάδων, οι μεταθέτριες υποομάδες των οποίων συμπίπτουν με τα κέντρα τους. Η εν λόγω οικογένεια περιγράφεται στο πόρισμα 5.6.8.

5.5.14 Εφαρμογή. (Μεταθέτρια υποομάδα τής $\mathfrak{A}_n$.) *Έστω $n \in \mathbb{N}$, $n \geq 3$. Τότε*

$$\boxed{\mathfrak{A}_n' = \begin{cases} \{\mathrm{id}\}, & \text{όταν } n = 3, \\ \mathbf{V}, & \text{όταν } n = 4, \\ \mathfrak{A}_n, & \text{όταν } n \geq 5. \end{cases}}$$

ΑΠΟΔΕΙΞΗ. Η $\mathfrak{A}_3$ είναι κυκλική, οπότε η μεταθέτρια υποομάδα της είναι τετριμμένη. Για φυσικούς αριθμούς $n \geq 5$ η $\mathfrak{A}_n$ είναι απλή (βλ. θεώρημα 4.3.6), οπότε η μεταθέτρια υποομάδα της είναι η ίδια η $\mathfrak{A}_n$ (διότι $\mathfrak{A}_n' \trianglelefteq \mathfrak{A}_n$ και η $\mathfrak{A}_n$ είναι μη αβελιανή, βλ. 5.5.6). Σε ό,τι αφορά στην ομάδα $\mathfrak{A}_4$, υπενθυμίζουμε ότι $\mathbf{V} \trianglelefteq \mathfrak{A}_4$ (βλ. 4.2.21) και ότι η πηλικοομάδα $\mathfrak{A}_4/\mathbf{V} \cong \mathbb{Z}_3$, ως κυκλική, είναι αβελιανή. Βάσει τής προτάσεως 5.5.11, $\mathfrak{A}_4' \sqsubseteq \mathbf{V}$. Άρα η $\mathfrak{A}_4'$ είναι *ή* η τετριμμένη *ή* μία εκ των

τριών κυκλικών υποομάδων τής $\mathbf{V}$ τάξεως 2 *ή* η ίδια η $\mathbf{V}$ (βλ. 4.1.41). Το πρώτο ενδεχόμενο αποκλείεται, διότι η $\mathfrak{A}_4$ δεν είναι αβελιανή (βλ. 5.5.11). Το δεύτερο ενδεχόμενο αποκλείεται, διότι $\mathfrak{A}_4' \trianglelefteq \mathfrak{A}_4$ και $\mathbf{NSubg}(\mathfrak{A}_4) = \{\{\mathrm{id}\}, \mathbf{V}, \mathfrak{A}_4\}$. (Βλ. τα σχόλια τής υποσημειώσεως στο εδ. 5.4.11.) Κατά συνέπειαν, $\mathfrak{A}_4' = \mathbf{V}$. □

5.5.15 Εφαρμογή. (Μεταθέτρια υποομάδα τής $\mathbf{GL}_2(\mathbb{R})$.) *Για τις ομάδες* $\mathrm{GL}_2(\mathbb{R})$ *και* $\mathrm{SL}_2(\mathbb{R})$ *ισχύουν τα εξής*:

(i) *Το σύνολο*

$$\left\{ \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \middle| \, r \in \mathbb{R} \right\} \cup \left\{ \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} \middle| \, r \in \mathbb{R} \right\} \cup \left\{ \begin{pmatrix} t & 0 \\ 0 & \frac{1}{t} \end{pmatrix} \middle| \begin{array}{l} t \in \mathbb{R}, \\ t \neq 0 \end{array} \right\}$$

αποτελεί ένα σύστημα γεννητόρων τής $\mathrm{SL}_2(\mathbb{R})$.

(ii) $\mathrm{GL}_2(\mathbb{R})' = \mathrm{SL}_2(\mathbb{R})$.

ΑΠΟΔΕΙΞΗ. (i) Έστω τυχόν στοιχείο $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$. Εάν $c \neq 0$, τότε

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & \frac{a-1}{c} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} 1 & \frac{d-1}{c} \\ 0 & 1 \end{pmatrix},$$

ενώ για $c = 0$ έχουμε

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix} \begin{pmatrix} 1 & \frac{b}{a} \\ 0 & 1 \end{pmatrix}.$$

Άρα το δοθέν σύνολο πινάκων είναι όντως ένα σύστημα γεννητόρων τής $\mathrm{SL}_2(\mathbb{R})$.

(ii) Επειδή $\mathrm{SL}_2(\mathbb{R}) \lhd \mathrm{GL}_2(\mathbb{R})$ και η πηλικοομάδα $\mathrm{GL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{R})$ είναι ισόμορφη με την αβελιανή πολλαπλασιαστική ομάδα $(\mathbb{R}\setminus\{0\}, \cdot)$ (βλ. 4.2.32 (ii) και 4.5.3 (vi)), η πρόταση 5.5.11 μας πληροφορεί ότι $\mathrm{GL}_2(\mathbb{R})' \sqsubseteq \mathrm{SL}_2(\mathbb{R})$. Απο την άλλη μεριά, επειδή

$$\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -r \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

και

$$\begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -s & 1 \end{pmatrix},$$

$$\begin{pmatrix} t & 0 \\ 0 & \frac{1}{t} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} t & 2t \\ 2t^2 & t^2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -\frac{1}{3t} & \frac{2}{3t} \\ \frac{2}{3t} & -\frac{1}{3t^2} \end{pmatrix},$$

για οιουσδήποτε $r, s \in \mathbb{R}$ και $t \in \mathbb{R}\setminus\{0\}$, καθένας εκ των πινάκων που ανήκουν στο σύστημα γεννητόρων τής $\mathrm{SL}_2(\mathbb{R})$ (το οποίο εδόθη στο (i)) είναι μεταθέτης ενός ζεύγους πινάκων ανηκόντων στην $\mathrm{GL}_2(\mathbb{R})$. Άρα κάθε πίνακας ανήκων στην $\mathrm{SL}_2(\mathbb{R})$ παρίσταται ως γινόμενο μεταθετών, απ' όπου έπεται ότι $\mathrm{SL}_2(\mathbb{R}) \sqsubseteq \mathrm{GL}_2(\mathbb{R})'$. □

5.5.16 Σημείωση. Με παρόμοιο τρόπο (αλλά με κάπως περισσότερο κόπο) αποδεικνύεται ότι για οιοδήποτε σώμα F και για οιονδήποτε φυσικό αριθμό $n \geq 2$ ισχύουν τα εξής:

$$\boxed{\mathrm{GL}_n(F)' \begin{cases} = \mathrm{SL}_n(F), & \text{όταν } (n, \chi\alpha\rho(F)) \neq (2,2), \\ \cong \mathbb{Z}_3, & \text{όταν } n = 2 \text{ και } F \cong \mathbb{Z}_2, \end{cases}} \tag{5.54}$$

και

$$\boxed{\mathrm{SL}_n(F)' \begin{cases} = \mathrm{SL}_n(F), & \text{όταν } (n, \chi\alpha\rho(F)) \notin \{(2,2),(2,3)\}, \\ \cong \mathbb{Z}_3, & \text{όταν } n = 2 \text{ και } F \cong \mathbb{Z}_2, \\ \cong \mathbf{Q}, & \text{όταν } n = 2 \text{ και } F \cong \mathbb{Z}_3, \end{cases}} \tag{5.55}$$

όπου $\mathbf{Q}$ η ομάδα των τετρανίων, $\mathrm{SL}_2(\mathbb{Z}_2) \cong \mathfrak{S}_3$ και $\mathrm{SL}_2(\mathbb{Z}_3)$ η λεγομένη **δυαδική τετραεδρική ομάδα** τάξεως 24.

5.5.17 Θεώρημα. (E. Spiegel, 1976) *Εάν υποτεθεί ότι η $(G,\cdot)$ είναι μια ομάδα έχουσα μια ορθόθετη αβελιανή υποομάδα H, τέτοια ώστε η G/H να είναι κυκλική, τότε η* (5.52) *ισχύει ως ισότητα.*

ΑΠΟΔΕΙΞΗ[47]. Κατ' αρχάς σημειώνουμε ότι αρκεί ο προσδιορισμός μιας ορθόθετης υποομάδας K τής G, τέτοιας ώστε η G/K να είναι αβελιανή και να ισχύει $K \subseteqq \{[x,y] \,|\, (x,y) \in G \times G\}$, διότι εν τοιαύτη περιπτώσει (λόγω τής "$\Rightarrow$" τής προτάσεως 5.5.11) θα έχουμε

$$G' \sqsubseteq K \subseteqq \{[x,y] \,|\, (x,y) \in G \times G\} \subseteqq G',$$

ήτοι $G' = \{[x,y] \,|\, (x,y) \in G \times G\}$. Εξ υποθέσεως, υπάρχει $g \in G$, τέτοιο ώστε να ισχύει $G/H = \langle gH \rangle$. Θέτοντας $K := \{[g,h] \,|\, h \in H\}$, παρατηρούμε ότι

$$e_G \in K \subseteqq \{[x,y] \,|\, (x,y) \in G \times G\}$$

και ότι για οιαδήποτε στοιχεία $h_1, h_2 \in H$,

$$[g,h_1]\left[g,h_2^{-1}\right] = \left[g,h_1h_2^{-1}\right]\left[\left[h_2^{-1},g\right],h_1\right]^{-1} = \left[g,h_1h_2^{-1}\right]\left[h_1,\left[h_2^{-1},g\right]\right]$$

(βλ. 5.5.2 (v)), όπου $\left[h_1,\left[h_2^{-1},g\right]\right] = e_G$, διότι

$$\left.\begin{aligned} h_2 \in H &\Rightarrow h_2^{-1} \in H \\ H \trianglelefteq G &\Rightarrow gh_2g^{-1} \in H \end{aligned}\right\} \Longrightarrow h_2^{-1}\left(gh_2g^{-1}\right) = \left[h_2^{-1},g\right] \in H$$

και η H είναι αβελιανή. Άρα $[g,h_1]\left[g,h_2^{-1}\right] = \left[g,h_1h_2^{-1}\right] \in K \Rightarrow K \sqsubseteq G$. Σημειωτέον ότι

$$K = \mathrm{ΚΛΣ}_G(g)\,\mathrm{ΚΛΣ}_G(g^{-1}). \tag{5.56}$$

Πράγματι· για κάθε $h \in H$ είναι πρόδηλο ότι

$$[g,h] = \underbrace{g}_{\in \mathrm{ΚΛΣ}_G(g)}\ \underbrace{hg^{-1}h^{-1}}_{\in \mathrm{ΚΛΣ}_G(g^{-1})} \Longrightarrow K \subseteqq \mathrm{ΚΛΣ}_G(g)\,\mathrm{ΚΛΣ}_G(g^{-1}).$$

Και αντιστρόφως· εάν $z \in \mathrm{ΚΛΣ}_G(g)$ και $w \in \mathrm{ΚΛΣ}_G(g^{-1})$, τότε υπάρχουν $x,y \in G$, τέτοια ώστε να ισχύουν οι ισότητες $z = xgx^{-1}$ και $w = yg^{-1}y^{-1}$. Επιπροσθέτως, επειδή $xH \in \langle gH \rangle$,

$$[\exists i \in \mathbb{Z} : xH = (gH)^i = g^iH] \Longrightarrow [\exists a \in H : x = ag^i].$$

[47] Η παρατιθέμενη απόδειξη αποτελεί ελαφρά παραλλαγή εκείνης τού Thm. 2 στο άρθρο τού E. Spiegel: *Calculating commutators in groups*, Mathematics Magazine **49** (1976), 192-194.

Κατ' αναλογίαν, επειδή $yH \in \langle gH\rangle$, συμπεραίνουμε ότι

$$[\exists j \in \mathbb{Z} : yH = (gH)^j = g^jH] \Longrightarrow [\exists b \in H : y = bg^j].$$

Επομένως,

$$\begin{aligned} zw &= (ag^i)g(ag^i)^{-1}(bg^i)g^{-1}(bg^i)^{-1} = (ag^igg^{-i}a^{-1})(bg^jg^{-1}g^{-j}b^{-1}) \\ &= (aga^{-1})(bg^{-1}b^{-1}) = a(g(b^{-1}a)^{-1}g^{-1})b^{-1} \end{aligned} \tag{5.57}$$

και

$$\left.\begin{array}{r} b^{-1} \in H \\ a \in H \end{array}\right\} \Rightarrow b^{-1}a \in H \Rightarrow (b^{-1}a)^{-1} \in H \underset{H\trianglelefteq G}{\Longrightarrow} g(b^{-1}a)^{-1}g^{-1} \in H. \tag{5.58}$$

Η υποομάδα H είναι εξ υποθέσεως αβελιανή. Ως εκ τούτου, από τις (5.57) και (5.58) έπεται ότι

$$a(g(b^{-1}a)^{-1}g^{-1}) \in H \Rightarrow zw = b^{-1}a(g(b^{-1}a)^{-1}g^{-1}) = [b^{-1}a, g] = [g, b^{-1}a]^{-1} \in K$$

(καθόσον $K \sqsubseteq G$). Συνεπώς ισχύει και ο αντίστροφος εγκλεισμός $\text{ΚΛΣ}_G(g)\,\text{ΚΛΣ}_G(g^{-1}) \subseteqq K$ και η ισότητα (5.56) είναι αληθής. Για οιαδήποτε $s \in G$ και $t \in K$ έχουμε $t = t_1t_2$ για κάποια στοιχεία $t_1 \in \text{ΚΛΣ}_G(g)$ και $t_2 \in \text{ΚΛΣ}_G(g^{-1})$, και

$$sts^{-1} = \underbrace{(st_1s^{-1})}_{\in \text{ΚΛΣ}_G(g)}\ \underbrace{(st_2s^{-1})}_{\in \text{ΚΛΣ}_G(g^{-1})} \in K \Rightarrow K \trianglelefteq G.$$

Άρα ορίζεται η πηλικοομάδα G/K, η οποία τυγχάνει να είναι και αβελιανή, καθότι

$$\begin{aligned} [gK, hK] &= \underbrace{[g,h]}_{\in K}K = K = e_{G/K} \Rightarrow (gK)\,(hK) = (hK)\,(gK) \\ &\Rightarrow (g^mK)\,(hK) = (hK)\,(g^mK)\,, \end{aligned} \tag{5.59}$$

για κάθε $h \in H$ και για κάθε $m \in \mathbb{Z}$. (Βλ. εδ. 5.5.3 και άσκηση **2-5**.) Επομένως, για οιαδήποτε στοιχεία $g_1, g_2 \in G$ έχουμε $g_1 = ag^i$, $g_2 = bg^j$, για κάποια $a, b \in H$ και κάποιους $i, j \in \mathbb{Z}$, και

$$\begin{aligned} &(g_1K)\,(g_2K) = \left(ag^iK\right)\left(bg^jK\right) = (aK)\left(g^iK\right)(bK)\left(g^jK\right) \\ &= (aK)\,(bK)\left(g^iK\right)\left(g^jK\right) = (bK)\,(aK)\left(g^jK\right)\left(g^iK\right) = (bK)\left(g^jK\right)(aK)\left(g^iK\right) \\ &= \left(bg^jK\right)\left(ag^iK\right) = (g_2K)\,(g_1K)\,, \end{aligned}$$

λογω τής (5.59) και τού ότι η H είναι αβελιανή. Εδώ λήγει η απόδειξη. □

5.5.18 Παραδείγματα. Το θεώρημα 5.5.17 είναι άμεσα εφαρμόσιμο στις ακόλουθες περιπτώσεις:

G	H
$\mathbf{Q} = \langle \mathbf{j}, \mathbf{k}\rangle$	$\langle \mathbf{j}\rangle$
$\mathfrak{A}_4$	$\mathbf{V}$
$\mathbf{D}_n = \langle \alpha, \beta\rangle$	$\langle \beta\rangle$

.

5.5.19 Θεώρημα. (R.M. Guralnick, 1980/ L.-Ch. Kappe & R.F. Morse, 2005) *Εάν μια ομάδα G ικανοποιεί κάποια εκ των ακολούθων τεσσάρων συνθηκών, τότε η* (5.52) *ισχύει ως ισότητα*[48].

(i) *$H\,G'$ είναι αβελιανή και είτε $|G| < 128$ είτε $|G'| < 16$.*

(ii) *$H\,G'$ είναι μη αβελιανή και είτε $|G| < 96$ είτε $|G'| < 24$.*

(iii) *$|G| = p^n$, όπου p είναι ένας περιττός πρώτος και $n \leq 5$.*

(iv) *$|G| = 2^n$, όπου $n \leq 6$.*

5.5.20 Θεώρημα. (I. Schur, 1904) *Έστω $(G, \cdot)$ μια (όχι κατ' ανάγκην πεπερασμένη) ομάδα. Εάν $|G : Z(G)| = n \in \mathbb{N}$, τότε ισχύουν τα εξής:*

(i) *$H\,G$ διαθέτει το πολύ n^2 σαφώς διακεκριμένους μεταθέτες.*

(ii) *Για κάθε $(x, y) \in G \times G$ αληθεύει η ισότητα*

$$[x, y]^{n+1} = \left[x, y^2\right] \left[yxy^{-1}, y\right]^{n-1}. \tag{5.60}$$

(iii) $|G'| \leq (n^2)^{n^3} < \infty$.

ΑΠΟΔΕΙΞΗ. (i) Έστω $\{z_1,..., z_n\}$ ένα σύστημα δεξιών εκπροσώπων τού κέντρου $Z(G)$ εντός τής G. Εξ ορισμού, $G = \coprod_{j=1}^{n} Z(G)z_j$. Εάν $[x_1, y_1], [x_2, y_2]$ είναι δυο μεταθέτες ανήκοντες στην G, αρκεί να αποδειχθεί η συνεπαγωγή

$$[Z(G)x_1 = Z(G)x_2 \text{ και } Z(G)y_1 = Z(G)y_2] \Rightarrow [x_1, y_1] = [x_2, y_2],$$

διότι τότε το σύνολο των διακεκριμένων μεταθετών τής G θα είναι υποσύνολο τού $\{[z_i, z_j] \,|1 \leq i, j \leq n\}$. Προφανώς,

$$\left[\begin{array}{c} Z(G)x_1 = Z(G)x_2 \\ \text{και } Z(G)y_1 = Z(G)y_2 \end{array}\right] \Rightarrow \left[\begin{array}{c} x_1x_2^{-1} \in Z(G) \\ \text{και } y_1y_2^{-1} \in Z(G) \end{array}\right],$$

πράγμα που σημαίνει ότι τα $x_1x_2^{-1}$ και $y_1y_2^{-1}$ μετατίθενται αμοιβαίως με κάθε στοιχείο τής G. Άρα

$$\begin{aligned}
[x_1, y_1] &= (x_2x_2^{-1})x_1(y_2y_2^{-1})y_1x_1^{-1}(x_2x_2^{-1})y_1^{-1}(y_2y_2^{-1}) \\
&= x_2\left(x_1^{-1}x_2\right)^{-1} y_2\left(y_1^{-1}y_2\right)^{-1}(x_1^{-1}x_2)x_2^{-1}(y_1^{-1}y_2)y_2^{-1} \\
&= x_2\left(\left(x_1^{-1}x_2\right)^{-1}(x_1^{-1}x_2)\right) y_2\left(\left(y_1^{-1}y_2\right)^{-1}(y_1^{-1}y_2)\right) x_2^{-1}y_2^{-1} \\
&= x_2e_Gy_2e_Gx_2^{-1}y_2^{-1} = x_2y_2x_2^{-1}y_2^{-1} = [x_2, y_2].
\end{aligned}$$

(ii) Επειδή $|G : Z(G)| = n = |G/Z(G)|$, έχουμε (λόγω τού πορίσματος 4.1.28)

$$[Z(G)g^n = (Z(G)g)^n = Z(G),\ \forall g \in G] \Longrightarrow [g^n \in Z(G),\ \forall g \in G].$$

[48]Για τις (i) και (ii) βλ. R.M. Guralnick: *Expressing group elements as commutators*, Rocky Mountain Journal of Mathematics **10** (1980), 651-654, ενώ για τις (iii) και (iv) βλ. L.-Ch. Kappe & R.F. Morse: *On commutators in p-groups*, Journal of Group Theory **8** (2005) 415-429.

Εξ αυτού συμπεραίνουμε ότι για κάθε ζεύγος $(x,y)\in G\times G$ ισχύει $[x,y]^n\in Z(G)$, ήτοι ότι το $[x,y]^n$ μετατίθεται αμοιβαίως με κάθε στοιχείο τής G. Ως εκ τούτου,

$$\begin{aligned}
[x,y]^{n+1} &= [x,y]\,[x,y]^n = xyx^{-1}y^{-1}\,[x,y]^n = xyx^{-1}\,[x,y]^n\,y^{-1}\\
&= xyx^{-1}\,[x,y]\,[x,y]^{n-1}\,y^{-1} = \big(xyx^{-1}\big)\,\big(xyx^{-1}y^{-1}\big)\,[x,y]^{n-1}\,y^{-1}\\
&= xy^2x^{-1}y^{-2}(y\,[x,y]^{n-1}\,y^{-1})\\
&= \big[x,y^2\big]\,\underbrace{((y\,[x,y]\,y^{-1})(y\,[x,y]\,y^{-1})\cdots(y\,[x,y]\,y^{-1}))}_{n-1\ \text{φορές}}\\
&= \big[x,y^2\big]\,(y\,[x,y]\,y^{-1})^{n-1} = \big[x,y^2\big]\,(\big[yxy^{-1},y\big])^{n-1},
\end{aligned}$$

όπου η τελευταία ισότητα έπεται από το 5.5.2 (ii).

(iii) Έστω $g\in G$ ένας *παγιωμένος* μεταθέτης (ενός ζεύγους στοιχείων) τής G. Για κάθε $(\mu,\nu)\in\mathbb{N}_0\times\mathbb{N}_0$ συμβολίζουμε ως A_ν το σύνολο των στοιχείων τής G τα οποία μπορούν να γραφούν ως γινόμενα ν μεταθετών που είναι $\neq g$ (με $A_0:=\{e_G\}$) και ως $B_{\mu,\nu}$ το σύνολο των στοιχείων τής G τα οποία μπορούν να γραφούν ως γινόμενα $\mu+\nu$ μεταθετών με τους μ εξ αυτών ίσους με το g και τους ν εξ αυτών $\neq g$. Το $\{g\}$ παραμένει αναλλοίωτο ύστερα από εφαρμογή τού αυτομορφισμού

$$\boldsymbol{\gamma}_g : G\longrightarrow G,\quad \boldsymbol{\gamma}_g(x)=gxg^{-1},\ \ \forall x\in G,$$

(βλ. 5.4.21), ήτοι $\boldsymbol{\gamma}_g(g)=g$. Επιπροσθέτως, ο αυτομορφισμός $\boldsymbol{\gamma}_g$ σταθεροποιεί τα A_ν και $B_{\mu,\nu}$, δηλαδή

$$\boldsymbol{\gamma}_g(A_\nu)=A_\nu,\ \ \boldsymbol{\gamma}_g(B_{\mu,\nu})=B_{\mu,\nu}.$$

Χρησιμοποιώντας μαθηματική επαγωγή ως προς τον μ θα δείξουμε ότι για κάθε $\nu\in\mathbb{N}_0$ ισχύει η ισότητα $B_{\mu,\nu}=A_\nu g^\mu$. Επειδή ο εγκλεισμός $A_\nu g^\mu\subseteq B_{\mu,\nu}$ είναι προφανής, θα περιορισθούμε στην απόδειξη τού αντιστρόφου εγκλεισμού $B_{\mu,\nu}\subseteq A_\nu g^\mu$. Αυτός είναι προφανώς αληθής για $\mu=0$. Θεωρούμε έναν $\mu\geq 1$ και υποθέτουμε ότι αυτός ο εγκλεισμός είναι αληθής για τον $\mu-1$. Έστω $\nu\in\mathbb{N}_0$ και έστω $x\in B_{\mu,\nu}$. Εξ ορισμού, το x μπορεί να γραφεί ως γινόμενο $\mu+\nu$ μεταθετών με τους $\mu\,(\geq 1)$ εξ αυτών ίσους με το g και τους ν εξ αυτών $\neq g$. Εάν ο πρώτος παράγοντας τού εν λόγω γινομένου που είναι ίσος με το g είναι ο i-οστός (όπου $i\in\{1,...,\mu+\nu\}$), τότε βλέπουμε ότι $x\in A_{i-1}gB_{\mu-1,\nu-i+1}$, όπου

$$\begin{aligned}
A_{i-1}gB_{\mu-1,\nu-i+1} &= A_{i-1}\,\big(gB_{\mu-1,\nu-i+1}g^{-1}\big)\,g\\
&= A_{i-1}\,\big(\boldsymbol{\gamma}_g(B_{\mu-1,\nu-i+1})\big)\,g = A_{i-1}B_{\mu-1,\nu-i+1}g\subseteq B_{\mu-1,\nu}g.
\end{aligned}$$

Κάνοντας χρήση τής επαγωγικής υποθέσεως λαμβάνουμε

$$x\in B_{\mu-1,\nu}g = A_\nu g^{\mu-1}g = A_\nu g^\mu.$$

Άρα η ισότητα $B_{\mu,\nu}=A_\nu g^\mu$ είναι όντως αληθής για κάθε ζεύγος $(\mu,\nu)\in\mathbb{N}_0\times\mathbb{N}_0$. Εν συνεχεία, για κάθε $m\in\mathbb{N}$ συμβολίζουμε ως E_m το σύνολο των στοιχείων τής G τα οποία μπορούν να γραφούν ως γινόμενα m μεταθετών και θέτουμε

$$k:=\text{card}(\{\text{μεταθέτες τής } G\}).$$

(Στο (i) έχουμε αποδείξει ότι $k \leq n^2$.) Εάν $m > nk$, τότε $E_m \subseteq E_{m-1}$. Εάν ένα $x \in G$ μπορεί να γραφεί ως γινόμενο m μεταθετών, όπου $m > nk$, τότε, επειδή υφίστανται εν συνόλω k (σαφώς διακεκριμένοι) μεταθέτες, τουλάχιστον ένας εξ αυτών -τον οποίο σκοπίμως «ονομάζουμε» g- επαναλαμβάνεται μ φορές εντός τού γινομένου, όπου $\mu > n$. Επανασυνδεόμενοι λοιπόν με τα προαναφερθέντα, παρατηρούμε ότι

$$\left.\begin{array}{r} x \in B_{\mu,m-\mu} = A_{m-\mu} g^{\mu} \\ \mu > n \end{array}\right\} \Rightarrow x \in E_{m-n-1} g^{n+1}.$$

Βάσει τής ισότητας (5.60), $g^{n+1} \in E_n$. Ως εκ τούτου, $x \in E_{m-n-1} E_n \subseteq E_{m-1}$. Εξ αυτού συμπεραίνουμε ότι για όλους τους $m \geq nk$ ισχύει ο εγκλεισμός $E_m \subseteq E_{nk}$. Είναι σαφές ότι το E_{nk} είναι κλειστό ως προς την πράξη τής ομάδας και ότι τα αντίστροφα των στοιχείων του ανήκουν σε αυτό (καθότι το αντίστροφο ενός μεταθέτη είναι αφ' εαυτού μεταθέτης, βλ. 5.5.2 (i)). Άρα το E_{nk} αποτελεί μια *υποομάδα* τής G. *Κάθε μεταθέτης* τής G ανήκει κατ' ανάγκην στο E_{nk}, διότι για *οιονδήποτε* μεταθέτη g υπάρχει κάποιος φυσικός αριθμός μ με $2\mu + 1 \geq nk$, οπότε $g = g^{\mu+1} g^{-\mu} \in E_{2\mu+1} \subseteq E_{nk}$. Κατά συνέπειαν, $E_{nk} = G'$. Τέλος, επειδή υφίστανται εν συνόλω k (σαφώς διακεκριμένοι) μεταθέτες, ο αριθμός των γινομένων nk μεταθετών είναι $\leq k^{nk}$. Αυτό σημαίνει ότι $|G'| \leq k^{nk} \leq (n^2)^{n^3}$. □

5.5.21 Σημείωση. Η ανωτέρω παρατεθείσα απόδειξη είναι εκτενής αλλά στοιχειώδης. Η αρχική απόδειξη τού Issai Schur[49] (1875-1941) (ισχύουσα μόνον για *πεπερασμένες* ομάδες) χρησιμοποιεί προτάσεις από τη Θεωρία Αναπαραστάσεων. Καλύτερα άνω φράγματα τής $|G'|$ για *ειδικές ομάδες* έχουν προσδιορισθεί από τους J. Wiegold[50] και R.M. Guralnick[51].

5.5.22 Πόρισμα. *Έστω $(G, \cdot)$ μια (όχι κατ' ανάγκην πεπερασμένη) ομάδα. Εάν $|G : Z(G)| = n \in \mathbb{N}$ και $|G'| > n^2$, τότε η* (5.52) *ισχύει ως γνήσιος εγκλεισμός.*

ΑΠΟΔΕΙΞΗ. Τούτο είναι προφανές, διότι (σύμφωνα με το 5.5.20 (i)) το πλήθος των σαφώς διακεκριμένων μεταθετών είναι $\leq n^2$. □

Μέσω τού προηγηθέντος θεωρήματος 5.5.20 και τού επομένου λήμματος 5.5.23 είναι δυνατή η παρουσίαση ενός εντυπωσιακού αποτελέσματος τού Y. Fedorov[52]: *Για την κυκλικότητα μιας άπειρης ομάδας αρκεί κάθε μη τετριμμένη υποομάδα της να είναι υποομάδα πεπερασμένου δείκτη εντός αυτής.* (Βλ. θεώρημα 5.5.24.)

5.5.23 Λήμμα. *Έστω $(G, \cdot)$ μια άπειρη ομάδα. Εάν $|G : H| < \infty$ για κάθε μη τετριμμένη υποομάδα H τής G, τότε ισχύουν τα εξής:*

(i) *Κάθε μη τετριμμένη υποομάδα H τής G είναι άπειρη.*

[49] I. Schur: *Über die Darstellung der endlichen Gruppen durch gebrochen lineare Substitutionen*, J. Reine und Angew. Math. **127** (1904), 20-50.

[50] J. Wiegold: *Multiplicators and groups with finite central factor-groups*, Math. Zeitschrift **89** (1965), 345-347.

[51] R.M. Guralnick: *On a result of Schur*, Journal of Algebra **52** (1979), 302-310.

[52] Βλ. Y. Fedorov: *On infinite groups of which all nontrivial subgroups have a finite index*, Uspekhi Mat. Nauk. **6** (1951), 187-189.

(ii) $\text{ord}(g) = \infty,\ \forall g \in G \setminus \{e_G\}$.

(iii) *Εάν* $x, y \in G \setminus \{e_G\}$, *τότε υπάρχουν* $a, b \in \mathbb{N}$, *τέτοιοι ώστε να ισχύει*

$$\langle x^a \rangle = \langle x \rangle \cap \langle y \rangle = \left\langle y^b \right\rangle .$$

(iv) $Z(G) \neq \{e_G\}$.

(v) *Εάν η* G *είναι αβελιανή, τότε η* G *είναι κατ' ανάγκην κυκλική.*

ΑΠΟΔΕΙΞΗ[53]. (i) Έστω H τυχούσα μη τετριμμένη υποομάδα τής G. Εξ υποθέσεως, $|G : H| = n$, για κάποιον $n \in \mathbb{N}$, οπότε υπάρχει σύστημα δεξιών εκπροσώπων $\{g_1 = e_G, g_2, ..., g_n\}$ τής H εντός τής G. Επειδή

$$G = \coprod_{j=1}^{n} Hg_j \ \text{ και } \ \text{card}(Hg_j) = |H| \, , \ \forall j \in \{1, ..., n\}$$

(βλ. εδ. 4.1.12), η H δεν μπορεί να είναι πεπερασμένη υποομάδα (διότι αλλιώς και το ίδιο το υποκείμενο σύνολο τής ομάδας αναφοράς μας, ως αποσυνδετή ένωση *πεπερασμένων* συνόλων, θα ήταν πεπερασμένο).

(ii) Επειδή για κάθε $g \in G$ ισχύει $\text{ord}(g) = |\langle g \rangle|$ (βλ. 2.3.2), τούτο είναι προφανές κατόπιν εφαρμογής τού (i) (για τις υποομάδες $\langle g \rangle \, , \, g \in G \setminus \{e_G\}$).

(iii) Εάν $x, y \in G \setminus \{e_G\}$, τότε το $\left\{ \langle x \rangle \, y^i \middle| \, i \in \mathbb{Z} \right\}$ είναι ένα σύνολο δεξιών πλευρικών κλάσεων τής $\langle x \rangle$ εντός τής G. Επειδή (εξ υποθέσεως) $|G : \langle x \rangle| < \infty$, αυτό οφείλει να είναι πεπερασμένο, οπότε

$$[\exists \, (i, j) \in \mathbb{Z} \times \mathbb{Z} : i > j \ \text{ και } \ \langle x \rangle \, y^i = \langle x \rangle \, y^j] \Rightarrow y^{i-j} \in \langle x \rangle$$

και, κατ' επέκταση,

$$\left.\begin{array}{r} y^{i-j} \in \langle y \rangle \Rightarrow y^{i-j} \in \langle x \rangle \cap \langle y \rangle \\ y \in G \setminus \{e_G\} \underset{\text{(ii)}}{\Longrightarrow} \text{ord}(y) = \infty \Rightarrow y^{i-j} \neq e_G \end{array}\right\} \Rightarrow \langle x \rangle \cap \langle y \rangle \neq \{e_G\}.$$

Από το ότι η μη τετριμμένη υποομάδα $\langle x \rangle \cap \langle y \rangle$ τής G αποτελεί υποομάδα αμφοτέρων των άπειρων κυκλικών ομάδων $\langle x \rangle$ και $\langle y \rangle$ έπεται (μέσω τού (i) τού πορίσματος 2.4.25) ότι $\langle x^a \rangle = \langle x \rangle \cap \langle y \rangle = \left\langle y^b \right\rangle$ για κάποιους $a, b \in \mathbb{N}$.

(iv) Έστω τυχόν $g \in G \setminus \{e_G\}$. Εξ υποθέσεως, $|G : \langle g \rangle| = n$, για κάποιον $n \in \mathbb{N}$, οπότε για κάθε σύστημα δεξιών εκπροσώπων $\{x_0 = e_G, x_1, ..., x_{n-1}\}$ τής $\langle g \rangle$ εντός τής G έχουμε

$$G = \langle g \rangle \coprod \langle g \rangle \, x_1 \coprod \cdots \coprod \langle g \rangle \, x_{n-1}. \tag{5.61}$$

Εάν $n = 1$, τότε $G = \langle g \rangle \Rightarrow G = Z(G) \neq \{e_G\}$. Ας υποθέσουμε ότι $n \geq 2$. Επειδή $g, x_i \in G \setminus \{e_G\}$ για κάθε $i \in \{1, ..., n-1\}$, από το (iii) εξασφαλίζεται η ύπαρξη φυσικών αριθμών m_i, l_i για τους οποίους ισχύει

$$g^{m_i} = x_i^{l_i} \in \langle x_i \rangle \, , \ \forall i \in \{1, ..., n-1\}.$$

[53] Εν προκειμένω ακολουθείται η εκ μέρους τού Ch. Lanski αισθητή απλοποίηση τής αρχικής αποδείξεως τού θεωρήματος 5.5.24 (τού Y. Fedorov) μέσω τής χρήσεως τού «αρκούντως στοιχειώδους» λήμματος 5.5.23, η οποία δημοσιεύθηκε 50 έτη αργότερα. Βλ. Ch. Lanski: *A characterization of infinite cyclic groups*, Mathematics Magazine, Vol. **74**, No. 1 (2001), 61-65.

Θέτοντας $m := \prod_{i=1}^{n-1} m_i$ και $r_i := \frac{m}{m_i} \in \mathbb{N}$ λαμβάνουμε

$$g^m = (g^{m_i})^{r_i} \in \langle x_i \rangle = Z(\langle x_i \rangle),\ \forall i \in \{1, ..., n-1\},$$

απ' όπου προκύπτει ότι[54] $g^m x_i = x_i g^m$ για κάθε $i \in \{0, 1, ..., n-1\}$. Για *οιοδήποτε στοιχείο* $y \in G$ υπάρχει (λόγω τής (5.61)) κάποιος $i \in \{0, 1, ..., n-1\}$, τέτοιος ώστε να ισχύει $y \in \langle g \rangle x_i$, οπότε $\exists k \in \mathbb{Z}$:

$$y = g^k x_i \Rightarrow g^m y = g^m (g^k x_i) = g^k (g^m x_i) = g^k (x_i g^m) = (g^k x_i) g^m = y g^m.$$

Επομένως, $g^m \in Z(G)$, όπου

$$g \in G \setminus \{e_G\} \underset{\text{(ii)}}{\Longrightarrow} \text{ord}(g) = |\langle g \rangle| = \infty \Rightarrow g^m \neq e_G.$$

Εξ αυτού έπεται ότι $Z(G) \neq \{e_G\}$.

(v) Ας υποθέσουμε ότι η G είναι *αβελιανή*. Εξ υποθέσεως, $|G : \langle g \rangle| < \infty$ για κάθε $g \in G \setminus \{e_G\}$. Επιλέγουμε ένα $x \in G \setminus \{e_G\}$, τέτοιο ώστε να ισχύει

$$|G : \langle x \rangle| = \min \{|G : \langle g \rangle| : g \in G \setminus \{e_G\}\}.$$

Περίπτωση πρώτη. Εάν $G = \langle x \rangle$, τότε η G είναι *κυκλική* και η απόδειξη λήγει εδώ.

Περίπτωση δεύτερη. Υποθέτοντας ότι $\langle x \rangle \sqsubset G$, καταλήγουμε *σε άτοπο* ως ακολούθως: Επιλέγουμε τυχόν $y \in G \setminus \langle x \rangle$. Δυνάμει τού (i) υπάρχουν $\nu, \xi \in \mathbb{N}$, τέτοιοι ώστε να ισχύει $x^\nu = y^\xi$. Θέτοντας $d := \text{μκδ}(\nu, \xi)$, $\nu' := \frac{\nu}{d}$ και $\xi' := \frac{\xi}{d}$ παρατηρούμε ότι

$$\begin{aligned} &xy = yx \Rightarrow (x^{\nu'} y^{-\xi'})^d = (x^{\nu'})^d (y^{-\xi'})^d = x^\nu y^{-\xi} = e_G \\ &\Rightarrow x^{\nu'} y^{-\xi'} = e_G \ (\text{διότι } x^{\nu'} y^{-\xi'} \neq e_G \Rightarrow \text{ord}(x^{\nu'} y^{-\xi'}) = \infty) \\ &\Rightarrow x^{\nu'} = y^{\xi'}. \end{aligned}$$

Επειδή $\text{μκδ}(\nu', \xi') = 1$ (βλ. Β.2.14 (ii)), υπάρχουν (κατά το πόρισμα Β.2.8) $r, s \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει $r\nu' + s\xi' = 1$. Για το *ειδικό στοιχείο* $g := x^s y^r$ έχουμε αφ' ενός μεν

$$\begin{aligned} &xy = yx \Rightarrow g^{\xi'} = (x^s y^r)^{\xi'} = (x^s)^{\xi'} (y^r)^{\xi'} \\ &= x^{s\xi'} (y^{\xi'})^r = x^{s\xi'} (x^{\nu'})^r = x^{s\xi' + r\nu'} = x, \end{aligned}$$

αφ' ετέρου δε

$$\begin{aligned} &xy = yx \Rightarrow g^{\nu'} = (x^s y^r)^{\nu'} = (x^s)^{\nu'} (y^r)^{\nu'} \\ &= (x^{\nu'})^s y^{r\nu'} = (y^{\xi'})^s y^{r\nu'} = y^{s\xi' + r\nu'} = y, \end{aligned}$$

οπότε $x, y \in \langle g \rangle$ και, ως εκ τούτου,

$$\left.\begin{array}{r} \langle x \rangle \sqsubseteq \langle g \rangle \\ y \in G \setminus \langle x \rangle,\ y \in \langle g \rangle \end{array}\right\} \Rightarrow \langle x \rangle \sqsubset \langle g \rangle \underset{4.1.50}{\Longrightarrow} |G : \langle g \rangle| < |G : \langle x \rangle|,$$

κάτι που *αντίκειται* στον ορισμό τού x. □

[54] Για $i = 0$ η εν λόγω ισότητα είναι προφανής.

5.5.24 Θεώρημα. (Y. Fedorov, 1951) *Έστω $(G,\cdot)$ μια άπειρη ομάδα. Εάν ισχύει $|G:H|<\infty$ για κάθε μη τετριμμένη υποομάδα H τής G, τότε η G είναι κατ' ανάγκην κυκλική* (*ήτοι ισόμορφη τής* $(\mathbb{Z},+)$, βλ. 2.4.23 (i)).

ΑΠΟΔΕΙΞΗ. Από το (iv) τού λήμματος 5.5.23 γνωρίζουμε ότι $Z(G)\neq\{e_G\}$, οπότε (εξ υποθέσεως) $|G:Z(G)|<\infty$. Από την άλλη μεριά, από το θεώρημα 5.5.20 έπεται ότι $|G'|<\infty \underset{5.5.23\,(i)}{\Longrightarrow} G'=\{e_G\}$. Άρα η G (σύμφωνα με την πρόταση 5.5.6) είναι αβελιανή και, ως εκ τούτου, κυκλική (βάσει τού (v) τού λήμματος 5.5.23). □

5.5.25 Ορισμός. Έστω $(G,\cdot)$ μια ομάδα. Συμβολίζουμε ως

$$\boxed{G^{\mathrm{ab}}:=G/G'}$$

την (κατ' ανάγκην *αβελιανή*) πηλικοομάδα τής G ως προς την G'. Η μετάβαση από την G στην G^{ab} (ή, ενίοτε, και η ίδια η G^{ab}) καλείται **αβελιανοποίηση**[55] **τής** G.

5.5.26 Παραδείγματα. (i) Βάσει των προαναφερθέντων στα εδάφια 5.4.18 (i) και 5.5.13,

$$\boxed{\mathbf{Q}^{\mathrm{ab}}:=\mathbf{Q}/\mathbf{Q}'=\mathbf{Q}/Z(\mathbf{Q})\cong\mathbf{V}.}$$

(ii) Έστω $n\in\mathbb{N}$, $n\geq 3$. Η $\langle\beta^2\rangle$ είναι μια ορθόθετη υποομάδα τής n-οστής διεδρικής ομάδας $\mathbf{D}_n=\langle\alpha,\beta\rangle$ με δείκτη

$$\left|\mathbf{D}_n:\langle\beta^2\rangle\right|=\left|\mathbf{D}_n/\langle\beta^2\rangle\right|=\begin{cases}2, & \text{όταν ο } n \text{ είναι περιττός,}\\ 4, & \text{όταν ο } n \text{ είναι άρτιος.}\end{cases}$$

Επομένως η $\mathbf{D}_n/\langle\beta^2\rangle$ οφείλει να είναι αβελιανή (βλ. 2.3.19 και 3.5.6). Σύμφωνα με την πρόταση 5.5.11 η μεταθέτρια υποομάδα $\mathbf{D}_n'$ τής $\mathbf{D}_n$ είναι υποομάδα τής $\langle\beta^2\rangle$. Εξάλλου,

$$[\beta,\alpha]=\beta\circ\left(\alpha\circ\beta^{-1}\right)\circ\alpha^{-1}\underset{(3.16)}{=}\beta\circ(\beta\circ\alpha)\circ\alpha^{-1}=\beta^2,$$

οπότε το β^2 είναι ένας μεταθέτης. Άρα $\mathbf{D}_n'=\langle\beta^2\rangle$. Κατά συνέπειαν,

$$\boxed{\mathbf{D}_n^{\mathrm{ab}}\cong\begin{cases}\mathbb{Z}_2, & \text{όταν ο } n \text{ είναι περιττός,}\\ \mathbf{V}, & \text{όταν ο } n \text{ είναι άρτιος.}\end{cases}}$$

(iii) Λαμβάνοντας υπ' όψιν τον μέχρις ισομορφισμού υπολογισμό τής μεταθέτριας υποομάδας $\mathfrak{S}_n'$ τής $\mathfrak{S}_n$ (βλ. 5.5.9), συμπεραίνουμε ότι

$$\boxed{\mathfrak{S}_n^{\mathrm{ab}}\cong\mathbb{Z}_2,\ \text{για κάθε } n\geq 2.}$$

[55] Η αβελιανοποίηση ομάδων έχει πληθώρα εφαρμογών στην Αλγεβρική Τοπολογία. Επί παραδείγματι, η πρώτη ιδιάζουσα ομάδα ομολογίας $H_1^{\mathrm{sing}}(X;\mathbb{Z})$ ενός δρομοσυνεκτικού τοπολογικού χώρου X είναι ισόμορφη με την αβελιανοποίηση $\pi_1^{\mathrm{ab}}(X)$ τής θεμελιώδους ομάδας $\pi_1(X)$ τού X. (Βλ., π.χ., M.J. Greenberg, J.R. Harper: *Algebraic Topology. A First Course*, Benjamin/Cummings Pub. Co., 1981, part II, section 12, σελ. 63-69.) Επίσης, η αβελιανοποίηση G^{ab} *οιασδήποτε* ομάδας G είναι ισόμορφη με την πρώτη ομάδα ομολογίας $H_1(G;\mathbb{Z})$ τής ιδίας τής G. (Βλ., π.χ., K.S. Brown: *Cohomology of Groups*, GTM, Vol. **87**, Springer-Verlag, 1982, Ch. II, section 3, σελ. 36.)

(iv) Λαμβάνοντας υπ' όψιν τον μέχρις ισομορφισμού υπολογισμό τής μεταθέτριας υποομάδας $\mathfrak{A}'_n$ τής $\mathfrak{A}_n$ (βλ. 5.5.14), συμπεραίνουμε ότι

$$\boxed{\mathfrak{A}_n^{\mathrm{ab}} \cong \begin{cases} \mathbb{Z}_3, & \text{όταν } n \in \{3,4\}, \\ \{\mathrm{id}\}, & \text{όταν } n \geq 5. \end{cases}}$$

(v) Βάσει των προαναφερθέντων στα εδάφια 4.5.3 (vi) και 5.5.16, για κάθε σώμα F και για κάθε φυσικό αριθμό $n \geq 2$ έχουμε

$$\boxed{\mathrm{GL}_n(F)^{\mathrm{ab}} \cong \begin{cases} F^\times \,(= F\setminus\{0_F\}), & \text{όταν } (n, \chi\alpha\rho(F)) \neq (2,2), \\ \mathbb{Z}_2, & \text{όταν } n = 2 \text{ και } F \cong \mathbb{Z}_2, \end{cases}}$$

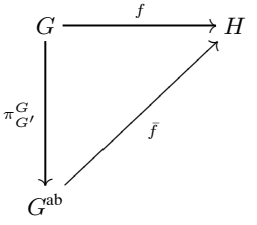
και

$$\boxed{\mathrm{SL}_n(F)^{\mathrm{ab}} \cong \begin{cases} \{\mathbf{I}_n\}, & \text{όταν } (n, \chi\alpha\rho(F)) \notin \{(2,2),(2,3)\}, \\ \mathbb{Z}_2, & \text{όταν } n = 2 \text{ και } F \cong \mathbb{Z}_2, \\ \mathbb{Z}_3, & \text{όταν } n = 2 \text{ και } F \cong \mathbb{Z}_3. \end{cases}}$$

5.5.27 Σημείωση. (i) Εάν η G είναι πεπερασμένως παραγόμενη, τότε και η G^{ab} είναι πεπερασμένως παραγόμενη (βλ. 4.4.18).

(ii) Εάν η G^{ab} είναι άπειρη, τότε και η G είναι άπειρη. Ωστόσο, το αντίστροφο δεν ισχύει: Υπάρχουν ομάδες άπειρης τάξεως έχουσες πεπερασμένες αβελιανοποιήσεις, όπως π.χ. η $\mathrm{SL}_2(\mathbb{C})$ με $\mathrm{SL}_2(\mathbb{C})^{\mathrm{ab}} = \{\mathbf{I}_2\}$ (βλ. 5.5.26 (v)). Προτείνεται ως άσκηση η απόδειξη τού ότι για την άπειρη διεδρική ομάδα $\mathbf{D}_\infty := \langle S, T_{-1}\rangle$ (βλ. εδάφια 3.4.14 και 3.4.15) ισχύει $\mathbf{D}'_\infty = \langle T_{-1}^2\rangle$ και $\mathbf{D}_\infty^{\mathrm{ab}} \cong \mathbf{V}$.

5.5.28 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω $\pi^G_{G'} : G \to G^{\mathrm{ab}}$ ο φυσικός επιμορφισμός. Τότε για κάθε ομομορφισμό ομάδων $f : (G,\cdot) \longrightarrow (H,*)$ που έχει ως εικόνα του μια αβελιανή υποομάδα τής H υφίσταται ένας και μόνον ομομορφισμός $\bar{f} : G^{\mathrm{ab}} \longrightarrow H$, τέτοιος ώστε να ισχύει $f = \bar{f} \circ \pi^G_{G'}$, δηλαδή τέτοιος ώστε το διάγραμμα*



να καθίσταται μεταθετικό.

ΑΠΟΔΕΙΞΗ. Για κάθε ζεύγος $(x,y) \in G \times G$ έχουμε $f([x,y]) = [f(x), f(y)]$. Εξ υποθέσεως, η $\mathrm{Im}(f)$ είναι αβελιανή, πράγμα που σημαίνει ότι

$$\begin{aligned} f([x,y]) &= f(x) * f(y) * f(x)^{-1} * f(y)^{-1} \\ &= f(x) * f(x)^{-1} * f(y) * f(y)^{-1} = e_H, \end{aligned}$$

οπότε $G' \subseteq \mathrm{Ker}(f)$. Αρκεί λοιπόν να εφαρμοσθεί το θεμελιώδες θεώρημα 4.5.1 περί πηλικοομάδων. □

5.5.29 Ορισμός. Έστω $(G,\cdot)$ μια ομάδα. Εάν $H \sqsubseteq G$ και $K \sqsubseteq G$, τότε η υποομάδα

$$\boxed{[H,K] := \langle \{[x,y] \mid (x,y) \in H \times K\} \rangle \sqsubseteq G}$$

καλείται **μεταθέτης των υποομάδων** H **και** K. Προφανώς,

$$\boxed{G' = [G,G]\,.}$$

5.5.30 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Εάν $H \sqsubseteq G$ και $K \sqsubseteq G$, τότε ισχύουν τα ακόλουθα*:

(i) $[H,K] = [K,H]$.

(ii) $[H,K] \sqsubseteq \mathrm{NCL}_G(H) \cap \mathrm{NCL}_G(K)$ (βλ. 4.2.10).

(iii) $[H,K] \trianglelefteq \langle H,K\rangle$, $H\,[H,K] \trianglelefteq \langle H,K\rangle$ *και* $K\,[H,K] \trianglelefteq \langle H,K\rangle$.

(iv) $(H\,[H,K]) \cdot (K\,[H,K]) = \langle H,K\rangle$.

(v) *Εάν* $H \trianglelefteq G$, *τότε* $[H,K] \sqsubseteq H$.

(vi) *Εάν* $H \trianglelefteq G$ *και* $K \trianglelefteq G$, *τότε* $[H,K] \sqsubseteq H \cap K$ *και* $[H,K] \trianglelefteq G$.

(vii) *Εάν* $K \trianglelefteq H$ *και* $H \trianglelefteq G$, *τότε* $H/K \sqsubseteq Z(G/K) \Longleftrightarrow [H,G] \sqsubseteq K$.

ΑΠΟΔΕΙΞΗ. (i) Εάν $(x,y) \in H \times K$, τότε $[x,y]^{-1} = [y,x]$ (βλ. 5.5.2 (i)). Επειδή $[H,K] \sqsubseteq G$ και $[K,H] \sqsubseteq G$, έχουμε προφανώς $[H,K] = [K,H]$.

(ii) Έστω τυχόν $(x,y) \in H \times K$. Τότε

$$\left.\begin{array}{c} xyx^{-1} \in \mathrm{NCL}_G(K) \\ y^{-1} \in K \sqsubseteq \mathrm{NCL}_G(K) \end{array}\right\} \Rightarrow [x,y] = \left(xyx^{-1}\right) y^{-1} \in \mathrm{NCL}_G(K).$$

Παρομοίως δείχνουμε ότι $[x,y] \in \mathrm{NCL}_G(H)$. Κατά συνέπειαν,

$$[x,y] \in \mathrm{NCL}_G(H) \cap \mathrm{NCL}_G(K),$$

απ' όπου έπεται ότι $[H,K] \sqsubseteq \mathrm{NCL}_G(H) \cap \mathrm{NCL}_G(K)$.

(iii) Προφανώς, $[H,K] \sqsubseteq \langle H,K\rangle$. Θεωρούμε τυχόντα στοιχεία $x,y \in H$ και $z \in K$. Τα $[xy,z]$ και $[x,z]$ ανήκουν στον μεταθέτη $[H,K]$. Κατά το 5.5.2 (iv),

$$[xy,z] = (x\,[y,z]\,x^{-1})\,[x,z] \Rightarrow x\,[y,z]\,x^{-1} = [xy,z]\,[x,z]^{-1} \in [H,K]\,. \tag{5.62}$$

Από την άλλη μεριά, εάν $x \in H$ και $y,z \in K$, έχουμε $[x,yz]\,,[x,y] \in [H,K]$. Κατά το 5.5.2 (iii),

$$[x,yz] = [x,y]\,(y\,[x,z]\,y^{-1}) \Rightarrow y\,[x,z]\,y^{-1} = [x,y]^{-1}\,[x,yz] \in [H,K]\,. \tag{5.63}$$

Από τις (5.62) και (5.63) έπεται ότι $g\,[a,b]\,g^{-1} \in [H,K]$ για κάθε $(a,b) \in H \times K$ και κάθε $g \in \langle H,K\rangle$, οπότε $[H,K] \trianglelefteq \langle H,K\rangle$. Το ότι $H\,[H,K] \trianglelefteq \langle H,K\rangle$ και $K\,[H,K] \trianglelefteq \langle H,K\rangle$ αποδεικνύεται παρομοίως.

(iv) Τούτο αποδεικνύεται όπως το (iii).

(v) Έστω τυχόν $(x,y) \in H \times K$. Τότε

$$\left.\begin{array}{c} yx^{-1}y^{-1} \in \mathrm{NCL}_G(H) \\ x \in H \sqsubseteq \mathrm{NCL}_G(H) \end{array}\right\} \Rightarrow [x,y] = x\left(yx^{-1}y^{-1}\right) \in \mathrm{NCL}_G(H).$$

Άρα $[H,K] \sqsubseteq \mathrm{NCL}_G(H)$. Επειδή $H \trianglelefteq G$, έχουμε $H = \mathrm{NCL}_G(H)$. Ως εκ τούτου, $[H,K] \sqsubseteq H$.

(vi) Κατόπιν εφαρμογής το (v) λαμβάνουμε $[H,K] \sqsubseteq H$ και $[H,K] \sqsubseteq K$, οπότε

$$[H,K] = [H,K] \cap [H,K] \subseteq H \cap K \underset{2.1.20}{\Longrightarrow} [H,K] \sqsubseteq H \cap K.$$

Εν συνεχεία, θεωρούμε τυχόντα στοιχεία $x \in H$, $y \in K$ και $g \in G$. Προφανώς,

$$\left.\begin{array}{c} H \trianglelefteq G \Rightarrow gxg^{-1} \in H \\ K \trianglelefteq G \Rightarrow gyg^{-1} \in K \end{array}\right\} \Rightarrow g\,[x,y]\,g^{-1} = \left[gxg^{-1}, gyg^{-1}\right] \in [H,K]\,,$$

οπότε $[H,K] \trianglelefteq G$.

(vii) Εάν $H/K \sqsubseteq Z(G/K)$, τότε κάθε στοιχείο hK της H/K ($h \in H$) μετατίθεται αμοιβαίως με κάθε στοιχείο gK της G/K ($g \in G$). Επομένως,

$$(hK)\,(gK) = (gK)\,(hK) \underset{K \trianglelefteq G}{\Longrightarrow} (hg)\,K = (gh)\,K \Rightarrow K\,(hg) = K\,(gh)$$

$$\Rightarrow hg\,(gh)^{-1} = hgh^{-1}g^{-1} = [h,g] \in K,$$

οπότε $[H,G] \sqsubseteq K$. Και αντιστρόφως· εάν $[H,G] \sqsubseteq K$, τότε για κάθε $h \in H$ και $g \in G$ έχουμε

$$hg\,(gh)^{-1} = hgh^{-1}g^{-1} = [h,g] \in K,$$

ή, ισοδυνάμως, $K\,(hg) = K\,(gh) \Rightarrow (hg)\,K = (gh)\,K \Rightarrow (hK)\,(gK) = (gK)\,(hK)$, οπότε κάθε στοιχείο τής H/K μετατίθεται αμοιβαίως με κάθε στοιχείο τής G/K. Άρα $H/K \sqsubseteq Z(G/K)$. □

5.5.31 Πρόταση. («Λήμμα των τριών μεταθετών») *Έστω $(G,\cdot)$ μια ομάδα. Εάν οι H, K και L είναι τρεις ορθόθετες υποομάδες της, τότε ισχύουν τα ακόλουθα*:

(i) $[H,KL] = [H,K]\,[H,L]$.

(ii) $[[H,K],L] \sqsubseteq [[H,L],K]\,[H,[K,L]]$.

ΑΠΟΔΕΙΞΗ. (i) Επειδή οι H, K και L είναι ορθόθετες υποομάδες τής G, από το (vi) τής προτάσεως 5.5.30 έπεται ότι $[H,K] \trianglelefteq G$ και $[H,L] \trianglelefteq G$. Θεωρούμε τυχόντα στοιχεία $x \in H$, $y \in K$ και $z \in L$. Επειδή $[H,L] \trianglelefteq G$, έχουμε (λόγω τού 5.5.2 (iii))

$$\left.\begin{array}{c} y\,[x,z]\,y^{-1} \in [H,L] \\ [x,yz] = [x,y]\,(y\,[x,z]\,y^{-1}) \in [H,K]\,[H,L] \end{array}\right\} \Rightarrow [x,yz] \in [H,K]\,[H,L]\,,$$

οπότε $[H,KL] \subseteq [H,K]\,[H,L] \sqsubseteq G \underset{2.1.20}{\Longrightarrow} [H,KL] \sqsubseteq [H,K]\,[H,L]$. Από την άλλη μεριά,

$$\left.\begin{array}{c} K \sqsubseteq KL \Rightarrow [H,K] \sqsubseteq [H,KL] \\ L \sqsubseteq KL \Rightarrow [H,L] \sqsubseteq [H,KL] \end{array}\right\} \Rightarrow [H,K]\,[H,L] \sqsubseteq [H,KL]\,.$$

Κατά συνέπειαν, $[H, KL] = [H, K]\,[H, L]$.
(ii) Κατά το 5.5.30 (vi),

$$[H,[K,L]] \trianglelefteq G,\ \ [H,[L,K]] \trianglelefteq G,\ \ [H,[K,L]] \trianglelefteq G.$$

Θεωρούμε τυχόντα στοιχεία $x \in H$, $y \in K$ και $z \in L$. Μέσω τής ταυτότητας (5.42) τού Witt (βλ. 5.5.2 (viii)) λαμβάνουμε

$$\left(x\left[z,\left[x^{-1},y\right]\right]x^{-1}\right) = \left(z\left[y,\left[z^{-1},x\right]\right]z^{-1}\right)^{-1}\left(y\left[x,\left[y^{-1},z\right]\right]y^{-1}\right)^{-1}.$$

Επειδή

$$\left[y,\left[z^{-1},x\right]\right] \in [K,[L,H]] = [[H,L],K] \Rightarrow \left(z\left[y,\left[z^{-1},x\right]\right]z^{-1}\right)^{-1} \in [K,[L,H]],$$

$$\left[x,\left[y^{-1},z\right]\right] \in [H,[K,L]] \Rightarrow \left(y\left[x,\left[y^{-1},z\right]\right]y^{-1}\right)^{-1} \in [H,[K,L]],$$

έχουμε

$$x\left[\left[x^{-1},y\right],z\right]^{-1}x^{-1} = x\left[z,\left[x^{-1},y\right]\right]x^{-1} \in [K,[L,H]]\,[H,[K,L]],$$

οπότε $[[H,K],L] \sqsubseteq [[H,L],K]\,[H,[K,L]]$. □

5.6 ΕΞΙΣΩΣΗ ΚΛΑΣΕΩΝ ΣΥΖΥΓΙΑΣ

Έστω $(G,\cdot)$ μια μη αβελιανή πεπερασμένη ομάδα. Πώς σχετίζεται η τάξη $|G|$ τής G με την τάξη $|Z(G)|$ τού κέντρου της; Η απάντηση δίδεται στην ακόλουθη:

5.6.1 Πρόταση. (Εξίσωση κλάσεων συζυγίας) *Έστω $(G,\cdot)$ μια μη αβελιανή πεπερασμένη ομάδα. Εάν τα $x_1,...,x_m$ είναι εκπρόσωποι εκείνων των σαφώς διακεκριμένων κλάσεων συζυγίας που δεν περιέχονται στο κέντρο $Z(G)$ τής G, τότε η τάξη $|G|$ τής G ικανοποιεί την εξίσωση*

$$\boxed{|G| = |Z(G)| + \sum_{j=1}^{m} |G : \mathrm{C}_G(x_j)|\,.} \tag{5.64}$$

ΑΠΟΔΕΙΞΗ. Εάν $Z(G) = \{e_G = z_1, z_2, ..., z_k\}$ και εάν οι $\mathcal{C}_1,...,\mathcal{C}_m$ είναι οι σαφώς διακεκριμένες κλάσεις συζυγίας που δεν περιέχονται στο $Z(G)$ με $x_j \in \mathcal{C}_j$ για κάθε $j \in \{1,...,m\}$, τότε το $\Xi := \{e_G = z_1, z_2, ..., z_k, x_1,...,x_m\}$ αποτελεί ένα πλήρες σύστημα εκπροσώπων τής G ως προς την "$\underset{\text{συζ.}}{\sim}$". Επομένως, $\mathcal{C}_j = \text{ΚΛΣ}_G(x_j)$ για κάθε $j \in \{1,...,m\}$ και

$$G = \left(\coprod_{\varrho=1}^{k}\{z_\varrho\}\right)\coprod\left(\coprod_{j=1}^{m}\text{ΚΛΣ}_G(x_j)\right) \Rightarrow |G| = k + \sum_{j=1}^{m}\text{card}(\mathcal{C}_j).$$

Η (5.64) έπεται θέτοντας $|Z(G)| = k$ και $\text{card}(\mathcal{C}_j) = |G : \mathrm{C}_G(x_j)|$ για κάθε δείκτη $j \in \{1,...,m\}$ επί τη βάσει τού πορίσματος 5.2.10. □

5.6.2 Παραδείγματα. (i) Επειδή η ομάδα $\mathbf{Q}$ των τετρανίων έχει ως κέντρο της το $Z(\mathbf{Q}) = \{\mathbf{I}_2, -\mathbf{I}_2\}$ και ως κλάσεις συζυγίας της τα

$$\{\mathbf{I}_2\},\ \{-\mathbf{I}_2\},\ \{\mathbf{i}, -\mathbf{i}\},\ \{\mathbf{j}, -\mathbf{j}\},\ \{\mathbf{k}, -\mathbf{k}\}$$

(βλ. 5.4.7 και 5.2.12), η εξίσωση κλάσεων συζυγίας (5.64) ως προς το πλήρες σύστημα εκπροσώπων $\Xi := \{\mathbf{I}_2, -\mathbf{I}_2, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ τής $\mathbf{Q}$ ως προς την "$\underset{\text{συζ.}}{\sim}$" δίδει

$$\begin{aligned} 8 &= |\mathbf{Q}| = |Z(\mathbf{Q})| + |\mathbf{Q} : \mathrm{C}_{\mathbf{Q}}(\mathbf{i})| + |\mathbf{Q} : \mathrm{C}_{\mathbf{Q}}(\mathbf{j})| + |\mathbf{Q} : \mathrm{C}_{\mathbf{Q}}(\mathbf{k})| \\ &= 2 + 2 + 2 + 2, \end{aligned}$$

διότι $\mathrm{C}_{\mathbf{Q}}(\mathbf{i}) = \langle \mathbf{i} \rangle$, $\mathrm{C}_{\mathbf{Q}}(\mathbf{j}) = \langle \mathbf{j} \rangle$ και $\mathrm{C}_{\mathbf{Q}}(\mathbf{k}) = \langle \mathbf{k} \rangle$.
(ii) Επειδή η διεδρική ομάδα $\mathbf{D}_4$ έχει ως κέντρο της το $Z(\mathbf{D}_4) = \{\mathrm{id}_{\mathcal{E}_4}, \beta^2\}$ και ως κλάσεις συζυγίας της τα

$$\{\mathrm{id}_{\mathcal{E}_4}\},\ \{\beta, \beta^3\},\ \{\beta^2\},\ \left\{\alpha, \alpha \circ \beta^2\right\},\ \{\alpha \circ \beta, \alpha \circ \beta^3\}$$

(βλ. 5.4.8 και 5.1.12), η εξίσωση κλάσεων συζυγίας (5.64) για την $\mathbf{D}_4$ ως προς το πλήρες σύστημα εκπροσώπων $\Xi := \{\mathrm{id}_{\mathcal{E}_4}, \beta, \beta^2, \alpha, \alpha \circ \beta\}$ δίδει

$$\begin{aligned} 8 &= |\mathbf{D}_4| = |Z(\mathbf{D}_4)| + |\mathbf{D}_4 : \mathrm{C}_{\mathbf{D}_4}(\beta)| + |\mathbf{D}_4 : \mathrm{C}_{\mathbf{D}_4}(\alpha)| + |\mathbf{D}_4 : \mathrm{C}_{\mathbf{D}_4}(\alpha \circ \beta)| \\ &= 2 + 2 + 2 + 2, \end{aligned}$$

διότι $\mathrm{C}_{\mathbf{D}_4}(\beta) = \langle \beta \rangle$, $\mathrm{C}_{\mathbf{D}_4}(\alpha) = \left\langle \alpha, \beta^2 \right\rangle$ και $\mathrm{C}_{\mathbf{D}_4}(\alpha \circ \beta) = \left\langle \alpha \circ \beta, \beta^2 \right\rangle$.
(iii) Επειδή η εναλλάσσουσα ομάδα $\mathfrak{A}_5$ έχει ως κέντρο της το $Z(\mathfrak{A}_5) = \{\mathrm{id}\}$ και ως ένα πλήρες σύστημα εκπροσώπων της ως προς την "$\underset{\text{συζ.}}{\sim}$" το

$$\Xi := \{\mathrm{id}, [1\ 2\ 3], [1\ 2] \circ [3\ 4], [1\ 2\ 3\ 4\ 5], [1\ 2\ 3\ 5\ 4]\}$$

(βλ. 5.4.11 και 5.3.20), η εξίσωση κλάσεων συζυγίας (5.64) δίδει

$$\begin{aligned} &60 = |\mathfrak{A}_5| = |Z(\mathfrak{A}_5)| + |\mathfrak{A}_5 : \mathrm{C}_{\mathfrak{A}_5}([1\ 2\ 3])| + |\mathfrak{A}_5 : \mathrm{C}_{\mathfrak{A}_5}([1\ 2] \circ [3\ 4])| \\ &+ |\mathfrak{A}_5 : \mathrm{C}_{\mathfrak{A}_5}([1\ 2\ 3\ 4\ 5])| + |\mathfrak{A}_5 : \mathrm{C}_{\mathfrak{A}_5}([1\ 2\ 3\ 5\ 4])| = 1 + 20 + 15 + 12 + 12. \end{aligned}$$

5.6.3 Θεώρημα. *Εάν $(G, \cdot)$ είναι μια ομάδα τάξεως $|G| = p^\nu$, όπου p πρώτος αριθμός και $\nu \in \mathbb{N}$, τότε $|Z(G)| > 1$.*

ΑΠΟΔΕΙΞΗ. Εάν η $(G, \cdot)$ είναι αβελιανή, τότε $G = Z(G)$ (βλ. 5.4.2), οπότε

$$|G| = |Z(G)| = p^\nu > 1.$$

Εάν η $(G, \cdot)$ δεν είναι αβελιανή, τότε, θεωρώντας εκπροσώπους $x_1, ..., x_m$ εκείνων των σαφώς διακεκριμένων κλάσεων συζυγίας που δεν περιέχονται στο κέντρο $Z(G)$ τής G, έχουμε (εκ κατασκευής) $|G : \mathrm{C}_G(x_j)| > 1$ για κάθε $j \in \{1, ..., m\}$ και η (5.64) γράφεται ως εξής:

$$p^\nu = |Z(G)| + \sum_{j=1}^{m} |G : \mathrm{C}_G(x_j)|.$$

Κατά το θεώρημα 4.1.22 τού Lagrange, $|G : \mathrm{C}_G(x_j)| \mid p^\nu$ για κάθε $j \in \{1, ..., m\}$, οπότε $\exists \xi_j \in \{1, ..., \nu\} : |G : \mathrm{C}_G(x_j)| = p^{\xi_j}$, $\forall j \in \{1, ..., m\}$ (βλ. λήμμα Β.3.14). Επομένως,

$$|Z(G)| = p\left(p^{\nu-1} - \sum_{j=1}^{m} p^{\xi_j - 1}\right),$$

απ' όπου έπεται ότι $p \mid |Z(G)| \Rightarrow 1 < p \leq |Z(G)|$. □

5.6.4 Σημείωση. Το κέντρο $Z(G)$ τής G οφείλει (λόγω τού θεωρήματος 4.1.22 τού Lagrange και τού λήμματος Β.3.14) να έχει τάξη $|Z(G)| = p^\kappa$, όπου $\kappa \in \{1, ..., \nu\}$ (με $\kappa = \nu$ εάν και μόνον εάν η G είναι αβελιανή).

5.6.5 Πόρισμα. *Εάν $(G, \cdot)$ είναι μια ομάδα τάξεως $|G| = p^\nu$, όπου p πρώτος αριθμός και $\nu \in \mathbb{N}$, τότε $\exists K \trianglelefteq G : |K| = p$.*

ΑΠΟΔΕΙΞΗ. Σύμφωνα με τα όσα προαναφέρθησαν στο εδάφιο 5.6.4, έχουμε $|Z(G)| = p^\kappa$, για κάποιον $\kappa \in \{1, ..., \nu\}$. Επιλέγουμε τυχόν $g \in Z(G) \setminus \{e_G\}$. Η τάξη τού g εντός τής ομάδας $Z(G)$ ισούται με p^λ, όπου λ κάποιος θετικός ακέραιος διαιρέτης τού κ (βλ. 4.1.27). Επειδή $(g^{p^{\lambda-1}})^p = e_{Z(G)} = e_G$, η τάξη τού στοιχείου $g^{p^{\lambda-1}}$ εντός τής ομάδας $Z(G)$ είναι $\leq p$ και, μάλιστα, *ίση* με το p (διότι $\left|\left\langle g^{p^{\lambda-1}}\right\rangle\right| \mid p^\lambda$ και δεν υφίσταται θετικός ακέραιος διαιρέτης τού p^λ που να είναι μικρότερος τού p και μεγαλύτερος τού 1). Επομένως η $K := \left\langle g^{p^{\lambda-1}}\right\rangle$ έχει τάξη p και $K \sqsubseteq Z(G) \underset{5.4.19\,(i)}{\Longrightarrow} K \trianglelefteq G$. □

5.6.6 Πόρισμα. *Εάν $(G, \cdot)$ είναι μια ομάδα τάξεως $|G| = p^\nu$, όπου p πρώτος αριθμός και $\nu \in \mathbb{N}$, τότε για κάθε $j \in \{0, 1, ..., \nu\}$ υφίσταται μία (τουλάχιστον) ορθόθετη υποομάδα τής G τάξεως p^j.*

ΑΠΟΔΕΙΞΗ. Χρησιμοποιούμε μαθηματική επαγωγή ως προς τον ν. Για $\nu = 1$ ο ισχυρισμός είναι προδήλως αληθής. Για $\nu \geq 2$ υποθέτουμε ότι αυτός είναι αληθής για όλες τις ομάδες τάξεως $p^{\nu-1}$ και θεωρούμε τυχούσα ομάδα G τάξεως p^ν. Σύμφωνα με το πόρισμα 5.6.5, $\exists K \trianglelefteq G : |K| = p$. Επειδή $|G/K| = p^{\nu-1}$, η πηλικο-ομάδα G/K διαθέτει (λόγω τής επαγωγικής υποθέσεώς μας) ορθόθετες υποομάδες H_j τάξεως p^j για κάθε $j \in \{0, 1, ..., \nu-1\}$. Οι αντίστροφες εικόνες αυτών μέσω τού φυσικού επιμορφισμού $\pi_K^G : G \longrightarrow G/K$ είναι ορθόθετες υποομάδες τής G τάξεως

$$\left|(\pi_K^G)^{-1}(H_j)\right| = \left|\mathrm{Ker}(\pi_K^G)\right| \cdot |H_j| = |K| \cdot |H_j| = p \cdot p^j = p^{j+1}$$

για κάθε $j \in \{0, 1, ..., \nu-1\}$. (Βλ. 4.2.30 (ii) και 4.1.13 (ii). Φυσικά, *και* η τετριμμένη υποομάδα τής G συγκαταλέγεται στις ορθόθετες υποομάδες της. Βλ. 4.2.5.) Άρα ο ισχυρισμός είναι αληθής *και* για ομάδες τάξεως p^ν. □

5.6.7 Πόρισμα. *Κάθε ομάδα τάξεως p^2, όπου p πρώτος αριθμός, είναι αβελιανή.*

ΑΠΟΔΕΙΞΗ. Έστω $(G,\cdot)$ μια ομάδα τάξεως $|G|=p^2$. Βάσει των προαναφερθέντων στο εδάφιο 5.6.4, $|Z(G)|\in\{p,p^2\}$. Εάν ίσχυε $|Z(G)|=p$, τότε θα είχαμε $|G/Z(G)|=p$ (βλ. 4.4.2 (iii)), οπότε η πηλικοομάδα $G/Z(G)$ θα ήταν κυκλική (δυνάμει τού πορίσματος 4.1.33), κάτι που (λόγω τής προτάσεως 5.4.17) θα σήμαινε ότι $G=Z(G)$ με $|Z(G)|=p<|G|$. Άτοπο! Άρα τελικώς $|Z(G)|=p^2$, απ' όπου έπεται ότι $Z(G)=G$, ήτοι ότι η G είναι όντως αβελιανή. □

5.6.8 Πόρισμα. *Έστω $(G,\cdot)$ μια μη αβελιανή ομάδα τάξεως p^3, όπου p πρώτος αριθμός. Τότε $|Z(G)|=p$ και $G'=Z(G)$.*

ΑΠΟΔΕΙΞΗ. Σύμφωνα με τα προαναφερθέντα στο εδάφιο 5.6.4, $|Z(G)|\in\{p,p^2\}$. Εάν ίσχυε $|Z(G)|=p^2$, τότε θα είχαμε $|G/Z(G)|=p$ (βλ. 4.4.2 (iii)), οπότε η πηλικοομάδα $G/Z(G)$ θα ήταν κυκλική (δυνάμει τού πορίσματος 4.1.33), κάτι που (λόγω τής προτάσεως 5.4.17) θα σήμαινε ότι $G=Z(G)$, ήτοι ότι η G είναι αβελιανή. Άτοπο! Κατά συνέπειαν, $|Z(G)|=p$ και $|G/Z(G)|=p^2$. Από την τελευταία ισότητα και από το πόρισμα 5.6.7 (εφαρμοζόμενο για την πηλικοομάδα $G/Z(G)$) έπεται ότι η $G/Z(G)$ είναι αβελιανή. Κατά την πρόταση 5.5.11, $G'\sqsubseteq Z(G)$. Επειδή $|Z(G)|=p$, το θεώρημα 4.1.22 τού Lagrange μας πληροφορεί ότι $|G'|\in\{1,p\}$. Η ισότητα $|G'|=1$ θα οδηγούσε σε αντίφαση (μέσω τής προτάσεως 5.5.6, αφού η G είναι μη αβελιανή). Άρα τελικώς $|G'|=p=|Z(G)|\Rightarrow G'=Z(G)$. □

Εν συνεχεία, μέσω τής εξισώσεως κλάσεων συζυγίας (5.64) και ενός χρήσιμου λήμματος αποδειχθέντος το έτος[56] 1903 από τον E. Landau (1877-1938) θα δείξουμε ότι ο πληθικός αριθμός τού συνόλου των κλάσεων ισομορφίας των πεπερασμένων ομάδων, καθεμιά των οποίων έχει ακριβώς $\ell\in\mathbb{N}$ κλάσεις συζυγίας, είναι *πεπερασμένος* (βλ. θεώρημα 5.6.15).

5.6.9 Λήμμα. (E. Landau, 1903) *Εάν $n,\ell\in\mathbb{N}$ και*

$$\mathcal{B}(n;\ell):=\left\{(\lambda_1,...,\lambda_\ell)\in\mathbb{N}^\ell\;\middle|\;\lambda_1\geq...\geq\lambda_\ell\ \text{ και }\ \sum_{j=1}^{\ell}\frac{1}{\lambda_j}=n\right\},$$

τότε

$$\boxed{\text{card}(\mathcal{B}(n;\ell))<\infty.}$$

ΑΠΟΔΕΙΞΗ. Θα χρησιμοποιήσουμε μαθηματική επαγωγή ως προς τον ℓ. Για $\ell=1$ ο ισχυρισμός είναι αληθής (αφού $\mathcal{B}(1;1)=\{1\}$ και $\mathcal{B}(n;1)=\varnothing$ για $n\geq 2$). Υποθέτουμε ότι είναι αληθής και για τον $\ell-1$, για κάποιον $\ell\geq 2$. Εάν $\mathcal{B}(n;\ell)=\varnothing$, τότε $\text{card}(\mathcal{B}(n;\ell))=0$. Εάν $\mathcal{B}(n;\ell)\neq\varnothing$, τότε θεωρούμε τυχόν στοιχείο $(\lambda_1,...,\lambda_\ell)$ τού συνόλου $\mathcal{B}(n;\ell)$ και παρατηρούμε ότι

$$n=\sum_{j=1}^{\ell}\frac{1}{\lambda_j}\leq\frac{\ell}{\lambda_\ell}\Rightarrow\lambda_\ell\leq\left\lfloor\frac{\ell}{n}\right\rfloor,$$

[56] E. Landau: *Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante,* Math. Ann., Bd. **56** (1903), 671-676.

οπότε υπάρχουν μόνον πεπερασμένου πλήθους δυνατές επιλογές τού λ_ℓ. Έστω

$$\mathcal{J}\,(n;\ell) := \left\{ (\lambda_1,...,\lambda_\ell) \in \mathbb{N}^\ell \;\middle|\; \begin{array}{c} \lambda_1 \geq ... \geq \lambda_{\ell-1},\ \lambda_\ell \leq \left\lfloor \frac{\ell}{n} \right\rfloor \\ \text{και} \quad \sum_{j=1}^{\ell-1} \frac{1}{\lambda_j} = n - \frac{1}{\lambda_\ell} \end{array} \right\}.$$

Τότε $\mathcal{B}\,(n;\ell) \subseteq \mathcal{J}\,(n;\ell)$. Επειδή για κάθε δυνατή επιλογή τού φυσικού αριθμού λ_ℓ το σύνολο $\mathcal{B}(n - \frac{1}{\lambda_\ell}; \ell - 1)$ είναι πεπερασμένο (λόγω τής επαγωγικής υποθέσεώς μας), το $\mathcal{J}\,(n;\ell)$ είναι ωσαύτως πεπερασμένο. Άρα και το ίδιο το $\mathcal{B}\,(n;\ell)$ είναι πεπερασμένο. □

5.6.10 Λήμμα. *Έστω ότι οι $(G,\cdot)$ και $(H,*)$ είναι δυο ομάδες. Τότε ισχύει η συνεπαγωγή*

$$(G,\cdot) \cong (H,*) \Longrightarrow \mathfrak{K}(G) = \mathfrak{K}(H).$$

ΑΠΟΔΕΙΞΗ. Έστω $f : G \longrightarrow H$ ένας ισομορφισμός και έστω $\Xi \subseteq G$ ένα πλήρες σύστημα εκπροσώπων τής G ως προς την "$\overset{G}{\underset{\text{συζ.}}{\sim}}$". Τότε η απεικόνιση

$$\Xi \ni x \longmapsto f(x) \in f(\Xi)$$

είναι αμφιρριπτική. Αρκεί λοιπόν να αποδείξουμε ότι η εικόνα $f(\Xi)$ τού Ξ μέσω τής f αποτελεί ένα πλήρες σύστημα εκπροσώπων τής H ως προς την "$\overset{H}{\underset{\text{συζ.}}{\sim}}$". Κατ' αρχάς, για κάθε $x \in \Xi$ έχουμε $f(\text{ΚΛΣ}_G(x)) = \text{ΚΛΣ}_H(f(x))$. Πράγματι· για οιοδήποτε $z \in \text{ΚΛΣ}_G(x)$ υπάρχει $g \in G : z = gxg^{-1}$, οπότε

$$f(z) = f(g) * f(x) * f(g)^{-1} \Rightarrow f(z) \in \text{ΚΛΣ}_H(f(x)),$$

απ' όπου έπεται ότι $f(\text{ΚΛΣ}_G(x)) \subseteq \text{ΚΛΣ}_H(f(x))$. Για την απόδειξη τής ισχύος τού αντιστρόφου εγκλεισμού θεωρούμε τυχόν στοιχείο $w \in \text{ΚΛΣ}_H(f(x))$. Εξ ορισμού,

$$\exists h \in H : w = h * f(x) * h^{-1} \Rightarrow w = f(gxg^{-1}) \in f(\text{ΚΛΣ}_G(x)),$$

όπου το $g \in G$ είναι το μοναδικό στοιχείο για το οποίο $f(g) = h$. Άρα ισχύει όντως και ο αντίστροφος εγκλεισμός $\text{ΚΛΣ}_H(f(x)) \subseteq f(\text{ΚΛΣ}_G(x))$. Επομένως,

$$\begin{aligned} H &= f(G) = f\left(\bigcup_{x\in\Xi} \text{ΚΛΣ}_G(x) \right) = \bigcup_{x\in\Xi} f(\text{ΚΛΣ}_G(x)) \\ &= \bigcup_{x\in\Xi} \text{ΚΛΣ}_H(f(x)) = \bigcup_{y\in f(\Xi)} \text{ΚΛΣ}_H(y). \end{aligned}$$

Απομένει να δειχθεί ότι η ανωτέρω ένωση είναι *αποσυνδετή*. Προς τούτο θεωρούμε στοιχεία $y_1, y_2 \in f(\Xi)$, τέτοια ώστε να ισχύει $\text{ΚΛΣ}_H(y_1) = \text{ΚΛΣ}_H(y_2)$. Επειδή υπάρχουν μονοσημάντως ορισμένα $x_1, x_2 \in \Xi$ με $f(x_1) = y_1$ και $f(x_2) = y_2$, παρατηρούμε ότι

$$f(\text{ΚΛΣ}_G(x_1)) = \text{ΚΛΣ}_H(f(x_1)) = \text{ΚΛΣ}_H(f(x_2)) = f(\text{ΚΛΣ}_G(x_2)),$$

οπότε $\text{ΚΛΣ}_G(x_1) = \text{ΚΛΣ}_G(x_2)$ (διότι η f είναι αμφιρριπτική), απ' όπου έπεται ότι $x_1 = x_2$ (διότι το Ξ είναι εξ υποθέσεως ένα πλήρες σύστημα εκπροσώπων τής G ως προς την "$\underset{\text{συζ.}}{\overset{G}{\sim}}$"). Άρα τελικώς, $y_1 = y_2$ και $H = \coprod\limits_{y \in f(\Xi)} \text{ΚΛΣ}_H(y)$. □

5.6.11 Συμβολισμός. Για οιονδήποτε $\ell \in \mathbb{N}$ θέτουμε

$$\mathbf{Gr}_{\text{συζ.}}(\ell) := (\{\text{πεπερασμένες ομάδες } G \mid \text{ℜ}(G) = \ell\}) \,/\, \cong .$$

Επειδή, βάσει τού προηγηθέντος λήμματος 5.6.10, δυο ισόμορφες πεπερασμένες ομάδες διαθέτουν το ίδιον αριθμό κλάσεων συζυγίας, το σύνολο $\mathbf{Gr}_{\text{συζ.}}(\ell)$ μπορεί να γραφεί ως ακολούθως[57]:

$$\mathbf{Gr}_{\text{συζ.}}(\ell) = \left\{ \begin{array}{l} \text{κλάσεις ισομορφίας } [G]_{\cong} \\ \text{πεπερασμένων ομάδων } G \end{array} \;\middle|\; \text{ℜ}(G) = \ell \right\}.$$

5.6.12 Λήμμα. *Έστω $\ell \in \mathbb{N}$ και έστω H μια πεπερασμένη ομάδα διαθέτουσα ℓ κλάσεις συζυγίας* (*δηλαδή* $[H]_{\cong} \in \mathbf{Gr}_{\text{συζ.}}(\ell)$). *Τότε υπάρχει κάποιος $\mathbf{c}(\ell) \in \mathbb{N}$* (*εξαρτώμενος από τον ℓ*), *ούτως ώστε να ισχύει*

$$\boxed{|G| \leq \mathbf{c}(\ell),\ \forall G \in [H]_{\cong}\,,}$$

ΑΠΟΔΕΙΞΗ. Έστω $G \in [H]_{\cong}$. Τότε η G (σύμφωνα με το λήμμα 5.6.10) διαθέτει ℓ κλάσεις συζυγίας. Έστω $Z(G) = \{e_G = z_1, z_2, ..., z_k\}$ το κέντρο τής G ($k \leq |G|$). Διακρίνουμε δύο περιπτώσεις:

Περίπτωση πρώτη. Εάν $G = Z(G)$, δηλαδή εάν η ομάδα G είναι αβελιανή, τότε έχουμε $k = |G| = \ell$ και αρκεί να θέσουμε $\mathbf{c}(\ell) := \ell$.

Περίπτωση δεύτερη. Εάν η G δεν είναι αβελιανή, τότε επιλέγουμε εκπροσώπους $x_1,...,x_m$ εκείνων των σαφώς διακεκριμένων κλάσεων συζυγίας που δεν περιέχονται στο κέντρο $Z(G)$ τής G (με $m = \ell - k \geq 1$) και μάλιστα (δίχως βλάβη τής γενικότητας, ήτοι μέχρις αναδιατάξεως των $x_1,...,x_m$) κατά τέτοιον τρόπο, ώστε

$$|\mathrm{C}_G(x_1)| \geq |\mathrm{C}_G(x_2)| \geq \cdots \geq |\mathrm{C}_G(x_m)|\,.$$

Σημειωτέον ότι $k \mid |G|$ (λόγω των 5.4.2 και 4.1.22) και ότι η εξίσωση των κλάσεων συζυγίας (5.64) γράφεται ως εξής:

$$|G| = k + \sum_{j=1}^{m} |G : \mathrm{C}_G(x_j)| = \frac{|G|}{(|G|\,/k)} + \sum_{j=1}^{m} \frac{|G|}{|\mathrm{C}_G(x_j)|}.$$

Κατόπιν διαιρέσεως αμφοτέρων των μελών διά $|G|$ λαμβάνουμε

$$\underbrace{\frac{1}{|G|} + \cdots + \frac{1}{|G|}}_{k \text{ φορές}} + \sum_{j=1}^{m} \frac{1}{|\mathrm{C}_G(x_j)|} = 1.$$

[57] Ως $[G]_{\cong}$ συμβολίζουμε την *κλάση ισομορφίας* $\{H \text{ ομάδα} \mid H \cong G\}$ (πρβλ. 2.4.22).

Από αυτήν την ισότητα έπεται ότι

$$(\underbrace{|G|,...,|G|}_{k\ \text{φορές}}, |\mathrm{C}_G(x_1)|,...,|\mathrm{C}_G(x_m)|) \in \mathcal{B}(1;\ell)\,.$$

Άρα $\mathcal{B}(1;\ell) \neq \varnothing$. Τούτο σημαίνει (λόγω τού λήμματος 5.6.9 τού Landau) ότι το $\mathcal{B}(1;\ell)$ είναι κατ' ανάγκην πεπερασμένο σύνολο. Επιλέγουμε ένα στοιχείο $(\lambda_1,...,\lambda_\ell) \in \mathcal{B}(1;\ell)$, τέτοιο ώστε ο λ_1 να είναι ο μέγιστος φυσικός αριθμός από το σύνολο των πρώτων συντεταγμένων όλων των στοιχείων τού $\mathcal{B}(1;\ell)$ και θέτουμε $\mathbf{c}(\ell) := \lambda_1$. Επειδή $k \geq 1$, έχουμε εκ κατασκευής $|G| \leq \mathbf{c}(\ell)$. □

5.6.13 Συμβολισμός. Για οιονδήποτε $n \in \mathbb{N}$ θέτουμε

$$\mathbf{Gr}_{\text{ταξ.}}(n) := (\{\text{πεπερασμένες ομάδες } G \,|\, |G| = n\}) \,/\, \cong\,.$$

Επειδή οι πληθικοί αριθμοί των υποκειμένων συνόλων δυο ισόμορφων ομάδων είναι ίσοι, το σύνολο $\mathbf{Gr}_{\text{ταξ.}}(n)$ μπορεί να γραφεί ως ακολούθως:

$$\mathbf{Gr}_{\text{ταξ.}}(n) = \left\{ \begin{array}{l} \text{κλάσεις ισομορφίας } [G]_\cong \\ \text{πεπερασμένων ομάδων } G \end{array} \;\middle|\; |G| = n \right\}.$$

5.6.14 Λήμμα. *Για κάθε $n \in \mathbb{N}$ έχουμε*

$$\boxed{\mathrm{card}(\mathbf{Gr}_{\text{ταξ.}}(n)) \leq n^{n^2} < \infty.}$$

ΑΠΟΔΕΙΞΗ. Έστω $n \in \mathbb{N}$ και έστω $(G,\cdot)$ τυχούσα ομάδα τάξεως $|G| = n$ (ήτοι $[G]_\cong \in \mathbf{Gr}_{\text{ταξ.}}(n)$). Εάν το A είναι οιοδήποτε σύνολο με $\mathrm{card}(A) = n$, τότε υφίσταται αμφίρριψη $f : G \longrightarrow A$, το δε A εφοδιαζόμενο με την εσωτερική πράξη " $\circledast$ " που ορίζεται μέσω τού τύπου

$$A \times A \longrightarrow A,\ \ (a_1,a_2) \longmapsto a_1 \circledast a_2 := f(f^{-1}(a_1)\cdot f^{-1}(a_2)),$$

καθίσταται *ομάδα* με $(A,\circledast) \cong (G,\cdot)$. Κατά συνέπειαν, ο πληθικός αριθμός $\mathrm{card}(\mathbf{Gr}_{\text{ταξ.}}(n))$ φράσσεται εκ των άνω από τον πληθικό αριθμό τού συνόλου των εσωτερικών πράξεων που μπορούν να ορισθούν επί τού A, δηλαδή

$$\mathrm{card}(\mathbf{Gr}_{\text{ταξ.}}(n)) \leq \mathrm{card}(\{\text{απεικονίσεις } A\times A \longrightarrow A\}) = \mathrm{card}(A)^{\mathrm{card}(A\times A)},$$

όπου $\mathrm{card}(A)^{\mathrm{card}(A\times A)} = n^{n^2}$ (διότι $\mathrm{card}(A\times A) = \mathrm{card}(A)^2 = n^2$). □

5.6.15 Θεώρημα. *Για κάθε $\ell \in \mathbb{N}$ έχουμε*

$$\boxed{\mathrm{card}(\mathbf{Gr}_{\text{συζ.}}(\ell)) < \infty.}$$

ΑΠΟΔΕΙΞΗ. Έστω $\ell \in \mathbb{N}$ και έστω H μια πεπερασμένη ομάδα διαθέτουσα ℓ κλάσεις συζυγίας (δηλαδή $[H]_\cong \in \mathbf{Gr}_{\text{συζ}}(\ell)$). Κατά το λήμμα 5.6.12 υπάρχει κάποιος $\mathbf{c}(\ell) \in \mathbb{N}$, τέτοιος ώστε να ισχύει

$$|G| \leq \mathbf{c}(\ell),\ \forall G \in [H]_\cong\,.$$

Ως εκ τούτου, από το λήμμα 5.6.14 έπεται ότι

$$\text{card}(\mathbf{Gr}_{\sigma\upsilon\zeta.}\,(\ell)) \leq \text{card}(\mathbf{Gr}_{\tau\alpha\xi.}\,(\mathbf{c}(\ell))) \leq \mathbf{c}(\ell)^{\mathbf{c}(\ell)^2} < \infty,$$

ήτοι ότι ο πληθικός αριθμός τού συνόλου των κλάσεων ισομορφίας των πεπερασμένων ομάδων, καθεμιά των οποίων έχει ακριβώς ℓ κλάσεις συζυγίας, είναι *πεπερασμένος*. □

5.6.16 Σημείωση. (i) Μια ομάδα G είναι αβελιανή $\Leftrightarrow \mathfrak{K}(G) = |G|$.

(ii) Εάν μια ομάδα G έχει μόνον μία κλάση συζυγίας, τότε αυτή είναι τετριμμένη, ενώ εάν έχει μόνον δύο κλάσεις συζυγίας, τότε η μία εξ αυτών θα είναι το μονοσύνολο $\{e_G\}$ και η άλλη πληθικό αριθμό $|G| - 1$. Σε αυτήν την περίπτωση, η G είναι $\cong \mathbb{Z}_2$, διότι εάν υποθέταμε ότι η G είναι μη αβελιανή, θα καταλήγαμε σε αντίφαση, καθόσον η εξίσωση κλάσεων συζυγίας

$$\frac{1}{|G|} + \frac{1}{|\mathbf{C}_G(x_1)|} = 1 \Leftrightarrow |\mathbf{C}_G(x_1)| = |G|\,(|\mathbf{C}_G(x_1)| - 1)$$

δεν θα διέθετε λύσεις $(|G|\,, |\mathbf{C}_G(x_1)|) \neq (2, 2)$.

(iii) Προτείνεται ως άσκηση η απόδειξη τού ότι κάθε ομάδα G που έχει τρεις κλάσεις συζυγίας οφείλει να είναι ισόμορφη με μία εκ των: $\mathbb{Z}_3, \mathfrak{S}_3$.

(iv) Προτείνεται ως άσκηση η απόδειξη τού ότι κάθε ομάδα G που έχει τέσσερεις κλάσεις συζυγίας οφείλει να είναι ισόμορφη με μία εκ των: $\mathbb{Z}_4, \mathbf{V}, \mathbf{D}_5, \mathfrak{A}_4$.

(v) Το πρόβλημα τού προσδιορισμού των πεπερασμένων ομάδων G με $\mathfrak{K}(G) \geq 5$ απαιτεί προκεχωρημένα τεχνικά μέσα και έχει απασχολήσει αρκετούς ερευνητές για σειρά ετών. Ορισμένα σημαντικά αποτελέσματα επ' αυτού συνοψίζονται στον κατάλογο που ακολουθεί[58]. (Εν προκειμένω, $\mathfrak{b}(G) := \text{card}(\mathbf{Min\text{-}NSubg}(G))$, ενώ στη στήλη υπό το "♯" καταχωρίζεται ο αριθμός των προσδιορισθεισών ανά δύο μη

[58] Βλ. (κατά χρονολογική σειρά) τα ακόλουθα:

- G. A. Miller: *Groups involving only a small number of sets of conjugate operators*, Arch. Math. and Phys. **17** (1910), 199-204.
- W.Burnside **[3]** (second ed., 1911), Note A, pp. 461-462.
- D.T. Sigley: *Groups involving five complete sets of non-invariant conjugate operators*, Duke Mathematical Journal **1** (1935), 477-479.
- J. Poland: *Finite groups with a given number of conjugate classes*, Canadian Journal of Math. **20** (1968), 456-464.
- E.K. Annavaddar: *Determination of the finite groups having eight conjugacy classes*, Ph.D. Thesis, Arizona State University, 1971.
- L.F. Kosvintsev: *Over the theory of groups with properties given over the centralizers of involutions*, Sverdlovsk (Ural.), Ph.D. Thesis, 1974.
- V.A. Odincov & A.I. Starostin: *Finite groups with 9 classes of conjugate elements* (Russian), Ural. Gos. Univ. Mat. Zap. 10, Issled Sovremen, Algebra **152** (1976), 114-134.
- A.G. Aleksandrov & K.A. Komissarcik: *Simple groups with a small number of conjugacy classes*, in: "Algorithmic Studies in Combinatorics" (Russian), Nauka, Moscow, 1978, pp. 162-172 & 187.
- A. Vera-Lopez & J. Vera-Lopez: *Classification of finite groups according to the number of conjugacy classes I*, Israel Journal of Mathematics **51** (1985), 305-338.
- A. Vera-Lopez & J. Vera-Lopez: *Classification of finite groups according to the number of conjugacy classes II*, Israel Journal of Mathematics **56** (1986), 188-221.

ισόμορφων ομάδων G όταν $\mathfrak{K}(G) \leq 12$.)

Προσδιορισμός πεπ. ομάδων G όταν	επιτευχθείς από τους	έτη δημοσιεύσεων	♯
$\mathfrak{K}(G) \in \{1,2,3,4,5\}$	G.A. Miller W.Burnside	1910 1911	$1,1,2,4,8$
$\mathfrak{K}(G) = 6$ (εν μέρει ελλιπής)	D.T. Sigley	1935	
$\mathfrak{K}(G) \in \{6,7\}$	J. Poland	1968	$8,12$
$\mathfrak{K}(G) = 8$	E.K. Annavaddar L.F. Kosvintsev	1971 1974	21
$\mathfrak{K}(G) = 9$	V.A. Odincov & A.I. Starostin	1976	26
$\mathfrak{K}(G) \leq 12$ και G απλή	A.G. Aleksandrov & K.A. Komissarcik	1978	
$\mathfrak{K}(G) \in \{10,11\}$	A. Vera-Lopez & J. Vera-Lopez	1985	$38,35$
$\mathfrak{K}(G) = 12$	A. Vera-Lopez & J. Vera-Lopez	1986	32
Είτε $\mathfrak{K}(G) \in \{13,...,20\}$, όπου $\mathfrak{b}(G) > \mathfrak{K}(G) - 12$, είτε $\mathfrak{K}(G) = n \geq 21$, όπου $\mathfrak{b}(G) = n - m$ και $m \in \{1,...,11\}$.	A. Vera-Lopez & J. Vera-Lopez	1986	

(vi) Εάν G είναι μια πεπερασμένη ομάδα με $|G| \geq 4$, τότε (όπως απεδείχθη το 2011 από τον T.M. Keller[59]) υπάρχει μια (προσδιορίσιμη) σταθερά $c > 0$, τέτοια ώστε να ισχύει

$$\boxed{\mathfrak{K}(G) \geq c\,\frac{\log_2(|G|)}{\left(\log_2\log_2(|G|)\right)^7}.}$$

Από την άλλη μεριά, υπάρχουν και *άπειρες* ομάδες έχουσες *πεπερασμένο* πλήθος κλάσεων συζυγίας, όπως δείχνει το κάτωθι θεώρημα[60] 5.6.17.

5.6.17 Θεώρημα. (G. Higman, B.H. Neumann, H. Neumann, 1949)
Εάν G είναι μια ομάδα είτε πεπερασμένη είτε άπειρη αριθμήσιμη, τότε η G είναι εμφυτεύσιμη σε μια άπειρη αριθμήσιμη (αλλά μη πεπερασμένως παραγόμενη) ομάδα $\widetilde{G}$, ούτως ώστε οιαδήποτε δύο στοιχεία τής $\widetilde{G}$ έχοντα ίσες τάξεις να ανήκουν στην ίδια κλάση συζυγίας (εντός τής $\widetilde{G}$) και να ισχύει

$$\{m \in \mathbb{N} |\, \exists x \in G : \mathrm{ord}(x) = m\} = \left\{ l \in \mathbb{N} |\, \exists y \in \widetilde{G} : \mathrm{ord}(y) = l \right\}.$$

[59] Βλ. T.M. Keller: *Finite groups have even more conjugacy classes*, Israel Journal of Mathematics **181** (2011), 433-444.

[60] Βλ. G. Higman, B.H. Neumann, H. Neumann, *Embedding theorems for groups*, Journal of London Mathematical Society **24** (1949), 247-254.

5.6.18 Παράδειγμα. Εάν $n \in \mathbb{N}, n \geq 3$, και $G := \mathbb{Z}_{2^{n-2}}$, τότε

$$\text{card}(\{\, m \in \mathbb{N} |\, \exists x \in G :\ \text{ord}(x) = m\}) = n - 1.$$

Η G εμφυτεύεται εντός μιας άπειρης αριθμήσιμης (μη πεπερασμένως παραγόμενης) ομάδας $\widetilde{G}$. Επειδή η $\widetilde{G}$ περιέχει κατ' ανάγκην κάποιο στοιχείο άπειρης τάξεως, συμπεραίνουμε τελικώς ότι $\aleph(\widetilde{G}) = n$.

5.6.19 Σημείωση. (i) Μια διαφορετική μέθοδος κατασκευής άπειρων ομάδων με πεπερασμένου πλήθους κλάσεις συζυγίας οφείλεται στον S. Ivanov[61]. Συγκεκριμένα, για κάθε αρκούντως μεγάλο πρώτο αριθμό p υφίσταται πάντοτε κάποια άπειρη ομάδα με εκθέτη p έχουσα ακριβώς p κλάσεις συζυγίας.

(ii) Αξίζει, τέλος, να αναφερθεί ότι ο D.V. Osin κατόρθωσε το[62] 2010 να τροποποιήσει καταλλήλως το θεώρημα 5.6.17 κατά τέτοιον τρόπο, ώστε η κατασκευαζόμενη άπειρη αριθμήσιμη ομάδα $\widetilde{G}$ (εντός τής οποίας εμφυτεύεται η G) να είναι πεπερασμένως παραγόμενη και μάλιστα παραγόμενη από *ακριβώς δύο στοιχεία*! Ιδιαιτέρως, κάθε πεπερασμένη ή άπειρη αριθμήσιμη ομάδα G χωρίς στρέψη είναι εμφυτεύσιμη σε μια άπειρη αριθμήσιμη ομάδα $\widetilde{G}$ χωρίς στρέψη, παραγόμενη από δύο στοιχεία και έχουσα ακριβώς δύο κλάσεις συζυγίας.

5.7 ΤΟ ΘΕΩΡΗΜΑ ΤΟΥ CAUCHY ΚΑΙ ΟΙ ΣΥΝΕΠΕΙΕΣ ΑΥΤΟΥ

Στο εδάφιο 4.4.21 αποδείξαμε το λεγόμενο *θεώρημα τού Cauchy* μόνον για *αβελιανές* πεπερασμένες ομάδες. Η εξίσωση κλάσεων συζυγίας (5.64) μας επιτρέπει να επεκτείνουμε την απόδειξή του και για *μη αβελιανές* πεπερασμένες ομάδες.

5.7.1 Θεώρημα. (Θεώρημα τού Cauchy, 1845) *Έστω $(G, \cdot)$ μια πεπερασμένη ομάδα. Εάν $p \mid |G|$, όπου p κάποιος πρώτος αριθμός, τότε*

$$\exists g \in G \setminus \{e_G\} : \text{ord}(g) = p,$$

ήτοι η $\langle g \rangle$ είναι μια υποομάδα τής G τάξεως p (βλ. (2.9)).

ΑΠΟΔΕΙΞΗ. Εάν η G είναι αβελιανή, τότε ο ισχυρισμός είναι αληθής (βλ. 4.4.21). Ας υποθέσουμε ότι η G είναι μη αβελιανή και τα $x_1,...,x_m$ είναι εκπρόσωποι εκείνων των σαφώς διακεκριμένων κλάσεων συζυγίας που δεν περιέχονται στο κέντρο $Z(G)$. Τότε η (5.64) γράφεται ως εξής:

$$|G| = |Z(G)| + \sum_{j=1}^{m} |G : \mathrm{C}_G(x_j)| = |Z(G)| + \sum_{j=1}^{m} \frac{|G|}{|\mathrm{C}_G(x_j)|}.$$

[61] Βλ. **[132]**, Thm. 41.2, p. 471.

[62] D.V. Osin: *Small cancellations over relatively hyperbolic groups and embedding theorems*, Annals of Mathematics **172** (2010), 1-39.

Διακρίνουμε δύο περιπτώσεις: *Περίπτωση πρώτη*. Εάν

$$p \mid |G : \mathrm{C}_G(x_j)|\,, \ \ \forall j \in \{1,...,m\}, \tag{5.65}$$

τότε $p \mid |Z(G)|$ (διότι εξ υποθέσεως $p \mid |G|$). Όμως το κέντρο $Z(G)$ ως αβελιανή ομάδα περιέχει κάποιο $g \in Z(G) \setminus \{e_G\}$ τάξεως p *εντός τού* $Z(G)$ (βλ. 4.4.21). Επειδή $g \in G \setminus \{e_G\}$ και $g^p = e_G$, η τάξη τού g *εντός τής* G θα διαιρεί τον p (βλ. 2.3.8), οπότε θα πρέπει να είναι ίση με τον p (διότι ο p είναι πρώτος και $g \neq e_G$). Επομένως ο ισχυρισμός είναι αληθής.

Περίπτωση δεύτερη. Εάν

$$\exists j_0 \in \{1,...,m\} : p \nmid |G : \mathrm{C}_G(x_{j_0})|\,, \tag{5.66}$$

θα χρησιμοποιήσουμε τη δεύτερη μορφή τής μαθηματικής επαγωγής ως προς την τάξη τής G. (Η επαγωγή ξεκινά από το 6, καθώς η $\mathfrak{S}_3$ είναι η μοναδική (μέχρις ισομορφισμού) μη αβελιανή ομάδα με τη μικρότερη δυνατή τάξη, για την οποία ικανοποιείται η ανωτέρω συνθήκη (5.66). Η εξίσωση κλάσεων συζυγίας για την $\mathfrak{S}_3$ δίδει $6 = 1+2+3$. Επειδή οι 2 και 3 είναι οι μόνοι πρώτοι διαιρέτες τού 6, αρκεί η υπόμνηση τού ότι η $\mathfrak{S}_3$ διαθέτει τρία στοιχεία τάξεως 2 και δύο στοιχεία τάξεως 3. Πρβλ. 3.2.2 και 4.1.42.) Θεωρούμε οιαδήποτε μη αβελιανή ομάδα G τάξεως > 6 πληρούσα τη συνθήκη (5.66) και υποθέτουμε ότι *όλες οι μη αβελιανές ομάδες* H *με* $|H| \in \{6,...,|G|-1\}$, *οι οποίες πληρούν την* (5.66) (όταν τεθούν στη θέση τής G)*, διαθέτουν κάποιο στοιχείο τάξεως ίσης με οιονδήποτε πρώτο διαιρέτη τής* $|H|$. Σημειωτέον ότι

$$\left.\begin{aligned} |G| = |G : \mathrm{C}_G(x_{j_0})|\,|\mathrm{C}_G(x_{j_0})| \\ p \mid |G| \\ p \nmid |G : \mathrm{C}_G(x_{j_0})| \end{aligned}\right\} \Rightarrow p \mid |\mathrm{C}_G(x_{j_0})|\,.$$

Εάν *για την ίδια την* $\mathrm{C}_G(x_{j_0})$ (και τον συγκεκριμένο p) δεν ικανοποιείται η (5.66) (όταν αυτή τεθεί στη θέση τής G), τότε θα ικανοποιείται η («συμπληρωματική») συνθήκη (5.65) που περιγράφεται στην πρώτη περίπτωση, οπότε η $\mathrm{C}_G(x_{j_0})$ θα διαθέτει κάποιο στοιχείο τάξεως p. Εάν *για την ίδια την* $\mathrm{C}_G(x_{j_0})$ (και τον συγκεκριμένο p) *ικανοποιείται* η (5.66), τότε η $\mathrm{C}_G(x_{j_0})$ θα διαθέτει κάποιο στοιχείο τάξεως p *λόγω τής επαγωγικής υποθέσεως* (αφού $|\mathrm{C}_G(x_{j_0})| < |G|$). Άρα η $\mathrm{C}_G(x_{j_0})$ θα διαθέτει *ούτως ή άλλως* κάποιο στοιχείο τάξεως p. Προφανώς, αυτό το στοιχείο θα έχει τάξη p *και εντός τής* G. Άρα ο ισχυρισμός είναι και σε αυτήν την περίπτωση αληθής. □

► **Συνέπειες τού θεωρήματος τού Cauchy**. Από το θεώρημα 5.7.1 προκύπτουν σημαντικά πορίσματα για ορισμένες *ειδικές* πεπερασμένες ομάδες.

5.7.2 Ορισμός. (“p-**ομάδες**”) Έστω p ένας πρώτος αριθμός. Μια ομάδα $(G, \cdot)$ καλείται p-**ομάδα** όταν κάθε στοιχείο της έχει ως τάξη του μια (μη αρνητική ακεραία) δύναμη τού p.

5.7.3 Πόρισμα. *Έστω p ένας πρώτος αριθμός. Μια πεπερασμένη ομάδα $(G,\cdot)$ είναι p-ομάδα εάν και μόνον εάν $\exists \nu \in \mathbb{N}_0 : |G| = p^\nu$.*

ΑΠΟΔΕΙΞΗ. Εάν η G είναι μια p-ομάδα και $\nu := \max\{n \in \mathbb{N}_0 : p^n \mid |G|\}$, τότε $|G| = p^\nu m$, όπου $m \in \mathbb{N}$ με μκδ$(p,m) = 1$. Ας υποθέσουμε ότι $m > 1$. Τότε υπάρχει κάποιος πρώτος αριθμός q, $p \neq q$, με $q \mid |G|$, οπότε, σύμφωνα με το θεώρημα 5.7.1 τού Cauchy, υπάρχει κάποιο στοιχείο $g \in G\setminus\{e_G\}$, τέτοιο ώστε να ισχύει $\mathrm{ord}(g) = q$. Τούτο αντιφάσκει προς το ότι η G υπετέθη ότι είναι μια p-ομάδα. Κατά συνέπειαν, $m = 1$ και $|G| = p^\nu$. Και αντιστρόφως· εάν $\exists \nu \in \mathbb{N}_0 : |G| = p^\nu$, τότε, θεωρώντας τυχόν στοιχείο $g \in G$, παρατηρούμε ότι $|\langle g\rangle| = \mathrm{ord}(g) \mid p^\nu$ (λόγω τού θεωρήματος 4.1.22 τού Lagrange), οπότε $\mathrm{ord}(g) = p^j$ για κάποιον $j \in \{0,1,...,\nu\}$ (βλ. λήμμα Β.3.14). Άρα η G είναι μια p-ομάδα. □

5.7.4 Σημείωση. Η $\mathbb{Z}(p^\infty)$ αποτελεί παράδειγμα *άπειρης* p-ομάδας. (Βλ. το (iii) τής ασκήσεως **4**-**41**.)

5.7.5 Πόρισμα. *Έστω $(G,\cdot)$ μια πεπερασμένη μη τετριμμένη ομάδα. Εάν έχουμε $\mathrm{ord}(g_1) = \mathrm{ord}(g_2)$ για οιαδήποτε στοιχεία $g_1, g_2 \in G\setminus\{e_G\}$, τότε υπάρχει κάποιος πρώτος αριθμός p, τέτοιος ώστε*

$$\mathrm{ord}(g) = p,\ \forall g \in G\setminus\{e_G\} \ \text{ και } \ \exists \nu \in \mathbb{N} : |G| = p^\nu.$$

ΑΠΟΔΕΙΞΗ. Εάν υπήρχαν πρώτοι αριθμοί p και q, $p \neq q$, με $p \mid |G|$ και $q \mid |G|$, τότε, σύμφωνα με το θεώρημα 5.7.1 τού Cauchy, θα υπήρχαν $g_1, g_2 \in G\setminus\{e_G\}$, τέτοια ώστε να ισχύει $\mathrm{ord}(g_1) = p \neq q = \mathrm{ord}(g_2)$, κάτι που θα αντέκειτο στην υπόθεσή μας. Άρα υπάρχει $\nu \in \mathbb{N}$ με $|G| = p^\nu$. Επιπροσθέτως, σύμφωνα με το θεώρημα 4.1.22 τού Lagrange, η τάξη οιουδήποτε στοιχείου τού $G\setminus\{e_G\}$ ανήκει στο σύνολο $\{p, p^2,..., p^\nu\}$. Κατά το θεώρημα 5.7.1 τού Cauchy υπάρχει *τουλάχιστον ένα* $g \in G\setminus\{e_G\}$ τάξεως $\mathrm{ord}(g) = p$. Άρα, βάσει τής υποθέσεώς μας, $\mathrm{ord}(g) = p$ *για κάθε* $g \in G\setminus\{e_G\}$. □

5.7.6 Πόρισμα. *Έστω $(F,+,\cdot)$ ένα πεπερασμένο σώμα. Τότε* $\mathrm{card}(F) = p^\nu$, *όπου p κάποιος πρώτος αριθμός και $\nu \in \mathbb{N}$, και η $(F,+)$ είναι μια (προσθετική) p-ομάδα.*

ΑΠΟΔΕΙΞΗ. Επειδή $1_F \neq 0_F$, ο πληθικός αριθμός τού F είναι ≥ 2. Για οιαδήποτε στοιχεία $a, b \in F\setminus\{0_F\}$ η απεικόνιση

$$f : F \longrightarrow F,\ \ x \longmapsto f(x) := (ba^{-1})x,$$

είναι ένας αυτομορφισμός τής (προσθετικής) ομάδας $(F,+)$ με $f(a) = b$, οπότε $\mathrm{ord}(a) = \mathrm{ord}(b)$ (λόγω τού (iv) τής προτάσεως 2.4.19). Κατά το πόρισμα 5.7.5 ο πληθικός αριθμός τού υποκειμένου συνόλου F τού σώματος $(F,+,\cdot)$ (που δεν είναι τίποτα άλλο παρά η τάξη τής ομάδας $(F,+)$) οφείλει να ισούται με p^ν, όπου p κάποιος πρώτος αριθμός και $\nu \in \mathbb{N}$. □

5.7.7 Σημείωση. Κατά το πόρισμα 5.7.6 κάθε πεπερασμένο σώμα έχει πληθικό αριθμό q, όπου q κάποια (θετική ακεραία) δύναμη ενός πρώτου αριθμού. Αποδεικνύεται ότι *για κάθε αριθμό q αυτής τής μορφής* υφίσταται κάποιο σώμα $\mathbb{F}_q$

με πληθικό αριθμό q. Επίσης, αποδεικνύεται ότι *κάθε* πεπερασμένο σώμα F με $\mathrm{card}(F) = q$ είναι ισόμορφο με το $\mathbb{F}_q$. (Βλ. C.2.15 και C.2.16.)

5.7.8 Πόρισμα. *Έστω $(G, \cdot)$ μια πεπερασμένη ομάδα και έστω $k \in \mathbb{Z}$. Τότε η*

$$G \ni g \longmapsto g^k \in G$$

είναι αμφιρριπτική απεικόνιση εάν και μόνον εάν $\text{μκδ}(|G|, k) = 1$. (Προσοχή! Για μη αβελιανές ομάδες η εν λόγω απεικόνιση **δεν είναι** κατ' ανάγκην ενδομορφισμός. Πρβλ. 2.1.12. Εδώ εξετάζεται μόνον το πότε είναι αμφιρριπτική.)

ΑΠΟΔΕΙΞΗ. Έστω $n := |G|$. Εάν $\text{μκδ}(n, k) = 1$, τότε $\exists i, j \in \mathbb{Z} : ik - jn = 1$ (βλ. πόρισμα B.2.8), οπότε

$$(g^k)^i = g^{jn+1} = (g^j)^n g = e_G g = g, \ \ \forall g \in G,$$

όπου η προτελευταία ισότητα έπεται από το πόρισμα 4.1.28. Αυτό σημαίνει ότι η απεικόνιση $g \longmapsto g^k$ είναι αμφιρριπτική έχουσα την $g \longmapsto g^i$ ως αντίστροφό της, καθόσον ισχύει $(g^k)^i = (g^i)^k = g$ για κάθε $g \in G$. Αντιστρόφως τώρα, εάν υποθέσουμε ότι $\text{μκδ}(n, k) > 1$, θα δείξουμε ότι η $g \longmapsto g^k$ δεν είναι αμφιρριπτική. Επειδή, βάσει τής υποθέσεώς μας, υπάρχει κάποιος πρώτος αριθμός p που είναι κοινός διαιρέτης των n και k, το θεώρημα 5.7.1 τού Cauchy μάς εγγυάται την ύπαρξη κάποιου στοιχείου $x \in G \smallsetminus \{e_G\}$ τάξεως p, το δε θεώρημα 4.1.22 τού Lagrange το ότι πληρούται η συνθήκη $p \mid n$. Συνεπώς, $x^k = (x^p)^{\frac{n}{p}} = e_G^{\frac{n}{p}} = e_G$, απ' όπου έπεται ότι η $g \longmapsto g^k$ δεν είναι ενριπτική, διότι $x^k = e_G = e_G^k$ αλλά $x \neq e_G$. □

Εν συνεχεία, θα δούμε το πώς μέσω τού θεωρήματος 5.7.1 τού Cauchy είναι εφικτή η ταξινόμηση (μέχρις ισομορφισμού) όλων των ομάδων τάξεως pq, όπου οι p, q είναι δυο πρώτοι αριθμοί με $p < q$. Προς τούτο θα απαιτηθούν ορισμένα προπαρασκευαστικά λήμματα.

5.7.9 Λήμμα. *Έστω $(G, \cdot)$ μια ομάδα τάξεως $|G| = pq$, όπου p, q είναι δυο πρώτοι αριθμοί με $p < q$. Τότε υφίσταται μία και μόνον υποομάδα τής G τάξεως q. Επιπροσθέτως, αυτή η ομάδα οφείλει να είναι ορθόθετη.*

ΑΠΟΔΕΙΞΗ. Κατά το θεώρημα 5.7.1 τού Cauchy,

$$\exists g \in G \smallsetminus \{e_G\} : \mathrm{ord}(g) = |\langle g \rangle| = q.$$

Θα δείξουμε ότι η κυκλική ομάδα $\langle g \rangle$ είναι η μοναδική υποομάδα τής G τάξεως q. Έστω τυχούσα $H \sqsubseteq G$ με $|H| = q$. Σύμφωνα με το (iii) τού πορίσματος 4.1.25, είτε $H = \langle g \rangle$ είτε $H \cap \langle g \rangle = \{e_G\}$. Στη δεύτερη περίπτωση, ο τύπος (4.35) τού γινομένου δίδει

$$\mathrm{card}(H \langle g \rangle) = \frac{|H| \, |\langle g \rangle|}{|H \cap \langle g \rangle|} = \frac{q \cdot q}{1} = q^2,$$

οπότε $H \langle g \rangle \subseteq G \Rightarrow [\mathrm{card}(H \langle g \rangle) = q^2 \leq pq = |G|] \Rightarrow q \leq p$, κάτι που αντίκειται στην υπόθεσή μας. Αυτό σημαίνει ότι $H = \langle g \rangle$. Άρα τελικώς η κυκλική ομάδα $\langle g \rangle$ είναι όντως η μοναδική υποομάδα τής G τάξεως q, κατ' ανάγκην *ορθόθετη* επί τη βάσει τού πορίσματος 4.4.24 (αφού $|G : \langle g \rangle| = p$). □

5.7.10 Παράδειγμα. Η μοναδική υποομάδα τάξεως 5 τής διεδρικής $\mathbf{D}_5 = \langle \alpha, \beta \rangle$ (όπου $|\mathbf{D}_5| = 10$) είναι η κυκλική υποομάδα $\langle \beta \rangle$. Άρα $\langle \beta \rangle \lhd \mathbf{D}_5$.

5.7.11 Λήμμα. *Έστω ότι οι p, q είναι δυο πρώτοι αριθμοί με $p < q$. Τότε ισχύουν τα ακόλουθα*:

(i) *Κάθε αβελιανή ομάδα τάξεως pq είναι κυκλική.*

(ii) *Εάν $q \not\equiv 1 (\mathrm{mod}\, p)$, τότε κάθε ομάδα τάξεως pq είναι κυκλική.*

ΑΠΟΔΕΙΞΗ. (i) Έστω G μια αβελιανή ομάδα τάξεως pq. Κατά το θεώρημα 5.7.1 τού Cauchy υπάρχουν $x, y \in G$ με $\mathrm{ord}(x) = p$ και $\mathrm{ord}(y) = q$. Τότε $\mathrm{ord}(xy) = pq$. Πράγματι· εάν $l := \mathrm{ord}(xy)$, τότε

$$(xy)^{pq} = x^{pq} y^{pq} = (x^p)^q \, (y^q)^p = e_G \underset{2.3.8}{\Longrightarrow} l \mid pq.$$

Από την άλλη μεριά,

$$e_G = (xy)^l = (xy)^{lp} = (x^p)^l \, y^{lp} = y^{lp} \underset{2.3.8}{\Longrightarrow} q \mid lp \Rightarrow q \mid l.$$

Παρομοίως, $p \mid l$. Επομένως, $pq \mid l$ (διότι οι p, q είναι πρώτοι και $p < q$, βλ. πόρισμα B.2.10). Τελικώς λοιπόν, $l = pq$ (βλ. B.1.5 (iii)). Άρα η G είναι κυκλική δυνάμει τής προτάσεως 2.3.7.

(ii) Εάν $q \not\equiv 1 (\mathrm{mod}\, p)$ και η G είναι μια ομάδα τάξεως pq, θεωρούμε εκ νέου στοιχεία $x, y \in G$ με $\mathrm{ord}(x) = p$ και $\mathrm{ord}(y) = q$. Σύμφωνα με το λήμμα 5.7.9 η $\langle y \rangle$ είναι η μοναδική υποομάδα τής G τάξεως q. Επιπροσθέτως, $\langle y \rangle \lhd G$. Επομένως,

$$x \langle y \rangle x^{-1} = \langle y \rangle \Rightarrow \exists k \in \{1, ..., q-1\} : xyx^{-1} = y^k. \tag{5.67}$$

Επαγωγικώς αποδεικνύεται ότι $x^m y x^{-m} = y^{k^m}$, $\forall m \in \mathbb{N}$. Για $m = p$ αυτή η ισότητα δίδει

$$\left.\begin{array}{c} x^p y x^{-p} = y^{k^p} \\ x^p = e_G = x^{-p} \end{array}\right\} \Rightarrow y = y^{k^p}.$$

Επειδή $\mathrm{ord}(y) = q$ και $\mathrm{ord}(y^{k^p}) = \frac{q}{\mathrm{μκδ}(q, k^p)}$ (βλ. 2.3.11), έχουμε $\mathrm{μκδ}(q, k^p) = 1$, οπότε $[k^p]_q = ([k]_q)^p = [1]_q$. Αυτό σημαίνει ότι η τάξη τής κλάσεως ισοτιμίας $[k]_q$ εντός τής πολλαπλασιαστικής ομάδας $\mathbb{Z}_q^\times$ διαιρεί τον p (βλ. 2.3.8), οπότε θα ισούται είτε με 1 είτε με p. Το δεύτερο ενδεχόμενο αποκλείεται από την υπόθεσή μας (διότι εν τοιαύτη περιπτώσει θα έπρεπε, λόγω τού θεωρήματος 4.1.22 τού Lagrange, να ισχύει $p \mid q - 1 = \left|\mathbb{Z}_q^\times\right|$). Άρα $[k]_q = [1]_q$, οπότε $k = 1$ και $xy = yx$ (λόγω τής (5.67)). Όπως στο (i) αποδεικνύουμε ότι $\mathrm{ord}(xy) = pq$, οπότε η G οφείλει να είναι κυκλική βάσει τής προτάσεως 2.3.7. □

5.7.12 Παραδείγματα. Κάθε ομάδα τάξεως $15, 33, 35, 51, 65, 69, 77, 85, 87, 91$ ή 95 είναι κυκλική.

5.7.13 Ορισμός. Εάν οι p, q είναι δυο πρώτοι αριθμοί με $p < q$ και $q \equiv 1(\mathrm{mod}\, p)$, τότε θέτουμε

$$\boxed{\mathbf{L}_{pq} := \left\{ \begin{pmatrix} [a]_q & [b]_q \\ [0]_q & [1]_q \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_q) \,\middle|\, a, b \in \mathbb{Z} \text{ και } a^p \equiv 1(\mathrm{mod}\, q) \right\}.}$$

Είναι άμεσος ο έλεγχος τού ότι το σύνολο $\mathbf{L}_{pq}$, εφοδιασμένο με την πράξη πολλαπλασιασμού πινάκων, αποτελεί μια υποομάδα τής $\mathrm{GL}_2(\mathbb{Z}_q)$.

5.7.14 Πρόταση. *Η $\mathbf{L}_{pq}$ είναι μια μη αβελιανή ομάδα τάξεως pq.*

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς, η κλάση ισοτιμίας $[b]_q$ μπορεί να λάβει οιαδήποτε εκ των q τιμών $[0]_q, [1]_q, ..., [q-1]_q$, διότι στον ορισμό τής $\mathbf{L}_{pq}$ δεν υπεισέρχεται κανένας περιορισμός σε ό,τι αφορά στον ακέραιο b. Άρα το πρόβλημα ανάγεται στην εύρεση τού αριθμού των σαφώς διακεκριμένων τιμών που μπορεί να λάβει η κλάση $[a]_q$. Επειδή εξ υποθέσεως $p \mid q-1$ (όπου $q-1 = \left|\mathbb{Z}_q^\times\right|$), το θεώρημα 5.7.1 τού Cauchy (εφαρμοζόμενο για την ομάδα $\mathbb{Z}_q^\times$) εξασφαλίζει την ύπαρξη τουλάχιστον μίας κλάσεως ισοτιμίας $[c]_q$ ($c \in \mathbb{Z}$) η οποία έχει τάξη p εντός τής $\mathbb{Z}_q^\times$. Προφανώς, λόγω τού πορίσματος 4.1.28, για κάθε $j \in \{0, 1, ..., p-1\}$ έχουμε

$$([c]_q^j)^p = \left[c^{jp}\right]_q = [1]_q \Rightarrow c^{jp} \equiv 1(\mathrm{mod}\, q).$$

Αυτό σημαίνει ότι υπάρχουν *τουλάχιστον* p (σαφώς διακεκριμένες) λύσεις[63] τής εξισώσεως $\mathsf{X}^p - [1]_q = [0]_q$ ανήκουσες στο σώμα $\mathbb{Z}_q$. Από την άλλη μεριά, το πολυώνυμο $\mathsf{X}^p - [1]_q \in \mathbb{Z}_q[\mathsf{X}]$ έχει βαθμό p. Επομένως, σύμφωνα με το πόρισμα C.2.27, το $\mathsf{X}^p - [1]_q$ έχει *το πολύ* p θέσεις μηδενισμού ανήκουσες στο $\mathbb{Z}_q$. Κατά συνέπειαν, το $\mathsf{X}^p - [1]_q$ έχει *ακριβώς* p θέσεις μηδενισμού ανήκουσες στο $\mathbb{Z}_q$, απ' όπου έπεται ότι ο αριθμός των σαφώς διακεκριμένων τιμών που μπορεί να λάβει η κλάση $[a]_q$ στον ορισμό τής $\mathbf{L}_{pq}$ ισούται με p και, κατ' επέκταση, ότι $|\mathbf{L}_{pq}| = pq$. Τέλος, η $\mathbf{L}_{pq}$ δεν είναι αβελιανή, καθότι τα στοιχεία

$$\begin{pmatrix} [1]_q & [1]_q \\ [0]_q & [1]_q \end{pmatrix} \begin{pmatrix} [a]_q & [0]_q \\ [0]_q & [1]_q \end{pmatrix} = \begin{pmatrix} [a]_q & [1]_q \\ [0]_q & [1]_q \end{pmatrix}$$

και

$$\begin{pmatrix} [a]_q & [0]_q \\ [0]_q & [1]_q \end{pmatrix} \begin{pmatrix} [1]_q & [1]_q \\ [0]_q & [1]_q \end{pmatrix} = \begin{pmatrix} [a]_q & [a]_q \\ [0]_q & [1]_q \end{pmatrix}$$

είναι διαφορετικά για οιονδήποτε $a \in \mathbb{Z}$, τέτοιον ώστε η τάξη τής κλάσεως ισοτιμίας $[a]_q$ εντός τής $\mathbb{Z}_q^\times$ να είναι ίση με p. □

5.7.15 Πρόταση. *Εάν οι p, q είναι δυο πρώτοι με $p < q$ και $q \equiv 1(\mathrm{mod}\, p)$, τότε η $\mathbf{L}_{pq}$ είναι μέχρις ισομορφισμού η μόνη μη αβελιανή ομάδα τάξεως pq.*

[63] Για οιουσδήποτε $j, j' \in \{0, 1, ..., p-1\}$ με $j < j'$ έχουμε $[c]_q^j \neq [c]_q^{j'}$, διότι εάν υποθέταμε ότι $[c]_q^j = [c]_q^{j'}$ θα έπρεπε να ισχύει $[c]_q^{j-j'} = [1]_q$, ήτοι κάτι που είναι αδύνατο, αφού $\mathrm{ord}([c]_q) = p$ και $j - j' < p$.

ΑΠΟΔΕΙΞΗ. Έστω G μια μη αβελιανή ομάδα τάξεως pq. Σύμφωνα με το θεώρημα 5.7.1 τού Cauchy υπάρχουν $x, y \in G$ με $\text{ord}(x) = p$ και $\text{ord}(y) = q$. Ακολουθούμε κατά γράμμα την απόδειξη τού (ii) τού λήμματος 5.7.11 μέχρι το σημείο εκείνο στο οποίο συμπεραίνουμε ότι $y = y^{k^p}$, για κάποιον $k \in \{1,...,q-1\}$, οπότε η τάξη τής κλάσεως ισοτιμίας $[k]_q$ εντός τής πολλαπλασιαστικής ομάδας $\mathbb{Z}_q^\times$ ισούται είτε με 1 είτε με p. Εν προκειμένω, αποκλείεται το *πρώτο* ενδεχόμενο (διότι αλλιώς καταλήγουμε στο ότι η G είναι κυκλική). Λόγω τού θεωρήματος 4.1.22 τού Lagrange, ισχύει $p \mid q-1 = \left|\mathbb{Z}_q^\times\right|$. Επειδή

$$\left.\begin{array}{c} \langle y\rangle \sqsubseteq \langle \langle y\rangle, \langle x\rangle\rangle \sqsubseteq G \\ \langle y\rangle \lhd G \end{array}\right\} \underset{4.2.19}{\Longrightarrow} \langle y\rangle \lhd \langle \langle y\rangle, \langle x\rangle\rangle,$$

έχουμε $\langle y\rangle \langle x\rangle \sqsubseteq G$ (βλ. 4.5.12 (ii)). Εξάλλου, από τον τύπο (4.35) τού γινομένου (βλ. 4.5.9) λαμβάνουμε

$$|\langle y\rangle \langle x\rangle| = \frac{|\langle y\rangle|\,|\langle x\rangle|}{|\langle y\rangle \cap \langle x\rangle|} = \frac{qp}{|\{e_G\}|} = pq,$$

οπότε

$$G = \langle y\rangle \langle x\rangle = \left\{ y^i x^j \middle| \, i \in \{0,1,...,q-1\}, j \in \{0,1,...,p-1\}\right\}.$$

Εν συνεχεία επανερχόμαστε στη μη αβελιανή ομάδα $\mathbf{L}_{pq}$ τάξεως pq. Θέτοντας

$$s := \left(\begin{array}{cc} [c]_q & [0]_q \\ [0]_q & [1]_q \end{array}\right), \;\; t := \left(\begin{array}{cc} [1]_q & [1]_q \\ [0]_q & [1]_q \end{array}\right),$$

όπου $[c]_q$ μια κλάση ισοτιμίας έχουσα τάξη p εντός τής $\mathbb{Z}_q^\times$, παρατηρούμε ότι $\text{ord}(s) = p$ και $\text{ord}(t) = q$ εντός τής $\mathbf{L}_{pq}$, και ότι κάθε στοιχείο τής $\mathbf{L}_{pq}$ μπορεί να γραφεί μονοσημάντως υπό τη μορφή

$$\left(\begin{array}{cc} [c^j]_q & [i]_q \\ [0]_q & [1]_q \end{array}\right) = \left(\begin{array}{cc} [1]_q & [i]_q \\ [0]_q & [1]_q \end{array}\right)\left(\begin{array}{cc} [c^j]_q & [0]_q \\ [0]_q & [1]_q \end{array}\right) = t^i s^j,$$

όπου $(i,j) \in \{0,1,...,q-1\} \times \{0,1,...,p-1\}$. Επομένως,

$$\mathbf{L}_{pq} = \langle t\rangle \langle s\rangle = \left\{ t^i s^j \middle| \, i \in \{0,1,...,q-1\}, j \in \{0,1,...,p-1\}\right\}.$$

Ορίζουμε την απεικόνιση

$$f : \mathbf{L}_{pq} \longrightarrow G, \;\; f(t^i s^j) := y^i x^j, \;\; \forall (i,j) \in \{0,1,...,q-1\} \times \{0,1,...,p-1\}.$$

Είναι εύκολο να ελεγχθεί ότι η f είναι ομομορφισμός ομάδων. Ο πυρήνας του είναι η υποομάδα

$$\text{Ker}(f) = \left\{ t^i s^j \in \mathbf{L}_{pq} \middle| \, y^i x^j = e_G \right\}.$$

Επειδή $y^i x^j = e_G \Leftrightarrow x^j = y^{-i} \in \langle y\rangle \cap \langle x\rangle = \{e_G\} \Rightarrow x^j = y^i = e_G \Longrightarrow p \mid j$ και $q \mid i$, έχουμε $t^i = s^j = \mathbf{I}_2$. Κατά συνέπειαν, η f είναι μονομορφισμός. Τέλος, επειδή $|\mathbf{L}_{pq}| = |G| = pq$, συμπεραίνουμε ότι η f είναι ισομορφισμός. □

5.7.16 Θεώρημα. (Ταξινόμηση ομάδων τάξεως $pq,\ p<q$**.)** *Έστω ότι οι* p, q *είναι δυο πρώτοι αριθμοί με* $p<q$*. Τότε ισχύουν τα ακόλουθα*:

(i) *Εάν* $q \not\equiv 1 (\mathrm{mod}\, p)$*, τότε κάθε ομάδα τάξεως* pq *είναι κυκλική. Ιδιαιτέρως, δυο τυχούσες ομάδες τάξεως* pq *είναι ισόμορφες.*

(ii) *Εάν* $q \equiv 1 (\mathrm{mod}\, p)$*, τότε υπάρχουν ακριβώς δύο μη ισόμορφες ομάδες τάξεως* pq*. Συγκεκριμένα, εάν η* $(G,\cdot)$ *μια ομάδα τάξεως* $|G|=pq$*, τότε είτε*

$$\boxed{G \cong \mathbb{Z}_{pq}} \quad \textit{είτε} \quad \boxed{G \cong \mathbf{L}_{pq}.}$$

ΑΠΟΔΕΙΞΗ. (i) Τούτο έπεται από το 5.7.11 (ii) και το θεώρημα 2.4.23.

(ii) Εάν η G είναι αβελιανή, τότε αυτή, σύμφωνα με το (i) τού λήμματος 5.7.11, οφείλει να είναι κυκλική, οπότε ο ισομορφισμός $G \cong \mathbb{Z}_{pq}$ έπεται από το θεώρημα 2.4.23. Εάν η G δεν είναι αβελιανή, τότε η πρόταση 5.7.15 μας πληροφορεί ότι $G \cong \mathbf{L}_{pq}$. □

5.7.17 Λήμμα. *Έστω* p *ένας περιττός πρώτος αριθμός. Τότε*

$$\boxed{\mathbf{L}_{2p} \cong \mathbf{D}_p.}$$

ΑΠΟΔΕΙΞΗ. Επειδή η διεδρική ομάδα $\mathbf{D}_p$ είναι μη αβελιανή και έχει τάξη $2p$, ισχύει κατ' ανάγκην $\mathbf{L}_{2p} \cong \mathbf{D}_p$ επί τη βάσει τής προτάσεως 5.7.15 (με το 2 στη θέση τού p και τον p στη θέση τού q). □

Το επόμενο θεώρημα γενικεύει το θεώρημα 4.1.37.

5.7.18 Θεώρημα. (Ταξινόμηση ομάδων τάξεως $2p,\ p\geq 3$**.)**
Έστω $(G,\cdot)$ *μια ομάδα τάξεως* $|G|=2p$*, όπου* p *περιττός πρώτος αριθμός. Τότε είτε*

$$\boxed{G \cong \mathbb{Z}_{2p}} \quad \textit{είτε} \quad \boxed{G \cong \mathbf{D}_p.}$$

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα ύστερα από εφαρμογή τού θεωρήματος 5.7.16 (με το 2 στη θέση τού p και τον p στη θέση τού q), σε συνδυασμό με το λήμμα 5.7.17. □

Ασκήσεις

5-1. Εάν $(G,\cdot)$ είναι μια πεπερασμένη ομάδα περιττής τάξεως και $x \in G \setminus \{e_G\}$, να αποδειχθεί ότι $x^{-1} \notin \mathrm{ΚΛΣ}_G(x)$.

5-2. Εάν $(G,\cdot)$ είναι μια ομάδα και $\varnothing \neq X \subseteq Y \subseteq G$, να αποδειχθούν τα εξής:

(i) $\mathrm{C}_G(Y) \sqsubseteq \mathrm{C}_G(X)$.

(ii) $X \subseteqq \mathrm{C}_G(\mathrm{C}_G(X))$.

(iii) $\mathrm{C}_G(\mathrm{C}_G(\mathrm{C}_G(X))) = \mathrm{C}_G(X)$.

5-3. Έστω $(G,\cdot)$ μια ομάδα και έστω $\varnothing \neq X \subseteq G$. Να δειχθεί ότι

$$\mathrm{C}_G(gXg^{-1}) = g\,\mathrm{C}_G(X)g^{-1},\ \ \mathrm{N}_G(gXg^{-1}) = g\,\mathrm{N}_G(X)g^{-1}$$

και $\langle gXg^{-1}\rangle = g\ \langle X\rangle\, g^{-1}$ για κάθε $g \in G$.

5-4. Εάν $(H_j)_{j\in J}$ είναι μια οικογένεια υποομάδων μιας ομάδας $(G,\cdot)$, να δειχθεί ότι για κάθε στοιχείο $g \in G$ ισχύουν τα ακόλουθα:

(i) $\bigcap\limits_{j\in J} gH_jg^{-1} = g(\bigcap\limits_{j\in J} H_j)g^{-1}$.

(ii) $\big\langle \{g\ H_jg^{-1}\big|\, j \in J\}\big\rangle = g\,\langle\{\,H_j|\, j \in J\}\rangle\, g^{-1}$.

5-5. Έστω $(G,\cdot)$ μια μη τετριμμένη ομάδα. Να αποδειχθεί η συνεπαγωγή:

$$H \in \mathbf{Max\text{-}Subg}(G) \Longrightarrow [gHg^{-1} \in \mathbf{Max\text{-}Subg}(G),\ \forall g \in G.]$$

5-6. Να δοθεί παράδειγμα υποομάδας H μιας ομάδας G με $\mathfrak{K}(H) > \mathfrak{K}(G)$. [*Υπόδειξη*: Αρκεί, π.χ., να θεωρηθούν οι $G := \mathbf{D}_5 = \langle\alpha,\beta\rangle$ και $H := \langle\beta\rangle \cong \mathbb{Z}_5$.]

5-7. Έστω $(G,\cdot)$ μια πεπερασμένη ομάδα. Να αποδειχθούν τα ακόλουθα:

(i) Ο αριθμός των κλάσεων συζυγίας τής G υπολογίζεται μέσω τού τύπου

$$\boxed{\mathfrak{K}(G) = \frac{1}{|G|}\sum_{x\in G} |\mathrm{C}_G(x)|\,.}$$

(ii) Εάν $H \sqsubseteq G$, τότε

$$\boxed{\frac{\mathfrak{K}(G)}{|G:H|} \leq \mathfrak{K}(H) \leq |G:H|\,\mathfrak{K}(G).}$$

Η πρώτη ανισοϊσότητα ισχύει ως ισότητα $\Leftrightarrow H \trianglelefteq G$. Η δεύτερη ανισοϊσότητα ισχύει ως ισότητα $\Leftrightarrow H = G$.

(iii) Εάν $H \trianglelefteq G$, τότε

$$\boxed{\mathfrak{K}(G/H) + \mathfrak{K}_G(H) - 1 \leq \mathfrak{K}(G) \leq \mathfrak{K}(G/H)\mathfrak{K}(H),}$$

όπου $\mathfrak{K}_G(H)$ είναι ο πληθικός αριθμός των (σαφώς διακεκριμένων) κλάσεων συζυγίας $\kappa\lambda\Sigma_G(x)$, όπου $x \in H$. Η δεύτερη ανισοϊσότητα ισχύει ως ισότητα $\Leftrightarrow [\mathrm{C}_{G/H}(gH) = \mathrm{C}_G(g)H, \forall g \in G.]$

5-8. Έστω $n \in \mathbb{N}, n \geq 3$. Να προσδιορισθούν οι κεντροποιητές των $2n$ στοιχείων, καθώς και οι ορθοθέτες όλων των υποομάδων τής διεδρικής ομάδας $\mathbf{D}_n$.

5-9. Να προσδιορισθούν οι κεντροποιητές των 12 στοιχείων, καθώς και οι ορθοθέτες των 10 υποομάδων τής εναλλάσσουσας ομάδας $\mathfrak{A}_4$.

5-10. Εάν $(G,\cdot)$ είναι μια ομάδα και $K \trianglelefteq G$, να αποδειχθούν τα εξής:

(i) Εάν $H \sqsubseteq G$ και $g \in G$, τότε $gK(HK/K)g^{-1}K = (gHg^{-1})K/K$.

(ii) Εάν H_1, H_2 είναι δυο συζυγείς υποομάδες τής G, τότε οι $H_1K/K, H_2K/K$ είναι συζυγείς υποομάδες τής πηλικοομάδας G/K.

(iii) Εάν $L_1/K, L_2/K$ είναι δυο συζυγείς υποομάδες τής πηλικοομάδας G/K, τότε οι L_1, L_2 είναι συζυγείς υποομάδες τής G.

5-11. Έστω $(G,\cdot)$ μια ομάδα. Ως γνωστόν, εάν $H \sqsubseteq G$, τότε $H \sqsubseteq \mathrm{N}_G(H)$. (Βλ. 5.2.4 (iv).) Να δειχθεί (μέσω καταλλήλου αντιπαραδείγματος) ότι εάν $\varnothing \neq X \subsetneqq G$ και το X *δεν είναι* υποομάδα τής G, ο εγκλεισμός $X \subseteq \mathrm{N}_G(X)$ δεν είναι πάντοτε αληθής.

5-12. Έστω $(G,\cdot)$ μια ομάδα. Εάν υποτεθεί ότι $K \sqsubseteq H \sqsubseteq G$ και $K \trianglelefteq G$, να αποδειχθεί η ισότητα $\mathrm{N}_G(H/K) = \mathrm{N}_G(H)/K$.

5-13. Εάν $(G,\cdot)$ είναι μια μη τετριμμένη ομάδα και $H \in \mathbf{Max\text{-}Subg}(G)$, να αποδειχθούν τα ακόλουθα:

(i) Είτε $\mathrm{N}_G(H) = H$ είτε $\mathrm{N}_G(H) = G$.

(ii) Εάν $H \ntrianglelefteq G$, τότε

$$\mathrm{card}(\{\, g \in G \smallsetminus \{e_G\} \,|\, g \in \kappa\lambda\Sigma_G(H)\}) \leq (|H| - 1)\,|G : H|\,.$$

5-14. Εάν H είναι μια γνήσια υποομάδα μιας πεπερασμένης ομάδας $(G,\cdot)$, να δειχθεί ότι $G \neq \bigcup_{g\in G} gHg^{-1}$.

5-15. Έστω $(G,\cdot)$ μια πεπερασμένη ομάδα και έστω $\Xi = \{x_1, x_2, ..., x_\nu\}$ είναι ένα πλήρες σύστημα εκπροσώπων αυτής ως προς την "$\underset{\text{συζ.}}{\sim}$". Εάν $x_i x_j = x_j x_i$ για οιουσδήποτε $i, j \in \{1, ..., \nu\}$, να αποδειχθεί ότι η G είναι αβελιανή.

5-16. Εάν H είναι μια γνήσια υποομάδα μιας ομάδας $(G,\cdot)$ με $|G : H| < \infty$, να αποδειχθεί ότι υπάρχει στοιχείο $x \in G$ το οποίο δεν ανήκει σε καμία εξ εκείνων των υποομάδων που είναι συζυγείς τής H.

5-17. Έστω $(G,\cdot)$ μια μη τετριμμένη ομάδα, κάθε γνήσια υποομάδα τής οποίας περιέχεται σε μια μεγιστική υποομάδα πεπερασμένου δείκτη. Εάν υποτεθεί ότι δυο τυχούσες μεγιστικές υποομάδες τής G είναι συζυγείς, να αποδειχθεί ότι αυτή είναι κατ' ανάγκην κυκλική.

5-18. Να δοθεί ο κατάλογος εκπροσώπων των κλάσεων συζυγίας τής $\mathfrak{S}_7$ (βάσει των προαναφερθέντων στο εδ. 5.3.17).

5-19. Να προσδιορισθεί ένας εκπρόσωπος για κάθε κλάση συζυγίας των στοιχείων τάξεως 4 τόσον εντός τής $\mathfrak{S}_8$ όσον και εντός τής $\mathfrak{S}_{12}$.

5-20. Έστω $n \in \mathbb{N}$, $n \geq 4$. Να δειχθεί ότι

$$|\mathrm{C}_{\mathfrak{S}_n}([1\,2] \circ [3\,4])| = 8(n-4)!$$

και να προσδιορισθούν όλα τα στοιχεία τής $\mathfrak{S}_n$ τα ανήκοντα στον κεντροποιητή $\mathrm{C}_{\mathfrak{S}_n}([1\,2] \circ [3\,4])$.

5-21. Έστω $n \in \mathbb{N}$, $n \geq 2$, και έστω $c \in \mathfrak{S}_n$ ένας n-κύκλος. Να αποδειχθεί ότι $\mathrm{C}_{\mathfrak{S}_n}(c) = \langle c \rangle$. (Ως εκ τούτου, εάν ισχύει $\sigma \circ c = c \circ \sigma$ για κάποια μετάταξη $\sigma \in \mathfrak{S}_n$, τότε $\sigma = c^j$ για κάποιον $j \in \mathbb{N}$.)

5-22. Έστω $n \in \mathbb{N}$, $n \geq 2$, και έστω p ένας πρώτος αριθμός $\leq n$. Να αποδειχθεί ότι (εντός τής $\mathfrak{S}_n$) το πλήθος των κλάσεων συζυγίας εκείνων των $\sigma \in \mathfrak{S}_n$ που έχουν τάξη $\mathrm{ord}(\sigma) = p$ ισούται με $\left\lfloor \frac{n}{p} \right\rfloor$.

5-23. Να αποδειχθεί ότι οι κυκλικές υποομάδες

$$H := \langle [1\,2\,3\,4\,5\,6] \rangle \;\text{ και }\; K := \langle [1\,2\,3] \circ [4\,5] \rangle$$

τής $\mathfrak{S}_6$ (με $|H| = |K| = 6 \Rightarrow H \cong \mathbb{Z}_6 \cong K$) δεν είναι συζυγείς.

5-24. Έστω H μια υποομάδα τής συμμετρικής ομάδας $\mathfrak{S}_4$.

(i) Εάν $|H| = 3$, να αποδειχθεί ότι το πλήθος των υπομάδων τής $\mathfrak{S}_4$ που είναι ισόμορφες με την H ισούται με τον δείκτη $|\mathfrak{S}_4 : \mathrm{N}_{\mathfrak{S}_4}(H)|$.

(ii) Να δειχθεί ότι αυτό παύει να ισχύει εάν $|H| = 2$.

5-25. Να αποδειχθεί ότι όλες οι κυκλικές υποομάδες τής συμμετρικής ομάδας $\mathfrak{S}_8$ που έχουν τάξη 15 είναι συζυγείς.

5-26. Έστω p ένας πρώτος αριθμός και έστω $H \sqsubseteq \mathfrak{S}_p$ υποομάδα τάξεως $|H| = p$. Να αποδειχθούν τα ακόλουθα:

(i) $\left|\mathrm{N}_{\mathfrak{S}_p}(H)\right| = p(p-1)$.

(ii) $\mathrm{N}_{\mathfrak{S}_p}(H)/\mathrm{C}_{\mathfrak{S}_p}(H) \cong \mathrm{Aut}(H)$.

5-27. (i) Να δοθεί μια απευθείας απόδειξη τής απλότητας τής $\mathfrak{A}_6$ μέσω τού τρίτου καταλόγου τού εδαφίου 5.3.20 και τού πορίσματος 5.1.16.

(ii) Χρησιμοποιώντας τό λήμμα 5.3.25 και το (i) να δοθεί μια (επιπρόσθετη) *τρίτη* απόδειξη τού θεωρήματος 4.3.6. [*Υπόδειξη*: Εάν υποτεθεί ότι $n \geq 7$, $\{\mathrm{id}\} \neq H \trianglelefteq \mathfrak{A}_n$ και $\sigma \in H \smallsetminus \{\mathrm{id}\}$, τότε $\exists l \in \{1, ..., n\} : \sigma(l) \neq l$. Αρκεί να επιλεγεί ένας 3-κύκλος $\tau = [i\,j\,k] \in \mathfrak{A}_n$, τέτοιος ώστε να ισχύει $l \notin \{i, j, k\}$ και $\sigma(l) \in \{i, j, k\}$, να δειχθεί ότι η $\rho := \tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1}$ μετατάσσει κυριολεκτικώς *το πολύ* 6 (σαφώς διακεκριμένα) στοιχεία τού $\{1, ..., n\}$ και να εφαρμοσθεί καταλλήλως το λήμμα 4.3.4, απ' όπου έπεται ότι $H = \mathfrak{A}_n$.]

5-28. Εάν για κάθε $n \in \mathbb{N}$ τεθεί $\mathfrak{a}_n := \mathrm{card}(\{\sigma \in \mathfrak{S}_n |\ \mathrm{card}(\mathrm{supp}(\sigma)) = n\})$, να αποδειχθούν τα εξής:

(i) Ο αριθμός $\mathfrak{a}_n$ (με $\mathfrak{a}_1 = 0, \mathfrak{a}_2 = 1$), ο οποίος καλείται, ιδιαιτέρως, **αριθμός των πλήρων αναδιευθετήσεων** (των $1, ..., n$) ικανοποιεί τις αναδρομικές σχέσεις

$$\mathfrak{a}_n = (n-1)(\mathfrak{a}_{n-1} + \mathfrak{a}_{n-2}) \;\text{ και }\; \mathfrak{a}_n = n\mathfrak{a}_{n-1} + (-1)^n$$

για κάθε $n \in \mathbb{N}$, $n \geq 3$, και -ως εκ τούτου- υπολογίζεται μέσω τού τύπου

$$\boxed{\mathfrak{a}_n = \sum_{j=0}^{n} (-1)^j (n-j)! \binom{n}{j} = n! \sum_{j=0}^{n} \frac{(-1)^j}{j!}.}$$

Για $n \in \{3,4,...,10\}$ οι τιμές που λαμβάνει ο $\mathfrak{a}_n$ είναι οι ακόλουθες[64]:

n	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
$\mathfrak{a}_n$	2	9	44	265	1854	14833	133496	1334961

(ii) $\sum\limits_{n=0}^{\infty} \mathfrak{a}_n \frac{t^n}{n!} = \frac{1}{(1-t)\mathrm{e}^t}$ και $\lim\limits_{n\longrightarrow\infty} \frac{\mathfrak{a}_n}{n!} = \frac{1}{\mathrm{e}}$.

(iii) Εάν, γενικότερα, για κάθε $n \in \mathbb{N}$ και κάθε $k \in \{0,1,...,n\}$ τεθεί

$$\mathfrak{a}_{n,k} := \mathrm{card}(\{\sigma \in \mathfrak{S}_n |\ \mathrm{card}(\mathrm{supp}(\sigma)) = n-k\}),$$

τότε ο $\mathfrak{a}_{n,k}$ (με $\mathfrak{a}_{n,0} = \mathfrak{a}_n, \mathfrak{a}_{n,n-1} = 0$, $\mathfrak{a}_{n,n} = \mathfrak{a}_0 := 1$), ο οποίος καλείται, ιδιαιτέρως, **αριθμός των k συναντήσεων**[65], υπολογίζεται μέσω τού τύπου

$$\boxed{\mathfrak{a}_{n,k} = \tbinom{n}{k}\mathfrak{a}_{n-k} = \tfrac{n!}{k!}\sum_{j=0}^{n}\tfrac{(-1)^j}{j!}.}$$

Για $(n,k) \in \{1,...,8\} \times \{0,1,...,8\}$ οι τιμές που λαμβάνει ο $\mathfrak{a}_{n,k}$ είναι οι ακόλουθες[66]:

$\mathfrak{a}_{n,k}$	$n \ \rightarrow$	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
k $\downarrow$	*	*	*	*	*	*	*	*	*
0	*	0	1	2	9	44	265	1854	14833
1	*	1	0	3	8	45	264	1855	14832
2	*	*	1	0	6	20	135	924	7420
3	*	*	*	1	0	10	40	315	2464
4	*	*	*	*	1	0	15	70	630
5	*	*	*	*	*	1	0	21	112
6	*	*	*	*	*	*	1	0	28
7	*	*	*	*	*	*	*	1	0
8	*	*	*	*	*	*	*	*	1

5-29. Εάν $n \in \mathbb{N}, n \geq 2, \nu \in \{1,...,n\}$ και $\mathfrak{c}_{n,\nu}$ είναι ο αριθμός όλων των μετατάξεων $\sigma \in \mathfrak{S}_n$ που διαθέτουν πλήρεις παραγοντοποιήσεις *σε ακριβώς ν κύκλους* (των 1-κύκλων συμπεριλαμβανομένων, βλ. λήμμα 5.3.3), να αποδειχθεί ότι

$$\boxed{\mathfrak{c}_{n,\nu} = |s(n,\nu)| = (-1)^{n-\nu}s(n,\nu),}$$

[64] Για την τιμή τού $\mathfrak{a}_n$ για μεγαλύτερους n βλ. http://oeis.org/A000166.

[65] Υπενθύμιση τού *κλασικού προβλήματος των συναντήσεων*: Από μια κάλπη που περιέχει n σφαιρίδια αριθμημένα από το 1 έως το n εξάγονται το ένα μετά το άλλο (χωρίς επανάθεση) όλα τα σφαιρίδια. Η εξαγωγή τού j-οστού σφαιριδίου κατά την j-οστή δοκιμή (για κάποιο $j \in \{1,...,n\}$) καλείται **συνάντηση**. Ο (προσδιοριστέος) αριθμός των τρόπων εξαγωγής των n σφαιριδίων από την κάλπη με $k \in \{0,1,...,n\}$ συναντήσεις ισούται με $\mathfrak{a}_{n,k}$.

[66] Για την τιμή τού $\mathfrak{a}_{n,k}$ για μεγαλύτερους n και k βλ. http://oeis.org/A008290.

όπου $s(n,\nu)$ είναι οι λεγόμενοι **αριθμοί Stirling πρώτου είδους** (με $s(n,n)=1$) οι προσδιοριζόμενοι ως συντελεστές τής εκφράσεως τού επίτυπου γινομένου

$$t(t-1)(t-2)\cdots(t-n+1)=\sum_{\nu=0}^{n}s(n,\nu)t^{\nu}$$

ως πολυωνύμου, από την οποία προκύπτει ο **τύπος τού Schlömilch**:

$$s(n,\nu)=\sum_{i=0}^{n-\nu}\sum_{j=0}^{i}(-1)^{j}\binom{i}{j}\binom{n+i-1}{k-1}\binom{2n-k}{n-k-i}\frac{j^{n-k+i}}{i!}.$$

Ο αριθμός $\mathfrak{c}_{n,\nu}$ υπολογίζεται απευθείας μέσω τής ταυτότητας

$$t(t+1)(t+2)\cdots(t+n-1)=\sum_{\nu=1}^{n}\mathfrak{c}_{n,\nu}t^{\nu},$$

από την οποία έπεται ότι

$$\boxed{\mathfrak{c}_{n,\nu}=\frac{n!}{\nu!}\sum\frac{1}{\lambda_1\lambda_2\cdots\lambda_\nu},}$$

όπου το άθροισμα λαμβάνεται υπεράνω όλων των ν-άδων τού συνόλου

$$\left\{(\lambda_1,\lambda_2,...,\lambda_\nu)\in\mathbb{N}_0^{\nu}\middle|\,\lambda_1+\lambda_2+\cdots+\lambda_\nu=n\right\}.$$

Για $(n,\nu)\in\{1,...,8\}\times\{1,...,8\}$ οι τιμές τού $\mathfrak{c}_{n,\nu}$ είναι οι ακόλουθες[67]:

$\mathfrak{c}_{n,\nu}$	$n\ \ \rightarrow$	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
ν $\downarrow$	*	*	*	*	*	*	*	*	*
1	*	1	1	2	6	24	120	720	5040
2	*	*	1	3	11	50	274	1764	13068
3	*	*	*	1	6	35	225	1624	13132
4	*	*	*	*	1	10	85	735	6769
5	*	*	*	*	*	1	15	175	1960
6	*	*	*	*	*	*	1	21	322
7	*	*	*	*	*	*	*	1	28
8	*	*	*	*	*	*	*	*	1

5-30. Για κάθε $m\in\mathbb{N}$ και για κάθε πρώτον αριθμό p ορίζεται ο μη αρνητικός ακέραιος

$$\boldsymbol{\nu}_p(m):=\begin{cases}\max\left\{k\in\mathbb{N}\,:\,p^k\mid m\right\}, & \text{όταν } p\mid m,\\ 0, & \text{όταν } p\nmid m.\end{cases}$$

[67] Για την τιμή τού $\mathfrak{c}_{n,\nu}$ για μεγαλύτερους n και ν βλ. http://oeis.org/A008275.

Προφανώς, $m = \prod_{p \text{ πρώτος με } p \leq m} p^{\nu_p(m)}$. Εάν $n \in \mathbb{N}$, $n \geq 2$, να αποδειχθούν τα ακόλουθα για τη συμμετρική ομάδα $\mathfrak{S}_n$:

(i) Για κάθε[68] $m \in \mathbb{N}$, $m \in \mathfrak{D}_{n!}$,

$$[\exists \sigma \in \mathfrak{S}_n : \mathbf{ord}(\sigma) = m] \Longleftrightarrow \sum_{p \text{ πρώτος με } p \leq m} p^{\nu_p(m)} \leq n.$$

(ii) Εάν[69] $\mathfrak{g}(n) := \max\{\mathbf{ord}(\sigma) |\ \sigma \in \mathfrak{S}_n\}$, τότε $\mathfrak{g}(n) \mid \exp(\mathfrak{S}_n)$ και

$$\boxed{\exp(\mathfrak{S}_n) = \mathbf{εκπ}(\{1, ..., n\}) = \prod_{p \text{ πρώτος με } p \leq n} p^{\lfloor \log_p(n) \rfloor}.}$$

(iii) Να δοθεί ο κατάλογος των τιμών που λαμβάνουν οι $\mathfrak{g}(n)$ και $\exp(\mathfrak{S}_n)$ όταν[70] $n \in \{2, 3, ..., 14\}$.

5-31. Έστω $(G, \cdot)$ μια ομάδα. Εάν $x, y \in G$, $z := xy$ και $z \in Z(G)$, να αποδειχθεί ότι $xy = yx$.

5-32. Εάν $(G, \cdot)$ είναι μια ομάδα και $H \trianglelefteq G$, να αποδειχθεί ότι $Z(H) \trianglelefteq G$.

5-33. Έστω H τυχούσα υποομάδα μιας ομάδας $(G, \cdot)$. Να δειχθεί ότι

$$Z(gHg^{-1}) = g\, Z(H) g^{-1},\ \forall g \in G.$$

5-34. Να αποδειχθεί ότι για κάθε ομάδα $(G, \cdot)$ ισχύουν οι ισότητες

$$\mathbf{C}_G(Z(G)) = G = \mathbf{N}_G(Z(G)).$$

5-35. Έστω $(G, \cdot)$ μια μη τετριμμένη ομάδα. Εάν υποτεθεί ότι $H \in \mathbf{Max\text{-}Subg}(G)$ με $|G : H| = n \in \mathbb{N}$, όπου ο n είναι σύνθετος αριθμός, να αποδειχθεί ότι $Z(G) \sqsubset H$.

5-36. Έστω $(F, +, \cdot)$ ένα σώμα. Να αποδειχθεί ότι το κέντρο τής ομάδας $\mathbf{Heis}(F)$ τού Heisenberg (βλ. D.2.24) είναι ισόμορφο με την προσθετική ομάδα $(F, +)$.

5-37. Λαμβανομένου υπ' όψιν ότι $|\mathbf{GL}_2(\mathbb{Z}_3)| = 48$, να αποδειχθούν τα εξής:

(i) $Z(\mathbf{GL}_2(\mathbb{Z}_3)) \sqsubseteq \mathbf{UT}_2(\mathbb{Z}_3)^{\times} \sqsubseteq \mathbf{GL}_2(\mathbb{Z}_3)$ με $\left|\mathbf{UT}_2(\mathbb{Z}_3)^{\times}\right| = 12$.

(ii) $\mathrm{Core}_{\mathbf{GL}_2(\mathbb{Z}_3)}(\mathbf{UT}_2(\mathbb{Z}_3)^{\times}) = Z(\mathbf{GL}_2(\mathbb{Z}_3))$.

(iii) $\mathbf{GL}_2(\mathbb{Z}_3)/Z(\mathbf{GL}_2(\mathbb{Z}_3)) \cong \mathfrak{S}_4$.

---

[68] Υπενθύμιση συμβολισμού: $\mathfrak{D}_{n!} := \{d \in \mathbb{N} : d \mid n!\}$ (βλ. B.2.34).

[69] Ο Edmund Landau (1877-1938) απέδειξε στην §61 τού βιβλίου του *Handbuch der Lehre von der Verteilung der Primzahlen*, Band I, Teubner Verlag, 1909, σελ. 222-229, ότι

$$\lim_{n \longrightarrow \infty} \frac{\ln(\mathfrak{g}(n))}{\sqrt{n \ln(n)}} = 1.$$

[70] Για αυτές τις μικρές τιμές τού n οι υπολογισμοί μπορούν να γίνουν απευθείας (κάνοντας, π.χ., χρήση τής (B.14) ή τής (B.26)). Για μεγαλύτερους n βλ., π.χ., τις ακολουθίες ακεραίων υπ. αρ. M0537 και M1590 στην *Encyclopedia of Integer Sequences* των N.J.A Sloane και S. Plouffe (Academic Press, 1995) ή τις ακολουθίες ακεραίων υπ. αρ. A000793 και A003418 στη διαδικτυακή έκδοση (http://oeis.org).

5-38. Εάν $(G,\cdot)$ είναι μια ομάδα και $H \trianglelefteq G$, να δειχθεί ότι $Z(G)H/H \sqsubseteq Z(G/H)$.

5-39. Έστω $(G,\cdot)$ μια ομάδα. Εάν $H,K,L \in \mathbf{NSubg}(G)$ και $L \sqsubseteq H$, να αποδειχθεί ότι ισχύει η συνεπαγωγή:

$$H/L \sqsubseteq Z(G/L) \Longrightarrow HK/LK \sqsubseteq Z(G/LK).$$

5-40. Κατά το θεώρημα 3.5.1 τού Cayley, $L(G) \cong G \cong R(G)$, όπου

$$L(G) := \{\, L_g \mid g \in G\} \sqsubseteq \mathfrak{S}_G,\ R(G) := \{\, R_g \mid g \in G\} \sqsubseteq \mathfrak{S}_G,$$

είναι οι εξ αριστερών και εκ δεξιών κανονικές αναπαραστάσεις τής G εντός τής $\mathfrak{S}_G$, αντιστοίχως, με

$$L_g : G \longrightarrow G,\ x \longmapsto L_g(x) := gx,\ \ R_g : G \longrightarrow G,\ x \longmapsto R_g(x) := xg.$$

Να αποδειχθούν τα εξής: (i) $L(G) \sqsubseteq \mathbf{C}_{\mathfrak{S}_G}(R(G))$ και $R(G) \sqsubseteq \mathbf{C}_{\mathfrak{S}_G}(L(G))$.
(ii) $L_g = R_g \Longleftrightarrow [\mathrm{ord}(g) \in \{1,2\}$ και $g \in Z(G)]$.
(iii) $L_{g_1} = R_{g_2} \Longleftrightarrow [g_1, g_2 \in Z(G)$ και $g_1 = g_2^{-1}]$.
(iv) $L(Z(G)) = L(G) \cap R(G) = R(Z(G))$.

5-41. Να αποδειχθεί ότι δεν υπάρχει καμία ομάδα G έχουσα ομάδα αυτομορφισμών $\mathrm{Aut}(G)$ ισόμορφη με κάποια εκ των $(\mathbb{Z},+), (\mathbb{Z}_{2m+1},+)$ (όπου $m \in \mathbb{N}$).

5-42. Έστω $(G,\cdot)$ μια πεπερασμένη ομάδα έχουσα έναν αυτομορφισμό ϑ, τέτοιον ώστε να ισχύει

$$\mathrm{card}(\{\, g \in G \mid \vartheta(g) = g^{-1}\}) > \frac{3}{4}\,|G|\,.$$

Να αποδειχθεί ότι η G είναι *αβελιανή* και ότι $\vartheta(g) = g^{-1}$, $\forall g \in G$. Εν συνεχεία, να δοθεί ένα παράδειγμα *μη αβελιανής* πεπερασμένης ομάδας έχουσας έναν αυτομορφισμό ο οποίος αντιστρέφει *ακριβώς τα* $\frac{3}{4}$ *των στοιχείων της*.

5-43. Έστω $(G,\cdot)$ μια πεπερασμένη ομάδα. Να αποδειχθεί ότι $|\mathbf{C}_G(x)| \geq |G/G'|$ για κάθε στοιχείο $x \in G$.

5-44. Έστω $(G,\cdot)$ μια ομάδα, για την οποία $\exists\, H \trianglelefteq G : |H| = 2$.
(i) Να αποδειχθεί ότι $H \sqsubseteq Z(G)$.
(ii) Ισχύει κατ' ανάγκην ότι $H \sqsubseteq G'$;
(iii) Εάν η G έχει ακριβώς ένα στοιχείο x τάξεως 2, να δειχθεί ότι $\langle x\rangle \sqsubseteq Z(G)$.

5-45. Έστω $(G,\cdot)$ μια ομάδα και έστω $K \trianglelefteq G$ με $K \cap G' = \{e_G\}$. Να αποδειχθούν τα εξής:
(i) $K \sqsubseteq Z(G)$.
(ii) $Z(G/K) = Z(G)/K$.

5-46. Έστω $(G,\cdot)$ μια πεπερασμένη ομάδα. Εάν $|G'| = 2$, να αποδειχθεί ότι ο δείκτης $|G : G'|$ είναι άρτιος.

5-47. Έστω $(G,\cdot)$ μια ομάδα και έστω $H := \left\{ ab^2 \middle| \, a \in G', b \in G \right\}$. Να αποδειχθούν τα εξής:

(i) $H \trianglelefteq G$.

(ii) Εάν η G είναι πεπερασμένη και έχει περιττή τάξη, τότε $H = G$.

5-48. Εάν $(G,\cdot)$ είναι μια ομάδα και $H \trianglelefteq G$, να δειχθεί ότι $(G/H)' = G'H/H$.

5-49. Εάν $(G,\cdot)$ είναι μια ομάδα και $(H,*)$ μια αβελιανή ομάδα, να δειχθεί ότι

$$\mathrm{Hom}(G,H) \cong \mathrm{Hom}(G/G',H).$$

5-50. Να αποδειχθούν οι σχέσεις (5.54) και (5.55).

5-51. Εάν $n \in \mathbb{N}$, $n \geq 2$, να δειχθεί ότι για κάθε σώμα F με $\chi\alpha\rho(F) \neq 2$ ισχύει

$$\mathbf{UT}_n^{[1]}(F) = \left[\mathbf{UT}_n(F)^{\times}, \mathbf{UT}_n(F)^{\times}\right] \left(= (\mathbf{UT}_n(F)^{\times})'\right).$$

5-52. Για την άπειρη διεδρική ομάδα $\mathbf{D}_\infty := \langle S, T_{-1} \rangle$ (βλ. 3.4.14 και 3.4.15) να αποδειχθούν τα ακόλουθα:

(i) Το σύνολο των υποομάδων της είναι το

$$\boxed{\mathbf{Subg}(\mathbf{D}_\infty) = \{\{\left\langle T_{-1}^k \right\rangle \big| \, k \in \mathbb{N}_0\}, \{H_k | \, k \in \mathbb{Z}\}, \{H_{k,l} | \, k \in \mathbb{N}, l \in \{0,..,k-1\}\}\},}$$

όπου $\left\langle T_{-1}^k \right\rangle \cong k\mathbb{Z}$, $H_k := \left\langle S \circ T_{-1}^k \right\rangle \cong \mathbb{Z}_2$ και $H_{k,l} := \left\langle T_{-1}^k, S \circ T_{-1}^l \right\rangle \cong \mathbf{D}_\infty$.

(ii) $\mathbf{NSubg}(\mathbf{D}_\infty) = \{\{\left\langle T_{-1}^k \right\rangle \big| \, k \in \mathbb{N}_0\}, H_{2,0}, H_{2,1}, \mathbf{D}_\infty\}$ και

$$\mathbf{D}_\infty / \langle T_{-1} \rangle \cong \mathbb{Z}_2, \qquad \mathbf{D}_\infty / \left\langle T_{-1}^2 \right\rangle \cong \mathbf{V},$$
$$\mathbf{D}_\infty / \left\langle T_{-1}^k \right\rangle \cong \mathbf{D}_k \ (\text{για } k \geq 3), \qquad \mathbf{D}_\infty / H_{2,0} \cong \mathbb{Z}_2 \cong \mathbf{D}_\infty / H_{2,1}.$$

(iii) $\mathbf{Min\text{-}NSubg}(\mathbf{D}_\infty) = \varnothing$.

(iv) Το κέντρο τής $\mathbf{D}_\infty$ είναι τετριμμένο.

(v) $\mathbf{D}'_\infty = \left\langle T_{-1}^2 \right\rangle$ και $\mathbf{D}_\infty^{\mathrm{ab}} \cong \mathbf{V}$.

5-53. Να αποδειχθεί ότι το σύνολο πινάκων

$$G := \left\{ \mathbf{A}(\varphi(\mathsf{X}), \psi(\mathsf{X}), \chi(\mathsf{X},\mathsf{Y})) \middle| \, \varphi(\mathsf{X}), \psi(\mathsf{X}) \in \mathbb{Q}[\mathsf{X}], \chi(\mathsf{X},\mathsf{Y}) \in \mathbb{Q}[\mathsf{X},\mathsf{Y}] \right\},$$

όπου

$$\mathbf{A}(\varphi(\mathsf{X}), \psi(\mathsf{X}), \chi(\mathsf{X},\mathsf{Y})) := \begin{pmatrix} 1 & \varphi(\mathsf{X}) & \chi(\mathsf{X},\mathsf{Y}) \\ 0 & 1 & \psi(\mathsf{X}) \\ 0 & 0 & 1 \end{pmatrix},$$

αποτελεί μια ομάδα (με τον πολλαπλασιασμό πινάκων ως πράξη της) έχουσα ως μεταθέτρια υποομάδα της την

$$G' = \left\{ \mathbf{A}(0,0,\chi(\mathsf{X},\mathsf{Y})) \middle| \, \chi(\mathsf{X},\mathsf{Y}) \in \mathbb{Q}[\mathsf{X},\mathsf{Y}] \right\}$$

και, εν συνεχεία, ότι ο πίνακας $\mathbf{A}(0,0,1+\mathsf{XY}+\mathsf{X}^2\mathsf{Y}^2) \in G'$ δεν είναι μεταθέτης δύο στοιχείων τής G.

5-54. Έστω $(G,\cdot)$ μια ομάδα. Εάν $H \sqsubseteq G$, να αποδειχθεί ότι

$$H \trianglelefteq G \Longleftrightarrow [H,G] \sqsubseteq H.$$

5-55. Έστω $(G,\cdot)$ μια ομάδα. Εάν $H \sqsubseteq G$, $K \sqsubseteq G$ και $L \trianglelefteq G$ να αποδειχθεί ότι

$$[HL,KL] \sqsubseteq [H,K]\,L,\ \ [HL,KL]\,L = [H,K]\,L$$

και $[HL/L, KL/L] = [H,K]\,L/L$.

5-56. Έστω $n \in \mathbb{N}$, $n \geq 3$. Να γραφεί η εξίσωση (5.64) των κλάσεων συζυγίας για τη διεδρική ομάδα $\mathbf{D}_n$ ως προς το πλήρες σύστημα εκπροσώπων Ξ_n αυτών που δίδεται στην πρόταση 5.1.10.

5-57. Εάν $n \in \mathbb{N}$, $n \geq 3$, να γραφεί η εξίσωση κλάσεων συζυγίας (5.64) για τη συμμετρική ομάδα $\mathfrak{S}_n$.

5-58. Εάν $(G,\cdot)$ είναι μια πεπερασμένη ομάδα, να δειχθούν τα εξής:

(i) Εάν $\mathfrak{K}(G) = 3$, τότε είτε $G \cong \mathbb{Z}_3$ είτε $G \cong \mathfrak{S}_3$.

(ii) Εάν $\mathfrak{K}(G) = 4$, τότε η G είναι ισόμορφη με μία εκ των: $\mathbb{Z}_4, \mathbf{V}, \mathbf{D}_5, \mathfrak{A}_4$.

5-59. Έστω $(G,\cdot)$ μια πεπερασμένη ομάδα. Να αποδειχθεί ότι το σύνολο G δεν μπορεί να γραφεί ως ένωση $G = \bigcup_{i\in I} H_i$ των μελών μιας οικογένειας υποομάδων της $(H_i)_{i\in I}$ εάν $\mathrm{card}(I) \geq 2$, $H_i \cap H_{i'} = \{e_G\}$ για οιουσδήποτε $i, i' \in I$ με $i \neq i'$ και $\mathrm{N}_G(H_i) = H_i$ για κάθε $i \in I$.

5-60. Να αποδειχθεί ότι για κάθε $n \in \mathbb{N}$ ισχύει η σχέση:

$$\boxed{\mathrm{card}(\mathbf{Gr}_{\text{ταξ.}}(n)) \leq n^{n\log_2(n)}.}$$

[*Υπόδειξη*: Να ακολουθηθεί η απόδειξη τού λήμματος 5.6.14 και να χρησιμοποιηθεί η άσκηση **4-30**.]

ΚΕΦΑΛΑΙΟ 6

Αναλλοίωτες υποομάδες, πλήρεις ομάδες και το ολόμορφο ομάδας

Έστω $(G, \cdot)$ μια ομάδα και έστω $H \sqsubseteq G$. Κατά την πρόταση 5.4.24,

$$H \trianglelefteq G \iff \vartheta(H) \subseteq H,\ \forall \vartheta \in \mathrm{Inn}(G).$$

Εάν σε αυτήν τη συνθήκη αντικαταστήσουμε την $\mathrm{Inn}(G)$ με τυχόν $\mathcal{A} \subseteq \mathrm{End}(G)$, τότε λαμβάνουμε μια άλλη κλάση υποομάδων: Λέμε ότι μια υποομάδα H τής G **μένει αναλλοίωτη ως προς το** $\mathcal{A}$ ή, απλούστερα, ότι η H είναι $\mathcal{A}$-**αναλλοίωτη** όταν $\vartheta(H) \subseteq H$ για κάθε $\vartheta \in \mathcal{A}$. Είναι προφανές ότι τόσον η τετριμμένη υποομάδα όσον και η ίδια η G είναι $\mathcal{A}$-αναλλοίωτες για *οιοδήποτε* $\mathcal{A} \subseteq \mathrm{End}(G)$. Κάθε μη τετριμμένη ομάδα G η οποία δεν διαθέτει άλλες $\mathcal{A}$-αναλλοίωτες υποομάδες (πέραν αυτών των δύο εμφανών) καλείται $\mathcal{A}$-**απλή ομάδα**. $\mathcal{A}$-αναλλοίωτες υποομάδες και $\mathcal{A}$-απλές ομάδες υπεισέρχονται (για διάφορα $\mathcal{A}$) σε πολλές εφαρμογές. Στις δύο πρώτες ενότητες τού παρόντος κεφαλαίου θα περιορισθούμε στην καταγραφή των κύριων ιδιοτήτων των *χαρακτηριστικών* και *πλήρως αναλλοιώτων* υποομάδων μιας ομάδας G και των *χαρακτηριστικώς απλών* ομάδων των συμπεριλαμβανομένων στον ακόλουθο κατάλογο (όπου $\mathcal{A} \in \{\mathrm{Aut}(G),\ \mathrm{End}(G)\}$), καθώς και στην παροχή χρήσιμων παραδειγμάτων.

$\mathcal{A}$	$\mathcal{A}$-**αναλλοίωτες υποομάδες**	$\mathcal{A}$-**απλές ομάδες**
$\mathrm{Inn}(G)$	ορθόθετες υποομάδες	απλές ομάδες
$\mathrm{Aut}(G)$	χαρακτηριστικές υποομάδες	χαρακτηριστικώς απλές ομάδες
$\mathrm{End}(G)$	πλήρως αναλλοίωτες υποομάδες	---

Εν συνεχεία θα παραθέσουμε κλάσεις *πλήρων ομάδων* (ήτοι ομάδων με τετριμμένο κέντρο και μόνον εσωτερικούς αυτομορφισμούς). Στην τελευταία ενότητα τού κε-

φαλαίου περιλαμβάνονται η κατασκευή και οι βασικές ιδιότητες τού λεγομένου *ολόμορφου* μιας ομάδας.

6.1 ΧΑΡΑΚΤΗΡΙΣΤΙΚΕΣ ΥΠΟΟΜΑΔΕΣ

6.1.1 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \sqsubseteq G$. Οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) $\vartheta(H) \subseteq H,\ \forall \vartheta \in \mathrm{Aut}(G)$.

(ii) $\vartheta(H) \sqsubseteq H,\ \forall \vartheta \in \mathrm{Aut}(G)$.

(iii) $\vartheta(H) = H,\ \forall \vartheta \in \mathrm{Aut}(G)$.

ΑΠΟΔΕΙΞΗ. Οι συνεπαγωγές (ii)⇒(i) και (iii)⇒(ii) είναι προφανείς, ενώ η (i)⇒(ii) έπεται από το πόρισμα 2.1.20. Απομένει να αποδειχθεί η (ii)⇒(iii). Έστω τυχών $\vartheta \in \mathrm{Aut}(G)$. Επειδή $\vartheta^{-1} \in \mathrm{Aut}(G)$, έχουμε

$$\vartheta^{-1}(H) \sqsubseteq H \Longrightarrow H = \vartheta(\vartheta^{-1}(H)) \sqsubseteq \vartheta(H).$$

Οι $\vartheta(H) \sqsubseteq H$ και $H \sqsubseteq \vartheta(H)$ δίδουν την ισότητα $\vartheta(H) = H$. □

6.1.2 Ορισμός. Μια υποομάδα H μιας ομάδας $(G,\cdot)$ καλείται **χαρακτηριστική υποομάδα** (σημειούμενη, ιδιαιτέρως, ως[1] $H \sqsubseteq_{\chi\alpha\rho.} G$) όταν ικανοποιεί μία (και, κατ' επέκταση, και τις τρεις) εκ των συνθηκών (i), (ii), (iii) τής προτάσεως 6.1.1.

6.1.3 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω*[2] *$H \sqsubseteq G$.*

(i) *Εάν η H είναι η μοναδική υποομάδα τής G τάξεως $|H|$, τότε $H \sqsubseteq_{\chi\alpha\rho.} G$.*

(ii) *Εάν η H είναι η μοναδική κυκλική (ή η μοναδική αβελιανή) υποομάδα τής G τάξεως $|H|$, τότε $H \sqsubseteq_{\chi\alpha\rho.} G$.*

ΑΠΟΔΕΙΞΗ. (i) Έστω τυχών αυτομορφισμός $\vartheta \in \mathrm{Aut}(G)$. Η εικόνα $\vartheta(H)$ τής H μέσω τού ϑ είναι μια υποομάδα τής $\vartheta(G) = G$ τάξεως $|\vartheta(H)| = |H|$ (βλ. 2.4.6 (i) και 2.4.19 (i)). Από την προϋποτεθείσα μοναδικότητα τής υποομάδας H (με αυτήν την ιδιότητα) έπεται ότι $\vartheta(H) = H$, δηλαδή ότι $H \sqsubseteq_{\chi\alpha\rho.} G$.

(ii) Η εικόνα $\vartheta(H)$ αυτής τής υποομάδας H μέσω ενός $\vartheta \in \mathrm{Aut}(G)$ είναι μια *κυκλική* (και αντιστοίχως, μια *αβελιανή*) υποομάδα τής $\vartheta(G) = G$ τάξεως $|\vartheta(H)| = |H|$ (βλ. 2.4.6 (i) και 2.4.19 (i), (ii) και (iii)). Από την προϋποτεθείσα μοναδικότητα τής H (με μία από αυτές τις ιδιότητες) έπεται ότι $\vartheta(H) = H$, δηλαδή ότι $H \sqsubseteq_{\chi\alpha\rho.} G$. □

6.1.4 Παράδειγμα. Έστω $n \in \mathbb{N},\ n \geq 3$. Στην n-οστή διεδρική ομάδα

$$\mathbf{D}_n = \langle \alpha, \beta \rangle = \left\{ \beta^j \,\middle|\, j \in \{0,1,...,n-1\} \right\} \cup \left\{ \alpha \circ \beta^j \,\middle|\, j \in \{0,1,...,n-1\} \right\}$$

[1] Κατ' αναλογίαν γράφουμε $H \sqsubset_{\chi\alpha\rho.} G$ όταν η H είναι χαρακτηριστική *γνήσια* υποομάδα τής G. Ο συμβολισμός "$H \not\sqsubseteq_{\chi\alpha\rho.} G$" θα σημαίνει ότι η H τού G *δεν είναι χαρακτηριστική υποομάδα* τής G.

[2] Εν προκειμένω, δεν υποτίθεται ότι η G ή η H είναι πεπερασμένη.

(βλ. 3.4.4) έχουμε αφ' ενός μεν (λόγω τού πορίσματος 2.3.11)

$$\mathrm{ord}(\beta^j) = \left|\left\langle \beta^j \right\rangle\right| = \frac{n}{\text{μκδ}(j,n)},\ \forall j \in \{0,1,...,n-1\},$$

αφ' ετέρου δε

$$\beta^{-j} \circ \alpha = \alpha \circ \beta^j \Rightarrow \alpha = \beta^j \circ \alpha \circ \beta^j \underset{\alpha=\alpha^{-1}}{\Longrightarrow} \mathrm{id}_{\mathcal{E}_n} = \alpha \circ \beta^j \circ \alpha \circ \beta^j = (\alpha \circ \beta^j)^2,$$

απ' όπου έπεται ότι $\mathrm{ord}(\alpha \circ \beta^j) = \left|\left\langle \alpha \circ \beta^j \right\rangle\right| = 2,\ \forall j \in \{0,1,...,n-1\}$. Κατά συνέπειαν, η $\langle\beta\rangle = \left\langle \beta^j \right\rangle$, όπου $j \in \{1,...,n-1\}$ με $\text{μκδ}(j,n) = 1$, είναι η *μοναδική* κυκλική υποομάδα τής $\mathbf{D}_n$ τάξεως n. Εξ αυτού έπεται (μέσω τού (ii) τής προτάσεως 6.1.3) ότι $\langle\beta\rangle \sqsubset_{\chi\alpha\varrho.} \mathbf{D}_n$.

6.1.5 Πρόταση. *Εάν $(H_j)_{j\in J}$ είναι μια οικογένεια χαρακτηριστικών υποομάδων μιας ομάδας $(G,\cdot)$, τότε ισχύουν τα ακόλουθα*:
(i) $\bigcap_{j\in J} H_j \sqsubseteq_{\chi\alpha\varrho.} G$.
(ii) $\langle\{\, H_j \,|\, j \in J\}\rangle \sqsubseteq_{\chi\alpha\varrho.} G$.

ΑΠΟΔΕΙΞΗ. Έστω τυχών $\vartheta \in \mathrm{Aut}(G)$. Εξ υποθέσεως,

$$\vartheta(H_j) \subseteq H_j,\ \forall j \in J. \tag{6.1}$$

(i) Προφανώς, $\vartheta(\bigcap\limits_{j\in J} H_j) = \bigcap\limits_{j\in J} \vartheta(H_j) \subseteq \bigcap\limits_{j\in J} H_j \Rightarrow \bigcap\limits_{j\in J} H_j \sqsubseteq_{\chi\alpha\varrho.} G$.
(ii) Έστω τυχόν $g \in \langle\{\, H_j \,|\, j \in J\}\rangle$. Αυτό (σύμφωνα με το πόρισμα 2.2.6) γράφεται υπό τη μορφή $g = h_{j_1} h_{j_2} \cdots h_{j_k}$, όπου $h_{j_\rho} \in H_{j_\rho},\ \forall \rho \in \{1,...,k\}$, για κάποιον $k \in \mathbb{N}$. Προφανώς,

$$\vartheta(g) = \underbrace{\vartheta(h_{j_1})}_{\in H_{j_1}} \underbrace{\vartheta(h_{j_2})}_{\in H_{j_2}} \cdots \underbrace{\vartheta(h_{j_k})}_{\in H_{j_k}} \in \langle\{\, H_j \,|\, j \in J\}\rangle$$

(λόγω των (6.1)), οπότε $\langle\{\, H_j \,|\, j \in J\}\rangle \sqsubseteq_{\chi\alpha\varrho.} G$. □

6.1.6 Πρόταση. *Το κέντρο οιασδήποτε ομάδας αποτελεί χαρακτηριστική υποομάδα αυτής.*

ΑΠΟΔΕΙΞΗ. Έστω $(G,\cdot)$ τυχούσα ομάδα και έστω $z \in Z(G)$. Επειδή *για κάθε* $g \in G$ και *κάθε* $\vartheta \in \mathrm{Aut}(G)$ έχουμε $\vartheta^{-1} \in \mathrm{Aut}(G)$, $\vartheta^{-1}(g) \in G$ και

$$\vartheta^{-1}(g)z = z\vartheta^{-1}(g) \Rightarrow g\vartheta(z) = \vartheta(\vartheta^{-1}(g)z) = \vartheta(z\vartheta^{-1}(g)) = \vartheta(z)g,$$

παρατηρούμε ότι $\vartheta(z) \in Z(G)$, οπότε $\vartheta(Z(G)) \subseteq Z(G) \Rightarrow Z(G) \sqsubseteq_{\chi\alpha\varrho.} G$. □

6.1.7 Πρόταση. *Για οιαδήποτε ομάδα $(G,\cdot)$ ισχύει η συνεπαγωγή*

$$H \sqsubseteq_{\chi\alpha\varrho.} G \Longrightarrow H \trianglelefteq G.$$

ΑΠΟΔΕΙΞΗ. Εάν $H \sqsubseteq_{\chi\alpha\varrho.} G$, τότε (εξ ορισμού) $\vartheta(H) = H$ για κάθε $\vartheta \in \mathrm{Aut}(G)$ και, ιδιαιτέρως, $\vartheta(H) = H$ για κάθε $\vartheta \in \mathrm{Inn}(G)$, οπότε $H \trianglelefteq G$ (βλ. 5.4.24). □

6.1.8 Σημείωση. Η αντίστροφη συνεπαγωγή δεν είναι πάντοτε αληθής. Υπάρχουν ορθόθετες υποομάδες ομάδων που δεν είναι χαρακτηριστικές. (Βλ. παράδειγμα 6.1.16.) Μια ικανή συνθήκη για να ισχύει και η αντίστροφη συνεπαγωγή (στην περίπτωση όπου η ομάδα αναφοράς μας είναι *πεπερασμένη*) δίδεται στην επομένη πρόταση.

6.1.9 Πρόταση. *Έστω $(G,\cdot)$ μια πεπερασμένη ομάδα. Εάν $H \trianglelefteq G$, τότε*

$$\text{μκδ}(|H|, |G:H|) = 1 \Longrightarrow H \sqsubseteq_{\text{χαρ.}} G.$$

ΑΠΟΔΕΙΞΗ. Έστω τυχών $\vartheta \in \text{Aut}(G)$. Θέτοντας $K := \vartheta(H)$ αρκεί να δείξουμε ότι $K \subseteq H$. Ας υποθέσουμε ότι $|H| = n$ και $|G:H| = |G/H| = m$. Λόγω τού υφιστάμενου ισομορφισμού $H \xrightarrow{\cong} K,\ h \longmapsto \vartheta(h)$, έχουμε $|K| = n$. Εξάλλου, επειδή $HK \sqsubseteq G$, ισχύει $HK/H \sqsubseteq G/H$. (Βλ. 4.2.24, 4.5.14 (i), 4.5.12 και 4.4.15 (i).) Αυτό, σύμφωνα με το θεώρημα 4.1.22 τού Lagrange, σημαίνει ότι $|HK/H| \mid m$. Από την άλλη μεριά, το 2ο θεώρημα ισομορφισμών 4.5.13 μας πληροφορεί ότι

$$HK/H \cong K/(H\cap K) \Rightarrow |HK/H| = \tfrac{|K|}{|H\cap K|} = \tfrac{n}{|H\cap K|},$$

οπότε $[|HK/H| \mid m \text{ και } |HK/H| \mid n] \underset{\text{B.2.6}}{\Longrightarrow} |HK/H| \mid \text{μκδ}(m,n) = 1$. Εξ αυτού έπεται ότι $|HK/H| = 1 \Rightarrow HK = H \Rightarrow K \subseteq H$. □

6.1.10 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Εάν $H \in \mathbf{Subg}(G)$ και $K \in \mathbf{Subg}(H)$, τότε ισχύουν οι εξής συνεπαγωγές*:

(i) $\left[K \sqsubseteq_{\text{χαρ.}} H \text{ και } H \sqsubseteq_{\text{χαρ.}} G\right] \Longrightarrow K \sqsubseteq_{\text{χαρ.}} G.$

(ii) $\left[K \sqsubseteq_{\text{χαρ.}} H \text{ και } H \trianglelefteq G\right] \Longrightarrow K \trianglelefteq G.$

ΑΠΟΔΕΙΞΗ. (i) Έστω τυχών $\vartheta \in \text{Aut}(G)$. Εξ υποθέσεως, $\vartheta(H) = H$. Προφανώς, $\vartheta|_H \in \text{Aut}(H)$. Επομένως, $\vartheta|_H(K) = K$. Επειδή $\vartheta|_H(K) = \vartheta(K)$, συμπεραίνουμε ότι $K \sqsubseteq_{\text{χαρ.}} G$.

(ii) Έστω τυχών $\vartheta \in \text{Inn}(G)$. Επειδή $H \trianglelefteq G$, έχουμε $\vartheta(H) = H$ (βλ. 5.4.24). Προφανώς, ο περιορισμός $\vartheta|_H$ τού ϑ επί τής υποομάδας H αποτελεί έναν (όχι κατ' ανάγκην εσωτερικό) αυτομορφισμό τής H. Επομένως, $\vartheta|_H(K) = K$. Επειδή $\vartheta|_H(K) = \vartheta(K) = K$, έχουμε (εκ νέου μέσω τής προτάσεως 5.4.24) $K \trianglelefteq G$. □

6.1.11 Παρατήρηση. (i) Εν αντιθέσει προς την "$\trianglelefteq$", η διμελής σχέση "$\sqsubseteq_{\text{χαρ.}}$" (επί τού $\mathbf{Subg}(G)$) είναι, σύμφωνα με το (i) τής προτάσεως 6.2.7, *μεταβατική*. (Πρβλ. εδ. 4.2.27.)

(ii) Κατά την πρόταση 4.2.19 ισχύει η συνεπαγωγή

$$[K \sqsubseteq H \sqsubseteq G \text{ και } K \trianglelefteq G] \Longrightarrow K \trianglelefteq H.$$

Αυτή παύει να ισχύει όταν η "$\trianglelefteq$" αντικατασταθεί με την "$\sqsubseteq_{\text{χαρ.}}$". Πράγματι· εάν θεωρήσουμε τις υποομάδες $K := \langle\beta^2\rangle \sqsubset \langle\alpha,\beta^2\rangle := H$ τής διεδρικής ομάδας $G := \mathbf{D}_4 = \langle\alpha,\beta\rangle$, τότε $Z(\mathbf{D}_4) = \langle\beta^2\rangle \sqsubset_{\text{χαρ.}} \mathbf{D}_4$ (όπου $\langle\beta^2\rangle \cong \mathbb{Z}_2$) και $\langle\alpha,\beta^2\rangle \cong \mathbf{V}$ (βλ. εδ. 5.4.8, 6.1.6 και 4.1.41). Ωστόσο, $\langle\beta^2\rangle \not\sqsubseteq_{\text{χαρ.}} \langle\alpha,\beta^2\rangle$. (Πρβλ. εδ. 6.1.16.)

6.1.12 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Εάν $K \sqsubseteq H \sqsubseteq G$, τότε ισχύει η συνεπαγωγή*

$$\big[K \sqsubseteq_{\text{χαρ.}} G \text{ και } H/K \sqsubseteq_{\text{χαρ.}} G/K\big] \Longrightarrow H \sqsubseteq_{\text{χαρ.}} G.$$

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς, επειδή $K \sqsubseteq_{\text{χαρ.}} G \underset{6.1.7}{\Longrightarrow} K \trianglelefteq G$, ορίζεται η πηλικοομάδα G/K. Επιπροσθέτως, επειδή (σύμφωνα με την πρόταση 4.2.19) $K \trianglelefteq H$, ορίζεται *και* η πηλικοομάδα H/K. Έστω τυχών $\vartheta \in \mathrm{Aut}(G)$ και έστω

$$G/K \xrightarrow{\vartheta^{\pi\eta\lambda.}} G/K,\ gK \longmapsto \vartheta^{\pi\eta\lambda.}(gK) := \vartheta(g)K,$$

ο μοναδικός ενδομορφισμός τής πηλικοομάδας G/K που καθιστά το διάγραμμα

$$\begin{array}{ccc} G & \xrightarrow{\ \vartheta\ } & G \\ {\scriptstyle \pi_K^G}\downarrow & \circlearrowleft & \downarrow{\scriptstyle \pi_K^G} \\ G/K & \xrightarrow[\vartheta^{\pi\eta\lambda.}]{} & G/K \end{array}$$

μεταθετικό. Επειδή $\vartheta(K) = K \Rightarrow K = \vartheta^{-1}(K)$ και $\mathrm{Im}(\vartheta) = G$, ο $\vartheta^{\pi\eta\lambda.}$ αποτελεί έναν *αυτομορφισμό* τής G/K. (Βλ. θεώρημα 4.5.5.) Εξ υποθέσεως,

$$H/K \sqsubseteq_{\text{χαρ.}} G/K \Longrightarrow \vartheta^{\pi\eta\lambda.}(H/K) = H/K. \tag{6.2}$$

Από την άλλη μεριά, $K \trianglelefteq H \underset{4.2.30\,\text{(i)}}{\Longrightarrow} K = \vartheta(K) \trianglelefteq \vartheta(H)$ και

$$\vartheta^{\pi\eta\lambda.}(H/K) = \Big\{\vartheta^{\pi\eta\lambda.}(gK)\,|g \in H\Big\} = \{\vartheta(g)K\,|g \in H\} = \vartheta(H)/K. \tag{6.3}$$

Από τις (6.2) και (6.3) έπεται ότι

$$H/K = \vartheta(H)/K \Longrightarrow \vartheta(H) = H \Longrightarrow H \sqsubseteq_{\text{χαρ.}} G,$$

όπου η πρώτη συνεπαγωγή οφείλεται στην αμφιρριπτικότητα τής απεικονίσεως $\Psi_{\pi_K^G} : \mathbf{Subg}(G;K) \longrightarrow \mathbf{Subg}(G/K)$ τού πορίσματος 4.4.15. □

6.1.13 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Εάν $H, K \in \mathbf{Subg}(G)$, τότε*

$$\big[H \sqsubseteq_{\text{χαρ.}} G \text{ και } K \sqsubseteq_{\text{χαρ.}} G\big] \Longrightarrow [H,K] \sqsubseteq_{\text{χαρ.}} G.$$

ΑΠΟΔΕΙΞΗ. Έστω τυχών $\vartheta \in \mathrm{Aut}(G)$. Για οιοδήποτε ζεύγος $(x,y) \in H \times K$ έχουμε

$$\vartheta([x,y]) = \vartheta(xyx^{-1}y^{-1}) = \vartheta(x)\vartheta(y)\vartheta(x)^{-1}\vartheta(y)^{-1} = [\vartheta(x),\vartheta(y)]\,,$$

οπότε το (i) τής προτάσεως 2.4.9 δίδει

$$\begin{aligned} \vartheta\left([H,K]\right) &= \vartheta\left(\langle\{[x,y]\,|\,(x,y) \in H \times K\,\}\rangle\right) \\ &= \langle\{\vartheta([x,y])\,|\,(x,y) \in H \times K\,\}\rangle \\ &= \langle\{[\vartheta(x),\vartheta(y)]\,|\,(x,y) \in H \times K\,\}\rangle = [\vartheta(H),\vartheta(K)]\,. \end{aligned}$$

Εξ υποθέσεως, $\vartheta(H) = H$ και $\vartheta(K) = K$. Άρα $\vartheta\left([H,K]\right) = [H,K]$. □

6.1.14 Πόρισμα. *Η μεταθέτρια υποομάδα* $G' = [G, G]$ *οιασδήποτε ομάδας* $(G, \cdot)$ *είναι χαρακτηριστική.*

6.1.15 Ορισμός. Μια μη τετριμμένη ομάδα καλείται **χαρακτηριστικώς απλή ομάδα** όταν διαθέτει ως χαρακτηριστικές υποομάδες της *μόνον* την τετριμμένη και τον εαυτό της[3].

Λόγω τής προτάσεως 6.1.7 κάθε απλή ομάδα είναι χαρακτηριστικώς απλή. Όμως το αντίστροφο δεν ισχύει.

6.1.16 Παράδειγμα. Για την ομάδα $\mathbf{V} := \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3\}$ των τεσσάρων στοιχείων τού Klein, όπου $\sigma_1 := [1\,2]\circ[3\,4]\,, \sigma_2 := [1\,3]\circ[2\,4]\,, \sigma_3 := [1\,4]\circ[2\,3]\,$, γνωρίζουμε ότι $\mathbf{Subg}(\mathbf{V}) = \{\{\mathrm{id}\}, \langle\sigma_1\rangle\,, \langle\sigma_2\rangle\,, \langle\sigma_3\rangle\,, \mathbf{V}\}$ και ότι $\mathbf{Aut}(\mathbf{V}) = \{\vartheta_0, \vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5\}$, όπου $\vartheta_0 := e_{\mathbf{Aut}(\mathbf{V})}$, $\vartheta_j(\mathrm{id}) = \mathrm{id}$, για κάθε $j \in \{1, 2, 3, 4, 5\}$,

$$\begin{array}{l} \vartheta_1\,(\sigma_1) := \sigma_1,\ \vartheta_1\,(\sigma_2) := \sigma_3,\ \vartheta_1\,(\sigma_3) := \sigma_2, \\ \vartheta_2\,(\sigma_1) := \sigma_2,\ \vartheta_2\,(\sigma_2) := \sigma_1,\ \vartheta_2\,(\sigma_3) := \sigma_3, \\ \vartheta_3\,(\sigma_1) := \sigma_2,\ \vartheta_3\,(\sigma_2) := \sigma_3,\ \vartheta_3\,(\sigma_3) := \sigma_1, \\ \vartheta_4\,(\sigma_1) := \sigma_3,\ \vartheta_4\,(\sigma_2) := \sigma_1,\ \vartheta_4\,(\sigma_3) := \sigma_2 \end{array}$$

και $\vartheta_5\,(\sigma_1) := \sigma_3,\ \vartheta_5\,(\sigma_2) := \sigma_2,\ \vartheta_5\,(\sigma_3) := \sigma_1$. (Βλ. εδ. 4.1.41, καθώς και την απόδειξη τού (ii) τού πορίσματος 3.5.8.) Επειδή, π.χ.,

$$\vartheta_1\,(\langle\sigma_2\rangle) = \langle\sigma_3\rangle \neq \langle\sigma_2\rangle\,,\ \ \vartheta_1\,(\langle\sigma_3\rangle) = \langle\sigma_2\rangle \neq \langle\sigma_3\rangle$$

και $\vartheta_2\,(\langle\sigma_1\rangle) = \langle\sigma_2\rangle \neq \langle\sigma_1\rangle\,$, οι $\langle\sigma_1\rangle\,, \langle\sigma_2\rangle\,, \langle\sigma_3\rangle$ *δεν είναι* χαρακτηριστικές υποομάδες τής $\mathbf{V}$, οπότε η $\mathbf{V}$ είναι χαρακτηριστικώς απλή. Από την άλλη μεριά, η $\mathbf{V}$ δεν είναι απλή, διότι οι $\langle\sigma_1\rangle\,, \langle\sigma_2\rangle\,, \langle\sigma_3\rangle$ *είναι* ορθόθετες υποομάδες της.

6.1.17 Παράδειγμα. Η ομάδα $(\mathbb{Q}, +)$ είναι χαρακτηριστικώς απλή. Πράγματι· κατά το θεώρημα 2.4.33, $\mathbf{Aut}(\mathbb{Q}) = \{\,\vartheta_\ell \mid \ell \in \mathbb{Q}\smallsetminus\{0\}\}$, όπου

$$\vartheta_\ell : \mathbb{Q} \longrightarrow \mathbb{Q},\ q \longmapsto \vartheta_\ell(q) := \ell q.$$

Έστω H τυχούσα μη τετριμμένη χαρακτηριστική υποομάδα τής $(\mathbb{Q}, +)$ και έστω $q \in H\smallsetminus\{0\}$. Για *κάθε* $r \in \mathbb{Q}\smallsetminus\{0\}$ θέτουμε $\ell := rq^{-1}$ και παρατηρούμε ότι

$$\left.\begin{array}{r} r = \ell q = \vartheta_\ell(q) \in \vartheta_\ell(H) = H \Rightarrow \mathbb{Q}\smallsetminus\{0\} \subseteq H \\ H \sqsubseteq \mathbb{Q} \Rightarrow 0 \in H \end{array}\right\} \Rightarrow H = \mathbb{Q}.$$

Άρα η $(\mathbb{Q}, +)$ είναι όντως χαρακτηριστικώς απλή (χωρίς, ωστόσο, να είναι απλή, διότι σύμφωνα με την πρόταση 4.3.2 καμία άπειρη αβελιανή ομάδα δεν είναι απλή).

[3] Το ότι αυτές οι δύο υποομάδες είναι πάντοτε χαρακτηριστικές υποομάδες *οιασδήποτε* ομάδας, είναι προφανές.

6.2 ΠΛΗΡΩΣ ΑΝΑΛΛΟΙΩΤΕΣ ΥΠΟΟΜΑΔΕΣ

6.2.1 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \sqsubseteq G$. Οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) $\vartheta(H) \subseteq H,\ \forall \vartheta \in \mathrm{End}(G)$.

(ii) $\vartheta(H) \sqsubseteq H,\ \forall \vartheta \in \mathrm{End}(G)$.

ΑΠΟΔΕΙΞΗ. Η συνεπαγωγή (ii)⇒(i) είναι προφανής, ενώ η (i)⇒(ii) έπεται από το πόρισμα 2.1.20. □

6.2.2 Ορισμός. Μια υποομάδα H μιας ομάδας $(G,\cdot)$ καλείται **πλήρως αναλλοίωτη υποομάδα** (σημειούμενη, ιδιαιτέρως, με το σύμβολο[4] $H \sqsubseteq_{\text{πλ. αν.}} G$) όταν ικανοποιεί τις συνθήκες (i), (ii) τής προτάσεως 6.2.1.

6.2.3 Πρόταση. *Εάν $(H_j)_{j\in J}$ είναι μια οικογένεια πλήρως αναλλοιώτων υποομάδων μιας ομάδας $(G,\cdot)$, τότε ισχύουν τα ακόλουθα*:

(i) $\bigcap_{j\in J} H_j \sqsubseteq_{\text{πλ. αν.}} G$.

(ii) $\langle \{\, H_j \,|\, j \in J\} \rangle \sqsubseteq_{\text{πλ. αν.}} G$.

ΑΠΟΔΕΙΞΗ. Πανομοιότυπη εκείνης τής προτάσεως 6.1.5. (Αρκεί κανείς να εκκινήσει από τυχόντα *ενδομορφισμό* τής G και να χρησιμοποιήσει τα ίδια επιχειρήματα.) □

6.2.4 Πρόταση. *Για οιαδήποτε ομάδα $(G,\cdot)$ ισχύει η συνεπαγωγή*

$$H \sqsubseteq_{\text{πλ. αν.}} G \Longrightarrow H \sqsubseteq_{\text{χαρ.}} G.$$

ΑΠΟΔΕΙΞΗ. Εάν $H \sqsubseteq_{\text{πλ. αν.}} G$, τότε (εξ ορισμού) $\vartheta(H) \subseteq H$ για κάθε $\vartheta \in \mathrm{End}(G)$ και, ιδιαιτέρως, $\vartheta(H) \subseteq H$ για κάθε $\vartheta \in \mathrm{Aut}(G)$, οπότε $H \sqsubseteq_{\text{χαρ.}} G$ (βλ. 6.1.1). □

6.2.5 Πρόταση. *Κάθε υποομάδα μιας κυκλικής ομάδας είναι πλήρως αναλλοίωτη (και, κατ' επέκταση, και χαρακτηριστική λόγω τής προτάσεως* 6.2.4).

ΑΠΟΔΕΙΞΗ. Έστω $(G,\cdot)$ μια κυκλική ομάδα και έστω $H \sqsubseteq G$. Τότε $G = \langle g \rangle$ για κάποιο στοιχείο $g \in G$ και $H = \langle g^d \rangle$ για κάποιον $d \in \mathbb{N}_0$. (Βλ. 2.4.25 (i).) Έστω τυχών $\vartheta \in \mathrm{End}(G)$. Επειδή $\vartheta(g) \in \langle g \rangle$, υπάρχει $m \in \mathbb{Z}$, τέτοιος ώστε να ισχύει $\vartheta(g) = g^m$. Επομένως,

$$\vartheta(H) = \vartheta\left(\left\langle g^d \right\rangle\right) = \left\langle \vartheta(g^d) \right\rangle = \left\langle \vartheta(g)^d \right\rangle = \left\langle (g^m)^d \right\rangle = \left\langle (g^d)^m \right\rangle = \left\langle (g^d)^{|m|} \right\rangle \sqsubseteq H.$$

(Βλ. 2.4.9 (i) και 2.4.25 (i).) □

[4] Κατ' αναλογίαν γράφουμε $H \sqsubset_{\text{πλ. αν.}} G$ όταν η H είναι πλήρως αναλλοίωτη *γνήσια* υποομάδα τής G. Ο συμβολισμός "$H \not\sqsubseteq_{\text{πλ. αν.}} G$" θα σημαίνει ότι η H τού G *δεν είναι πλήρως αναλλοίωτη υποομάδα* τής G.

6.2.6 Σημείωση. Στην πρόταση 6.1.6 αποδείξαμε ότι το κέντρο $Z(G)$ μιας ομάδας $(G,\cdot)$ αποτελεί μια χαρακτηριστική υποομάδα αυτής. Εντούτοις, το $Z(G)$ δεν είναι κατ' ανάγκην πλήρως αναλλοίωτη υποομάδα της. Μάλιστα, ένα απλό παράδειγμα χαρακτηριστικής, μη πλήρως αναλλοίωτης υποομάδας μιας οικείας μας ομάδας είναι το κέντρο $Z(\mathbf{GL}_2(\mathbb{Q}))$ τής γενικής γραμμικής ομάδας $\mathbf{GL}_2(\mathbb{Q})$. Πράγματι· βάσει των αποδειχθέντων στην πρόταση 5.4.12,

$$Z(\mathbf{GL}_2(\mathbb{Q})) = \left\{ \begin{pmatrix} q & 0 \\ 0 & q \end{pmatrix} \middle| \, q \in \mathbb{Q}\smallsetminus\{0\} \right\}.$$

Επιπροσθέτως, η ορίζουσα οιουδήποτε $\mathbf{A} \in \mathbf{GL}_2(\mathbb{Q})$ γράφεται υπό τη μορφή $\det(\mathbf{A}) = \dfrac{2^{m_{\mathbf{A}}}s}{t}$, όπου s,t περιττοί ακέραιοι και $m_{\mathbf{A}}$ ένας (μονοσημάντως ορισμένος) ακέραιος αριθμός εξαρτώμενος από τον $\mathbf{A}$. Επειδή η ορίζουσα τού γινομένου δύο πινάκων ισούται με το γινόμενο των οριζουσών αυτών (βλ. D.2.11), έχουμε

$$m_{\mathbf{AB}} = m_{\mathbf{A}} + m_{\mathbf{B}}, \;\; \forall(\mathbf{A},\mathbf{B}) \in \mathbf{GL}_2(\mathbb{Q}) \times \mathbf{GL}_2(\mathbb{Q}).$$

Ως εκ τούτου, η απεικόνιση

$$\vartheta : \mathbf{GL}_2(\mathbb{Q}) \longrightarrow \mathbf{GL}_2(\mathbb{Q}), \; \mathbf{A} \longmapsto \vartheta(\mathbf{A}) := \begin{pmatrix} 1 & m_{\mathbf{A}} \\ 0 & 1 \end{pmatrix},$$

αποτελεί έναν ενδομορφισμό τής $\mathbf{GL}_2(\mathbb{Q})$, διότι

$$\begin{aligned} \vartheta(\mathbf{AB}) &= \begin{pmatrix} 1 & m_{\mathbf{AB}} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & m_{\mathbf{A}} + m_{\mathbf{B}} \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & m_{\mathbf{A}} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & m_{\mathbf{B}} \\ 0 & 1 \end{pmatrix} = \vartheta(\mathbf{A})\vartheta(\mathbf{B}) \end{aligned}$$

για κάθε $(\mathbf{A},\mathbf{B}) \in \mathbf{GL}_2(\mathbb{Q}) \times \mathbf{GL}_2(\mathbb{Q})$. Επειδή

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \in Z(\mathbf{GL}_2(\mathbb{Q})) \;\text{ με }\; \vartheta\left(\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\right) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \notin Z(\mathbf{GL}_2(\mathbb{Q})),$$

έχουμε $Z(\mathbf{GL}_2(\mathbb{Q})) \not\sqsubseteq_{\text{πλ. αν.}} \mathbf{GL}_2(\mathbb{Q})$.

6.2.7 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Εάν $H \in \mathbf{Subg}(G)$ και $K \in \mathbf{Subg}(H)$, τότε ισχύει η συνεπαγωγή*

$$[K \sqsubseteq_{\text{πλ. αν.}} H \text{ και } H \sqsubseteq_{\text{πλ. αν.}} G] \Longrightarrow K \sqsubseteq_{\text{πλ. αν.}} G.$$

ΑΠΟΔΕΙΞΗ. Έστω τυχών $\vartheta \in \mathrm{End}(G)$. Εξ υποθέσεως, $\vartheta(H) \sqsubseteq H$. Προφανώς, $\vartheta|_H \in \mathrm{End}(H)$. Επομένως, $\vartheta|_H(K) \sqsubseteq K$. Επειδή $\vartheta|_H(K) = \vartheta(K)$, συμπεραίνουμε ότι $K \sqsubseteq_{\text{πλ. αν.}} G$. □

6.2.8 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Εάν $H,K \in \mathbf{Subg}(G)$, τότε*

$$[H \sqsubseteq_{\text{πλ. αν.}} G \text{ και } K \sqsubseteq_{\text{πλ. αν.}} G] \Longrightarrow [H,K] \sqsubseteq_{\text{πλ. αν.}} G.$$

ΑΠΟΔΕΙΞΗ. Έστω τυχόν $g \in [H,K]$. Το g γράφεται υπό τη μορφή

$$g = [x_1,y_1]^{\varepsilon_1}[x_2,y_2]^{\varepsilon_2}\cdots[x_k,y_k]^{\varepsilon_k},\ k\in\mathbb{N},$$

όπου $x_j \in H$, $y_j \in K$ και $\varepsilon_j \in \{\pm 1\}$, $\forall j \in \{1,...,k\}$. (Βλ. 5.5.29 και (2.6).) Επειδή

$$\vartheta([x_j,y_j]) = \vartheta(x_jy_jx_j^{-1}y_j^{-1}) = \vartheta(x_j)\vartheta(y_j)\vartheta(x_j)^{-1}\vartheta(y_j)^{-1} = [\vartheta(x_j),\vartheta(y_j)]$$

και $\vartheta(x_j) \in \vartheta(H) \subseteq H$, $\vartheta(y_j) \in \vartheta(K) \subseteq K$, για κάθε $j \in \{1,...,k\}$, λαμβάνουμε

$$\vartheta(g) = \prod_{j=1}^{k} [\vartheta(x_j),\vartheta(y_j)]^{\varepsilon_j} \in [H,K],$$

οπότε $\vartheta([H,K]) \subseteq [H,K] \Rightarrow [H,K] \sqsubseteq_{\text{πλ. αν.}} G$. □

6.2.9 Πόρισμα. *Η μεταθέτρια υποομάδα $G' = [G,G]$ οιασδήποτε ομάδας $(G,\cdot)$ είναι πλήρως αναλλοίωτη.*

6.3 ΠΛΗΡΕΙΣ ΟΜΑΔΕΣ

Η ομάδα $\mathrm{Out}(G)$ των εξωτερικών αυτομορφισμών μιας ομάδας $(G,\cdot)$ (βλ. 5.4.31) ενδέχεται να είναι τετριμμένη, όπως, π.χ., συμβαίνει στην περίπτωση κατά την οποία η $(G,\cdot)$ είναι *πλήρης ομάδα*.

6.3.1 Ορισμός. Μια ομάδα $(G,\cdot)$ καλείται **πλήρης ομάδα** όταν $Z(G) = \{e_G\}$ και (ταυτοχρόνως) $\mathrm{Aut}(G) = \mathrm{Inn}(G)$.

6.3.2 Παρατήρηση. Προφανώς, $\mathrm{Aut}(G) \cong G$ (βλ. (5.41)) και η $\mathrm{Out}(G)$ είναι τετριμμένη για κάθε πλήρη ομάδα $(G,\cdot)$.

Σημαντικές οικογένειες πλήρων ομάδων δίδονται στα θεωρήματα 6.3.5, 6.3.21 και 6.3.22. (Οι αποδείξεις των θεωρημάτων 6.3.5 και 6.3.8 οφείλονται στον Γερμανό μαθηματικό[5] Otto Hölder (1859-1937).)

6.3.3 Λήμμα. *Έστω $n \in \mathbb{N}$, $n \geq 2$. Εάν $\sigma \in \mathfrak{S}_n$, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) $\mathrm{ord}(\sigma) = 2$.

(ii) $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k$, *όπου οι $\tau_1,\tau_2,...,\tau_k$ είναι k ανά δύο ξένες μεταξύ τους αντιμεταθέσεις για κάποιον $k \leq \frac{n}{2}$.*

ΑΠΟΔΕΙΞΗ. Προφανώς, $\mathrm{ord}(\sigma) = 1 \Leftrightarrow \sigma = \mathrm{id}$. Γι' αυτόν τον λόγο μπορούμε δίχως βλάβη τής γενικότητας να υποθέσουμε ότι $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{id}\}$. Η σ μπορεί (επί τη βάσει τού θεωρήματος 3.2.7) να γραφεί υπό τη μορφή $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k$ επαλλήλων συνθέσεων ανά δύο ξένων μεταξύ τους κύκλων $\tau_1,\tau_2,...,\tau_k$ μήκους ≥ 2. (Αυτή η έκφραση είναι *μονοσημάντως ορισμένη* μέχρις αναδιατάξεως των μετεχόντων

[5] Βλ. Otto Hölder: *Bildung zusammengesetzter Gruppen*, Math. Annalen, Bd. **46** (1895), 321-422.

κύκλων.) Εάν l_j είναι το μήκος τού τ_j για κάθε $j \in \{1, ..., k\}$, τότε $\mathrm{ord}(\sigma) = l_1$ όταν $k = 1$ και $\mathrm{ord}(\sigma) = \text{εκπ}(l_1, ..., l_k)$ όταν $k \geq 2$ (βλ. 3.2.10). Επειδή για $k \geq 2$ έχουμε

$$\left\{ \begin{array}{c} \text{εκπ}(l_1, ..., l_k) = 2, \\ \text{όπου } l_1 \geq 2, ..., l_k \geq 2 \end{array} \right\} \Longleftrightarrow l_1 = \cdots = l_k = 2,$$

η ισοδυναμία των συνθηκών (i) και (ii) είναι προφανής. □

6.3.4 Λήμμα. *Έστω $n \in \mathbb{N}$, $n \geq 3$. Εάν $\vartheta \in \mathrm{Aut}(\mathfrak{S}_n)$, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Η εικόνα οιασδήποτε αντιμεταθέσεως μέσω τού ϑ είναι μια αντιμετάθεση.*

(ii) $\vartheta \in \mathrm{Inn}(\mathfrak{S}_n)$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Ας υποθέσουμε ότι $\vartheta([1\ i]) = [\alpha_i\ \beta_i]$, με $\alpha_i \neq \beta_i$, για κάθε $i \in \{2, ..., n\}$. Προφανώς, $\vartheta([1\ 2] \circ [1\ i]) = [\alpha_2\ \beta_2] \circ [\alpha_i\ \beta_i]$, $\forall i \in \{2, ..., n\}$. Για οιονδήποτε $i \in \{3, ..., n\}$ η σύνθεση $[1\ 2] \circ [1\ i] = [1\ i\ 2]$ έχει τάξη 3. (Βλ. (3.3) και 3.2.3 (v)). Φυσικά, *και* η εικόνα της $[\alpha_2\ \beta_2] \circ [\alpha_i\ \beta_i]$ μέσω τού αυτομορφισμού ϑ έχει τάξη 3. (Βλ. 2.4.19 (iii).) Αυτό σημαίνει ότι[6] $\{\alpha_2, \beta_2\} \cap \{\alpha_i, \beta_i\} \neq \varnothing$, δηλαδή ότι είτε $\alpha_i \in \{\alpha_2, \beta_2\}$ είτε $\beta_i \in \{\alpha_2, \beta_2\}$. Εναλλάσσοντας εν ανάγκη τα α_i και β_i μπορούμε δίχως βλάβη τής γενικότητας να υποθέσουμε (από εδώ και στο εξής) ότι $\alpha_i \in \{\alpha_2, \beta_2\}$ για κάθε $i \in \{3, ..., n\}$.

Ισχυρισμός: Είτε $\alpha_i = \alpha_2, \forall i \in \{3, ..., n\}$, είτε $\alpha_i = \beta_2, \forall i \in \{3, ..., n\}$. Όταν $n = 3$, αυτός είναι προδήλως αληθής. Για την επαλήθευσή του όταν $n \geq 4$ θα χρησιμοποιήσουμε «εις άτοπον απαγωγή». Υποθέτουμε ότι $n \geq 4$ και ότι υπάρχουν $i, j \in \{3, ..., n\}$, $i \neq j$, τέτοιοι ώστε να ισχύει $\alpha_i = \alpha_2$ και $\alpha_j = \beta_2$. Εν προκειμένω, έχουμε αφ' ενός μεν $\alpha_2 \neq \beta_i$, $\beta_2 \neq \beta_j$ (εξ υποθέσεως), αφ' ετέρου δε $\alpha_2 \neq \beta_j$ και $\beta_i \neq \beta_j$. (Πράγματι· επειδή η σύνθεση $[1\ 2] \circ [1\ i] \circ [1\ j] = [1\ j\ i\ 2]$ έχει τάξη 4 (βλ. (3.3) και 3.2.3 (v)), *και* η εικόνα της

$$\begin{aligned} &\vartheta([1\ 2] \circ [1\ i] \circ [1\ j]) = \vartheta([1\ 2])\vartheta([1\ i])\vartheta([1\ j]) \\ &= [\alpha_2\ \beta_2] \circ [\alpha_i\ \beta_i] \circ [\alpha_j\ \beta_j] = [\alpha_2\ \beta_2] \circ [\alpha_2\ \beta_i] \circ [\beta_2\ \beta_j] \\ &= [\alpha_2\ \beta_i\ \beta_2] \circ [\beta_2\ \beta_j] = \left\{ \begin{array}{ll} [\beta_2\ \beta_i], & \text{όταν } \alpha_2 = \beta_j \text{ και } \beta_i \neq \beta_j, \\ [\alpha_2\ \beta_i], & \text{όταν } \alpha_2 \neq \beta_j \text{ και } \beta_i = \beta_j, \\ [\alpha_2\ \beta_i\ \beta_2\ \beta_j], & \text{όταν } \alpha_2 \neq \beta_j \text{ και } \beta_i \neq \beta_j, \end{array} \right. \end{aligned}$$

μέσω τού ϑ οφείλει, λόγω τού (iii) τής προτάσεως 2.4.19, να έχει τάξη 4. Αυτό σημαίνει ότι $\alpha_2 \neq \beta_j$ και $\beta_i \neq \beta_j$.) Επιπροσθέτως, η $[1\ i\ 2] \circ [1\ j\ 2] = [1\ j] \circ [2\ i]$ έχει τάξη 2. (Βλ. 3.2.10.) Συνεπώς *και* η εικόνα της μέσω τού ϑ οφείλει, λόγω τού (iii) τής προτάσεως 2.4.19, να έχει τάξη 2. Όμως η

$$\vartheta([1\ i\ 2] \circ [1\ j\ 2]) = \vartheta([1\ i\ 2]) \circ \vartheta([1\ j\ 2]) = [\alpha_2\ \beta_2] \circ [\alpha_i\ \beta_i] \circ [\alpha_2\ \beta_2] \circ [\alpha_j\ \beta_j]$$

$$= [\alpha_2\ \beta_2] \circ [\alpha_2\ \beta_i] \circ [\alpha_2\ \beta_2] \circ [\beta_2\ \beta_j] = [\alpha_2\ \beta_i\ \beta_2] \circ [\alpha_2\ \beta_2\ \beta_j] = [\beta_2\ \beta_j\ \beta_i]$$

[6] Εάν ίσχυε $\{\alpha_2, \beta_2\} \cap \{\alpha_i, \beta_i\} = \varnothing$, τότε θα είχαμε $\mathrm{ord}([\alpha_2\ \beta_2] \circ [\alpha_i\ \beta_i]) = 2$ (βλ. 3.2.10).

έχει τάξη 3. (Βλ. (3.3), (3.2) και 3.2.10.) Άτοπο! Άρα ο ισχυρισμός είναι αληθής και για $n \geq 4$.

Στην περίπτωση όπου $\alpha_i = \alpha_2$ (και αντιστοίχως, στην περίπτωση όπου $\alpha_i = \beta_2$) για κάθε $i \in \{3, ..., n\}$, λαμβάνουμε

$$\vartheta([1\ i]) = [\alpha_2\ \beta_i],\ \text{με}\ \alpha_2 \neq \beta_i,\ \forall i \in \{2, 3, ..., n\}.$$

(και αντιστοίχως, $\vartheta([1\,2]) = [\alpha_2\ \beta_2] = [\beta_2\ \alpha_2]$ και $\vartheta([1\ i]) = [\beta_2\ \beta_i]$, με $\beta_i \neq \beta_2$, $\forall i \in \{3, ..., n\}$.) Από την ενριπτικότητα τού ϑ συμπεραίνουμε ότι

$$i \neq j \Rightarrow [1\ i] \neq [1\ j] \Rightarrow \vartheta([1\ i]) = [\alpha_2\ \beta_i] \neq [\alpha_2\ \beta_j] = \vartheta([1\ j]) \Rightarrow \beta_i \neq \beta_j$$

για κάθε $(i, j) \in \{2, 3, ..., n\} \times \{2, 3, ..., n\}$ (και αντιστοίχως, ότι

$$i \neq j \Rightarrow [1\ i] \neq [1\ j] \Rightarrow \vartheta([1\ i]) = [\beta_2\ \beta_i] \neq [\beta_2\ \beta_j] = \vartheta([1\ j]) \Rightarrow \beta_i \neq \beta_j$$

για κάθε $(i, j) \in \{3, ..., n\} \times \{3, ..., n\}$.) Θέτοντας

$$\tau := \begin{bmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ \alpha_2 & \beta_2 & \beta_3 & \beta_4 & \cdots & \beta_n \end{bmatrix}$$

$$\left(\text{και αντιστοίχως, } \tau := \begin{bmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ \beta_2 & \alpha_2 & \beta_3 & \beta_4 & \cdots & \beta_n \end{bmatrix}\right),$$

παρατηρούμε (κάνοντας χρήση τού (vii) τής προτάσεως 3.2.3) ότι

$$\vartheta([1\ i]) = [\alpha_2\ \beta_i] = [\tau(1)\ \tau(i)] = \tau \circ [1\ i] \circ \tau^{-1},\ \forall i \in \{2, 3, ..., n\}.$$

(και αντιστοίχως, ότι $\vartheta([1\,2]) = [\beta_2\ \alpha_2] = \tau \circ [1\ 2] \circ \tau^{-1}$ και

$$\vartheta([1\ i]) = [\beta_2\ \beta_i] = \tau \circ [1\ i] \circ \tau^{-1}$$

για κάθε $i \in \{3, ..., n\}$). Επειδή $\mathfrak{S}_n = \langle\{[1\ i]\ \mid\ i \in \{2, ..., n\}\}\rangle$ (σύμφωνα με το (i) τού πορίσματος 3.2.13), για κάθε $\sigma \in \mathfrak{S}_n$ υπάρχει κάποιος $k \in \{1, ..., n-1\}$ και $\lambda_\varrho \in \{2, ..., n\}$, $\varrho \in \{1, ..., k\}$, ούτως ώστε να ισχύει

$$\sigma = [1\ \lambda_1]^{\varepsilon_1} \circ [1\ \lambda_2]^{\varepsilon_2} \circ \cdots \circ [1\ \lambda_k]^{\varepsilon_k}$$

για κάποιους ε_1,..., $\varepsilon_k \in \{\pm 1\}$. (Βλ. (2.6).) Κατά συνέπειαν[7],

$$\sigma = [1\ \lambda_1] \circ [1\ \lambda_2] \circ \cdots \circ [1\ \lambda_k] \Rightarrow \vartheta(\sigma) = \vartheta([1\ \lambda_1]) \circ \vartheta([1\ \lambda_2]) \circ \cdots \circ \vartheta([1\ \lambda_k])$$

$$\Rightarrow \vartheta(\sigma) = (\tau \circ [1\ \lambda_1] \circ \tau^{-1}) \circ (\tau \circ [1\ \lambda_2] \circ \tau^{-1}) \circ \cdots \circ (\tau \circ [1\ \lambda_k] \circ \tau^{-1}) = \tau \circ \sigma \circ \tau^{-1},$$

οπότε $\vartheta \in \mathrm{Inn}(\mathfrak{S}_n)$.

(ii)⇒(i) Επειδή κάθε $\vartheta \in \mathrm{Inn}(\mathfrak{S}_n)$ απεικονίζει κάθε στοιχείο τής $\mathfrak{S}_n$ σε ένα συζυγές του, τούτο έπεται από την πρόταση 5.1.8 και από το θεώρημα 5.3.6. □

[7] Προφανώς, $\mathrm{ord}([1\ \lambda_\varrho]) = 2 \Rightarrow [1\ \lambda_\varrho]^{\varepsilon_\varrho} = [1\ \lambda_\varrho], \forall \varrho \in \{1, ..., k\}$.

6.3.5 Θεώρημα. (O. Hölder, 1895) *Οι συμμετρικές ομάδες* $(\mathfrak{S}_n, \circ)$ *είναι πλήρεις όταν* $n \geq 3$ *και* $n \neq 6$.

ΑΠΟΔΕΙΞΗ. Ως γνωστόν, $Z(\mathfrak{S}_n) = \{\mathrm{id}\}$ για κάθε $n \geq 3$ (βλ. 5.4.9). Αρκεί λοιπόν να αποδειχθεί ότι $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Inn}(\mathfrak{S}_n)$ όταν $n \geq 3$ και $n \neq 6$. Έστω τυχών αυτομορφισμός $\vartheta \in \mathrm{Aut}(\mathfrak{S}_n)$ και έστω $\mathcal{C}_k$ η κλάση συζυγίας τής $\mathfrak{S}_n$ η περιέχουσα εκείνες τις μετατάξεις που γράφονται ως συνθέσεις k ανά δύο ξένων μεταξύ τους αντιμεταθέσεων, για κάποιον παγιωμένο $k \leq \frac{n}{2}$. Σύμφωνα με το θεώρημα 5.3.6 και το (ii) τού θεωρήματος 5.3.16,

$$\mathcal{C}_k = \{\, \sigma \in \mathfrak{S}_n \,|\, \mathbf{tp}(\sigma) = (\underbrace{1, ..., 1}_{n-2k \text{ φορές}}, \underbrace{2, ..., 2}_{k \text{ φορές}})\} \underset{(5.21)}{\Longrightarrow} \mathrm{card}(\mathcal{C}_k) = \frac{n!}{2^k k!(n-2k)!}.$$

Ο ϑ (κατά την πρόταση 5.1.8) απεικονίζει κάθε κλάση συζυγίας τής $\mathfrak{S}_n$ σε μια κλάση συζυγίας τής $\mathfrak{S}_n$. Ειδικότερα, η εικόνα τής κλάσεως συζυγίας $\mathcal{C}_1$ (τής απαρτιζομένης από όλες τις αντιμεταθέσεις τής $\mathfrak{S}_n$) μέσω τού ϑ είναι μια κλάση συζυγίας περιέχουσα μόνον στοιχεία τάξεως 2. (Βλ. 2.4.19 (iv).) Δυνάμει τού λήμματος 6.3.3, $\vartheta(\mathcal{C}_1) = \mathcal{C}_k$ για κάποιον $k \in \mathbb{N}$, $1 \leq k \leq \frac{n}{2}$. Κατά συνέπειαν,

$$\begin{aligned} \tfrac{n!}{2(n-2)!} &= \tfrac{n(n-1)}{2} = \mathrm{card}(\mathcal{C}_1) = \mathrm{card}(\vartheta(\mathcal{C}_1)) \\ &= \mathrm{card}(\mathcal{C}_k) = \tfrac{n!}{2^k k!(n-2k)!} = \tfrac{n(n-1)(n-2)\cdots(n-2k+1)}{2^k k!}. \end{aligned}$$

Εάν $k > 1$, τούτο ισοδυναμεί με την ισότητα

$$(n-2)(n-3)\cdots(n-2k+1) = 2^{k-1}k!. \tag{6.4}$$

Επειδή $n \geq 3$, η (6.4) δεν μπορεί να είναι αληθής όταν[8] $k = 2$. Επίσης, για $k = 3$ η (6.4) επαληθεύεται μόνον όταν[9] $n = 6$. (Όμως, *εξ υποθέσεως*, $n \neq 6$.) Αλλά ακόμη και για $k \geq 4$ έχουμε[10]

$$n \geq 2k \Rightarrow \prod_{j=3}^{2k}(n-j+1) \geq \prod_{j=3}^{2k}(2k-j+1) = (2k-2)! > 2^{k-1}k!.$$

Τελικό συμπέρασμα: $k = 1 \Rightarrow \vartheta(\mathcal{C}_1) = \mathcal{C}_1$ και, ως εκ τούτου, η εικόνα οιασδήποτε αντιμεταθέσεως μέσω τού ϑ είναι μια αντιμετάθεση. Σύμφωνα με το λήμμα 6.3.4, $\vartheta \in \mathrm{Inn}(\mathfrak{S}_n)$. □

[8] Εν τοιαύτη περιπτώσει, το δεξιό μέλος τής (6.4) ισούται με 4, ενώ το αριστερό της μέλος ισούται με 0 όταν $n = 3$, με 2 όταν $n = 4$, και είναι ≥ 6 όταν $n \geq 5$.

[9] Για $k = 3$ το δεξιό μέλος τής (6.4) ισούται με 24, ενώ το αριστερό της μέλος ισούται με 0 όταν $n \in \{3, 4, 5\}$ και είναι ≥ 120 όταν $n \geq 7$.

[10] Το ότι ισχύει η ανισότητα $(2k-2)! > 2^{k-1}k!$ για κάθε $k \geq 4$ αποδεικνύεται επαγωγικώς. Για $k = 4$ λαμβάνουμε $720 > 192$. Εάν υποθέσουμε ότι αυτή είναι αληθής για κάποιον $k \geq 4$, τότε

$$(2(k+1)-2)! = (2k)! = (2k-2)!(2k-1)2k > 2^{k-1}k!(2k-1)2k = 2^k k!(2k-1)k > 2^k(k+1)!,$$

όπου η τελευταία ανισότητα έπεται από το ότι

$$2(k-1)k \geq 2 \cdot 3 \cdot 4 = 24 > 1 \Rightarrow (2k-1)k > k+1 \Rightarrow k!(2k-1)k > k!(k+1) = (k+1)!.$$

6.3.6 Πόρισμα. $\mathrm{Aut}(\mathfrak{S}_n) \cong \mathfrak{S}_n$ *όταν* $n \geq 3$ *και* $n \neq 6$.

► **Τι συμβαίνει με τις ομάδες** $\mathfrak{S}_6$ **και** $\mathfrak{A}_n$; Όπως θα δούμε (ύστερα από κάποια απαραίτητη προεργασία) στα θεωρήματα 6.3.8, 6.3.18 και 6.3.19, τόσον η *ειδική* συμμετρική ομάδα $\mathfrak{S}_6$ όσον και οι εναλλάσσουσες ομάδες $\mathfrak{A}_n$, $n \geq 4$, *δεν* είναι πλήρεις (παρά το γεγονός ότι τα κέντρα τους είναι τετριμμένα).

6.3.7 Λήμμα. $|\mathrm{Out}(\mathfrak{S}_6)| \leq 2$. *Κατά συνέπειαν, υπάρχει το πολύ ένας εξωτερικός αυτομορφισμός τής* $\mathfrak{S}_6$ *που είναι* $\neq e_{\mathrm{Out}(\mathfrak{S}_6)} (= \mathrm{id}_{\mathfrak{S}_6} \circ \mathrm{Inn}(\mathfrak{S}_6))$.

ΑΠΟΔΕΙΞΗ. Έστω τυχών αυτομορφισμός $\vartheta \in \mathrm{Aut}(\mathfrak{S}_6)$ και έστω $\mathcal{C}_k$ η κλάση συζυγίας τής $\mathfrak{S}_6$ η περιέχουσα εκείνες τις μετατάξεις που γράφονται ως συνθέσεις k ανά δύο ξένων μεταξύ τους αντιμεταθέσεων, για κάποιον παγιωμένο $k \in \{1, 2, 3\}$. Ως γνωστόν, $\mathrm{card}(\mathcal{C}_1) = \mathrm{card}(\mathcal{C}_3) = 15$ και $\mathrm{card}(\mathcal{C}_2) = 45$. (Βλ. (5.21) ή τον κατάλογο τού εδαφίου 5.3.17). Ο ϑ (κατά την πρόταση 5.1.8) απεικονίζει κάθε κλάση συζυγίας τής $\mathfrak{S}_6$ σε μια κλάση συζυγίας τής $\mathfrak{S}_6$. Ειδικότερα, $\vartheta(\mathcal{C}_2) = \mathcal{C}_2$ και

$$\text{είτε } \ [\vartheta(\mathcal{C}_1) = \mathcal{C}_1 \ \text{ και } \ \vartheta(\mathcal{C}_3) = \mathcal{C}_3] \ \text{ είτε } \ [\vartheta(\mathcal{C}_1) = \mathcal{C}_3 \ \text{ και } \ \vartheta(\mathcal{C}_3) = \mathcal{C}_1] \,.$$

(Βλ. 2.4.19 (iv) και 6.3.3.) Στην πρώτη περίπτωση, η εικόνα οιασδήποτε αντιμεταθέσεως μέσω τού ϑ είναι μια αντιμετάθεση, οπότε $\vartheta \in \mathrm{Inn}(\mathfrak{S}_6)$ (δυνάμει τού λήμματος 6.3.4). Στη δεύτερη περίπτωση, $\vartheta \in \mathrm{Aut}(\mathfrak{S}_6) \setminus \mathrm{Inn}(\mathfrak{S}_6)$ (και πάλι λόγω τού λήμματος 6.3.4). Επιπροσθέτως, για *οιονδήποτε* $\vartheta' \in \mathrm{Aut}(\mathfrak{S}_6) \setminus \mathrm{Inn}(\mathfrak{S}_6)$ έχουμε κατ' ανάγκην $\vartheta'(\mathcal{C}_1) = \mathcal{C}_3$ και

$$\vartheta^{-1}\left(\vartheta'(\mathcal{C}_1)\right) = \vartheta^{-1}(\mathcal{C}_3) = \mathcal{C}_1 \Longrightarrow \vartheta^{-1} \circ \vartheta' \in \mathrm{Inn}(\mathfrak{S}_6) \Rightarrow \vartheta' \in \vartheta \circ \mathrm{Inn}(\mathfrak{S}_6),$$

οπότε

$$\mathrm{Aut}(\mathfrak{S}_6) = \mathrm{Inn}(\mathfrak{S}_6) \coprod (\vartheta \circ \mathrm{Inn}(\mathfrak{S}_6)) \tag{6.5}$$

και $|\mathrm{Out}(\mathfrak{S}_6)| = 2 \underset{2.3.19}{\Longrightarrow} \mathrm{Out}(\mathfrak{S}_6) \cong \mathbb{Z}_2$. (Εκ των ανωτέρω έπεται μόνον ότι $|\mathrm{Out}(\mathfrak{S}_6)| \leq 2$. Εν συνεχεία, στο θεώρημα 6.3.8 θα αποδείξουμε ότι αυτή η σχέση ισχύει ως ισότητα.) □

6.3.8 Θεώρημα. (O. Hölder, 1895) *Υπάρχει ακριβώς ένας εξωτερικός αυτομορφισμός τής* $\mathfrak{S}_6$ *που είναι* $\neq e_{\mathrm{Out}(\mathfrak{S}_6)} (= \mathrm{id}_{\mathfrak{S}_6} \circ \mathrm{Inn}(\mathfrak{S}_6))$, *οπότε* $\mathrm{Out}(\mathfrak{S}_6) \cong \mathbb{Z}_2$ *και* $|\mathrm{Aut}(\mathfrak{S}_6)| = 1440$.

ΑΠΟΔΕΙΞΗ[11]. Αρκεί (επί τη βάσει των προαναφερθέντων στην απόδειξη τού λήμματος 6.3.7) να αποδείξουμε ότι υπάρχει τουλάχιστον *ένας* μη εσωτερικός αυτομορφισμός ϑ τής $\mathfrak{S}_6$. (Εν τοιαύτη περιπτώσει, ο ζητούμενος μοναδικός εξωτερικός αυτομορφισμός $\neq e_{\mathrm{Out}(\mathfrak{S}_6)}$ τής $\mathfrak{S}_6$ θα είναι η πλευρική κλάση $\vartheta \circ \mathrm{Inn}(\mathfrak{S}_6)$.)

[11] Η αρχικώς δοθείσα απόδειξη τού Hölder είναι κατά τι διαφορετική. Η απόδειξη που παρατίθεται εδώ είναι βασισμένη σε μια ελαφρά παραλλαγή κάποιων υπολογισμών που έχουν δημοσιευθεί στα εξής άρθρα:

• D.W. Miller: *On a Theorem of Hölder*, American Math. Monthly **65** (1958), 252-254.

• P.J. Lorimer: *The Outer Automorphisms of* $\mathfrak{S}_6$, American Math. Monthly **73** (1966), 642-643.

Για λεπτομερείς (αλγεβρικές και γεωμετρικές) περιγραφές των 1440 στοιχείων τής ομάδας $\mathrm{Aut}(\mathfrak{S}_6)$, βλ.

• G. Janusz & J.J. Rotman: *Outer Automorphisms of* $\mathfrak{S}_6$, American Math. Monthly **89** (1982), 407-410,

• Th.A. Fournelle: *Symmetries of the Cube and Outer Automorphisms of* $\mathfrak{S}_6$, American Math. Monthly **100** (1993), 377-380,

Ως γνωστόν, $\mathfrak{S}_6 = \langle [1\ 2], [2\ 3], [3\ 4], [4\ 5], [5\ 6] \rangle$. (Βλ. 3.2.13 (ii).) Ορίζοντας τις μετατάξεις $\sigma_1 := [1\ 2] \circ [3\ 4] \circ [5\ 6]$ και

$$\sigma_2 := [1\ 4] \circ [2\ 5] \circ [3\ 6], \quad \sigma_3 := [1\ 3] \circ [2\ 4] \circ [5\ 6],$$

$$\sigma_4 := [1\ 2] \circ [3\ 6] \circ [4\ 5], \quad \sigma_5 := [1\ 4] \circ [2\ 3] \circ [5\ 6]$$

(τις ανήκουσες στην κλάση συζυγίας $\mathcal{C}_3$) παρατηρούμε ότι $\sigma_i^2 = \mathrm{id}$, $\forall i \in \{1, ..., 5\}$,

$$(\sigma_i \circ \sigma_j)^2 = \mathrm{id} \ \text{ για } i, j \in \{1, .., 5\} \text{ με } |i - j| \geq 2 \text{ και } (\sigma_i \circ \sigma_{i+1})^3 = \mathrm{id}, \forall i \in \{1, .., 4\}.$$

Επειδή $\sigma_3 \circ \sigma_5 \circ \sigma_1 = [5\ 6], \sigma_1 \circ \sigma_2 \circ \sigma_4 = [1\ 6\ 5\ 2\ 3\ 4]$ και $\sigma_2 \circ \sigma_3 \circ \sigma_4 = [2\ 6\ 4\ 3]$, λαμβάνουμε

$$\begin{aligned} [2\ 3] &= (\sigma_1 \circ \sigma_2 \circ \sigma_4)^2 \circ (\sigma_3 \circ \sigma_5 \circ \sigma_1) \circ (\sigma_1 \circ \sigma_2 \circ \sigma_4)^{-2}, \\ [3\ 4] &= (\sigma_1 \circ \sigma_2 \circ \sigma_4)^3 \circ (\sigma_3 \circ \sigma_5 \circ \sigma_1) \circ (\sigma_1 \circ \sigma_2 \circ \sigma_4)^{-3}, \\ [4\ 5] &= (\sigma_2 \circ \sigma_3 \circ \sigma_4) \circ (\sigma_3 \circ \sigma_5 \circ \sigma_1) \circ (\sigma_2 \circ \sigma_3 \circ \sigma_4)^{-1} \end{aligned}$$

και

$$\begin{aligned} &[1\ 2] = \sigma_1 \circ [5\ 6] \circ [3\ 4] \\ &= \sigma_1 \circ (\sigma_3 \circ \sigma_5 \circ \sigma_1) \circ (\sigma_1 \circ \sigma_2 \circ \sigma_4)^3 \circ (\sigma_3 \circ \sigma_5 \circ \sigma_1) \circ (\sigma_1 \circ \sigma_2 \circ \sigma_4)^{-3}, \end{aligned}$$

οπότε κάθε αντιμετάθεση τής μορφής $[j\ \ j+1]$ (όπου $j \in \{1, ..., 5\}$) μπορεί να γραφεί ως σύνθεση (πεπερασμένου πλήθους) μετατάξεων που ανήκουν στο σύνολο $\{\sigma_1, ..., \sigma_5\}$. Αυτό σημαίνει ότι $\mathfrak{S}_6 = \langle \sigma_1, ..., \sigma_5 \rangle$. Είναι εύκολος ο έλεγχος τού ότι η απεικόνιση

$$\mathfrak{S}_6 \ni [\xi_1\ \ \xi_1 + 1]^{\varepsilon_1} \circ \cdots \circ [\xi_5\ \ \xi_5 + 1]^{\varepsilon_5} \longmapsto \sigma_{\xi_1}^{\varepsilon_1} \circ \cdots \circ \sigma_{\xi_5}^{\varepsilon_5} \in \mathfrak{S}_6,$$

(όπου τα μέλη τής διατεταγμένης πεντάδας $(\xi_1,..., \xi_5)$ συμβολίζουν οιαδήποτε αναδιάταξη των μελών τής διατεταγμένης πεντάδας $(1,..., 5)$ και $(\varepsilon_1,..., \varepsilon_5) \in \mathbb{Z}^5$) αποτελεί έναν αυτομορφισμό ϑ τής $\mathfrak{S}_6$ τάξεως 2. Προφανώς, $\vartheta([j\ \ j+1]) = \sigma_j$ για κάθε $j \in \{1, ..., 5\}$ και $\vartheta(\mathcal{C}_1) = \mathcal{C}_3$, οπότε $\vartheta \in \mathrm{Aut}(\mathfrak{S}_6) \setminus \mathrm{Inn}(\mathfrak{S}_6)$ και η (6.5) δίδει

$$2 = |\mathrm{Out}(\mathfrak{S}_6)| = \tfrac{|\mathrm{Aut}(\mathfrak{S}_6)|}{|\mathrm{Inn}(\mathfrak{S}_6)|} = \tfrac{|\mathrm{Aut}(\mathfrak{S}_6)|}{|\mathfrak{S}_6|} = \tfrac{|\mathrm{Aut}(\mathfrak{S}_6)|}{6!},$$

απ' όπου έπεται ότι $\mathrm{Out}(\mathfrak{S}_6) \cong \mathbb{Z}_2$ και $|\mathrm{Aut}(\mathfrak{S}_6)| = 1440$. □

6.3.9 Παρατήρηση. Επειδή η $\mathfrak{S}_1$ είναι τετριμμένη και $\mathfrak{S}_2 \cong \mathbb{Z}_2$, μέσω των προαναφερθέντων στα εδάφια 5.4.9 και 5.4.30 (iii), και των αποδειχθέντων στα θεωρήματα 2.4.32, 6.3.5 και 6.3.8, καταλήγουμε στον ακόλουθο ολοκληρωμένο κατάλογο:

n	$Z(\mathfrak{S}_n)$	$\mathrm{Aut}(\mathfrak{S}_n)$	$\mathrm{Inn}(\mathfrak{S}_n)$	$\mathrm{Out}(\mathfrak{S}_n)$
1	$\{\mathrm{id}\}$	$\{\mathrm{id}_{\mathfrak{S}_1}\}$	$\{\mathrm{id}_{\mathfrak{S}_1}\}$	τετριμμένη
2	$\mathbb{Z}_2$	$\{\mathrm{id}_{\mathfrak{S}_2}\}$	$\{\mathrm{id}_{\mathfrak{S}_2}\}$	τετριμμένη
≥ 3 και $\neq 6$	$\{\mathrm{id}\}$	$\mathfrak{S}_n$	$\mathfrak{S}_n$	τετριμμένη
6	$\{\mathrm{id}\}$	$\mathfrak{S}_6 \rtimes \mathbb{Z}_2$	$\mathfrak{S}_6$	$\langle \vartheta \circ \mathrm{Inn}(\mathfrak{S}_6) \rangle \cong \mathbb{Z}_2$

• T.Y. Lam & D.B. Leep: *Combinatorial Structure of the Automorphism Group of* $\mathfrak{S}_6$, Expositiones Mathematicae **11** (1993), no. 4, 289-308,

• J.J. Rotman: *An Introduction to the Theory of Groups*, GTM, Vol. **148**, fourth ed., Springer-Verlag, (1995), σελ. 159-162, και

• B. Howard, J. Millson, A. Snowden & R. Vakil: *A description of the outer automorphism of* $\mathfrak{S}_6$ *and the invariants of six points in projective space*, Journal of Combinatorial Theory, Series A, **115** (2008), 1296-1303.

[Για $n \geq 3$ έχουμε $Z(\mathfrak{S}_n) = \{\mathrm{id}\}$ και ταυτίζουμε την ομάδα $\mathrm{Inn}(\mathfrak{S}_n)$ με την ίδια την $\mathfrak{S}_n$ μέσω τού ισομορφισμού $\mathfrak{S}_n \cong \mathfrak{S}_n/\{\mathrm{id}\} \xrightarrow{\cong} \mathrm{Inn}(\mathfrak{S}_n)$. (Βλ. 5.4.28.) Για $n = 6$ έχουμε (λόγω τής (6.5))

$$\mathrm{Aut}(\mathfrak{S}_6) = \langle\vartheta\rangle \circ \mathrm{Inn}(\mathfrak{S}_6) = \mathrm{Inn}(\mathfrak{S}_6) \circ \langle\vartheta\rangle = \langle \mathrm{Inn}(\mathfrak{S}_6), \langle\vartheta\rangle\rangle\,,$$

όπου ϑ οιοσδήποτε μη εσωτερικός αυτομορφισμός τής ομάδας $\mathfrak{S}_6$ (κατ' ανάγκην τάξεως 2), όπως είναι, π.χ., εκείνος που κατασκευάσαμε στο θεώρημα 6.3.8. Επειδή $\mathrm{Inn}(\mathfrak{S}_6) \cap \langle\vartheta\rangle = \{\mathrm{id}\}$, η ομάδα $\langle \mathrm{Inn}(\mathfrak{S}_6), \langle\vartheta\rangle\rangle$ αποτελεί το λεγόμενο *εσωτερικό ημιευθύ γινόμενο* των $\mathrm{Inn}(\mathfrak{S}_6) \cong \mathfrak{S}_6$ και $\langle\vartheta\rangle \cong \mathbb{Z}_2$, συμβολιζόμενο ιδιαιτέρως ως $\mathfrak{S}_6 \rtimes \mathbb{Z}_2$. (Βλ. εδ. 7.6.43.)]

6.3.10 Λήμμα. *Έστω $n \in \mathbb{N}$, $n \geq 3$. Εάν $\sigma \in \mathfrak{S}_n$, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) $\mathrm{ord}(\sigma) = 3$.

(ii) $\sigma = c_1 \circ c_2 \circ \cdots \circ c_k$, *όπου οι* $c_1, c_2, ..., c_k$ *είναι* k *ανά δύο ξένοι* 3*-κύκλοι για κάποιον* k, $1 \leq k \leq \frac{n}{3}$.

ΑΠΟΔΕΙΞΗ. Προφανώς, $\mathrm{ord}(\sigma) = 1 \Leftrightarrow \sigma = \mathrm{id}$. Γι' αυτόν τον λόγο μπορούμε δίχως βλάβη τής γενικότητας να υποθέσουμε ότι $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{id}\}$. Η σ μπορεί (επί τη βάσει τού θεωρήματος 3.2.7) να γραφεί υπό τη μορφή $\sigma = c_1 \circ c_2 \circ \cdots \circ c_k$ επαλλήλων συνθέσεων ανά δύο ξένων μεταξύ τους κύκλων $c_1, c_2, ..., c_k$ μήκους ≥ 2. (Αυτή η έκφραση είναι *μονοσημάντως ορισμένη* μέχρις αναδιατάξεως των μετεχόντων κύκλων.) Εάν l_j είναι το μήκος τού c_j για κάθε $j \in \{1, ..., k\}$, τότε $\mathrm{ord}(\sigma) = l_1$ όταν $k = 1$ και $\mathrm{ord}(\sigma) = \mathrm{εκπ}(l_1, ..., l_k)$ όταν $k \geq 2$ (βλ. 3.2.10). Επειδή για $k \geq 2$ έχουμε

$$\left\{ \begin{array}{c} \mathrm{εκπ}(l_1, ..., l_k) = 3, \\ \text{όπου } l_1 \geq 2, ..., l_k \geq 2 \end{array} \right\} \Longleftrightarrow l_1 = \cdots = l_k = 3,$$

η ισοδυναμία των συνθηκών (i) και (ii) είναι προφανής. □

6.3.11 Λήμμα. (i) *Εάν $n \in \mathbb{N}$, $n \geq 5$, και εάν $c \in \mathfrak{A}_n$ είναι ένας* 3*-κύκλος*[12]*, τότε* $\mathrm{ΚΛΣ}_{\mathfrak{A}_n}(c) = \mathrm{ΚΛΣ}_{\mathfrak{S}_n}(c)$.

(ii) *Εάν $n \in \mathbb{N}$, $n \geq 6$, και εάν $\sigma = c_1 \circ \cdots \circ c_k \in \mathfrak{A}_n$ είναι η σύνθεση k ανά δύο ξένων μεταξύ τους* 3*-κύκλων* $c_1, ..., c_k$, *όπου* $2 \leq k \leq \frac{n}{3}$, *τότε* $\mathrm{ΚΛΣ}_{\mathfrak{A}_n}(\sigma) = \mathrm{ΚΛΣ}_{\mathfrak{S}_n}(\sigma)$.

ΑΠΟΔΕΙΞΗ. (i) Προφανώς, $\mathbf{tp}(c) = (\underbrace{1, ..., 1}_{n-3 \text{ φορές}}, 3)$. Επειδή $n - 3 \geq 2$, η ισότητα $\mathrm{ΚΛΣ}_{\mathfrak{A}_n}(c) = \mathrm{ΚΛΣ}_{\mathfrak{S}_n}(c)$ έπεται από το (ii) τού θεωρήματος 5.3.19.

(ii) Προφανώς, $\mathbf{tp}(\sigma) = (\underbrace{1, ..., 1}_{n-3k \text{ φορές}}, \underbrace{3, ..., 3}_{k \text{ φορές}})$. Επειδή (εξ υποθέσεως) $k \geq 2$, η ισότητα $\mathrm{ΚΛΣ}_{\mathfrak{A}_n}(\sigma) = \mathrm{ΚΛΣ}_{\mathfrak{S}_n}(\sigma)$ έπεται και πάλι από το 5.3.19 (ii). □

[12] Κατά το (iii) τού θεωρήματος 3.3.5 *κάθε* 3-κύκλος εντός τής $\mathfrak{S}_n$ (όπου $n \geq 3$) είναι άρτια μετάταξη, οπότε ανήκει στην $\mathfrak{A}_n$.

6.3.12 Σημείωση. Εάν $n \in \mathbb{N}$, $n \geq 4$, τότε η σύνθεση δύο 3-κύκλων ανηκόντων στην $\mathfrak{A}_n$ μπορεί να γραφεί υπό τη μορφή:

(i) $[a\ b\ c] \circ [a\ b\ d] = [a\ c] \circ [b\ d]$,

(ii) $[a\ b\ c] \circ [a\ d\ b] = [a\ d\ c]$,

(iii) $[a\ b\ c] \circ [a\ d\ e] = [a\ b\ c\ d\ e]$, όταν $n \geq 5$, ή

(iv) $[a\ b\ c] \circ [d\ e\ f]$, όταν $n \geq 6$,

όπου τα a, b, c, d, e, f συμβολίζουν σαφώς διακεκριμένα στοιχεία τού $\{1, ..., n\}$. Κατά συνέπειαν, *η σύνθεση δύο 3-κύκλων ανηκόντων στην $\mathfrak{A}_n$ έχει τάξη 2 μόνον στην περίπτωση* (i). Το γεγονός αυτό χρησιμοποιείται κατά τρόπο ουσιαστικό στην απόδειξη τού ακόλουθου λήμματος:

6.3.13 Λήμμα. *Έστω $n \in \mathbb{N}, n \geq 4$, και έστω $\vartheta \in \mathrm{Aut}(\mathfrak{A}_n)$. Εάν η εικόνα οιουδήποτε 3-κύκλου μέσω τού ϑ είναι ένας 3-κύκλος, τότε υπάρχει κάποια μετάταξη $\tau \in \mathfrak{S}_n$, τέτοια ώστε να ισχύει $\vartheta = \boldsymbol{\gamma}_\tau|_{\mathfrak{A}_n}$, όπου $\boldsymbol{\gamma}_\tau : \mathfrak{S}_n \longrightarrow \mathfrak{S}_n,\ \boldsymbol{\gamma}_\tau(\sigma) := \tau \circ \sigma \circ \tau^{-1}$, για κάθε $\sigma \in \mathfrak{S}_n$.* (Βλ. 5.4.21.)

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι $\vartheta([1\ 2\ 3]) = [\alpha_1\ \alpha_2\ \alpha_3], \{\alpha_1, \alpha_2, \alpha_3\} \subsetneqq \{1, ..., n\}$ με $\alpha_1 \neq \alpha_2$, $\alpha_2 \neq \alpha_3$ και $\alpha_3 \neq \alpha_1$. Επειδή η σύνθεση

$$[1\ 2\ 3] \circ [1\ 2\ 4] = [1\ 3] \circ [2\ 4]$$

έχει τάξη 2 (βλ. 3.2.10), *και* η εικόνα της

$$\begin{aligned} [\alpha_1\ \alpha_2\ \alpha_3] \circ \vartheta([1\ 2\ 4]) &= \vartheta([1\ 2\ 3]) \circ \vartheta([1\ 2\ 4]) \\ &= \vartheta([1\ 2\ 3] \circ [1\ 2\ 4]) = \vartheta([1\ 3] \circ [2\ 4]) \end{aligned}$$

μέσω τού αυτομορφισμού ϑ οφείλει να έχει τάξη 2 (βλ. 2.4.19 (iii)). Κατά τα προαναφερθέντα στη σημείωση 6.3.12, $\vartheta([1\ 2\ 4]) = [\alpha_1\ \alpha_2\ \alpha_4]$, για κάποιον $\alpha_4 \in \{1, ..., n\} \setminus \{\alpha_1, \alpha_2, \alpha_3\}$. Εν συνεχεία, για οιονδήποτε $i \in \{5, ..., n\}$ (στην περίπτωση όπου $n \geq 5$) παρατηρούμε ότι η σύνθεση

$$\begin{aligned} [\alpha_1\ \alpha_2\ \alpha_3] \circ \vartheta([1\ 2\ i]) &= \vartheta([1\ 2\ 3]) \circ \vartheta([1\ 2\ i]) \\ &= \vartheta([1\ 2\ 3] \circ [1\ 2\ i]) = \vartheta([1\ 3] \circ [2\ i]) \end{aligned}$$

έχει ωσαύτως τάξη 2, οπότε (εκ νέου βάσει των προαναφερθέντων στη σημείωση 6.3.12)

$$\text{είτε } \vartheta([1\ 2\ i]) = [\alpha_1\ \alpha_2\ \alpha_i] \text{ είτε } \vartheta([1\ 2\ i]) = [\alpha_2\ \alpha_3\ \beta] \text{ είτε } \vartheta([1\ 2\ i]) = [\alpha_3\ \alpha_1\ \delta],$$

όπου $\alpha_i \in \{1, ..., n\} \setminus \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ και $\beta, \delta \in \{1, ..., n\} \setminus \{\alpha_1, \alpha_2, \alpha_3\}$. Τα δύο τελευταία ενδεχόμενα αποκλείονται, διότι εν τοιαύτη περιπτώσει

$$\mathrm{ord}([1\ 2\ 4] \circ [1\ 2\ i]) = \mathrm{ord}([1\ 4] \circ [2\ i]) = 2,$$

αλλά[13] $\mathrm{ord}(\vartheta([1\ 2\ 4] \circ [1\ 2\ i])) \in \{3, 4, 5\}$. Επομένως,

$$\vartheta([1\ 2\ i]) = [\alpha_1\ \alpha_2\ \alpha_i],\ \forall i \in \{3, ..., n\},$$

[13] $[\alpha_1\ \alpha_2\ \alpha_4] \circ [\alpha_2\ \alpha_3\ \beta] = [\alpha_1\ \alpha_2\ \alpha_3\ \beta\ \alpha_4]$ όταν $\beta \neq \alpha_4$ και $[\alpha_1\ \alpha_2\ \alpha_4] \circ [\alpha_2\ \alpha_3\ \alpha_4] = [\alpha_1\ \alpha_2\ \alpha_3]$ όταν $\beta = \alpha_4$. Κατ' αναλογίαν, $[\alpha_1\ \alpha_2\ \alpha_4] \circ [\alpha_3\ \alpha_1\ \delta] = [\alpha_1\ \delta\ \alpha_3\ \alpha_2]$ όταν $\delta \neq \alpha_4$ και $[\alpha_1\ \alpha_2\ \alpha_4] \circ [\alpha_3\ \alpha_1\ \alpha_4] = [\alpha_2\ \alpha_4\ \alpha_3]$ όταν $\delta = \alpha_4$.

όπου $\alpha_i \neq \alpha_j$ για οιουσδήποτε $i, j \in \{3, ..., n\}$ με $i \neq j$ (λόγω τής ενριπτικότητας τού αυτομορφισμού ϑ). Θέτοντας

$$\tau := \begin{bmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \cdots & \alpha_n \end{bmatrix}$$

παρατηρούμε (κάνοντας χρήση τού (vii) τής προτάσεως 3.2.3) ότι

$$\vartheta([1\ 2\ i]) = [\tau(1)\ \tau(2)\ \tau(i)] = \tau \circ [1\ 2\ i] \circ \tau^{-1} = \boldsymbol{\gamma}_\tau|_{\mathfrak{A}_n}([1\ 2\ i])$$

για κάθε $i \in \{3, ..., n\}$. Επειδή $\mathfrak{A}_n = \langle \{[1\ 2\ i] \mid 3 \leq i \leq n\} \rangle$ (σύμφωνα με το (iv) τής προτάσεως 3.3.13), έχουμε

$$\vartheta|_{\{[1\ 2\ i]\ \mid\ 3 \leq i \leq n\}} = \boldsymbol{\gamma}_\tau|_{\{[1\ 2\ i]\ \mid\ 3 \leq i \leq n\}} \Longrightarrow \vartheta = \boldsymbol{\gamma}_\tau|_{\mathfrak{A}_n}$$

επί τη βάσει τού (ii) τής προτάσεως 2.4.9. □

6.3.14 Σημείωση. Εάν $n \in \mathbb{N}$, $n \geq 3$, τότε ορίζεται ένας ομομορφισμός

$$\mathfrak{k} : \mathrm{Aut}(\mathfrak{S}_n) \longrightarrow \mathrm{Aut}(\mathfrak{A}_n),\ \vartheta \longmapsto \mathfrak{k}(\vartheta) := \vartheta|_{\mathfrak{A}_n}. \tag{6.6}$$

(Πράγματι· για κάθε $\vartheta \in \mathrm{Aut}(\mathfrak{S}_n)$ και κάθε $i \in \{3, ..., n\}$ η μετάταξη

$$\vartheta([1\ 2\ i]) = \vartheta|_{\mathfrak{A}_n}([1\ 2\ i]) = \mathfrak{k}(\vartheta)([1\ 2\ i])$$

έχει τάξη 3, οπότε -σύμφωνα με το λήμμα 6.3.10- γράφεται υπό τη μορφή επαλλήλων συνθέσεων (πεπερασμένου πλήθους) ανά δύο ξένων μεταξύ τους 3-κύκλων. Άρα $\mathfrak{k}(\vartheta)([1\ 2\ i]) \in \mathfrak{A}_n$ και, κατ' επέκταση, $\mathfrak{k}(\vartheta)(\mathfrak{A}_n) \subseteq \mathfrak{A}_n$. Βλ. 3.3.13 (iv). Επιπροσθέτως, έχουμε $\mathrm{Ker}(\mathfrak{k}(\vartheta)) = \mathrm{Ker}(\vartheta) \cap \mathfrak{A}_n = \{\mathrm{id}\} \cap \mathfrak{A}_n = \{\mathrm{id}\}$, απ' όπου έπεται ότι $\mathfrak{k}(\vartheta) \in \mathrm{Aut}(\mathfrak{A}_n)$, διότι η $\mathfrak{A}_n$ είναι πεπερασμένη ομάδα. Το ότι η απεικόνιση (6.6) αποτελεί έναν ομομορφισμό ομάδων είναι προφανές.)

6.3.15 Λήμμα. $\mathbf{NSubg}(\mathfrak{S}_4) = \{\{\mathrm{id}\}, \mathbf{V}, \mathfrak{A}_4, \mathfrak{S}_4\}$.

ΑΠΟΔΕΙΞΗ. Έστω H μια μη τετριμμένη ορθόθετη υποομάδα τής $\mathfrak{S}_4$. Η $\mathfrak{S}_4$ έχει τάξη 24 και διαθέτει 5 κλάσεις συζυγίας. (Η πρώτη εξ αυτών περιέχει μόνον την id, η δεύτερη όλες τις αντιμεταθέσεις, η τρίτη όλους τους 3-κύκλους, η τέταρτη όλες τις συνθέσεις δύο ξένων μεταξύ τους αντιμεταθέσεων και η πέμπτη όλους τους 4-κύκλους, με πληθικούς αριθμούς $1, 6, 8, 3$ και 6, αντιστοίχως. Βλ. 5.3.17.) Η υποομάδα $H \neq \{\mathrm{id}\}$ θα ισούται (σύμφωνα με το πόρισμα 5.1.15) με την ένωση *τουλάχιστον δύο* εκ των 5 κλάσεων συζυγίας (με την $\{\mathrm{id}\}$ συμπεριλαμβανόμενη πάντοτε σε αυτές). Εάν η H περιέχει *τουλάχιστον μία* αντιμετάθεση, τότε περιέχει όλες τις αντιμεταθέσεις (ήτοι τη δεύτερη κλάση συζυγίας καθ' ολοκληρίαν), οπότε $H = \mathfrak{S}_4$. (Βλ. 3.2.12.) Εάν η H περιέχει *τουλάχιστον έναν* 3-κύκλο, τότε περιέχει όλους τους 3-κύκλους (ήτοι την τρίτη κλάση συζυγίας καθ' ολοκληρίαν), οπότε $H \in \{\mathfrak{A}_4, \mathfrak{S}_4\}$, καθώς οι 3-κύκλοι παράγουν την $\mathfrak{A}_4$ και δεν υπάρχει καμία γνήσια υποομάδα τής $\mathfrak{S}_4$ περιέχουσα *γνησίως* την $\mathfrak{A}_4$. (Βλ. 4.1.24.) Εάν η H περιέχει *τουλάχιστον έναν* 4-κύκλο $[\alpha_1\ \alpha_2\ \alpha_3\ \alpha_4]$, τότε περιέχει όλους τους 4-κύκλους (ήτοι την

πέμπτη κλάση συζυγίας καθ' ολοκληρίαν) και, ιδιαιτέρως, τον $[\alpha_2\ \alpha_1\ \alpha_3\ \alpha_4]$ και τη σύνθεση αυτών $[\alpha_1\ \alpha_2\ \alpha_3\ \alpha_4]\circ[\alpha_2\ \alpha_1\ \alpha_3\ \alpha_4]=[\alpha_1\ \alpha_4\ \alpha_3]$, η οποία αποτελεί έναν 3-κύκλο. Εν τοιαύτη περιπτώσει η H περιέχει όλους τους 3- και 4-κύκλους, οπότε η H περιέχει *γνησίως* την $\mathfrak{A}_4$ (αφού οι 4-κύκλοι είναι περιττές μετατάξεις) και, ως εκ τούτου, $H=\mathfrak{S}_4$. Τέλος, εάν η H δεν περιέχει καμία αντιμετάθεση, κανέναν 3-κύκλο και κανέναν 4-κύκλο, τότε (ούσα μη τετριμμένη) θα περιέχει *και* τις τρεις συνθέσεις δύο ξένων μεταξύ τους αντιμεταθέσεων (ήτοι την τέταρτη κλάση συζυγίας καθ' ολοκληρίαν), οπότε $H=\mathbf{V}$. □

6.3.16 Λήμμα. $\mathrm{C}_{\mathfrak{S}_n}(\mathfrak{A}_n)=\{\mathrm{id}\}$ *για κάθε* $n\geq 4$.

ΑΠΟΔΕΙΞΗ. Επειδή $\mathfrak{A}_n\lhd\mathfrak{S}_n \underset{5.2.2\,(\mathrm{iii})}{\Longrightarrow} \mathrm{C}_{\mathfrak{S}_n}(\mathfrak{A}_n)\trianglelefteq\mathfrak{S}_n$, συνάγεται ότι

$$\left\{\begin{array}{ll}\mathrm{C}_{\mathfrak{S}_4}(\mathfrak{A}_4)\in\{\{\mathrm{id}\},\mathbf{V},\mathfrak{A}_4,\mathfrak{S}_4\}, & \text{όταν } n=4,\\ \mathrm{C}_{\mathfrak{S}_n}(\mathfrak{A}_n)\in\{\{\mathrm{id}\},\mathfrak{A}_n,\mathfrak{S}_n\}, & \text{όταν } n\geq 5.\end{array}\right\}$$

(Βλ. λήμμα 6.3.15 και θεώρημα 4.3.12.) Για κάθε $n\geq 4$ έχουμε $\mathrm{C}_{\mathfrak{S}_n}(\mathfrak{A}_n)\neq\mathfrak{S}_n$, διότι το κέντρο τής ομάδας $\mathfrak{S}_n$ είναι τετριμμένο. (Βλ. 5.4.9 και 5.4.3 (ii).) Επίσης, για κάθε $n\geq 4$ έχουμε $\mathrm{C}_{\mathfrak{S}_n}(\mathfrak{A}_n)\neq\mathfrak{A}_n$, διότι η $\mathfrak{A}_n$ δεν είναι αβελιανή. (Βλ. 3.3.12 και 5.2.2 (ii).) Τέλος, για $n=4$, $\mathrm{C}_{\mathfrak{S}_4}(\mathfrak{A}_4)\neq\mathbf{V}$, διότι[14] $[1\ 2]\circ[3\ 4]\in\mathbf{V}\smallsetminus\mathrm{C}_{\mathfrak{S}_4}(\mathfrak{A}_4)$. Κατά συνέπειαν, $\mathrm{C}_{\mathfrak{S}_n}(\mathfrak{A}_n)=\{\mathrm{id}\}$ για κάθε $n\geq 4$. □

6.3.17 Λήμμα. *Ο ομομορφισμός* (6.6) *είναι μονομορφισμός (οπότε η* $\mathrm{Aut}(\mathfrak{S}_n)$ *εμφυτεύεται στην* $\mathrm{Aut}(\mathfrak{A}_n)$*) για κάθε* $n\geq 4$.

ΑΠΟΔΕΙΞΗ. Έστω $\vartheta\in\mathrm{Ker}(\mathfrak{k})$, ήτοι ένας $\vartheta\in\mathrm{Aut}(\mathfrak{S}_n)$ με $\vartheta|_{\mathfrak{A}_n}=\mathrm{id}_{\mathfrak{A}_n}$. Αρκεί (λόγω τής προτάσεως 2.4.15) να αποδείξουμε ότι $\vartheta=\mathrm{id}_{\mathfrak{S}_n}$. Έστω τυχούσα μετάταξη $\sigma\in\mathfrak{S}_n$. Θέτουμε $\pi_\sigma:=\sigma^{-1}\circ\vartheta(\sigma)$ και παρατηρούμε ότι $\vartheta(\sigma)=\sigma\circ\pi_\sigma$ και ότι για κάθε $\tau\in\mathfrak{A}_n$ ισχύει $\pi_\tau=\mathrm{id}$ (διότι $\vartheta|_{\mathfrak{A}_n}=\mathrm{id}_{\mathfrak{A}_n}$) και

$$\sigma\circ\pi_\sigma\circ\tau=(\sigma\circ\pi_\sigma)\circ(\tau\circ\ \mathrm{id})=(\sigma\circ\pi_\sigma)\circ(\tau\circ\pi_\tau)=\vartheta(\sigma)\circ\vartheta(\tau)=\vartheta(\sigma\circ\tau)$$
$$=\vartheta((\sigma\circ\tau\circ\sigma^{-1})\circ\sigma)=\vartheta(\sigma\circ\tau\circ\sigma^{-1})\circ\vartheta(\sigma)=\vartheta(\sigma\circ\tau\circ\sigma^{-1})\circ(\sigma\circ\pi_\sigma).$$

Λαμβάνοντας υπ' όψιν ότι

$$\left.\begin{array}{c}\sigma\in\mathfrak{S}_n,\ \tau\in\mathfrak{A}_n\\ \mathfrak{A}_n\lhd\mathfrak{S}_n\end{array}\right\}\Longrightarrow\sigma\circ\tau\circ\sigma^{-1}\in\mathfrak{A}_n\underset{\vartheta|_{\mathfrak{A}_n}=\mathrm{id}_{\mathfrak{A}_n}}{\Longrightarrow}\vartheta(\sigma\circ\tau\circ\sigma^{-1})=\sigma\circ\tau\circ\sigma^{-1},$$

συμπεραίνουμε ότι $\sigma\circ\pi_\sigma\circ\tau=(\sigma\circ\tau\circ\sigma^{-1})\circ(\sigma\circ\pi_\sigma)=\sigma\circ\tau\circ\pi_\sigma$ και, κατ' επέκταση, ότι $[\pi_\sigma\circ\tau=\tau\circ\pi_\sigma,\ \forall\tau\in\mathfrak{A}_n]\Longrightarrow\pi_\sigma\in\mathrm{C}_{\mathfrak{S}_n}(\mathfrak{A}_n)$. Εξ υποθέσεως, $n\geq 4$. Κατά το λήμμα 6.3.16, $\mathrm{C}_{\mathfrak{S}_n}(\mathfrak{A}_n)=\{\mathrm{id}\}$. Επομένως, $\pi_\sigma=\mathrm{id}\Rightarrow\vartheta(\sigma)=\sigma$. Αυτό σημαίνει ότι $\vartheta=\mathrm{id}_{\mathfrak{S}_n}$. □

6.3.18 Θεώρημα. $\mathrm{Aut}(\mathfrak{A}_n)\cong\mathfrak{S}_n$ *όταν* $n\geq 4$ *και* $n\neq 6$.

[14] $[1\ 2]\circ[3\ 4]\in\mathbf{V}$ και $[1\ 2\ 3]\in\mathfrak{A}_4$ αλλά $[1\ 2]\circ[3\ 4]\circ[1\ 2\ 3]=[2\ 4\ 3]$ και $[1\ 2\ 3]\circ[1\ 2]\circ[3\ 4]=[1\ 3\ 4]$.

ΑΠΟΔΕΙΞΗ. Υποθέτοντας ότι $n \geq 4$ και $n \neq 6$, αρκεί να δειχθεί ότι ο (σύμφωνα με το λήμμα 6.3.17) *μονομορφισμός* (6.6) είναι *ισομορφισμός* (και να χρησιμοποιηθεί κατόπιν αυτού το πόρισμα 6.3.6). Προς τούτο θεωρούμε τυχόντα αυτομορφισμό $\vartheta \in \mathrm{Aut}(\mathfrak{A}_n)$ και τυχόντα 3-κύκλο $c \in \mathfrak{A}_n$. Ο ϑ (κατά την πρόταση 5.1.8) απεικονίζει κάθε κλάση συζυγίας τής $\mathfrak{A}_n$ σε μια κλάση συζυγίας τής $\mathfrak{A}_n$. Επομένως, $\vartheta(\text{ΚΛΣ}_{\mathfrak{A}_n}(c)) = \text{ΚΛΣ}_{\mathfrak{A}_n}(\vartheta(c))$. Επειδή ισχύει $\mathrm{ord}(c) = 3$, έχουμε $\mathrm{ord}(\vartheta(c)) = 3$. (Βλ. 2.4.19 (iv).) Κατά το λήμμα 6.3.10 η μετάταξη $\vartheta(c)$ γράφεται ως σύνθεση k ανά δύο ξένων μεταξύ τους 3-κύκλων, για κάποιον παγιωμένο k, $1 \leq k \leq \frac{n}{3}$. Εξάλλου, κατά το λήμμα 6.3.11, $\text{ΚΛΣ}_{\mathfrak{A}_n}(c) = \text{ΚΛΣ}_{\mathfrak{S}_n}(c)$ και

$$\vartheta(\text{ΚΛΣ}_{\mathfrak{A}_n}(c)) = \text{ΚΛΣ}_{\mathfrak{A}_n}(\vartheta(c)) = \text{ΚΛΣ}_{\mathfrak{S}_n}(\vartheta(c)) = \vartheta(\text{ΚΛΣ}_{\mathfrak{S}_n}(c)).$$

Έστω $\mathcal{C}_k$ η κλάση συζυγίας τής $\mathfrak{S}_n$ η περιέχουσα εκείνες τις μετατάξεις που γράφονται ως συνθέσεις k ανά δύο ξένων μεταξύ τους 3-κύκλων. Σύμφωνα με το θεώρημα 5.3.6 και το (ii) τού θεωρήματος 5.3.16,

$$\mathcal{C}_k = \{\, \sigma \in \mathfrak{S}_n \,|\, \mathbf{tp}(\sigma) = (\underbrace{1, ..., 1}_{n-3k \text{ φορές}}, \underbrace{3, ..., 3}_{k \text{ φορές}})\} \underset{(5.21)}{\Longrightarrow} \mathrm{card}(\mathcal{C}_k) = \frac{n!}{3^k k!(n-3k)!}.$$

Προφανώς, $\text{ΚΛΣ}_{\mathfrak{A}_n}(c) = \mathcal{C}_1$, $\text{ΚΛΣ}_{\mathfrak{A}_n}(\vartheta(c)) = \mathcal{C}_k$ και $\vartheta(\mathcal{C}_1) = \mathcal{C}_k$. Κατά συνέπειαν,

$$\begin{aligned} \tfrac{n!}{3(n-3)!} &= \tfrac{n(n-1)(n-2)}{3} = \mathrm{card}(\mathcal{C}_1) = \mathrm{card}(\vartheta(\mathcal{C}_1)) \\ &= \mathrm{card}(\mathcal{C}_k) = \tfrac{n!}{3^k k!(n-3k)!} = \tfrac{n(n-1)(n-2)\cdots(n-3k+1)}{3^k k!}. \end{aligned}$$

Εάν $k > 1$, τούτο ισοδυναμεί με την ισότητα

$$(n-3)(n-4)\cdots(n-3k+1) = 3^{k-1}k! \tag{6.7}$$

Για $k = 2$ ($\Rightarrow n \geq 6$) η (6.7) επαληθεύεται μόνον όταν[15] $n = 6$. (Όμως, *εξ υποθέσεως*, $n \neq 6$.) Αλλά ακόμη και για $k \geq 3$ έχουμε[16]

$$n \geq 3k \Rightarrow \prod_{j=4}^{3k}(n-j+1) \geq \prod_{j=4}^{3k}(3k-j+1) = (3k-3)! > 3^{k-1}k!.$$

Τελικό συμπέρασμα: $k = 1 \Rightarrow \vartheta(\mathcal{C}_1) = \mathcal{C}_1$ και, ως εκ τούτου, η εικόνα οιουδήποτε 3-κύκλου μέσω τού ϑ είναι ένας 3-κύκλος. Σύμφωνα με το λήμμα 6.3.13, υπάρχει κάποια μετάταξη $\tau \in \mathfrak{S}_n$, τέτοια ώστε να ισχύει $\vartheta = \gamma_\tau|_{\mathfrak{A}_n} = \mathfrak{k}(\gamma_\tau)$. Άρα ο $\mathfrak{k}$ είναι πράγματι *και* επιμορφισμός. □

[15] Όταν $k = 2$ και $n \geq 7$, το δεξιό μέλος τής (6.7) ισούται με 6, ενώ το αριστερό της μέλος είναι ≥ 24.

[16] Το ότι ισχύει η ανισότητα $(3k-3)! > 3^{k-1}k!$ για κάθε $k \geq 3$ αποδεικνύεται επαγωγικώς. Για $k = 3$ λαμβάνουμε $720 > 54$. Εάν υποθέσουμε ότι αυτή είναι αληθής για κάποιον $k \geq 3$, τότε

$$\begin{aligned} &(3(k+1)-3)! = (3k)! = (3k-3)!(3k-2)(3k-1)3k > 3^{k-1}k!(3k-2)(3k-1)3k \\ &= 3^k k!(3k-2)(3k-1)k > 3^k(k+1)!, \end{aligned}$$

όπου η τελευταία ανισότητα έπεται από το ότι

$$\begin{aligned} &((3k-2)(3k-1)-1)k \geq (7\cdot 8-1)\cdot 3 = 165 > 1 \Rightarrow (3k-2)(3k-1)k > k+1 \\ &\Rightarrow k!(3k-2)(3k-1)k > k!(k+1) = (k+1)!. \end{aligned}$$

6.3.19 Θεώρημα. $\mathrm{Aut}(\mathfrak{A}_6) \cong \mathrm{Aut}(\mathfrak{S}_6)$.

ΑΠΟΔΕΙΞΗ. Επειδή ο ομομορφισμός (6.6) είναι μονομορφισμός *και* για $n = 6$, η $\mathrm{Aut}(\mathfrak{S}_6)$ εμφυτεύεται στην $\mathrm{Aut}(\mathfrak{A}_6)$, οπότε

$$\mathrm{Aut}(\mathfrak{S}_6) \cong \mathfrak{k}(\mathrm{Aut}(\mathfrak{S}_6)) \sqsubseteq \mathrm{Aut}(\mathfrak{A}_6), \;\; \mathrm{Inn}(\mathfrak{S}_6) \cong \mathfrak{k}(\mathrm{Inn}(\mathfrak{S}_6)) \lhd \mathfrak{k}(\mathrm{Aut}(\mathfrak{S}_6))$$

και, ως εκ τούτου,

$$|\mathrm{Aut}(\mathfrak{A}_6) : \mathfrak{k}(\mathrm{Aut}(\mathfrak{S}_6))|\,|\mathfrak{k}(\mathrm{Aut}(\mathfrak{S}_6)) : \mathfrak{k}(\mathrm{Inn}(\mathfrak{S}_6))| = |\mathrm{Aut}(\mathfrak{A}_6) : \mathfrak{k}(\mathrm{Inn}(\mathfrak{S}_6))| \quad (6.8)$$

(βλ. 4.1.50), όπου

$$|\mathfrak{k}(\mathrm{Aut}(\mathfrak{S}_6)) : \mathfrak{k}(\mathrm{Inn}(\mathfrak{S}_6))| = |\mathrm{Aut}(\mathfrak{S}_6)) : \mathrm{Inn}(\mathfrak{S}_6)| = |\mathrm{Out}(\mathfrak{S}_6)| \underset{6.3.8}{=} 2. \quad (6.9)$$

Θεωρούμε τυχόντα αυτομορφισμό $\vartheta \in \mathrm{Aut}(\mathfrak{A}_6)$ και τυχόντα 3-κύκλο $c \in \mathfrak{A}_6$. Ο $\vartheta \in \mathrm{Aut}(\mathfrak{A}_6)$ (κατά την πρόταση 5.1.8) απεικονίζει κάθε κλάση συζυγίας τής $\mathfrak{A}_6$ σε μια κλάση συζυγίας τής $\mathfrak{A}_6$. Επομένως, $\vartheta(\kappa\lambda\sigma_{\mathfrak{A}_6}(c)) = \kappa\lambda\sigma_{\mathfrak{A}_6}(\vartheta(c))$. Επειδή $\mathrm{ord}(c) = 3$, έχουμε $\mathrm{ord}(\vartheta(c)) = 3$. (Βλ. 2.4.19 (iv).) Κατά το λήμμα 6.3.10 η μετάταξη $\vartheta(c)$ γράφεται ως σύνθεση k ανά δύο ξένων μεταξύ τους 3-κύκλων, για κάποιον $k \in \{1, 2\}$. Ακολουθώντας κατά γράμμα και τους λοιπούς συλλογισμούς που χρησιμοποιήσαμε στην απόδειξη τού θεωρήματος 6.3.18 (με τους ίδιους συμβολισμούς, μέχρι το σημείο που είχε επισημανθεί ότι η (6.7) για $n = 6$ επαληθεύεται για κάθε $k \in \{1, 2\}$) και λαμβάνοντας υπ' όψιν ότι $\mathrm{card}(\mathcal{C}_1) = \mathrm{card}(\mathcal{C}_2) = 40$, συμπεραίνουμε ότι

$$\text{είτε } \; [\vartheta(\mathcal{C}_1) = \mathcal{C}_1 \;\text{ και }\; \vartheta(\mathcal{C}_2) = \mathcal{C}_2] \;\; \text{είτε } \; [\vartheta(\mathcal{C}_1) = \mathcal{C}_2 \;\text{ και }\; \vartheta(\mathcal{C}_2) = \mathcal{C}_1]\,.$$

Στην πρώτη περίπτωση, η εικόνα οιουδήποτε 3-κύκλου μέσω τού ϑ είναι ένας 3-κύκλος, οπότε $\vartheta \in \mathfrak{k}(\mathrm{Inn}(\mathfrak{S}_6))$ (δυνάμει τού λήμματος 6.3.13). Στη δεύτερη περίπτωση, για *οιονδήποτε* $\vartheta' \in \mathrm{Aut}(\mathfrak{A}_6)$ για τον οποίο ισχύει $\vartheta'(\mathcal{C}_1) = \mathcal{C}_2$, έχουμε

$$\vartheta^{-1}\left(\vartheta'(\mathcal{C}_1)\right) = \vartheta^{-1}(\mathcal{C}_2) = \mathcal{C}_1 \Rightarrow \vartheta^{-1} \circ \vartheta' \in \mathfrak{k}(\mathrm{Inn}(\mathfrak{S}_6)) \Rightarrow \vartheta' \in \vartheta \circ \mathfrak{k}(\mathrm{Inn}(\mathfrak{S}_6)),$$

οπότε

$$\mathrm{Aut}(\mathfrak{A}_6) = \begin{cases} \mathfrak{k}(\mathrm{Inn}(\mathfrak{S}_6), & \text{όταν } \vartheta \in \mathfrak{k}(\mathrm{Inn}(\mathfrak{S}_6)), \\ \mathfrak{k}(\mathrm{Inn}(\mathfrak{S}_6) \coprod (\vartheta \circ \mathfrak{k}(\mathrm{Inn}(\mathfrak{S}_6)), & \text{όταν } \vartheta \notin \mathfrak{k}(\mathrm{Inn}(\mathfrak{S}_6)), \end{cases}$$

Εξ αυτών έπεται (μόνον) ότι

$$|\mathrm{Aut}(\mathfrak{A}_6) : \mathfrak{k}(\mathrm{Inn}(\mathfrak{S}_6))| \leq 2. \quad (6.10)$$

Εντούτοις, από τις (6.8), (6.9) και (6.10) συνάγεται ότι

$$|\mathrm{Aut}(\mathfrak{A}_6) : \mathfrak{k}(\mathrm{Inn}(\mathfrak{S}_6))| = 2 \;\text{ και }\; |\mathrm{Aut}(\mathfrak{A}_6) : \mathfrak{k}(\mathrm{Aut}(\mathfrak{S}_6))| = 1,$$

οπότε $\mathrm{Aut}(\mathfrak{A}_6) = \mathfrak{k}(\mathrm{Aut}(\mathfrak{S}_6)) \cong \mathrm{Aut}(\mathfrak{S}_6)$. □

6.3.20 Παρατήρηση. Επειδή η $\mathfrak{A}_2$ είναι τετριμμένη και $\mathfrak{A}_3 \cong \mathbb{Z}_3$, μέσω των προαναφερθέντων στα εδάφια 5.4.11 και 5.4.30 (iv), και των αποδειχθέντων στα θεωρήματα 2.4.32, 6.3.18 και 6.3.19, καταλήγουμε στον ακόλουθο ολοκληρωμένο κατάλογο:

n	$Z(\mathfrak{A}_n)$	$\mathrm{Aut}(\mathfrak{A}_n)$	$\mathrm{Inn}(\mathfrak{A}_n)$	$\mathrm{Out}(\mathfrak{A}_n)$
2	$\{\mathrm{id}\}$	$\{\mathrm{id}_{\mathfrak{A}_2}\}$	$\{\mathrm{id}_{\mathfrak{A}_2}\}$	τετριμμένη
3	$\mathbb{Z}_3$	$\mathbb{Z}_3^\times \cong \mathbb{Z}_2$	$\{\mathrm{id}_{\mathfrak{A}_3}\}$	$\mathbb{Z}_2$
≥ 4 και $\neq 6$	$\{\mathrm{id}\}$	$\mathrm{Aut}(\mathfrak{S}_n) \cong \mathfrak{S}_n$	$\mathfrak{A}_n$	$\mathbb{Z}_2$
6	$\{\mathrm{id}\}$	$\mathrm{Aut}(\mathfrak{S}_6)$ (βλ. 6.3.9)	$\mathfrak{A}_6$	$\mathbf{V}$

► **Περαιτέρω κλάσεις πλήρων ομάδων**. Στα κάτωθι θεωρήματα[17] 6.3.21 και 6.3.22 δίδονται δύο επιπρόσθετες κλάσεις πλήρων ομάδων.

6.3.21 Θεώρημα. (J. Schreier & S. Ulam, 1937) *Η συμμετρική ομάδα* $(\mathfrak{S}_A, \circ)$ *επί οιουδήποτε αριθμήσιμου απειροσυνόλου* A *είναι πλήρης.*

6.3.22 Θεώρημα. *Η ομάδα αυτομορφισμών* $\mathrm{Aut}(G)$ *οιασδήποτε μη αβελιανής απλής ομάδας* $(G, \cdot)$ *είναι πλήρης.*

ΑΠΟΔΕΙΞΗ. Έστω $(G, \cdot)$ τυχούσα μη αβελιανή απλή ομάδα. Το κέντρο της είναι κατ' ανάγκην η τετριμμένη υποομάδα της (βλ. 5.4.10). Ύστερα από διπλή εφαρμογή τού πορίσματος 5.4.36 (ήτοι τόσον για την G όσον και για την $\mathrm{Aut}(G)$) λαμβάνουμε

$$Z(G) = \{e_G\} \Rightarrow Z(\mathrm{Aut}(G)) = \{\mathrm{id}_G\} \Rightarrow Z(\mathrm{Aut}(\mathrm{Aut}(G))) = \{\mathrm{id}_{\mathrm{Aut}(G)}\}.$$

Αρκεί λοιπόν να αποδειχθεί ότι $\mathrm{Aut}(\mathrm{Aut}(G)) = \mathrm{Inn}(\mathrm{Aut}(G))$. Έστω τυχών αυτομορφισμός $\vartheta \in \mathrm{Aut}(\mathrm{Aut}(G))$. Προφανώς,

$$5.4.25 \Rightarrow \mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G) \underset{4.2.30\,(\mathrm{i})}{\Longrightarrow} \vartheta(\mathrm{Inn}(G)) \trianglelefteq \mathrm{Im}(\vartheta) = \mathrm{Aut}(G)$$
$$\underset{4.2.22}{\Longrightarrow} \mathrm{Inn}(G) \cap \vartheta(\mathrm{Inn}(G)) \trianglelefteq \mathrm{Inn}(G).$$

Επειδή η $\mathrm{Inn}(G) \cong G$ είναι απλή, έχουμε είτε $\mathrm{Inn}(G) \cap \vartheta(\mathrm{Inn}(G)) = \{\mathrm{id}_G\}$ είτε

$$\mathrm{Inn}(G) \cap \vartheta(\mathrm{Inn}(G)) = \mathrm{Inn}(G) \Rightarrow \vartheta(\mathrm{Inn}(G)) \subseteq \mathrm{Inn}(G) \underset{2.1.20}{\Longrightarrow} \vartheta(\mathrm{Inn}(G)) \sqsubseteq \mathrm{Inn}(G).$$

Το πρώτο ενδεχόμενο αποκλείεται. (Εάν $\delta \in \mathrm{Inn}(G)$ και $\varepsilon \in \vartheta(\mathrm{Inn}(G))$, τότε

$$\left.\begin{array}{r} \vartheta(\mathrm{Inn}(G)) \trianglelefteq \mathrm{Aut}(G) \Rightarrow \delta \circ \varepsilon \circ \delta^{-1} \in \vartheta(\mathrm{Inn}(G)) \\ \varepsilon \in \vartheta(\mathrm{Inn}(G)) \Rightarrow \varepsilon^{-1} \in \vartheta(\mathrm{Inn}(G)) \end{array}\right\} \Rightarrow \delta \circ \varepsilon \circ \delta^{-1} \circ \varepsilon^{-1} \in \vartheta(\mathrm{Inn}(G))$$

και

$$\left.\begin{array}{r} \delta \in \mathrm{Inn}(G) \Rightarrow \delta^{-1} \in \mathrm{Inn}(G) \\ \mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G) \Rightarrow \varepsilon \circ \delta^{-1} \circ \varepsilon^{-1} \in \mathrm{Inn}(G) \end{array}\right\} \Rightarrow \delta \circ \varepsilon \circ \delta^{-1} \circ \varepsilon^{-1} \in \mathrm{Inn}(G).$$

[17] Για την απόδειξη τού θεωρήματος 6.3.21 βλ. το άρθρο: J. Schreier, S. Ulam: *Über die Automorphismen der Permutationsgruppe der natürlichen Zahlenfolge*, Fund. Math. **28** (1937), 258-260.

Εάν υποθέσουμε ότι $\mathrm{Inn}(G) \cap \vartheta(\mathrm{Inn}(G)) = \{\mathrm{id}_G\}$, τότε

$$\delta \circ \varepsilon \circ \delta^{-1} \circ \varepsilon^{-1} = \mathrm{id}_G \Rightarrow \delta \circ \varepsilon = \varepsilon \circ \delta,$$

οπότε $\vartheta(\mathrm{Inn}(G)) \sqsubseteq \mathrm{Aut_c}(G) := \mathrm{C}_{\mathrm{Aut}(G)}(\mathrm{Inn}(G))$. Επειδή $Z(G) = \{e_G\}$, η πρόταση 5.4.35 μας πληροφορεί ότι $\mathrm{Aut_c}(G) = \{\mathrm{id}_G\}$. Επομένως,

$$\vartheta(\mathrm{Inn}(G)) = \{\mathrm{id}_G\} \Rightarrow \mathrm{Inn}(G) \sqsubseteq \mathrm{Ker}(\vartheta) = \{\mathrm{id}_{\mathrm{Aut}(G)}\},$$

ήτοι $\mathrm{Inn}(G) = \{\mathrm{id}_{\mathrm{Aut}(G)}\}$. Άρα και η ίδια η $G \cong \mathrm{Inn}(G)$ είναι τετριμμένη. Άτοπο!)

Αυτό σημαίνει ότι $\vartheta(\mathrm{Inn}(G)) \sqsubseteq \mathrm{Inn}(G)$. Παρομοίως αποδεικνύεται[18] ότι $\mathrm{Inn}(G) \sqsubseteq \vartheta(\mathrm{Inn}(G))$. Άρα $\mathrm{Inn}(G) = \vartheta(\mathrm{Inn}(G))$ και, ως εκ τούτου,

$$\widetilde{\vartheta} := \vartheta|_{\mathrm{Inn}(G)} \in \mathrm{Aut}(\mathrm{Inn}(G)).$$

Επειδή $Z(G) = \{e_G\}$ και $\mathrm{Inn}(G) := \left\{ \boldsymbol{\gamma}_g \middle| \, g \in G \right\}$, όπου

$$\boldsymbol{\gamma}_g : G \longrightarrow G, \quad \boldsymbol{\gamma}_g(x) := gxg^{-1}, \ \ \forall x \in G,$$

ο κανονιστικός ισομορφισμός μεταξύ των G και $\mathrm{Inn}(G)$ είναι ο

$$f_G : G \xrightarrow{\cong} \mathrm{Inn}(G), \ g \longmapsto f_G(g) := \boldsymbol{\gamma}_g.$$

(Βλ. 5.4.26 και 5.4.28.) Μέσω αυτού ορίζεται ο $\eta := f_G^{-1} \circ \widetilde{\vartheta} \circ f_G \in \mathrm{Aut}(G)$.

$$\begin{array}{ccc} G & \overset{\eta}{- - \to} & G \\ {\scriptstyle f_G}\downarrow{\scriptstyle \cong} & \circlearrowleft & {\scriptstyle \cong}\downarrow{\scriptstyle f_G} \quad \curvearrowright {\scriptstyle f_G^{-1}} \\ \mathrm{Inn}(G) & \underset{\widetilde{\vartheta}}{\xrightarrow{\cong}} & \mathrm{Inn}(G) \end{array}$$

Σημειωτέον ότι για κάθε $g \in G$ υπάρχει ακριβώς ένα στοιχείο $g' \in G$, για το οποίο ισχύει $\widetilde{\vartheta}(\boldsymbol{\gamma}_g) = \boldsymbol{\gamma}_{g'}$. Προφανώς,

$$\eta\,(g) = (f_G^{-1} \circ \widetilde{\vartheta} \circ f_G)(g) = f_G^{-1}(\widetilde{\vartheta}(\boldsymbol{\gamma}_g)) = f_G^{-1}(\boldsymbol{\gamma}_{g'}) = g', \ \forall g \in G.$$

Από την άλλη μεριά, $\mathrm{Inn}(\mathrm{Aut}(G)) := \{\, \Gamma_\varphi | \, \varphi \in \mathrm{Aut}(G)\} \trianglelefteq \mathrm{Aut}(\mathrm{Aut}(G))$, όπου

$$\Gamma_\varphi : \mathrm{Aut}(G) \longrightarrow \mathrm{Aut}(G), \quad \psi \longmapsto \Gamma_\varphi(\psi) := \varphi \circ \psi \circ \varphi^{-1}, \ \ \forall \psi \in \mathrm{Aut}(G).$$

Ισχυρισμός: $\Gamma_\eta = \vartheta$. Για την επαλήθευση τού ισχυρισμού θέτουμε

$$\chi := \vartheta \circ \Gamma_\eta^{-1} \in \mathrm{Aut}(\mathrm{Aut}(G))$$

και παρατηρούμε ότι για κάθε $g \in G$ ισχύουν οι ισότητες

$$\begin{aligned} \chi(\boldsymbol{\gamma}_g) &= \vartheta(\Gamma_\eta^{-1}(\boldsymbol{\gamma}_g)) = \vartheta(\Gamma_{\eta^{-1}}(\boldsymbol{\gamma}_g)) = \vartheta(\eta^{-1} \circ \boldsymbol{\gamma}_g \circ \eta) \\ &= \vartheta(\boldsymbol{\gamma}_{\eta^{-1}(g)}) = \widetilde{\vartheta}(\boldsymbol{\gamma}_{\eta^{-1}(g)}) = \boldsymbol{\gamma}_{\eta(\eta^{-1}(g))} = \boldsymbol{\gamma}_g, \end{aligned}$$

[18] Αρκεί να επαναληφθούν τα ανωτέρω επιχειρήματα με τον αυτομορφισμό ϑ^{-1} τής G στη θέση τού ϑ. Προφανώς, $\vartheta^{-1}(\mathrm{Inn}(G)) \sqsubseteq \mathrm{Inn}(G) \Rightarrow \mathrm{Inn}(G) \sqsubseteq \vartheta(\mathrm{Inn}(G))$.

καθόσον για κάθε $x \in G$ έχουμε

$$\begin{aligned}(\eta^{-1} \circ \boldsymbol{\gamma}_g \circ \eta)(x) &= \eta^{-1}(\boldsymbol{\gamma}_g(\eta(x))) = \eta^{-1}(g\eta(x)g^{-1}) \\ &= \eta^{-1}(g)\eta^{-1}(\eta(x))\eta^{-1}(g^{-1}) = \eta^{-1}(g)x(\eta^{-1}(g))^{-1},\end{aligned}$$

οπότε $\eta^{-1} \circ \boldsymbol{\gamma}_g \circ \eta = \boldsymbol{\gamma}_{\eta^{-1}(g)}$. Κατά συνέπειαν, $\chi|_{\mathrm{Inn}(G)} = \mathrm{id}_{\mathrm{Inn}(G)}$. Θα αποδείξουμε ότι $\chi = \mathrm{id}_{\mathrm{Aut}(G)}$ χρησιμοποιώντας «εις άτοπον απαγωγή». Υποθέτουμε ότι υπάρχει κάποιος $\rho \in \mathrm{Aut}(G) \setminus \mathrm{Inn}(G)$, τέτοιος ώστε να ισχύει $\chi(\rho) \neq \rho$. Για κάθε $g \in G$,

$$\left.\begin{array}{r} \boldsymbol{\gamma}_g \in \mathrm{Inn}(G) \\ \mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G) \end{array}\right\} \Rightarrow \rho \circ \boldsymbol{\gamma}_g \circ \rho^{-1} \in \mathrm{Inn}(G),$$

οπότε από την $\chi|_{\mathrm{Inn}(G)} = \mathrm{id}_{\mathrm{Inn}(G)}$ έπεται ότι

$$\begin{aligned}&\rho \circ \boldsymbol{\gamma}_g \circ \rho^{-1} = \chi(\rho \circ \boldsymbol{\gamma}_g \circ \rho^{-1}) = \chi(\rho) \circ \chi(\boldsymbol{\gamma}_g) \circ \chi(\rho^{-1}) = \chi(\rho) \circ \boldsymbol{\gamma}_g \circ \chi(\rho)^{-1} \\ &\Rightarrow \big(\chi(\rho)^{-1} \circ \rho\big) \circ \boldsymbol{\gamma}_g = \boldsymbol{\gamma}_g \circ \big(\chi(\rho)^{-1} \circ \rho\big) \Rightarrow \chi(\rho)^{-1} \circ \rho \in \mathrm{Aut}_{\mathrm{c}}(G) = \{\mathrm{id}_G\},\end{aligned}$$

ήτοι ότι $\chi(\rho)^{-1} \circ \rho = \mathrm{id}_G \Rightarrow \chi(\rho) = \rho$. Άτοπο! Τελικώς,

$$\chi = \vartheta \circ \Gamma_\eta^{-1} = \mathrm{id}_{\mathrm{Aut}(G)} \Rightarrow \Gamma_\eta = \vartheta \in \mathrm{Inn}(\mathrm{Aut}(G)),$$

ο ισχυρισμός είναι όντως αληθής και η $\mathrm{Aut}(G)$ είναι πλήρης ομάδα. □

6.4 ΤΟ ΟΛΟΜΟΡΦΟ ΜΙΑΣ ΟΜΑΔΑΣ

Έστω $(G, \cdot)$ μια ομάδα. Εάν $K \trianglelefteq G$, τότε $\boldsymbol{\gamma}_g(K) = K$ για κάθε $\boldsymbol{\gamma}_g \in \mathrm{Inn}(G)$ (όπου $g \in G$, βλ. 5.4.21 και 5.4.23). Επομένως, μέσω τού $\boldsymbol{\gamma}_g$ επάγεται ο αυτομορφισμός $\boldsymbol{\gamma}_g\big|_K \in \mathrm{Aut}(K)$ τής K. Ωστόσο αυτός δεν είναι κατ' ανάγκην εσωτερικός αυτομορφισμός τής K. Ενδέχεται λοιπόν να ισχύει[19] $\{\boldsymbol{\gamma}_g\big|_K : g \in G\} \subsetneqq \mathrm{Aut}(K)$, δηλαδή ενδέχεται να υπάρχουν αυτομορφισμοί τής K που να μην επάγονται από εσωτερικούς αυτομορφισμούς τής G (υπό την ως άνω έννοια).

Τίθεται λοιπόν ευλόγως το ερώτημα: Δοθείσας μιας ομάδας $(G, \cdot)$, είναι δυνατή η εμφύτευσή της εντός μιας «ευρύτερης» ομάδας H (εξαρτώμενης από την G), ούτως ώστε *κάθε* αυτομορφισμός τής G να επάγεται από έναν *εσωτερικό* αυτομορφισμό τής H (ήτοι να είναι ο περιορισμός κάποιου *εσωτερικού* αυτομορφισμού τής H επί τής G); Όπως θα δούμε στην πρόταση 6.4.2, μια τέτοιου είδους εμφύτευση είναι πάντοτε δυνατή (εάν κανείς ως H χρησιμοποιήσει το λεγόμενο «ολόμορφο» τής ομάδας G).

Κατά το θεώρημα 3.5.1 τού Cayley, $L(G) \cong G \cong R(G)$, όπου

$$L(G) := \{L_g \mid g \in G\} \sqsubseteq \mathfrak{S}_G,\ R(G) := \{R_g \mid g \in G\} \sqsubseteq \mathfrak{S}_G,$$

[19] Επί παραδείγματι, η υποομάδα $K := \langle \alpha \circ \beta, \beta^2 \rangle$ τής διεδρικής ομάδας $\mathbf{D}_{14} = \langle \alpha, \beta \rangle$ (με $|\mathbf{D}_{14}| = 28$) είναι ισόμορφη με τη διεδρική ομάδα $\mathbf{D}_7$ (τάξεως $|\mathbf{D}_7| = 14$) και ισχύει

$$\mathrm{card}(\{\boldsymbol{\gamma}_g\big|_K : g \in \mathbf{D}_{14}\}) \leq |\mathrm{Inn}(\mathbf{D}_{14})| \underset{5.4.30\,(\mathrm{ii})}{=} |\mathbf{D}_7| = 14 < 42 = 7 \cdot \phi(7) \underset{7.6.36}{=} |\mathrm{Aut}(\mathbf{D}_7)| = |\mathrm{Aut}(K)|\,,$$

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

είναι οι εξ αριστερών και εκ δεξιών κανονικές αναπαραστάσεις τής G εντός τής $\mathfrak{S}_G$, αντιστοίχως, με

$$L_g : G \longrightarrow G,\ x \longmapsto L_g(x) := gx,\ \ R_g : G \longrightarrow G,\ x \longmapsto R_g(x) := xg.$$

Σημειωτέον ότι $\mathrm{Aut}(G) \sqsubseteq \mathfrak{S}_G$ και ότι υφίστανται ισομορφισμοί

$$\mathrm{Aut}(G) \xrightarrow{\cong} \mathrm{Aut}(L(G)),\ \vartheta \longmapsto \mathfrak{Y}_\vartheta^{\alpha\varrho\cdot},\ \ \mathrm{Aut}(G) \xrightarrow{\cong} \mathrm{Aut}(R(G)),\ \vartheta \longmapsto \mathfrak{Y}_\vartheta^{\delta\varepsilon\xi\cdot},$$

όπου $\mathfrak{Y}_\vartheta^{\alpha\varrho\cdot}(L_g) := L_{\vartheta(g)}$ και $\mathfrak{Y}_\vartheta^{\delta\varepsilon\xi\cdot}(R_g) := R_{\vartheta(g)}$ για κάθε $g \in G$.

6.4.1 Ορισμός. Ως το **ολόμορφο** τής G ορίζεται ο ορθοθέτης

$$\boxed{\mathrm{Hol}(G) := \mathrm{N}_{\mathfrak{S}_G}(L(G))}$$

τής εξ αριστερών κανονικής αναπαράστασεως $L(G)$ τής G εντός τής $\mathfrak{S}_G$.

6.4.2 Πρόταση. $\mathrm{Aut}(G) \cong \mathrm{Aut}(L(G)) \sqsubseteq \mathrm{Hol}(G)$ *και*

$$\boxed{\mathrm{Aut}(L(G)) \ni \mathfrak{Y}_\vartheta^{\alpha\varrho\cdot} = \boldsymbol{\gamma}_\vartheta\big|_{L(G)},\ \forall \vartheta \in \mathrm{Aut}(G),}$$

όπου $\boldsymbol{\gamma}_\vartheta : \mathrm{Hol}(G) \longrightarrow \mathrm{Hol}(G),\ \omega \longmapsto \boldsymbol{\gamma}_\vartheta(\omega) := \vartheta \circ \omega \circ \vartheta^{-1}$, *ο εσωτερικός αυτομορφισμός τού* $\mathrm{Hol}(G)$ *ο δημιουργούμενος μέσω τού* ϑ.

ΑΠΟΔΕΙΞΗ. Για κάθε $g \in G$ και κάθε $\vartheta \in \mathrm{Aut}(G)$ ισχύει

$$\vartheta \circ L_g = L_{\vartheta(g)} \circ \vartheta, \tag{6.11}$$

καθόσον για κάθε $x \in G$ έχουμε

$$(\vartheta \circ L_g)(x) = \vartheta(L_g(x)) = \vartheta(gx) = \vartheta(g)\vartheta(x) = L_{\vartheta(g)}(\vartheta(x)) = \big(L_{\vartheta(g)} \circ \vartheta\big)\,(x).$$

Από την (6.11) έπεται αφ' ενός μεν ότι $\vartheta \in \mathrm{Hol}(G)$ (διότι $L_g, L_{\vartheta(g)} \in L(G)$), οπότε

$$\mathrm{Aut}(G) \subseteq \mathrm{Hol}(G) \underset{2.1.20}{\Longrightarrow} \mathrm{Aut}(G) \sqsubseteq \mathrm{Hol}(G),$$

αφ' ετέρου δε ότι $\boldsymbol{\gamma}_\vartheta|_{L(G)}\,(L_g) = \vartheta \circ L_g \circ \vartheta^{-1} = L_{\vartheta(g)} =: \mathfrak{Y}_\vartheta^{\alpha\varrho\cdot}(L_g)$. □

6.4.3 Παρατήρηση. Επειδή για κάθε $\omega \in \mathrm{Hol}(G)$ και κάθε $g \in G$ έχουμε

$$\omega \circ L_g \circ \omega^{-1} = L_{\omega(g)} \in L(G)\ \text{ και }\ \omega \circ R_g \circ \omega^{-1} = R_{\omega(g)} \in R(G)$$

(ισότητες αποδεικνυόμενες όπως η (6.11)), συμπεραίνουμε ότι

$$L(G) \trianglelefteq \mathrm{Hol}(G)\ \text{ και }\ R(G) \trianglelefteq \mathrm{Hol}(G).$$

6.4.4 Πρόταση. $\mathrm{C}_{\mathfrak{S}_G}(L(G)) = R(G)$ *και* $\mathrm{C}_{\mathfrak{S}_G}(R(G)) = L(G)$.

ΑΠΟΔΕΙΞΗ. Έστω $\sigma \in \mathrm{C}_{\mathfrak{S}_G}(L(G))$. Εξ ορισμού,

$$\sigma \circ L_g = L_g \circ \sigma,\ \forall g \in G. \tag{6.12}$$

Επειδή για οιοδήποτε $g \in G$ ισχύει

$$(\sigma \circ L_g)\,(e_G) = \sigma(g) \text{ και } (L_g \circ \sigma)(e_G) = L_g(\sigma(e_G)) = g\sigma(e_G),$$

η (6.12) δίδει $\sigma(g) = g\sigma(e_G) = R_{\sigma(e_G)}(g) \Rightarrow \sigma = R_{\sigma(e_G)} \in R(G)$. Και αντιστρόφως· εάν θεωρήσουμε τυχόν στοιχείο $R_g \in R(G)$ (όπου $g \in G$), τότε για οιαδήποτε $g' \in G$ και $x \in G$ έχουμε

$$\begin{aligned}(R_g \circ L_{g'})(x) &= R_g(L_{g'}(x)) = R_g(g'x) = g'xg \\ &= L_{g'}(xg) = L_{g'}(R_g(x)) = (L_{g'} \circ R_g)(x),\end{aligned}$$

οπότε

$$R_g \circ L_{g'} = L_{g'} \circ R_g. \tag{6.13}$$

Εξ αυτού έπεται ότι $R_g \in \mathrm{C}_{\mathfrak{S}_G}(L(G))$. Η ισότητα $\mathrm{C}_{\mathfrak{S}_G}(R(G)) = L(G)$ αποδεικνύεται παρομοίως. □

6.4.5 Παρατήρηση. Από την (6.13) προκύπτει ότι $L(G) \circ R(G) = R(G) \circ L(G)$, οπότε (βάσει τής προτάσεως 4.1.4) $L(G) \circ R(G) \sqsubseteq \mathrm{Hol}(G)$.

6.4.6 Πρόταση. $\mathrm{Inn}(G) \sqsubseteq L(G) \circ R(G)$.

ΑΠΟΔΕΙΞΗ. Για τυχόντα εσωτερικό αυτομορφισμό $\boldsymbol{\gamma}_g \in \mathrm{Inn}(G)$ (όπου $g \in G$) έχουμε

$$\boldsymbol{\gamma}_g(x) = gxg^{-1} = g(R_{g^{-1}}(x)) = L_g(R_{g^{-1}}(x)) = (L_g \circ R_{g^{-1}})(x)$$

για κάθε $x \in G$, οπότε $\boldsymbol{\gamma}_g = L_g \circ R_{g^{-1}} \in L(G) \circ R(G)$. □

6.4.7 Πόρισμα. $L(G) \circ R(G) = \mathrm{Inn}(G) \circ L(G) = \mathrm{Inn}(G) \circ R(G)$.

ΑΠΟΔΕΙΞΗ. Επειδή $\boldsymbol{\gamma}_g \circ R_g = L_g$ για κάθε $g \in G$, έχουμε

$$L(G) \sqsubseteq \mathrm{Inn}(G) \circ R(G) \Rightarrow L(G) \circ R(G) \sqsubseteq \mathrm{Inn}(G) \circ R(G).$$

Από την άλλη μεριά, από την πρόταση 6.4.6 έπεται ότι

$$\mathrm{Inn}(G) \sqsubseteq L(G) \circ R(G) \Rightarrow \mathrm{Inn}(G) \circ R(G) \sqsubseteq L(G) \circ R(G),$$

οπότε $L(G) \circ R(G) = \mathrm{Inn}(G) \circ R(G)$. Εξάλλου, επειδή $\boldsymbol{\gamma}_g \circ L_g^{-1} = \boldsymbol{\gamma}_g \circ L_{g^{-1}} = R_{g^{-1}}$ για κάθε $g \in G$, έχουμε

$$R(G) \sqsubseteq \mathrm{Inn}(G) \circ L(G) \Rightarrow L(G) \circ R(G) \underset{6.4.5}{=} R(G) \circ L(G) \sqsubseteq \mathrm{Inn}(G) \circ L(G).$$

Από την πρόταση 6.4.6 έπεται ότι

$$\mathrm{Inn}(G) \sqsubseteq L(G) \circ R(G) \underset{6.4.5}{=} R(G) \circ L(G) \Rightarrow \mathrm{Inn}(G) \circ L(G) \sqsubseteq R(G) \circ L(G),$$

οπότε $L(G) \circ R(G) = R(G) \circ L(G) = \mathrm{Inn}(G) \circ L(G)$. □

6.4.8 Θεώρημα. (i) *Το ολόμορφο τής G γράφεται υπό τη μορφή*

$$\boxed{\mathrm{Hol}(G) = L(G) \circ \mathrm{Aut}(G) = R(G) \circ \mathrm{Aut}(G).}$$

(ii) *Εάν* $\sigma \in \mathrm{Hol}(G)$, *τότε* $\sigma \in \mathrm{Aut}(G) \Longleftrightarrow \sigma\left(e_G\right) = e_G$.
(iii) $L(G) \cap \mathrm{Aut}(G) = R(G) \cap \mathrm{Aut}(G) = \{e_{\mathfrak{S}_G}\} = \{\mathrm{id}_G\}$.

ΑΠΟΔΕΙΞΗ. (i) Κατ' αρχάς,

$$\left.\begin{array}{r} L(G) \sqsubseteq \mathrm{Hol}(G) \\ \mathrm{Aut}(G) \sqsubseteq \mathrm{Hol}(G) \end{array}\right\} \Rightarrow L(G) \circ \mathrm{Aut}(G) \subseteq \mathrm{Hol}(G) \tag{6.14}$$

και

$$\left.\begin{array}{r} R(G) \sqsubseteq \mathrm{Hol}(G) \\ \mathrm{Aut}(G) \sqsubseteq \mathrm{Hol}(G) \end{array}\right\} \Rightarrow R(G) \circ \mathrm{Aut}(G) \subseteq \mathrm{Hol}(G). \tag{6.15}$$

Έστω $\omega \in \mathrm{Hol}(G)$. Επειδή $L(G) \trianglelefteq \mathrm{Hol}(G)$ (βλ. εδάφιο 6.4.3), έχουμε προφανώς $\boldsymbol{\gamma}_\omega|_{L(G)} \in \mathrm{Aut}(L(G))$. Όμως

$$\mathrm{Aut}(L(G)) = \left\{ \mathfrak{Y}_\vartheta^{\alpha\varrho.} \middle| \, \vartheta \in \mathrm{Aut}(G) \right\} \Rightarrow \exists \vartheta \in \mathrm{Aut}(G) : \mathfrak{Y}_\vartheta^{\alpha\varrho.} = \boldsymbol{\gamma}_\omega|_{L(G)}$$

και (κατά την πρόταση 6.4.2) $\boldsymbol{\gamma}_\vartheta|_{L(G)} = \mathfrak{Y}_\vartheta^{\alpha\varrho.} = \boldsymbol{\gamma}_\omega|_{L(G)}$. Αυτό σημαίνει ότι για κάθε $g \in G$ ισχύει

$$\vartheta \circ L_g \circ \vartheta^{-1} = \boldsymbol{\gamma}_\vartheta\big|_{L(G)}\left(L_g\right) = \boldsymbol{\gamma}_\omega|_{L(G)}\left(L_g\right) = \omega \circ L_g \circ \omega^{-1}$$

ή, ισοδυνάμως,

$$(\omega^{-1} \circ \vartheta) \circ L_g = L_g \circ (\omega^{-1} \circ \vartheta) \Rightarrow \omega^{-1} \circ \vartheta \in \mathbf{C}_{\mathfrak{S}_G}(L(G)) \underset{6.4.4}{=} R(G),$$

οπότε $\omega \in R(G) \circ \vartheta$ και, κατ' επέκταση,

$$\omega \in R(G) \circ \mathrm{Aut}(G) \Rightarrow \mathrm{Hol}(G) \subseteq R(G) \circ \mathrm{Aut}(G). \tag{6.16}$$

Από τις (6.15) και (6.16) λαμβάνουμε $\mathrm{Hol}(G) = R(G) \circ \mathrm{Aut}(G)$. Εξάλλου,

$$\left[R_g = L_g \circ \boldsymbol{\gamma}_{g^{-1}},\ \forall g \in G\right] \Rightarrow R(G) \subseteq L(G) \circ \mathrm{Inn}(G) \tag{6.17}$$

και

$$\left.\begin{array}{r} \mathrm{Hol}(G) = R(G) \circ \mathrm{Aut}(G) \underset{(6.17)}{\subseteq} L(G) \circ \mathrm{Inn}(G) \circ \mathrm{Aut}(G) \\ \mathrm{Inn}(G) \sqsubseteq \mathrm{Aut}(G) \end{array}\right\} \Rightarrow \mathrm{Hol}(G) \subseteq L(G) \circ \mathrm{Aut}(G). \tag{6.18}$$

Από τις (6.14) και (6.18) λαμβάνουμε $\mathrm{Hol}(G) = L(G) \circ \mathrm{Aut}(G)$.
(ii) Η συνεπαγωγή "$\Rightarrow$" είναι προφανής. Για την απόδειξη τής "$\Leftarrow$" υποθέτουμε ότι $\sigma\left(e_G\right) = e_G$. Λόγω τού (i) υπάρχουν $g \in G$ και $\vartheta \in \mathrm{Aut}(G) : \sigma = L_g \circ \vartheta$. Επομένως,

$$e_G = \sigma\left(e_G\right) = L_g\left(\vartheta\left(e_G\right)\right) = L_g\left(e_G\right) = g \Rightarrow \sigma = L_{e_G} \circ \vartheta = \vartheta.$$

(iii) Εάν $\vartheta \in L(G) \cap \mathrm{Aut}(G)$, τότε $\vartheta = L_g$ για κάποιο $g \in G$ και

$$e_G = \vartheta(e_G) = L_g(e_G) = g \Rightarrow \vartheta = L_{e_G} = \mathrm{id}_G.$$

Η ισότητα $R(G) \cap \mathrm{Aut}(G) = \{\mathrm{id}_G\}$ αποδεικνύεται παρομοίως. □

6.4.9 Παράδειγμα. Το ολόμορφο τής ομάδας $(\mathbf{V}, \circ)$ των τεσσάρων στοιχείων τού Klein (βλ. 3.4.2 (ii)) είναι το

$$\mathrm{Hol}(\mathbf{V}) = L(\mathbf{V}) \circ \mathrm{Aut}(\mathbf{V}) \cong \mathbf{V} \circ \mathfrak{S}_3 \cong \mathbf{V} \circ K = \mathfrak{S}_4,$$

όπου $K := \{\sigma \in \mathfrak{S}_4 \,|\, \sigma(4) = 4\} \cong \mathfrak{S}_3$, διότι $L(\mathbf{V}) \cong \mathbf{V} \sqsubset \mathfrak{S}_4$ και $\mathrm{Aut}(\mathbf{V}) \cong \mathfrak{S}_3$. (Βλ. εδάφια 3.5.1, 3.5.8 (ii) και 4.5.16.)

Ασκήσεις

6-1. Να προσδιορισθούν οι χαρακτηριστικές υποομάδες
(i) τής συμμετρικής ομάδας $\mathfrak{S}_n$ για κάθε $n \in \mathbb{N}$, $n \geq 2$,
(ii) τής διεδρικής ομάδας $\mathbf{D}_n$ για κάθε $n \in \mathbb{N}$, $n \geq 3$, και
(iii) τής ομάδας $\mathbf{Q}$ των τετρανίων.

6-2. Να αποδειχθεί ότι όλες οι υποομάδες τής $\mathbb{Z}(p^\infty)$ (βλ. άσκηση **4-41**) είναι χαρακτηριστικές.

6-3. Έστω $(G, \cdot)$ μια ομάδα και έστω $H \trianglelefteq G$. Να αποδειχθεί ότι $H' \trianglelefteq G$.

6-4. Εάν $(G, \cdot)$ είναι μια ομάδα και $H := \{g \in G |\, \mathrm{card}(\kappa\lambda\Sigma_G(g)) < \infty\}$, να αποδειχθούν τα ακόλουθα:
(i) $H \sqsubseteq_{\chi\alpha\rho.} G$.
(ii) $|K'| < \infty$ για κάθε πεπερασμένως παραγόμενη υποομάδα K τής H.

6-5. Εάν $(G, \cdot)$ είναι μια πεπερασμένως παραγόμενη ομάδα, να αποδειχθούν τα ακόλουθα:
(i) $\mathrm{card}(\{H \in \mathbf{Subg}(G) |\, |G : H| < \infty\}) \in \mathbb{N}_0$.
(ii) Εάν η G διαθέτει μια υποομάδα πεπερασμένου δείκτη, τότε διαθέτει και μια χαρακτηριστική υποομάδα πεπερασμένου δείκτη.

6-6. Έστω $(G, \cdot)$ μια ομάδα και έστω $n \in \mathbb{N}$. Να αποδειχθεί ότι αμφότερες οι υποομάδες $H := \langle\{g^n |\, g \in G\}\rangle$ και $K := \langle\{g \in G |\, g^n = e_G\}\rangle$ είναι πλήρως αναλλοίωτες.

6-7. Έστω $(G, \cdot)$ μια ομάδα. Να αποδειχθεί ότι η $H := \langle \mathrm{tors}(G)\rangle \sqsubseteq G$ που παράγεται από το σύνολο στρέψεως αυτής (βλ. εδ. 2.3.1) είναι πλήρως αναλλοίωτη.

6-8. Να αποδειχθεί ότι $\mathrm{Hol}(\mathbb{Z}_2) \cong \mathbb{Z}_2$, $\mathrm{Hol}(\mathbb{Z}_3) \cong \mathfrak{S}_3$ και $\mathrm{Hol}(\mathbb{Z}_4) \cong \mathbf{D}_4$.

6-9. Έστω $(G, \cdot)$ μια ομάδα. Μια μετάταξη $\sigma \in \mathfrak{S}_G$ καλείται **ολομορφισμός** όταν

$$\sigma(xy^{-1}z) = \sigma(x)\sigma(y^{-1})\sigma(z),\ \forall (x, y, z) \in G \times G \times G.$$

Να αποδειχθεί ότι $\mathrm{Hol}(G) = K$, όπου $K := \{\sigma \in \mathfrak{S}_G | \, \sigma \text{ ολομορφισμός}\}$.

6-10. Εάν $(G, \cdot)$ είναι μια πλήρης ομάδα, να δειχθεί ότι $\mathrm{Hol}(G) = R(G) \circ L(G)$.

ΚΕΦΑΛΑΙΟ 7

Ευθέα, ημιευθέα και στεφανιαία γινόμενα

Στην πρώτη ενότητα τού παρόντος κεφαλαίου παρατίθενται ο ορισμός και οι κύριες ιδιότητες τού λεγομένου *ευθέος γινομένου* δύο ή και περισσότερων ομάδων (τόσον στην «εξωτερική» όσον και στην «εσωτερική» του εκδοχή). Στην §7.2 δίδεται η απόδειξη τού *θεωρήματος των Krull, Remak και Schmidt* (που είναι το ανάλογο τού *θεωρήματος τής ανταλλαγής* τού Steinitz που συναντά κανείς στη Γραμμική Άλγεβρα). Εν συνεχεία, παρατίθενται τρία σημαντικά θεωρήματα, στις αποδείξεις των οποίων υπεισέρχονται κατά τρόπο ουσιαστικό ορισμένες χαρακτηριστικές ιδιότητες των ευθέων γινομένων. (Βλ. 7.3.13, 7.4.2 και 7.5.3.) Συγκεκριμένα, στην ενότητα 7.3 περιγράφονται λεπτομερώς οι συνθήκες (τού Gauss) υπό τις οποίες η αβελιανή ομάδα $(\mathbb{Z}_m^\times, \cdot)$ είναι *κυκλική*, στην ενότητα 7.4 οι φυσικοί αριθμοί n για τους οποίους *όλες* οι ομάδες τάξεως n είναι κυκλικές (ήτοι ισόμορφες με την $(\mathbb{Z}_n, +)$) και στην ενότητα 7.5 ο τρόπος δομήσεως των *χαμιλτονιανών ομάδων*, ήτοι των μη αβελιανών ομάδων, όλες οι υποομάδες των οποίων είναι ορθόθετες.

Τέλος, οι ενότητες 7.6 και 7.8 είναι αφιερωμένες στην εισαγωγή και στην πρωταρχική μελέτη των χρησιμότερων γενικεύσεων τού ευθέος γινομένου, ήτοι τού *ημιευθέος γινομένου* και τού *στεφανιαίου γινόμενου*, αντιστοίχως. Εμβολίμως, στην §7.7, ολοκληρώνεται (κάνοντας ουσιαστική χρήση τού ημιευθέος γινομένου, τής εξισώσεως κλάσεων συζυγίας (5.64), τού θεωρήματος 5.7.1 τού Cauchy και τού τεχνάσματος 4.4.23 τού Poincaré) η μέχρις ισομορφισμού ταξινόμηση *όλων των ομάδων τάξεως* ≤ 15.

7.1 ΕΥΘΕΑ ΓΙΝΟΜΕΝΑ

► **«Εξωτερικό» ευθύ γινόμενο δύο ομάδων**. Το καρτεσιανό γινόμενο δύο ομάδων καθίσταται *κατά τρόπο φυσικό* (ήτοι μέσω «πολλαπλασιασμού κατά συντεταγμένες») *ομάδα*.

7.1.1 Ορισμός. (i) Έστω ότι οι $(G_1, \circledast)$ και $(G_2, \circledcirc)$ είναι τυχούσες ομάδες. Εφοδιάζοντας το καρτεσιανό γινόμενο $G_1 \times G_2$ των υποκειμένων συνόλων τους με την εσωτερική πράξη

$$\boxed{\begin{array}{c}(G_1 \times G_2) \times (G_1 \times G_2) \longrightarrow G_1 \times G_2 \\ ((x_1, x_2), (y_1, y_2)) \longmapsto (x_1, x_2) \boxdot (y_1, y_2) := (x_1 \circledast y_1, x_2 \circledcirc y_2),\end{array}} \tag{7.1}$$

παρατηρούμε ότι το ζεύγος $(G_1 \times G_2, \boxdot)$ αποτελεί ομάδα έχουσα (ως προς την ορισθείσα πράξη " $\boxdot$ ") το (e_{G_1}, e_{G_2}) ως ουδέτερο στοιχείο της και το (x_1^{-1}, x_2^{-1}) ως αντίστροφο (= συμμετρικό) στοιχείο οιουδήποτε $(x_1, x_2) \in G_1 \times G_2$, όπου x_1^{-1} το αντίστροφο στοιχείο τού $x_1 \in G_1$ ως προς την " $\circledast$ " και x_2^{-1} το αντίστροφο στοιχείο τού $x_2 \in G_2$ ως προς την "$\circledcirc$" (βλ. πρόταση 1.2.16). Η ομάδα $(G_1 \times G_2, \boxdot)$ καλείται **εξωτερικό ευθύ γινόμενο των** $(G_1, \circledast)$ **και** $(G_2, \circledcirc)$.

(ii) Η επίρριψη

$$\mathrm{pr}_1 : G_1 \times G_2 \to G_1,\ (x_1, x_2) \mapsto x_1, \quad (\text{και αντ., η } \mathrm{pr}_2 : G_1 \times G_2 \to G_2,\ (x_1, x_2) \mapsto x_2)$$

καλείται **πρώτη** (και αντιστοίχως, **δεύτερη**) **φυσική προβολή τής** $G_1 \times G_2$ **επί τής** G_1 (και αντιστοίχως, **επί τής** G_2). Επίσης, η ένριψη

$$\iota_1 : G_1 \to G_1 \times G_2,\ x \mapsto (x, e_{G_2}), \quad (\text{και αντ., η } \iota_2 : G_2 \to G_1 \times G_2,\ y \mapsto (e_{G_1}, y))$$

καλείται **φυσική εμφύτευση τής** G_1 **εντός τής** $G_1 \times G_2$ (και αντιστοίχως, **τής** G_2 **εντός τής** $G_1 \times G_2$).

(iii) Θεωρώντας τό εξωτερικό ευθύ γινόμενο των $(G_2, \circledcirc)$ και $(G_1, \circledast)$ (ήτοι *εναλλάσσοντας* τους ρόλους των δοθεισών ομάδων), παρατηρούμε ότι η απεικόνιση

$$G_1 \times G_2 \ni (x_1, x_2) \longmapsto (x_2, x_1) \in G_2 \times G_1$$

αποτελεί ισομορφισμό. Ως εκ τούτου, ο ανωτέρω ορισμός τού εξωτερικού ευθέος γινομένου είναι *μέχρις ισομορφισμού ανεξάρτητος* τού ποιον εκ δύο «παραγόντων» αναφέρουμε ως πρώτο και ποιον ως δεύτερο.

(iv) Εάν μια ομάδα είναι *ισόμορφη* με την $(G_1 \times G_2, \boxdot)$, τότε είθισται να λέμε ότι οι $(G_1, \circledast)$ και $(G_2, \circledcirc)$ είναι **ευθείς παράγοντές της**.

7.1.2 Πρόταση. *Οι* pr_1 *και* pr_2 *είναι επιμορφισμοί ομάδων έχοντες ως πυρήνες τους τις υποομάδες* $\mathrm{Ker}(\mathrm{pr}_1) = \{e_{G_1}\} \times G_2, \mathrm{Ker}(\mathrm{pr}_2) = G_1 \times \{e_{G_2}\}$, *οπότε*

$$(G_1 \times G_2) \,/\, (\{e_{G_1}\} \times G_2) \cong G_1 \ \text{ και } \ (G_1 \times G_2) \,/\, (G_1 \times \{e_{G_2}\}) \cong G_2.$$

ΑΠΟΔΕΙΞΗ. Για οιαδήποτε στοιχεία $(x_1, x_2), (y_1, y_2) \in G_1 \times G_2$ έχουμε

$$\begin{aligned} \mathrm{pr}_1((x_1, x_2) \boxdot (y_1, y_2)) &= \mathrm{pr}_1 (x_1 \circledast y_1, x_2 \circledcirc y_2) = x_1 \circledast y_1 \\ &= \mathrm{pr}_1 (x_1, x_2) \circledast \mathrm{pr}_1 (y_1, y_2) \end{aligned}$$

και, κατ' αναλογίαν,

$$\begin{aligned} \mathrm{pr}_2((x_1, x_2) \boxdot (y_1, y_2)) &= \mathrm{pr}_2 (x_1 \circledast y_1, x_2 \circledcirc y_2) = x_2 \circledcirc y_2 \\ &= \mathrm{pr}_2 (x_1, x_2) \circledcirc \mathrm{pr}_2 (y_1, y_2) . \end{aligned}$$

Άρα οι pr_1 και pr_2 είναι επιμορφισμοί ομάδων. Επιπροσθέτως,

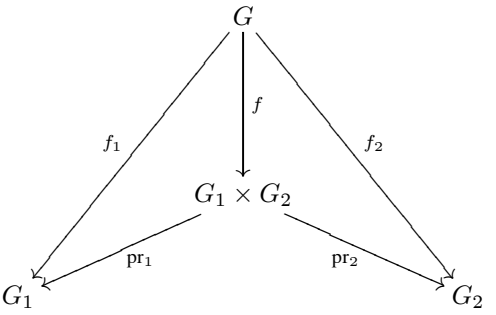
$$\mathrm{Ker}\,(\mathrm{pr}_1) = \{(x_1, x_2) \in G_1 \times G_2 \,|\mathrm{pr}_1((x_1, x_2) = e_{G_1}\} = \{e_{G_1}\} \times G_2$$

και, κατ' αναλογίαν, $\mathrm{Ker}(\mathrm{pr}_2) = G_1 \times \{e_{G_2}\}$. Οι ανωτέρω ισομορφισμοί προκύπτουν κατόπιν εφαρμογής τού 1ου θεωρήματος ισομορφισμών 4.5.2. □

7.1.3 Πρόταση. («Καθολική ιδιότητα» εξωτερικού ευθέος γινομένου) *Έστω $(G, *)$ μια ομάδα. Εάν οι $f_1 : G \longrightarrow G_1$ και $f_2 : G \longrightarrow G_2$ είναι ομομορφισμοί ομάδων, τότε υφίσταται ένας και μόνον ομομορφισμός ομάδων*

$$f : (G, *) \longrightarrow (G_1 \times G_2, \boxdot),$$

τέτοιος ώστε να ισχύει $\mathrm{pr}_1 \circ f = f_1$ και $\mathrm{pr}_2 \circ f = f_2$, δηλαδή τέτοιος ώστε το διάγραμμα



να καθίσταται μεταθετικό.

ΑΠΟΔΕΙΞΗ. Ορίζουμε την απεικόνιση

$$f : G \longrightarrow G_1 \times G_2, g \longmapsto f(g) := (f_1(g), f_2(g)).$$

Για κάθε $g \in G$ έχουμε

$$(\mathrm{pr}_1 \circ f)\,(g) = \mathrm{pr}_1(f_1(g), f_2(g)) = f_1(g)$$

και, κατ' αναλογίαν, $(\mathrm{pr}_2 \circ f)\,(g) = f_2(g)$. Εάν η $h : G \longrightarrow G_1 \times G_2$ είναι *τυχούσα* απεικόνιση με $\mathrm{pr}_1 \circ h = f_1$ και $\mathrm{pr}_2 \circ h = f_2$, τότε για κάθε $g \in G$ έχουμε

$$h(g) = (\mathrm{pr}_1(h(g)), \mathrm{pr}_2(h(g))) = (f_1(g), f_2(g)) = f(g),$$

οπότε $h = f$. Επιπροσθέτως, για οιαδήποτε στοιχεία $x, y \in G$ ισχύουν τα εξής:

$$f(x*y) = (\mathrm{pr}_1(f(x*y)), \mathrm{pr}_2(f(x*y))) = ((\mathrm{pr}_1 \circ f)(x*y), (\mathrm{pr}_2 \circ f)(x*y))$$
$$= (f_1(x*y), f_2(x*y)) = (f_1(x) \circledast f_1(y), f_2(x) \circledcirc f_2(y)) = (f_1(x), f_2(x)) \boxdot (f_1(y), f_2(y))$$
$$= ((\mathrm{pr}_1 \circ f)(x), (\mathrm{pr}_2 \circ f)(x)) \boxdot ((\mathrm{pr}_1 \circ f)(y), (\mathrm{pr}_2 \circ f)(y)) = f(x) \boxdot f(y).$$

Άρα η f είναι ομομορφισμός ομάδων. □

7.1.4 Πρόταση. *Ας συμβολίσουμε ως*

$$\overline{G}_1 := \mathrm{Im}(\iota_1) \ \textit{και} \ \ \overline{G}_2 := \mathrm{Im}(\iota_2)$$

τις εικόνες των φυσικών εμφυτεύσεων $\iota_1 : G_1 \longrightarrow G_1 \times G_2$ *και* $\iota_2 : G_2 \longrightarrow G_1 \times G_2$ *των* G_1, G_2 *εντός τής* $G_1 \times G_2$. *Τότε ισχύουν τα ακόλουθα*:

(i) *Οι* ι_1 *και* ι_2 *είναι μονομορφισμοί ομάδων και, ως εκ τούτου,*

$$G_1 \cong \iota_1(G_1) =: \overline{G}_1, \ \ G_2 \cong \iota_2(G_2) =: \overline{G}_2.$$

(ii) $\overline{G}_1 = \mathrm{Ker}(\mathrm{pr}_2) \trianglelefteq G_1 \times G_2$ *και* $\overline{G}_2 = \mathrm{Ker}(\mathrm{pr}_1) \trianglelefteq G_1 \times G_2$.
(iii) $\overline{G}_1 \cap \overline{G}_2 = \{e_{G_1 \times G_2}\}$.
(iv) $\overline{G}_1 \boxdot \overline{G}_2 = G_1 \times G_2$.

ΑΠΟΔΕΙΞΗ. (i) Για οιαδήποτε στοιχεία $x_1, y_1 \in G_1, x_2, y_2 \in G_2$ έχουμε

$$\iota_1(x_1 \circledast y_1) = (x_1 \circledast y_1, e_{G_2}) = \iota_1(x_1) \boxdot \iota_1(y_1)$$

και, κατ' αναλογίαν, $\iota_2(x_2 \circledast y_2) = \iota_2(x_2) \boxdot \iota_2(y_2)$, οπότε οι ι_1 και ι_2 είναι μονομορφισμοί ομάδων.
(ii) Λόγω τής προτάσεως 7.1.2,

$$\overline{G}_1 := \mathrm{Im}(\iota_1) = \{\iota_1(x_1) \,|x_1 \in G_1\} = \{(x_1, e_{G_2}) \,|x_1 \in G_1\} = G_1 \times \{e_{G_2}\} = \mathrm{Ker}\,(\mathrm{pr}_2)$$

και, κατ' αναλογίαν, $\overline{G}_2 = \mathrm{Ker}(\mathrm{pr}_1)$. Άρα $\overline{G}_1 \trianglelefteq G_1 \times G_2$ και $\overline{G}_2 \trianglelefteq G_1 \times G_2$. (Βλ. πόρισμα 4.2.31.)
(iii) Προφανώς,

$$\overline{G}_1 \cap \overline{G}_2 = \big\{(x_1, x_2) \in G_1 \times G_2 \,\big|(x_1, x_2) \in \overline{G}_1 \ \text{και} \ (x_1, x_2) \in \overline{G}_2\big\}$$
$$\underset{\text{(ii)}}{=} \{(x_1, x_2) \in G_1 \times G_2 \,|x_1 = e_{G_1} \ \text{και} \ x_2 = e_{G_2}\} = \{(e_{G_1}, e_{G_2})\} = \{e_{G_1 \times G_2}\}.$$

(iv) Προφανώς,

$$\overline{G}_1 \boxdot \overline{G}_2 := \big\{(x_1, x_2) \boxdot (y_1, y_2) \,\big|(x_1, x_2) \in \overline{G}_1 \ \text{και} \ (x_1, x_2) \in \overline{G}_2\big\} \subseteq G_1 \times G_2.$$

Από την άλλη μεριά, για οιοδήποτε στοιχείο $(x_1, x_2) \in G_1 \times G_2$ έχουμε

$$(x_1, x_2) = (x_1, e_{G_2}) \boxdot (e_{G_1}, x_2) \in \overline{G}_1 \boxdot \overline{G}_2,$$

οπότε ισχύει και ο αντίστροφος εγκλεισμός $G_1 \times G_2 \subseteq \overline{G}_1 \boxdot \overline{G}_2$. □

7.1.5 Σημείωση. (Απλούστευση συμβολισμού) Στον ορισμό 7.1.1 και στις προτάσεις 7.1.2, 7.1.3 και 7.1.4 χρησιμοποιήσαμε τα σύμβολα " $\circledast$ ", " $\circledcirc$ ", " $\boxdot$ " για τη σήμανση των εσωτερικών πράξεων επί των G_1, G_2 και $G_1 \times G_2$, αντιστοίχως, προκειμένου να περιγράψουμε επακριβώς τους μεταξύ τους υφιστάμενους συσχετισμούς και τη συμπεριφορά τους ύστερα από εφαρμογή των φυσικών προβολών, των εμφυτεύσεων κ.ά. Ωστόσο, η περαιτέρω διατήρηση ενός τόσο δυσκίνητου συμβολισμού θα μας ήταν κάτι το πολύ φορτικό. Γι' αυτόν τον λόγο θα μεταβούμε, από εδώ και στο εξής, στον *απλουστευμένο πολλαπλασιαστικό* συμβολισμό των πράξεων *και των τριών* ομάδων G_1, G_2 και $G_1 \times G_2$ (μέσω τού συνήθους dot[1] " $\cdot$ "), χωρίς επιπρόσθετη συμβολιστική επιβάρυνση[2]. Εξαίρεση θα αποτελέσει μόνον η περίπτωση κατά την οποία θα χρησιμοποιούμε τον *προσθετικό συμβολισμό* για τις πράξεις *αμφοτέρων* των G_1 και G_2, οπότε και θα γράφουμε (ιδιαιτέρως) $G_1 \oplus G_2$ αντί τού $G_1 \times G_2$.

► **Υποομάδες εξωτερικού ευθέος γινομένου δύο ομάδων**. Εάν η H_1 είναι μια υποομάδα μιας ομάδας G_1 και η H_2 μια υποομάδα μιας ομάδας G_2, τότε το εξωτερικό ευθύ γινόμενο $H_1 \times H_2$ των H_1 και H_2 αποτελεί υποομάδα τής $G_1 \times G_2$. Ωστόσο, το αντίστροφο δεν είναι πάντοτε αληθές: Εν γένει, ενδέχεται να υπάρχουν υποομάδες $L \sqsubseteq G_1 \times G_2$ οι οποίες δεν εκφράζονται ως εξωτερικά ευθέα γινόμενα τού προαναφερθέντος είδους. Πλήρης περιγραφή των υποομάδων και των ορθόθετων υποομάδων τής $G_1 \times G_2$ παρέχεται μέσω των θεωρημάτων 7.1.10 και 7.1.14, αντιστοίχως, των οφειλομένων στους μαθηματικούς E. Goursat[3] (1858-1936) και R. Remak[4] (1888-1943).

7.1.6 Πρόταση. *Εάν οι G_1, G_2 είναι δυο ομάδες, τότε για την $G_1 \times G_2$ ισχύουν τα εξής*:

(i) *Εάν $H_1 \sqsubseteq G_1$ και $H_2 \sqsubseteq G_2$, τότε $H_1 \times H_2 \sqsubseteq G_1 \times G_2$, οπότε*

$$\mathbf{Subg}(G_1) \times \mathbf{Subg}(G_2) \subseteq \mathbf{Subg}(G_1 \times G_2).$$

(ii) *Εάν $H_1 \trianglelefteq G_1$ και $H_2 \trianglelefteq G_2$, τότε $H_1 \times H_2 \trianglelefteq G_1 \times G_2$, οπότε*

$$\mathbf{Subg}(G_1) \times \mathbf{NSubg}(G_2) \subseteq \mathbf{NSubg}(G_1 \times G_2).$$

Επιπροσθέτως,

$$\boxed{(G_1 \times G_2) \,/\, (H_1 \times H_2) \cong (G_1/H_1) \times (G_2/H_2)\,.} \tag{7.2}$$

(iii) *Εάν $H_1 \sqsubseteq G_1$, $H_2 \sqsubseteq G_2$ και $H_1 \times H_2 \trianglelefteq G_1 \times G_2$, τότε $H_1 \trianglelefteq G_1$ και $H_2 \trianglelefteq G_2$.*

[1] Είναι βεβαίως αυτονόητο ότι σε ορισμένες εφαρμογές και σε ορισμένα παραδείγματα, στα οποία μία εκ των υπεισερχομένων ομάδων έχει ως πράξη της τη σύνθεση ή τη (συνήθη) πρόσθεση, το dot υποκαθίσταται αυτομάτως από τα " $\circ$ " και " $+$ ".

[2] Γράφοντας, από εδώ και στο εξής, $G_1 \times G_2$ (χωρίς άλλα σχόλια), θα εννοούμε ότι το εν λόγω καρτεσιανό γινόμενο είναι εφοδιασμένο με την πράξη (7.1). (Ως γνωστόν, ένα τέτοιο καρτεσιανό γινόμενο ομάδων θα μπορούσε να καταστεί ομάδα και με κάποια πράξη *διαφορετική* τής (7.1). Πρβλ. άσκηση **2-33**.)

[3] Βλ. σελ. 48 τού άρθρου τού E. Goursat: *Sur les substitutions orthogonales et des divisions régulières de l' espace,* Ann. Sci. Ècole Norm. Sup. **6** (1889), 9-102.

[4] Βλ. R. Remak: *Über die Darstellung der endlichen Gruppen als Untergruppen direkter Produkte*, Jour. reine und angew. Math. **163** (1930), 1-44.

ΑΠΟΔΕΙΞΗ. (i) Εάν $H_1 \sqsubseteq G_1$ και $H_2 \sqsubseteq G_2$, τότε

$$H_1 \times H_2 \subseteq G_1 \times G_2, \;\; e_{G_1 \times G_2} = (e_{G_1}, e_{G_2}) \in H_1 \times H_2$$

και για οιαδήποτε διατεταγμένα ζεύγη $(x_1, y_1), (x_2, y_2) \in H_1 \times H_2$ έχουμε

$$(x_1, y_1)(x_2, y_2)^{-1} = (x_1, y_1)\left(x_2^{-1}, y_2^{-1}\right) = \left(x_1 x_2^{-1}, y_1 y_2^{-1}\right) \in H_1 \times H_2,$$

οπότε $H_1 \times H_2 \sqsubseteq G_1 \times G_2$ (επί τη βάσει τού (iii) τής προτάσεως 2.1.16).

(ii) Εάν $H_1 \trianglelefteq G_1$ και $H_2 \trianglelefteq G_2$, τότε ορίζεται ο επιμορφισμός ομάδων

$$f : G_1 \times G_2 \longrightarrow (G_1/H_1) \times (G_2/H_2),$$
$$(g_1, g_2) \longmapsto f(g_1, g_2) := (\pi_{H_1}^{G_1}(g_1), \pi_{H_2}^{G_2}(g_2)) = (g_1 H_1, g_2 H_2).$$

Επειδή $\mathrm{Ker}(f) = \{(g_1, g_2) \in G_1 \times G_2 \,|\, g_1 \in H_1 \text{ και } g_2 \in H_2\} = H_1 \times H_2$, έχουμε $H_1 \times H_2 \trianglelefteq G_1 \times G_2$ (βλ. πόρισμα 4.2.31). Εφαρμόζοντας το 1ο θεώρημα ισομορφισμών 4.5.2 για τον f διασφαλίζουμε την ύπαρξη ενός ισομορφισμού (7.2).

(iii) Ας υποθέσουμε ότι $H_1 \sqsubseteq G_1$, $H_2 \sqsubseteq G_2$ και $H_1 \times H_2 \trianglelefteq G_1 \times G_2$. Για $i = 1, 2$ θεωρούμε τυχόντα στοιχεία $x_i \in H_i$ και $g_i \in G_i$. Τότε

$$H_1 \times H_2 \ni (g_1, g_2)(x_1, x_2)(g_1, g_2)^{-1},$$
$$(g_1, g_2)(x_1, x_2)(g_1, g_2)^{-1} = (g_1, g_2)(x_1, x_2)(g_1^{-1}, g_2^{-1}) = \left(g_1 x_1 g_1^{-1}, g_2 x_2 g_2^{-1}\right),$$

οπότε $[g_1 x_1 g_1^{-1} \in H_1 \text{ και } g_2 x_2 g_2^{-1} \in H_2] \Rightarrow [H_1 \trianglelefteq G_1 \text{ και } H_2 \trianglelefteq G_2]$. □

7.1.7 Σημείωση. Εάν $G := \mathbb{Z}_2 \oplus \mathbb{Z}_4$ και $H_1 := \mathbb{Z}_2 \oplus \{[0]_4\}, H_2 := \{[0]_2\} \oplus \langle [2]_4 \rangle$, τότε $H_1 \trianglelefteq G$ και $H_2 \trianglelefteq G$ (λόγω τού (ii) τής προτάσεως 7.1.6) και $G/H_1 \cong \mathbb{Z}_4$ (βλ. 7.1.2). Από την άλλη μεριά,

$$G/H_2 = \{H_2, ([0]_2, [1]_4) + H_2, ([1]_2, [0]_4) + H_2, ([1]_2, [1]_4) + H_2\}$$

και η απεικόνιση

$$H_2 \longmapsto \mathrm{id}, \qquad ([0]_2, [1]_4) + H_2 \longmapsto [1\,2] \circ [3\,4],$$
$$([1]_2, [0]_4) + H_2 \longmapsto [1\,3] \circ [2\,4], \quad ([1]_2, [1]_4) + H_2 \longmapsto [1\,4] \circ [2\,3],$$

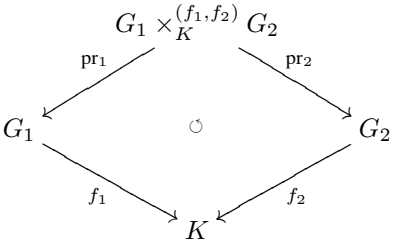
αποτελεί έναν ισομορφισμό μεταξύ τής πηλικοομάδας G/H_2 και τής ομάδας $\mathbf{V}$ των τεσσάρων στοιχείων τού Klein (3.4.2 (ii)). Επομένως,

$$H_1 \cong H_2 \cong \mathbb{Z}_2 \;\text{ αλλά }\; G/H_1 \cong \mathbb{Z}_4 \ncong \mathbf{V} \cong G/H_2. \;\text{ (Βλ. 4.5.7 (iii)).}$$

7.1.8 Ορισμός. Εάν G_1, G_2 είναι δυο ομάδες και $f_1 : G_1 \longrightarrow K$, $f_2 : G_2 \longrightarrow K$ ομομορφισμοί ομάδων, τότε το

$$\boxed{G_1 \times_K^{(f_1, f_2)} G_2 := \{(x, y) \in G_1 \times G_2 |\, f_1(x) = f_2(y)\}}$$

καλείται **ινικό γινόμενο** των f_1 και f_2 και καθιστά το ακόλουθο διάγραμμα μεταθετικό:



7.1.9 Λήμμα. $G_1 \times_K^{(f_1,f_2)} G_2 \sqsubseteq G_1 \times G_2$.

ΑΠΟΔΕΙΞΗ. Προφανώς, $e_{G_1\times G_2} = (e_{G_1}, e_{G_2}) \in G_1 \times_K^{(f_1,f_2)} G_2$, διότι (σύμφωνα με το (i) τής προτάσεως 2.4.3) ισχύει $f_1(e_{G_1}) = e_K = f_2(e_{G_2})$. Επίσης, εάν $(x_1, y_1), (x_2, y_2) \in G_1 \times_K^{(f_1,f_2)} G_2$, τότε

$$(x_1, y_1)\,(x_2, y_2)^{-1} = (x_1, y_1)\left(x_2^{-1}, y_2^{-1}\right) = \left(x_1 x_2^{-1}, y_1 y_2^{-1}\right) \in G_1 \times_K^{(f_1,f_2)} G_2,$$

διότι

$$\begin{aligned} f_1(x_1 x_2^{-1}) &= f_1(x_1) f_1(x_2^{-1}) = f_1(x_1) f_1(x_2)^{-1} \\ &= f_2(y_1) f_2(y_2)^{-1} = f_2(y_1) f_2(y_2^{-1}) = f_2(y_1 y_2^{-1}), \end{aligned}$$

οπότε $G_1 \times_K^{(f_1,f_2)} G_2 \sqsubseteq G_1 \times G_2$. (Βλ. 2.1.16 (iii).) □

7.1.10 Θεώρημα. (E. Goursat, 1889/ R. Remak, 1930) *Εάν G_1, G_2 είναι δυο ομάδες, τότε για την $G_1 \times G_2$ ισχύουν τα εξής*:

(i) *Υφίσταται μια αμφίρριψη*

$$\mathbf{Subg}(G_1 \times G_2) \xrightarrow{\mathfrak{V}} \left\{ \begin{array}{c} \text{τριάδες} \\ (H_1/K_1, H_2/K_2, f) \end{array} \middle| \begin{array}{c} H_1, K_1 \in \mathbf{Subg}(G_1) : K_1 \trianglelefteq H_1, \\ H_2, K_2 \in \mathbf{Subg}(G_2) : K_2 \trianglelefteq H_2, \\ \text{και } f : H_1/K_1 \longrightarrow H_2/K_2 \\ \text{ένας ισομορφισμός} \end{array} \right\}$$

οριζόμενη μέσω τού τύπου

$$\boxed{L \longmapsto \mathfrak{V}(L) := \left(\mathrm{pr}_1(L)/\mathrm{pr}_1(\overline{G}_1 \cap L), \mathrm{pr}_2(L)/\mathrm{pr}_2(\overline{G}_2 \cap L), f_L\right),}$$

για κάθε $L \sqsubseteq G_1 \times G_2$, όπου

$$f_L(x\,\mathrm{pr}_1(\overline{G}_1 \cap L)) := y\,\mathrm{pr}_2(\overline{G}_2 \cap L),$$

για κάθε $x \in \mathrm{pr}_1(L)$ και $y \in G_2$, τέτοιο ώστε $(x, y) \in L$. Η $\mathfrak{V}$ έχει την

$$\boxed{(H_1/K_1, H_2/K_2, f) \longmapsto L_f,} \tag{7.3}$$

ως αντίστροφό της, όπου

$$L_f := H_1 \times_{H_2/K_2}^{(f\circ\pi_{K_1}^{H_1},\pi_{K_2}^{H_2})} H_2 = \{(x,y) \in H_1 \times H_2 \,|f\,(xK_1) = yK_2\}\,.$$

(ii) *Εάν* $L \sqsubseteq G_1 \times G_2$, *τότε* $\mathrm{pr}_1(\overline{G}_1 \cap L) \times \mathrm{pr}_2(\overline{G}_2 \cap L) \trianglelefteq L$ *και*

$$\boxed{\begin{aligned} L/(\mathrm{pr}_1(\overline{G}_1 \cap L) \times \mathrm{pr}_2(\overline{G}_2 \cap L)) &\cong \mathrm{pr}_1(L)/\mathrm{pr}_1(\overline{G}_1 \cap L) \\ &\cong \mathrm{pr}_2(L)/\mathrm{pr}_2(\overline{G}_2 \cap L). \end{aligned}} \tag{7.4}$$

Ως εκ τούτου,

$$\boxed{\begin{aligned} L = \mathrm{pr}_1(\overline{G}_1 \cap L) \times \mathrm{pr}_2(\overline{G}_2 \cap L) \quad &\Longleftrightarrow \quad \mathrm{pr}_1(\overline{G}_1 \cap L) = \mathrm{pr}_1(L) \\ &\Longleftrightarrow \quad \mathrm{pr}_2(\overline{G}_2 \cap L) = \mathrm{pr}_2(L). \end{aligned}}$$

(iii) *Εάν οι* G_1, G_2 *είναι πεπερασμένες ομάδες και* $L \sqsubseteq G_1 \times G_2$, *τότε*

$$\boxed{|\mathrm{pr}_1(L)|\,\left|\mathrm{pr}_2(\overline{G}_2 \cap L)\right| = |L| = \left|\mathrm{pr}_1(\overline{G}_1 \cap L)\right|\,|\mathrm{pr}_2(L)|} \tag{7.5}$$

και

$$\boxed{|G_1 : \mathrm{pr}_1(L)|\,\left|G_2 : \mathrm{pr}_2(\overline{G}_2 \cap L)\right| = |G_1 \times G_2 : L| = \left|G_1 : \mathrm{pr}_1(\overline{G}_1 \cap L)\right|\,|G_2 : \mathrm{pr}_2(L)|\,.}$$

ΑΠΟΔΕΙΞΗ. (i) Έστω τυχούσα $L \sqsubseteq G_1 \times G_2$. Επειδή για $i = 1, 2$ η προβολή pr_i είναι επιμορφισμός και $\overline{G}_i \trianglelefteq G_1 \times G_2$ (βλ. 7.1.2 και 7.1.4 (ii)) έχουμε

$$\left.\begin{aligned} \overline{G}_i &\trianglelefteq G_1 \times G_2 \\ \overline{G}_i &\sqsubseteq \langle \overline{G}_i, L\rangle \sqsubseteq G_1 \times G_2 \end{aligned}\right\} \underset{4.2.19}{\Longrightarrow} \overline{G}_i \trianglelefteq \langle \overline{G}_i, L\rangle \underset{4.5.12\,\text{(ii)}}{\Longrightarrow} \overline{G}_i \cap L \trianglelefteq L$$

και (σύμφωνα με το (i) τής προτάσεως 2.4.6 και το (i) τής προτάσεως 4.2.30)

$$\overline{G}_i \cap L \trianglelefteq L \sqsubseteq G_1 \times G_2 \Rightarrow \mathrm{pr}_i(\overline{G}_i \cap L) \trianglelefteq \mathrm{pr}_i(L) \sqsubseteq \mathrm{pr}_i(G_1 \times G_2) = G_i,$$

όπου

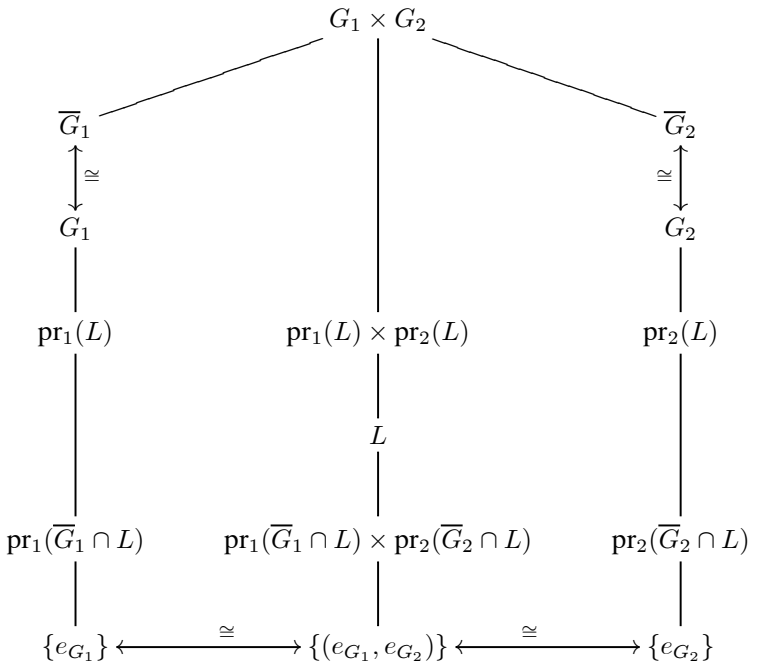
$$\mathrm{pr}_1(L) = \{x \in G_1 \,|\exists y \in G_2 : (x,y) \in L\}\,,\ \mathrm{pr}_2(L) = \{y \in G_2 \,|\exists x \in G_1 : (x,y) \in L\}\,,$$

και $\mathrm{pr}_1(\overline{G}_1 \cap L) = \{x \in G_1 \,|(x, e_{G_2}) \in L\}\,, \mathrm{pr}_2(\overline{G}_2 \cap L) = \{y \in G_2 \,|(e_{G_1}, y) \in L\}\,.$

Προφανώς,

$$\mathrm{pr}_1(\overline{G}_1 \cap L) \times \mathrm{pr}_2(\overline{G}_2 \cap L) \sqsubseteq L \sqsubseteq \mathrm{pr}_1(L) \times \mathrm{pr}_2(L).$$

Τα τμήματα των διαγραμμάτων τού Hasse για τις ανωτέρω υποομάδες των G_1, G_2 και $G_1 \times G_2$ εικονογραφούνται ως ακολούθως:



Εν συνεχεία ορίζουμε την $\theta_L : \mathrm{pr}_1(L) \longrightarrow \mathrm{pr}_2(L)/\mathrm{pr}_2(\overline{G}_2 \cap L)$ ως εξής: Για κάθε στοιχείο $x \in \mathrm{pr}_1(L)$ υπάρχει κάποιο $y \in G_2 : (x, y) \in L$. Προφανώς, $y \in \mathrm{pr}_2(L)$. Θέτουμε $\theta_L(x) := y\ \mathrm{pr}_2(\overline{G}_2 \cap L)$. Επειδή το y *δεν* είναι κατ' ανάγκην μονοσημάντως ορισμένο μέσω τού x, για να αποδείξουμε ότι η θ_L είναι *καλώς ορισμένη απεικόνιση* αρκεί να αποδείξουμε ότι η πλευρική κλάση $\theta_L(x)$ δεν εξαρτάται από την επιλογή τού y. Προς τούτο θεωρούμε οιοδήποτε $z \in \mathrm{pr}_2(L)$ για το οποίο $(x, z) \in L$. Τότε

$$L \ni (x, y)^{-1}(x, z) = \left(x^{-1}, y^{-1}\right)(x, z) = \left(x^{-1}x, y^{-1}z\right) = \left(e_{G_1}, y^{-1}z\right) \in \overline{G}_2,$$

οπότε $\left(e_{G_1}, y^{-1}z\right) \in \overline{G}_2 \cap L \Rightarrow y^{-1}z \in \mathrm{pr}_2(\overline{G}_2 \cap L) \Rightarrow y\ \mathrm{pr}_2(\overline{G}_2 \cap L) = z\ \mathrm{pr}_2(\overline{G}_2 \cap L)$. Για τυχόντα $x_1, x_2 \in \mathrm{pr}_1(L)$ και $y_1, y_2 \in G_2$ με $(x_1, y_1) \in L$ και $(x_2, y_2) \in L$ έχουμε $y_1, y_2 \in \mathrm{pr}_2(L)$ και

$$\begin{aligned}
&(x_1x_2, y_1, y_2) = (x_1, y_1)(x_2, y_2) \in L \\
&\Rightarrow \theta_L(x_1x_2) = (y_1y_2)\ \mathrm{pr}_2(\overline{G}_2 \cap L) = \left(y_1\ \mathrm{pr}_2(\overline{G}_2 \cap L)\right)\left(y_2\ \mathrm{pr}_2(\overline{G}_2 \cap L)\right) \\
&\Rightarrow \theta_L(x_1x_2) = \theta_L(x_1)\,\theta_L(x_2),
\end{aligned}$$

οπότε η θ_L είναι ομομορφισμός ομάδων. Επίσης, η θ_L είναι επιριπτική (διότι για κάθε $y \in \mathrm{pr}_2(L)$ υπάρχει κάποιο στοιχείο $x \in G_1$ με $(x, y) \in L$, οπότε $x \in \mathrm{pr}_1(L)$ και $\theta_L(x) = y\ \mathrm{pr}_2(\overline{G}_2 \cap L)$). Επειδή

$$\begin{aligned}
\mathrm{Ker}(\theta_L) &= \left\{x \in \mathrm{pr}_1(L) \,\middle|\, \exists y \in \mathrm{pr}_2(\overline{G}_2 \cap L) : (x, y) = (x, e_{G_2})(e_{G_1}, y) \in L\right\} \\
&= \left\{x \in \mathrm{pr}_1(L) \,\middle|\, x \in \mathrm{pr}_1(\overline{G}_1)\right\} = \mathrm{pr}_1(\overline{G}_1 \cap L),
\end{aligned}$$

το 1ο θεώρημα ισομορφισμών 4.5.2 μας πληροφορεί ότι η απεικόνιση

$$f_L : \mathrm{pr}_1(L)/\mathrm{pr}_1(\overline{G}_1 \cap L) \longrightarrow \mathrm{pr}_2(L)/\mathrm{pr}_2(\overline{G}_2 \cap L)$$
$$f_L(x\,\mathrm{pr}_1(\overline{G}_1 \cap L)) := \theta_L(x)\,,\ \forall x \in \mathrm{pr}_1(L),$$

αποτελεί ισομορφισμό ομάδων. Επιπροσθέτως,

$$\begin{aligned}
L_{f_L} &= \left\{(x,y) \in \mathrm{pr}_1(L) \times \mathrm{pr}_2(L) \,\middle|\, f_L(x\,\mathrm{pr}_1(\overline{G}_1 \cap L)) = y\,\mathrm{pr}_2(\overline{G}_2 \cap L)\right\} \\
&= \left\{(x,y) \in \mathrm{pr}_1(L) \times \mathrm{pr}_2(L) \,\middle|\, \begin{array}{c} w\,\mathrm{pr}_2(\overline{G}_2 \cap L) = y\,\mathrm{pr}_2(\overline{G}_2 \cap L) \\ \text{για κάποιο } w \in G_2 : (x,w) \in L \end{array}\right\} \\
&= \left\{(x,y) \in \mathrm{pr}_1(L) \times \mathrm{pr}_2(L) \,\middle|\, \begin{array}{c} w^{-1}y \in \mathrm{pr}_2(\overline{G}_2 \cap L) \\ \text{για κάποιο } w \in G_2 : (x,w) \in L \end{array}\right\} \\
&= \left\{(x,y) \in \mathrm{pr}_1(L) \times \mathrm{pr}_2(L) \,\middle|\, \begin{array}{c} (e_{G_1}, w^{-1}y) \in L \text{ για κάποιο} \\ w \in G_2 : (x,w) \in L \end{array}\right\} = L,
\end{aligned}$$

διότι $(x,w)\,(e_{G_1}, w^{-1}y) = (x,y) \in L$. Και αντιστρόφως· εάν $H_i, K_i \in \mathbf{Subg}(G_i)$: $K_i \trianglelefteq H_i$ για $i = 1,2$ και $f : H_1/K_1 \longrightarrow H_2/K_2$ ένας ισομορφισμός, τότε

$$L_f := H_1 \times_{H_2/K_2}^{(f\circ\pi_{K_1}^{H_1}, \pi_{K_2}^{H_2})} H_2 \sqsubseteq H_1 \times H_2 \Rightarrow L_f \sqsubseteq G_1 \times G_2.$$

(Βλ. λήμμα 7.1.9 και 7.1.6 (i).) Επιπροσθέτως,

$$\begin{aligned}
\mathrm{pr}_1(L_f) &= \{x \in G_1 \,|\exists y \in G_2 : (x,y) \in L_f\} \\
&= \{x \in H_1 \,|\exists y \in H_2 : f(xK_1) = yK_2\} = H_1
\end{aligned}$$

(διότι η f είναι εξ υποθέσεως ισομορφισμός) και

$$\begin{aligned}
\mathrm{pr}_1(\overline{G}_1 \cap L_f) &= \{x \in G_1 \,|(x, e_{G_2}) \in L_f\} = \{x \in G_1 \,|x \in H_1,\ xK_1 \in \mathrm{Ker}(f)\} \\
&= \{x \in H_1 \,|xK_1 \in \mathrm{Ker}(f)\} = K_1
\end{aligned}$$

(διότι $\mathrm{Ker}(f) = K_1$). Κατ' αναλογίαν, $\mathrm{pr}_2(L_f) = H_2$ και $\mathrm{pr}_2(\overline{G}_2 \cap L_f) = K_2$. Άρα η $\mathfrak{V}$ είναι όντως μια αμφίρριψη.

(ii) Έστω $\mathrm{pr}_1|_L : L \longrightarrow \mathrm{pr}_1(L)$ ο περιορισμός τής πρώτης προβολής επί τού L και έστω

$$\pi = \pi^{\mathrm{pr}_1(L)}_{\mathrm{pr}_1(\overline{G}_1 \cap L)} : \mathrm{pr}_1(L) \longrightarrow \mathrm{pr}_1(L)/\mathrm{pr}_1(\overline{G}_1 \cap L)$$

ο φυσικός επιμορφισμός. Ο πυρήνας τού επιμορφισμού $\pi \circ (\mathrm{pr}_1|_L)$ είναι η ομάδα

$$\begin{aligned}
\mathrm{Ker}(\pi \circ (\mathrm{pr}_1|_L)) &= \left\{(x,y) = (x, e_{G_2})\,(e_{G_1}, y) \in L \,\middle|\, x \in \mathrm{pr}_1(\overline{G}_1 \cap L)\right\} \\
&= \left\{(x,y) \in L \middle| x \in \mathrm{pr}_1(\overline{G}_1 \cap L), (e_{G_1}, y) = (x, e_{G_2})^{-1}\,(x,y) \in L\right\} \\
&= \mathrm{pr}_1(\overline{G}_1 \cap L) \times \mathrm{pr}_2(\overline{G}_2 \cap L),
\end{aligned}$$

οπότε $\mathrm{pr}_1(\overline{G}_1 \cap L) \times \mathrm{pr}_2(\overline{G}_2 \cap L) \trianglelefteq L$ (βλ. 4.2.31) και (βάσει τού 1ου θεωρήματος ισομορφισμών 4.5.2)

$$L/(\mathrm{pr}_1(\overline{G}_1 \cap L) \times \mathrm{pr}_2(\overline{G}_2 \cap L)) \cong \mathrm{pr}_1(L)/\mathrm{pr}_1(\overline{G}_1 \cap L) \xrightarrow[f_L]{\cong} \mathrm{pr}_2(L)/\mathrm{pr}_2(\overline{G}_2 \cap L).$$

(iii) Λόγω των (7.4) οι ισότητες (7.5) είναι αληθείς. Οι ισότητες στις οποίες υπεισέρχονται οι δείκτες αποδεικνύονται με τη βοήθεια τού θεωρήματος 4.1.22 τού Lagrange. □

7.1.11 Πόρισμα. *Εάν G_1, G_2 είναι δυο πεπερασμένες ομάδες, για τις τάξεις των οποίων ισχύει* $\mu\kappa\delta(|G_1|, |G_2|) = 1$ *και* $L \sqsubseteq G_1 \times G_2$, *τότε*

$$L = \mathrm{pr}_1(\overline{G}_1 \cap L) \times \mathrm{pr}_2(\overline{G}_2 \cap L) \tag{7.6}$$

$$\text{και } \mathbf{Subg}(G_1) \times \mathbf{Subg}(G_2) = \mathbf{Subg}(G_1 \times G_2). \tag{7.7}$$

ΑΠΟΔΕΙΞΗ. Επειδή (κατά το 7.1.10 (i)) $\mathrm{pr}_1(L) \sqsubseteq G_1$ και $\mathrm{pr}_2(L) \sqsubseteq G_2$, έχουμε (σύμφωνα με το θεώρημα 4.1.22 τού Lagrange και το πόρισμα B.2.6)

$$\left\{ \begin{array}{l} \mu\kappa\delta(|\mathrm{pr}_1(L)|, |\mathrm{pr}_2(L)|) \mid |\mathrm{pr}_1(L)| \text{ και } |\mathrm{pr}_1(L)| \mid |G_1| \Rightarrow \mu\kappa\delta(|\mathrm{pr}_1(L)|, |\mathrm{pr}_2(L)|) \mid |G_1| \\ \mu\kappa\delta(|\mathrm{pr}_1(L)|, |\mathrm{pr}_2(L)|) \mid |\mathrm{pr}_2(L)| \text{ και } |\mathrm{pr}_2(L)| \mid |G_2| \Rightarrow \mu\kappa\delta(|\mathrm{pr}_1(L)|, |\mathrm{pr}_2(L)|) \mid |G_2| \end{array} \right\},$$

και $\mu\kappa\delta(|\mathrm{pr}_1(L)|, |\mathrm{pr}_2(L)|) \mid \mu\kappa\delta(|G_1|, |G_2|) = 1 \Rightarrow \mu\kappa\delta(|\mathrm{pr}_1(L)|, |\mathrm{pr}_2(L)|) = 1$. Κατά το 7.1.10 (i),

$$\mathrm{pr}_1(L)/\mathrm{pr}_1(\overline{G}_1 \cap L) \xrightarrow[f_L]{\cong} \mathrm{pr}_2(L)/\mathrm{pr}_2(\overline{G}_2 \cap L),$$

απ' όπου έπεται ότι

$$\left. \begin{array}{r} |\mathrm{pr}_1(L)|\,|\mathrm{pr}_2(\overline{G}_2 \cap L)| = |\mathrm{pr}_2(L)|\,|\mathrm{pr}_1(\overline{G}_1 \cap L)| \\ \mu\kappa\delta(|\mathrm{pr}_1(L)|, |\mathrm{pr}_2(L)|) = 1 \end{array} \right\} \underset{\text{B.2.9}}{\Longrightarrow} \left\{ \begin{array}{l} |\mathrm{pr}_1(L)| \mid |\mathrm{pr}_1(\overline{G}_1 \cap L)| \\ |\mathrm{pr}_2(L)| \mid |\mathrm{pr}_2(\overline{G}_2 \cap L)| \end{array} \right\}.$$

Επειδή $\mathrm{pr}_i(\overline{G}_i \cap L) \trianglelefteq \mathrm{pr}_i(L)$, έχουμε τελικώς $\mathrm{pr}_i(L) = \mathrm{pr}_i(\overline{G}_i \cap L)$ για $i = 1, 2$. Η (7.6) προκύπτει από το 7.1.10 (ii). Για την απόδειξη τής ισότητας (7.7) αρκεί να συνδυάσουμε τον εγκλεισμό " $\subseteqq$ " τον αποδειχθέντα στο (i) τής προτάσεως 7.1.6 με τον εγκλεισμό " $\supseteqq$ " τον προκύπτοντα από την (7.6). □

7.1.12 Παρατήρηση. Εάν οι G_1 και G_2 είναι δυο πεπερασμένες ομάδες με $\mu\kappa\delta(|G_1|, |G_2|) \geq 2$ και $L \sqsubseteq G_1 \times G_2$, τότε η L δεν είναι κατ' ανάγκην εκφράσιμη υπό τη μορφή (7.6). Επί παραδείγματι, εάν $G_1 = \langle a \rangle$ και $G_2 = \langle b \rangle$ είναι δυο κυκλικές ομάδες τάξεως 2, τότε η κυκλική υποομάδα

$$L := \langle (a, b) \rangle = \langle (a, e_{G_2})(e_{G_1}, b) \rangle = \{(e_{G_1}, e_{G_2}), (a, b)\}$$

τής $G_1 \times G_2$ έχει τάξη 2, ενώ

$$\begin{aligned} \mathrm{pr}_1(\overline{G}_1 \cap L) &= \mathrm{pr}_1\left(\{(e_{G_1}, e_{G_2}), (a, e_{G_2})\} \cap \{(e_{G_1}, e_{G_2}), (a, b)\}\right) \\ &= \mathrm{pr}_1\left(\{(e_{G_1}, e_{G_2})\}\right) = \{e_{G_1}\} \subsetneqq \mathrm{pr}_1(L) = \{e_{G_1}, a\} \end{aligned}$$

και, κατ' αναλογίαν,

$$\begin{aligned} \mathrm{pr}_2(\overline{G}_2 \cap L) &= \mathrm{pr}_2\left(\{(e_{G_1}, e_{G_2}), (e_{G_1}, b)\} \cap \{(e_{G_1}, e_{G_2}), (a, b)\}\right) \\ &= \mathrm{pr}_2\left(\{(e_{G_1}, e_{G_2})\}\right) = \{e_{G_2}\} \subsetneqq \mathrm{pr}_2(L) = \{e_{G_2}, b\}, \end{aligned}$$

οπότε $\{e_{G_1}\} \times \{e_{G_2}\} = \{(e_{G_1}, e_{G_2})\} \subsetneqq L$.

7.1.13 Παράδειγμα. Ποιο είναι το σύνολο $\mathbf{Subg}(\mathbb{Z}_3\oplus\mathbb{Z}_9)$ των υποομάδων τής ομάδας $\mathbb{Z}_3 \oplus \mathbb{Z}_9$; Κατ' αρχάς,

$$\mathbf{Subg}(\mathbb{Z}_3) = \{\{[0]_3\},\, \mathbb{Z}_3\},\ \mathbf{Subg}(\mathbb{Z}_9) = \{\{[0]_9\},\, \langle [3]_9\rangle\ (\cong \mathbb{Z}_3),\, \mathbb{Z}_9\}$$

(βλ. 2.4.26 (ii)) και

$$\mathbf{Subg}(\mathbb{Z}_3) \times \mathbf{Subg}(\mathbb{Z}_9) = \left\{ \begin{array}{c} \{([0]_3, [0]_9)\},\, \{[0]_3\} \oplus \langle [3]_9\rangle\,,\, \{[0]_3\} \oplus \mathbb{Z}_9, \\ \mathbb{Z}_3 \oplus \{[0]_3\},\, \mathbb{Z}_3 \oplus \langle [3]_9\rangle\,,\, \mathbb{Z}_3 \oplus \mathbb{Z}_9. \end{array} \right\}.$$

Αρκεί λοιπόν ο προσδιορισμός τού $\mathbf{Subg}(\mathbb{Z}_3\oplus\mathbb{Z}_9)\smallsetminus(\mathbf{Subg}(\mathbb{Z}_3)\times\mathbf{Subg}(\mathbb{Z}_9))$. Προς τούτο θεωρούμε το σύνολο

$$\left\{ \begin{array}{c} \text{ζεύγη} \\ (H_1/K_1, H_2/K_2) \end{array} \middle| \begin{array}{c} H_1, K_1 \in \mathbf{Subg}(\mathbb{Z}_3) : K_1 \lhd H_1, \\ H_2, K_2 \in \mathbf{Subg}(\mathbb{Z}_9) : K_2 \lhd H_2, \\ H_1/K_1 \cong H_2/K_2. \end{array} \right\}. \tag{7.8}$$

Το (7.8) ισούται με το $\{(\mathbb{Z}_3/\{[0]_3\}, \langle [3]_9\rangle/\{[0]_9\}), (\mathbb{Z}_3/\{[0]_3\}, \mathbb{Z}_9/\langle [3]_9\rangle)\}$. Παρατηρούμε ότι καθεμιά εκ των προκυπτουσών πηλικοομάδων είναι ισόμορφη με την $\mathbb{Z}_3$ και υπενθυμίζουμε ότι η ομάδα των αυτομορφισμών τής $\mathbb{Z}_3$ είναι ισόμορφη με την $\mathbb{Z}_3^\times$ (που είναι μια κυκλική ομάδα τάξεως 2), βλ. 2.4.32 (ii). Άρα μεταξύ των μελών καθενός εκ των ανωτέρω ζευγών πηλικοομάδων υφίστανται ακριβώς δύο (διαφορετικοί) ισομορφισμοί, ήτοι οι

$$\begin{array}{ccc} \mathbb{Z}_3/\{[0]_3\} \xrightarrow{f_1} \langle [3]_9\rangle/\{[0]_9\}, & \Big\| & \mathbb{Z}_3/\{[0]_3\} \xrightarrow{f_2} \langle [3]_9\rangle/\{[0]_9\}, \\ [0]_3 + \{[0]_3\} \mapsto [0]_9 + \{[0]_9\} & \Big\| & [0]_3 + \{[0]_3\} \mapsto [0]_9 + \{[0]_9\} \\ [1]_3 + \{[0]_3\} \mapsto [3]_9 + \{[0]_9\} & \Big\| & [1]_3 + \{[0]_3\} \mapsto [6]_9 + \{[0]_9\} \\ [2]_3 + \{[0]_3\} \mapsto [6]_9 + \{[0]_9\} & \Big\| & [2]_3 + \{[0]_3\} \mapsto [3]_9 + \{[0]_9\} \end{array}$$

και

$$\begin{array}{ccc} \mathbb{Z}_3/\{[0]_3\} \xrightarrow{\check{f}_1} \mathbb{Z}_9/\langle [3]_9\rangle\,, & \Big\| & \mathbb{Z}_3/\{[0]_3\} \xrightarrow{\check{f}_2} \mathbb{Z}_9/\langle [3]_9\rangle\,, \\ [0]_3 + \{[0]_3\} \mapsto [0]_9 + \langle [3]_9\rangle & \Big\| & [0]_3 + \{[0]_3\} \mapsto [0]_9 + \langle [3]_9\rangle \\ [1]_3 + \{[0]_3\} \mapsto [1]_9 + \langle [3]_9\rangle & \Big\| & [1]_3 + \{[0]_3\} \mapsto [2]_9 + \langle [3]_9\rangle \\ [2]_3 + \{[0]_3\} \mapsto [2]_9 + \langle [3]_9\rangle & \Big\| & [2]_3 + \{[0]_3\} \mapsto [1]_9 + \langle [3]_9\rangle \end{array}$$

αντιστοίχως. Αυτό σημαίνει ότι

$$\mathbf{Subg}(\mathbb{Z}_3 \oplus \mathbb{Z}_9)\smallsetminus(\mathbf{Subg}(\mathbb{Z}_3) \times \mathbf{Subg}(\mathbb{Z}_9)) = \left\{L_{f_1}, L_{f_2}, L_{\check{f}_1}, L_{\check{f}_2}\right\},$$

όπου οι υποομάδες $L_{f_1}, L_{f_2}, L_{\check{f}_1}, L_{\check{f}_2}$ τής $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ καθορίζονται μέσω τού συνόλου

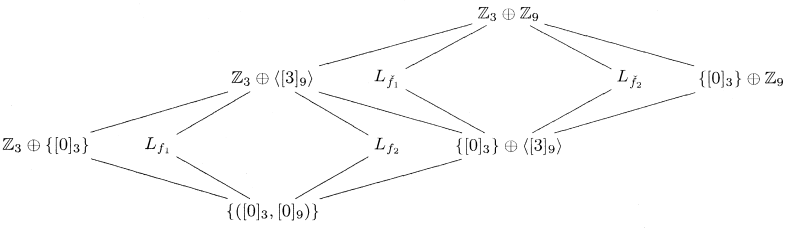
(7.8) και τής αμφιρρίψεως (7.3):

$$(\mathbb{Z}_3/\{[0]_3\}, \langle [3]_9\rangle/\{[0]_9\}, f_1) \mapsto L_{f_1} = \{([0]_3,[0]_9), ([1]_3,[3]_9), ([2]_3,[6]_9)\},$$
$$(\mathbb{Z}_3/\{[0]_3\}, \langle [3]_9\rangle/\{[0]_9\}, f_2) \mapsto L_{f_2} = \{([0]_3,[0]_9), ([1]_3,[6]_9), ([2]_3,[3]_9)\},$$

$$(\mathbb{Z}_3/\{[0]_3\}, \mathbb{Z}_9/\langle [3]_9\rangle, \check{f}_1) \mapsto L_{\check{f}_1} = \left\{ \begin{array}{l} ([0]_3,[0]_9), ([0]_3,[3]_9), ([0]_3,[6]_9), \\ ([1]_3,[1]_9), ([1]_3,[4]_9), ([1]_3,[7]_9), \\ ([2]_3,[2]_9), ([2]_3,[5]_9), ([2]_3,[8]_9) \end{array} \right\},$$

$$(\mathbb{Z}_3/\{[0]_3\}, \mathbb{Z}_9/\langle [3]_9\rangle, \check{f}_2) \mapsto L_{\check{f}_2} = \left\{ \begin{array}{l} ([0]_3,[0]_9), ([0]_3,[3]_9), ([0]_3,[6]_9), \\ ([1]_3,[2]_9), ([1]_3,[5]_9), ([1]_3,[8]_9), \\ ([2]_3,[1]_9), ([2]_3,[4]_9), ([2]_3,[7]_9) \end{array} \right\}.$$

Το διάγραμμα τού Hasse για τον σύνδεσμο $(\mathbf{Subg}(\mathbb{Z}_3 \oplus \mathbb{Z}_9), \sqsubseteq)$ είναι το εξής:



7.1.14 Θεώρημα. (R. Remak, 1930) *Εάν G_1, G_2 είναι δυο ομάδες και L μια υποομάδα τής $G_1 \times G_2$, τότε τα ακόλουθα είναι ισοδύναμα*:

(i) $L \trianglelefteq G_1 \times G_2$.

(ii) *Για $i = 1, 2$ η L ικανοποιεί τις συνθήκες:*

$$\boxed{\mathrm{pr}_i(\overline{G}_i \cap L) \trianglelefteq G_i \ \text{ και } \ \mathrm{pr}_i(L)/\mathrm{pr}_i(\overline{G}_i \cap L) \sqsubseteq Z(G_i/\mathrm{pr}_i(\overline{G}_i \cap L)).}$$

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Επειδή $\overline{G}_i \trianglelefteq G_1 \times G_2$ για $i = 1, 2$ (βλ. 7.1.4 (ii)) και (εξ υποθέσεως) $L \trianglelefteq G_1 \times G_2$, λαμβάνουμε (μέσω τής προτάσεως 4.2.8)

$$\overline{G}_i \cap L \trianglelefteq G_1 \times G_2 \underset{4.2.30\,\text{(i)}}{\Longrightarrow} \mathrm{pr}_i(\overline{G}_i \cap L) \trianglelefteq \mathrm{pr}_i(G_1 \times G_2) = G_i,$$

οπότε ορίζεται η υποομάδα $G_i/\mathrm{pr}_i(\overline{G}_i \cap L)$. Έστω τυχόν στοιχείο $x \in \mathrm{pr}_1(L)$. Τότε $\exists y \in G_2 : (x, y) \in L$. Για *οιοδήποτε* $z \in G_1$ έχουμε $(z, e_{G_2}) \in G_1 \times G_2$ και

$$L \trianglelefteq G_1 \times G_2 \Rightarrow (zxz^{-1}, y) = (z, e_{G_2})(x, y)(z, e_{G_2})^{-1} \in L.$$

Επειδή

$$\left.\begin{array}{r} (x,y) \in L \Rightarrow (x,y)^{-1} \in L \\ (zxz^{-1}, y) \in L \end{array}\right\} \Rightarrow (zxz^{-1}, y)(x,y)^{-1} = (zxz^{-1}x^{-1}, e_{G_2}) \in \overline{G}_1 \cap L,$$

συμπεραίνουμε ότι $zxz^{-1}x^{-1} = (zx)(xz)^{-1} \in \mathrm{pr}_1(\overline{G}_1 \cap L)$, οπότε

$$(zx)\,\mathrm{pr}_1(\overline{G}_1 \cap L) = (xz)\,\mathrm{pr}_1(\overline{G}_1 \cap L) \Rightarrow x\,\mathrm{pr}_1(\overline{G}_1 \cap L) \in Z(G_1/\mathrm{pr}_1(\overline{G}_1 \cap L)).$$

Εξ αυτού έπεται ότι $\mathrm{pr}_1(L)/\mathrm{pr}_1(\overline{G}_1 \cap L) \sqsubseteq Z(G_1/\mathrm{pr}_1(\overline{G}_1 \cap L))$. Κατ' αναλογίαν,

$$\mathrm{pr}_2(L)/\mathrm{pr}_2(\overline{G}_2 \cap L) \sqsubseteq Z(G_2/\mathrm{pr}_2(\overline{G}_2 \cap L)).$$

(ii)⇒(i) Χάριν συντομίας θέτουμε $M := \mathrm{pr}_1(\overline{G}_1 \cap L) \times \mathrm{pr}_2(\overline{G}_2 \cap L)$. Από το (ii) τού θεωρήματος 7.1.10 γνωρίζουμε ότι $M \trianglelefteq L$. Επειδή $\mathrm{pr}_i(\overline{G}_i \cap L) \trianglelefteq G_i$ για $i = 1, 2$ (εξ υποθέσεως), έχουμε επιπροσθέτως $M \trianglelefteq G_1 \times G_2$ (βλ. 7.1.6 (ii)). Επειδή (εξ υποθέσεως) για $i = 1, 2$

$$\mathrm{pr}_i(L)/\mathrm{pr}_i(\overline{G}_i \cap L) \sqsubseteq Z(G_i/\mathrm{pr}_i(\overline{G}_i \cap L)),$$

συνάγεται (μέσω τού 7.1.6 (i)) ότι

$$\mathrm{pr}_1(L)/\mathrm{pr}_1(\overline{G}_1 \cap L) \times \mathrm{pr}_2(L)/\mathrm{pr}_2(\overline{G}_2 \cap L) \sqsubseteq Z(G_1/\mathrm{pr}_1(\overline{G}_1 \cap L)) \times Z(G_2/\mathrm{pr}_2(\overline{G}_2 \cap L)). \tag{7.9}$$

Εν συνεχεία, παρατηρούμε ότι

$$\mathrm{pr}_1(L)/\mathrm{pr}_1(\overline{G}_1 \cap L) \times \mathrm{pr}_2(L)/\mathrm{pr}_2(\overline{G}_2 \cap L) \cong (\mathrm{pr}_1(L) \times \mathrm{pr}_2(L))\,/M \tag{7.10}$$

(επί τη βάσει τού (7.2)). Παρομοίως,

$$G_1/\mathrm{pr}_1(\overline{G}_1 \cap L) \times G_2/\mathrm{pr}_2(\overline{G}_2 \cap L) \cong (G_1 \times G_2)/M,$$

οπότε

$$Z(G_1/\mathrm{pr}_1(\overline{G}_1 \cap L)) \times Z(G_2/\mathrm{pr}_2(\overline{G}_2 \cap L)) \cong Z((G_1 \times G_2)/M). \tag{7.11}$$

Λόγω των (7.9), (7.10) και (7.11) η πηλικοομάδα $(\mathrm{pr}_1(L) \times \mathrm{pr}_2(L))\,/M$ είναι ισόμορφη με μια υποομάδα τού κέντρου $Z((G_1 \times G_2)/M)$ (με την οποία και την ταυτίζουμε). Ως εκ τούτου,

$$L \sqsubseteq \mathrm{pr}_1(L) \times \mathrm{pr}_2(L) \underset{\text{4.4.15 (i)}}{\Longrightarrow} L/M \sqsubseteq (\mathrm{pr}_1(L) \times \mathrm{pr}_2(L))\,/M \sqsubseteq Z((G_1 \times G_2)/M).$$

Κατά το (i) τής προτάσεως 5.4.19,

$$L/M \sqsubseteq Z((G_1 \times G_2)/M) \Longrightarrow L/M \trianglelefteq (G_1 \times G_2)/M,$$

οπότε $L \trianglelefteq G_1 \times G_2$ (βλ. 4.5.20 (i)). □

7.1.15 Πόρισμα. *Εάν G_1, G_2 είναι δυο ομάδες και $L \trianglelefteq G_1 \times G_2$, τότε*

$$\boxed{L/(\mathrm{pr}_1(\overline{G}_1 \cap L) \times \mathrm{pr}_2(\overline{G}_2 \cap L)) \cong (\mathrm{pr}_1(L) \times \mathrm{pr}_2(L))/L.}$$

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς,

$$[L \trianglelefteq G_1 \times G_2 \text{ και } L \sqsubseteq \mathrm{pr}_1(L) \times \mathrm{pr}_2(L) \sqsubseteq G_1 \times G_2] \underset{4.2.19}{\Longrightarrow} L \trianglelefteq \mathrm{pr}_1(L) \times \mathrm{pr}_2(L),$$

οπότε ορίζεται η πηλικοομάδα $(\mathrm{pr}_1(L)\times\ \mathrm{pr}_2(L))/L$. Επειδή (σύμφωνα με το (ii) τού θεωρήματος 7.1.10)

$$L/(\mathrm{pr}_1(\overline{G}_1 \cap L) \times \mathrm{pr}_2(\overline{G}_2 \cap L)) \cong \mathrm{pr}_1(L)/\mathrm{pr}_1(\overline{G}_1 \cap L),$$

αρκεί να αποδείξουμε ότι $(\mathrm{pr}_1(L)\times \mathrm{pr}_2(L))/L \cong \mathrm{pr}_1(L)/\mathrm{pr}_1(\overline{G}_1 \cap L)$. Έστω $(x,y)\,L$ η πλευρική κλάση τυχόντος στοιχείου $(x,y) \in \mathrm{pr}_1(L)\times \mathrm{pr}_2(L)$ εντός τής πηλικοομάδας $(\mathrm{pr}_1(L)\times \mathrm{pr}_2(L))/L$. Επειδή $y \in \mathrm{pr}_2(L)$, $\exists a \in G_1 : (a,y) \in L$. Θεωρούμε την

$$(\mathrm{pr}_1(L) \times \mathrm{pr}_2(L))/L \ni (x,y)\,L \overset{\mathfrak{z}}{\longmapsto} (xa^{-1})\mathrm{pr}_1(\overline{G}_1 \cap L).$$

Αυτή είναι *ανεξάρτητη τής επιλογής τού* a. Πράγματι· για *οιοδήποτε* $b \in G_1 : (b,y) \in L$ έχουμε

$$\left.\begin{aligned} (a,y) \in L &\Rightarrow (a,y)^{-1} \in L \\ (b,y) \in L &\Rightarrow (a,y)^{-1}(b,y) \in L \\ (x,e_{G_2}) &\in \mathrm{pr}_1(L) \times \mathrm{pr}_2(L) \\ L &\trianglelefteq \mathrm{pr}_1(L) \times \mathrm{pr}_2(L) \end{aligned}\right\} \Rightarrow (xa^{-1}bx^{-1}, e_{G_2}) \in \overline{G}_1 \cap L,$$

διότι $(xa^{-1}bx^{-1}, e_{G_2}) = (x,e_{G_2})\left((a,y)^{-1}(b,y)\right)(x,e_{G_2})^{-1}$. Επομένως,

$$\begin{aligned} &xa^{-1}bx^{-1} = (xa^{-1})(xb^{-1})^{-1} \in \mathrm{pr}_1(\overline{G}_1 \cap L) \\ &\Rightarrow (xa^{-1})\mathrm{pr}_1(\overline{G}_1 \cap L) = (xb^{-1})\mathrm{pr}_1(\overline{G}_1 \cap L). \end{aligned}$$

Επιπροσθέτως, η $\mathfrak{z}$ είναι *καλώς ορισμένη απεικόνιση*. Πράγματι· για οιαδήποτε στοιχεία $(x,y), (x',y') \in \mathrm{pr}_1(L)\times \mathrm{pr}_2(L)$ και $a, a' \in G_1 : (a,y) \in L$, $(a',y') \in L$, για τα οποία ισχύει

$$(x,y)\,L = (x',y')\,L \Rightarrow (x,y)\,(x',y')^{-1} = \left(xx'^{-1}, yy'^{-1}\right) \in L,$$

έχουμε $(a,y) \in L \Rightarrow (a,y)^{-1} = (a^{-1}, y^{-1}) \in L$ και

$$(a,y)^{-1}\left(xx'^{-1}, yy'^{-1}\right)(a',y') = (a^{-1}xx'^{-1}a', e_{G_2}) \in \overline{G}_1 \cap L,$$

οπότε $a^{-1}xx'^{-1}a' = \left(a^{-1}x\right)\left(a'^{-1}x'\right)^{-1} \in \mathrm{pr}_1(\overline{G}_1 \cap L)$. Εξ αυτού έπεται ότι

$$\left(a^{-1}x\right)\mathrm{pr}_1(\overline{G}_1 \cap L) = (a'^{-1}x')\mathrm{pr}_1(\overline{G}_1 \cap L).$$

Επειδή $L \trianglelefteq G_1 \times G_2$, η πηλικοομάδα $\mathrm{pr}_1(L)/\mathrm{pr}_1(\overline{G}_1 \cap L)$ είναι *αβελιανή*, αφού

$$\mathrm{pr}_1(L)/\mathrm{pr}_1(\overline{G}_1 \cap L) \sqsubseteq Z(G_1/\mathrm{pr}_1(\overline{G}_1 \cap L))$$

(βλ. 7.1.14 (i)⇒(ii)). Ως εκ τούτου,

$$\begin{aligned}
\mathfrak{z}((x,y)\,L) &= (xa^{-1})\mathrm{pr}_1(\overline{G}_1\cap L) = \left(x\,\mathrm{pr}_1(\overline{G}_1\cap L)\right)\left(a^{-1}\mathrm{pr}_1(\overline{G}_1\cap L)\right)\\
&= \left(a^{-1}\mathrm{pr}_1(\overline{G}_1\cap L)\right)\left(x\,\mathrm{pr}_1(\overline{G}_1\cap L)\right) = \left(a^{-1}x\right)\mathrm{pr}_1(\overline{G}_1\cap L)\\
&= (a'^{-1}x')\mathrm{pr}_1(\overline{G}_1\cap L) = \left(a'^{-1}\mathrm{pr}_1(\overline{G}_1\cap L)\right)\left(x'\,\mathrm{pr}_1(\overline{G}_1\cap L)\right)\\
&= \left(x'\,\mathrm{pr}_1(\overline{G}_1\cap L)\right)\left(a'^{-1}\mathrm{pr}_1(\overline{G}_1\cap L)\right)\\
&= (x'a'^{-1})\mathrm{pr}_1(\overline{G}_1\cap L) = \mathfrak{z}((x',y')L).
\end{aligned}$$

Η (προφανώς επιρριπτική) απεικόνιση $\mathfrak{z}$ είναι *επιμορφισμός* ομάδων, διότι για οιαδήποτε στοιχεία $(x,y)\,,(x',y')\in \mathrm{pr}_1(L)\times\,\mathrm{pr}_2(L)$ και

$$a,a'\in G_1 : (a,y)\in L, (a',y')\in L,$$

έχουμε $(aa',yy')\in L$ και

$$\begin{aligned}
&\mathfrak{z}(((x,y)\,L)((x',y')\,L)) = \mathfrak{z}((xx',yy')\,L) = \left(xx'(aa')^{-1}\right)\mathrm{pr}_1(\overline{G}_1\cap L)\\
&= \left(x\left(x'a'^{-1}\right)a^{-1}\right)\mathrm{pr}_1(\overline{G}_1\cap L) = \left((xa^{-1})\left(x'a'^{-1}\right)\right)\mathrm{pr}_1(\overline{G}_1\cap L)\\
&= \left(\left(xa^{-1}\right)\mathrm{pr}_1(\overline{G}_1\cap L)\right)\left(\left(x'a'^{-1}\right)\mathrm{pr}_1(\overline{G}_1\cap L)\right) = \mathfrak{z}((x,y)\,L)\mathfrak{z}((x',y')L),
\end{aligned}$$

όπου η τέταρτη ισότητα έπεται από το ότι η $\mathrm{pr}_1(L)/\mathrm{pr}_1(\overline{G}_1\cap L)$ είναι (όπως προαναφέραμε) αβελιανή. Ο πυρήνας τού επιμορφισμού $\mathfrak{z}$ είναι η υποομάδα

$$\begin{aligned}
\mathrm{Ker}(\mathfrak{z}) &= \left\{(x,y)\,L\in(\mathrm{pr}_1(L)\times\mathrm{pr}_2(L))/L\,\middle|\,(xa^{-1})\mathrm{pr}_1(\overline{G}_1\cap L) = \mathrm{pr}_1(\overline{G}_1\cap L)\right\}\\
&= \left\{(x,y)\,L\in(\mathrm{pr}_1(L)\times\mathrm{pr}_2(L))/L\,\middle|\,xa^{-1}\in\mathrm{pr}_1(\overline{G}_1\cap L)\right\}\\
&= \left\{(x,y)\,L\in(\mathrm{pr}_1(L)\times\mathrm{pr}_2(L))/L\,\middle|\,(xa^{-1},e_{G_2})\in L\right\}\\
&= \left\{(x,y)\,L\in(\mathrm{pr}_1(L)\times\mathrm{pr}_2(L))/L\,|\,(x,y)\in L\right\} = L,
\end{aligned}$$

όπου η προτελευταία ισότητα οφείλεται στο ότι $(a,y)\in L$ και $(xa^{-1},e_{G_2})\in L$, οπότε $(x,y) = (xa^{-1},e_{G_2})(a,y)\in L$. Κατά συνέπειαν, η $\mathfrak{z}$ είναι *ισομορφισμός* ομάδων (βλ. 2.4.15 και 4.5.2). □

► **Αυτομορφισμοί εξωτερικού ευθέος γινομένου δύο ομάδων**. Δοθεισών δυο ομάδων G_1 και G_2, πώς σχετίζονται οι ομάδες $\mathrm{Aut}(G_1)\times\,\mathrm{Aut}(G_2)$ και $\mathrm{Aut}(G_1\times G_2)$;

7.1.16 Πρόταση. *Εάν G_1,G_2 είναι δυο ομάδες, τότε η $\mathrm{Aut}(G_1)\times\,\mathrm{Aut}(G_2)$ είναι εμφυτεύσιμη εντός τής $\mathrm{Aut}(G_1\times G_2)$.*

ΑΠΟΔΕΙΞΗ. Ορίζουμε την απεικόνιση

$$\begin{aligned}
f : \mathrm{Aut}(G_1)\times\mathrm{Aut}(G_2) &\longrightarrow \mathrm{Aut}(G_1\times G_2)\\
(\vartheta_1,\vartheta_2) &\longmapsto f\,(\vartheta_1,\vartheta_2)
\end{aligned}$$

μέσω τού τύπου

$$\boxed{f\,(\vartheta_1,\vartheta_2)\,(g_1,g_2) := (\vartheta_1(g_1),\vartheta_2(g_2)),\ \forall(g_1,g_2)\in G_1\times G_2.} \tag{7.12}$$

Σημειωτέον ότι $f\left(\mathrm{id}_{G_1}, \mathrm{id}_{G_2}\right) = \mathrm{id}_{G_1 \times G_2}$. Και γενικότερα, για οιουσδήποτε αυτομορφισμούς $\vartheta_1, \chi_1 \in \mathrm{Aut}(G_1)$ και $\vartheta_2, \chi_2 \in \mathrm{Aut}(G_2)$ έχουμε

$$\left(f\left((\vartheta_1, \vartheta_2\right)\left(\chi_1, \chi_2\right)\right) :=) \, f\left(\vartheta_1 \circ \chi_1, \vartheta_2 \circ \chi_2\right) = f\left(\vartheta_1, \vartheta_2\right) \circ f\left(\chi_1, \chi_2\right).$$

Πράγματι· για κάθε στοιχείο $(g_1, g_2) \in G_1 \times G_2$ ισχύουν οι ισότητες

$$\begin{aligned} f\left(\vartheta_1 \circ \chi_1, \vartheta_2 \circ \chi_2\right)(g_1, g_2) &= \left(\left(\vartheta_1 \circ \chi_1\right)(g_1), \left(\vartheta_2 \circ \chi_2\right)(g_2)\right) \\ &= \left(\vartheta_1\left(\chi_1(g_1)\right), \vartheta_2\left(\chi_2(g_2)\right)\right) \\ &= f\left(\vartheta_1, \vartheta_2\right)\left(\chi_1(g_1), \chi_2(g_2)\right) \\ &= f\left(\vartheta_1, \vartheta_2\right)\left(f\left(\chi_1, \chi_2\right)(g_1, g_2)\right) \\ &= \left(f\left(\vartheta_1, \vartheta_2\right) \circ f\left(\chi_1, \chi_2\right)\right)(g_1, g_2). \end{aligned}$$

Άρα η f είναι ομομορφισμός ομάδων. Επιπροσθέτως,

$$\begin{aligned} \mathrm{Ker}\,(f) &= \left\{\left(\vartheta_1, \vartheta_2\right) \in \mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2) \,|\, f\left(\vartheta_1, \vartheta_2\right) = \ \mathrm{id}_{G_1 \times G_2}\right\} \\ &= \left\{\left(\vartheta_1, \vartheta_2\right) \in \mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2) \,\middle|\, \begin{array}{c} \left(\vartheta_1(g_1), \vartheta_2(g_2)\right) = (g_1, g_2), \\ \forall (g_1, g_2) \in G_1 \times G_2 \end{array}\right\} \\ &= \left\{\left(\vartheta_1, \vartheta_2\right) \in \mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2) \,\middle|\, \begin{array}{c} \vartheta_1(g_1) = g_1, \ \forall g_1 \in G_1 \\ \text{και } \vartheta_2(g_2) = g_2, \ \forall g_2 \in G_2 \end{array}\right\} \\ &= \left\{\left(\mathrm{id}_{G_1}, \mathrm{id}_{G_2}\right)\right\}, \end{aligned}$$

οπότε η f είναι μονομορφισμός (βλ. πρόταση 2.4.15) και το εξωτερικό ευθύ γινόμενο $\mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2)$ των ομάδων αυτομορφισμών $\mathrm{Aut}(G_1)$ και $\mathrm{Aut}(G_2)$ εμφυτεύεται στην ομάδα των αυτομορφισμών $\mathrm{Aut}(G_1 \times G_2)$ τού εξωτερικού ευθέος γινομένου $G_1 \times G_2$ των G_1 και G_2 (βλ. ορισμό 2.4.14). □

Ο μονομορφισμός (7.12) δεν είναι πάντοτε ισομορφισμός. (Πρβλ. τα παραδείγματα 7.1.73 και 7.1.74). Ορισμένες ικανές συνθήκες για να είναι ο (7.12) ισομορφισμός δίδονται στις προτάσεις 7.1.17 και 7.1.19.

7.1.17 Πρόταση. *Εάν G_1, G_2 είναι δυο ομάδες με*

$$\overline{G}_1 := \mathrm{Im}(\iota_1) \sqsubseteq_{\text{χαρ.}} G_1 \times G_2 \ \text{ και } \ \overline{G}_2 := \mathrm{Im}(\iota_2) \sqsubseteq_{\text{χαρ.}} G_1 \times G_2,$$

τότε

$$\boxed{\mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2) \cong \mathrm{Aut}(G_1 \times G_2).}$$

ΑΠΟΔΕΙΞΗ. Έστω τυχών αυτομορφισμός $\omega \in \mathrm{Aut}(G_1 \times G_2)$. Ορίζουμε τους επιριπτικούς[5] ενδομορφισμούς

$$\varkappa_1 : \overline{G}_1 \longrightarrow \overline{G}_1, \ \left(g_1, e_{G_2}\right) \longmapsto \varkappa_1\left(g_1, e_{G_2}\right) := \left(\mathrm{pr}_1(\omega\left(g_1, e_{G_2}\right)), e_{G_2}\right),$$
$$\varkappa_2 : \overline{G}_2 \longrightarrow \overline{G}_2, \ \left(e_{G_1}, g_2\right) \longmapsto \varkappa_2\left(e_{G_1}, g_2\right) := \left(e_{G_1}, \mathrm{pr}_2(\omega\left(e_{G_1}, g_2\right))\right).$$

[5] Για $i = 1, 2$ η $\mathrm{pr}_i \circ \omega$ είναι επιριπτική ως σύνθεση επιριπτικών απεικονίσεων. Άρα και η $\varkappa_i$ είναι επιριπτική.

Επειδή $\overline{G}_1 \sqsubseteq_{\text{χαρ.}} G_1 \times G_2$ και $\overline{G}_2 \sqsubseteq_{\text{χαρ.}} G_1 \times G_2$ έχουμε για κάθε $(g_1, g_2) \in G_1 \times G_2$,

$$\omega\,(g_1, e_{G_2}) \in \overline{G}_1 = G_1 \times \{e_{G_2}\} \Rightarrow \mathrm{pr}_2(\omega\,(g_1, e_{G_2})) = e_{G_2},$$
$$\omega\,(e_{G_1}, g_2) \in \overline{G}_2 = \{e_{G_1}\} \times G_2 \Rightarrow \mathrm{pr}_1(\omega\,(e_{G_1}, g_2)) = e_{G_1}.$$

Έστω τυχόν $g_1 \in G_1$ με $(g_1, e_{G_2}) \in \mathrm{Ker}(\varkappa_1)$. Τότε $\mathrm{pr}_1(\omega\,(g_1, e_{G_2})) = e_{G_1}$, οπότε

$$\begin{aligned}\omega\,(g_1, e_{G_2}) &= (\mathrm{pr}_1(\omega\,(g_1, e_{G_2})), \mathrm{pr}_2(\omega\,(g_1, e_{G_2}))) \\ &= (e_{G_1}, e_{G_2}) = \omega(e_{G_1}, e_{G_2}) \Rightarrow g = e_{G_1}\end{aligned}$$

(λόγω τής ενριπτικότητας τού ω). Επομένως, $\mathrm{Ker}(\varkappa_1) = \{(e_{G_1}, e_{G_2})\} = \{e_{\overline{G}_1}\}$, απ' όπου έπεται ότι ο $\varkappa_1$ είναι *και* ενριπτικός (βλ. πρόταση 2.4.15). Ως εκ τούτου, έχουμε $\varkappa_1 \in \mathrm{Aut}(\overline{G}_1)$. Παρομοίως αποδεικνύουμε ότι $\varkappa_2 \in \mathrm{Aut}(\overline{G}_2)$. Εν συνεχεία, παρατηρούμε ότι μέσω των αυτομορφισμών $\varkappa_i$, $i = 1, 2$ κατασκευάζονται οι αυτομορφισμοί $\vartheta_i := \iota_i \circ \varkappa_i \circ (\iota_i^{-1}\big|_{\overline{G}_i}) \in \mathrm{Aut}(G_i)$ με

$$\vartheta_1 : G_1 \longrightarrow G_1,\ g_1 \longmapsto \vartheta_1\,(g_1) = \mathrm{pr}_1(\omega\,(g_1, e_{G_2})),$$
$$\vartheta_2 : G_2 \longrightarrow G_2,\ g_2 \longmapsto \vartheta_2\,(g_2) = \mathrm{pr}_2(\omega\,(e_{G_1}, g_2)).$$

Προφανώς,

$$\begin{aligned}\omega\,(g_1, g_2) &= \omega\,((g_1, e_{G_2})\,(e_{G_1}, g_2)) = \omega\,((g_1, e_{G_2}))\,\omega\,((e_{G_1}, g_2)) \\ &= (\mathrm{pr}_1(\omega\,(g_1, e_{G_2})), \mathrm{pr}_2(\omega\,(g_1, e_{G_2})))\,(\mathrm{pr}_1(\omega\,(e_{G_1}, g_2)), \mathrm{pr}_2(\omega\,(e_{G_1}, g_2))) \\ &= (\vartheta_1(g_1), e_{G_2})\,(e_{G_1}, \vartheta_2(g_2)) = (\vartheta_1(g_1)e_{G_1}, e_{G_2}\vartheta_2(g_2)) \\ &= (\vartheta_1(g_1), \vartheta_2(g_2)) = f(\vartheta_1, \vartheta_2)\,(g_1, g_2)\,.\end{aligned}$$

Αυτό σημαίνει ότι $\omega = f(\vartheta_1, \vartheta_2)$, ήτοι ότι η απεικόνιση f (η ορισθείσα μέσω τού τύπου (7.12)) είναι *και επιρριπτική*, οπότε αποτελεί έναν *ισομορφισμό* ομάδων.□

7.1.18 Παρατήρηση. Εάν G_1, G_2 είναι δυο ομάδες, τότε οι $\overline{G}_1$ και $\overline{G}_2$ δεν είναι κατ' ανάγκην χαρακτηριστικές (καίτοι *είναι* ορθόθετες) υποομάδες τής $G_1 \times G_2$. Επί παραδείγματι, εάν $G_1 = G_2 =: G$, με την G *μη τετριμμένη*, τότε η απεικόνιση

$$\vartheta : G \times G \longrightarrow G \times G,\ (g_1, g_2) \longmapsto \vartheta(g_1, g_2) := (g_2, g_1),$$

είναι ένας αυτομορφισμός τής $G \times G$. Ωστόσο, για κάθε $g \in G \smallsetminus \{e_G\}$ έχουμε

$$\vartheta(g, e_G) = (e_G, g) \notin G \times \{e_G\} \ \text{ και } \ \vartheta(e_G, g) = (g, e_G) \notin \{e_G\} \times G.$$

7.1.19 Πρόταση. *Εάν G_1, G_2 είναι δυο πεπερασμένες ομάδες, για τις τάξεις των οποίων ισχύει* μκδ$(|G_1|, |G_2|) = 1$, *τότε*

$$\boxed{\mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2) \cong \mathrm{Aut}(G_1 \times G_2).}$$

ΑΠΟΔΕΙΞΗ. Αρκεί να αποδείξουμε ότι, εν τοιαύτη περιπτώσει, ο μονομορφισμός (7.12) είναι ισομορφισμός. Έστω τυχών αυτομορφισμός $\omega \in \mathrm{Aut}(G_1 \times G_2)$. Θεωρούμε τους ομομορφισμούς

$$\begin{array}{cc} \delta : G_2 \longrightarrow G_1 & \varepsilon : G_1 \longrightarrow G_2 \\ y \longmapsto \delta(y) := \mathrm{pr}_1(\omega(e_{G_1}, y)) & x \longmapsto \varepsilon(x) := \mathrm{pr}_2(\omega(x, e_{G_2})). \end{array}$$

Παρατηρούμε ότι $\left\{ y^{|G_1|} \,|y \in G_2 \right\} \subseteq \mathrm{Ker}(\delta)$, καθόσον

$$\delta\left(y^{|G_1|}\right) = \mathrm{pr}_1(\omega\left(e_{G_1}, y^{|G_1|}\right)) = \mathrm{pr}_1(\omega(e_{G_1}, y)^{|G_1|}) = \mathrm{pr}_1(\omega(e_{G_1}, y))^{|G_1|} = e_{G_1}.$$

Επειδή $\mu\kappa\delta(|G_1|, |G_2|) = 1$, έχουμε[6] $\mathrm{card}\left(\left\{ y^{|G_1|} \,|y \in G_2 \right\}\right) = |G_2|$, οπότε

$$\left\{ y^{|G_1|} \,|y \in G_2 \right\} = \mathrm{Ker}(\delta) = G_2. \tag{7.13}$$

Κατ' αναλογίαν αποδεικνύουμε ότι

$$\left\{ x^{|G_2|} \,|x \in G_1 \right\} = \mathrm{Ker}(\varepsilon) = G_1. \tag{7.14}$$

Εν συνεχεία, ορίζουμε τους ενδομορφισμούς $\omega_1 \in \mathrm{End}(G_1)$ και $\omega_2 \in \mathrm{End}(G_2)$ ως εξής:

$$x \longmapsto \omega_1(x) := \mathrm{pr}_1(\omega(x, e_{G_2})), \qquad y \longmapsto \omega_2(y) := \mathrm{pr}_2(\omega(e_{G_1}, y)).$$

Ισχυρισμός: $\omega_1 \in \mathrm{Aut}(G_1)$ και $\omega_2 \in \mathrm{Aut}(G_2)$. Πράγματι· για οιοδήποτε στοιχείο $x \in \mathrm{Ker}(\omega_1)$ έχουμε $\omega(x, e_{G_2}) = (\omega_1(x), \omega_2(e_{G_2})) = (e_{G_1}, e_{G_2}) \Rightarrow x = e_{G_1}$ (λόγω τής ενριπτικότητας τού ω). Επομένως, $\mathrm{Ker}(\omega_1) = \{e_{G_1}\}$, απ' όπου έπεται ότι ο ενδομορφισμός ω_1 είναι ενριπτικός (βλ. πρόταση 2.4.15). Επειδή η G_1 είναι πεπερασμένη ομάδα, ο ω_1 είναι κατ' ανάγκην και επιρριπτικός. Ως εκ τούτου, έχουμε $\omega_1 \in \mathrm{Aut}(G_1)$. Παρομοίως αποδεικνύουμε ότι $\omega_2 \in \mathrm{Aut}(G_2)$, οπότε ο ισχυρισμός είναι αληθής.

Τέλος, για κάθε ζεύγος $(x, y) \in G_1 \times G_2$ έχουμε $\delta(y) = e_{G_2}$ και $\varepsilon(x) = e_{G_1}$ (βάσει των (7.13) και (7.14)), οπότε

$$\begin{aligned} \omega(x, y) &= \omega((x, e_{G_2})(e_{G_1}, y)) = \omega((x, e_{G_2}))\,\omega((e_{G_1}, y)) \\ &= (\mathrm{pr}_1(\omega(x, e_{G_2})), \mathrm{pr}_2(\omega(x, e_{G_2})))\,(\mathrm{pr}_1(\omega(e_{G_1}, y)), \mathrm{pr}_2(\omega(e_{G_1}, y))) \\ &= (\omega_1(x), \varepsilon(x))\,(\delta(y), \omega_2(y)) = (\omega_1(x)\delta(y), \varepsilon(x)\,\omega_2(y)) \\ &= (\omega_1(x)e_{G_2}, e_{G_1}\omega_2(y)) = (\omega_1(x), \omega_2(y)) = f(\omega_1, \omega_2)(x, y). \end{aligned}$$

Αυτό σημαίνει ότι $\omega = f(\omega_1, \omega_2)$, ήτοι ότι η απεικόνιση f (η ορισθείσα μέσω τού τύπου (7.12)) είναι *και επιρριπτική*, οπότε αποτελεί έναν *ισομορφισμό* ομάδων. □

[6] Εάν $\exists y, z \in G_2 : y^{|G_1|} = z^{|G_1|}$, τότε $\left(yz^{-1}\right)^{|G_1|} = e_{G_2}$, οπότε (βάσει τής προτάσεως 2.3.8 και τού πορίσματος 4.1.27) έχουμε $\mathrm{ord}(yz^{-1}) \mid |G_1|$ και $\mathrm{ord}(yz^{-1}) \mid |G_2|$. Εξ αυτού έπεται ότι

$$\mathrm{ord}(yz^{-1}) \mid \mu\kappa\delta(|G_1|, |G_2|) = 1 \Rightarrow \mathrm{ord}(yz^{-1}) = 1 \Rightarrow yz^{-1} = e_{G_2} \Rightarrow y = z.$$

Μια ενδιαφέρουσα γενίκευση τής προτάσεως 7.1.19 περιλαμβάνεται στο επόμενο θεώρημα[7]:

7.1.20 Θεώρημα. (J.N.S. Bidwell, M.J. Curran και D.J. McCauchan, 2006) *Εάν G_1, G_2 είναι δυο πεπερασμένες ομάδες χωρίς κοινούς ευθείς παράγοντες*[8]*, τότε*

$$\boxed{\mathrm{Aut}(G_1 \times G_2) \cong \mathcal{A}\,,}$$

όπου το

$$\mathcal{A} := \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \middle| \begin{array}{ccc} \alpha \in \mathrm{Aut}(G_1), & & \beta \in \mathrm{Hom}(G_2, Z(G_1)) \\ \gamma \in \mathrm{Hom}(G_1, Z(G_2)), & & \delta \in \mathrm{Aut}(G_2) \end{array} \right\}$$

είναι εφοδιασμένο με τη δομή ομάδας μέσω «πολλαπλασιασμού πινάκων[9]*»*

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} := \begin{pmatrix} \alpha \circ \alpha' + \beta \circ \gamma' & \alpha \circ \beta' + \beta \circ \delta' \\ \gamma \circ \alpha' + \delta \circ \gamma' & \gamma \circ \beta' + \delta \circ \delta' \end{pmatrix}.$$

Ιδιαιτέρως,

$$|\mathrm{Aut}(G_1 \times G_2)| = |\mathrm{Aut}(G_1)|\,|\mathrm{Aut}(G_2)|\,|\mathrm{Hom}(G_1, Z(G_2))|\,|\mathrm{Hom}(G_2, Z(G_1))|\,.$$

Επιπροσθέτως, ισχύουν τα εξής:

(i) *Έστω p ένας πρώτος αριθμός. Η* $\mathrm{Aut}(G_1 \times G_2)$ *είναι μια p-ομάδα* (βλ. εδάφια 5.7.2, 5.7.3) *εάν και μόνον εάν αμφότερες οι ομάδες αυτομορφισμών* $\mathrm{Aut}(G_1)$ *και* $\mathrm{Aut}(G_2)$ *είναι p-ομάδες.*

(ii) *Εάν* $\mu\kappa\delta(\left|G_1^{\mathrm{ab}}\right|, |Z(G_2)|) = 1 = \mu\kappa\delta(\left|G_2^{\mathrm{ab}}\right|, |Z(G_1)|)$*, τότε*

$$\mathrm{Aut}(G_1 \times G_2) \cong \mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2).$$

Κατ' αναλογίαν, μέχρις ισομορφισμού, η ομάδα των κεντρικών αυτομορφισμών τής $G_1 \times G_2$ (βλ. 5.4.33) *είναι η*

$$\boxed{\mathrm{Aut_c}(G_1 \times G_2) \cong \mathcal{A}_{\mathrm{c}}\,,}$$

όπου

$$\mathcal{A}_{\mathrm{c}} := \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \middle| \begin{array}{ccc} \alpha \in \mathrm{Aut_c}(G_1), & & \beta \in \mathrm{Hom}(G_2, Z(G_1)) \\ \gamma \in \mathrm{Hom}(G_1, Z(G_2)), & & \delta \in \mathrm{Aut_c}(G_2) \end{array} \right\} \sqsubseteq \mathcal{A}$$

και $|\mathrm{Aut_c}(G_1 \times G_2)| = |\mathrm{Aut_c}(G_1)|\,|\mathrm{Aut_c}(G_2)|\,|\mathrm{Hom}(G_1, Z(G_2))|\,|\mathrm{Hom}(G_2, Z(G_1))|\,.$

[7] Για την απόδειξή του βλ. J.N.S. Bidwell, M.J. Curran & D.J. McCauchan: *Automorphisms of direct products of finite groups*, Archiv der Math. (Basel) **86** (2006), 481-489.

[8] Λέμε ότι **οι G_1 και G_2 δεν έχουν κοινούς ευθείς παράγοντες** όταν είναι μη ισόμορφες και όταν ικανοποιούνται οι εξής συνθήκες: (i) Δεν υπάρχουν μη τετριμμένες ομάδες G_{11}, G_{12}, τέτοιες ώστε $G_1 \cong G_{11} \times G_{12}$ και $G_2 \cong G_{1i}$ για κάποιον $i \in \{1, 2\}$. (ii) Δεν υπάρχουν μη τετριμμένες ομάδες G_{21}, G_{22}, τέτοιες ώστε $G_2 \cong G_{21} \times G_{22}$ και $G_1 \cong G_{2i}$ για κάποιον $i \in \{1, 2\}$. (iii) Δεν υπάρχουν μη τετριμμένες ομάδες G_{11}, G_{12} και μη τετριμμένες ομάδες G_{21}, G_{22}, τέτοιες ώστε $G_1 \cong G_{11} \times G_{12}$, $G_2 \cong G_{21} \times G_{22}$ και $G_{1i} \cong G_{2j}$ για κάποιους $i, j \in \{1, 2\}$.

[9] Έστω ότι οι G και H είναι δυο ομάδες. Εάν οι f_1, f_2 ανήκουν στο σύνολο $\mathrm{Hom}(G, H)$ των ομομορφισμών από την G στην H και $\mathrm{Im}(f_1)\,\mathrm{Im}(f_2) = \mathrm{Im}(f_2)\,\mathrm{Im}(f_1)$, τότε η απεικόνιση $f_1 + f_2 : G \longrightarrow H$ η οριζόμενη μέσω τού τύπου $(f_1 + f_2)(g) := f_1(g) f_2(g)$, $\forall g \in G$, είναι ένας ομομορφισμός και θεωρείται ως το **άθροισμα** των f_1 και f_2 στον λογισμό με τους πίνακες που υπεισέρχονται στο προκείμενο θεώρημα. (Όταν η H είναι *αβελιανή*, το ανωτέρω *άθροισμα* συμπίπτει με το ήδη ορισθέν στο εδάφιο 2.4.13 (ii).)

► **«Εσωτερικό» ευθύ γινόμενο δύο υποομάδων μιας ομάδας.** Η πρόταση 7.1.4 δρα ως κίνητρο για τη θέσπιση τού ακόλουθου ορισμού:

7.1.21 Ορισμός. Έστω ότι η $(G,\cdot)$ είναι μια ομάδα και ότι $H \sqsubseteq G$ και $K \sqsubseteq G$. Λέμε ότι η G είναι το **εσωτερικό**[10] **ευθύ γινόμενο των υποομάδων** H **και** K (και γράφουμε[11] $G = H \times_{\text{εσ.}} K$) όταν πληρούνται οι εξής συνθήκες:
(i) $H \trianglelefteq G$ και $K \trianglelefteq G$,
(ii) $G = \langle H, K\rangle$ ($\underset{4.2.24}{=} HK = KH$), και
(iii) $H \cap K = \{e_G\}$.

7.1.22 Παράδειγμα. Η ομάδα $\mathbf{V} := \{\mathrm{id}, [1\,2]\circ[3\,4]\,, [1\,3]\circ[2\,4]\,, [1\,4]\circ[2\,3]\}$ των τεσσάρων στοιχείων τού Klein (ως προς την πράξη τής συνθέσεως μετατάξεων) είναι το εσωτερικό γινόμενο

$$\mathbf{V} = \langle [1\,2]\circ[3\,4]\rangle \times_{\text{εσ.}} \langle [1\,3]\circ[2\,4]\rangle\,,$$

διότι $[1\,4]\circ[2\,3] = ([1\,2]\circ[3\,4])\circ([1\,3]\circ[2\,4])$ (βλ. 3.4.2 (ii) και 4.2.6).

7.1.23 Πρόταση. *Έστω $f : (G,\cdot) \longrightarrow (L,*)$ ένας ομομορφισμός ομάδων και έστω $H \trianglelefteq G$. Εάν ο περιορισμός $f|_H : H \longrightarrow L$ είναι ένας ισομορφισμός μεταξύ των H και L, τότε $G = H \times_{\text{εσ.}} K$, όπου $K := \mathrm{Ker}(f)$.*

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το πόρισμα 4.2.31 και την πρόταση 4.2.24 έχουμε $K \trianglelefteq G$ και $\langle H, K\rangle = HK \trianglelefteq G$. Εάν $g \in G$, τότε $f(g) \in L$, οπότε $\exists x \in H : f(x) = f(g)$. Αυτό σημαίνει ότι $f(x^{-1} * g) = e_L$, απ' όπου έπεται ότι

$$g = x(x^{-1}g), \;\; \text{όπου } x \in H \text{ και } x^{-1}g \in K \Rightarrow G = HK.$$

Έστω τώρα τυχόν στοιχείο $g \in H \cap K$. Επειδή η $f|_H : H \longrightarrow L$ είναι ένας ισομορφισμός μεταξύ των H και L, έχουμε

$$f|_H(g) = f(g) = e_L = f(e_G) \Rightarrow g = e_G.$$

Κατά συνέπειαν, $G = H \times_{\text{εσ.}} K$. □

7.1.24 Παραδείγματα. Εφαρμόζοντας την πρόταση 7.1.23 για τους ομομορφισμούς

$$f : (\mathbb{C},+) \longrightarrow (\mathbb{R},+), \;\; x+iy \longmapsto x,$$
$$f : (\mathbb{Q}\setminus\{0\},\cdot) \longrightarrow (\{\pm 1\},\cdot), \;\; x \longmapsto \tfrac{x}{|x|},$$
$$f : (\mathbb{R}\setminus\{0\},\cdot) \longrightarrow (\{\pm 1\},\cdot), \;\; x \longmapsto \tfrac{x}{|x|},$$
$$f : (\mathbb{C}\setminus\{0\},\cdot) \longrightarrow (\mathbb{R}_{>0},\cdot), \;\; x+iy \longmapsto \sqrt{x^2+y^2},$$

[10] Για τον καθορισμό τού *εσωτερικού* ευθέος γινομένου εκκινούμε από μια δεδομένη ομάδα $(G,\cdot)$ και προσδιορίζουμε δύο *υποομάδες της* H και K, τέτοιες ώστε η G να είναι *ισόμορφη* με το *εξωτερικό* ευθύ γινόμενο αυτών (ιδωμένων ως ανεξαρτήτων ομάδων). Το ότι οι συνθήκες που αρκούν προς τούτο είναι *ακριβώς* οι (i)-(iii) θα αναφανεί στο θεώρημα 7.1.43. (Αντιθέτως, για τον σχηματισμό τού *εξωτερικού* ευθέος γινομένου εκκινούμε από *οιεσδήποτε* ομάδες G_1 και G_2, χωρίς να προϋποθέτουμε εκ των προτέρων κάποιον αλληλοσυσχετισμό τους, και δομούμε τη «μεγαλύτερη» ομάδα $G_1 \times G_2$ βάσει των προαναφερθέντων στο εδάφιο 7.1.1.)

[11] Στην περίπτωση κατά την οποία χρησιμοποιούμε τον *προσθετικό συμβολισμό* για την πράξη τής G, γράφουμε $G = H \oplus_{\text{εσ.}} K$ αντί τού $G = H \times_{\text{εσ.}} K$ και το ονομάζουμε **εσωτερικό ευθύ άθροισμα των** H **και** K.

λαμβάνουμε

$$\boxed{\begin{array}{ll} \mathbb{C} = \mathbb{R} \oplus_{\text{εσ.}} \mathbb{R}, & \mathbb{Q} \smallsetminus \{0\} = \{\pm 1\} \times_{\text{εσ.}} \mathbb{Q}_{>0}, \\ \mathbb{R} \smallsetminus \{0\} = \{\pm 1\} \times_{\text{εσ.}} \mathbb{R}_{>0}, & \mathbb{C} \smallsetminus \{0\} = \mathbb{R}_{>0} \times_{\text{εσ.}} \mathbb{S}^1. \end{array}}$$

7.1.25 Θεώρημα. *Έστω ότι οι H και K είναι υποομάδες μιας ομάδας $(G, \cdot)$. Τότε τα* (a) *και* (b) *είναι ισοδύναμα*:

(a) $H \trianglelefteq G$, $K \trianglelefteq G$ *και* $G = H \times_{\text{εσ.}} K$.

(b) *Για τις H και K ισχύουν τα ακόλουθα*:

(i) $xy = yx$, $\forall x \in H$ *και* $\forall y \in K$,

(ii) *Κάθε στοιχείο $g \in G$ γράφεται μονοσημάντως υπό τη μορφή $g = xy$, όπου $x \in H$ και $y \in K$.*

ΑΠΟΔΕΙΞΗ. (a)⇒(b) Εάν $H \trianglelefteq G$, $K \trianglelefteq G$ και $G = H \times_{\text{εσ.}} K$, τότε για οιαδήποτε στοιχεία $x \in H$ και $y \in K$ έχουμε

$$\left.\begin{array}{r} K \ni \underbrace{(xyx^{-1})}_{\in K} y^{-1} = x \underbrace{(yx^{-1}y^{-1})}_{\in H} \in H \\ \text{7.1.21 (iii)} \Rightarrow H \cap K = \{e_G\} \end{array}\right\} \Rightarrow xyx^{-1}y^{-1} = e_G,$$

απ' όπου έπεται το (i), ήτοι ότι $xy = yx$. Έστω τώρα τυχόν στοιχείο $g \in G$. Επειδή εξ ορισμού $G = HK$ (βλ. 7.1.21 (ii)), το g γράφεται υπό τη μορφή $g = xy$ για κάποια $x \in H$ και $y \in K$. Για την απόδειξη τού (ii) αρκεί να ελεγχθεί ότι η εν λόγω έκφραση τού g είναι μοναδική. Προς τούτο υποθέτουμε ότι $g = zw$, όπου $z \in H$ και $w \in K$. Προφανώς,

$$\left.\begin{array}{r} xy = zw \Rightarrow H \ni z^{-1}x = wy^{-1} \in K \\ \text{7.1.21 (iii)} \Rightarrow H \cap K = \{e_G\} \end{array}\right\} \Rightarrow x = z \text{ και } y = w.$$

(b)⇒(a) Έστω ότι ισχύουν τα (i) και (ii) και έστω τυχόν στοιχείο $g \in G$. Κατά το (ii) το g γράφεται υπό τη μορφή $g = xy$, όπου $x \in H$ και $y \in K$. Επομένως, για οιαδήποτε $a \in H$ και $b \in K$ έχουμε

$$gag^{-1} = (xy)\, a\, (xy)^{-1} = x\left(yay^{-1}\right) x^{-1} \underset{\text{(i)}}{=} x\left(yy^{-1}a\right) x^{-1} = xax^{-1} \in H \Rightarrow H \trianglelefteq G$$

και

$$gbg^{-1} = (xy)\, b\, (xy)^{-1} = (x \underbrace{yby^{-1}}_{\in K}) x^{-1} \underset{\text{(i)}}{=} (yby^{-1}) xx^{-1} = yby^{-1} \in K \Rightarrow K \trianglelefteq G.$$

(Σημειωτέον ότι για την ανωτέρω απόδειξη τού ότι $H \trianglelefteq G$ και $K \trianglelefteq G$ *δεν* χρησιμοποιήθηκε η *μονοσήμαντη* γραφή τού g ως γινομένου στοιχείων των H και K.) Επιπροσθέτως, από το (ii) έπεται άμεσα ότι $G = HK$. Τέλος, εάν $g \in H \cap K$, τότε

$$\left.\begin{array}{l} g = ge_G,\ g \in H, e_G \in K \\ g = e_G g,\ e_G \in H, g \in K \end{array}\right\} \underset{\text{(ii)}}{\Longrightarrow} g = e_G \Rightarrow H \cap K = \{e_G\}.$$

(Εν προκειμένω, χρησιμοποιήθηκε *ουσιαστικώς* η *μονοσήμαντη* γραφή τού g ως γινομένου στοιχείων των H και K.) Άρα $G = H \times_{\text{εσ.}} K$. □

7.1.26 Θεώρημα. *Έστω ότι οι H και K είναι υποομάδες μιας ομάδας $(G, \cdot)$. Τότε τα* (a) *και* (b) *είναι ισοδύναμα*:

(a) $H \trianglelefteq G$, $K \trianglelefteq G$ *και* $G = H \times_{\text{εσ.}} K$.

(b) *Για τις H και K ισχύουν τα ακόλουθα*:

(i) $G = HK$,

(ii) $H \cap K = \{e_G\}$, *και*

(iii) $xy = yx$, $\forall x \in H$ *και* $\forall y \in K$.

ΑΠΟΔΕΙΞΗ. (a)⇒(b) Τα (i) και (ii) ισχύουν λόγω τού ορισμού 7.1.21. Το (iii) έπεται από τη συνεπαγωγή (a)⇒(b) (i) στο θεώρημα 7.1.25.

(b)⇒(a) Από το (iii) έπεται ότι $H \trianglelefteq G$ και $K \trianglelefteq G$ (αρκεί κανείς να επαναλάβει την απόδειξη που παρετέθη προς τούτο κατά την επαλήθευση τής ισχύος τής συνεπαγωγής (b)⇒(a) στο θεώρημα 7.1.25). Λόγω των (i) και (ii) ικανοποιούνται *και* οι συνθήκες (ii) και (iii) τού ορισμού 7.1.21. Συνεπώς, $G = H \times_{\text{εσ.}} K$. □

7.1.27 Παρατήρηση. Εάν $G = H \times_{\text{εσ.}} K$, τότε $G = K \times_{\text{εσ.}} H$.

7.1.28 Παραδείγματα. (i) Η (αβελιανή, μη κυκλική, πολλαπλασιαστική) ομάδα $\left(\mathbb{Z}_8^{\times}, \cdot\right)$, όπου $\mathbb{Z}_8^{\times} = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ (βλ. 2.1.7 (iii) και 2.4.20 (ii)), είναι το εσωτερικό γινόμενο των κυκλικών υποομάδων της

$$H := \langle [3]_8 \rangle = \{[1]_8, [3]_8\} \quad \text{και} \quad K := \langle [5]_8 \rangle = \{[1]_8, [5]_8\},$$

διότι $[7]_8 = [3]_8 \cdot [5]_8$ και $\langle [3]_8 \rangle \cap \langle [5]_8 \rangle = \{[1]_8\}$.

(ii) Η διεδρική ομάδα $\mathbf{D}_6 = \langle \alpha, \beta \rangle$ (τάξεως 12) είναι το εσωτερικό γινόμενο των υποομάδων της

$$H := \left\{\mathrm{id}_{\mathcal{E}_6}, \beta^2, \beta^4, \alpha, \alpha \circ \beta^2, \alpha \circ \beta^4\right\} \quad \text{και} \quad K := \left\langle \beta^3 \right\rangle = \left\{\mathrm{id}_{\mathcal{E}_6}, \beta^3\right\}.$$

(iii) Εάν $K := \{\sigma \in \mathfrak{S}_4 \,|\, \sigma(4) = 4\}$, τότε η συμμετρική ομάδα $\mathfrak{S}_4$ *δεν είναι* το εσωτερικό γινόμενο των υποομάδων $\mathbf{V} \lhd \mathfrak{S}_4$ και K, *καίτοι* ισχύει

$$\mathfrak{S}_4 = \mathbf{V} \circ K = \langle \mathbf{V}, K \rangle = K \circ \mathbf{V} \quad \text{και} \quad \mathbf{V} \cap K = \{\mathrm{id}\}$$

(βλ. 4.2.24 και 4.5.16). Πράγματι· συγκρίνοντας τον κατάλογο

$\circ$	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] ∘ [3 4]	[1 2] ∘ [3 4]	[3 4]	[1 4 3 2]	[1 2 4 3]	[2 4 3]	[1 4 3]
[1 3] ∘ [2 4]	[1 3] ∘ [2 4]	[1 4 2 3]	[2 4]	[1 3 4 2]	[1 4 2]	[2 3 4]
[1 4] ∘ [2 3]	[1 4] ∘ [2 3]	[1 3 2 4]	[1 2 3 4]	[1 4]	[1 3 4]	[1 2 4]

των συνθέσεων $\sigma \circ \tau$, όπου $\sigma \in \mathbf{V}$, $\tau \in K$, με τον κατάλογο

$\circ$	id	$[1\,2] \circ [3\,4]$	$[1\,3] \circ [2\,4]$	$[1\,4] \circ [2\,3]$
id	id	$[1\,2] \circ [3\,4]$	$[1\,3] \circ [2\,4]$	$[1\,4] \circ [2\,3]$
$[1\,2]$	$[1\,2]$	$[3\,4]$	$[1\,3\,2\,4]$	$[1\,4\,2\,3]$
$[1\,3]$	$[1\,3]$	$[1\,2\,3\,4]$	$[2\,4]$	$[1\,4\,3\,2]$
$[2\,3]$	$[2\,3]$	$[1\,3\,4\,2]$	$[1\,2\,4\,3]$	$[1\,4]$
$[1\,2\,3]$	$[1\,2\,3]$	$[1\,3\,4]$	$[2\,4\,3]$	$[1\,4\,2]$
$[1\,3\,2]$	$[1\,3\,2]$	$[2\,3\,4]$	$[1\,2\,4]$	$[1\,4\,3]$

των συνθέσεων $\sigma \circ \tau$, όπου $\sigma \in K$, $\tau \in \mathbf{V}$, παρατηρούμε ότι η συνθήκη (b) (iii) τού θεωρήματος 7.1.26 *δεν* ικανοποιείται, αφού, π.χ.,

$$([1\,2] \circ [3\,4]) \circ [1\,3] = [1\,4\,3\,2] \neq [1\,2\,3\,4] = [1\,3] \circ ([1\,2] \circ [3\,4])\,.$$

(Εξ αυτού εξάγεται, ιδιαιτέρως, το συμπέρασμα ότι $K \not\trianglelefteq \mathfrak{S}_4$.)

7.1.29 Πρόταση. *Εάν H και K είναι ορθόθετες υποομάδες μιας ομάδας $(G, \cdot)$, τέτοιες ώστε να ισχύει $G = H \times_{\text{εσ.}} K$, τότε*

$$\boxed{G/H \cong K} \quad \text{και} \quad \boxed{G/K \cong H.}$$

ΑΠΟΔΕΙΞΗ. Επειδή ισχύει $G = HK$ και $H \cap K = \{e_G\}$, το 2ο θεώρημα ισομορφισμών 4.5.13 δίδει $G/H = HK/\,H \cong K/\,H \cap K = K/\{e_G\} \underset{4.4.5}{\cong} K$. (Ο δεύτερος ισομορφισμός έπεται ύστερα από εναλλαγή των ρόλων των H και K.) □

7.1.30 Πόρισμα. *Εάν οι H, K και L είναι ορθόθετες υποομάδες μιας ομάδας $(G, \cdot)$, τέτοιες ώστε να ισχύει $G = H \times_{\text{εσ.}} K = H \times_{\text{εσ.}} L$, τότε*[12] *$K \cong L$.*

ΑΠΟΔΕΙΞΗ. Επειδή (κατά την πρόταση 7.1.29) $G/H \cong K$ και $G/H \cong L$, έχουμε $K \cong L$. □

7.1.31 Παρατήρηση. (i) Κατά το πόρισμα 7.1.30,

$$G = H \times_{\text{εσ.}} K = H \times_{\text{εσ.}} L \Rightarrow K \cong L.$$

Ωστόσο, δεν αποκλείεται το ενδεχόμενο να έχουμε $K \neq L$. Επί παραδείγματι, για την ομάδα $\mathbf{V}$ των τεσσάρων στοιχείων τού Klein ισχύουν οι ισότητες

$$\mathbf{V} = \langle [1\,2] \circ [3\,4] \rangle \times_{\text{εσ.}} \langle [1\,3] \circ [2\,4] \rangle = \langle [1\,2] \circ [3\,4] \rangle \times_{\text{εσ.}} \langle [1\,4] \circ [2\,3] \rangle\,,$$

με $\langle [1\,3] \circ [2\,4] \rangle \neq \langle [1\,4] \circ [2\,3] \rangle$ και $\langle [1\,3] \circ [2\,4] \rangle \cong \langle [1\,4] \circ [2\,3] \rangle \cong \mathbb{Z}_2$.

(ii) Εάν οι H_1, K_1 είναι ορθόθετες υποομάδες μιας ομάδας G_1 και οι H_2, K_2 ορθόθετες υποομάδες μιας ομάδας G_2, τέτοιες ώστε να ισχύει $G_1 = H_1 \times_{\text{εσ.}} K_1$, $G_2 = H_2 \times_{\text{εσ.}} K_2$ και $G_1 \cong G_2$, τότε δεν αποκλείεται το ενδεχόμενο να έχουμε (ταυτοχρόνως)

$$H_1 \ncong H_2,\ H_1 \ncong K_2,\ K_1 \ncong H_2 \ \text{ και } \ K_1 \ncong K_2.$$

[12] Στο ίδιο συμπέρασμα καταλήγουμε ακόμη και αν υποθέσουμε ότι $G = K \times_{\text{εσ.}} H = L \times_{\text{εσ.}} H$.

Επί παραδείγματι, θέτοντας $G_1 := \mathbb{Z}_7^\times \times \mathbb{Z}_{15}^\times$, $G_2 := \mathbb{Z}_{21}^\times \times \mathbb{Z}_5^\times$,

$$\overline{\mathbb{Z}}_i^\times := \mathbb{Z}_i^\times \times \{[1]_{\frac{105}{i}}\},\ \overline{\mathbb{Z}}_j^\times := \{[1]_{\frac{105}{j}}\} \times \mathbb{Z}_j^\times \ \text{ για } \ (i,j) \in \{(7,15),(21,5)\},$$

και $H_1 := \overline{\mathbb{Z}}_7^\times$, $K_1 := \overline{\mathbb{Z}}_{15}^\times$, $H_2 := \overline{\mathbb{Z}}_{21}^\times$ και $K_2 := \overline{\mathbb{Z}}_5^\times$, λαμβάνουμε

$$\left.\begin{array}{l} \mathbb{Z}_{105}^\times \cong \mathbb{Z}_7^\times \times \mathbb{Z}_{15}^\times = G_1 = H_1 \times_{\text{εσ.}} K_1 \\ \mathbb{Z}_{105}^\times \cong \mathbb{Z}_{21}^\times \times \mathbb{Z}_5^\times = G_2 = H_2 \times_{\text{εσ.}} K_2 \end{array}\right\} \Rightarrow G_1 \cong G_2$$

(βλ. 7.3.2 και 7.1.43 (i)), όπου $\mathbb{Z}_7^\times \simeq \overline{\mathbb{Z}}_7^\times$, $\mathbb{Z}_{15}^\times \cong \overline{\mathbb{Z}}_{15}^\times$, $\mathbb{Z}_{21}^\times \cong \overline{\mathbb{Z}}_{21}^\times$, $\mathbb{Z}_5^\times \cong \overline{\mathbb{Z}}_5^\times$. Εντούτοις, $\mathbb{Z}_7^\times \ncong \mathbb{Z}_{21}^\times$, $\mathbb{Z}_7^\times \ncong \mathbb{Z}_5^\times$, $\mathbb{Z}_{15}^\times \ncong \mathbb{Z}_{21}^\times$ και $\mathbb{Z}_{15}^\times \ncong \mathbb{Z}_5^\times$.

Μια γενίκευση τού πορίσματος 7.1.30 θα διατυπωθεί και θα αποδειχθεί στην επόμενη ενότητα. (Βλ. θεώρημα 7.2.25.) Σε αυτήν υπεισέρχεται, μεταξύ άλλων, και η έννοια τής «αποσυνθεσιμότητας» μιας ομάδας.

7.1.32 Ορισμός. Λέμε ότι μια ομάδα $(G,\cdot)$ είναι **αποσυνθέσιμη** όταν είναι μη τετριμμένη και υπάρχουν *μη τετριμμένες γνήσιες* ορθόθετες υποομάδες της H και K, τέτοιες ώστε $G = H \times_{\text{εσ.}} K$. Εάν αυτό δεν συμβαίνει, τότε η $(G,\cdot)$ καλείται **αναποσυνθέσιμη**.

7.1.33 Παραδείγματα. (i) Κάθε απλή ομάδα είναι προδήλως αναποσυνθέσιμη.

(ii) Η $(\mathfrak{A}_4,\circ)$ είναι (μη απλή) αναποσυνθέσιμη ομάδα, καθότι διαθέτει *μία και μόνον* μη τετριμμένη γνήσια ορθόθετη υποομάδα (συγκεκριμένα, την $\mathbf{V}$ τάξεως 4).

(iii) Η άπειρη κυκλική (προσθετική) ομάδα $(\mathbb{Z},+)$ είναι αναποσυνθέσιμη: Κάθε μη τετριμμένη γνήσια υποομάδα της είναι ορθόθετη (βλ. πρόταση 4.2.6) και έχει τη μορφή $(m\mathbb{Z},+)$, για κάποιον $m \in \mathbb{N}, m \geq 2$ (βλ. 2.2.19 (i)). Ωστόσο, για οιουσδήποτε φυσικούς αριθμούς $m,n \geq 2$ έχουμε $m\mathbb{Z} \cap n\mathbb{Z} = \text{εκπ}(m,n)\mathbb{Z}$ (επί τη βάσει τού (iii) τής προτάσεως 2.2.20), οπότε $\text{εκπ}(m,n) \geq 2$ και $\{0\} \subsetneqq m\mathbb{Z} \cap n\mathbb{Z}$.

(iv) Η ομάδα $\mathbf{Q}$ των τετρανίων είναι αναποσυνθέσιμη: Ως γνωστόν, όλες οι υποομάδες της είναι ορθόθετες (βλ. 4.2.18) και οι μόνες μη τετριμμένες γνήσιες υποομάδες της είναι οι $\langle -\mathbf{I}_2\rangle, \langle \mathbf{i}\rangle, \langle \mathbf{j}\rangle, \langle \mathbf{k}\rangle$ (βλ. 4.1.43). Ωστόσο, η τομή οιουδήποτε ζεύγους εξ αυτών είναι μη τετριμμένη, αφού

$$\{\mathbf{I}_2\} \subsetneqq \langle -\mathbf{I}_2\rangle = \langle \mathbf{i}\rangle \cap \langle -\mathbf{I}_2\rangle = \langle \mathbf{j}\rangle \cap \langle -\mathbf{I}_2\rangle = \langle \mathbf{k}\rangle \cap \langle -\mathbf{I}_2\rangle,$$
$$\{\mathbf{I}_2\} \subsetneqq \langle -\mathbf{I}_2\rangle = \langle \mathbf{i}\rangle \cap \langle \mathbf{j}\rangle = \langle \mathbf{i}\rangle \cap \langle \mathbf{k}\rangle = \langle \mathbf{j}\rangle \cap \langle \mathbf{k}\rangle.$$

(v) Σύμφωνα με τα προαναφερθέντα στα εδάφια 7.1.22, 7.1.24 και 7.1.28 (i) οι ομάδες $(\mathbf{V},\circ)$, $(\mathbb{C},+)$, $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\},\cdot)$, $(\mathbb{C}\setminus\{0\},\cdot)$ και $\left(\mathbb{Z}_8^\times,\cdot\right)$ είναι αποσυνθέσιμες.

7.1.34 Πρόταση. *Έστω $(G,\cdot)$ μια μη τετριμμένη πεπερασμένη κυκλική ομάδα. Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Η G είναι αναποσυνθέσιμη.*

(ii) $(G,\cdot) \cong (\mathbb{Z}_{p^\nu},+)$, *όπου p κάποιος πρώτος αριθμός και $\nu \in \mathbb{N}$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Επειδή η G είναι μη τετριμμένη, υπάρχει κάποιος πρώτος αριθμός p ο οποίος διαιρεί την τάξη της. Έστω $\nu := \max\{\kappa \in \mathbb{N} : p^\kappa \mid |G|\}$. Τότε $|G| = p^\nu m$, για κάποιον $m \in \mathbb{N}$ με μκδ$(p, m) = 1$. Υποθέτοντας ότι η $G = \langle g\rangle$ (όπου $g \in G\setminus\{e_G\}$) είναι αναποσυνθέσιμη, αρκεί (λόγω τού (ii) τού θεωρήματος 2.4.23) να δείξουμε ότι $m = 1$. Θα εργασθούμε με «εις άτοπον απαγωγή». Προς τούτο υποθέτουμε ότι $m \geq 2$. Έστω $H := \langle g^m\rangle$ και έστω $K := \left\langle g^{p^\nu}\right\rangle$. Τότε $H \lhd G$, $K \lhd G$ και $|H| = p^\nu$, $|K| = m$. (Βλ. την πρόταση 2.3.10, το πόρισμα 2.3.23 και την πρόταση 4.2.6.) Κατά το (ii) τού πορίσματος 4.1.25, $H \cap K = \{e_G\}$. Εξάλλου, από τον τύπο (4.35) τού γινομένου προκύπτει ότι

$$\text{card}(HK) = \frac{|H|\ |K|}{|H \cap K|} = |H|\ |K| = p^\nu m = |G| \Rightarrow G = HK.$$

Επομένως, οι ομάδες H και K ικανοποιούν τις συνθήκες (i), (ii) και (iii) τού ορισμού 7.1.21. Ως εκ τούτου, $G = H \times_{\text{εσ.}} K$. Άτοπο! Άρα τελικώς $m = 1$.

(ii)⇒(i) Εξ υποθέσεως, $G = \langle g\rangle$, $g \in G\setminus\{e_G\}$ και $|G| = p^\nu$, όπου p κάποιος πρώτος αριθμός και $\nu \in \mathbb{N}$. Θεωρούμε *τυχούσες* μη τετριμμένες γνήσιες υποομάδες της H και K. Τότε (σύμφωνα με το πόρισμα 2.3.23)

$$\exists m, n \in \mathbb{N},\ 2 \leq m, n < p^\nu : m \mid p^\nu \text{ και } n \mid p^\nu \text{ με } H = \langle g^m\rangle \text{ και } K = \langle g^n\rangle.$$

Κατά το λήμμα Β.3.14,

$$\exists \kappa, \lambda \in \{1,..., \nu - 1\} \in \mathbb{N} : m = p^\kappa \ \text{ και } \ n = p^\lambda$$

(οπότε $|H| = p^{\nu-\kappa}$ και $|K| = p^{\nu-\lambda}$). Επειδή $m \mid n$ ($\Rightarrow p^{\nu-\lambda} \mid p^{\nu-\kappa}$) όταν $\kappa \leq \lambda$ και $n \mid m$ όταν $\lambda \leq \kappa$, έχουμε (εκ νέου κατόπιν εφαρμογής τού πορίσματος 2.3.23, αλλ' αυτήν τη φορά για τις ίδιες τις K και H)

$$K \sqsubseteq H \text{ όταν } \kappa \leq \lambda \text{ και } H \sqsubseteq K \text{ όταν } \lambda \leq \kappa,$$

οπότε $H \cap K \in \{K, H\} \Rightarrow \{e_G\} \subsetneqq H \cap K$. Αυτό σημαίνει ότι η G είναι αναποσυνθέσιμη. □

7.1.35 Ορισμός. Ένας ενδομορφισμός ϑ μιας ομάδας $(G, \cdot)$ καλείται **ορθόθετος ενδομορφισμός** όταν

$$\boxed{g_1\vartheta(g_2)g_1^{-1} = \vartheta(g_1g_2g_1^{-1}),\ \forall (g_1, g_2) \in G \times G.}$$

ή, ισοδυνάμως, όταν

$$\boxed{\boldsymbol{\gamma}_g \circ \vartheta = \vartheta \circ \boldsymbol{\gamma}_g,\ \forall g \in G.}$$

7.1.36 Πρόταση. *Εάν ϑ είναι ένας ορθόθετος αυτομορφισμός μιας ομάδας $(G, \cdot)$, τότε και ο αντίστροφός του ϑ^{-1} είναι ορθόθετος.*

ΑΠΟΔΕΙΞΗ. Για κάθε $g \in G$ έχουμε

$$\begin{aligned} \vartheta^{-1} \circ \boldsymbol{\gamma}_g &= \vartheta^{-1} \circ (\boldsymbol{\gamma}_{g^{-1}})^{-1} = (\boldsymbol{\gamma}_{g^{-1}} \circ \vartheta)^{-1} \\ &= (\vartheta \circ \boldsymbol{\gamma}_{g^{-1}})^{-1} = (\boldsymbol{\gamma}_{g^{-1}})^{-1} \circ \vartheta^{-1} = \boldsymbol{\gamma}_g \circ \vartheta^{-1}, \end{aligned}$$

οπότε και ο ϑ^{-1} είναι ορθόθετος. □

7.1.37 Πρόταση. *Εάν ϑ_1, ϑ_2 είναι ορθόθετοι ενδομορφισμοί μιας ομάδας $(G, \cdot)$, τότε και οι συνθέσεις $\vartheta_1 \circ \vartheta_2$ και $\vartheta_2 \circ \vartheta_1$ είναι ορθόθετοι ενδομορφισμοί αυτής.*

ΑΠΟΔΕΙΞΗ. Για κάθε $g \in G$ έχουμε

$$\begin{aligned} \boldsymbol{\gamma}_g \circ (\vartheta_1 \circ \vartheta_2) &= (\boldsymbol{\gamma}_g \circ \vartheta_1) \circ \vartheta_2 = (\vartheta_1 \circ \boldsymbol{\gamma}_g) \circ \vartheta_2 = \vartheta_1 \circ (\boldsymbol{\gamma}_g \circ \vartheta_2) \\ &= \vartheta_1 \circ (\vartheta_2 \circ \boldsymbol{\gamma}_g) = (\vartheta_1 \circ \vartheta_2) \circ \boldsymbol{\gamma}_g \end{aligned}$$

και κατ' αναλογίαν $\boldsymbol{\gamma}_g \circ (\vartheta_2 \circ \vartheta_1) = (\vartheta_2 \circ \vartheta_1) \circ \boldsymbol{\gamma}_g$. □

7.1.38 Πρόταση. *Εάν ϑ είναι ένας ορθόθετος ενδομορφισμός μιας ομάδας $(G, \cdot)$, τότε ισχύουν τα εξής*:

(i) $g^{-1}\vartheta(g) \in \mathrm{C}_G(\mathrm{Im}(\vartheta)), \forall g \in G$.

(ii) *Εάν* $\vartheta \in \mathrm{Aut}(G)$, *τότε* $g^{-1}\vartheta(g) \in Z(G), \forall g \in G$.

ΑΠΟΔΕΙΞΗ. (i) Εάν $y \in \mathrm{Im}(\vartheta)$, τότε $\exists x \in G : y = \vartheta(x)$, οπότε για κάθε $g \in G$ έχουμε

$$\begin{aligned} &gyg^{-1} = g\vartheta(x)g^{-1} = \vartheta(gxg^{-1}) \Rightarrow \vartheta(x)g^{-1} = g^{-1}\vartheta(g)\vartheta(x)\vartheta(g)^{-1} \\ &\Rightarrow \vartheta(x)\left(g^{-1}\vartheta(g)\right) = \left(g^{-1}\vartheta(g)\right)\vartheta(x) \Rightarrow y\left(g^{-1}\vartheta(g)\right) = \left(g^{-1}\vartheta(g)\right)y \\ &\Rightarrow g^{-1}\vartheta(g) \in \mathrm{C}_G(\mathrm{Im}(\vartheta)). \end{aligned}$$

(ii) Προφανές, διότι εν τοιαύτη περιπτώσει $\mathrm{Im}(\vartheta) = G$ και $Z(G) := \mathrm{C}_G(G)$. □

7.1.39 Πρόταση. *Εάν H και K είναι ορθόθετες υποομάδες μιας ομάδας $(G, \cdot)$, τέτοιες ώστε $G = H \times_{\mathrm{εσ.}} K$, τότε ισχύουν τα ακόλουθα*:

(i) *Εάν $L \trianglelefteq H$ (και αντιστοίχως, εάν $L \trianglelefteq K$), τότε $L \trianglelefteq G$.*

(ii) *Εάν ϑ είναι ένας ορθόθετος ενδομορφισμός τής G με $\vartheta(H) \subseteq H$ (και αντιστοίχως, με $\vartheta(K) \subseteq K$), τότε ο περιορισμός $\vartheta|_H$ τού ϑ επί τής H (και αντιστοίχως, ο περιορισμός $\vartheta|_K$ τού ϑ επί τής K) είναι ένας ορθόθετος ενδομορφισμός τής H (και αντιστοίχως, τής K).*

ΑΠΟΔΕΙΞΗ. (i) Έστω τυχόν $g \in G$. Το g (λόγω τού (b) (ii) τού θεωρήματος 7.1.25) γράφεται μονοσημάντως υπό τη μορφή $g = xy$, όπου $x \in H$ και $y \in K$. Για κάθε $z \in L$ έχουμε $z \in H$ και $zy = yz$, οπότε

$$\begin{aligned} \boldsymbol{\gamma}_g(z) &= gzg^{-1} = xyz(xy)^{-1} = x\,(yz)\,y^{-1}x^{-1} \\ &= xzyy^{-1}x^{-1} = xze_Gx^{-1} = xzx^{-1} \in L \end{aligned}$$

(διότι $L \trianglelefteq H$). Αυτό σημαίνει ότι $\boldsymbol{\gamma}_g(L) \subseteq L$. Από την πρόταση 5.4.24 έπεται ότι $L \trianglelefteq G$. (Η συνεπαγωγή $L \trianglelefteq K \Rightarrow L \trianglelefteq G$ αποδεικνύεται παρομοίως.)

(ii) Εάν ϑ είναι ένας ορθόθετος ενδομορφισμός τής G με $\vartheta(H) \subseteq H$ (και αντιστοίχως, με $\vartheta(K) \subseteq K$), τότε $\boldsymbol{\gamma}_h \circ \vartheta|_H = \vartheta|_H \circ \boldsymbol{\gamma}_h$ για κάθε $h \in H$ (και αντιστοίχως, $\boldsymbol{\gamma}_k \circ \vartheta|_K = \vartheta|_K \circ \boldsymbol{\gamma}_k$ για κάθε $k \in K$). □

7.1.40 Θεώρημα. (Κριτήριο «αποσυνθεσιμότητας».) *Έστω $(G, \cdot)$ μια μη τετριμμένη ομάδα. Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Η G είναι αποσυνθέσιμη.*

(ii) *Υπάρχει κάποιος μη ενριπτικός, μη επιρριπτικός ορθόθετος ενδομορφισμός ϑ τής G, διάφορος τού τετριμμένου*[13]*, τέτοιος ώστε να ισχύει $\vartheta^2 = \vartheta$. (Εν τοιαύτη περιπτώσει, $G = \mathrm{Im}(\vartheta) \times_{\text{εσ.}} \mathrm{Ker}(\vartheta)$.)*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν $G = H \times_{\text{εσ.}} K$ για κάποιες μη τετριμμένες γνήσιες ορθόθετες υποομάδες H και K τής G, και εάν $g \in G$, τότε (λόγω τού (b) (ii) τού θεωρήματος 7.1.25) υπάρχουν *μονοσημάντως* ορισμένα στοιχεία $x \in H$ και $y \in K$, τέτοια ώστε $g = xy$. Ορίζουμε την απεικόνιση

$$\vartheta : G \longrightarrow G,\ g \longmapsto \vartheta(g) := x.$$

Η ϑ αποτελεί έναν ενδομορφισμό τής G, διότι για οιαδήποτε στοιχεία $g_1, g_2 \in G$ με $g_1 = x_1y_1$, $g_2 = x_2y_2$ (όπου τα $x_1, x_2 \in H$ και $y_1, y_2 \in K$ είναι *μονοσημάντως* ορισμένα) έχουμε (λόγω τού (b) (i) τού θεωρήματος 7.1.25)

$$\vartheta(g_1g_2) = \vartheta(x_1y_1x_2y_2) = \vartheta((x_1x_2)(y_1y_2)) = x_1x_2 = \vartheta(g_1)\,\vartheta(g_2).$$

Επίσης, εκ κατασκευής, $K = \mathrm{Ker}(\vartheta)$ και $H = \mathrm{Im}(\vartheta)$. Η ϑ δεν είναι ούτε ενριπτική (αφού $\{e_G\} \sqsubset K$) ούτε επιρριπτική (αφού $H \sqsubset G$) ούτε ο τετριμμένος ενδομορφισμός (αφού[14] $K \sqsubset G$). Εξάλλου,

$$\vartheta^2(g) = \vartheta(\vartheta(g)) = \vartheta(x) = \vartheta(xe_G) = x = \vartheta(g)$$

για κάθε $g = xy$ (υπό την ανωτέρω μονοσημάντως ορισμένη παράστασή του). Τέλος, για κάθε $(g_1, g_2) \in G \times G$, όπου $g_1 = x_1y_1$, $g_2 = x_2y_2$ (όπως προηγουμένως), έχουμε (λόγω τού (b) (i) τού θεωρήματος 7.1.25)

$$\begin{aligned} g_1\vartheta(g_2)g_1^{-1} &= x_1y_1x_2\,(x_1y_1)^{-1} = x_1\,(y_1x_2)\,y_1^{-1}{x_1}^{-1} = x_1\,(x_2y_1)\,y_1^{-1}{x_1}^{-1} \\ &= x_1x_2\left(y_1y_1^{-1}\right){x_1}^{-1} = x_1x_2e_G{x_1}^{-1} = x_1x_2{x_1}^{-1} \end{aligned}$$

και

$$\begin{aligned} \vartheta(g_1g_2g_1^{-1}) &= \vartheta(x_1y_1x_2y_2y_1^{-1}{x_1}^{-1}) = \vartheta(x_1x_2\left(y_1y_2y_1^{-1}\right){x_1}^{-1}) \\ &= \vartheta(\left(x_1x_2{x_1}^{-1}\right)\left(y_1y_2y_1^{-1}\right)) = x_1x_2{x_1}^{-1}, \end{aligned}$$

[13] Με τον όρο *τετριμμένος ενδομορφισμός* εννοούμε τον ενδομορφισμό τής G που στέλνει κάθε στοιχείο τής G να απεικονισθεί στο ουδέτερο στοιχείο e_G τής G.

[14] Σημειωτέον ότι $K = G \Leftrightarrow \vartheta(g) = e_G,\ \forall g \in G \Leftrightarrow H = \{e_G\}$.

οπότε $g_1\vartheta(g_2)g_1^{-1} = \vartheta(g_1g_2g_1^{-1})$ και ο είναι ορθόθετος ενδομορφισμός.
(ii)⇒(i) Εάν υπάρχει ορθόθετος ενδομορφισμός $\vartheta \in \mathrm{End}(G)$ με τις ως άνω ιδιότητες, τότε θέτοντας $H := \mathrm{Im}(\vartheta)$ και $K := \mathrm{Ker}(\vartheta)$, παρατηρούμε ότι

$$\{e_G\} \sqsubset H \sqsubset G \text{ και } \{e_G\} \sqsubset K \sqsubset G$$

(διότι εξ υποθέσεως η G είναι μη τετριμμένη και ο ϑ μη ενριπτικός, μη επιρριπτικός, μη τετριμμένος ενδομορφισμός τής G). Θεωρώντας τυχόν $g \in G$ διαπιστώνουμε ότι για τα $x := \vartheta(g)$ και $y := x^{-1}g$ ισχύει η ισότητα

$$g = x(x^{-1}g), \text{ όπου } x \in H \text{ και } x^{-1}g \in K \Rightarrow G = HK \tag{7.15}$$

(διότι $\vartheta\left(x^{-1}g\right) = \vartheta\left(x^{-1}\right)\vartheta(g) = \vartheta\left(x^{-1}e_G\right)\vartheta(g) = x^{-1}x = e_G \Rightarrow x^{-1}g \in K$). Επιπροσθέτως, εάν $z \in H \cap K$, τότε

$$\left.\begin{array}{r} \exists g \in G : \vartheta(g) = z \text{ και } \vartheta(z) = e_G \\ z = \vartheta(g) = \vartheta(\vartheta(g)) = \vartheta(z) \end{array}\right\} \Rightarrow z = e_G \Rightarrow H \cap K = \{e_G\}. \tag{7.16}$$

Τέλος, για *οιαδήποτε* $x \in H$ και $y \in K$ υπάρχει $g \in G : \vartheta(g) = x$ και $\vartheta(y) = e_G$, οπότε έχουμε αφ' ενός μεν

$$\vartheta(x) = \vartheta(\vartheta(g)) = \vartheta(g) = x, \tag{7.17}$$

αφ' ετέρου δε

$$\left.\begin{array}{r} yxy^{-1} = y\vartheta(g)y^{-1} = \vartheta(ygy^{-1}) \in H \\ yxy^{-1} = \vartheta(ygy^{-1}) = \vartheta(\vartheta(ygy^{-1})) = \vartheta(yxy^{-1}) \end{array}\right\} \Rightarrow \vartheta(yxy^{-1}) = yxy^{-1}. \tag{7.18}$$

Επειδή $y, y^{-1} \in K$, συνάγεται ότι

$$\vartheta(yxy^{-1}) = \vartheta(y)\vartheta(x)\vartheta(y^{-1}) = e_G\vartheta(x)e_G = \vartheta(x). \tag{7.19}$$

Οι (7.17), (7.18) και (7.19) δίδουν

$$yxy^{-1} = x \Rightarrow xy = yx. \tag{7.20}$$

Κατά συνέπειαν, λόγω των (7.15), (7.16) και (7.20) ικανοποιούνται οι συνθήκες (b) (i)-(iii) τού θεωρήματος 7.1.26, πράγμα που σημαίνει ότι $H \lhd G$, $K \lhd G$ και $G = H \times_{\text{εσ.}} K$. □

7.1.41 Πρόταση. *Εάν υποθέσουμε ότι $(G, \cdot)$ και $(L, *)$ είναι δυο αναποσυνθέσιμες ομάδες και $f_1 : G \longrightarrow L$, $f_2 : L \longrightarrow G$ δυο ομομορφισμοί, τέτοιοι ώστε να ισχύει $f_1 \circ f_2 \in \mathrm{Aut}(L)$ και $\mathrm{Im}(f_2) \trianglelefteq G$, τότε αμφότεροι οι f_1, f_2 είναι ισομορφισμοί.*

ΑΠΟΔΕΙΞΗ. Επειδή η $(f_1 \circ f_2)^{-1} \circ f_1 : G \longrightarrow L$ (ως απεικόνιση) αποτελεί αριστερό αντίστροφο τής f_2 (ως προς την πράξη τής συνθέσεως), η f_2 είναι ενριπτική και η $\widetilde{f_2} : L \longrightarrow \mathrm{Im}(f_2)$, η προκύπτουσα ύστερα από περιορισμό τού πεδίου τιμών τής f_2 επί τής $\mathrm{Im}(f_2)$, αμφιρριπτική και, κατ' επέκταση, ισομορφισμός. Ο περιορισμός

$(f_1 \circ f_2)^{-1} \circ f_1\Big|_{\mathrm{Im}(f_2)} : \mathrm{Im}\,(f_2) \longrightarrow L$ τής $(f_1 \circ f_2)^{-1} \circ f_1$ επί τής $\mathrm{Im}(f_2)$ είναι ένας ισομορφισμός[15] μεταξύ των $H := \mathrm{Im}\,(f_2) \trianglelefteq G$ και L, οπότε η πρόταση 7.1.23 μας πληροφορεί ότι $G = H \times_{\text{εσ.}} K$, όπου $K := \mathrm{Ker}((f_1 \circ f_2)^{-1} \circ f_1) = \mathrm{Ker}(f_1)$. Επειδή η G είναι εξ υποθέσεως αναποσυνθέσιμη και η f_2 δεν είναι ο τετριμμένος ομομορφισμός[16], λαμβάνουμε $K = \{e_G\}$ και $H = G$, οπότε αμφότεροι οι f_2 και $f_1 = (f_1 \circ f_2) \circ f_2^{-1}$ είναι ισομορφισμοί. □

7.1.42 Λήμμα. *Εάν οι H και K είναι υποομάδες μιας ομάδας $(G, \cdot)$, τότε για την απεικόνιση*

$$f_{H,K} : H \times K \longrightarrow G,\ (x, y) \longmapsto f_{H,K}(x, y) := xy, \tag{7.21}$$

ισχύουν τα εξής:

(i) $\mathrm{Im}(f_{H,K}) = HK$.

(ii) *H $f_{H,K}$ είναι ενριπτική απεικόνιση εάν και μόνον εάν $H \cap K = \{e_G\}$.*

(iii) *H $f_{H,K}$ είναι ομομορφισμός εάν και μόνον εάν $xy = yx,\ \forall x \in H$ και $\forall y \in K$.*

ΑΠΟΔΕΙΞΗ. (i) Προφανώς,

$$\mathrm{Im}(f_{H,K}) = \{f_{H,K}(x, y)\,|(x, y) \in H \times K\} = \{xy\,|(x, y) \in H \times K\} = HK.$$

(ii) Εάν η $f_{H,K}$ είναι ενριπτική απεικόνιση και $z \in H \cap K$, τότε

$$\left.\begin{array}{r} z \in H,\ z \in K \Rightarrow z^{-1} \in K \\ f_{H,K}(z, z^{-1}) = zz^{-1} = e_G = f(e_G, e_G) \end{array}\right\} \Rightarrow \left(z, z^{-1}\right) = (e_G, e_G) \Rightarrow z = e_G.$$

Και αντιστρόφως· εάν $H \cap K = \{e_G\}$ και $f_{H,K}\,(x_1, y_1) = f_{H,K}\,(x_2, y_2)$ για κάποια στοιχεία (x_1, y_1) και (x_2, y_2) τού $H \times K$, τότε $x_1y_1 = x_2y_2 \Rightarrow x_2^{-1}x_1 = y_2y_1^{-1}$. Επειδή το αριστερό μέλος αυτής τής τελευταίας ισότητας ανήκει στην H και το δεξιό στην K, *και* τα δύο μέλη θα ανήκουν στην τομή $H \cap K = \{e_G\}$. Άρα

$$x_2^{-1}x_1 = e_G = y_2{y_1}^{-1} \Longrightarrow x_1 = x_2,\ y_1 = y_2,$$

οπότε η $f_{H,K}$ είναι ενριπτική.

(iii) Εάν η $f_{H,K}$ είναι ομομορφισμός ομάδων και $x \in H$, $y \in K$, τότε

$$xy = f_{H,K}(x, y) = f_{H,K}\left((e_G, y)(x, e_G)\right) = f_{H,K}(e_G, y) f_{H,K}(x, e_G) = yx.$$

Και αντιστρόφως· εάν ικανοποιείται η ανωτέρω συνθήκη, τότε για οιαδήποτε στοιχεία $(x_1, y_1), (x_2, y_2) \in H \times K$ έχουμε

$$\begin{aligned} f_{H,K}\left((x_1, y_1)(x_2, y_2)\right) &= f_{H,K}\left(x_1x_2, y_1y_2\right) = x_1x_2y_1y_2 \\ &= x_1y_1x_2y_2 \left(\begin{array}{c} \text{επειδή εξ υποθέσεως κάθε στοιχείο} \\ \text{τής υποομάδας } H \text{ μετατίθεται} \\ \text{αμοιβαίως με κάθε στοιχείο τής } K \end{array}\right) \\ &= f_{H,K}\left(x_1, y_1\right) f_{H,K}\left(x_2, y_2\right). \end{aligned}$$

[15] Πρόκειται για τον αντίστροφο τού $\tilde{f}_2$.

[16] Εάν ίσχυε $H = f_2(L) = \{e_G\}$, τότε η f_2 δεν θα ήταν ενριπτική, διότι $\exists x \in L \setminus \{e_L\}$ (αφού η ομάδα L, ούσα αναποσυνθέσιμη, δεν είναι τετριμμένη) με $f_2(x) = e_G = f_2(e_G)$.

Τούτο σημαίνει ότι η $f_{H,K}$ είναι ομομορφισμός. □

► **Συσχετισμός εξωτερικού και εσωτερικού ευθέος γινομένου**. Αυτός αποσαφηνίζεται στο ακόλουθο:

7.1.43 Θεώρημα. (i) *Εάν, δοθεισών δυο ομάδων G_1, G_2, συμβολίσουμε ως*

$$\overline{G}_1 := \mathrm{Im}(\iota_1) \ \text{ και } \ \overline{G}_2 := \mathrm{Im}(\iota_2)$$

τις εικόνες των φυσικών εμφυτεύσεων

$$\iota_1 : G_1 \longrightarrow G_1 \times G_2 \ \text{ και } \ \iota_2 : G_2 \longrightarrow G_1 \times G_2,$$

αντιστοίχως, τότε

$$\boxed{\overline{G}_1 \times_{\text{εσ.}} \overline{G}_2 = G_1 \times G_2.}$$

(ii) *Εάν οι H και K είναι ορθόθετες υποομάδες μιας ομάδας $(G, \cdot)$, τέτοιες ώστε να ισχύει $G = H \times_{\text{εσ.}} K$, τότε η απεικόνιση* (7.21) *είναι ισομορφισμός ομάδων, οπότε*

$$\boxed{H \times K \cong G = H \times_{\text{εσ.}} K.}$$

ΑΠΟΔΕΙΞΗ. (i) Βλ. το (iv) τής προτάσεως 7.1.4.

(ii) Εάν $G = H \times_{\text{εσ.}} K$, τότε, λαμβάνοντας υπ' όψιν τη συνεπαγωγή (a)⇒(b) στο θεώρημα 7.1.26, το λήμμα 7.1.42 μας πληροφορεί ότι η απεικόνιση (7.21) είναι ισομορφισμός ομάδων. □

7.1.44 Σημείωση. Λόγω τού θεωρήματος 7.1.43 είθισται να μην γίνεται *ομαδοθεωρητική διάκριση*[17] μεταξύ τού εξωτερικού ευθέος γινομένου $H \times K$ και τού εσωτερικού ευθέος γινομένου $H \times_{\text{εσ.}} K$, και οι H και K να αναφέρονται απλώς ως **ευθείς παράγοντές του** (ή ως **ευθείς προσθετέοι του**, όταν χρησιμοποιείται ο προσθετικός συμβολισμός). Ωστόσο, υπάρχουν «λεπτές πτυχές» κάποιων σημαντικών θεωρητικών επιχειρημάτων που μας υπαγορεύουν την περαιτέρω διατήρηση των διακριτών συμβολισμών.

7.1.45 Πόρισμα. *Εάν η $(G, \cdot)$ είναι μια μη τετριμμένη ομάδα, τότε τα ακόλουθα είναι ισοδύναμα*:

(i) *Η G είναι αποσυνθέσιμη ομάδα* (*υπό την έννοια τού ορισμού* 7.1.32).

(ii) *Υπάρχουν μη τετριμμένες ομάδες G_1, G_2, τέτοιες ώστε να ισχύει $G = G_1 \times G_2$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν $G = H \times_{\text{εσ.}} K$ για κάποιες μη τετριμμένες γνήσιες ορθόθετες υποομάδες H και K τής G, τότε (σύμφωνα με το (ii) τού θεωρήματος 7.1.43) η απεικόνιση

$$f_{H,K} : H \times K \longrightarrow G, \ (x, y) \longmapsto f_{H,K}(x, y) := xy,$$

[17] Στην πραγματικότητα, η μόνη διαφορά μεταξύ των δύο ειδών ευθέων γινομένων δύο ομάδων, ήτοι τού *εσωτερικού* και τού *εξωτερικού*, έγκειται στο ότι το πρώτο εξ αυτών περιέχει τους παράγοντές του, ενώ το δεύτερο περιέχει ισόμορφα «αντίτυπα» αυτών.

είναι ισομορφισμός, οπότε αρκεί να θέσουμε $G_1 := f_{H,K}(H)$ και $G_2 := f_{H,K}(K)$.
(ii)⇒(i) Εάν υπάρχουν μη τετριμμένες ομάδες G_1, G_2, τέτοιες ώστε $G = G_1 \times G_2$, τότε θέτοντας $H := \overline{G}_1$ και $K := \overline{G}_2$ (όπου $\overline{G}_1 = G_1 \times \{e_{G_2}\}$ και $\overline{G}_2 = \{e_{G_1}\} \times G_2$), λαμβάνουμε $G = H \times_{\text{εσ.}} K$ μέσω τού (i) τού θεωρήματος 7.1.43. □

► **Πρώτες εφαρμογές.** Από το πόρισμα 5.6.7 γνωρίζουμε ότι οι ομάδες τάξεως p^2, όπου p κάποιος πρώτος αριθμός, είναι αβελιανές. Αυτές ταξινομούνται πλήρως (μέχρις ισομορφισμού) μέσω τού ακόλουθου θεωρήματος:

7.1.46 Θεώρημα. (Ταξινόμηση ομάδων τάξεως p^2.) *Εάν η $(G, \cdot)$ είναι μια ομάδα τάξεως $|G| = p^2$, όπου p πρώτος αριθμός, τότε είτε*

$$\boxed{G \cong \mathbb{Z}_{p^2}} \quad \textit{είτε} \quad \boxed{G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p.}$$

ΑΠΟΔΕΙΞΗ. Έστω $(G, \cdot)$ μια ομάδα τάξεως $|G| = p^2$. Κατά το πόρισμα 5.6.7, η G είναι *αβελιανή*. Εάν υπάρχει ένα στοιχείο τής G τάξεως p^2, τότε $G \cong \mathbb{Z}_{p^2}$. (Βλ. 2.3.7 και 2.4.23 (ii).) Εάν δεν υπάρχει κανένα στοιχείο τής G τάξεως p^2, τότε (σύμφωνα με το θεώρημα 4.1.22 τού Lagrange) *κάθε στοιχείο* διαφορετικό τού ουδετέρου *οφείλει να έχει τάξη* p. Εν τοιαύτη περιπτώσει, επιλέγοντας ένα $x \in G \setminus \{e_G\}$ και ένα $y \in G \setminus \langle x \rangle$ παρατηρούμε ότι $\langle x \rangle \lhd G$, $\langle y \rangle \lhd G$ (βλ. 4.2.6) και $|\langle x \rangle| = |\langle y \rangle| = p$, απ' όπου έπεται ότι[18] $\langle x \rangle \cap \langle y \rangle = \{e_G\}$ και ότι τα p^2 στοιχεία $x^i y^j, 1 \leq i, j \leq p$, είναι σαφώς διακεκριμένα[19]. Επομένως, $\langle x \rangle \langle y \rangle = G$ και (σύμφωνα με το (ii) τού θεωρήματος 7.1.43) έχουμε $G = \langle x \rangle \times_{\text{εσ.}} \langle y \rangle \cong \langle x \rangle \times \langle y \rangle$, οπότε $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$. (Βλ. 2.3.7 και 2.4.23 (ii)). □

7.1.47 Σημείωση. Κατά το (iv) τής προτάσεως 2.4.19, $\mathbb{Z}_p \oplus \mathbb{Z}_p \ncong \mathbb{Z}_{p^2}$.

7.1.48 Θεώρημα. *Έστω ότι οι H και K είναι ορθόθετες υποομάδες μιας πεπερασμένης ομάδας $(G, \cdot)$. Εάν $|G| = mn$ και $|H| = m$, $|K| = n$, όπου $m, n \in \mathbb{N}$ με* μκδ$(m, n) = 1$, *τότε $G = H \times_{\text{εσ.}} K \cong H \times K$.*

ΑΠΟΔΕΙΞΗ. Κατά το (ii) τού πορίσματος 4.1.25, $H \cap K = \{e_G\}$. Εξάλλου, από τον τύπο (4.35) τού γινομένου προκύπτει ότι

$$\text{card}(HK) = \frac{|H|\ |K|}{|H \cap K|} = |H|\ |K| = mn = |G| \Rightarrow G = HK.$$

Άρα οι H και K ικανοποιούν τις συνθήκες (i), (ii) και (iii) τού ορισμού 7.1.21. Ως εκ τούτου, $G = H \times_{\text{εσ.}} K \cong H \times K$ (βλ. 7.1.43 (ii)). □

7.1.49 Θεώρημα. *Έστω $(G, \cdot)$ πεπερασμένη αβελιανή ομάδα τάξεως $|G| = mn$, όπου $m, n \in \mathbb{N}$ με* μκδ$(m, n) = 1$. *Τότε υπάρχει μία και μόνον υποομάδα H τής ομάδας G τάξεως $|H| = m$ και μία και μόνον υποομάδα K τής G τάξεως $|K| = n$. Επιπροσθέτως, $G = H \times_{\text{εσ.}} K \cong H \times K$.*

[18] Προφανώς, $y \in G \setminus \langle x \rangle \Rightarrow \langle x \rangle \neq \langle y \rangle \Rightarrow \langle x \rangle \cap \langle y \rangle \sqsubset \langle y \rangle \underset{4.1.24}{\Longrightarrow} \langle x \rangle \cap \langle y \rangle = \{e_G\}$.

[19] Εάν $x^i y^j = x^{i'} y^{j'}$ για κάποιους $i, i', j, j' \in \{1, ..., p\}$, τότε $\langle x \rangle \ni x^{i-i'} = y^{j'-j} \in \langle y \rangle$ και (επειδή $\langle x \rangle \cap \langle y \rangle = \{e_G\}$) ισχύει $x^{i-i'} = e_G = y^{j'-j} \Rightarrow x^i = x^{i'}$ και $y^j = y^{j'}$.

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το θεώρημα 4.4.21 $\exists\, x, y \in G$, τέτοια ώστε $|\langle x\rangle| = m$ και $|\langle y\rangle| = n$. Θέτουμε $H := \langle x\rangle$ και $K := \langle y\rangle$. Επειδή η G είναι αβελιανή ομάδα, έχουμε $H \lhd G$ και $K \lhd G$. (Βλ. πρόταση 4.2.6). Προφανώς, $|G/H| = n$ και $|G/K| = m$. Κατά το πόρισμα 4.5.17 η H είναι η μοναδική υποομάδα τής G τάξεως m και η K είναι η μοναδική υποομάδα τής G τάξεως n. Επιπροσθέτως, από το θεώρημα 7.1.48 έπεται ότι $G = H \times_{\text{εσ.}} K \cong H \times K$. □

► **«Εξωτερικό» ευθύ γινόμενο με πεπερασμένο πλήθος παραγόντων**. Ο ορισμός 7.1.1 γενικεύεται για s τυχούσες ομάδες (όπου $s \in \mathbb{N}$, $s \geq 2$) ως ακολούθως:

7.1.50 Ορισμός. Έστω ότι $s \in \mathbb{N}$, $s \geq 2$, και ότι οι

$$(G_1, \circledast_1), (G_1, \circledast_2),..., (G_{s-1}, \circledast_{s-1}), (G_s, \circledast_s)$$

είναι s τυχούσες ομάδες. Εφοδιάζοντας το καρτεσιανό γινόμενο

$$\prod_{j=1}^{s} G_j := G_1 \times G_2 \times \cdots \times G_{s-1} \times G_s,$$

των υποκειμένων συνόλων τους με την εσωτερική πράξη

$$\prod_{j=1}^{s} G_j \times \prod_{j=1}^{s} G_j \longrightarrow \prod_{j=1}^{s} G_j$$
$$((x_1, .., x_s), (y_1, .., y_s)) \longmapsto (x_1, .., x_s) \boxdot (y_1, .., y_s) := (x_1 \circledast_1 y_1, .., x_s \circledast_s y_s),$$

παρατηρούμε ότι το ζεύγος $(\prod_{j=1}^{s} G_j, \boxdot)$ αποτελεί ομάδα έχουσα (ως προς την ορισθείσα πράξη "$\boxdot$") το $(e_{G_1},..., e_{G_s})$ ως ουδέτερο στοιχείο της και το $(x_1^{-1},..., x_s^{-1})$ ως αντίστροφο στοιχείο οιουδήποτε $(x_1,..., x_s) \in \prod_{j=1}^{s} G_j$, όπου x_j^{-1} το αντίστροφο στοιχείο τού $x_j \in G_j$ ως προς την " $\circledast_j$ " για κάθε $j \in \{1,..., s\}$. Η ομάδα $(\prod_{j=1}^{s} G_j, \boxdot)$ καλείται **εξωτερικό ευθύ γινόμενο των** $(G_1, \circledast_1),..., (G_s, \circledast_s)$. Έστω $i \in \{1,..., s\}$. Η επίρριψη

$$\text{pr}_i : \prod_{j=1}^{s} G_j \longrightarrow G_i,\ (x_1,..., x_s) \mapsto x_i,$$

καλείται (i-οστή) **φυσική προβολή τής** $\prod_{j=1}^{s} G_j$ **επί τής** G_i. Επίσης, η ένριψη

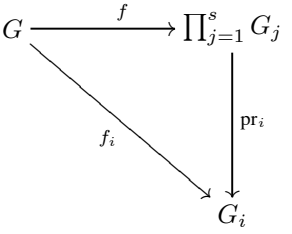
$$\iota_i : G_i \longrightarrow \prod_{j=1}^{s} G_j,\ x \mapsto (e_{G_1},..., e_{G_{i-1}}, x, e_{G_{i+1}}..., , e_{G_s}),$$

καλείται (i-οστή) **φυσική εμφύτευση τής** G_i **εντός τής** $\prod_{j=1}^{s} G_j$.

Οι προτάσεις 7.1.51, 7.1.52 και 7.1.53 μπορούν να θεωρηθούν ως άμεσες γενικεύσεις των προτάσεων 7.1.2, 7.1.3 και 7.1.4. Γι' αυτόν τον λόγο οι αποδείξεις τους αφήνονται ως ασκήσεις για τον αναγνώστη.

7.1.51 Πρόταση. *Οι* pr_i *είναι επιμορφισμοί ομάδων έχοντες ως πυρήνες τους τις υποομάδες* $\text{Ker}(\text{pr}_i) = G_1 \times \cdots \times G_{i-1} \times \{e_{G_i}\} \times G_{i+1} \times \cdots \times G_s$, *οπότε για κάθε* $i \in \{1,..., s\}$ *έχουμε* $(\prod_{j=1}^{s} G_j)/\,(G_1 \times \cdots \times G_{i-1} \times \{e_{G_i}\} \times G_{i+1} \times \cdots \times G_s) \cong G_i$.

7.1.52 Πρόταση. («Καθολική ιδιότητα» εξωτερικού ευθέος γινομένου.) *Έστω $(G,*)$ μια ομάδα. Εάν οι $f_i : G \longrightarrow G_i$ είναι ομομορφισμοί ομάδων, τότε υφίσταται ένας και μόνον ομομορφισμός ομάδων $f : (G,*) \longrightarrow (\prod_{j=1}^{s} G_j, \boxdot)$, τέτοιος ώστε να ισχύει $\mathrm{pr}_i \circ f = f_i$, δηλαδή τέτοιος ώστε το διάγραμμα*



να καθίσταται μεταθετικό για κάθε $i \in \{1,...,s\}$.

7.1.53 Πρόταση. *Για $i \in \{1,...,s\}$ ας συμβολίσουμε ως $\overline{G}_i := \mathrm{Im}(\iota_i)$ την εικόνα τής φυσικής εμφυτεύσεως $\iota_i : G_i \longrightarrow \prod_{j=1}^{s} G_j,\ x \mapsto (e_{G_1},...,e_{G_{i-1}},x,e_{G_{i+1}},...,,e_{G_s})$. Τότε για κάθε $i \in \{1,...,s\}$ ισχύουν τα ακόλουθα:*

(i) *Η ι_i είναι μονομορφισμός ομάδων και, ως εκ τούτου, $G_i \cong \overline{G}_i$.*

(ii) $\overline{G}_i = \{e_{G_1}\} \times \cdots \times \{e_{G_{i-1}}\} \times G_i \times \{e_{G_{i+1}}\} \times \cdots \times \{e_{G_s}\} \trianglelefteq \prod_{j=1}^{s} G_j$.

(iii) $\overline{G}_i \cap \left(\overline{G}_1 \boxdot \overline{G}_2 \boxdot \cdots \boxdot \overline{G}_{i-1} \boxdot \overline{G}_{i+1} \boxdot \cdots \boxdot \overline{G}_s\right) = \{(e_{G_1},...,e_{G_s})\}$.

(iv) $\overline{G}_1 \boxdot \overline{G}_2 \boxdot \cdots \boxdot \overline{G}_s = \prod_{j=1}^{s} G_j$.

7.1.54 Σημείωση. (Απλούστευση συμβολισμού.) (i) Όπως συνέβη και στην περίπτωση κατά την οποία $s = 2$ (βλ. σημείωση 7.1.5), θα μεταβούμε, από εδώ και στο εξής, στον *απλουστευμένο πολλαπλασιαστικό* συμβολισμό των πράξεων των ομάδων $G_1,...,G_s$ και $\prod_{j=1}^{s} G_j$ (μέσω τού συνήθους dot "$\cdot$"), με μόνη εξαίρεση τις (κατά τα ειωθότα θεωρούμενες ως) *προσθετικές* ομάδες (για τις οποίες γράφουμε $\bigoplus_{j=1}^{s} G_j$ αντί τού $\prod_{j=1}^{s} G_j$).

(ii) Εάν $G_1 = \cdots = G_s =: G$, τότε αντί τού $\prod_{j=1}^{s} G_j$ γράφουμε απλώς G^s. (Σύμβαση: Ο συμβολισμός αυτός επεκτείνεται προδήλως και για $s = 1$ και $s = 0$. Όταν $s = 0$, τότε ως G^0 νοείται η τετριμμένη ομάδα.)

7.1.55 Πρόταση. *Έστω ότι $s \in \mathbb{N}$, $s \geq 2$, και ότι οι $G_1,...,G_s$ είναι s τυχούσες ομάδες. Τότε ισχύουν τα εξής:*

(i) $\left|\prod_{j=1}^{s} G_j\right| = \prod_{j=1}^{s} |G_j|$. *Ως εκ τούτου, το εξωτερικό ευθύ γινόμενο $\prod_{j=1}^{s} G_j$ των $G_1,...,G_s$ είναι πεπερασμένη (και αντιστοίχως, άπειρη) ομάδα εάν και μόνον εάν όλες οι ομάδες $G_1,...,G_s$ είναι πεπερασμένες (και αντιστοίχως, εάν και μόνον εάν μία τουλάχιστον εκ των $G_1,...,G_s$ είναι άπειρη).*

(ii) *Για κάθε μετάταξη $\sigma \in \mathfrak{S}_s$ υφίσταται ισομορφισμός ομάδων*

$$\boxed{\prod_{j=1}^{s} G_j \cong \prod_{j=1}^{s} G_{\sigma(j)}.}$$

(iii) *Εάν* $r \in \mathbb{N}, r+1 \leq s,$ *και* $\kappa_1, .., \kappa_r \in \mathbb{N}$ *με* $1 \leq \kappa_1 < \kappa_2 < ... < \kappa_r < s,$ *τότε*

$$\boxed{\prod_{j=1}^{s} G_j \cong (G_1 \times \cdots \times G_{\kappa_1}) \times (G_{\kappa_1+1} \times \cdots \times G_{\kappa_2}) \times \cdots \times (G_{\kappa_r+1} \times \cdots \times G_s)\,.}$$

(iv) *Εάν υπάρχει δείκτης* $i \in \{1,...,s\}$ *, τέτοιος ώστε η* G_i *να είναι τετριμμένη, τότε*

$$\boxed{\prod_{j=1}^{s} G_j \cong \prod_{j \in \{1,..,s\} \setminus \{i\}} G_j.}$$

(v) *Εάν οι* $H_1,...,H_s$ *είναι* s *ομάδες, τέτοιες ώστε να ισχύει* $G_j \cong H_j$ *για κάθε δείκτη* $j \in \{1,...,s\}$ *, τότε*

$$\boxed{\prod_{j=1}^{s} G_j \cong \prod_{j=1}^{s} H_j.}$$

ΑΠΟΔΕΙΞΗ. (i) Τούτο έπεται άμεσα από τις ιδιότητες των πληθικών αριθμών που είναι γνωστές από τη Θεωρία Συνόλων.

(ii) Είναι άμεσος ο έλεγχος τού ότι η απεικόνιση

$$\prod_{j=1}^{s} G_j \ni (g_1,...,g_s) \longmapsto (g_{\sigma(1)},...,g_{\sigma(s)}) \in \prod_{j=1}^{s} G_{\sigma(j)}$$

αποτελεί ισομορφισμό ομάδων.

(iii) Παρομοίως, διαπιστώνουμε ότι η απεικόνιση

$$\begin{aligned} \prod_{j=1}^{s} G_j &\longrightarrow (G_1 \times \cdots \times G_{\kappa_1}) \times \cdots \times (G_{\kappa_r+1} \times \cdots \times G_s) \\ (g_1,...,g_s) &\longmapsto ((g_1,...,g_{\kappa_1}),...,(g_{\kappa_r+1},...,g_s)) \end{aligned}$$

είναι ισομορφισμός ομάδων.

(iv) Η απεικόνιση

$$\prod_{j=1}^{s} G_j \longrightarrow \prod_{j \in \{1,..,s\} \setminus \{i\}} G_j,\ (g_1,..,g_{i-1},e_{G_i},g_{i+1},..,g_s) \mapsto (g_1,..,g_{i-1},g_{i+1},..,g_s),$$

είναι προδήλως ένας ισομορφισμός ομάδων.

(v) Έστω ότι οι $f_j : G_j \longrightarrow H_j$ είναι ισομορφισμοί για κάθε $j \in \{1,...,s\}$. Τότε και η απεικόνιση $\prod_{j=1}^{s} G_j \ni (g_1,...,g_s) \longmapsto (f_1(g_1),...,f_s(g_s)) \in \prod_{j=1}^{s} H_j$ είναι ισομορφισμός ομάδων. □

7.1.56 Πόρισμα. *Για οιεσδήποτε ομάδες* G_1, G_2, G_3 *υφίστανται ισομορφισμοί*

$$G_1 \times G_2 \cong G_2 \times G_1 \ \text{ και } \ (G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3)\,.$$

7.1.57 Πρόταση. *Έστω ότι* $s \in \mathbb{N}$, $s \geq 2$, *και ότι οι* $G_1,...,G_s$ *είναι* s *τυχούσες ομάδες. Τότε ισχύουν τα εξής*:

(i) *Το κέντρο τής ομάδας* $\prod_{j=1}^{s} G_j$ *ισούται με*

$$\boxed{Z(\prod_{j=1}^{s} G_j) = \prod_{j=1}^{s} Z(G_j).}$$

(ii) $H \prod_{j=1}^{s} G_j$ *είναι αβελιανή* $\Longleftrightarrow$ *η* G_j *είναι αβελιανή για κάθε* $j \in \{1,...,s\}$.

(iii) *Εάν* $H_j \sqsubseteq G_j$ *για κάθε* $j \in \{1,...,s\}$, *τότε* $\prod_{j=1}^{s} H_j \sqsubseteq \prod_{j=1}^{s} G_j$.

(iv) *Εάν* $H_j \trianglelefteq G_j$ *για κάθε* $j \in \{1,...,s\}$, *τότε* $\prod_{j=1}^{s} H_j \trianglelefteq \prod_{j=1}^{s} G_j$ *και*

$$\boxed{(\prod_{j=1}^{s} G_j)/(\prod_{j=1}^{s} H_j) \cong \prod_{j=1}^{s} (G_j/H_j)\,.} \tag{7.22}$$

(v) *Εάν* $H_j \sqsubseteq G_j$ *για κάθε* $j \in \{1,...,s\}$ *και* $\prod_{j=1}^{s} H_j \trianglelefteq \prod_{j=1}^{s} G_j$, *τότε* $H_j \trianglelefteq G_j$ *για κάθε* $j \in \{1,...,s\}$.

(vi) *Εάν οι* $(\prod_{j=1}^{s} G_j)' = [\prod_{j=1}^{s} G_j, \prod_{j=1}^{s} G_j]$ *και* $G_j{}' = [G_j, G_j]$ *είναι οι μεταθέτριες υποομάδες των* $\prod_{j=1}^{s} G_j$ *και* G_j, *αντιστοίχως, για κάθε* $j \in \{1,...,s\}$ (βλ. ορισμούς 5.5.4 και 5.5.29), *τότε*

$$\boxed{(\prod_{j=1}^{s} G_j)' = \prod_{j=1}^{s} G_j{}'.}$$

(vii) *Εάν οι* $(\prod_{j=1}^{s} G_j)^{\text{ab}}$ *και* G_j^{ab} *είναι οι αβελιανοποιήσεις των* $\prod_{j=1}^{s} G_j$ *και* G_j, *αντιστοίχως, για κάθε* $j \in \{1,...,s\}$ (βλ. 5.5.25), *τότε*

$$\boxed{(\prod_{j=1}^{s} G_j)^{\text{ab}} \cong \prod_{j=1}^{s} G_j^{\text{ab}}.}$$

ΑΠΟΔΕΙΞΗ. (i) Προφανώς, $(a_1,...,a_s) \in Z(\prod_{j=1}^{s} G_j)$ εάν και μόνον εάν

$$(a_1,...,a_s)(b_1,...,b_s) = (b_1,...,b_s)(a_1,...,a_s),\ \forall (b_1,...,b_s) \in \prod_{j=1}^{s} G_j,$$

$$\Leftrightarrow (a_1b_1,...,a_sb_s) = (b_1a_1,...,b_sa_s),\ \forall (b_1,...,b_s) \in \prod_{j=1}^{s} G_j,$$

$$\Leftrightarrow [a_jb_j = b_ja_j,\ \forall b_j \in G_j \ \text{ και } \ \forall j \in \{1,...,s\}] \Leftrightarrow [a_j \in Z(G_j),\ \forall j \in \{1,...,s\}].$$

(ii) Τούτο έπεται από το (i) και την πρόταση 5.4.2.

(iii) Εάν $H_j \sqsubseteq G_j$ για κάθε $j \in \{1,...,s\}$, τότε

$$\prod_{j=1}^{s} H_j \subseteq \prod_{j=1}^{s} G_j, \ \ (e_{G_1},...,e_{G_s}) \in \prod_{j=1}^{s} H_j$$

και για οιαδήποτε στοιχεία $(x_1,...,x_s), (y_1,...,y_s) \in \prod_{j=1}^{s} H_j$ έχουμε

$$(x_1,...,x_s)(y_1,...,y_s)^{-1} = (x_1,...,x_s)\left(y_1^{-1},...,y_s^{-1}\right) = \left(x_1y_1^{-1},...,x_sy_s^{-1}\right) \in \prod_{j=1}^{s} H_j$$

οπότε $\prod_{j=1}^{s} H_j \sqsubseteq \prod_{j=1}^{s} G_j$ (επί τη βάσει τού (iii) τής προτάσεως 2.1.16).

(iv) Εάν $H_j \trianglelefteq G_j$ για κάθε $j \in \{1,...,s\}$, τότε ορίζεται ο επιμορφισμός ομάδων

$$f : \prod_{j=1}^{s} G_j \longrightarrow \prod_{j=1}^{s} (G_j/H_j),$$

$$(g_1,...,g_s) \longmapsto f(g_1,...,g_s) := (\pi_{H_1}^{G_1}(g_1),...,\pi_{H_s}^{G_s}(g_s)) = (g_1H_1,...,g_sH_s).$$

Επειδή

$$\mathrm{Ker}(f) = \left\{ (g_1,...,g_s) \in \prod_{j=1}^{s} G_j \,\middle|\, g_j \in H_j, \ \forall j \in \{1,...,s\} \right\} = \prod_{j=1}^{s} H_j,$$

έχουμε $\prod_{j=1}^{s} H_j \trianglelefteq \prod_{j=1}^{s} G_j$ (βλ. πόρισμα 4.2.31). Εφαρμόζοντας το 1ο θεώρημα ισομορφισμών 4.5.2 για τον f διασφαλίζουμε την ύπαρξη ενός ισομορφισμού (7.22).

(v) Ας υποθέσουμε ότι $H_j \sqsubseteq G_j$ για κάθε $j \in \{1,...,s\}$ και $\prod_{j=1}^{s} H_j \trianglelefteq \prod_{j=1}^{s} G_j$. Για $j \in \{1,...,s\}$ θεωρούμε τυχόντα στοιχεία $x_j \in H_j$ και $g_j \in G_j$. Τότε

$$\prod_{j=1}^{s} H_j \ni (g_1,...,g_s)(x_1,...,x_s)(g_1,...,g_s)^{-1},$$

$$(g_1,...,g_s)(x_1,...,x_s)(g_1,...,g_s)^{-1} = \left(g_1x_1g_1^{-1},...,g_sx_sg_s^{-1}\right),$$

οπότε $g_jx_jg_j^{-1} \in H_j \Rightarrow H_j \trianglelefteq G_j$.

(vi) Ο μεταθέτης δυο στοιχείων $(a_1,...,a_s), (b_1,...,b_s) \in \prod_{j=1}^{s} G_j$ ισούται με

$$\begin{aligned}
&[(a_1,...,a_s),(b_1,...,b_s)] = (a_1,...,a_s)(b_1,...,b_s)(a_1,...,a_s)^{-1}(b_1,...,b_s)^{-1} \\
&= (a_1,...,a_s)(b_1,...,b_s)(a_1^{-1},...,a_s^{-1})(b_1^{-1},...,b_s^{-1}) \\
&= \left(a_1b_1a_1^{-1}b_1^{-1},...,a_sb_sa_s^{-1}b_s^{-1}\right) = \left([a_1,b_1],...,[a_s,b_s]\right).
\end{aligned}$$

Οιοδήποτε στοιχείο τής $(\prod_{j=1}^{s} G_j)'$ γράφεται ως γινόμενο μεταθετών υπό τη μορφή

$$\prod_{\lambda=1}^{k} \left[(a_1^{(\lambda)},...,a_s^{(\lambda)}),(b_1^{(\lambda)},...,b_s^{(\lambda)})\right]^{\varepsilon_\lambda},\ \ \varepsilon_\lambda \in \mathbb{Z},\ \forall \lambda \in \{1,..,k\},\ k \in \mathbb{N},$$

όπου $(a_1^{(\lambda)},...,a_s^{(\lambda)}),(b_1^{(\lambda)},...,b_s^{(\lambda)}) \in \prod_{j=1}^{s} G_j,\ \forall \lambda \in \{1,..,k\}$. Βάσει των προαναφερθέντων αυτό το γινόμενο γράφεται ως εξής:

$$\prod_{\lambda=1}^{k} \left(\left[a_1^{(\lambda)},b_1^{(\lambda)}\right],...,\left[a_s^{(\lambda)},b_s^{(\lambda)}\right]\right)^{\varepsilon_\lambda} = \prod_{\lambda=1}^{k} \left(\left[a_1^{(\lambda)},b_1^{(\lambda)}\right]^{\varepsilon_\lambda},...,\left[a_s^{(\lambda)},b_s^{(\lambda)}\right]^{\varepsilon_\lambda}\right)$$
$$= \prod_{\lambda=1}^{k} \left(\left[a_1^{(\lambda)},b_1^{(\lambda)}\right]^{\varepsilon_\lambda},...,\left[a_s^{(\lambda)},b_s^{(\lambda)}\right]^{\varepsilon_\lambda}\right) = \left(\prod_{\lambda=1}^{k} \left[a_1^{(\lambda)},b_1^{(\lambda)}\right]^{\varepsilon_\lambda},...,\prod_{\lambda=1}^{k} \left[a_s^{(\lambda)},b_s^{(\lambda)}\right]^{\varepsilon_\lambda}\right),$$

οπότε ανήκει στην $\prod_{j=1}^{s} G_j'$. Άρα $(\prod_{j=1}^{s} G_j)' \subseteq \prod_{j=1}^{s} G_j'$. Ο αντίστροφος εγκλεισμός αποδεικνύεται παρομοίως.

(vii) Λόγω τού (vi) έχουμε

$$(\prod_{j=1}^{s} G_j)^{\text{ab}} := (\prod_{j=1}^{s} G_j)/(\prod_{j=1}^{s} G_j)' = (\prod_{j=1}^{s} G_j)/(\prod_{j=1}^{s} G_j') \cong \prod_{j=1}^{s} \left(G_j/G_j'\right) =: \prod_{j=1}^{s} G_j^{\text{ab}},$$

όπου ο αναγραφόμενος ισομορφισμός είναι ο (7.22) εφαρμοζόμενος για τις ορθόθετες υποομάδες $H_j := G_j'$ τής G_j για κάθε $j \in \{1,...,s\}$. □

7.1.58 Σημείωση. Το θεώρημα 7.1.10 των Goursat και Remak είναι δυνατόν να γενικευθεί καταλλήλως και για το εξωτερικό ευθύ γινόμενο $s \geq 3$ ομάδων, έστω κι αν οι σχετικές λεπτομέρειες φαντάζουν αρκούντως περίπλοκες[20].

7.1.59 Πρόταση. *Έστω ότι $s \in \mathbb{N}$, $s \geq 2$, και ότι οι $G_1,...,G_s$ είναι s τυχούσες ομάδες. Η τάξη οιουδήποτε στοιχείου $(g_1,...,g_s) \in \prod_{j=1}^{s} G_j$ υπολογίζεται ως ακολούθως*:

(i) *Εάν η τάξη* $\text{ord}(g_j)$ *τού στοιχείου g_j εντός τής ομάδας G_j είναι πεπερασμένη για κάθε $j \in \{1,...,s\}$, τότε* $\text{ord}((g_1,...,g_s)) = \text{εκπ}(\text{ord}(g_1),...,\text{ord}(g_s))$.

(ii) *Εάν υπάρχει δείκτης $i_0 \in \{1,...,s\}$, τέτοιος ώστε η τάξη* $\text{ord}(g_{i_0})$ *τού g_{i_0} εντός τής G_{i_0} να είναι άπειρη, τότε* $\text{ord}((g_1,...,g_s)) = \infty$.

ΑΠΟΔΕΙΞΗ. (i) Εάν η τάξη $\text{ord}(g_j)$ τού g_j εντός τής G_j είναι πεπερασμένη για κάθε $j \in \{1,...,s\}$ και $k \in \mathbb{N}$, τέτοιος ώστε να ισχύει

$$(g_1^k,...,g_s^k) = (g_1,...,g_s)^k = (e_{G_1},...,e_{G_s}),$$

τότε $g_j^k = e_{G_j} \underset{2.3.8}{\Longrightarrow} \text{ord}(g_j) \mid k$ για κάθε $j \in \{1,...,s\}$, οπότε ο k είναι κάποιο *κοινό* πολλαπλάσιο των $\text{ord}(g_1)$,..., $\text{ord}(g_s)$. Κατά συνέπειαν, το *ελάχιστο* κοινό πολλαπλάσιο των $\text{ord}(g_1)$,..., $\text{ord}(g_s)$ είναι ο ελάχιστος φυσικός αριθμός που πληροί την ανωτέρω συνθήκη.

[20] Βλ. K. Bauer, D. Sen & P. Zvengrowski: *A generalized Goursat Lemma*, arXiv:1109.0024, preprint, 2011.

(ii) Εάν $i_0 \in \{1,...,s\}$ με $\text{ord}(g_{i_0}) = \infty$, τότε $g_{i_0}^k \neq e_{G_{i_0}}$ για κάθε $k \in \mathbb{N}$, οπότε

$$(g_1,...,g_{i_0},...,g_s)^k = (g_1^k,...,g_{i_0}^k,...,g_s^k) \neq (e_{G_1},...,e_{G_{i_0}},...,e_{G_s}),$$

για κάθε $k \in \mathbb{N}$. Αυτό σημαίνει ότι $\text{ord}((g_1,...,g_s)) = \infty$. □

7.1.60 Παράδειγμα. Εάν $s \in \mathbb{N}$, $s \geq 2$, και εάν οι $m_1,...,m_s$ είναι s φυσικοί αριθμοί, τότε δυνάμει τού πορίσματος 2.3.14 η τάξη οιουδήποτε στοιχείου

$$([a_1]_{m_1},...,[a_s]_{m_s}) \in \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s}$$

ισούται με $\text{ord}(([a_1]_{m_1},...,[a_s]_{m_s})) = \text{εκπ}\Big(\frac{m_1}{\text{μκδ}(m_1,a_1)},...,\frac{m_s}{\text{μκδ}(m_s,a_s)}\Big)$.

7.1.61 Θεώρημα. *Έστω ότι $s \in \mathbb{N}$, $s \geq 2$, και ότι οι $G_1,...,G_s$ είναι s πεπερασμένες ομάδες. Τότε*

$$\exp(\prod_{j=1}^{s} G_j) = \text{εκπ}(\exp(G_1),...,\exp(G_s)). \tag{7.23}$$

ΑΠΟΔΕΙΞΗ. Θέτουμε $r_j := \exp(G_j),\ \forall j \in \{1,...,s\}$. Εάν $s = 2$, τότε

$$G_1 \cong G_1 \times \{e_{G_2}\} \sqsubseteq G_1 \times G_2,\ \ G_2 \cong \{e_{G_1}\} \times G_2 \sqsubseteq G_1 \times G_2$$

και $\text{εκπ}(r_1,r_2) = r_1t_1 = r_2t_2$ για κάποιους $t_1,t_2 \in \mathbb{N}$. Το 2.3.25 (iii) δίδει

$$\left.\begin{array}{l} r_1 = \exp(G_1 \times \{e_{G_2}\}) \mid \exp(G_1 \times G_2) \\ r_2 = \exp(\{e_{G_1}\} \times G_2) \mid \exp(G_1 \times G_2) \end{array}\right\} \underset{\text{B.2.25}}{\Longrightarrow} \text{εκπ}(r_1,r_2) \mid \exp(G_1 \times G_2),$$

οπότε $\text{εκπ}(r_1,r_2) \leq \exp(G_1 \times G_2)$. Εξάλλου, για *οιοδήποτε* $(g_1,g_2) \in G_1 \times G_2$ λαμβάνουμε

$$(g_1,g_2)^{\text{εκπ}(r_1,r_2)} = ((g_1^{r_1})^{t_1},(g_2^{r_2})^{t_2}) = (e_{G_1}^{t_1},e_{G_2}^{t_2}) = (e_{G_1},e_{G_2}) = e_{G_1 \times G_2}$$

και από τον ορισμό 2.3.24 τού εκθέτη έπεται ότι $\exp(G_1 \times G_2) \leq \text{εκπ}(r_1,r_2)$. Κατά συνέπειαν, $\exp(G_1 \times G_2) = \text{εκπ}(r_1,r_2)$. Εάν $s \geq 3$, τότε χρησιμοποιούμε μαθηματική επαγωγή ως προς το s. Υποθέτουμε ότι η ισότητα (7.23) είναι αληθής για το εξωτερικό ευθύ γινόμενο $s-1$ πεπερασμένων ομάδων. Προφανώς,

$$\begin{aligned} \exp(\prod_{j=1}^{s} G_j) &= \exp(G_1 \times (\prod_{j=2}^{s} G_j)) = \text{εκπ}(r_1,\exp(\prod_{j=2}^{s} G_j)) \\ &= \text{εκπ}(r_1,\text{εκπ}(r_2,...,r_s)) = \text{εκπ}(r_1,r_2,...,r_s), \end{aligned}$$

όπου η δεύτερη ισότητα προκύπτει από ό,τι είχαμε αποδείξει στην περίπτωση δύο παραγόντων, η τρίτη από την επαγωγική μας υπόθεση και η τέταρτη από την πρόταση Β.2.27. Άρα η (7.23) είναι αληθής και για s παράγοντες, για *κάθε* $s \geq 2$. □

► **Περί τής «κυκλικότητας» τής $\prod_{j=1}^{s} G_j$.** Βάσει τού 7.1.57 (ii) η $\prod_{j=1}^{s} G_j$ είναι αβελιανή *εάν και μόνον εάν* η G_j είναι αβελιανή για κάθε $j \in \{1,...,s\}$. Κατ' αναλογίαν, εάν η $\prod_{j=1}^{s} G_j$ είναι κυκλική, τότε και η G_j είναι κυκλική ομάδα για κάθε $j \in \{1,...,s\}$. Ωστόσο, εάν οι G_j, $j \in \{1,...,s\}$, είναι κυκλικές ομάδες, τότε η $\prod_{j=1}^{s} G_j$ *δεν είναι κατ' ανάγκην κυκλική*, εκτός κι αν πληρούνται κάποιες *επιπρόσθετες συνθήκες* (βλ. τα θεωρήματα 7.1.64 και 7.1.69, και το πόρισμα 7.1.70).

7.1.62 Θεώρημα. *Εάν $s \in \mathbb{N}$, $s \geq 2$, και εάν οι $m_1, m_2,..., m_s$ είναι s σχετικώς πρώτοι ανά δύο φυσικοί αριθμοί, τότε*

$$\boxed{\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s},}$$

όπου $m := m_1 m_2 \cdots m_s$.

ΑΠΟΔΕΙΞΗ. Θεωρούμε την

$$f : \mathbb{Z}_m \longrightarrow \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s},\ [a]_m \longmapsto f([a]_m) := ([a]_{m_1}, [a]_{m_2},..., [a]_{m_s}).$$

Προφανώς, για οιουσδήποτε $a, b \in \mathbb{Z}$ ισχύουν οι αμφίπλευρες συνεπαγωγές

$$[a]_m = [b]_m \Leftrightarrow a \equiv b (\mathrm{mod}\, m) \Leftrightarrow m \mid a - b \underset{\text{B.4.9}}{\Longleftrightarrow} (m_j \mid a - b,\ \ \forall j \in \{1,..., s\})$$

$$\Leftrightarrow \Big([a]_{m_j} = [b]_{m_j},\ \ \forall j \in \{1,..., s\}\Big) \Leftrightarrow f([a]_m) = f([b]_m).$$

Ακολουθώντας αυτές προς τη (δεξιά) κατεύθυνση "$\Rightarrow$" διαπιστώνουμε ότι η θεωρηθείσα f είναι μια καλώς ορισμένη απεικόνιση. Ακολουθώντας τες προς την (αριστερή) κατεύθυνση "$\Leftarrow$" συμπεραίνουμε ότι η f είναι ενριπτική απεικόνιση. Επειδή $|\mathbb{Z}_m| = m = m_1 m_2 \cdots m_s = |\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s}|$, η f, ως ενριπτική απεικόνιση μεταξύ ισοπληθικών πεπερασμένων συνόλων, είναι επιριπτική και, κατ' επέκταση, αμφιριπτική. Επιπροσθέτως, επειδή για οιουσδήποτε $a, b \in \mathbb{Z}$ έχουμε

$$\begin{aligned} &f([a]_m + [b]_m) = f([a+b]_m) = ([a+b]_{m_1}, [a+b]_{m_2},..., [a+b]_{m_s}) \\ &= ([a]_{m_1} + [b]_{m_1}, [a]_{m_2} + [b]_{m_2},..., [a]_{m_s} + [b]_{m_s}) \\ &= ([a]_{m_1}, [a]_{m_2},..., [a]_{m_s}) + ([b]_{m_1}, [b]_{m_2},..., [b]_{m_s}) = f([a]_m) + f([b]_m), \end{aligned}$$

η f είναι ομομορφισμός (προσθετικών) ομάδων και, βάσει των προαναφερθέντων, ισομορφισμός. □

7.1.63 Πόρισμα. *Έστω $n = p_1^{\nu_1} p_2^{\nu_2} \cdots p_\kappa^{\nu_\kappa}$, $\kappa \in \mathbb{N}$, η κανονική παράσταση* (B.19) *ενός φυσικού αριθμού $n \geq 2$ ως γινομένου (δυνάμεων) πρώτων αριθμών $p_1,..., p_\kappa$ με $p_1 < \cdots < p_\kappa$ (όταν $\kappa \geq 2$) και $\nu_1,..., \nu_\kappa \in \mathbb{N}$. Τότε*

$$\boxed{\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\nu_1}} \oplus \mathbb{Z}_{p_2^{\nu_2}} \oplus \cdots \oplus \mathbb{Z}_{p_\kappa^{\nu_\kappa}}.}$$

7.1.64 Θεώρημα. *Εάν $s \in \mathbb{N}$, $s \geq 2$, και εάν οι $G_1, G_2,..., G_s$ είναι s πεπερασμένες κυκλικές ομάδες, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Η ομάδα $G := G_1 \times G_2 \times \cdots \times G_s$ είναι κυκλική.*

(ii) μκδ $(|G_i|, |G_j|) = 1$ *για οιουσδήποτε $i, j \in \{1, ..., s\}, i \neq j$.*

ΑΠΟΔΕΙΞΗ. Έστω ότι $|G_j| =: m_j \in \mathbb{N}$ για κάθε $j \in \{1, ..., s\}$.

(ii)$\Rightarrow$(i) Εάν μκδ$(m_i, m_j) = 1$ για οιουσδήποτε $i, j \in \{1, ..., s\}$, $i \neq j$, τότε το (ii) τού θεωρήματος 2.4.23, το (v) τής προτάσεως 7.1.55 και το θεώρημα 7.1.62 μας πληροφορούν ότι

$$G := G_1 \times G_2 \times \cdots \times G_s \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s} \cong \mathbb{Z}_m,$$

όπου $m := m_1 m_2 \cdots m_s$, ήτοι ότι η G είναι κυκλική τάξεως m.

(i)⇒(ii) Εάν η G είναι κυκλική και εάν υποθέσουμε ότι $\exists i, j \in \{1, ..., s\}$, $i \neq j$, με $d := \text{μκδ}(m_i, m_j) > 1$, τότε, σύμφωνα με το (ii) τού θεωρήματος 2.3.21, υπάρχει ακριβώς μία μη τετριμμένη υποομάδα H τής G_i και ακριβώς μία μη τετριμμένη υποομάδα K τής G_j με $|H| = d = |K|$. Οι υποομάδες

$$\begin{aligned} \overline{H} &:= \left\{ \left(e_{G_1}, ..., e_{G_{i-1}}, x, e_{G_{i+1}}, ..., e_{G_s}\right) \middle| \, x \in H \right\}, \\ \overline{K} &:= \left\{ \left(e_{G_1}, ..., e_{G_{j-1}}, y, e_{G_{j+1}}, ..., e_{G_s}\right) \middle| \, y \in K \right\}, \end{aligned}$$

τής G έχουν τάξη d και $\overline{H} \neq \overline{K}$. Άρα η G δεν είναι κυκλική (εκ νέου λόγω τού (ii) τού θεωρήματος 2.3.21). Άτοπο! Ως εκ τούτου, οι τάξεις $m_1, ..., m_s$ των $G_1, ..., G_s$ είναι κατ' ανάγκην σχετικώς πρώτοι ανά δύο. □

7.1.65 Πόρισμα. *Εάν $s \in \mathbb{N}$, $s \geq 2$, και εάν οι $G_1, ..., G_s$ είναι s πεπερασμένες κυκλικές ομάδες, τέτοιες ώστε η $\prod_{j=1}^{s} G_j$ να είναι ωσαύτως κυκλική, τότε για ένα στοιχείο $(g_1, ..., g_s) \in \prod_{j=1}^{s} G_j$ ισχύει η αμφίπλευρη συνεπαγωγή*:

$$\prod_{j=1}^{s} G_j = \langle (g_1, ..., g_s) \rangle \iff [G_j = \langle g_j \rangle \, , \, \forall j \in \{1, ..., s\}].$$

ΑΠΟΔΕΙΞΗ. Εάν υποθέσουμε ότι $\prod_{j=1}^{s} G_j = \langle (g_1, ..., g_s) \rangle$ και εάν θεωρήσουμε τυχόντα στοιχεία $x_1 \in G_1, ..., x_s \in G_s$, τότε υπάρχουν $k_1, ..., k_s \in \mathbb{Z}$, τέτοιοι ώστε να ισχύουν οι ισότητες

$$(g_1, ..., g_s)^{k_j} = (e_{G_1}, ..., e_{G_{j-1}}, x_j, e_{G_{j+1}}, ..., e_{G_s}), \ \forall j \in \{1, ..., s\},$$

οπότε $[x_j = g_j^{k_j}, \ \forall j \in \{1, ..., s\}] \Longrightarrow [x_j \in \langle g_j \rangle \, , \ \forall j \in \{1, ..., s\}]$ και, ως εκ τούτου, $G_j = \langle g_j \rangle \, , \ \forall j \in \{1, ..., s\}$. Και αντιστρόφως· εάν έχουμε $G_j = \langle g_j \rangle \, , \ \forall j \in \{1, ..., s\}$, τότε από την υπόθεσή μας και το θεώρημα 7.1.64 έπεται ότι $\text{μκδ}(|G_i| \, , |G_j|) = 1$ για οιουσδήποτε $i, j \in \{1, ..., s\}$, $i \neq j$. Εξ αυτού συμπεραίνουμε (μέσω τού πορίσματος B.3.19) ότι

$$\text{εκπ}(|G_1| \, , ..., |G_s|) = \prod_{j=1}^{s} |G_j| = \left| \prod_{j=1}^{s} G_j \right|. \tag{7.24}$$

Επιπροσθέτως, μέσω τού 7.1.59 (i) λαμβάνουμε

$$\text{ord}(g_1, ..., g_s) = \text{εκπ}(\text{ord}\,(g_1) \, , ..., \text{ord}\,(g_2)) = \text{εκπ}(|G_1| \, , ..., |G_s|), \tag{7.25}$$

όπου η δεύτερη ισότητα προκύπτει από την πρόταση 2.3.7. Οι (7.24) και (7.25) δίδουν $\text{ord}(g_1, ..., g_s) = \left| \prod_{j=1}^{s} G_j \right|$, οπότε εκ νέου εφαρμογή τής προτάσεως 2.3.7 μας οδηγεί στο ότι ισχύει η ισότητα $\prod_{j=1}^{s} G_j = \langle (g_1, ..., g_s) \rangle$. □

7.1.66 Πόρισμα. *Εάν οι G_1 και G_2 είναι δυο πεπερασμένες κυκλικές ομάδες, τότε ισχύουν τα εξής*:

(i) *Η* $G_1 \times G_2$ *είναι κυκλική εάν και μόνον εάν* μκδ$(|G_1|, |G_2|) = 1$.

(ii) *Εάν η* $G_1 \times G_2$ *είναι κυκλική και* $g_1 \in G_1$, $g_2 \in G_2$, *τότε*

$$G_1 \times G_2 = \langle (g_1, g_2) \rangle \Longleftrightarrow [G_1 = \langle g_1 \rangle \text{ και } G_2 = \langle g_2 \rangle].$$

7.1.67 Παράδειγμα. Κατά το (i) τού πορίσματος 7.1.66 η αβελιανή ομάδα $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ είναι μη κυκλική τάξεως 4. Επομένως, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong \mathbf{V}$ (βλ. 3.5.6 (iii)).

7.1.68 Λήμμα. *Εάν η* $(H, \cdot)$ *είναι μια μη τετριμμένη ομάδα, τότε η* $H \times \mathbb{Z}$ *είναι μη κυκλική.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι η $H \times \mathbb{Z}$ είναι κυκλική. Τότε υπάρχουν στοιχεία $a \in H \setminus \{e_H\}$ και $b \in \mathbb{Z} \setminus \{0\}$, τέτοια ώστε να ισχύει $H \times \mathbb{Z} = \langle (a, b) \rangle$. Επειδή $(a, 0) \in H \times \mathbb{Z}$, θα πρέπει να υπάρχει κάποιος $k \in \mathbb{Z}$ με

$$(a, b)^k = (a^k, kb) = (a, 0) \Rightarrow k = 0 \text{ και } a = a^0 = e_H.$$

Άτοπο (αφού εξ υποθέσεως $a \neq e_H$)! Άρα η $H \times \mathbb{Z}$ είναι όντως μη κυκλική. □

7.1.69 Θεώρημα. *Έστω ότι* $s \in \mathbb{N}$, $s \geq 2$, *και ότι οι* $G_1, G_2, ..., G_s$ *είναι* s *ομάδες. Εάν η* $G := G_1 \times \cdots \times G_s$ *είναι κυκλική, τότε ισχύουν τα ακόλουθα*:

(i) *Η* G_j *είναι κυκλική ομάδα για κάθε* $j \in \{1, ..., s\}$.

(ii) *Εάν η* G *είναι πεπερασμένη, τότε* μκδ $(|G_i|, |G_j|) = 1$ *για οιουσδήποτε δείκτες* $i, j \in \{1, ..., s\}, i \neq j$.

(iii) *Εάν η* G *είναι πεπερασμένη και* $G = \langle (g_1, ..., g_s) \rangle$, *τότε* $G_j = \langle g_j \rangle$ *για κάθε δείκτη* $j \in \{1, ..., s\}$.

(iv) *Εάν η* G *είναι άπειρη, τότε* $\exists i_0 \in \{1, ..., s\} : G_{i_0} \cong \mathbb{Z}$ *και η* G_j *είναι τετριμμένη για κάθε* $j \in \{1, ..., s\} \setminus \{i_0\}$.

ΑΠΟΔΕΙΞΗ. (i) Κατά τα 7.1.53 (i)-(ii), $G_j \cong \overline{G}_j \trianglelefteq G$, οπότε G_j είναι κυκλική ομάδα για κάθε $j \in \{1, ..., s\}$ (βλ. 2.2.19 (ii) και 2.4.19 (iii)).

(ii) Τούτο έπεται από το θεώρημα 7.1.64.

(iii) Η απόδειξη είναι πανομοιότυπη εκείνης τής συνεπαγωγής " $\Rightarrow$ " τού πορίσματος 7.1.65.

(iv) Εάν η G είναι άπειρη, τότε $\exists i_0 \in \{1, ..., s\}$, τέτοιος ώστε η G_{i_0} να είναι άπειρη (βλ. 7.1.55 (i)) και (λόγω τού (i)) κυκλική. Άρα $G_{i_0} \cong \mathbb{Z}$ (βλ. 2.4.23 (i)). Ας υποθέσουμε ότι $\nu := \text{card}(\{j \in \{1, ..., s\} \setminus \{i_0\} \mid G_j \text{ μη τετριμμένη}\})$. Προφανώς (λόγω των 7.1.55 (ii) και (iv)) $G \cong H \times \mathbb{Z}$, για κάποια ομάδα $H \cong \mathbb{Z}^\nu$. Θα αποδείξουμε ότι $\nu = 0$.

Απόδειξη πρώτη. Εάν $\nu \geq 1$, τότε η G δεν θα ήταν κυκλική επί τη βάσει τού λήμματος 7.1.68.

Απόδειξη δεύτερη. Για την ίδια την G έχουμε $G \cong \mathbb{Z}$ (βλ. 2.4.23 (i)). Επειδή η $\mathbb{Z}$ είναι αναποσυνθέσιμη (βλ. 7.1.33 (iii)), από το πόρισμα 7.1.45 συνάγεται ότι $\nu = 0$.

Απόδειξη τρίτη. Επειδή $G \cong \mathbb{Z} \cong H \times \mathbb{Z}$ με $H \cong \mathbb{Z}^\nu$, έχουμε $\mathbb{Z}/\mathbb{Z} \cong (H \times \mathbb{Z})/\overline{\mathbb{Z}} \cong \mathbb{Z}^\nu$. Όμως η $\mathbb{Z}^\nu$ είναι τετριμμένη εάν και μόνον εάν $\nu = 0$. □

7.1.70 Πόρισμα. *Έστω ότι $s \in \mathbb{N}$, $s \geq 2$, και ότι οι $G_1, G_2, ..., G_s$ είναι s κυκλικές ομάδες. Εάν η $G := G_1 \times \cdots \times G_s$ είναι άπειρη και το πλήθος των μη τετριμμένων παραγόντων της είναι ≥ 2, τότε η G είναι αβελιανή μη κυκλική.*

ΑΠΟΔΕΙΞΗ. Εάν η G ήταν κυκλική, τότε (σύμφωνα με το 7.1.69 (iv)) θα όφειλε να διαθέτει μόνον έναν μη τετριμμένο παράγοντα. □

7.1.71 Πόρισμα. (Πεπερασμένες ομάδες με εκθέτη 2.) *Κάθε πεπερασμένη ομάδα $(G, \cdot)$ έχουσα εκθέτη $\exp(G) = 2$ (βλ. 2.3.24) είναι αβελιανή άρτιας τάξεως. Επιπροσθέτως, υπάρχει $m \in \mathbb{N}$, τέτοιος ώστε να ισχύει $G \cong \underbrace{\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2}_{m \text{ φορές}}$.*

(Όταν $|G| \geq 4$, τότε η G, σύμφωνα με το (iii) τής προτάσεως 2.4.19 και το (ii) τού θεωρήματος 7.1.69, δεν είναι κυκλική.)

ΑΠΟΔΕΙΞΗ. Έστω $(G, \cdot)$ τυχούσα ομάδα με $\exp(G) = 2$. Η G είναι (προφανώς) μη τετριμμένη και $\mathrm{ord}(g) = 2, \forall g \in G \setminus \{e_G\}$. Άρα η G είναι αβελιανή. (Βλ. 2.3.9 (iv).) Παγιώνοντας κάποιο $x \in G \setminus \{e_G\}$ παρατηρούμε ότι

$$\mathrm{ord}(x) = |\langle x \rangle| = 2 \Longrightarrow |G| \equiv 0 (\mathrm{mod}\, 2).$$

Εάν $|G| = 2$, τότε $G \underset{\text{2.4.23 (ii)}}{\cong} \mathbb{Z}_2$. Εάν $|G| \geq 4$, τότε εργαζόμαστε με μαθηματική επαγωγή ως προς την τάξη $|G|$ υποθέτοντας ότι ο ισχυρισμός (περί τής υπάρξεως ενός τέτοιου ισομορφισμού) είναι αληθής για κάθε πεπερασμένη ομάδα έχουσα εκθέτη 2 και τάξη $< |G|$. Επιλέγοντας ένα $y \in G \setminus \langle x \rangle$ λαμβάνουμε

$$\langle x \rangle \cap \langle y \rangle \sqsubseteq \langle x \rangle \underset{4.1.22}{\Longrightarrow} |\langle x \rangle \cap \langle y \rangle| \mid |\langle x \rangle| = 2 \Rightarrow [\text{είτε } \langle x \rangle \cap \langle y \rangle = \{e_G\} \text{ είτε } \langle x \rangle \cap \langle y \rangle = \langle x \rangle].$$

Το δεύτερο ενδεχόμενο αποκλείεται (διότι $y \in G \setminus \langle x \rangle$), οπότε $\langle x \rangle \cap \langle y \rangle = \{e_G\}$. Έστω τώρα[21] $K \in \{H \in \mathbf{Subg}(G) : \langle x \rangle \cap H = \{e_G\}\}$, τέτοια ώστε να ισχύει

$$|K| = \max \{ |H| \,|\, H \in \mathbf{Subg}(G) : \langle x \rangle \cap H = \{e_G\} \}.$$

Επειδή η G είναι αβελιανή, έχουμε $\langle x \rangle K \sqsubseteq G$. Ας υποθέσουμε ότι $\langle x \rangle K \sqsubset G$. Επιλέγοντας ένα $z \in G \setminus \langle x \rangle K$ λαμβάνουμε $K \sqsubset \langle z \rangle K$ και

$$\begin{aligned} &\langle x \rangle K \cap \langle z \rangle \sqsubseteq \langle z \rangle \underset{4.1.22}{\Longrightarrow} |\langle x \rangle K \cap \langle z \rangle| \mid |\langle z \rangle| = 2 \\ &\Rightarrow [\text{είτε } \langle x \rangle K \cap \langle z \rangle = \{e_G\} \text{ είτε } \langle x \rangle K \cap \langle z \rangle = \langle z \rangle]. \end{aligned}$$

Το δεύτερο ενδεχόμενο αποκλείεται (διότι εξ υποθέσεως $z \in G \setminus \langle x \rangle K$), οπότε $\langle x \rangle K \cap \langle z \rangle = \{e_G\}$. Από την άλλη μεριά, κάθε $g \in \langle x \rangle \cap \langle z \rangle K$ γράφεται υπό τη μορφή $g = x^i = z^j k$ για κάποιο $k \in K$ και κάποιους $i, j \in \mathbb{Z}$. Επομένως,

$$gk^{-1} = x^i k^{-1} = z^j \in \langle x \rangle K \cap \langle z \rangle = \{e_G\} \Rightarrow g = k \in \langle x \rangle \cap K = \{e_G\} \Rightarrow g = e_G.$$

[21] Προφανώς, $\{H \in \mathbf{Subg}(G) : \langle x \rangle \cap H = \{e_G\}\} \neq \varnothing$, διότι η κυκλική υποομάδα $\langle y \rangle$ είναι στοιχείο αυτού τού συνόλου.

Αυτό σημαίνει ότι $\langle x\rangle \cap \langle z\rangle\, K = \{e_G\}$ με $|\langle z\rangle\, K| > |K|$. Άτοπο! Άρα $G = \langle x\rangle\, K$ και $\langle x\rangle \cap K = \{e_G\}$ (με $\langle x\rangle \lhd G$, $K \lhd G$, λόγω τής προτάσεως 4.2.6), οπότε

$$\left.\begin{aligned} G = \langle x\rangle \times_{\text{εσ. }} K &\underset{\text{7.1.43 (ii)}}{\cong} \langle x\rangle \times K \\ |\langle x\rangle| = 2 &\underset{\text{2.4.23 (ii)}}{\Longrightarrow} \langle x\rangle \cong \mathbb{Z}_2 \\ (\text{από επ. υπ.})\ \exists l \in \mathbb{N} : K \cong \underbrace{\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2}_{l \text{ φορές}} & \end{aligned}\right\} \underset{\text{7.1.55 (v), (iii)}}{\Longrightarrow} G \cong \underbrace{\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2}_{l+1 \text{ φορές}}.$$

Αρκεί λοιπόν να θέσουμε $m := l + 1$. □

► **Αυτομορφισμοί τής $\prod_{j=1}^{s} G_j$.** Οι γενικεύσεις των προτάσεων 7.1.16, 7.1.17 και 7.1.19 για την $\prod_{j=1}^{s} G_j$ είναι οι 7.1.72, 7.1.75 και 7.1.76, αντιστοίχως.

7.1.72 Πρόταση. *Έστω ότι $s \in \mathbb{N}$, $s \geq 2$, και ότι οι $G_1, G_2, ..., G_s$ είναι s ομάδες. Τότε η $\prod_{j=1}^{s} \mathrm{Aut}(G_j)$ είναι εμφυτεύσιμη εντός τής $\mathrm{Aut}(\prod_{j=1}^{s} G_j)$.*

ΑΠΟΔΕΙΞΗ. Πανομοιότυπη τής αποδείξεως τής προτάσεως 7.1.16. □

7.1.73 Παράδειγμα. Εάν $s = 2$ και $G_1 = G_2 = \mathbb{Z}$, τότε (λόγω τού (i) τού θεωρήματος 2.4.32 και τού (v) τής προτάσεως 7.1.55) έχουμε

$$\mathrm{Aut}(\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong \mathbf{V}.$$

Ωστόσο, η ομάδα αυτομορφισμών $\mathrm{Aut}(\mathbb{Z} \oplus \mathbb{Z})$ τής $\mathbb{Z} \oplus \mathbb{Z}$ είναι πολύ μεγαλύτερη (και μάλιστα άπειρη). Πράγματι· εάν $\vartheta \in \mathrm{Aut}(\mathbb{Z} \oplus \mathbb{Z})$ και εάν $\vartheta\,((1,0)) = (a,b)$ και $\vartheta\,((0,1)) = (c,d)$, τότε για κάθε $(m,n) \in \mathbb{Z} \oplus \mathbb{Z}$ λαμβάνουμε

$$\vartheta\,((m,n)) = m\vartheta\,((1,0)) + n\vartheta\,(0,1)) = (ma + nc, mb + nd) = (m,n)\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

οπότε ο αυτομορφισμός ϑ αναπαριστάται μέσω ενός 2×2 πίνακα με ακέραιες εγγραφές. Η ορίζουσα $ad - bc$ αυτού τού πίνακα ανήκει στο δισύνολο $\{\pm 1\}$, καθότι αυτός είναι αντιστρέψιμος. (Αλλά και ο αντίστροφός του οφείλει, με τη σειρά του, να αναπαριστάται μέσω ενός 2×2 πίνακα με ακέραιες εγγραφές.) Ως εκ τούτου, η ομάδα αυτομορφισμών $\mathrm{Aut}(\mathbb{Z} \oplus \mathbb{Z})$ είναι ισόμορφη τής ομάδας $\mathrm{GL}_2(\mathbb{Z})$ των 2×2 πινάκων με ακέραιες εγγραφές και ορίζουσα ± 1. (Βλ. D.2.20 (iii).)

7.1.74 Παράδειγμα. Εάν $s = 2$ και $G_1 = G_2 = \mathbb{Z}_p$, όπου p πρώτος αριθμός, τότε (με επιχειρήματα ανάλογα εκείνων που προαναφέρθησαν στο παράδειγμα 7.1.73) αποδεικνύεται ότι

$$\mathrm{Aut}(\mathbb{Z}_p \oplus \mathbb{Z}_p) \cong \mathrm{GL}_2(\mathbb{Z}_p).$$

Αυτή η ομάδα έχει τάξη $(p^2 - 1)(p^2 - p) = p(p+1)(p-1)^2$. Αντιθέτως, η ομάδα

$$\mathrm{Aut}(\mathbb{Z}_p) \times \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^{\times} \oplus \mathbb{Z}_p^{\times}$$

έχει τάξη $(p-1)^2$. (Βλ. 2.4.32 (ii) και 7.1.55 (v).)

7.1.75 Πρόταση. *Έστω ότι* $s \in \mathbb{N}$, $s \geq 2$, *και ότι οι* $G_1, G_2, ..., G_s$ *είναι* s *ομάδες, τέτοιες ώστε* $\overline{G_i} := \mathrm{Im}(\iota_i) \sqsubseteq_{\chi\alpha\varrho.} \prod_{j=1}^{s} G_j$, $\forall i \in \{1, ..., s\}$. *Τότε*

$$\boxed{\prod_{j=1}^{s} \mathrm{Aut}(G_j) \cong \mathrm{Aut}(\prod_{j=1}^{s} G_j).}$$

ΑΠΟΔΕΙΞΗ. Πανομοιότυπη τής αποδείξεως τής προτάσεως 7.1.17. □

7.1.76 Πρόταση. *Έστω ότι* $s \in \mathbb{N}$, $s \geq 2$, *και ότι οι* $G_1, G_2, ..., G_s$ *είναι* s *πεπερασμένες ομάδες, για τις τάξεις των οποίων ισχύει* $\mu\kappa\delta\left(|G_i|, |G_j|\right) = 1$ *για οιουσδήποτε δείκτες* $i, j \in \{1, ..., s\}, i \neq j$. *Τότε*

$$\boxed{\prod_{j=1}^{s} \mathrm{Aut}(G_j) \cong \mathrm{Aut}(\prod_{j=1}^{s} G_j).}$$

ΑΠΟΔΕΙΞΗ. Θα εργασθούμε με τη βοήθεια τής μαθηματικής επαγωγής ως προς τον αριθμό s των παραγόντων. Για $s = 2$ ο ισχυρισμός είναι αληθής επί τη βάσει τής προτάσεως 7.1.19. Ας υποθέσουμε ότι είναι αληθής και για το εξωτερικό γινόμενο $s-1$ ομάδων, για κάποιον $s \geq 3$. Τότε (επί τη βάσει των (iii) και (v) τής προτάσεως 7.1.55 και τής επαγωγικής υποθέσεώς μας)

$$\textstyle\prod_{j=1}^{s} \mathrm{Aut}(G_j) \cong (\prod_{j=1}^{s-1} \mathrm{Aut}(G_j)) \times \mathrm{Aut}(G_s) \cong (\mathrm{Aut}(\prod_{j=1}^{s-1} G_j)) \times \mathrm{Aut}(G_s).$$

Δυνάμει τής προτάσεως B.3.17 λαμβάνουμε

$$\mu\kappa\delta\left(\left|\textstyle\prod_{j=1}^{s-1} G_j\right|, |G_s|\right) = \mu\kappa\delta(\prod_{j=1}^{s-1} |G_j|, |G_s|) = \prod_{j=1}^{s-1} \mu\kappa\delta(|G_j|, |G_s|) = 1,$$

οπότε ο ισχυρισμός είναι αληθής (εκ νέου λόγω τής προτάσεως 7.1.19, εφαρμοζόμενης για τις $\prod_{j=1}^{s-1} G_j$ και G_s) *και* για το εξωτερικό γινόμενο s ομάδων. □

Το θεώρημα 7.1.20 γενικεύεται για s πεπερασμένες ομάδες ως εξής[22]:

7.1.77 Θεώρημα. (J.N.S. Bidwell, 2008) *Έστω ότι* $s \in \mathbb{N}$, $s \geq 2$, *και ότι οι* $G_1, G_2, ..., G_s$ *είναι* s *πεπερασμένες ομάδες. Εάν οι* G_i *και* G_j *δεν διαθέτουν κοινούς ευθείς παράγοντες για οιουσδήποτε δείκτες* $i, j \in \{1, ..., s\}, i \neq j$, *τότε*

$$\boxed{\mathrm{Aut}(\prod_{j=1}^{s} G_j) \cong \mathcal{A}\,,}$$

όπου το

$$\mathcal{A} := \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1s} \\ \vdots & \ddots & \vdots \\ a_{s1} & \cdots & a_{ss} \end{pmatrix} \middle| a_{ij} \in \begin{cases} \mathrm{Aut}(G_i), & \text{όταν } i = j \\ \mathrm{Hom}(G_j, Z(G_i)), & \text{όταν } i \neq j \end{cases} \right\}$$

είναι εφοδιασμένο με τη δομή ομάδας μέσω «πολλαπλασιασμού πινάκων».

[22] J.N.S. Bidwell: *Automorphisms of direct products of finite groups II*, Archiv der Math. (Basel) **91** (2008), 111-121.

► **«Εσωτερικό» ευθύ γινόμενο με πεπερασμένο πλήθος παραγόντων**. Η πρόταση 7.1.53 δρα ως κίνητρο για τη θέσπιση τού ακόλουθου ορισμού:

7.1.78 Ορισμός. Έστω ότι $s \in \mathbb{N}$, $s \geq 2$, και ότι οι $H_1,...,H_s$ είναι s υποομάδες μιας ομάδας $(G,\cdot)$. Λέμε ότι η G είναι το **εσωτερικό ευθύ γινόμενο των υποομάδων** $H_1,...,H_s$ (και γράφουμε[23] $G = \prod_{j=1}^{s}{}^{\text{εσ.}} H_j$ ή $G = H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_s$) όταν πληρούνται οι ακόλουθες συνθήκες:

(i) $H_i \trianglelefteq G, \forall i \in \{1,...,s\}$,

(ii) $G = H_1H_2\cdots H_s$, και

(iii) $H_i \cap (H_1\cdots H_{i-1}H_{i+1}\cdots H_s) = \{e_G\}$, $\forall i \in \{1,...,s\}$, όπου στην περίπτωση κατά την οποία $i = 1$ (και αντιστοίχως, $i = s$) το $H_1\cdots H_{i-1}H_{i+1}\cdots H_s$ αντικαθίσταται με το $H_2\cdots H_s$ (και αντιστοίχως, με το $H_1\cdots H_{s-1}$).

7.1.79 Θεώρημα. *Έστω ότι $s \in \mathbb{N}$, $s \geq 2$, και ότι οι $H_1,...,H_s$ είναι s υποομάδες μιας ομάδας $(G,\cdot)$. Τότε τα* (a) *και* (b) *είναι ισοδύναμα*:

(a) $H_i \trianglelefteq G, \forall i \in \{1,...,s\}$, *και* $G = \prod_{j=1}^{s}{}^{\text{εσ.}} H_j$.

(b) *Για τις $H_1,...,H_s$ ισχύουν τα ακόλουθα*:

(i) *Εάν $x_i \in H_i$, $x_j \in H_j$, για $i,j \in \{1,...,s\}$, $i \neq j$, τότε $x_ix_j = x_jx_i$.*

(ii) *Κάθε στοιχείο $g \in G$ γράφεται μονοσημάντως υπό τη μορφή $g = x_1x_2\cdots x_s$, όπου $x_i \in H_i$ για κάθε $i \in \{1,...,s\}$.*

ΑΠΟΔΕΙΞΗ. (a)⇒(b) Εάν $H_i \trianglelefteq G$, $\forall i \in \{1,...,s\}$, και $G = \prod_{j=1}^{s}{}^{\text{εσ.}} H_j$, τότε για οιαδήποτε στοιχεία $x_i \in H_i$, $x_j \in H_j$, $i,j \in \{1,...,s\}$, $i \neq j$, έχουμε

$$\left.\begin{array}{r} H_j \ni (\underbrace{x_ix_jx_i^{-1}}_{\in H_j})x_j^{-1} = x_i(\underbrace{x_jx_i^{-1}x_j^{-1}}_{\in H_i}) \in H_i \\ \text{7.1.78 (iii)} \Rightarrow H_i \cap (H_1\cdots H_{i-1}H_{i+1}\cdots H_s) = \{e_G\} \end{array}\right\} \Rightarrow x_ix_jx_i^{-1}x_j^{-1} = e_G,$$

απ' όπου έπεται το (i), ήτοι ότι $x_ix_j = x_jx_i$. Έστω τώρα τυχόν στοιχείο $g \in G$. Επειδή εξ ορισμού $G = H_1H_2\cdots H_s$ (βλ. 7.1.78 (ii)), το g γράφεται υπό τη μορφή $g = x_1x_2\cdots x_s$, όπου $x_i \in H_i$ για κάθε $i \in \{1,...,s\}$. Για την απόδειξη τού (ii) αρκεί να ελεγχθεί ότι η εν λόγω έκφραση τού g είναι μοναδική. Προς τούτο υποθέτουμε ότι $g = y_1y_2\cdots y_s$, όπου $y_i \in H_i$ για κάθε $i \in \{1,...,s\}$. Προφανώς, λόγω τού (i) έχουμε για κάθε $i \in \{1,...,s\}$

$$\left.\begin{array}{r} y_i^{-1}x_i = \left(x_1^{-1}y_1\right)\cdots\left(x_{i-1}^{-1}y_{i-1}\right)\left(x_{i+1}^{-1}y_{i+1}\right)\cdots\left(x_s^{-1}y_s\right) \\ \text{7.1.78 (iii)} \Rightarrow H_i \cap (H_1\cdots H_{i-1}H_{i+1}\cdots H_s) = \{e_G\} \end{array}\right\} \Rightarrow x_i = y_i,\ \forall i \in \{1,...,s\}.$$

[23] Στην περίπτωση κατά την οποία χρησιμοποιούμε τον *προσθετικό συμβολισμό* για την πράξη τής ομάδας G, γράφουμε $G = \bigoplus_{j=1}^{s}{}^{\text{εσ.}} H_j$ αντί τού $G = \prod_{j=1}^{s}{}^{\text{εσ.}} H_j$ και το ονομάζουμε **εσωτερικό ευθύ άθροισμα των** $H_1,...,H_s$.

(b)⇒(a) Έστω ότι ισχύουν τα (i) και (ii) και έστω τυχόν στοιχείο $g \in G$. Κατά το (ii) το g γράφεται υπό τη μορφή $g = x_1x_2\cdots x_s$, όπου $x_i \in H_i$ για κάθε δείκτη $i \in \{1,...,s\}$. Επομένως, για οιοδήποτε $a \in H_i$ έχουμε (μέσω τού (i))

$$\begin{aligned}
&gag^{-1} = (x_1x_2\cdots x_s)\,a\,(x_1x_2\cdots x_s)^{-1} = x_1x_2\cdots\left(x_sax_s^{-1}\right)\cdots x_2^{-1}x_1^{-1}\\
&= x_1x_2\cdots\left(x_sx_s^{-1}a\right)\cdots x_2^{-1}x_1^{-1} = x_1x_2\cdots\left(x_{s-1}ax_{s-1}^{-1}\right)\cdots x_2^{-1}x_1^{-1}\\
&= x_1x_2\cdots\left(x_{s-1}x_{s-1}^{-1}a\right)\cdots x_2^{-1}x_1^{-1} = x_1x_2\cdots\left(x_{i+1}ax_{i+1}^{-1}\right)\cdots x_2^{-1}x_1^{-1}\\
&= x_1x_2\cdots\left(x_{i+1}x_{i+1}^{-1}a\right)\cdots x_2^{-1}x_1^{-1} = (x_1x_2\cdots x_{i-1})\,x_iax_i^{-1}\left(x_{i-1}^{-1}\cdots x_2^{-1}x_1^{-1}\right)\\
&= x_i\,(x_1x_2\cdots x_{i-1})\,a\left(x_{i-1}^{-1}\cdots x_2^{-1}x_1^{-1}\right)x_i^{-1}\\
&= x_i\,(x_1x_2\cdots x_{i-2})\,x_{i-1}ax_{i-1}^{-1}\left(x_{i-2}^{-1}\cdots x_2^{-1}x_1^{-1}\right)x_i^{-1}\\
&= x_i\,(x_1x_2\cdots x_{i-2})\,x_{i-1}ax_{i-1}^{-1}\left(x_{i-2}^{-1}\cdots x_2^{-1}x_1^{-1}\right)x_i^{-1}\\
&= x_i\,(x_1x_2\cdots x_{i-2})\left(x_{i-1}x_{i-1}^{-1}a\right)\left(x_{i-2}^{-1}\cdots x_2^{-1}x_1^{-1}\right)x_i^{-1}\\
&= \cdots = x_iax_i^{-1} \in H_i \Rightarrow H_i \trianglelefteq G,\ \forall i \in \{1,...,s\}.
\end{aligned}$$

Επιπροσθέτως, από το (ii) έπεται άμεσα η ισότητα $G = H_1H_2\cdots H_s$. Τέλος, εάν $g \in H_i \cap (H_1\cdots H_{i-1}H_{i+1}\cdots H_s)$ για κάποιον $i \in \{1,...,s\}$, τότε υπάρχουν

$$x_1 \in H_1,...,x_{i-1} \in H_{i-1}, x_{i+1} \in H_{i+1},...,x_s \in H_s : g = x_1\cdots x_{i-1}x_{i+1}\cdots x_s,$$

οπότε

$$\left.\begin{aligned} g &= x_1\cdots x_{i-1}e_Gx_{i+1}\cdots x_s\\ g &= e_G\cdots e_Gge_G\cdots e_G \end{aligned}\right\} \underset{\text{(ii)}}{\Longrightarrow} g = e_G \Rightarrow H_i \cap (H_1\cdots H_{i-1}H_{i+1}\cdots H_s) = \{e_G\}.$$

Άρα $G = \prod_{j=1}^{s}{}^{\text{εσ.}}\, H_j$. □

7.1.80 Παρατήρηση. Εάν $G = \prod_{j=1}^{s}{}^{\text{εσ.}}\, H_j$, τότε $G = \prod_{j=1}^{s}{}^{\text{εσ.}}\, H_{\sigma(j)}$, $\forall \sigma \in \mathfrak{S}_s$.

7.1.81 Πόρισμα. *Έστω ότι $s \in \mathbb{N}$, $s \geq 2$, και ότι οι $H_1,...,H_s$ είναι s υποομάδες μιας ομάδας $(G,\cdot)$. Τότε τα* (a) *και* (b) *είναι ισοδύναμα*:

(a) $H_i \trianglelefteq G$, $\forall i \in \{1,...,s\}$, *και* $G = \prod_{j=1}^{s}{}^{\text{εσ.}}\, H_j$.

(b) *Για τις $H_1,...,H_s$ ισχύουν τα ακόλουθα*:

(i) $H_i \trianglelefteq G$, $\forall i \in \{1,...,s\}$,

(ii) $G = H_1H_2\cdots H_s$, *και*

(iii) $H_i \cap (H_1\cdots H_{i-1}) = \{e_G\}$, $\forall i \in \{2,...,s\}$.

ΑΠΟΔΕΙΞΗ. (a)⇒(b) Τούτο έπεται άμεσα από τον ορισμό 7.1.78.

(b)⇒(a) Αρκεί να αποδειχθεί ότι από τις οι συνθήκες (b) (i)-(iii) έπονται οι συνθήκες (b) (i)-(ii) τού θεωρήματος 7.1.79. Επειδή $H_i \trianglelefteq G$, $\forall i \in \{1,...,s\}$, για οιαδήποτε στοιχεία $x_i \in H_i$, $x_j \in H_j$, $i,j \in \{1,...,s\}$, $i > j$, έχουμε

$$\left.\begin{array}{r} H_j \ni (\underbrace{x_i x_j x_i^{-1}}_{\in H_j}) x_j^{-1} = x_i (\underbrace{x_j x_i^{-1} x_j^{-1}}_{\in H_i}) \in H_i \\ H_i \cap (H_1 \cdots H_{i-1}) = \{e_G\} \end{array}\right\} \Rightarrow x_i x_j x_i^{-1} x_j^{-1} = e_G,$$

απ' όπου έπεται ότι $x_i x_j = x_j x_i$. (Εάν $i < j$, τότε καταλήγουμε στο ίδιο συμπέρασμα εναλλάσσοντας τους ρόλους των δεικτών i και j.) Επειδή $G = H_1 H_2 \cdots H_s$, κάθε $g \in G$ γράφεται υπό τη μορφή $g = x_1 x_2 \cdots x_s$, όπου $x_i \in H_i$ για κάθε $i \in \{1,...,s\}$. Απομένει να δείξουμε ότι η έκφραση αυτή είναι *μοναδική*. Προς τούτο υποθέτουμε ότι για κάποιο $g \in G$

$$g = x_1 x_2 \cdots x_s = y_1 y_2 \cdots y_s,$$

όπου $x_i, y_i \in H_i$ για κάθε $i \in \{1,...,s\}$. Εάν υπήρχε $i_0 \in \{2,...,s\}$, τέτοιο ώστε

$$x_{i_0} \neq y_{i_0} \text{ και } x_j = y_j,\ \forall j \in \{i_0+1,...,s\},$$

τότε (λόγω τής ισχύος τού 7.1.79 (b) (i)) θα είχαμε

$$y_{i_0}{}^{-1} x_{i_0} = \left(x_1^{-1} y_1\right) \cdots \left(x_{i_0-1}^{-1} y_{i_0-1}\right) \underset{\text{(iii)}}{\Longrightarrow} y_{i_0}{}^{-1} x_{i_0} = e_G \Rightarrow x_{i_0} = y_{i_0}.$$

Άτοπο! Άρα η ανωτέρω έκφραση είναι όντως μοναδική. □

7.1.82 Πόρισμα. *Έστω ότι $s \in \mathbb{N}$, $s \geq 2$, και ότι οι $H_1,...,H_s$ είναι s ορθόθετες υποομάδες μιας ομάδας $(G,\cdot)$, τέτοιες ώστε να ισχύει $G = H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_s$. Τότε $Z(G) = Z(H_1) \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} Z(H_s)$.*

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς παρατηρούμε ότι $Z(H_j) \trianglelefteq Z(G)$, $\forall j \in \{1,...,r\}$, καθόσον για κάθε $x \in Z(G)$ και $z \in Z(H_j)$ έχουμε $xzx^{-1} \in Z(H_j)$, αφού για κάθε $y \in H_j$ ισχύουν οι ισότητες

$$\begin{aligned} y(xzx^{-1}) &= y \underbrace{x}_{\in Z(G)} \left(zx^{-1}\right) = y\left(zx^{-1}\right)x = y \underbrace{z}_{\in Z(H_j)} \\ &= zy = \underbrace{x^{-1}}_{\in Z(G)} (xz)y = (xzx^{-1})y. \end{aligned}$$

Επίσης, για κάθε $i \in \{2,...,s\}$, $Z(H_i) \cap (Z(H_1) \cdots Z(H_{i-1})) = \{e_G\}$, διότι

$$Z(H_i) \cap (Z(H_1) \cdots Z(H_{i-1})) \subseteq H_i \cap (H_1 \cdots H_{i-1}) = \{e_G\}.$$

Έστω τυχόν στοιχείο $g \in G$. Επειδή ισχύει $G = H_1 H_2 \cdots H_s$, το g γράφεται υπό τη μορφή $g = x_1 x_2 \cdots x_s$, όπου $x_i \in H_i$ για κάθε $i \in \{1,...,s\}$. Εάν $z_1 \in Z(H_1) \trianglelefteq H_1$,

..., $z_s \in Z(H_s) \trianglelefteq H_s$, τότε $z_i x_j = x_j z_i$, για οιουσδήποτε $i, j \in \{1, ..., s\}$, $i \neq j$, οπότε

$$g(z_1 z_2 \cdots z_s)g^{-1} = (x_1 x_2 \cdots x_s)(z_1 z_2 \cdots z_s)g^{-1} = (x_1 \cdots x_{s-1})(z_1 x_s)(z_2 \cdots z_s)g^{-1}$$
$$= (x_1 \cdots z_1 x_{s-1} x_s)(z_2 \cdots z_s)g^{-1} = \cdots = (z_1 x_1 \cdots x_{s-1} x_s)(z_2 \cdots z_s)g^{-1}$$
$$= \cdots = (z_1 z_2)g(z_3 \cdots z_s)g^{-1} = \cdots = (z_1 z_2 \cdots z_s)gg^{-1} = z_1 z_2 \cdots z_s,$$

απ' όπου προκύπτει ότι $z_1 z_2 \cdots z_s \in Z(G) \Rightarrow Z(H_1) \cdots Z(H_s) \subseteq Z(G)$. Και αντιστρόφως· εάν $z \in Z(G) \trianglelefteq G = H_1 H_2 \cdots H_s$, τότε το z γράφεται υπό τη μορφή $z = h_1 h_2 \cdots h_s$, όπου $h_i \in H_i$ για κάθε $i \in \{1, ..., s\}$. Έστω τυχόν $x_1 \in H_1$. Επειδή $h_j^{-1} \in H_j \Rightarrow x_1 h_j^{-1} = h_j^{-1} x_1$ για κάθε $j \in \{2, ..., s\}$, έχουμε

$$x_1 h_1 = x_1 z h_s^{-1} h_{s-1}^{-1} \cdots h_2^{-1} = z x_1 h_s^{-1} h_{s-1}^{-1} \cdots h_2^{-1} = z h_s^{-1} x_1 h_{s-1}^{-1} \cdots h_2^{-1}$$
$$= z h_s^{-1} h_{s-1}^{-1} x_1 \cdots h_2^{-1} = \cdots = z h_s^{-1} h_{s-1}^{-1} \cdots h_2^{-1} x_1 = h_1 x_1,$$

οπότε $h_1 \in Z(H_1)$. Παρομοίως αποδεικνύεται ότι $h_2 \in Z(H_2), ..., h_s \in Z(H_s)$, απ' όπου προκύπτει ότι $z \in Z(H_1) \cdots Z(H_s)$, ήτοι ότι ισχύει και ο αντίστροφος εγκλεισμός $Z(G) \subseteq Z(H_1) \cdots Z(H_s)$. Τελικώς λοιπόν ο ισχυρισμός είναι αληθής επί τη βάσει τής συνεπαγωγής (b)⇒(a) τού πορίσματος 7.1.81. □

7.1.83 Πόρισμα. *Έστω ότι $s \in \mathbb{N}$, $s \geq 2$, και ότι οι H_1,..., H_s είναι s ορθόθετες υποομάδες μιας ομάδας $(G, \cdot)$, τέτοιες ώστε να ισχύει $G = H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_s$. Τότε $G' = H_1' \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_s'$.*

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς θα αποδείξουμε ότι $H_i' \trianglelefteq G'$ για κάθε $i \in \{1, ..., r\}$. Έστω $i \in \{1, ..., r\}$ και έστω $t_i = [x_i, y_i]$ ο μεταθέτης τυχόντων στοιχείων $x_i, y_i \in H_i$. Για τον μεταθέτη $g = [u, w]$ οιωνδήποτε στοιχείων $u, w \in G$ ισχύει

$$g t_i g^{-1} = [u, w][x_i, y_i][u, w]^{-1} = [u, w][x_i, y_i][w, u]. \tag{7.26}$$

Επειδή $u = h_1 h_2 \cdots h_s, w = \hat{h}_1 \hat{h}_2 \cdots \hat{h}_s$ για κάποια μονοσημάντως ορισμένα $h_1, \hat{h}_1 \in H_1, ..., h_s, \hat{h}_s \in H_s$, έχουμε[24]

$$[u, w] = [h_1 h_2 \cdots h_s, \hat{h}_1 \hat{h}_2 \cdots \hat{h}_s] = [h_1, \hat{h}_1][h_2, \hat{h}_2] \cdots [h_s, \hat{h}_s], \tag{7.27}$$

οπότε οι (7.26) και (7.27) δίδουν

$$g t_i g^{-1} = \left(\prod_{j=1}^{s} \underbrace{[h_j, \hat{h}_j]}_{\in H_j} \right) [x_i, y_i] \left(\prod_{j=1}^{s} \underbrace{[\hat{h}_j, h_j]}_{\in H_j} \right)$$
$$= \left(\prod_{j \in \{1,...,s\} \setminus \{i\}}^{s} [h_j, \hat{h}_j] \right) \underbrace{[h_i, \hat{h}_i][x_i, y_i][\hat{h}_i, h_i]}_{\in H_i} \left(\prod_{j \in \{1,...,s\} \setminus \{i\}}^{s} [\hat{h}_j, h_j] \right)$$
$$= \left(\prod_{j \in \{1,...,s\} \setminus \{i\}}^{s} [h_j, \hat{h}_j] \right) \left(\prod_{j \in \{1,...,s\} \setminus \{i\}}^{s} [\hat{h}_j, h_j] \right) [h_i, \hat{h}_i][x_i, y_i][\hat{h}_i, h_i]$$
$$= [h_i, \hat{h}_i][x_i, y_i][\hat{h}_i, h_i] \in H_i'.$$

[24] Η δεύτερη ισότητα αποδεικνύεται επαγωγικώς λαμβάνοντας υπ' όψιν την ιδιότητα (b) (i) τού θεωρήματος 7.1.79 για τις H_1,..., H_s.

Γενικότερα, για κάθε $\widetilde{g} := g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_\nu^{\varepsilon_\nu} \in G'$, όπου $\nu \in \mathbb{N}$, $\varepsilon_1, ..., \varepsilon_\nu \in \mathbb{Z}$, και $g_1, ..., g_\nu$ μεταθέτες στοιχείων τής G,

$$g_k = \prod_{j=1}^{s} [h_j^{(k)}, \hat{h}_j^{(k)}],\ \forall k \in \{1, ..., \nu\},$$

($h_1^{(k)}, \hat{h}_1^{(k)} \in H_1, ..., h_s^{(k)}, \hat{h}_s^{(k)} \in H_s$), λαμβάνουμε

$$\widetilde{g} t_i \widetilde{g}^{-1} = \prod_{k=1}^{\nu} [h_i^{(k)}, \hat{h}_i^{(k)}]^{\varepsilon_k} [x_i, y_i] [\hat{h}_i^{(k)}, h_i^{(k)}]^{\varepsilon_k} \in H_i'$$

και, κατ' επέκταση, για κάθε $\widetilde{t_i} := \prod_{l=1}^{\xi} [x_i^{(l)}, y_i^{(l)}]^{\delta_l} \in H_i'$ (όπου $\xi \in \mathbb{N}$, $\delta_1, ..., \delta_\xi \in \mathbb{Z}$),

$$\widetilde{g}\, \widetilde{t_i}\, \widetilde{g}^{-1} = \prod_{l=1}^{\xi} (\widetilde{g}\, [x_i^{(l)}, y_i^{(l)}]^{\delta_l} \widetilde{g}^{-1}) \in H_i' \Longrightarrow H_i' \trianglelefteq G'.$$

Επίσης, για κάθε $i \in \{2, ..., s\}$, $H_i' \cap (H_1' \cdots H_{i-1}') = \{e_G\}$, διότι

$$H_i' \cap (H_1' \cdots H_{i-1}') \subseteq H_i \cap (H_1 \cdots H_{i-1}) = \{e_G\}.$$

Από το (i) τής προτάσεως 5.5.31 συνάγεται ότι

$$G' = [G, G] = [H_1 H_2 \cdots H_s, H_1 H_2 \cdots H_s] = \prod_{i=1}^{s} [H_1 H_2 \cdots H_s, H_i]$$
$$= \prod_{i=1}^{s} [(H_1 \cdots H_{i-1} H_{i+1} \cdots H_s) H_i, H_i] = \prod_{i=1}^{s} [H_1 \cdots H_{i-1} H_{i+1} \cdots H_s, H_i][H_i, H_i].$$

Επειδή $[H_1 \cdots H_{i-1} H_{i+1} \cdots H_s, H_i] \underset{\text{5.5.30 (vi)}}{\sqsubseteq} (H_1 \cdots H_{i-1} H_{i+1} \cdots H_s) \cap H_i = \{e_G\}$, η μεταθέτρια υποομάδα τής G ισούται με

$$G' = [H_1, H_1][H_2, H_2] \cdots [H_s, H_s] = H_1' H_2' \cdots H_s'.$$

Άρα ο ισχυρισμός είναι αληθής επί τη βάσει τής συνεπαγωγής (b)⇒(a) τού πορίσματος 7.1.81. □

7.1.84 Λήμμα. *Έστω ότι $s \in \mathbb{N}$, $s \geq 2$, και ότι οι H_1,..., H_s είναι s υποομάδες μιας ομάδας $(G, \cdot)$. Τότε για την απεικόνιση*

$$f_{H_1,..,H_s} : \prod_{j=1}^{s} H_j \longrightarrow G,\ (x_1, x_2, ..., x_s) \longmapsto x_1 x_2 \cdots x_s, \tag{7.28}$$

ισχύουν τα εξής:

(i) $\mathrm{Im}(f_{H_1,..,H_s}) = H_1 H_2 \cdots H_s$.

(ii) *Η $f_{H_1,..,H_s}$ είναι ομομορφισμός ομάδων εάν και μόνον εάν $x_i x_j = x_j x_i$ για οιαδήποτε στοιχεία $x_i \in H_i$, $x_j \in H_j$, όπου $i, j \in \{1, ..., s\}$, $i \neq j$.*

ΑΠΟΔΕΙΞΗ. (i) Προφανώς,

$$\begin{aligned}\mathrm{Im}(f_{H_1,..,H_s}) &= \left\{ f_{H_1,..,H_s}(x_1,...,x_s) \,\middle|\, (x_1,...,x_s) \in \prod_{j=1}^{s} H_j \right\} \\ &= \left\{ x_1x_2\cdots x_s \,\middle|\, (x_1,...,x_s) \in \prod_{j=1}^{s} H_j \right\} = H_1H_2\cdots H_s.\end{aligned}$$

(ii) Εάν η $f_{H_1,..,H_s}$ είναι ομομορφισμός και $x_i \in H_i$, $x_j \in H_j$, όπου $i,j \in \{1,...,s\}$, $i<j$, τότε

$$\begin{aligned}x_ix_j &= f_{H_1,..,H_s}(e_G,...,e_G, \underbrace{x_i}_{i\text{-οστή θέση}}, e_G,...,e_G, \underbrace{x_j}_{j\text{-οστή θέση}}, e_G,...,e_G) \\ &= f_{H_1,..,H_s}(e_G,...,e_G, \underbrace{x_j}_{j\text{-οστή θέση}}, e_G,...,e_G) f_{H_1,..,H_s}(e_G,...,e_G, \underbrace{x_i}_{i\text{-οστή θέση}}, e_G,...,e_G) \\ &= x_jx_i.\end{aligned}$$

(Εάν $i>j$, τότε καταλήγουμε στο ίδιο συμπέρασμα εναλλάσσοντας τους ρόλους των δεικτών i και j.) Και αντιστρόφως· εάν ικανοποιείται η ανωτέρω συνθήκη, τότε για οιαδήποτε στοιχεία $(x_1,...,x_s),(y_1,...,y_s) \in \prod_{j=1}^{s} H_j$ έχουμε

$$\begin{aligned}&f_{H_1,..,H_s}\left((x_1,..,x_s)(y_1,..,y_s)\right) = f_{H_1,..,H_s}(x_1y_1,..,x_sy_s) = (x_1y_1)\cdots(x_sy_s) \\ &= (x_1\cdots x_s)\,(y_1\cdots y_s) \quad \left(\begin{array}{c} \text{επειδή εξ υποθέσεως κάθε στοιχείο} \\ \text{τής υποομάδας } H_i \text{ μετατίθεται} \\ \text{αμοιβαίως με κάθε στοιχείο τής } H_j \end{array} \right) \\ &= f_{H_1,..,H_s}(x_1,...,x_s) f_{H_1,..,H_s}(y_1,...,y_s)\end{aligned}$$

Τούτο σημαίνει ότι η $f_{H_1,..,H_s}$ είναι ομομορφισμός. □

7.1.85 Θεώρημα. (i) *Έστω ότι $s \in \mathbb{N}$, $s \geq 2$, και ότι οι $G_1,...,G_s$ είναι s τυχούσες ομάδες. Για $i \in \{1,...,s\}$ ας συμβολίσουμε ως $\overline{G}_i := \mathrm{Im}(\iota_i)$ την εικόνα τής φυσικής εμφυτεύσεως $\iota_i : G_i \longrightarrow \prod_{j=1}^{s} G_j,\ x \longmapsto (e_{G_1},...,e_{G_{i-1}},x,e_{G_{i+1}},...,e_{G_s})$. Τότε*

$$\boxed{\prod_{j=1}^{s}{}^{\text{εσ.}}\, \overline{G}_j = \prod_{j=1}^{s} G_j.}$$

(ii) *Έστω ότι $s \in \mathbb{N}$, $s \geq 2$, και ότι οι $H_1,...,H_s$ είναι s ορθόθετες υποομάδες μιας ομάδας $(G,\cdot)$, τέτοιες ώστε να ισχύει $G = \prod_{j=1}^{s}{}^{\text{εσ.}}\, H_j$. Τότε η απεικόνιση* (7.28) *είναι ισομορφισμός ομάδων, οπότε*

$$\boxed{\prod_{j=1}^{s} H_j \cong G = \prod_{j=1}^{s}{}^{\text{εσ.}}\, H_j.}$$

ΑΠΟΔΕΙΞΗ. (i) Βλ. το (iv) τής προτάσεως 7.1.53.

(ii) Εάν $G = \prod_{j=1}^{s}{}^{\text{εσ.}} H_j$, τότε το λήμμα 7.1.84 μας πληροφορεί ότι η απεικόνιση (7.28) είναι επιμορφισμός ομάδων. Η ενριπτικότητα τής (7.28) οφείλεται στη συνθήκη (b) (ii) τού θεωρήματος 7.1.79. □

7.1.86 Παραδείγματα. (i) Θεωρώντας τήν $G_1 \times G_2 \times G_3$, όπου $G_1 := \mathfrak{S}_3$, $G_2 := \mathbb{Z}_6$, $G_3 := \mathbb{Z}_4^\times$, καθώς και τις $\overline{G}_1 := \{(\sigma, [0]_6, [1]_4) \,|\sigma \in \mathfrak{S}_3\}$

$$\overline{G}_2 := \{(\mathrm{id}, [a]_6, [1]_4) \,|a \in \mathbb{Z}\}, \;\; \overline{G}_3 := \{(\mathrm{id}, [0]_6, [b]_4) \,|b \in \mathbb{Z}\},$$

λαμβάνουμε (μέσω τού (i) τού θεωρήματος 7.1.85) $\mathfrak{S}_3 \times \mathbb{Z}_6 \times \mathbb{Z}_4^\times = \prod_{j=1}^{3}{}^{\text{εσ.}} \overline{G}_j$.

(ii) Η συνθήκη (iii) τού ορισμού 7.1.78 τού εσωτερικού γινομένου $\prod_{j=1}^{s}{}^{\text{εσ.}} H_j$ *δεν* μπορεί να αντικατασταθεί με την $H_i \cap H_j = \{e_G\}$, για οιουσδήποτε δείκτες $i, j \in \{1, ..., s\}, i \neq j$, *όταν* $s \geq 3$. Επί παραδείγματι, για τις κυκλικές υποομάδες $H_1 := \langle [1\,2] \circ [3\,4] \rangle$, $H_2 := \langle [1\,3] \circ [2\,4] \rangle$, $H_3 := \langle [1\,4] \circ [2\,3] \rangle$ τής ομάδας $\mathbf{V} := \{\mathrm{id}, [1\,2] \circ [3\,4], [1\,3] \circ [2\,4], [1\,4] \circ [2\,3]\}$ των τεσσάρων στοιχείων τού Klein έχουμε

$$\mathbf{V} = H_1 \circ H_2 \circ H_3, \quad H_1 \cap H_2 = H_1 \cap H_3 = H_2 \cap H_3 = \{\mathrm{id}\},$$

αλλά η $\mathbf{V}$ *δεν είναι* το εσωτερικό γινόμενο των H_1, H_2, H_3. (Εάν συνέβαινε αυτό, τότε θα έπρεπε, σύμφωνα με το 7.1.85 (ii), να ισχύει $\mathbf{V} \cong H_1 \times H_2 \times H_3$, πράγμα αδύνατο, καθόσον $|\mathbf{V}| = 4$, ενώ $|H_1 \times H_2 \times H_3| = 8$.)

7.1.87 Σημείωση. Λόγω τού θεωρήματος 7.1.85 είθισται να μην γίνεται *ομαδοθεωρητική διάκριση* μεταξύ τού εξωτερικού ευθέος γινομένου $\prod_{j=1}^{s} H_j$ και τού εσωτερικού ευθέος γινομένου $\prod_{j=1}^{s}{}^{\text{εσ.}} H_j$, και οι H_1,..., H_s να αναφέρονται απλώς ως **ευθείς παράγοντές του** (ή ως **ευθείς προσθετέοι του**, όταν χρησιμοποιείται ο αντίστοιχος *προσθετικός συμβολισμός*). Ωστόσο, υπάρχουν «λεπτές πτυχές» κάποιων σημαντικών θεωρητικών επιχειρημάτων που μας υπαγορεύουν την περαιτέρω διατήρηση των διακριτών συμβολισμών.

► **Περαιτέρω γενίκευση τής εννοίας τού ευθέος γινομένου.** Η έννοια τού ευθέος γινομένου γενικεύεται καταλλήλως και για απειροπληθείς οικογένειες ομάδων.

7.1.88 Ορισμός. Έστω ότι I είναι ένα μη κενό (όχι κατ' ανάγκην πεπερασμένο) σύνολο και ότι $(G_i, \circledast_i)_{i \in I}$ είναι τυχούσα οικογένεια ομάδων με τους δείκτες της ειλημμένους από το I. Εφοδιάζοντας το καρτεσιανό γινόμενο

$$\prod_{i \in I} G_i := \left\{ x = (x_i)_{i \in I} \;\middle|\; \begin{array}{c} x : I \longrightarrow \bigcup\limits_{i \in I} G_i \text{ απεικονίσεις} \\ \text{με } x(i) =: x_i \in G_i, \; \forall i \in I \end{array} \right\}$$

των υποκειμένων συνόλων τους με την εσωτερική πράξη

$$\prod_{i\in I} G_i \times \prod_{i\in I} G_i \longrightarrow \prod_{i\in I} G_i$$
$$((x_i)_{i\in I}, (y_i)_{i\in I}) \longmapsto (x_i)_{i\in I} \boxdot (y_i)_{i\in I} := (x_i \circledast_i y_i)_{i\in I}\,,$$

παρατηρούμε ότι το ζεύγος $(\prod_{i\in I} G_i, \boxdot)$ αποτελεί μια ομάδα έχουσα (ως προς την ορισθείσα πράξη " $\boxdot$ ") το $(e_{G_i})_{i\in I}$ ως ουδέτερο στοιχείο της και το $(x_i^{-1})_{i\in I}$ ως αντίστροφο στοιχείο οιουδήποτε $(x_i)_{i\in I} \in \prod_{i\in I} G_i$, όπου x_i^{-1} το αντίστροφο στοιχείο τού $x_i \in G_i$ ως προς την " $\circledast_i$ " για κάθε $i \in I$. Η ομάδα $(\prod_{i\in I} G_i, \boxdot)$ καλείται **απεριόριστο εξωτερικό ευθύ γινόμενο** των μελών τής οικογενείας $(G_i, \circledast_i)_{i\in I}$. Έστω τώρα τυχών δείκτης $j \in I$. Η επίριψη

$$\mathrm{pr}_j : \prod_{i\in I} G_i \longrightarrow G_j,\ (x_i)_{i\in I} \mapsto x_j, \tag{7.29}$$

καλείται **φυσική προβολή τής** $\prod_{i\in I} G_i$ **επί τής** G_j. Επίσης, η ένριψη

$$\iota_j : G_j \longrightarrow \prod_{i\in I} G_i,\ g \mapsto (x_i)_{i\in I},\ \ x_i := \begin{cases} e_{G_i}, & \text{όταν } i \in I \smallsetminus \{j\}, \\ g, & \text{όταν } i = j, \end{cases} \tag{7.30}$$

καλείται **φυσική εμφύτευση τής** G_j **εντός τής** $\prod_{i\in I} G_i$.

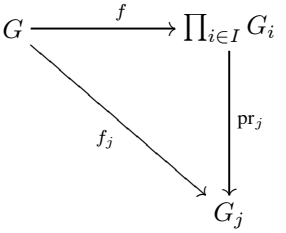
7.1.89 Παρατήρηση. Είναι προφανές ότι η (7.29) αποτελεί έναν επιμορφισμό ομάδων για κάθε $j \in I$.

Οι αποδείξεις των προτάσεων 7.1.90 και 7.1.96 αφήνονται ως ασκήσεις.

7.1.90 Πρόταση. («Καθολική ιδιότητα» απεριόριστου εξωτερικού ευθέος γινομένου.) *Έστω $(G, *)$ τυχούσα ομάδα. Εάν I είναι ένα μη κενό σύνολο και εάν $(f_i : G \longrightarrow G_i)_{i\in I}$ είναι μια οικογένεια ομομορφισμών ομάδων με τους δείκτες της ειλημμένους από το I, τότε υφίσταται ένας και μόνον ομομορφισμός ομάδων*

$$f : (G, *) \longrightarrow (\prod_{i\in I} G_i, \boxdot),$$

τέτοιος ώστε να ισχύει $\mathrm{pr}_j \circ f = f_j$, δηλαδή τέτοιος ώστε το διάγραμμα



να καθίσταται μεταθετικό για κάθε $j \in I$.

7.1.91 Σημείωση. Η πρόταση 7.1.57 γενικεύεται άμεσα και για απεριόριστα εξωτερικά ευθέα γινόμενα.

7.1.92 Ορισμός. Έστω I ένα μη κενό σύνολο και έστω $(G_i, \circledast_i)_{i\in I}$ τυχούσα οικογένεια ομάδων με τους δείκτες της ειλημμένους από το I. Για κάθε στοιχείο $x = (x_i)_{i\in I}$ τής $(\prod_{i\in I} G_i, \boxdot)$ ορίζεται το σύνολο $\mathrm{supp}(x) := \{\, i \in I |\, x_i \neq e_{G_i}\}$, το οποίο καλείται -ιδιαιτέρως- **φορέας τού** x. Το

$$\prod_{i\in I}^{\pi\varepsilon\varrho.} G_i := \left\{ x \in \prod_{i\in I} G_i \,\middle|\, \mathrm{card}(\mathrm{supp}(x)) < \infty \right\}$$

καλείται **περιορισμένο (ή ασθενές) εξωτερικό ευθύ γινόμενο** των μελών τής οικογενείας $(G_i, \circledast_i)_{i\in I}$.

7.1.93 Πρόταση. $\prod_{i\in I}^{\pi\varepsilon\varrho.} G_i \trianglelefteq \prod_{i\in I} G_i$.

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς,

$$\mathrm{supp}(e_{\prod_{i\in I} G_i}) = \varnothing \Rightarrow e_{\prod_{i\in I} G_i} \in \prod_{i\in I}^{\pi\varepsilon\varrho.} G_i.$$

Επιπροσθέτως, για οιαδήποτε $x, y \in \prod_{i\in I}^{\pi\varepsilon\varrho.} G_i$ έχουμε $\mathrm{supp}(y^{-1}) = \mathrm{supp}(y)$ και, κατ' επέκταση,

$$\mathrm{supp}(x \boxdot y^{-1}) \subseteq \mathrm{supp}(x) \cup \mathrm{supp}(y^{-1}) = \mathrm{supp}(x) \cup \mathrm{supp}(y)$$

$\Rightarrow \mathrm{card}(\mathrm{supp}(x \boxdot y^{-1})) \leq \mathrm{card}(\mathrm{supp}(x)) + \mathrm{card}(\mathrm{supp}(y)) - \mathrm{card}(\mathrm{supp}(x) \cap \mathrm{supp}(y)) < \infty$. Επομένως,

$$x \boxdot y^{-1} \in \prod_{i\in I}^{\pi\varepsilon\varrho.} G_i \underset{2.1.16}{\Longrightarrow} \prod_{i\in I}^{\pi\varepsilon\varrho.} G_i \sqsubseteq \prod_{i\in I} G_i.$$

Εν συνεχεία, θεωρούμε τυχόντα $x = (x_i)_{i\in I} \in \prod_{i\in I}^{\pi\varepsilon\varrho.} G_i$ και $y = (y_i)_{i\in I} \in \prod_{i\in I} G_i$. Επειδή

$$y \boxdot x \boxdot y^{-1} = (y_i \circledast_i x_i \circledast_i y_i^{-1})_{i\in I} \quad \text{με } y_i \circledast_i x_i \circledast_i y_i^{-1} = e_{G_i},\ \forall i \in I \smallsetminus \mathrm{supp}(x),$$

έχουμε $\mathrm{supp}(y \boxdot x \boxdot y^{-1}) = \mathrm{supp}(x)$ και

$$\mathrm{card}(\mathrm{supp}(y \boxdot x \boxdot y^{-1})) = \mathrm{card}(\mathrm{supp}(x)) < \infty \Rightarrow y \boxdot x \boxdot y^{-1} \in \prod_{i\in I}^{\pi\varepsilon\varrho.} G_i,$$

απ' όπου έπεται ότι $\prod_{i\in I}^{\pi\varepsilon\varrho.} G_i \trianglelefteq \prod_{i\in I} G_i$. □

7.1.94 Σημείωση. (Απλούστευση συμβολισμού.) (i) Όπως συνέβη και στην περίπτωση θεωρήσεως μιας *πεπερασμένης* οικογενείας ομάδων (βλ. σημείωση 7.1.54), θα μεταβούμε, από εδώ και στο εξής, στον *απλουστευμένο πολλαπλασιαστικό* συμβολισμό των πράξεων των $G_i, i \in I$, $\prod_{i\in I}^{\pi\varepsilon\varrho.} G_i$ και $\prod_{i\in I} G_i$ (μέσω τού συνήθους dot

"$\cdot$"), με μόνη εξαίρεση τις οικογένειες τις αποτελούμενες από *προσθετικές* ομάδες (για τις οποίες γράφουμε[25] $\bigoplus_{i\in I}^{\text{πεφ.}} G_i$ αντί τού $\prod_{i\in I}^{\text{πεφ.}} G_i$ και $\bigoplus_{i\in I} G_i$ αντί τού $\prod_{i\in I} G_i$).

(ii) Εάν $G_i = G$ για κάθε $i \in I$, τότε γράφουμε απλώς $G^{(I)}$ αντί τού $\prod_{i\in I}^{\text{πεφ.}} G_i$ και G^I αντί τού $\prod_{i\in I} G_i$. Προφανώς,

$$G^{(I)} = \left\{ x \in G^I \,\middle|\, \text{card}(\text{supp}(x)) < \infty \right\}.$$

Συνήθης σύμβαση: Ο ορισμός τής $G^{(I)}$ επεκτείνεται ακόμη και στην περίπτωση κατά την οποία $I = \varnothing$. Η $G^{(\varnothing)}$ θεωρείται ότι είναι μια τετριμμένη ομάδα. Εξάλλου, όταν το I είναι ένα *μονοσύνολο*, η $G^{(I)}$ ταυτίζεται με την ίδια την G.

7.1.95 Παρατήρηση. (i) Εάν είτε το I είναι πεπερασμένο σύνολο είτε μόνον πεπερασμένο πλήθος των μελών τής οικογενείας $(G_i)_{i\in I}$ είναι μη τετριμμένες ομάδες, τότε οι ομάδες $\prod_{i\in I}^{\text{πεφ.}} G_i$ και $\prod_{i\in I} G_i$ είναι ίσες. Εν γένει, η $\prod_{i\in I}^{\text{πεφ.}} G_i$ μπορεί να είναι *γνήσια* ορθόθετη υποομάδα τής $\prod_{i\in I} G_i$. Επί παραδείγματι, εάν $I := \mathbb{N}$ και καθεμιά εκ των G_i είναι ισόμορφη με την προσθετική ομάδα $(\mathbb{Z}, +)$, τότε

$$\bigoplus_{i\in\mathbb{N}}^{\text{πεφ.}} G_i \cong \mathbb{Z}^{(\mathbb{N})} \lhd \mathbb{Z}^{\mathbb{N}} \cong \bigoplus_{i\in\mathbb{N}} G_i,$$

καθώς υπάρχουν, π.χ., ακολουθίες ακεραίων αριθμών με *όλους τους* τούς όρους διαφορετικούς τού μηδενός.

(ii) Επειδή κάθε στοιχείο τής ομάδας $\mathbb{Z}_2^{\mathbb{N}}$ έχει τάξη ≤ 2, η $\mathbb{Z}_2^{\mathbb{N}}$ είναι μια *άπειρη* (περιοδική) ομάδα έχουσα εκθέτη $\exp(\mathbb{Z}_2^{\mathbb{N}}) = 2$.

7.1.96 Πρόταση. *Έστω I ένα μη κενό σύνολο και έστω $(G_i)_{i\in I}$ οιαδήποτε οικογένεια ομάδων με τους δείκτες της ειλημμένους από το I. Για κάθε $j \in I$ ας συμβολίσουμε ως $\overline{G}_j := \text{Im}(\iota_j)$ την εικόνα τής φυσικής εμφυτεύσεως* (7.30)*. Τότε ισχύουν τα ακόλουθα*:

(i) *Η ι_j είναι μονομορφισμός ομάδων και, ως εκ τούτου, $G_j \cong \overline{G}_j, \forall j \in I$.*

(ii) $\overline{G}_j \trianglelefteq \prod_{i\in I} G_i, \forall j \in I$.

(iii) $\overline{G}_i \cap \left\langle \left\{ \overline{G}_j \,\middle|\, j \in I \smallsetminus \{i\} \right\} \right\rangle = \{ e_{\prod_{i\in I} G_i} \}, \forall i \in I$.

(iv) $\left\langle \left\{ \overline{G}_i \,\middle|\, i \in I \right\} \right\rangle = \prod_{i\in I}^{\text{πεφ.}} G_i$.

7.1.97 Ορισμός. Έστω I ένα μη κενό σύνολο και έστω $(H_i)_{i\in I}$ μια οικογένεια υποομάδων μιας ομάδας $(G, \cdot)$ με τους δείκτες της ειλημμένους από το I. Λέμε ότι η G είναι το **εσωτερικό ευθύ γινόμενο** των μελών τής οικογενείας $(H_i)_{i\in I}$ (και γράφουμε[26] $G = \prod_{i\in I}^{\text{εσ.}} H_i$) όταν πληρούνται οι ακόλουθες συνθήκες:

---

[25] Ορισμένοι συγγραφείς αντί τού $\bigoplus_{i\in I}^{\text{πεφ.}} G_i$ χρησιμοποιούν τον συμβολισμό $\sum_{i\in I} G_i$.

[26] Στην περίπτωση κατά την οποία χρησιμοποιούμε τον *προσθετικό συμβολισμό* για την πράξη τής G, γράφουμε $G = \bigoplus_{i\in I}^{\text{εσ.}} H_i$ αντί τού $G = \prod_{i\in I}^{\text{εσ.}} H_i$ και το ονομάζουμε **εσωτερικό ευθύ άθροισμα** των μελών τής οικογενείας $(H_i)_{i\in I}$.

(i) $H_i \trianglelefteq G, \forall i \in I$,

(ii) $G = \langle \{ H_i | \, i \in I \} \rangle$, και

(iii) $H_i \cap \langle \{ H_j | \, j \in I \smallsetminus \{i\} \} \rangle = \{e_G\}, \forall i \in I$.

7.1.98 Θεώρημα. *Έστω I ένα μη κενό σύνολο και έστω $(H_i)_{i \in I}$ μια οικογένεια υποομάδων μιας ομάδας $(G, \cdot)$ με τους δείκτες της ειλημμένους από το I. Τότε τα* (a) *και* (b) *είναι ισοδύναμα*:

(a) $H_i \trianglelefteq G, \forall i \in I$, *και* $G = \prod\limits_{i \in I}^{\text{εσ.}} H_i$.

(b) *Για τα μέλη τής οικογενείας $(H_i)_{i \in I}$ ισχύουν τα ακόλουθα*:

(i) *Εάν $x_i \in H_i, x_j \in H_j$, για $i, j \in I, i \neq j$, τότε $x_i x_j = x_j x_i$.*

(ii) *Κάθε στοιχείο $g \in G$ γράφεται μονοσημάντως (μέχρις αναδιατάξεως των δεικτών) υπό τη μορφή*

$$g = x_{j_1} \cdots x_{j_k},$$

με $x_{j_\rho} \in H_{j_\rho}$ για κάθε $\rho \in \{1, ..., k\}$ και για κάποιον $k \in \mathbb{N}$, όπου οι δείκτες $j_1, ..., j_k \in I$ είναι σαφώς διακεκριμένοι.

ΑΠΟΔΕΙΞΗ. (a)⇒(b) Εάν $H_i \trianglelefteq G, \forall i \in I$, και $G = \prod\limits_{i \in I}^{\text{εσ.}} H_i$, τότε για οιαδήποτε στοιχεία $x_i \in H_i, x_j \in H_j, i, j \in I, i \neq j$, έχουμε

$$\left.\begin{array}{r} H_j \ni (\underbrace{x_i x_j x_i^{-1}}_{\in H_j}) x_j^{-1} = x_i (\underbrace{x_j x_i^{-1} x_j^{-1}}_{\in H_i}) \in H_i \\ \text{7.1.97 (iii)} \Rightarrow H_i \cap \langle \{ H_j | \, j \in I \smallsetminus \{i\} \} \rangle = \{e_G\} \end{array}\right\} \Rightarrow x_i x_j x_i^{-1} x_j^{-1} = e_G,$$

απ' όπου έπεται το (i), ήτοι ότι $x_i x_j = x_j x_i$. Έστω τώρα τυχόν στοιχείο $g \in G$. Επειδή εξ ορισμού $G = \langle \{ H_i | \, i \in I \} \rangle$ (βλ. 7.1.97 (ii)), το g (κατά το πόρισμα 2.2.6) γράφεται υπό τη μορφή $g = x_{j_1} \cdots x_{j_k}$, όπου $k \in \mathbb{N}$ και $\{j_1, ..., j_k\}$ ένα υποσύνολο k σαφώς διακεκριμένων στοιχείων τού I, τέτοιο ώστε $x_{j_\rho} \in H_{j_\rho}$ για κάθε υποδείκτη $\rho \in \{1, ..., k\}$. Για την απόδειξη τού (ii) αρκεί να ελεγχθεί ότι η εν λόγω έκφραση τού g είναι μοναδική. Προς τούτο υποθέτουμε ότι[27] $g = y_{j_1} \cdots y_{j_k}$, όπου $y_{j_\rho} \in H_{j_\rho}$ για κάθε $\rho \in \{1, ..., k\}$. Προφανώς, λόγω τού (i) έχουμε για κάθε $\rho \in \{1, ..., k\}$

$$\left.\begin{array}{r} y_{j_\rho}^{-1} x_{j_\rho} = \prod\limits_{\nu \in \{1, ..., k\} \smallsetminus \{\rho\}} (x_{j_\nu}^{-1} y_{j_\nu}) \\ \text{7.1.97 (iii)} \Rightarrow H_i \cap \langle \{ H_j | \, j \in I \smallsetminus \{i\} \} \rangle = \{e_G\} \end{array}\right\} \Rightarrow x_{j_\rho} = y_{j_\rho}, \forall \rho \in \{1, ..., k\}.$$

(b)⇒(a) Έστω ότι ισχύουν τα (i) και (ii) και έστω τυχόν στοιχείο $g \in G$. Κατά το (ii) το g γράφεται υπό τη μορφή $g = x_{j_1} \cdots x_{j_k}$, όπου $k \in \mathbb{N}$ και $\{j_1, ..., j_k\}$ ένα υποσύνολο k σαφώς διακεκριμένων στοιχείων τού I, τέτοιο ώστε $x_{j_\rho} \in H_{j_\rho}$

[27] Εν προκειμένω, δεν επέρχεται βλάβη τής γενικότητας (υποθέτοντας ότι αυτή η δεύτερη παράσταση τού g διαθέτει *ακριβώς* k παράγοντες από τις H_{j_ρ}, $\rho \in \{1, ..., k\}$), διότι εν ανάγκη μπορούμε να συμπεριλαμβάνουμε το e_G ως παράγοντα κατά βούληση.

για κάθε $\rho \in \{1,...,k\}$. Επομένως, για οιονδήποτε $\rho \in \{1,...,k\}$ και οιοδήποτε στοιχείο $a \in H_{j_\rho}$ έχουμε (μέσω τού (i))

$$
\begin{aligned}
&gag^{-1} = (x_{j_1}\cdots x_{j_k})\, a\, (x_{j_1}\cdots x_{j_k})^{-1} = x_{j_1}x_{j_2}\cdots\left(x_{j_k}ax_{j_k}^{-1}\right)\cdots x_{j_2}^{-1}x_{j_1}^{-1}\\
&= x_{j_1}x_{j_2}\cdots\left(x_{j_k}x_{j_k}^{-1}a\right)\cdots x_{j_2}^{-1}x_{j_1}^{-1} = x_{j_1}x_{j_2}\cdots\left(x_{j_{k-1}}ax_{j_{k-1}}^{-1}\right)\cdots x_{j_2}^{-1}x_{j_1}^{-1} = \cdots\\
&\cdots = x_{j_1}x_{j_2}\cdots(x_{j_\rho+1}ax_{j_\rho+1}^{-1})\cdots x_{j_2}^{-1}x_{j_1}^{-1} = x_{j_1}x_{j_2}\cdots\left(x_{i+1}x_{i+1}^{-1}a\right)\cdots x_{j_2}^{-1}x_{j_1}^{-1}\\
&= \left(x_{j_1}x_{j_2}\cdots x_{j_\rho-1}\right)x_{j_\rho}ax_{j_\rho}^{-1}(x_{j_\rho-1}^{-1}\cdots x_{j_2}^{-1}x_{j_1}^{-1})\\
&= x_{j_\rho}\left(x_{j_1}x_{j_2}\cdots x_{j_\rho-1}\right)a(x_{j_\rho-1}^{-1}\cdots x_{j_2}^{-1}x_{j_1}^{-1})x_{j_\rho}^{-1} = \cdots\cdots = x_{j_\rho}ax_{j_\rho}^{-1} \in H_{j_\rho}
\end{aligned}
$$

οπότε $H_{j_\rho} \trianglelefteq G$, $\forall \rho \in \{1,...,k\}$. Επειδή *κάθε* δείκτης $i \in I$ είναι τής μορφής j_ρ στην ανωτέρω παράσταση *κάποιου* $g \in G$, έχουμε $H_i \trianglelefteq G$, $\forall i \in I$. Επιπροσθέτως, από το (ii) έπεται άμεσα η ισότητα $G = \langle\{\, H_i |\, i \in I\}\rangle$. Τέλος, εάν $g \in H_i \cap \langle\{\, H_j |\, j \in I\smallsetminus\{i\}\}\rangle)$ για κάποιον $i \in I$, τότε υπάρχουν ένας $k \in \mathbb{N}$ και ένα υποσύνολο $\{j_1,...,j_k\}$ αποτελούμενο από k σαφώς διακεκριμένα στοιχεία τού $I\smallsetminus\{i\}$, τέτοιο ώστε $g = x_{j_1}\cdots x_{j_k}$, όπου $x_{j_\rho} \in H_{j_\rho}$ για κάθε $\rho \in \{1,...,k\}$, οπότε

$$
\left.\begin{aligned} g &= e_G x_{j_1}\cdots x_{j_k}\\ g &= g\underbrace{e_G\cdots e_G}_{k\ \text{φορές}}\end{aligned}\right\} \underset{\text{(ii)}}{\Longrightarrow} g = e_G \Rightarrow H_i \cap \langle\{\, H_j |\, j \in I\smallsetminus\{i\}\}\rangle) = \{e_G\}.
$$

Άρα $G = \prod\limits_{i\in I}^{\text{εσ.}} H_i$. □

7.1.99 Λήμμα. *Έστω I ένα μη κενό σύνολο και έστω $(H_i)_{i\in I}$ μια οικογένεια υποομάδων μιας ομάδας $(G,\cdot)$ με τους δείκτες της ειλημμένους από το I. Τότε για την απεικόνιση*

$$
f_{(H_i)_{i\in I}} : \prod_{i\in I}^{\text{περ.}} H_i \longrightarrow G,
$$

$$
x = (x_i)_{i\in I} \longmapsto f_{(H_i)_{i\in I}}(x) := \begin{cases} e_G, & \text{όταν } x = e_G,\\ \displaystyle\prod_{i\in \operatorname{supp}(x)} x_i, & \text{όταν } x \neq e_G,\end{cases} \tag{7.31}
$$

ισχύουν τα εξής:

(i) $\operatorname{Im}(f_{(H_i)_{i\in I}}) = \langle\{\, H_i |\, i \in I\}\rangle$.

(ii) *H $f_{(H_i)_{i\in I}}$ είναι ομομορφισμός ομάδων εάν και μόνον εάν $x_ix_j = x_jx_i$ για οιαδήποτε στοιχεία $x_i \in H_i$, $x_j \in H_j$, όπου $i,j \in I$, $i \neq j$.*

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς παρατηρούμε ότι $f_{(H_i)_{i\in I}}(\iota_j(x_j)) = x_j$ για κάθε $x_j \in H_j$ και για κάθε $j \in I$.

(i) Προφανώς, $e_G = f_{(H_i)_{i\in I}}(e_G) \in \operatorname{Im}(f_{(H_i)_{i\in I}})$. Έστω $g \in \operatorname{Im}(f_{(H_i)_{i\in I}})\smallsetminus\{e_G\}$. Τότε

$$
\exists x = (x_i)_{i\in I} \in \prod_{i\in I}^{\text{περ.}} H_i : g = f_{(H_i)_{i\in I}}(x) = \prod_{i\in\, \operatorname{supp}(x)} x_i.
$$

Επειδή $g = \prod_{i\in\text{supp}(x)} x_i \in \langle\{H_i|\, i\in I\}\rangle$, έχουμε $\text{Im}(f_{(H_i)_{i\in I}}) \subseteq \prod_{i\in I}^{\text{εσ.}} H_i$. Και αντιστρόφως· κάθε $g \in \langle\{H_i|\, i\in I\}\rangle_i$ γράφεται υπό τη μορφή $g = h_{j_1}\cdots h_{j_k}$, όπου $k \in \mathbb{N}$ και $\{j_1, ..., j_k\}$ ένα υποσύνολο k σαφώς διακεκριμένων στοιχείων τού I, τέτοιο ώστε $h_{j_\rho} \in H_{j_\rho}$ για κάθε υποδείκτη $\rho \in \{1, ..., k\}$. Επειδή έχουμε $g = h_{j_1}\cdots h_{j_k} = f_{(H_i)_{i\in I}}(\iota_{j_1}(h_{j_1})\cdots\iota_{j_k}(h_{j_k})) \in \text{Im}(f_{(H_i)_{i\in I}})$, *και* ο αντίστροφος εγκλεισμός $\langle\{H_i|\, i\in I\}\rangle \subseteq \text{Im}(f_{(H_i)_{i\in I}})$ είναι αληθής.

(ii) Εάν η $f_{(H_i)_{i\in I}}$ είναι ομομορφισμός και $x_i \in H_i$, $x_j \in H_j$, με $i, j \in I$, $i \neq j$, τότε

$$x_i x_j = f_{(H_i)_{i\in I}}(\iota_i(x_i))f_{(H_i)_{i\in I}}(\iota_j(x_j)) = f_{(H_i)_{i\in I}}(\iota_i(x_i)\iota_j(x_j)) = f_{(H_i)_{i\in I}}(\iota_j(x_j)\iota_i(x_i))$$
$$= f_{(H_i)_{i\in I}}(\iota_j(x_j))f_{(H_i)_{i\in I}}(\iota_i(x_i)) = x_j x_i,$$

όπου η τρίτη ισότητα οφείλεται στο ότι[28] $\underbrace{\iota_i(x_i)}_{\in\overline{H}_i}\underbrace{\iota_j(x_j)}_{\in\overline{H}_j} = \underbrace{\iota_j(x_j)}_{\in\overline{H}_j}\underbrace{\iota_i(x_i)}_{\in\overline{H}_i}$. Και αντιστρόφως· εάν ικανοποιείται η ανωτέρω συνθήκη, τότε για οιαδήποτε στοιχεία $x = (x_i)_{i\in I}, y = (y_i)_{i\in I} \in (\prod_{i\in I}^{\text{περ.}} H_i)\setminus\{e_G\}$ έχουμε

$$f_{(H_i)_{i\in I}}(xy) = \prod_{i\in\,\text{supp}(xy)} x_i y_i = \prod_{i\in\,\text{supp}(x)} x_i \prod_{i\in\,\text{supp}(y)} y_i = f_{(H_i)_{i\in I}}(x) f_{(H_i)_{i\in I}}(y)$$

(Η ισότητα $f_{(H_i)_{i\in I}}(xy) = f_{(H_i)_{i\in I}}(x)f_{(H_i)_{i\in I}}(y)$ είναι προφανής όταν τουλάχιστον ένα εκ των x, y είναι ίσο με το e_G.) Άρα η $f_{(H_i)_{i\in I}}$ είναι ομομορφισμός. □

7.1.100 Θεώρημα. (i) *Έστω $(G_i)_{i\in I}$ τυχούσα οικογένεια ομάδων με τους δείκτες της ειλημμένους από ένα σύνολο $I \neq \varnothing$. Για κάθε $j \in I$ ας συμβολίσουμε και πάλι ως $\overline{G}_j := \text{Im}(\iota_j)$ την εικόνα τής* (7.30) *τής G_j εντός τής $\prod_{i\in I} G_i$. Τότε*

$$\boxed{\prod_{i\in I}^{\text{εσ.}} \overline{G}_i = \prod_{i\in I}^{\text{περ.}} G_i.}$$

(ii) *Έστω $(H_i)_{i\in I}$ μια οικογένεια υποομάδων μιας ομάδας $(G, \cdot)$, με τους δείκτες της ειλημμένους από ένα σύνολο $I \neq \varnothing$, τέτοια ώστε να ισχύει $G = \prod_{i\in I}^{\text{εσ.}} H_i$. Τότε η απεικόνιση* (7.31) *είναι ισομορφισμός ομάδων, οπότε*

$$\boxed{\prod_{i\in I}^{\text{περ.}} H_i \cong G = \prod_{i\in I}^{\text{εσ.}} H_i.}$$

ΑΠΟΔΕΙΞΗ. (i) Βλ. το (iv) τής προτάσεως 7.1.96.

(ii) Εάν $G = \prod_{i\in I}^{\text{εσ.}} H_i$, τότε το λήμμα 7.1.99 μας πληροφορεί ότι η απεικόνιση (7.31) είναι επιμορφισμός ομάδων. Η ενριπτικότητα τής (7.31) οφείλεται στη συνθήκη (b) (ii) τού θεωρήματος 7.1.98. □

7.1.101 Σημείωση. Λόγω τού θεωρήματος 7.1.100 είθισται να μη γίνεται *ομαδοθεωρητική διάκριση* μεταξύ των $\prod_{i\in I}^{\text{εσ.}} H_i$ και $\prod_{i\in I}^{\text{περ.}} H_i$.

[28] Αρκεί να ληφθεί υπ' όψιν η συνθήκη (b) (i) τού θεωρήματος 7.1.98 (αλλά με τις $\overline{H}_i$ στη θέση των εκεί παρατεθεισών H_i), σε συνδυασμό με την πρόταση 7.1.96.

7.2 ΘΕΩΡΗΜΑ ΤΩΝ KRULL, REMAK KAI SCHMIDT

Στο εδάφιο 7.1.32 ορίσθηκε η έννοια τής αναποσυνθέσιμης ομάδας και μέσω τού θεωρήματος 7.1.40 αποδείχθηκε ότι η αποσυνθεσιμότητα ισοδυναμεί με την ύπαρξη ενός ορθόθετου ενδομορφισμού με κάποιες ειδικές ιδιότητες. Ευλόγως γεννώνται τα εξής ερωτήματα:

(i) Παριστάται πάντοτε μια μη τετριμμένη ομάδα ως εσωτερικό ευθύ γινόμενο *πεπερασμένου πλήθους* αναποσυνθέσιμων ορθόθετων υποομάδων της;

(ii) Όταν υφίσταται μια τέτοιου είδους παράσταση, είναι αυτή (υπό κάποια έννοια[29]) *μονοσημάντως ορισμένη*;

Το ερώτημα (i) δέχεται καταφατική απάντηση για *πεπερασμένες ομάδες*, κάτι που είχε επισημανθεί σε εργασίες των R. Remak[30] και O. Schmidt[31]. (Βλ. πρόταση 7.2.11.) Ωστόσο, τούτο δεν συμβαίνει εν γένει και για *τυχούσες* άπειρες ομάδες. Όπως αποδεικνύεται μέσω τού γενικότερου θεωρήματος 7.2.12, μια *τυχούσα* ομάδα G διαθέτει (τουλάχιστον) μία παράσταση αυτού τού είδους όταν πληροί είτε τη *συνθήκη των ανιουσών αλυσίδων* είτε τη *συνθήκη των κατιουσών αλυσίδων* επί τού συνόλου $\mathbf{NSubg}(G)$. (Οι εν λόγω συνθήκες ορίζονται επί οιουδήποτε μη κενού υποσυνόλου $\mathfrak{X}$ τού συνόλου $\mathbf{Subg}(G)$ στο εδάφιο 7.2.2, ενώ κάποιες κύριες ιδιότητες ομάδων που πληρούν τουλάχιστον μία εξ αυτών περιγράφονται στις προτάσεις 7.2.5, 7.2.6, 7.2.7 και 7.2.9.)

Το κύριο θεώρημα 7.2.25 τής παρούσας ενότητας αφορά στο ερώτημα (ii) και μας πληροφορεί ότι η μοναδικότητα μιας παραστάσεως αυτού τού είδους (τόσον *μέχρις ισομορφισμού όρων* όσον και *σε επίπεδο ανταλλαγής όρων*) είναι διασφαλισμένη για τις ομάδες G που πληρούν *αμφότερες* τις συνθήκες επί τού $\mathbf{NSubg}(G)$. (Η παρατιθέμενη απόδειξή του βασίζεται σε περαιτέρω εργασίες των W. Krull[32] και O. Schmidt[33], καθώς και στο εμβόλιμο πόρισμα 7.2.17 τού λεγομένου *λήμματος τού Fitting* 7.2.16.) Από την άλλη μεριά, για τη διασφάλιση τής λεγομένης *ουσιώδους* μοναδικότητας απαιτείται να ικανοποιείται και μια *επιπρόσθετη* συνθήκη. (Βλ. θεώρημα 7.2.28.)

7.2.1 Ορισμός. Έστω $(G, \cdot)$ μια ομάδα και έστω $\varnothing \neq \mathfrak{X} \subseteq \mathbf{Subg}(G)$.

(i) Μια ακολουθία $\{H_i\}_{i\in\mathbb{N}}$ (όχι κατ' ανάγκην σαφώς διακεκριμένων) ομάδων που ανήκουν στο $\mathfrak{X}$ καλείται **ανιούσα αλυσίδα** στοιχείων τού $\mathfrak{X}$ όταν[34]

$$H_i \sqsubseteq H_{i+1},\ \forall i \in \mathbb{N}.$$

[29] Εάν στην παράσταση δεν προαπαιτηθεί η *αναποσυνθεσιμότητα* των μετεχόντων ευθέων παραγόντων, τότε η ιδιότητα τής *μέχρις ισομορφισμού* μοναδικότητας αυτών των δομικών όρων αναφοράς δεν διατηρείται, όπως δείχνει το παράδειγμα 7.1.31 (ii).

[30] R. Remak: *Über die Zerlegung endlicher Gruppen in direkte unzerlegbare Faktoren*, Jour. reine und ang. Math. **139** (1911), 293-308.

[31] O. Schmidt: *Über die Zerlegung endlicher Gruppen in unzerlegbare Faktoren*, Izv. Kiev Univ. (1912), 1-6, και *Sur les produits directs*, S.M.F. Bull. **41** (1913), 161-164.

[32] W. Krull: *Über verallgemeinerte endliche abelsche Gruppen*, Math. Zeitschrift **23** (1925), 161-196.

[33] O. Schmidt: *Über unendliche Gruppen mit endlicher Kette*, Math. Zeitschrift **29** (1928), 34-41.

[34] Εν τοιαύτη περιπτώσει, το υποκείμενο σύνολο τής εν λόγω ακολουθίας (στην «ανηγμένη» του μορφή) αποτελεί μια (*ειδικής φύσεως*) *αλυσίδα* τού μερικώς διατεταγμένου συνόλου $(\mathfrak{X}, \sqsubseteq)$ υπό την έννοια τού ορισμού Α.2.18.

Λέμε ότι μια ανιούσα αλυσίδα $\{H_i\}_{i\in\mathbb{N}}$ στοιχείων τού $\mathfrak{X}$ είναι **στάσιμη** όταν υπάρχει κάποιος $\nu \in \mathbb{N}$ για τον οποίο ισχύει $H_i = H_\nu$ για κάθε φυσικό αριθμό $i \geq \nu$.

(ii) Μια ακολουθία $\{K_i\}_{i\in\mathbb{N}}$ (όχι κατ' ανάγκην σαφώς διακεκριμένων) ομάδων που ανήκουν στο $\mathfrak{X}$ καλείται **κατιούσα αλυσίδα** στοιχείων τού $\mathfrak{X}$ όταν

$$K_{i+1} \sqsubseteq K_i,\ \forall i \in \mathbb{N}.$$

Λέμε ότι μια κατιούσα αλυσίδα $\{K_i\}_{i\in\mathbb{N}}$ στοιχείων τού $\mathfrak{X}$ είναι **στάσιμη** όταν υπάρχει κάποιος $\nu \in \mathbb{N}$ για τον οποίο ισχύει $K_i = K_\nu$ για κάθε φυσικό αριθμό $i \geq \nu$.

7.2.2 Ορισμός. Έστω $(G, \cdot)$ μια ομάδα και έστω $\varnothing \neq \mathfrak{X} \subseteq \mathbf{Subg}(G)$.

(i) Λέμε ότι η G **πληροί τη συνθήκη των ανιουσών αλυσίδων** (εν συντομία, **Σ.Α.Α.**) **επί τού** $\mathfrak{X}$ όταν *κάθε* ανιούσα αλυσίδα στοιχείων τού $\mathfrak{X}$ είναι στάσιμη.

(ii) Λέμε ότι η G **πληροί τη συνθήκη των κατιουσών αλυσίδων** (εν συντομία, **Σ.Κ.Α.**) **επί τού** $\mathfrak{X}$ όταν *κάθε* κατιούσα αλυσίδα στοιχείων τού $\mathfrak{X}$ είναι στάσιμη.

7.2.3 Πρόταση. *Έστω $(G, \cdot)$ μια ομάδα και έστω $\mathfrak{X}$ ένα μη κενό υποσύνολο τού $\mathbf{Subg}(G)$. Τότε ισχύουν τα ακόλουθα*:

(i) *Η G πληροί τη Σ.Α.Α. επί τού $\mathfrak{X}$ εάν και μόνον εάν κάθε μη κενό υποσύνολο τού $\mathfrak{X}$ διαθέτει (τουλάχιστον) ένα μεγιστικό στοιχείο (ως προς την "$\sqsubseteq$").*

(ii) *Η G πληροί τη Σ.Κ.Α. επί τού $\mathfrak{X}$ εάν και μόνον εάν κάθε μη κενό υποσύνολο τού $\mathfrak{X}$ διαθέτει (τουλάχιστον) ένα ελαχιστικό στοιχείο (ως προς την "$\sqsubseteq$").*

ΑΠΟΔΕΙΞΗ. (i) Υποθέτουμε εν πρώτοις ότι η G πληροί τη Σ.Α.Α. επί τού $\mathfrak{X}$. Εάν $\varnothing \neq \mathfrak{Y} \subseteq \mathfrak{X}$, τότε υπάρχει κάποιο στοιχείο, ας το πούμε H_1, εντός τού $\mathfrak{Y}$. Εάν το H_1 είναι μεγιστικό στοιχείο τού $\mathfrak{Y}$, τότε έχει καλώς. Ειδάλλως, θα υπάρχει κάποιο $H_2 \in \mathfrak{Y}$, τέτοιο ώστε να ισχύει $H_1 \sqsubseteq H_2$. Εάν το H_2 είναι μεγιστικό στοιχείο τού $\mathfrak{Y}$, τότε έχει καλώς. Ειδάλλως, θα υπάρχει κάποιο $H_3 \in \mathfrak{Y}$, τέτοιο ώστε να ισχύει $H_2 \sqsubseteq H_3$. Εφαρμόζοντας κατ' επανάληψη την ίδια (επαγωγική) συλλογιστική σχηματίζουμε μια ανιούσα αλυσίδα

$$H_1 \sqsubseteq H_2 \sqsubseteq \cdots \sqsubseteq H_i \sqsubseteq H_{i+1} \sqsubseteq \cdots$$

υποομάδων τής G ανηκουσών στο $\mathfrak{Y}$, η οποία είναι εξ υποθέσεως στάσιμη, ήτοι υπάρχει κάποιος $\nu \in \mathbb{N}$ για τον οποίο ισχύει $H_i = H_\nu$ για κάθε φυσικό αριθμό $i \geq \nu$. Η υποομάδα H_ν τής G οφείλει να είναι μεγιστικό στοιχείο τού $\mathfrak{Y}$. Πράγματι· εάν η H είναι οιαδήποτε υποομάδα τής G ανήκουσα στο $\mathfrak{Y}$ για την οποία ισχύει $H_\nu \sqsubseteq H$, τότε (λόγω τού τρόπου κατασκευής τής ως άνω αλυσίδας) θα υπάρχει κάποιος $j \in \mathbb{N}$ με $H \sqsubseteq H_j$, οπότε

$$\left.\begin{array}{ll} H \sqsubseteq H_j \sqsubseteq H_\nu, & \text{όταν } j \leq \nu \\ H \sqsubseteq H_j = H_\nu, & \text{όταν } j \geq \nu \end{array}\right\} \Longrightarrow H_\nu = H.$$

Άρα η H_ν είναι όντως μεγιστικό στοιχείο τού $\mathfrak{Y}$. Και αντιστρόφως· εάν κάθε μη κενό υποσύνολο τού $\mathfrak{X}$ διαθέτει (τουλάχιστον) ένα μεγιστικό στοιχείο (ως προς την "$\sqsubseteq$"), θεωρήσουμε *τυχούσα* ανιούσα αλυσίδα

$$H_1 \sqsubseteq H_2 \sqsubseteq \cdots \sqsubseteq H_i \sqsubseteq H_{i+1} \sqsubseteq \cdots$$

και υποθέσουμε ότι η H_m είναι μεγιστικό στοιχείο τού συνόλου $\{H_i | i \in \mathbb{N}\}$, τότε για κάθε φυσικό αριθμό $i \geq m$ έχουμε $H_m \sqsubseteq H_i$, οπότε $H_i = H_m$. Αυτό σημαίνει ότι η G πληροί τη Σ.Α.Α. επί τού $\mathfrak{X}$.

(ii) Τούτο αποδεικνύεται παρομοίως. □

7.2.4 Παραδείγματα. Εν γένει, για μια ομάδα G δεν υφίσταται αλληλεξάρτηση μεταξύ τής Σ.Α.Α. και τής Σ.Κ.Α. επί τού $\mathbf{NSubg}(G)$ ή επί τού (ιδίου τού) $\mathbf{Subg}(G)$.

(i) Εάν η G είναι *πεπερασμένη*, τότε πληροί προφανώς *αμφότερες* τις συνθήκες τόσον επί τού $\mathbf{NSubg}(G)$ όσον και επί τού $\mathbf{Subg}(G)$.

(ii) Η άπειρη προσθετική κυκλική ομάδα $(\mathbb{Z}, +)$ πληροί τη Σ.Α.Α. επί τού

$$\mathbf{NSubg}(G) = \mathbf{Subg}(\mathbb{Z}) \underset{\text{2.2.19 (i)}}{=} \{d\mathbb{Z} | d \in \mathbb{N}_0\},$$

διότι εάν

$$d_1\mathbb{Z} \sqsubseteq d_2\mathbb{Z} \sqsubseteq d_3\mathbb{Z} \sqsubseteq \cdots\cdots \sqsubseteq d_i\mathbb{Z} \sqsubseteq d_{i+1}\mathbb{Z} \sqsubseteq \cdots\cdots$$

για κάποιους $d_1, d_2, ..., d_i, d_{i+1}, ...$ ($i \in \mathbb{N}$), τότε είτε ισχύει $d_i = 0, \forall i \in \mathbb{N}$, είτε $\exists j \in \mathbb{N} : d_j \neq 0$. Στη δεύτερη περίπτωση, $d_{j+k+1} \mid d_{j+k}$ για κάθε $k \in \mathbb{N}_0$. (Βλ. το (i) τού πορίσματος 2.2.20.) Επομένως, $\exists \nu \in \mathbb{N} : d_i = d_\nu$ για κάθε φυσικό αριθμό $i \geq \nu$. (Προφανώς, $\nu \leq \text{card}(\mathfrak{D}_j)$, όπου $\mathfrak{D}_j$ είναι το σύνολο των θετικών ακεραίων διαιρετών τού j. Βλ. Β.2.34.) Από την άλλη μεριά, η $(\mathbb{Z}, +)$ δεν πληροί τη Σ.Κ.Α. επί τού $\mathbf{Subg}(\mathbb{Z})$, διότι π.χ. η

$$\cdots\cdots \sqsubset 2^{i+1}\mathbb{Z} \sqsubset 2^i\mathbb{Z} \sqsubset \cdots\cdots \sqsubset 4\mathbb{Z} \sqsubset 2\mathbb{Z} \sqsubset \mathbb{Z}$$

αποτελεί μια μη στάσιμη κατιούσα αλυσίδα υποομάδων αυτής.

(iii) Η άπειρη προσθετική αβελιανή ομάδα $\mathbb{Z}(p^\infty)$ (βλ. άσκηση **4-41**) δεν πληροί τη Σ.Α.Α. επί τού $\mathbf{NSubg}(\mathbb{Z}(p^\infty)) = \mathbf{Subg}(\mathbb{Z}(p^\infty))$, διότι (σύμφωνα με το (vii) τής εν λόγω ασκήσεως) το σύνολο $\mathbf{Subg}(\mathbb{Z}(p^\infty)) \setminus \{\mathbb{Z}(p^\infty)\}$ των γνησίων υποομάδων της δεν διαθέτει κανένα μεγιστικό στοιχείο ως προς τη σχέση διατάξεως "$\sqsubseteq$". Ωστόσο, η $\mathbb{Z}(p^\infty)$ πληροί τη Σ.Κ.Α. επί τού $\mathbf{Subg}(\mathbb{Z}(p^\infty))$. Πράγματι· επειδή έχουμε $\mathbf{Subg}(\mathbb{Z}(p^\infty)) = \{H_m | m \in \mathbb{N}_0\} \coprod \{\mathbb{Z}(p^\infty)\}$, όπου $H_m := \langle p^{-m} + \mathbb{Z} \rangle$ υποομάδα τάξεως $|H_m| = p^m$, εάν υποθέσουμε ότι υπάρχει κάποια μη στάσιμη κατιούσα αλυσίδα υποομάδων τής $\mathbb{Z}(p^\infty)$, τότε αυτή θα είναι τής μορφής

$$\cdots\cdots \sqsubset H_{m_{i+1}} \sqsubset H_{m_i} \sqsubset \cdots\cdots \sqsubset H_{m_3} \sqsubset H_{m_2} \sqsubset H_{m_1} \sqsubset H,$$

όπου είτε $H = \mathbb{Z}(p^\infty)$ είτε $H = H_{m_0}$ (για κάποιον $m_0 \in \mathbb{N}_0$) και $|H_{m_i}| = p^{m_i}$, οπότε $\cdots < m_{i+1} < m_i < \cdots < m_2 < m_1$. Τούτο όμως είναι αδύνατον, καθότι $\exists j \in \mathbb{N}_0$: $j \leq m_1$ και $m_j = 0$.

(iv) Η άπειρη προσθετική ομάδα $(\mathbb{Q}, +)$ των ρητών αριθμών δεν πληροί καμία εκ των συνθηκών επί τού $\mathbf{NSubg}(\mathbb{Q}) = \mathbf{Subg}(\mathbb{Q})$, διότι π.χ. η

$$\tfrac{1}{2}\mathbb{Z} \sqsubset \tfrac{1}{4}\mathbb{Z} \sqsubset \cdots\cdots \sqsubset \tfrac{1}{2^i}\mathbb{Z} \sqsubset \tfrac{1}{2^{i+1}}\mathbb{Z} \sqsubset \cdots\cdots$$

αποτελεί μια μη στάσιμη ανιούσα[35] και η

$$\cdots\cdots \sqsubset 2^{i+1}\mathbb{Z} \sqsubset 2^{i}\mathbb{Z} \sqsubset \cdots\cdots \sqsubset 4\mathbb{Z} \sqsubset 2\mathbb{Z} \sqsubset \mathbb{Z} \sqsubset \mathbb{Q}$$

μια μη στάσιμη κατιούσα αλυσίδα υποομάδων αυτής.

7.2.5 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \trianglelefteq G$. Τότε τα ακόλουθα είναι ισοδύναμα*:

(i) *Η G πληροί τη Σ.Α.Α. (και αντιστοίχως, τη Σ.Κ.Α.) επί τού* $\mathbf{Subg}(G;H)$.

(ii) *Η πηλικοομάδα G/H πληροί τη Σ.Α.Α. (και αντιστοίχως, τη Σ.Κ.Α.) επί τού* $\mathbf{Subg}(G/H)$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Έστω $M_1 \sqsubseteq M_2 \sqsubseteq \cdots\cdots \sqsubseteq M_i \sqsubseteq M_{i+1} \sqsubseteq \cdots\cdots$ τυχούσα ανιούσα (και αντιστοίχως,

$$\cdots\cdots \sqsubseteq N_{i+2} \sqsubseteq N_{i+1} \sqsubseteq N_i \sqsubseteq \cdots\cdots \sqsubseteq N_2 \sqsubseteq N_1$$

τυχούσα κατιούσα) αλυσίδα στοιχείων τού $\mathbf{Subg}(G/H)$. Κατά το πόρισμα 4.4.15,

$$M_i = K_i/H, \ \text{(και αντ. } N_i = L_i/H), \ \text{όπου } K_i \text{ (και αντ. } L_i) \in \mathbf{Subg}(G;H)$$

με $K_1 \sqsubseteq K_2 \sqsubseteq \cdots\cdots \sqsubseteq K_i \sqsubseteq K_{i+1} \sqsubseteq K_{i+2} \sqsubseteq \cdots\cdots$, (και αντιστοίχως,

$$\cdots\cdots \sqsubseteq L_{i+2} \sqsubseteq L_{i+1} \sqsubseteq L_i \sqsubseteq \cdots\cdots \sqsubseteq L_2 \sqsubseteq L_1),$$

για κάθε $i \in \mathbb{N}$. Εξ υποθέσεως, $\exists \nu_1 \in \mathbb{N}$ (και αντιστοίχως, $\exists \nu_2 \in \mathbb{N}$) για τον οποίο ισχύει $K_i = K_{\nu_1}$ για κάθε φυσικό αριθμό $i \geq \nu_1$ (και αντιστοίχως, $L_i = L_{\nu_2}$ για κάθε φυσικό αριθμό $i \geq \nu_2$). Επομένως, $M_i = M_{\nu_1}$ για κάθε φυσικό αριθμό $i \geq \nu_1$ (και αντιστοίχως, $N_i = N_{\nu_2}$ για κάθε φυσικό αριθμό $i \geq \nu_2$).

(i)⇒(ii) Τούτο αποδεικνύεται παρομοίως. □

7.2.6 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \trianglelefteq G$. Τότε τα ακόλουθα είναι ισοδύναμα*:

(i) *Η G πληροί τη Σ.Α.Α. (και αντιστοίχως, τη Σ.Κ.Α.) επί τού* $\mathbf{NSubg}(G;H)$.

(ii) *Η πηλικοομάδα G/H πληροί τη Σ.Α.Α. (και αντιστοίχως, τη Σ.Κ.Α.) επί τού* $\mathbf{NSubg}(G/H)$.

ΑΠΟΔΕΙΞΗ. Πανομοιότυπη εκείνης τής προτάσεως 7.2.5 (κατόπιν εφαρμογής τού πορίσματος 4.5.18). □

7.2.7 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H \trianglelefteq G$. Εάν η H πληροί τη Σ.Α.Α. (και αντιστοίχως, τη Σ.Κ.Α.) επί τού* $\mathbf{Subg}(H)$ *και η G/H πληροί τη Σ.Α.Α. (και αντιστοίχως, τη Σ.Κ.Α.) επί τού* $\mathbf{Subg}(G/H)$, *τότε η G πληροί τη Σ.Α.Α. (και αντιστοίχως, τη Σ.Κ.Α.) επί τού* $\mathbf{Subg}(G)$.

[35] Επειδή $\nexists a \in \mathbb{Z} : \frac{1}{2^{i+1}} = \frac{a}{2^i}$, έχουμε $\frac{1}{2^{i+1}} \in \frac{1}{2^{i+1}}\mathbb{Z} \smallsetminus \frac{1}{2^i}\mathbb{Z}$ για κάθε $i \in \mathbb{N}$.

ΑΠΟΔΕΙΞΗ. Εάν η H πληροί τη Σ.Α.Α. επί τού $\mathbf{Subg}(H)$ και η G/H πληροί τη Σ.Α.Α. επί τού $\mathbf{Subg}(G/H)$, και θεωρήσουμε τυχούσα ανιούσα αλυσίδα

$$K_1 \sqsubseteq K_2 \sqsubseteq \cdots\cdots \sqsubseteq K_i \sqsubseteq K_{i+1} \sqsubseteq K_{i+2} \sqsubseteq \cdots\cdots$$

στοιχείων τού $\mathbf{Subg}(G)$, τότε οι

$$K_1 \cap H \sqsubseteq K_2 \cap H \sqsubseteq \cdots\cdots \sqsubseteq K_i \cap H \sqsubseteq K_{i+1} \cap H \sqsubseteq \cdots\cdots$$
$$K_1H \sqsubseteq K_2H \sqsubseteq \cdots\cdots \sqsubseteq K_iH \sqsubseteq K_{i+1}H \sqsubseteq K_{i+2}H \sqsubseteq \cdots\cdots$$

είναι ανιούσες αλυσίδες στοιχείων των $\mathbf{Subg}(H)$ και $\mathbf{Subg}(G;H)$, αντιστοίχως. (Βλ. πρόταση 4.2.24.) Επειδή η H πληροί (εξ υποθέσεως) τη Σ.Α.Α. επί τού $\mathbf{Subg}(H)$,υπάρχει κάποιος $\nu_1 \in \mathbb{N}$ για τον οποίο ισχύει $K_i \cap H = K_{\nu_1} \cap H$ για κάθε φυσικό αριθμό $i \geq \nu_1$. Επειδή (λόγω τού δευτέρου σκέλους τής υποθέσεώς μας και τής προτάσεως 7.2.5) η G πληροί τη Σ.Α.Α. επί τού $\mathbf{Subg}(G;H)$, υπάρχει κάποιος $\nu_2 \in \mathbb{N}$ για τον οποίο ισχύει $K_iH = K_{\nu_2}H$ για κάθε φυσικό αριθμό $i \geq \nu_2$. Κατά συνέπειαν, από το (ii) τής ασκήσεως **4-3** συμπεραίνουμε ότι

$$[K_i \cap H = K_\nu \cap H \text{ και } K_iH = K_\nu H] \Longrightarrow K_i = K_\nu$$

για κάθε φυσικό αριθμό $i \geq \nu$, όπου $\nu := \max\{\nu_1, \nu_2\}$. Άρα η G πληροί τη Σ.Α.Α. και επί (ολοκλήρου) τού $\mathbf{Subg}(G)$. Η αντίστοιχη απόδειξη με τη Σ.Κ.Α. (στη θέση τής Σ.Α.Α.) είναι παρόμοια. □

7.2.8 Σημείωση. Λόγω τής προτάσεως 7.2.6 η πρόταση 7.2.7 παραμένει εν ισχύ όταν σε αυτήν τα "**Subg**" αντικατασταθούν με "**NSubg**".

7.2.9 Πρόταση. *Το εξωτερικό ευθύ γινόμενο $G_1 \times G_2$ δυο ομάδων G_1, G_2 πληροί τη Σ.Α.Α. (και αντιστοίχως, τη Σ.Κ.Α.) επί τού $\mathbf{Subg}(G_1 \times G_2)$ εάν και μόνον εάν η G_1 πληροί την ίδια συνθήκη επί τού $\mathbf{Subg}(G_1)$ και η G_2 επί τού $\mathbf{Subg}(G_2)$.*

ΑΠΟΔΕΙΞΗ. Εάν η Σ.Α.Α. ικανοποιείται από την G_1 επί τού $\mathbf{Subg}(G_1)$ και από την G_2 επί τού $\mathbf{Subg}(G_2)$, τότε ικανοποιείται και από την $\overline{G}_1 = G_1 \times \{e_{G_2}\}$ επί τού $\mathbf{Subg}(\overline{G}_1)$ και από την $\overline{G}_2 = \{e_{G_2}\} \times G_2$ επί τού $\mathbf{Subg}(\overline{G}_2)$. Επειδή (σύμφωνα με την πρόταση 7.1.2) $(G_1 \times G_2)/\overline{G}_1 \cong G_2 \cong \overline{G}_2$, η $(G_1 \times G_2)/\overline{G}_1$ πληροί την Σ.Α.Α. επί τού $\mathbf{Subg}((G_1 \times G_2)/\overline{G}_1)$. Επειδή όμως και η $\overline{G}_1$ πληροί τη Σ.Α.Α. επί τού $\mathbf{Subg}(\overline{G}_1)$, η πρόταση 7.2.7 μας πληροφορεί ότι και η $G_1 \times G_2$ πληροί τη Σ.Α.Α. επί τού $\mathbf{Subg}(G_1 \times G_2)$. Και αντιστρόφως· εάν υποθέσουμε ότι η $G_1 \times G_2$ πληροί τη Σ.Α.Α. επί τού $\mathbf{Subg}(G_1 \times G_2)$, τότε

$$\mathbf{Subg}(\overline{G}_1) \subseteq \mathbf{Subg}(G_1 \times G_2) \text{ και } \mathbf{Subg}(\overline{G}_2) \subseteq \mathbf{Subg}(G_1 \times G_2),$$

οπότε και η $G_1 \cong \overline{G}_1$ πληροί την ίδια συνθήκη επί τού $\mathbf{Subg}(G_1)$ και η $G_2 \cong \overline{G}_2$ επί τού $\mathbf{Subg}(G_2)$. Η αντίστοιχη απόδειξη με τη Σ.Κ.Α. (στη θέση τής Σ.Α.Α.) είναι παρόμοια. □

7.2.10 Σημείωση. Λόγω τής προτάσεως 7.2.6 η πρόταση 7.2.9 παραμένει εν ισχύ όταν σε αυτήν τα "**Subg**" αντικατασταθούν με "**NSubg**".

7.2.11 Πρόταση. *Κάθε μη τετριμμένη πεπερασμένη ομάδα είναι είτε αφ' εαυτής αναποσυνθέσιμη είτε το εσωτερικό ευθύ γινόμενο πεπερασμένου πλήθους αναποσυνθέσιμων ορθόθετων υποομάδων της.*

ΑΠΟΔΕΙΞΗ. Έστω $(G, \cdot)$ μια πεπερασμένη ομάδα τάξεως $|G| =: n \geq 2$. Θα εφαρμόσουμε τη δεύτερη μορφή τής μαθηματικής επαγωγής ως προς τον n. Εάν $n = 2$, τότε $G \cong \mathbb{Z}_2$ και η G είναι αναποσυνθέσιμη. (Βλ. την πρόταση 2.3.19, το (ii) τού θεωρήματος 2.4.23 και την πρόταση 7.1.34.) Εάν $n \geq 3$, τότε υποθέτουμε ότι ο ισχυρισμός είναι αληθής για όλες τις μη τετριμμένες πεπερασμένες ομάδες τάξεως $< n$. Εάν η G είναι αφ' εαυτής αναποσυνθέσιμη, τότε σταματούμε. Εάν η G είναι αποσυνθέσιμη, τότε υπάρχουν μη τετριμμένες γνήσιες ορθόθετες υποομάδες της H και K, ούτως ώστε να ισχύει $G = H \times_{\text{εσ.}} K$. Εν τοιαύτη περιπτώσει, $2 \leq |H| < n$ και $2 \leq |K| < n$, οπότε υπάρχουν $k, l \in \mathbb{N}$, $k < l$, και μη τετριμμένες αναποσυνθέσιμες ορθόθετες υποομάδες $G_1, ..., G_k$ τής H και $G_{k+1}, ..., G_l$ τής K, τέτοιες ώστε να ισχύει $H = G_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} G_k$ και $K = G_{k+1} \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} G_l$. Σύμφωνα με το (i) τής προτάσεως 7.1.39 οι $G_1, ..., G_l$ είναι ορθόθετες υποομάδες *τής* G. Προφανώς,

$$G = (G_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} G_k) \times_{\text{εσ.}} (G_{k+1} \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} G_l) = \prod_{i=1}^{l}{}^{\text{εσ.}} G_i$$

και ο ισχυρισμός είναι αληθής και για την ίδια την G. □

Η πρόταση 7.2.11 γενικεύεται ως ακολούθως:

7.2.12 Θεώρημα. *Εάν μια μη τετριμμένη ομάδα $(G, \cdot)$ πληροί είτε τη Σ.Α.Α. είτε τη Σ.Κ.Α. επί τού* $\mathbf{NSubg}(G)$*, τότε η G είναι είτε αφ' εαυτής αναποσυνθέσιμη είτε το εσωτερικό ευθύ γινόμενο πεπερασμένου πλήθους αναποσυνθέσιμων ορθόθετων υποομάδων της.*

ΑΠΟΔΕΙΞΗ. Θα χρησιμοποιήσουμε «εις άτοπον απαγωγή». Υποθέτουμε ότι η G πληροί (τουλάχιστον) μία εξ αυτών των συνθηκών και δεν είναι ούτε αφ' εαυτής αναποσυνθέσιμη ούτε το εσωτερικό ευθύ γινόμενο πεπερασμένου πλήθους αναποσυνθέσιμων ορθόθετων υποομάδων της. Θεωρούμε το σύνολο

$$\mathfrak{U} := \left\{ H \in \mathbf{NSubg}(G) \;\middle|\; \begin{array}{l} \exists J_H \in \mathbf{NSubg}(G) : G = H \times_{\text{εσ.}} J_H \\ \text{και η } H \text{ δεν είναι ούτε αφ' εαυτής} \\ \text{αναποσυνθέσιμη ούτε το εσωτερικό ευθύ} \\ \text{γινόμενο πεπερασμένου πλήθους αναπο-} \\ \text{συνθέσιμων ορθόθετων υποομάδων τής } G \end{array} \right\}.$$

Εξ υποθέσεως[36], $G \in \mathfrak{U}$, οπότε $\mathfrak{U} \neq \varnothing$. Έστω τώρα *τυχούσα* $H \in \mathfrak{U}$. Η ομάδα H είναι αποσυνθέσιμη, οπότε υπάρχουν $K_H, L_H \in \mathbf{NSubg}(H) \setminus \{\{e_G\}, H\}$, τέτοιες ώστε να ισχύει

$$H = K_H \times_{\text{εσ.}} L_H \;\; (= L_H \times_{\text{εσ.}} K_H)\,. \tag{7.32}$$

[36] Αρκεί να θέσουμε $J_G := \{e_G\}$.

Σύμφωνα με το (i) τής προτάσεως 7.1.39, $K_H \trianglelefteq G$ και $L_H \trianglelefteq G$. Θέτοντας

$$\Gamma_H := \left\{ N \in \mathfrak{U} \;\middle|\; \begin{array}{l} N \in \mathbf{NSubg}(H) \text{ που δεν είναι ούτε} \\ \text{αφ' εαυτής αναποσυνθέσιμη ούτε το} \\ \text{εσωτερικό ευθύ γινόμενο πεπερασμένου} \\ \text{πλήθους αναποσυνθέσιμων} \\ \text{ορθόθετων υποομάδων τής } G \end{array} \right\}$$

παρατηρούμε ότι $\Gamma_H \neq \varnothing$, διότι είτε $K_H \in \Gamma_H$ είτε $L_H \in \Gamma_H$. (Πράγματι· εάν αμφότερες οι K_H και L_H δεν ανήκαν στο Γ_H, τότε αυτές θα ήταν αναποσυνθέσιμες ή εσωτερικά ευθέα γινόμενα πεπερασμένου πλήθους αναποσυνθέσιμων ορθόθετων υποομάδων τής G, κάτι που θα αντέκειτο στην υπόθεσή μας ότι $H \in \mathfrak{U}$.) Σύμφωνα με το αξίωμα τής επιλογής, $(\Gamma_H \neq \varnothing,\ \forall H \in \mathfrak{U}) \Rightarrow \prod\limits_{H\in\mathfrak{U}} \Gamma_H \neq \varnothing$, οπότε υπάρχει μια απεικόνιση

$$f : \mathfrak{U} \longrightarrow \bigcup_{H\in\mathfrak{U}} \Gamma_H, \quad \text{με } f(H) \in \Gamma_H,\ \forall H \in \mathfrak{U}.$$

Λόγω τής (7.32) μπορούμε δίχως βλάβη τής γενικότητας να υποθέσουμε ότι ισχύει $f(H) = K_H, \forall H \in \mathfrak{U}$, και να ορίσουμε μια αναδρομική απεικόνιση $\mathfrak{t} : \mathbb{N} \longrightarrow \mathfrak{U}$ μέσω των τύπων

$$\mathfrak{t}(1) := G_1 := G, \qquad \mathfrak{t}(i+1) := f(\mathfrak{t}(i)) =: K_{\mathfrak{t}(i)} =: G_{i+1}, \ \ \forall i \in \mathbb{N},$$

όπου $G_i = K_{G_i} \times_{\text{εσ.}} L_{G_i}, \forall i \in \mathbb{N}$. Κατ' αυτόν τον τρόπο σχηματίζεται μια κατιούσα *μη στάσιμη* αλυσίδα

$$\cdots\cdots \sqsubset G_{i+2} \sqsubset G_{i+1} \sqsubset G_i \sqsubset \cdots\cdots \sqsubset G_2 \sqsubset G_1 := G$$

στοιχείων τού $\mathbf{NSubg}(G)$. Ως εκ τούτου, η G δεν μπορεί να πληροί τη Σ.Κ.Α. επί τού $\mathbf{NSubg}(G)$. Όμως η G δεν μπορεί να πληροί *ούτε* τη Σ.Α.Α. επί τού $\mathbf{NSubg}(G)$, διότι

$$\begin{aligned} G = G_1 &= K_{G_1} \times_{\text{εσ.}} L_{G_1} = G_2 \times_{\text{εσ.}} L_{G_1} = K_{G_2} \times_{\text{εσ.}} L_{G_2} \times_{\text{εσ.}} L_{G_1} \\ &= G_3 \times_{\text{εσ.}} L_{G_2} \times_{\text{εσ.}} L_{G_1} = K_{G_3} \times_{\text{εσ.}} L_{G_3} \times_{\text{εσ.}} L_{G_2} \times_{\text{εσ.}} L_{G_1} \\ &= G_4 \times_{\text{εσ.}} L_{G_3} \times_{\text{εσ.}} L_{G_2} \times_{\text{εσ.}} L_{G_1} = \cdots\cdots, \end{aligned}$$

και, κατ' επέκταση,

$$G = G_{i+1} \times_{\text{εσ.}} L_{G_i} \times_{\text{εσ.}} L_{G_{i-1}} \times_{\text{εσ.}} \cdots\cdots \times_{\text{εσ.}} L_{G_2} \times_{\text{εσ.}} L_{G_1} \tag{7.33}$$

και δημιουργείται μια ανιούσα *μη στάσιμη* αλυσίδα[37]

$$L_{G_1} \sqsubset L_{G_2} \times L_{G_1} \sqsubset \cdots\cdots \sqsubset L_{G_i} \times \cdots \times L_{G_1} \sqsubset L_{G_{i+1}} \times \cdots \times L_{G_1} \sqsubset \cdots\cdots$$

στοιχείων τού $\mathbf{NSubg}(G)$. Άτοπο! □

[37] Εννοείται ότι ταυτίζουμε την $L_{G_j} \times \cdots \times L_{G_1}$ με την υποομάδα $\underbrace{\{e_G\} \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} \{e_G\}}_{i-j+1 \text{ φορές}} \times_{\text{εσ.}} L_{G_j} \times \cdots \times_{\text{εσ.}} L_{G_1}$ τής (7.33) για κάθε $j \leq i$.

7.2.13 Λήμμα. *Εάν $(G,\cdot)$ είναι μια ομάδα που πληροί τη Σ.Α.Α. επί τού $\mathbf{NSubg}(G)$ και $f \in \mathrm{End}(G)$, τότε*

$$f \in \mathrm{Aut}(G) \iff \text{ο } f \text{ είναι επιμορφισμός.}$$

ΑΠΟΔΕΙΞΗ. Η "$\Rightarrow$" είναι προφανής. Για την "$\Leftarrow$" αρκεί να αποδείξουμε ότι ο f είναι και μονομορφισμός. Προς τούτο θεωρούμε την ανιούσα αλυσίδα

$$\{e_G\} \sqsubseteq \mathrm{Ker}(f) \sqsubseteq \mathrm{Ker}(f^2) \sqsubseteq \cdots\cdots \sqsubseteq \mathrm{Ker}(f^i) \sqsubseteq \mathrm{Ker}(f^{i+1}) \sqsubseteq \cdots\cdots \tag{7.34}$$

στοιχείων τού $\mathbf{NSubg}(G)$. Αυτή οφείλει να είναι στάσιμη. Επομένως, $\exists \nu \in \mathbb{N}$: $\mathrm{Ker}(f^\nu) = \mathrm{Ker}(f^{\nu+1})$. Προφανώς,

$$\mathrm{Im}(f) = G \Rightarrow \mathrm{Im}(f^2) = f^2(G) = f(\mathrm{Im}(G)) = f(G) = \mathrm{Im}(f) = G$$

και, κατ' επέκταση, $\mathrm{Im}(f^\nu) = f^\nu(G) = f^{\nu-1}(\mathrm{Im}(G)) = \cdots = f(G) = \mathrm{Im}(f) = G$. Εάν $y \in \mathrm{Ker}(f)$, τότε $f(y) = e_G$ και $\exists x \in G : y = f^\nu(x)$. Κατά συνέπειαν,

$$e_G = f(y) = f^{\nu+1}(x) \Rightarrow x \in \mathrm{Ker}(f^{\nu+1}) = \mathrm{Ker}(f^\nu) \Rightarrow y = f^\nu(x) = e_G,$$

πράγμα που σημαίνει ότι $\mathrm{Ker}(f) = \{e_G\}$, ήτοι ότι ο f είναι μονομορφισμός. (Βλ. πρόταση 2.4.15.) □

7.2.14 Λήμμα. *Εάν $(G,\cdot)$ είναι μια ομάδα που πληροί τη Σ.Κ.Α. επί τού $\mathbf{NSubg}(G)$ και ο f είναι ένας ορθόθετος ενδομορφισμός τής G* (βλ. 7.1.35)*, τότε*

$$f \in \mathrm{Aut}(G) \iff \text{ο } f \text{ είναι μονομορφισμός.}$$

ΑΠΟΔΕΙΞΗ. Η "$\Rightarrow$" είναι προφανής. Για την "$\Leftarrow$" αρκεί να αποδείξουμε ότι ο f είναι και επιμορφισμός. Επειδή ο f είναι ορθόθετος ενδομορφισμός τής G, για οιαδήποτε $g, x \in G$ και οιονδήποτε $i \in \mathbb{N}$ έχουμε

$$gf^i(x)g^{-1} = gf(f^{i-1}(x))g^{-1} = f(gf^{i-1}(x)g^{-1}) = \cdots = f^i(gxg^{-1}) \in \mathrm{Im}(f^i),$$

οπότε $\mathrm{Im}(f^i) \trianglelefteq G$. Θεωρούμε την ανιούσα αλυσίδα στοιχείων τού $\mathbf{NSubg}(G)$

$$\cdots\cdots \sqsubseteq \mathrm{Im}(f^{i+1}) \sqsubseteq \mathrm{Im}(f^i) \sqsubseteq \cdots\cdots \sqsubseteq \mathrm{Im}(f^2) \sqsubseteq \mathrm{Im}(f) \sqsubseteq G. \tag{7.35}$$

Αυτή οφείλει να είναι στάσιμη. Άρα $\exists \nu \in \mathbb{N} : \mathrm{Im}(f^\nu) = \mathrm{Im}(f^{\nu+1})$. Έστω *τυχόν* $y \in G$. Προφανώς, $\exists x \in G : f^\nu(y) = f^{\nu+1}(x)$. Εξάλλου, για κάθε $z \in \mathrm{Ker}(f^\nu)$,

$$\begin{aligned}
&e_G = f^\nu(z) = f(f^{\nu-1}(z)) \Rightarrow f^{\nu-1}(z) \in \mathrm{Ker}(f) \underset{\mathrm{Ker}(f)=\{e_G\}}{\Longrightarrow} f^{\nu-1}(z) = e_G \\
&\Rightarrow e_G = f^{\nu-1}(z) = f(f^{\nu-2}(z)) \Rightarrow f^{\nu-2}(z) \in \mathrm{Ker}(f) \underset{\mathrm{Ker}(f)=\{e_G\}}{\Longrightarrow} f^{\nu-2}(z) = e_G \\
&\Longrightarrow \cdots \Longrightarrow f(z) = e_G \Rightarrow z \in \mathrm{Ker}(f) \underset{\mathrm{Ker}(f)=\{e_G\}}{\Longrightarrow} z = e_G.
\end{aligned}$$

Ως εκ τούτου, $\mathrm{Ker}(f^\nu) = \{e_G\} \underset{2.4.15}{\Longrightarrow}$ ο f^ν είναι μονομορφισμός και

$$f^\nu(y) = f^{\nu+1}(x) = f^\nu(f(x)) \Rightarrow y = f(x).$$

Άρα ο f είναι όντως επιμορφισμός. □

7.2.15 Ορισμός. Λέμε ότι ένας ενδομορφισμός f μιας ομάδας $(G,\cdot)$ είναι **μηδενοδύναμος ενδομορφισμός** όταν υπάρχει κάποιος $\kappa\in\mathbb{N}$, τέτοιος ώστε να ισχύει $f^{\kappa}(g)=e_G$ για κάθε $g\in G$.

7.2.16 Θεώρημα. (Λήμμα τού Fitting, 1934) *Εάν $(G,\cdot)$ είναι μια ομάδα που πληροί τόσον τη Σ.Α.Α. όσον και τη Σ.Κ.Α. επί τού* $\mathbf{NSubg}(G)$, *και f ένας ορθόθετος ενδομορφισμός της, τότε ισχύουν τα εξής*:

(i) *Υπάρχει κάποιος $\nu\in\mathbb{N}$, τέτοιος ώστε*

$$\boxed{G=\mathrm{Ker}(f^{\nu})\times_{\text{εσ.}}\mathrm{Im}(f^{\nu}).}$$

(ii) *Οι ομάδες* $\mathrm{Ker}(f^{\nu})$ *και* $\mathrm{Im}(f^{\nu})$ *είναι f-αναλλοίωτες*[38].

(iii) *Ο* $f|_{\mathrm{Ker}(f^{\nu})}\in\mathrm{End}(\mathrm{Ker}(f^{\nu}))$ *είναι μηδενοδύναμος και ο* $f|_{\mathrm{Im}(f^{\nu})}\in\mathrm{End}(\mathrm{Im}(f^{\nu}))$ *επιρριπτικός ενδομορφισμός.*

ΑΠΟΔΕΙΞΗ[39]. (i) Ως γνωστόν, $\mathrm{Im}(f^{i})\trianglelefteq G$, $\forall i\in\mathbb{N}$, και οι αλυσίδες (7.34) και (7.35) οφείλουν να είναι στάσιμες. Άρα υπάρχουν $\nu_1,\nu_2\in\mathbb{N}$, τέτοιοι ώστε να ισχύει $\mathrm{Ker}(f^{j})=\mathrm{Ker}(f^{\nu_1})$ για κάθε φυσικό αριθμό $j\geq\nu_1$ και $\mathrm{Im}(f^{k})=\mathrm{Im}(f^{\nu_2})$ για κάθε φυσικό αριθμό $k\geq\nu_2$. Θέτοντας $\nu:=\max\{\nu_1,\nu_2\}$ παρατηρούμε ότι

$$\mathrm{Ker}(f^{i})=\mathrm{Ker}(f^{\nu})\ \text{ και }\ \mathrm{Im}(f^{i})=\mathrm{Im}(f^{\nu}) \tag{7.36}$$

για κάθε φυσικό αριθμό $i\geq\nu$. Έστω τυχόν $y\in\mathrm{Ker}(f^{\nu})\cap\mathrm{Im}(f^{\nu})$. Προφανώς, $y=f^{\nu}(x)$ για κάποιο $x\in G$ και

$$f^{2\nu}(x)=f^{\nu}(f^{\nu}(x))=f^{\nu}(y)=e_G\Rightarrow x\in\mathrm{Ker}(f^{2\nu})\underset{(7.36)}{=}\mathrm{Ker}(f^{\nu})\Rightarrow e_G=f^{\nu}(x)=y.$$

Επομένως, $\mathrm{Ker}(f^{\nu})\cap\mathrm{Im}(f^{\nu})=\{e_G\}$. Από την άλλη μεριά, για κάθε $w\in G$ έχουμε

$$f^{\nu}(w)\in\mathrm{Im}(f^{\nu})\underset{(7.36)}{=}\mathrm{Im}(f^{2\nu})\Rightarrow\exists z\in G:f^{\nu}(w)=f^{2\nu}(z),$$

οπότε $f^{\nu}(wf^{\nu}(z^{-1}))=f^{\nu}(w)f^{2\nu}(z^{-1})=f^{\nu}(w)f^{2\nu}(z)^{-1}=f^{\nu}(w)f^{\nu}(w)^{-1}=e_G$ και

$$w=(\underbrace{wf^{\nu}(z^{-1})}_{\in\mathrm{Ker}(f^{\nu})})(\underbrace{f^{\nu}(z)}_{\in\mathrm{Im}(f^{\nu})}).$$

Άρα $G=(\mathrm{Ker}(f^{\nu}))(\mathrm{Im}(f^{\nu}))$ και, ως εκ τούτου, $G=\mathrm{Ker}(f^{\nu})\times_{\text{εσ.}}\mathrm{Im}(f^{\nu})$.

(ii) Τούτο είναι προφανές, διότι αφ' ενός μεν για κάθε $x\in\mathrm{Ker}(f^{\nu})$ έχουμε

$$f^{\nu}(f(x))=f(f^{\nu}(x))=f(e_G)=e_G\Rightarrow f(x)\in\mathrm{Ker}(f^{\nu}),$$

[38] Αυτό σημαίνει ότι η εικόνα τού πυρήνα $\mathrm{Ker}(f^{\nu})$ (και αντιστοίχως, τής $\mathrm{Im}(f^{\nu})$) μέσω τού f είναι υποομάδα τού $\mathrm{Ker}(f^{\nu})$ (και αντιστοίχως, τής $\mathrm{Im}(f^{\nu})$).

[39] Βλ. H. Fitting: *Über die direkten Produktzerlegungen einer Gruppe in direkt unzerlegbare Faktoren*, Math. Zeitschrift **39** (1934), 16-30.

αφ' ετέρου δε για κάθε $y \in \mathrm{Im}(f^\nu)$ υπάρχει $x \in G : y = f^\nu(x)$, οπότε

$$f(y) = f(f^\nu(x)) = f^\nu(f(x)) \in \mathrm{Im}(f^\nu).$$

(iii) Επειδή $f^\nu(x) = e_G$ για κάθε $x \in \mathrm{Ker}(f^\nu)$, ο $(f|_{\mathrm{Ker}(f^\nu)})^\nu$ είναι ο τετριμμένος ενδομορφισμός (ο απεικονίζων όλα τα στοιχεία τού πυρήνα $\mathrm{Ker}(f^\nu)$ στο e_G). Άρα ο $f|_{\mathrm{Ker}(f^\nu)}$ είναι μηδενοδύναμος ενδομορφισμός τού $\mathrm{Ker}(f^\nu)$. Εξάλλου,

$$\begin{aligned}&\mathrm{Im}(f|_{\mathrm{Im}(f^\nu)}) = f|_{\mathrm{Im}(f^\nu)}(\mathrm{Im}(f^\nu)) = f(\mathrm{Im}(f^\nu)) = f(f^\nu(G))\\ &= f^{\nu+1}(G) = \mathrm{Im}(f^{\nu+1}) \underset{(7.36)}{=} \mathrm{Im}(f^\nu),\end{aligned}$$

οπότε ο $f|_{\mathrm{Im}(f^\nu)}$ είναι επιρριπτικός ενδομορφισμός τής $\mathrm{Im}(f^\nu)$. □

7.2.17 Πόρισμα. *Εάν $(G,\cdot)$ είναι μια αναποσυνθέσιμη ομάδα που πληροί τόσον τη Σ.Α.Α. όσον και τη Σ.Κ.Α. επί τού $\mathbf{NSubg}(G)$, και f ένας ορθόθετος ενδομορφισμός της, τότε ο f είναι είτε μηδενοδύναμος είτε αυτομορφισμός.*

ΑΠΟΔΕΙΞΗ. Από το λήμμα τού Fitting γνωρίζουμε ότι υπάρχει κάποιος $\nu \in \mathbb{N}$, τέτοιος ώστε να ισχύει $G = \mathrm{Ker}(f^\nu) \times_{\text{εσ.}} \mathrm{Im}(f^\nu)$, όπου ο $f|_{\mathrm{Ker}(f^\nu)}$ είναι μηδενοδύναμος ενδομορφισμός τού $\mathrm{Ker}(f^\nu)$ και ο $f|_{\mathrm{Im}(f^\nu)}$ επιρριπτικός ενδομορφισμός τής $\mathrm{Im}(f^\nu)$. Επειδή η G είναι αναποσυνθέσιμη, έχουμε είτε $\mathrm{Im}(f^\nu) = \{e_G\}$ είτε $\mathrm{Ker}(f^\nu) = \{e_G\}$. Στην πρώτη περίπτωση ο $f = f|_{\mathrm{Ker}(f^\nu)}$ είναι μηδενοδύναμος. Στη δεύτερη περίπτωση ο $f = f|_{\mathrm{Im}(f^\nu)}$ είναι επιρριπτικός ενδομορφισμός, οπότε είναι αυτομορφισμός δυνάμει τού λήμματος 7.2.13. □

7.2.18 Σημείωση. Έστω $(G,\cdot)$ μια ομάδα. Είθισται να χρησιμοποιείται ο *προσθετικός συμβολισμός*

$$G^G \times G^G \ni (f_1, f_2) \longmapsto f_1 + f_2 \in G^G$$

για την πράξη μέσω τής οποίας το σύνολο G^G των απεικονίσεων $f : G \to G$ καθίσταται (κατά τρόπο φυσικό) ομάδα, όπου

$$(f_1 + f_2)(x) := f_1(x) f_2(x),\ \forall x \in G.$$

(Πρβλ. 7.1.94 (ii).) Το ουδέτερο στοιχείο 0_{G^G} αυτής τής πράξεως είναι ο *τετριμμένος ενδομορφισμός* τής G (ο απεικονίζων κάθε στοιχείο τής G στο e_G). Εάν η G είναι αβελιανή και αμφότερες οι f_1, f_2 είναι ενδομορφισμοί τής G, τότε η $f_1 + f_2$ είναι ενδομορφισμός αυτής και το ζεύγος $(\mathrm{End}(G), +)$ υποομάδα τής $\left(G^G, +\right)$. (Πρβλ. 2.4.13 (ii).) Όταν η G είναι μη αβελιανή, τούτο παύει να ισχύει. Επί παραδείγματι, όταν $G := \mathfrak{S}_3$ και $f_1 := \boldsymbol{\gamma}_{\tau_1}$, $f_2 := \boldsymbol{\gamma}_{\tau_2}$, οι εσωτερικοί αυτομορφισμοί

$$\mathfrak{S}_3 \ni \sigma \mapsto \boldsymbol{\gamma}_{\tau_i}(\sigma) := \sigma \circ \tau_i \circ \sigma^{-1} \in \mathfrak{S}_3,\ \ i \in \{1,2\},$$

όπου $\tau_1 := [1\,2\,3]$, $\tau_2 := [1\,3\,2] = \tau_1^{-1}$, τότε $\boldsymbol{\gamma}_{\tau_1} + \boldsymbol{\gamma}_{\tau_2} \notin \mathrm{End}(\mathfrak{S}_3)$, διότι έχουμε αφ' ενός μεν

$$(\boldsymbol{\gamma}_{\tau_1} + \boldsymbol{\gamma}_{\tau_2})([1\,3]^2) = (\boldsymbol{\gamma}_{\tau_1} + \boldsymbol{\gamma}_{\tau_2})(\mathrm{id}) = \boldsymbol{\gamma}_{\tau_1}(\mathrm{id}) \circ \boldsymbol{\gamma}_{\tau_2}(\mathrm{id}) = \mathrm{id},$$

αφ' ετέρου δε (σύμφωνα με τον κατάλογο 3.2.2 τής πράξεως "$\circ$" τής $\mathfrak{S}_3$)

$$((\boldsymbol{\gamma}_{\tau_1}+\boldsymbol{\gamma}_{\tau_2})([1\,3]))^2=(\boldsymbol{\gamma}_{\tau_1}([1\,3])\circ\boldsymbol{\gamma}_{\tau_2}([1\,3]))^2$$
$$=(\tau_1\circ[1\,3]\circ\tau_2\circ\tau_2\circ[1\,3]\circ\tau_1)^2=([1\,2]\circ[2\,3])^2=\tau_1^2=\tau_2\neq\mathrm{id}.$$

7.2.19 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα. Εάν $f_1,f_2\in\mathrm{End}(G)$, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) $f_1+f_2\in\mathrm{End}(G)$.

(ii) $y_1y_2=y_2y_1,\ \forall(y_1,y_2)\in\mathrm{Im}(f_1)\times\mathrm{Im}(f_2)$.

(iii) $[\mathrm{Im}(f_1),\mathrm{Im}(f_2)]=\{e_G\}$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν $(y_1,y_2)\in\mathrm{Im}(f_1)\times\mathrm{Im}(f_2)$, τότε υπάρχει $(x_1,x_2)\in G\times G$, τέτοιο ώστε να ισχύει $y_1=f_1(x_1)$ και $y_2=f_2(x_2)$. Εξ υποθέσεως,

$$f_1(x_2)f_1(x_1)f_2(x_2)f_2(x_1)=f_1(x_2x_1)f_2(x_2x_1)=(f_1+f_2)(x_2x_1)$$
$$=(f_1+f_2)(x_2)(f_1+f_2)(x_1)=f_1(x_2)f_2(x_2)f_1(x_1)f_2(x_1),$$

οπότε οι νόμοι 2.1.9 (i) τής διαγραφής δίδουν

$$y_1y_2=f_1(x_1)f_2(x_2)=f_2(x_2)f_1(x_1)=y_2y_1.$$

(ii)⇒(i) Έστω τυχόν ζεύγος $(x_1,x_2)\in G\times G$. Επειδή $f_1(x_1)f_2(x_2)=f_2(x_2)f_1(x_1)$, έχουμε $(f_1+f_2)(x_2x_1)=(f_1+f_2)(x_2)(f_1+f_2)(x_1)$, οπότε $f_1+f_2\in\mathrm{End}(G)$. Η αμφίπλευρη συνεπαγωγή (ii)⇔(iii) είναι προφανής. □

7.2.20 Σημείωση. (i) Όταν ισχύει $f_1+f_2\in\mathrm{End}(G)$, τότε $f_1+f_2=f_2+f_1$, ενώ για κάθε $f_3\in\mathrm{End}(G)$ έχουμε $f_1\circ f_3+f_2\circ f_3=(f_1+f_2)\circ f_3\in\mathrm{End}(G)$ και, αντιστοίχως, $f_3\circ f_1+f_3\circ f_2=f_3\circ(f_1+f_2)\in\mathrm{End}(G)$.

(ii) Γενικότερα, εάν $s\in\mathbb{N}$, $s\geq 2$, και $f_1,...,f_s$ είναι ενδομορφισμοί τής G, τέτοιοι ώστε να ισχύει $f_i+f_j\in\mathrm{End}(G)$ για οιουσδήποτε $i,j\in\{1,...,s\}$, $i\neq j$, τότε η απεικόνιση

$$\sum_{i=1}^{s}f_i\in G^G,\ \ \left(\sum_{i=1}^{s}f_i\right)(x):=f_1(x)\cdots f_s(x),\ \forall x\in G,$$

αποτελεί έναν ενδομορφισμό τής G και για κάθε $t\in\{1,...,s-1\}$ ισχύει

$$\sum_{i=1}^{s}f_i=\left(\sum_{i=1}^{t}f_i\right)+\left(\sum_{i=t+1}^{s}f_i\right).$$

7.2.21 Λήμμα. *Εάν f_1,f_2 είναι δυο ορθόθετοι ενδομορφισμοί μιας ομάδας $(G,\cdot)$, τέτοιοι ώστε $f_1+f_2\in\mathrm{End}(G)$,τότε και ο f_1+f_2 είναι ορθόθετος.*

ΑΠΟΔΕΙΞΗ. Για κάθε $g\in G$ έχουμε

$$\boldsymbol{\gamma}_g\circ(f_1+f_2)=\boldsymbol{\gamma}_g\circ f_1+\boldsymbol{\gamma}_g\circ f_2=f_1\circ\boldsymbol{\gamma}_g+f_2\circ\boldsymbol{\gamma}_g=(f_1+f_2)\circ\boldsymbol{\gamma}_g,$$

οπότε ο f_1+f_2 είναι όντως ορθόθετος. □

7.2.22 Λήμμα. *Έστω $(G,\cdot)$ μια αναποσυνθέσιμη ομάδα που πληροί τόσον τη Σ.Α.Α. όσον και τη Σ.Κ.Α. επί τού* $\mathbf{NSubg}(G)$. *Εάν f_1, f_2 είναι δυο ορθόθετοι ενδομορφισμοί τής G, τέτοιοι ώστε $f_1+f_2 \in \mathrm{Aut}(G)$, τότε είτε $f_1 \in \mathrm{Aut}(G)$ είτε $f_2 \in \mathrm{Aut}(G)$.*

ΑΠΟΔΕΙΞΗ. Επειδή ο f_1+f_2 (βάσει τού λήμματος 7.2.21) είναι *ορθόθετος* αυτομορφισμός τής G, τόσον ο $(f_1+f_2)^{-1}$ όσον και οι $\widetilde{f}_1 := (f_1+f_2)^{-1}\circ f_1$, $\widetilde{f}_2 := (f_1+f_2)^{-1}\circ f_2 \in \mathrm{End}(G)$ είναι ορθόθετοι (δυνάμει των προτάσεων 7.1.36 και 7.1.37). Σημειωτέον ότι $\widetilde{f}_1+\widetilde{f}_2 = (f_1+f_2)^{-1}\circ(f_1+f_2) = \mathrm{id}_G$ και ότι για κάθε $x \in G$ ισχύει

$$(\widetilde{f}_1\circ\widetilde{f}_2)(x) = \widetilde{f}_1(\widetilde{f}_2(x)) = \widetilde{f}_1(\widetilde{f}_1(x^{-1})\widetilde{f}_1(x)\widetilde{f}_2(x)) = \widetilde{f}_1(\widetilde{f}_1(x^{-1})(\widetilde{f}_1+\widetilde{f}_2)(x))$$
$$= \widetilde{f}_1(\widetilde{f}_1(x^{-1})\,\mathrm{id}_G(x)) = \widetilde{f}_1(\widetilde{f}_1(x^{-1})x) = \widetilde{f}_1(\widetilde{f}_1(x^{-1}))\widetilde{f}_1(x) = \widetilde{f}_1(\widetilde{f}_1(x^{-1}))\,\mathrm{id}_G(\widetilde{f}_1(x))$$
$$= \widetilde{f}_1(\widetilde{f}_1(x^{-1}))\,(\widetilde{f}_1+\widetilde{f}_2)(\widetilde{f}_1(x)) = \widetilde{f}_1(\widetilde{f}_1(x^{-1}))\widetilde{f}_1(\widetilde{f}_1(x))(\,\widetilde{f}_2(\widetilde{f}_1(x)))$$
$$= \widetilde{f}_2(\widetilde{f}_1(x)) = (\widetilde{f}_2\circ\widetilde{f}_1)(x),$$

οπότε $\widetilde{f}_1\circ\widetilde{f}_2 = \widetilde{f}_2\circ\widetilde{f}_1$. Ας υποθέσουμε ότι κανείς εκ των $\widetilde{f}_1, \widetilde{f}_2$ δεν είναι αυτομορφισμός τής G. Τότε αμφότεροι οι $\widetilde{f}_1, \widetilde{f}_2$ είναι μηδενοδύναμοι ενδομορφισμοί τής G (βάσει τού πορίσματος 7.2.17). Αυτό σημαίνει ότι υπάρχουν $\nu_1, \nu_2 \in \mathbb{N}$, τέτοιοι ώστε $\widetilde{f}_1^{\nu_1} = 0_{G^G}$ και $\widetilde{f}_2^{\nu_2} = 0_{G^G}$. Επομένως, $\widetilde{f}_1^{\nu} = 0_{G^G} = \widetilde{f}_2^{\nu}$, όπου $\nu := \max\{\nu_1,\nu_2\}$, και[40]

$$\mathrm{id}_G = \mathrm{id}_G^{2\nu} = (\widetilde{f}_1+\widetilde{f}_2)^{2\nu} = \sum_{j=0}^{2\nu}\tbinom{2\nu}{j}(\widetilde{f}_1)^j\circ(\widetilde{f}_2)^{2\nu-j} = 0_{G^G},$$

διότι $(\widetilde{f}_1)^j = 0_{G^G}$, $\forall j \in \{\nu,...,2\nu\}$, και $(\widetilde{f}_2)^{2\nu-j} = 0_{G^G}$, $\forall j \in \{1,...,\nu\}$. Τούτο αντίκειται στο ότι η G δεν είναι τετριμμένη. Άρα είτε $\widetilde{f}_1 \in \mathrm{Aut}(G)$ είτε $\widetilde{f}_2 \in \mathrm{Aut}(G)$ και, κατ' επέκταση, είτε $f_1 \in \mathrm{Aut}(G)$ είτε $f_2 \in \mathrm{Aut}(G)$. □

7.2.23 Συμβολισμός. Έστω ότι $s \in \mathbb{N}$, $s \geq 2$, και ότι οι $H_1,...,H_s$ είναι s ορθόθετες υποομάδες μιας ομάδας $(G,\cdot)$, τέτοιες ώστε να ισχύει $G = H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_s$. Για κάθε $i \in \{1,...,s\}$ συμβολίζουμε ως $\eta_i^{H_1,...,H_s} : G \longrightarrow G$ τον ενδομορφισμό τής G τον οριζόμενο μέσω τού τύπου

$$\boxed{\eta_i^{H_1,...,H_s}(h_1h_2\cdots h_s) := h_i}$$

όπου $h_1 \in H_1, ..., h_s \in H_s$, ήτοι τη σύνθεση

$$\boxed{\eta_i^{H_1,...,H_s} := \mathrm{id}_G|_{H_i}\circ\mathrm{pr}_i\circ f^{-1}_{H_1,...,H_s}}$$

τής εμφυτεύσεως $\mathrm{id}_G|_{H_i} : H_i \hookrightarrow G$, τής i-οστής φυσικής προβολής

$$\mathrm{pr}_i : H_1\times\cdots\times H_s \longrightarrow H_i$$

και τού αντιστρόφου τού ισομορφισμού

$$H_1\times\cdots\times H_s \ni (h_1,h_2,...,h_s) \underset{f_{H_1,...,H_s}}{\longmapsto} h_1h_2\cdots h_s \in G.$$

(Βλ. (7.28) και 7.1.85 (ii).)

[40] Η τρίτη ισότητα αποδεικνύεται επαγωγικώς κάνοντας χρήση τής $\widetilde{f}_1\circ\widetilde{f}_2 = \widetilde{f}_2\circ\widetilde{f}_1$.

7.2.24 Λήμμα. *Έστω ότι $s \in \mathbb{N}$, $s \geq 2$, και ότι οι $H_1,...,H_s$ είναι s ορθόθετες υποομάδες μιας ομάδας $(G,\cdot)$, τέτοιες ώστε $G = H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_s$. Ο ενδομορφισμός $\eta_i := \eta_i^{H_1,...,H_s}$ της G είναι ορθόθετος για κάθε $i \in \{1,...,s\}$ και $\eta_i + \eta_j \in \text{End}(G)$ για οιουσδήποτε $i,j \in \{1,...,s\}$, $i \neq j$. Επιπροσθέτως, για $i,j \in \{1,...,s\}$,*

$$\eta_i \circ \eta_j = \begin{cases} 0_{G^G}, & \text{όταν } i \neq j, \\ \eta_i, & \text{όταν } i = j, \end{cases}$$

και $\sum_{i=1}^{s} \eta_i = \text{id}_G$.

ΑΠΟΔΕΙΞΗ. Εάν $g \in G$ και $h_1 \in H_1,...,h_s \in H_s$, τότε για κάθε $i \in \{1,...,s\}$ έχουμε

$$\begin{aligned} \eta_i(g(h_1h_2\cdots h_s)g^{-1}) &= \eta_i((\underbrace{gh_1g^{-1}}_{\in H_1})(\underbrace{gh_2g^{-1}}_{\in H_2})\cdots(\underbrace{gh_sg^{-1}}_{\in H_s})) \\ &= gh_ig^{-1} = g(\eta_i(h_1h_2\cdots h_s))g^{-1}, \end{aligned}$$

οπότε ο ενδομορφισμός η_i είναι ορθόθετος. Για οιουσδήποτε $i,j \in \{1,...,s\}$, $i \neq j$, ισχύει $\eta_i(G) = H_i$, $\eta_j(G) = H_j$. Επειδή $h_ih_j = h_jh_i$ για οιαδήποτε $h_i \in H_i$ και $h_j \in H_j$ (βλ. 7.1.79), η απεικόνιση $\eta_i+\eta_j$ αποτελεί ενδομορφισμό[41] της G (δυνάμει της προτάσεως 7.2.19). Εξάλλου, για $i,j \in \{1,...,s\}$ και $h_1 \in H_1,...,h_s \in H_s$,

$$\left(\eta_i \circ \eta_j\right)(h_1h_2\cdots h_s) = \eta_i(h_j) = \begin{cases} e_G, & \text{όταν } i \neq j, \\ h_i, & \text{όταν } i = j, \end{cases}$$

και $(\sum_{i=1}^{s} \eta_i)(h_1h_2\cdots h_s) = \eta_1(h_1h_2\cdots h_s)\cdots\eta_s(h_1h_2\cdots h_s) = h_1h_2\cdots h_s$. □

7.2.25 Θεώρημα. («Θεώρημα των Krull, Remak και Schmidt») *Έστω $(G,\cdot)$ μια ομάδα που πληροί τόσον τη Σ.Α.Α. όσον και τη Σ.Κ.Α. επί τού* $\mathbf{NSubg}(G)$. *Εάν $r,s \in \mathbb{N}$ και $H_1,...,H_r,K_1,...,K_s$ είναι αναποσυνθέσιμες ορθόθετες υποομάδες τής G, τέτοιες ώστε να ισχύει $G = H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_r = K_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} K_s$, τότε $r = s$ και υπάρχει μετάταξη $\sigma \in \mathfrak{S}_s$, καθώς και ένας ορθόθετος αυτομορφισμός ϑ τής G, με $\vartheta(K_{\sigma(\iota)}) = H_\iota$ για κάθε $\iota \in \{1,...,s\}$ και*

$$\boxed{G = H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_n \times_{\text{εσ.}} K_{\sigma(n+1)} \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} K_{\sigma(s)}}$$

για κάθε[42] *$n \in \{1,...,s-1\}$.*

ΑΠΟΔΕΙΞΗ. Έστω $\Pi\Pi(n)$ ο ακόλουθος προτασιακός τύπος με σύνολο αναφοράς του το $\{n \in \mathbb{N}_0 \mid 0 \leq n \leq \min\{r,s\}\}$:

$$\Pi\Pi(0) : G = K_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} K_s$$

[41] Σημειωτέον ότι ο ενδομορφισμός $\eta_i + \eta_j$ είναι κατ' ανάγκην ορθόθετος (αφού αμφότεροι οι η_i και η_j είναι ορθόθετοι).

[42] Τούτο το συμπέρασμα είναι σαφώς ισχυρότερο τού ότι οι ευθείς παράγοντες είναι προσδιορίσιμοι μέχρις ισομορφισμού. Υπάρχει η δυνατότητα *αντικαταστάσεως* ευθέων παραγόντων τής μίας παραστάσεως με κατάλληλους ευθείς παράγοντες τής άλλης.

και για[43] $n \in \{1, ..., \min\{r, s\}\}$:

$$\Pi\Pi(n): \left[\begin{array}{l} \exists \sigma \in \mathfrak{S}_s \text{ και ορθόθετος } \vartheta_n \in \mathrm{Aut}(G) \text{ με} \\ \vartheta_n(K_{\sigma(\varrho)}) = \left\{\begin{array}{ll} H_\varrho, & \text{όταν } \varrho \in \{1, ..., n\}, \\ K_{\sigma(\varrho)}, & \text{όταν } \varrho \in \{n+1, ..., s\}, \end{array}\right. \\ \text{και, ως εκ τούτου,} \\ G = \left\{\begin{array}{ll} H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_n \times_{\text{εσ.}} K_{\sigma(n+1)} \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} K_{\sigma(s)}, & \text{όταν } n < s, \\ H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_n, & \text{όταν } n = s. \end{array}\right. \end{array}\right]$$

Θα αποδείξουμε *επαγωγικώς* ότι για κάθε $n \in \{0, 1, ..., \min\{r, s\}\}$ ο $\Pi\Pi(n)$ είναι αληθής. Επειδή είναι προδήλως αληθής για $n = 0$, υποθέτουμε ότι $n \geq 1$ και ότι αυτός είναι ωσαύτως αληθής για τον[44] $n - 1$:

$$\Pi\Pi(n-1): \left[\begin{array}{l} \exists \tau \in \mathfrak{S}_s \text{ και ορθόθετος } \vartheta_{n-1} \in \mathrm{Aut}(G) \text{ με} \\ \vartheta_{n-1}(K_{\tau(\varrho)}) = \left\{\begin{array}{ll} H_\varrho, & \text{όταν } n \geq 2 \ \ \varrho \in \{1, ..., n-1\}, \\ K_{\tau(\varrho)}, & \text{όταν } \varrho \in \{n, ..., s\}, \end{array}\right. \\ \text{και, ως εκ τούτου,} \\ G = \left\{\begin{array}{ll} K_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} K_s, & \text{όταν } n = 1, \\ H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_{n-1} \times_{\text{εσ.}} K_{\tau(n)} \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} K_{\tau(s)}, & 2 \leq n \leq s. \end{array}\right. \end{array}\right]$$

Εισάγουμε τις συντομογραφίες $\eta_i := \eta_i^{H_1, ..., H_r}$ (για κάθε $i \in \{1, ..., r\}$) και

$$\eta'_j := \left\{\begin{array}{ll} \eta_j^{K_1, ..., K_s}, & \text{όταν } n = 1, \\ \eta_j^{H_1, ..., H_{n-1}, K_{\tau(n)}, ..., K_{\tau(s)}}, & \text{όταν } n \geq 2, \end{array}\right.$$

(για κάθε $j \in \{1, ..., s\}$). Προφανώς, $\eta_i|_{H_i} = \mathrm{id}_{H_i}$ και (βάσει τού λήμματος 7.2.24)

$$\eta_i \circ \eta_k = \left\{\begin{array}{ll} 0_{G^G}, & \text{όταν } i \neq k, \\ \eta_i, & \text{όταν } i = k, \end{array}\right. \Bigg| \ \eta'_j \circ \eta'_l = \left\{\begin{array}{ll} 0_{G^G}, & \text{όταν } j \neq l, \\ \eta'_j, & \text{όταν } j = l, \end{array}\right.$$

$\sum_{i=1}^r \eta_i = \mathrm{id}_G$, $\sum_{j=1}^s \eta'_j = \mathrm{id}_G$ και $\mathrm{Im}(\eta_i) = \eta_i(G) = H_i$,

$$\mathrm{Im}(\eta'_j) = \eta'_j(G) = \left\{\begin{array}{ll} H_j, & \text{όταν } j < n, \\ K_{\tau(j)}, & \text{όταν } j \geq n, \end{array}\right.$$

για οιουσδήποτε δείκτες $i, k \in \{1, ..., r\}$ και $j, l \in \{1, ..., s\}$. Σημειωτέον ότι

$$\eta_n \circ \eta'_j = 0_{G^G}, \ \forall j \in \{1, ..., n-1\}, \tag{7.37}$$

[43] Αιτιολόγηση τού συμπεράσματος εντός τού $\Pi\Pi(n)$: Επειδή $G = K_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} K_s = K_{\sigma(1)} \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} K_{\sigma(s)}$ (βλ. 7.1.80), έχουμε

$$\begin{array}{l} G = \vartheta_n(G) = \vartheta_n(K_{\sigma(1)} \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} K_{\sigma(s)}) = \vartheta_n(K_{\sigma(1)}) \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} \vartheta_n(K_{\sigma(s)}) \\ = \left\{\begin{array}{ll} H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_n \times_{\text{εσ.}} K_{\sigma(n+1)} \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} K_{\sigma(s)}, & \text{όταν } n < s, \\ H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_s, & \text{όταν } n = s. \end{array}\right. \end{array}$$

[44] Όταν $n = 1$, θέτουμε $\vartheta_0 := \mathrm{id}_G$ και $\tau := \mathrm{id}$.

(όταν $n \geq 2$), διότι για κάθε $x \in G$ έχουμε $\eta'_j(x) \in H_j$ και[45]

$$(\eta_n \circ \eta'_j)(x) = (\eta_n \circ \mathrm{id}_{H_j} \circ \eta'_j)(x) = (\eta_n \circ (\textstyle\sum_{i=1}^{r} \eta_i|_{H_j}) \circ \eta'_j)(x)$$
$$= (\eta_n \circ \eta_j\big|_{H_j} \circ \eta'_j)(x) = (\eta_n \circ \eta_j)(\eta'_j(x)) = 0_{G^G}(\eta'_j(x)) = e_G.$$

Επομένως, για $n \geq 1$,

$$\eta_n = \eta_n \circ \mathrm{id}_G = \eta_n \circ \left(\sum_{j=1}^{s} \eta'_j\right) = \sum_{j=1}^{s} \left(\eta_n \circ \eta'_j\right) \underset{(7.37)}{=} \sum_{j=n}^{s} \left(\eta_n \circ \eta'_j\right), \tag{7.38}$$

όπου τόσον οι $\eta_n \circ \eta'_\nu$ για κάθε $\nu \in \{n, ..., s\}$ όσον και οι $\eta_n \circ \eta'_\nu + \eta_n \circ \eta'_\xi$ για οιουσδήποτε $\nu, \xi \in \{n, ..., s\}$, $\nu \neq \xi$, (όταν $n < s$) είναι ορθόθετοι ενδομορφισμοί τής G (λόγω τής προτάσεως 7.1.37 και τού λήμματος 7.2.21). Επειδή

$$\sum_{j=n}^{s} \left(\eta_n \circ \eta'_j\right)\big|_{H_n} \underset{(7.38)}{=} \eta_n|_{H_n} = \mathrm{id}_{H_n} \in \mathrm{Aut}(H_n),$$

έχουμε αφ' ενός μεν $(\eta_n \circ \eta'_n)|_{H_n} = \mathrm{id}_{H_n} \in \mathrm{Aut}(H_n)$ όταν $n = s$, αφ' ετέρου δε

$$\sum_{j=n}^{s} \left(\eta_n \circ \eta'_j\right)\big|_{H_n} = (\eta_n \circ \eta'_\kappa)|_{H_n} + \sum_{j \in \{n,...,s\} \setminus \{\kappa\}} \left(\eta_n \circ \eta'_j\right)\big|_{H_n} = \mathrm{id}_{H_n} \in \mathrm{Aut}(H_n)$$

για κάθε $\kappa \in \{n, ..., s\}$ όταν $n < s$, όπου αμφότεροι οι προσθετέοι είναι ορθόθετοι ενδομορφισμοί τού H_n. (Βλ. 7.2.20 (ii) και 7.2.21.)

Στη δεύτερη περίπτωση, λαμβάνοντας υπ' όψιν ότι η H_n είναι αναποσυνθέσιμη και πληροί[46] τόσον τη Σ.Α.Α. όσον και τη Σ.Κ.Α. επί τού $\mathbf{NSubg}(H_n)$, εφαρμόζουμε το λήμμα 7.2.22 (για την H_n!) και συμπεραίνουμε ότι τουλάχιστον ένας εκ των ανωτέρω προσθετέων οφείλει να είναι αυτομορφισμός τής H_n. Κατά συνέπειαν, σε *αμφότερες* τις περιπτώσεις,

$$\exists t \in \{n, ..., s\} : (\eta_n|_{K_{\tau(t)}}) \circ (\eta'_t|_{H_n}) = (\eta_n \circ \eta'_t)|_{H_n} \in \mathrm{Aut}(H_n). \tag{7.39}$$

Επιπροσθέτως, επειδή οι $K_{\tau(t)}$ και H_n είναι εξ υποθέσεως *αναποσυνθέσιμες* και[47] $\mathrm{Im}(\eta'_t|_{H_n}) \trianglelefteq K_{\tau(t)}$, αμφότεροι οι ομομορφισμοί

$$\eta_n|_{K_{\tau(t)}} : K_{\tau(t)} \longrightarrow H_n \ \text{ και } \ \eta'_t|_{H_n} : H_n \longrightarrow K_{\tau(t)}$$

[45] Η τρίτη ισότητα έπεται από το ότι, για $i \neq j$, ο περιορισμός $\eta_i|_{H_j}$ τού ενδομορφισμού $\eta_i \in \mathrm{End}(G)$ επί τής H_j είναι τετριμμένος (καθόσον $\mathrm{Im}(\eta_i|_{H_j}) \subseteq H_i \cap H_j = \{e_G\}$) και η πέμπτη από το ότι $\eta_n \circ \eta_j = 0_{G^G}$ (καθόσον $j < n$).

[46] Επειδή η $G = H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_r \underset{7.1.85\,\text{(ii)}}{\cong} H_1 \times \cdots \times H_r \underset{7.1.55\,\text{(ii)},\,\text{(iii)}}{\cong} H_n \times (\prod_{i \in \{1,\ldots,r\} \setminus \{n\}} H_i)$ πληροί τόσον τη Σ.Α.Α. όσον και τη Σ.Κ.Α. επί τού $\mathbf{NSubg}(G)$, η H_n (με $n \leq r$) πληροί τόσον τη Σ.Α.Α. όσον και τη Σ.Κ.Α. επί τού $\mathbf{NSubg}(H_n)$. (Βλ. 7.2.9 και 7.2.10.)

[47] Εάν $x \in H_n$ και $y \in K_{\tau(t)}$, τότε $\eta'_t|_{K_{\tau(t)}} = \mathrm{id}_{K_{\tau(t)}}$, οπότε $\eta'_t(y) = y$ και

$$y(\eta'_t|_{H_n}(x))y^{-1} = \eta'_t(y)\eta'_t(x)\eta'_t(y)^{-1} = \eta'_t(yxy^{-1}) \in \mathrm{Im}(\eta'_t|_{H_n}).$$

είναι *ισομορφισμοί*. (Βλ. πρόταση 7.1.41.) Ιδιαιτέρως,

$$\mathrm{Ker}(\eta'_t|_{H_n}) = \mathrm{Ker}(\eta'_t) \cap H_n = \{e_G\} \tag{7.40}$$

και

$$\left\{ \begin{array}{l} K_{\tau(t)} = \eta'_t(H_n) = \eta'_t(\eta_n(G)) = (\eta'_t \circ \eta_n)(G), \\ H_n = \eta_n(K_{\tau(t)}) = \eta_n(\eta'_t(G)) = (\eta_n \circ \eta'_t)(G). \end{array} \right\} \tag{7.41}$$

Ισχυρισμός: Η απεικόνιση

$$\boxed{\omega := \sum_{j \in \{1,\ldots,s\} \setminus \{t\}} \eta'_j + (\eta_n \circ \eta'_t) \in G^G}$$

αποτελεί έναν ορθόθετο αυτομορφισμό τής G, για τον οποίο ισχύει

$$\left\{ \begin{array}{ll} \omega(H_\varrho) = H_\varrho, & \text{όταν } 1 \leq \varrho \leq n-1, \\ \omega(K_{\tau(t)}) = H_n, & \\ \omega(K_{\tau(\varrho)}) = K_{\tau(\varrho)}, & \text{όταν } 1 \leq n \leq \varrho \leq s \text{ και } \varrho \neq t. \end{array} \right\} \tag{7.42}$$

Σημειώνουμε εν πρώτοις ότι από τον ορισμό των η'_j, $j \in \{1,...,s\}$, προκύπτουν τα εξής:

(i) Εάν $n \geq 2$ και $j \in \{1,...,n-1\}$, τότε για κάθε $\varrho \in \{1,...,n-1\}$ λαμβάνουμε

$$\eta'_j(H_\varrho) = \left\{ \begin{array}{ll} H_\varrho, & \text{όταν } \varrho = j, \\ \{e_G\}, & \text{όταν } \varrho \neq j. \end{array} \right.$$

(ii) Εάν $n \geq 1$ και $j \in \{n,...,s\}$, τότε για κάθε $\varrho \in \{n,...,s\}$ λαμβάνουμε

$$\eta'_j(K_{\tau(\varrho)}) = \left\{ \begin{array}{ll} K_{\tau(\varrho)}, & \text{όταν } \varrho = j, \\ \{e_G\}, & \text{όταν } \varrho \neq j, \end{array} \right.$$

(iii) Εάν $n \geq 2$, τότε $(\eta_n \circ \eta'_t)(H_\varrho) = \{e_G\}$ για κάθε $\varrho \in \{1,...,n-1\}$.

(iv) Εάν $n \geq 1$, τότε για κάθε $\varrho \in \{n,...,s\}$ λαμβάνουμε

$$(\eta_n \circ \eta'_t)(K_{\tau(\varrho)}) = \left\{ \begin{array}{ll} \eta_n(\eta'_t(K_{\tau(t)})) = \eta_n(K_{\tau(t)}) \underset{(7.41)}{=} H_n, & \text{όταν } \varrho = t, \\ \{e_G\}, & \text{όταν } \varrho \neq t. \end{array} \right.$$

Οι ισότητες (7.42) έπονται άμεσα από τα (i)-(iv). Από την άλλη μεριά, από το λήμμα 7.2.24 γνωρίζουμε ότι οι $\eta'_{j_1} + \eta'_{j_2}$ είναι ορθόθετοι ενδομορφισμοί τής G για οιουσδήποτε $j_1, j_2 \in \{1,...,s\} \setminus \{t\}$, $j_1 \neq j_2$. Επίσης, για κάθε $j \in \{1,...,s\} \setminus \{t\}$ το άθροισμα $\eta'_j + (\eta_n \circ \eta'_t)$ είναι ενδομορφισμός τής G (κατ' ανάγκην ορθόθετος λόγω τής προτάσεως 7.1.37 και τού λήμματος 7.2.21). Πράγματι· εάν $j < n$ και $z \in \mathrm{Im}(\eta_n \circ \eta'_t) = H_n$, $y \in \mathrm{Im}(\eta'_j) = H_j$, τότε το (b) (i) τού θεωρήματος 7.1.79 δίδει $zy = yz$. Εάν $j \geq n$, $z \in \mathrm{Im}(\eta_n \circ \eta'_t) = H_n$ και $y \in \mathrm{Im}(\eta'_j) = K_{\tau(j)}$, τότε υπάρχει $x \in K_{\tau(t)}$ με $z = \eta_n(x)$ και (επειδή ο η_n είναι ορθόθετος ενδομορφισμός τής G)

$$z = \eta_n(x) = \eta_n(y \underbrace{y^{-1}}_{\in K_{\tau(j)}} \underbrace{x}_{\in K_{\tau(t)}}) = \eta_n(yxy^{-1}) = y\eta_n(x)y^{-1} = yzy^{-1} \Rightarrow zy = yz$$

Άρα $\eta'_j + (\eta_n \circ \eta'_t) \in \mathrm{End}(G), \forall j \in \{1,...,s\}\setminus\{t\}$. (Βλ. 7.2.19 (ii)⇒(i).) Από τα προαναφερθέντα προκύπτει ότι η ω είναι ένας ορθόθετος ενδομορφισμός τής G. (Βλ. 7.2.20 (ii) και 7.2.21.) Επειδή (κατά την επαγωγική μας υπόθεση[48])

$$G = \begin{cases} K_1K_2\cdots K_s, & \text{όταν } n=1, \\ H_1\cdots H_{n-1}K_{\tau(n)}\cdots K_{\tau(s)}, & \text{όταν } 2\le n\le s, \end{cases}$$

η εικόνα τής G μέσω τού ω υπολογίζεται μέσω των ισοτήτων (7.42):

$$\omega(G) = \begin{cases} K_1\cdots K_{t-1}H_1K_{t+1}\cdots K_s, & \text{όταν } n=1, \\ H_1\cdots H_{n-1}K_{\tau(n)}\cdots K_{\tau(t-1)}H_nK_{\tau(t+1)}\cdots K_{\tau(s)}, & \text{όταν } 2\le n\le s. \end{cases}$$

Εν προκειμένω,

$$\mathrm{Ker}(\eta'_t) = K_1\cdots K_{t-1}K_{t+1}\cdots K_s = K_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} K_{t-1} \times_{\text{εσ.}} K_{t+1} \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} K_s$$

όταν $n=1$ και

$$\begin{aligned} \mathrm{Ker}(\eta'_t) &= H_1\cdots H_{n-1}K_{\tau(n)}\cdots K_{\tau(t-1)}K_{\tau(t+1)}\cdots K_{\tau(s)} \\ &= \left(\prod_{i=1}^{n-1}{}^{\text{εσ.}}\, H_j\right) \times_{\text{εσ.}} \left(\prod_{j\in\{n,\ldots,s\}\setminus\{t\}}{}^{\text{εσ.}}\, K_{\tau(j)}\right) \end{aligned}$$

όταν $2\le n\le s$. Από την (7.40) συνάγεται ότι

$$\omega(G) = \mathrm{Ker}(\eta'_t) \times_{\text{εσ.}} H_n$$

$$\underset{7.1.80}{=} \begin{cases} K_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} K_{t-1} \times_{\text{εσ.}} H_1 \times_{\text{εσ.}} K_{t+1} \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} K_s, & \text{όταν } n=1, \\ \left(\prod_{i=1}^{n-1}{}^{\text{εσ.}}\, H_j\right) \times_{\text{εσ.}} \left(\prod_{j=n}^{t-1}{}^{\text{εσ.}}\, K_{\tau(j)}\right) \times_{\text{εσ.}} H_n \times_{\text{εσ.}} \left(\prod_{j=t+1}^{s}{}^{\text{εσ.}}\, K_{\tau(j)}\right), & 2\le n\le s. \end{cases}$$

Εάν $2\le n\le s$ και εάν θεωρήσουμε τυχόν $g\in\mathrm{Ker}(\omega)$, τότε αυτό γράφεται υπό τη μορφή

$$g = h_1h_2\cdots h_{n-1}k_nk_{n+1}\cdots k_s,$$

όπου τα $h_1\in H_1,...,h_{n-1}\in H_{n-1}, k_n\in K_{\tau(n)},...,k_s\in K_{\tau(s)}$ είναι *μονοσημάντως ορισμένα* και

$$\begin{aligned} &\omega(g) = \omega(h_1h_2\cdots h_{n-1}k_n\cdots k_t\cdots k_s) = \omega(h_1)\omega(h_2)\cdots\omega(h_{n-1})\omega(k_n)\cdots\omega(k_t)\cdots\omega(k_s) \\ &= h_1h_2\cdots h_{n-1}k_n\cdots k_{t-1}\omega(k_t)k_{t+1}\cdots k_s = e_G = \underbrace{e_Ge_G\cdots e_Ge_G}_{s\ \text{φορές}}, \end{aligned}$$

οπότε $h_1=\cdots=h_{n-1}=k_n=\cdots=k_{t-1}=\omega(k_t)=k_{t+1}=\cdots=k_s=e_G$. Επειδή $\omega(k_t)=\omega|_{K_{\tau(t)}}(k_t)=e_G$ και ο περιορισμός $\omega|_{K_{\tau(t)}}$ ισούται με τον ισομορφισμό $\eta_n|_{K_{\tau(t)}}: K_{\tau(t)}\longrightarrow H_n$, έχουμε $k_t=e_G\Rightarrow g=e_G$. (Παρομοίως αποδεικνύεται ότι $\mathrm{Ker}(\omega)=\{e_G\}$ ακόμη και στην περίπτωση όπου $n=1$.) Κατά συνέπειαν, ο ορθόθετος ενδομορφισμός ω τής G είναι ενριπτικός και, ως εκ τούτου, αυτομορφισμός τής G (λόγω τού λήμματος 7.2.14) και ο ισχυρισμός είναι αληθής[49].

[48] Όπως έχει ήδη προαναφερθεί, $\tau := \mathrm{id}$ όταν $n=1$.

[49] Σημειωτέον ότι $G=\omega(G)$, οπότε η ανωτέρω δοθείσα παράσταση τής $\omega(G)$ ως εσωτερικού ευθέος γινομένου αναποσυνθέσιμων υποομάδων αποτελεί μια παράσταση *τής ίδιας τής* G.

Αποπεράτωση τής αποδείξεως. Από την επαγωγική μας υπόθεση υπάρχει ένας ορθόθετος αυτομορφισμός ϑ_{n-1} τής G, ούτως ώστε να ισχύει

$$\vartheta_{n-1}(K_{\tau(\varrho)}) = \begin{cases} H_\varrho, & \text{όταν } \varrho \in \{1,...,n-1\}, \\ K_{\tau(\varrho)}, & \text{όταν } \varrho \in \{n,...,s\}. \end{cases}$$

Όταν $t = n$, θέτουμε $\sigma := \tau$, ενώ όταν $t \neq n$ ορίζουμε την $\sigma \in \mathfrak{S}_s$ μέσω τού τύπου:

$$\sigma(\varrho) := \begin{cases} \tau(n), & \text{όταν } \varrho = t, \\ \tau(t), & \text{όταν } \varrho = n, \\ \tau(\varrho), & \text{όταν } \varrho \in \{1,...,s\} \setminus \{n,t\}. \end{cases}$$

Εν συνεχείᾳ, θέτουμε $\boxed{\vartheta_n := \omega \circ \vartheta_{n-1} \in \mathrm{Aut}(G)}$ και παρατηρούμε ότι ο ϑ_n είναι ορθόθετος (λόγω τής προτάσεως 7.1.37) και ότι ικανοποιεί τις σχέσεις

$$\vartheta_n\left(K_{\sigma(\varrho)}\right) = \omega\left(\vartheta_{n-1}(K_{\sigma(\varrho)})\right) = \omega\left(\vartheta_{n-1}(K_{\tau(\varrho)})\right) = \omega(H_\varrho) = H_\varrho$$

όταν $1 \leq \varrho \leq n-1$,

$$\vartheta_n\left(K_{\sigma(\varrho)}\right) = \omega\left(\vartheta_{n-1}(K_{\sigma(\varrho)})\right) = \omega\left(\vartheta_{n-1}(K_{\tau(\varrho)})\right) = \omega(K_{\tau(\varrho)}) = K_{\tau(\varrho)}$$

όταν $n+1 \leq \varrho \leq s$ και $\varrho \neq t$, και

$$\vartheta_n\left(K_{\sigma(t)}\right) = \omega\left(\vartheta_{n-1}(K_{\tau(n)})\right) = \omega(K_{\tau(n)}) = K_{\tau(n)} = K_{\sigma(t)},$$
$$\vartheta_n\left(K_{\sigma(n)}\right) = \omega\left(\vartheta_{n-1}(K_{\tau(t)})\right) = \omega(K_{\tau(t)}) = H_n.$$

Άρα ο ΠΡ(n) είναι αληθής για κάθε $n \in \{0,1,...,\min\{r,s\}\}$. Εάν $r < s$, τότε για $n = r$ λαμβάνουμε

$$H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_r = G = H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_r \times_{\text{εσ.}} K_{\sigma(r+1)} \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} K_{\sigma(s)}. \tag{7.43}$$

Εάν $s < r$, τότε για $n = s$ λαμβάνουμε

$$H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_r = G = H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_s. \tag{7.44}$$

Επειδή όλοι οι ευθείς παράγοντες στις (7.43) και (7.44) είναι αναποσυνθέσιμοι (και, ως εκ τούτου, μη τετριμμένοι), αυτές δεν είναι δυνατόν να ισχύουν. Επομένως έχουμε κατ' ανάγκην $r = s$. Τέλος, θέτοντας $\vartheta := \vartheta_s$ λαμβάνουμε τη ζητούμενη ισότητα $\vartheta(K_{\sigma(\iota)}) = H_\iota$ για κάθε $\iota \in \{1,...,s\}$. □

7.2.26 Σημείωση. Το θεώρημα 7.2.25 δεν ισχύει κατ' ανάγκην για άπειρες ομάδες, οι οποίες δεν πληρούν *αμφότερες* τις Σ.Α.Α. και Σ.Κ.Α. επί τού συνόλου των ορθόθετων υποομάδων τους, ακόμη κι αν αυτές είναι πεπερασμένως παραγόμενες. Όπως απέδειξε ο Gilbert Baumslag[50] το 1975, για *οιουσδήποτε* φυσικούς αριθμούς $r > 1$ και $s > 1$, υφίσταται μια πεπερασμένως παραγόμενη άπειρη ομάδα G χωρίς στρέψη με παραστάσεις

$$H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_r = G = K_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} K_s,$$

όπου $H_1,...,H_r,K_1,...,K_s$ είναι αναποσυνθέσιμες ορθόθετες υποομάδες της, τέτοιες ώστε $H_i \ncong K_j, \forall (i,j) \in \{1,...,r\} \times \{1,...,s\}$.

[50] G. Baumslag: *Direct decompositions of finitely generated torsion-free nilpotent groups*, Mathematische Zeitschrift **147** (1975), 1-10.

7.2.27 Ορισμός. Έστω $(G,\cdot)$ μια ομάδα που πληροί τόσον τη Σ.Α.Α. όσον και τη Σ.Κ.Α. επί τού $\mathbf{NSubg}(G)$. Λέμε ότι μια παράσταση $G = H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_r$ τής G ως εσωτερικού γινομένου r αναποσυνθέσιμων ορθόθετων υποομάδων της $H_1, ..., H_r$ είναι **ουσιωδώς μονοσημάντως ορισμένη** όταν για οιαδήποτε άλλη ομοειδή παράσταση $G = K_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} K_r$ υπάρχει μια μετάταξη $\sigma \in \mathfrak{S}_r$, τέτοια ώστε να ισχύει $H_i = K_{\sigma(i)}$ για κάθε $i \in \{1, ..., r\}$.

7.2.28 Θεώρημα. (Κριτήριο «ουσιώδους μοναδικότητας») *Έστω $(G,\cdot)$ μια ομάδα που πληροί τόσον τη Σ.Α.Α. όσον και τη Σ.Κ.Α. επί τού $\mathbf{NSubg}(G)$. Εάν*

$$G = H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_r \tag{7.45}$$

είναι μια παράσταση τής G ως εσωτερικού γινομένου r αναποσυνθέσιμων ορθόθετων υποομάδων της $H_1, ..., H_r$, όπου $r \geq 2$, τότε τα ακόλουθα είναι ισοδύναμα:

(i) *H (7.45) είναι ουσιωδώς μονοσημάντως ορισμένη.*

(ii) *Για οιουσδήποτε $i, j \in \{1, ..., r\}$, $i \neq j$, ο μόνος υφιστάμενος ομομορφισμός $H_i \longrightarrow Z(H_j)$ είναι ο τετριμμένος ομομορφισμός.*

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το πόρισμα 7.1.82, $Z(H_j) \trianglelefteq Z(G), \forall j \in \{1, ..., r\}$, και

$$Z(G) = Z(H_1) \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} Z(H_r). \tag{7.46}$$

(i)⇒(ii) Ας υποθέσουμε ότι $i, j \in \{1, ..., r\}$, $i \neq j$, είναι τέτοιοι, ώστε να υφίσταται κάποιος *μη τετριμμένος* ομομορφισμός $f : H_i \longrightarrow Z(H_j)$. Θέτουμε

$$\widehat{H}_i := \{\, h_i f(h_i) |\, h_i \in H_i \}\,.$$

Επειδή $e_G \in \widehat{H}_i$, και για $h_i, h_i' \in H_i$, $g \in G$, ισχύει

$$\begin{aligned}(h_i f(h_i))\,(h_i' f(h_i'))^{-1} &= h_i f(h_i) f(h_i')^{-1} (h_i')^{-1} = h_i f(h_i) f((h_i')^{-1})(h_i')^{-1} \\ &= h_i \underbrace{f(h_i (h_i')^{-1})}_{\in Z(H_j)\,(\trianglelefteq Z(G))} (h_i')^{-1} = \underbrace{h_i (h_i')^{-1}}_{\in H_i} \underbrace{f(h_i (h_i')^{-1})}_{\in H_i} \in \widehat{H}_i\end{aligned}$$

και

$$\begin{aligned} & g h_i \underbrace{f(h_i)}_{\in Z(G)} g^{-1} = (g h_i g^{-1}) f(h_i) = (g h_i g^{-1}) f(e_G h_i) \\ & = (g h_i g^{-1}) f(g g^{-1} h_i) = (g h_i g^{-1}) f(g) f(g^{-1}) \underbrace{f(h_i)}_{\in Z(G)} \\ & = (g h_i g^{-1}) f(g) f(h_i) f(g^{-1}) = \underbrace{(g h_i g^{-1})}_{\in H_i} \underbrace{f(g h_i g^{-1})}_{\in H_i} \in \widehat{H}_i, \end{aligned}$$

έχουμε $\widehat{H}_i \trianglelefteq G$. Επιπροσθέτως, κάθε στοιχείο $g \in G$ γράφεται υπό τη μορφή

$$g = h_1 \cdots h_i \cdots h_r = h_1 \cdots h_{i-1} \underbrace{(h_i f(h_i))}_{\in \widehat{H}_i} \underbrace{f(h_i^{-1})}_{\in Z(G)} h_{i+1} \cdots h_r$$

$$= \begin{cases} h_1 \cdots h_{j-1} \underbrace{f(h_i^{-1})}_{\text{στην } j\text{-οστή θέση}} h_j \cdots \underbrace{(h_i f(h_i))}_{\in \widehat{H}_i} h_{i+1} \cdots h_r, & \text{όταν } i > j, \\ h_1 \cdots h_{i-1} \underbrace{(h_i f(h_i))}_{\in \widehat{H}_i} \cdots h_{j-1} \underbrace{f(h_i^{-1})}_{\text{στην } j\text{-οστή θέση}} h_j \cdots h_r, & \text{όταν } i < j, \end{cases}$$

(με $f(h_i^{-1})h_j \in H_j$), όπου $h_1 \in H_1, ..., h_r \in H_r$. Εάν

$$x \in \widehat{H}_i \cap (H_1 \cdots H_{i-1}H_{i+1} \cdots H_r),$$

τότε $x = yf(y)$, για κάποιο $y \in H_i$, και

$$f(y) \in H_j \Rightarrow f(y)^{-1} \in H_j \subseteq H_1 \cdots H_{i-1}H_{i+1} \cdots H_r,\ x \in H_1 \cdots H_{i-1}H_{i+1} \cdots H_r$$
$$\Rightarrow y = xf(y)^{-1} \in H_1 \cdots H_{i-1}H_{i+1} \cdots H_r,$$

οπότε $y \in H_i \cap (H_1 \cdots H_{i-1}H_{i+1} \cdots H_r) = \{e_G\} \Rightarrow y = e_G \Rightarrow x = e_G$, απ' όπου προκύπτει ότι

$$G = H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_{i-1} \times_{\text{εσ.}} \widehat{H}_i \times_{\text{εσ.}} H_{i+1} \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_r.$$

Άρα η (7.45) δεν είναι ουσιωδώς μονοσημάντως ορισμένη, διότι[51] $\widehat{H}_i \neq H_i$. Άτοπο!

(ii)⇒(i) Ας υποθέσουμε ότι η (7.45) δεν είναι ουσιωδώς μονοσημάντως ορισμένη, δηλαδή ότι υφίσταται μια άλλη ομοειδής παράσταση $G = K_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} K_r$ τής G, καθώς και κάποιος $i_0 \in \{1, ..., r\}$, τέτοιος ώστε να ισχύει $H_{i_0} \notin \{K_1, ..., K_r\}$. Σύμφωνα με το θεώρημα 7.2.25 υπάρχει μια μετάταξη $\sigma \in \mathfrak{S}_r$, καθώς και ένας ορθόθετος αυτομορφισμός ϑ τής G, με $\vartheta(K_{\sigma(1)}) = H_1, ..., \vartheta(K_{\sigma(r)}) = H_r$ ή, ισοδυνάμως, με $\vartheta^{-1}(H_1) = K_{\sigma(1)}, ..., \vartheta^{-1}(H_r) = K_{\sigma(r)}$. Για κάθε $x \in H_{i_0}$ ισχύει $x^{-1}\vartheta^{-1}(x) \in Z(G)$, οπότε (λόγω τής (7.46)) έχουμε $x^{-1}\vartheta^{-1}(x) = z_1 \cdots z_r$ για κάποια μονοσημάντως ορισμένα $z_1 \in Z(H_1), ..., z_r \in Z(H_r)$. (Βλ. 7.1.36, 7.1.38 (ii) και 7.1.79.) Κατ' αυτόν τον τρόπο δημιουργείται μια απεικόνιση

$$H_{i_0} \ni x \overset{f_j}{\longmapsto} z_j \in Z(H_j)$$

για κάθε $j \in \{1, ..., r\}$, η οποία είναι ομομορφισμός ομάδων, διότι για $\widetilde{x} \in H_{i_0}$ με $\widetilde{x}^{-1}\vartheta^{-1}(\widetilde{x}) = \widetilde{z}_1 \cdots \widetilde{z}_r$ (όπου $\widetilde{z}_1 \in Z(H_1), ..., \widetilde{z}_r \in Z(H_r)$) λαμβάνουμε

$$(x\widetilde{x})^{-1}\vartheta^{-1}(x\widetilde{x}) = \widetilde{x}^{-1}\underbrace{x^{-1}\vartheta^{-1}(x)}_{\in Z(G)}\vartheta^{-1}(\widetilde{x}) = \left(x^{-1}\vartheta^{-1}(x)\right)\left(\widetilde{x}^{-1}\vartheta^{-1}(\widetilde{x})\right)$$
$$= z_1 \cdots z_j \cdots z_r\widetilde{z}_1 \cdots \widetilde{z}_j \cdots \widetilde{z}_r = z_1\widetilde{z}_1 \cdots z_j\widetilde{z}_j \cdots z_r\widetilde{z}_r \Rightarrow f_j(x\widetilde{x}) = f_j(x)f_j(\widetilde{x}).$$

Εάν ο f_j ήταν ο τετριμμένος ομομορφισμός για κάθε $j \in \{1, ..., r\} \setminus \{i_0\}$, τότε για κάθε $x \in H_{i_0}$ θα ίσχυε

$$[f_j(x) = e_G, \forall j \in \{1, .., r\} \setminus \{i_0\}] \Rightarrow x^{-1}\vartheta^{-1}(x) = e_G \cdots e_G z_{i_0} e_G \cdots e_G = z_{i_0} \in Z(H_{i_0}),$$

οπότε θα είχαμε $\vartheta^{-1}(x) = xz_{i_0} \in H_{i_0} \Rightarrow K_{\sigma(i_0)} = \vartheta^{-1}(H_{i_0}) \subseteq H_{i_0}$ και ο $\vartheta^{-1}\big|_{H_{i_0}}$ (σύμφωνα με το (ii) τής προτάσεως 7.1.39) θα ήταν ορθόθετος ενδομορφισμός τής H_{i_0} και, ως εκ τούτου, αυτομορφισμός[52] τής H_{i_0} με

$$K_{\sigma(i_0)} = \vartheta^{-1}(H_{i_0}) = H_{i_0},$$

[51] Εξ υποθέσεως, $\exists h \in H_i \setminus \{e_G\} : f(h) \in H_j \setminus \{e_G\}$, απ' όπου έπεται ότι $hf(h) \in \hat{H}_i \setminus H_i$. (Πράγματι· εάν ίσχυε $hf(h) \in H_i$, τότε θα είχαμε $hf(h) = h'$ για κάποιο στοιχείο $h' \in H_i$, ήτοι $f(h) = h^{-1}h' \in H_i \cap H_j$, όπου $H_i \cap H_j \subseteq H_i \cap (H_1 \cdots H_{i-1}H_{i+1} \cdots H_r) = \{e_G\} \Rightarrow H_i \cap H_j = \{e_G\}$, και θα συμπεραίναμε ότι $f(h) = e_G$.)

[52] Επειδή η $G = H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_r \underset{7.1.85\,\text{(ii)}}{\cong} H_1 \times \cdots \times H_r \underset{7.1.55\,\text{(ii), (iii)}}{\cong} H_{i_0} \times (\prod_{j \in \{1,\ldots,r\} \setminus \{i_0\}} H_j)$ πληροί τη Σ.Κ.Α. επί τού $\mathbf{NSubg}(G)$, η H_{i_0} πληροί τη Σ.Κ.Α. επί τού $\mathbf{NSubg}(H_{i_0})$. (Βλ. 7.2.9 και 7.2.10.) Επομένως,

$$\text{Ker}(\vartheta^{-1}\big|_{H_{i_0}}) = \text{Ker}(\vartheta^{-1}) \cap H_{i_0} = \{e_G\} \underset{2.4.15}{\Longrightarrow} \vartheta^{-1}\big|_{H_{i_0}} \text{ μονομορφισμός} \underset{7.2.14}{\Longrightarrow} \vartheta^{-1}\big|_{H_{i_0}} \in \text{Aut}(H_{i_0}).$$

κάτι που θα αντέκειτο στο ότι $H_{i_0} \notin \{K_1, ..., K_r\}$. Άρα τουλάχιστον ένας εκ των ομομορφισμών $f_j, j \in \{1, ..., r\} \setminus \{i_0\}$, οφείλει να είναι μη τετριμμένος. Άτοπο! □

7.2.29 Παραδείγματα. Έστω $(G, \cdot)$ μια ομάδα που πληροί τόσον τη Σ.Α.Α. όσον και τη Σ.Κ.Α. επί τού $\mathbf{NSubg}(G)$.

(i) Εάν $Z(G) = \{e_G\}$, τότε (προφανώς) κάθε παράσταση (7.45) είναι ουσιωδώς μονοσημάντως ορισμένη.

(ii) Εάν η $(G, \cdot)$ είναι μια *τέλεια ομάδα* (βλ. 5.5.4), τότε κάθε παράσταση (7.45) είναι ωσαύτως ουσιωδώς μονοσημάντως ορισμένη, διότι (σύμφωνα με το πόρισμα 7.1.83) έχουμε[53]

$$G = G' = H_1' \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_r' \Rightarrow [H_i = H_i',\ \forall i \in \{1, ..., r\}],$$

οπότε για $i, j \in \{1, ..., r\}$, $i \neq j$, $\nu \in \mathbb{N}$, $x_1, y_1, ..., x_\nu, y_\nu \in H_i$, $\varepsilon_1, ..., \varepsilon_\nu \in \mathbb{Z}$, και για οιονδήποτε $f \in \mathrm{Hom}(H_i, Z(H_j))$ ισχύει

$$f(\prod_{k=1}^{\nu} [x_k, y_k]^{\varepsilon_k}) = \prod_{k=1}^{\nu} f([x_k, y_k])^{\varepsilon_k} = \prod_{k=1}^{\nu} [f(x_k), f(y_k)]^{\varepsilon_k} = e_G,$$

καθόσον $f(x_k), f(y_k) \in Z(H_j) \Rightarrow [f(x_k), f(y_k)] = e_G$.

7.3 ΠΟΤΕ ΕΙΝΑΙ Η $\mathbb{Z}_m^\times$ ΚΥΚΛΙΚΗ;

Έστω $m \in \mathbb{N}$, $m \geq 2$, και έστω $(\mathbb{Z}_m^\times, \cdot)$ η πολλαπλασιαστική αβελιανή ομάδα

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

των αντιστρέψιμων κλάσεων ισοτιμίας (ή «κλάσεων υπολοίπων») κατά το μόδιο m τάξεως $|\mathbb{Z}_m^\times| = \phi(m)$, όπου ϕ η συνάρτηση τού Euler (βλ. 2.1.7 (iii)). Ερώτημα: *Για ποιους m είναι η $(\mathbb{Z}_m^\times, \cdot)$ κυκλική*; Το ερώτημα αυτό είναι αμιγώς *αριθμοθεωρητικής φύσεως*, καθόσον ισοδυναμεί με την αναζήτηση εκείνης τής ικανής και αναγκαίας συνθήκης που θα πρέπει να πληρούται, ούτως ώστε να υπάρχει μια κλάση ισοτιμίας τάξεως $\phi(m)$ *εντός τής* $(\mathbb{Z}_m^\times, \cdot)$ (βλ. πρόταση 2.3.7). Επί παραδείγματι, οι $\mathbb{Z}_2^\times, \mathbb{Z}_3^\times$ και $\mathbb{Z}_4^\times$ είναι κυκλικές (διότι έχουν τάξη ≤ 2, βλ. 2.3.19), ενώ η $\mathbb{Z}_8^\times$ (όπως διαπιστώσαμε στο εδάφιο 2.4.20 (ii)) δεν είναι κυκλική. *Πλήρης απάντηση* στο εν λόγω ερώτημα δίδεται μέσω τού θεωρήματος 7.3.13. Παρότι αυτό το θεώρημα μπορεί να αποδειχθεί κάνοντας χρήση τεχνικών μέσων προερχομένων μόνον από τη Στοιχειώδη Θεωρία Αριθμών (και η πρώτη του απόδειξη εμφανίζεται στις ενότητες 85-92 τού έργου[54] *Disquisitiones Arithmeticae* τού Carl Friedrich Gauss (1777-1855) τού δημοσιευθέντος στα Λατινικά το 1801), η παρεμβολή ορισμένων ομαδοθεωρητικών αποτελεσμάτων επιταχύνει *ουσιωδώς* την ακολουθούμενη αποδεικτική πορεία.

[53] Σημειωτέον ότι $G/G' = G/(H_1' \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_r') \cong (H_1/H_1') \times \cdots \times (H_r/H_r')$. Επειδή $G = G'$, η συνεπαγωγή είναι πρόδηλη.

[54] Βλ. C.-F. Gauss: *Disquisitiones Arithmeticae*, translated from A. Clarke, Yale University Press, 1966, σελ. 55-61.

7.3.1 Λήμμα. *Εάν* $s \in \mathbb{N},\ s \geq 2,\ a, b_1,..., b_s \in \mathbb{Z}\setminus\{0\}$ *και εάν οι* $b_1,..., b_s$ *είναι σχετικώς πρώτοι ανά δύο, τότε*

$$\text{μκδ}(a, \prod_{j=1}^{s} b_j) = 1 \Longleftrightarrow (\text{μκδ}(a, b_j) = 1, \forall j \in \{1,..., s\}). \tag{7.47}$$

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το πόρισμα Β.3.17. □

7.3.2 Θεώρημα. *Εάν* $s \in \mathbb{N}, s \geq 2$, *και εάν οι* $m_1, m_2,..., m_s$ *είναι* s *σχετικώς πρώτοι ανά δύο φυσικοί αριθμοί, τότε*

$$\boxed{\mathbb{Z}_m^\times \cong \mathbb{Z}_{m_1}^\times \times \mathbb{Z}_{m_2}^\times \times \cdots \times \mathbb{Z}_{m_s}^\times,} \tag{7.48}$$

όπου $m := m_1 m_2 \cdots m_s$. *Ως εκ τούτου, η συνάρτηση* ϕ *τού Euler είναι «πολλαπλασιαστική», ήτοι ισχύει η ισότητα*

$$\boxed{\phi\,(m) = \phi\,(m_1)\,\phi\,(m_2)\ \cdots\ \phi\,(m_s)\,.}$$

ΠΡΩΤΗ ΑΠΟΔΕΙΞΗ. Θεωρούμε την

$$f : \mathbb{Z}_m \longrightarrow \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s},\ [a]_m \longmapsto f([a]_m) := ([a]_{m_1}, [a]_{m_2},..., [a]_{m_s}).$$

Όπως γνωρίζουμε από την απόδειξη τού θεωρήματος 7.1.62, η f είναι μια αμφιριπτική απεικόνιση. Προφανώς, για οιονδήποτε $a \in \mathbb{Z}$ ισχύουν οι αμφίπλευρες συνεπαγωγές

$$[a]_m \in \mathbb{Z}_m^\times \Leftrightarrow \text{μκδ}(a, m) = 1 \underset{(7.47)}{\Longleftrightarrow} (\text{μκδ}(a, m_j) = 1,\ \forall j \in \{1,..., s\})$$
$$\Longleftrightarrow f([a]_m) \in \mathbb{Z}_{m_1}^\times \times \mathbb{Z}_{m_2}^\times \times \cdots \times \mathbb{Z}_{m_s}^\times.$$

Βάσει αυτών ο περιορισμός $f|_{\mathbb{Z}_m^\times}$ τής f επί τού $\mathbb{Z}_m^\times$ (ο οποίος είναι μια ένριψη) έχει ως εικόνα του το ευθύ γινόμενο

$$\text{Im}(\,f|_{\mathbb{Z}_m^\times}) = \mathbb{Z}_{m_1}^\times \times \mathbb{Z}_{m_2}^\times \times \cdots \times \mathbb{Z}_{m_s}^\times.$$

Κατά συνέπειαν, η επαγομένη απεικόνιση

$$\hat{f} : \mathbb{Z}_m^\times \longrightarrow \mathbb{Z}_{m_1}^\times \times \mathbb{Z}_{m_2}^\times \times \cdots \times \mathbb{Z}_{m_s}^\times,\ [a]_m \longmapsto\ \hat{f}([a]_m) := f([a]_m)$$

είναι αμφιρριπτική. Επειδή για οιουσδήποτε $a, b \in \mathbb{Z}$ ισχύουν οι ισότητες

$$\hat{f}([a]_m\,[b]_m) = \hat{f}([ab]_m) = ([ab]_{m_1}, [ab]_{m_2},..., [ab]_{m_s})$$
$$= ([a]_{m_1}\,[b]_{m_1}, [a]_{m_2}\,[b]_{m_2},..., [a]_{m_s}\,[b]_{m_s})$$
$$= ([a]_{m_1}, [a]_{m_2},..., [a]_{m_s})([b]_{m_1}, [b]_{m_2},..., [b]_{m_s}) = \hat{f}([a]_m)\hat{f}([b]_m),$$

η $\hat{f}$ είναι ομομορφισμός πολλαπλασιαστικών(!) ομάδων και, βάσει των προαναφερθέντων, ισομορφισμός.

ΔΕΥΤΕΡΗ ΑΠΟΔΕΙΞΗ. Μέσω τού θεωρήματος 7.1.62 και τής προτάσεως 7.1.76 συνάγεται ότι

$$\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s} \Rightarrow \text{Aut}(\mathbb{Z}_m) \cong \text{Aut}(\mathbb{Z}_{m_1}) \times \cdots \times \text{Aut}(\mathbb{Z}_{m_s}). \tag{7.49}$$

Από την άλλη μεριά, κατά το (ii) τού θεωρήματος 2.4.32,

$$\text{Aut}(\mathbb{Z}_m) \cong \mathbb{Z}_m^\times,\ \text{Aut}(\mathbb{Z}_{m_1}) \cong \mathbb{Z}_{m_1}^\times,\ldots,\ \text{Aut}(\mathbb{Z}_{m_s}) \cong \mathbb{Z}_{m_s}^\times. \tag{7.50}$$

Οι (9.46) και (9.47), και το (v) τής προτάσεως 7.1.55 διασφαλίζουν την ύπαρξη ενός ισομορφισμού (7.48). □

7.3.3 Πόρισμα. *Έστω $m = p_1^{\nu_1} p_2^{\nu_2} \cdots p_\kappa^{\nu_\kappa},\ \kappa \in \mathbb{N}$, η κανονική παράσταση* (B.19) *ενός φυσικού αριθμού $m \geq 2$ ως γινομένου (δυνάμεων) σαφώς διακεκριμένων πρώτων αριθμών $p_1,\ldots,p_\kappa$ με $p_1 < \cdots < p_\kappa$ (όταν $\kappa \geq 2$) και $\nu_1,\ldots,\nu_\kappa \in \mathbb{N}$. Τότε*

$$\boxed{\mathbb{Z}_m^\times \cong \mathbb{Z}_{p_1^{\nu_1}}^\times \times \mathbb{Z}_{p_2^{\nu_2}}^\times \times \cdots \times \mathbb{Z}_{p_\kappa^{\nu_\kappa}}^\times.}$$

Ως εκ τούτου,

$$\boxed{\phi(m) = \prod_{j=1}^{\kappa} \phi(p_j^{\nu_j}) = \prod_{j=1}^{\kappa} (p_j^{\nu_j} - p_j^{\nu_j - 1}) = m \prod_{j=1}^{\kappa} \left(1 - \frac{1}{p_j}\right).}$$

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το πόρισμα B.2.13, το θεώρημα 7.3.2 και το λήμμα B.4.19. □

7.3.4 Συμβολισμός. Έστω p ένας πρώτος αριθμός. Για κάθε $d \in \mathbb{N}$ με $d \mid p-1$ συμβολίζουμε ως

$$\mathfrak{N}_p(d) := \text{card}\left(\left\{[l]_p \in \mathbb{Z}_p^\times \;\middle|\; \text{ord}([l]_p) = d\right\}\right)$$

το πλήθος των στοιχείων τής $\mathbb{Z}_p^\times$ που έχουν τάξη ίση με d.

7.3.5 Λήμμα. *Έστω p ένας πρώτος αριθμός. Τότε ισχύουν τα εξής*:

(i) $\sum_{d \in \mathfrak{D}_{p-1}} \mathfrak{N}_p(d) = p-1$, *όπου* $\mathfrak{D}_{p-1} := \{d \in \mathbb{N} : d \mid p-1\}$ (πρβλ. B.2.34).

(ii) *Για κάθε $d \in \mathbb{N}$ με $d \mid p-1$ αληθεύει η συνεπαγωγή*

$$\mathfrak{N}_p(d) \geq 1 \Longrightarrow \mathfrak{N}_p(d) = \phi(d).$$

(iii) *Για κάθε $d \in \mathbb{N}$ με $d \mid p-1$ έχουμε $\mathfrak{N}_p(d) \leq \phi(d)$.*

ΑΠΟΔΕΙΞΗ. (i) Τούτο είναι προφανές, διότι $p-1 = \left|\mathbb{Z}_p^\times\right|$ και κάθε στοιχείο τής ομάδας $\left(\mathbb{Z}_p^\times, \cdot\right)$ έχει ως τάξη του κάποιον (θετικό ακέραιο) διαιρέτη τού $p-1$ (βλ. πόρισμα 4.1.27).

(ii) Όταν $\mathfrak{N}_p(d) \geq 1$, υπάρχει κάποιο στοιχείο, ας το πούμε $[\lambda]_p \in \mathbb{Z}_p^\times$, τάξεως d. Το $[\lambda]_p$ αποτελεί μια λύση τής πολυωνυμικής εξισώσεως $\mathsf{X}^d - [1]_p = [0]_p$. Προφανώς, λόγω τού πορίσματος 4.1.28 έχουμε

$$([\lambda]_p^j)^d = \left[\lambda^{jd}\right]_p = [1]_p\,,\ \ \forall j \in \{0,1,...,d-1\}.$$

Αυτό σημαίνει ότι υπάρχουν *τουλάχιστον* d (σαφώς διακεκριμένες) λύσεις[55] τής εξισώσεως $\mathsf{X}^d - [1]_p = [0]_p$ ανήκουσες *στο σώμα* $\mathbb{Z}_p$. Από την άλλη μεριά, το πολυώνυμο $\mathsf{X}^d - [1]_p \in \mathbb{Z}_p[\mathsf{X}]$ έχει βαθμό d. Σύμφωνα με το πόρισμα C.2.27, το $\mathsf{X}^d - [1]_p$ έχει *το πολύ* d θέσεις μηδενισμού ανήκουσες *στο σώμα* $\mathbb{Z}_p$. Κατά συνέπειαν, το $\mathsf{X}^d - [1]_p$ έχει *ακριβώς* d θέσεις μηδενισμού ανήκουσες *στο σώμα* $\mathbb{Z}_p$. Επειδή *κάθε* στοιχείο τάξεως d *εντός τής ομάδας* $\mathbb{Z}_p^\times$ αποτελεί λύση τής εξισώσεως $\mathsf{X}^d - [1]_p = [0]_p$ και $[1]_p \neq [0]_p$, τα μόνα στοιχεία *τής ομάδας* $\mathbb{Z}_p^\times$ που έχουν τάξη d είναι οι δυνάμεις $[\lambda]_p^j$, $j \in \{0,1,...,d-1\}$, που έχουν τάξη d. Επομένως,

$$\left\{[l]_p \in \mathbb{Z}_p^\times \;\middle|\; \mathrm{ord}([l]_p) = d\right\} = \left\{[\lambda]_p^j \;\middle|\; j \in \{0,1,...,d-1\},\ \mathrm{ord}([\lambda]_p^j) = d\right\}.$$

Λαμβάνοντας υπ' όψιν ότι

$$\mathrm{ord}([\lambda]_p^j) = \frac{\mathrm{ord}([\lambda]_p)}{\text{μκδ}(\mathrm{ord}([\lambda]_p), j)} = \frac{d}{\text{μκδ}\,(d,j)}$$

(βλ. πόρισμα 2.3.11) και ότι το τελευταίο κλάσμα ισούται με d εάν και μόνον εάν $\text{μκδ}(d,j) = 1$, συμπεραίνουμε ότι

$$\left\{[l]_p \in \mathbb{Z}_p^\times \;\middle|\; \mathrm{ord}([l]_p) = d\right\} = \left\{[\lambda]_p^j \;\middle|\; j \in \{0,1,...,d-1\},\ \text{μκδ}\,(d,j) = 1\right\},$$

απ' όπου προκύπτει ότι $\mathfrak{N}_p(d) = \phi\,(d)$.

(iii) Λόγω τού (ii), για κάθε $d \in \mathbb{N}$ με $d \mid p-1$ έχουμε $\mathfrak{N}_p(d) \in \{0, \phi\,(d)\}$, απ' όπου έπεται η ανισοϊσότητα $\mathfrak{N}_p(d) \leq \phi\,(d)$. □

7.3.6 Λήμμα. *Για κάθε $m \in \mathbb{N}$ ισχύει η ισότητα*

$$\sum_{d \in \mathfrak{D}_m} \phi\,(d) = m, \tag{7.51}$$

όπου $\mathfrak{D}_m := \{d \in \mathbb{N} : d \mid m\}$ (βλ. Β.2.34). Ιδιαιτέρως, για κάθε πρώτο αριθμό p ισχύει η ισότητα

$$\sum_{d \in \mathfrak{D}_{p-1}} \phi\,(d) = p-1. \tag{7.52}$$

ΑΠΟΔΕΙΞΗ. Βλ. πρόταση Β.4.31. □

7.3.7 Πρόταση. *Για κάθε πρώτο αριθμό p η ομάδα $\left(\mathbb{Z}_p^\times, \cdot\right)$ είναι κυκλική.*

[55] Για οιουσδήποτε $j, j' \in \{0,1,...,d-1\}$ με $j < j'$ έχουμε $[l]_p^j \neq [l]_p^{j'}$, διότι εάν υποθέταμε ότι $[l]_p^j = [l]_p^{j'}$ θα έπρεπε να ισχύει $[l]_p^{j-j} = [1]_p$, ήτοι κάτι που είναι αδύνατο, αφού $\mathrm{ord}([l]_p) = d$ και $j - j' < d$.

ΑΠΟΔΕΙΞΗ. Κατά το 7.3.5 (iii), για κάθε $d \in \mathbb{N}$ με $d \mid p-1$ έχουμε $\mathfrak{N}_p(d) \le \phi(d)$. Κατά συνέπειαν, το 7.3.5 (i) δίδει

$$p-1 = \sum_{d \in \mathfrak{D}_{p-1}} \mathfrak{N}_p(d) \le \sum_{d \in \mathfrak{D}_{p-1}} \phi(d). \tag{7.53}$$

Επειδή (λόγω τής (7.52)) το δεξιό μέλος τής ανισοϊσότητας (7.53) ισούται ωσαύτως με $p-1$, όλες οι ανισοϊσότητες $\mathfrak{N}_p(d) \le \phi(d)$ οφείλουν να ισχύουν *ταυτοχρόνως* ως *ισότητες*! Ιδιαιτέρως, για $d = p-1$ λαμβάνουμε $\mathfrak{N}_p(p-1) = \phi(p-1) \ge 1$, οπότε υφίσταται τουλάχιστον ένα στοιχείο τής $\mathbb{Z}_p^\times$ που έχει τάξη ίση με

$$p-1 = \phi(p) = \left|\mathbb{Z}_p^\times\right|$$

και, ως εκ τούτου, η $\left(\mathbb{Z}_p^\times, \cdot\right)$ είναι κυκλική επί τη βάσει τής προτάσεως 2.3.7. □

7.3.8 Λήμμα. *Έστω p ένας πρώτος αριθμός. Τότε για ακεραίους αριθμούς i, a, b, ν ισχύουν τα ακόλουθα*:

(i) *Εάν $i \in \{1,...,p-1\}$, τότε $p \mid \binom{p}{i}$.*

(ii) *Εάν $\nu \ge 1$ και $a \equiv b (\mathrm{mod}\, p^\nu)$, τότε $a^p \equiv b^p (\mathrm{mod}\, p^{\nu+1})$.*

(iii) *Εάν $\nu \ge 2$ και ο p είναι περιττός, τότε $(1+ap)^{p^{\nu-2}} \equiv (1+ap^{\nu-1}) (\mathrm{mod}\, p^\nu)$.*

(iv) *Εάν $\nu \ge 2$ και ο p είναι περιττός με $p \nmid a$, τότε*

$$(1+ap)^{p^{\nu-1}} \equiv 1 (\mathrm{mod}\, p^\nu) \text{ και } (1+ap)^{p^{\nu-2}} \not\equiv 1 (\mathrm{mod}\, p^\nu).$$

ΑΠΟΔΕΙΞΗ. (i) Βλ. λήμμα B.4.10.

(ii) Εάν $\exists \lambda \in \mathbb{Z} : a = b + \lambda p^\nu$, τότε

$$a^p = (b+\lambda p^\nu)^p = \sum_{j=0}^{p} \binom{p}{j} b^{p-j} (\lambda p^\nu)^j$$

$$= b^p + \binom{p}{1} b^{p-1} \lambda p^\nu + \binom{p}{2} b^{p-2} \lambda^2 p^{2\nu} + \cdots + \binom{p}{p-1} b \lambda^{p-1} p^{\nu(p-1)} + \lambda^p p^{\nu p}$$

$$= b^p + p^\nu \left(\binom{p}{1} b^{p-1} \lambda + \binom{p}{2} b^{p-2} (\lambda p)^2 + \cdots + \binom{p}{p-1} b (\lambda p)^{p-1} + p(\lambda^p p^{p-1}) \right).$$

Επειδή (κατά το (i)) $p \mid \binom{p}{i}$ για κάθε $i \in \{1,...,p-1\}$, έχουμε $p^{\nu+1} \mid a^p - b^p$.

(iii) Θα χρησιμοποιήσουμε μαθηματική επαγωγή ως προς τον ν. Για $\nu = 2$ η ισοτιμία είναι προδήλως αληθής. Υποθέτουμε ότι αυτή είναι ωσαύτως αληθής για κάποιον $\nu \ge 2$, ήτοι ότι ισχύει $(1+ap)^{p^{\nu-2}} \equiv (1+ap^{\nu-1}) (\mathrm{mod}\, p^\nu)$. Κατόπιν εφαρμογής τού (ii) (με το $(1+ap)^{p^{\nu-2}}$ στη θέση τού εκεί παρατεθέντος a και με το $1+ap^{\nu-1}$ στη θέση τού εκεί παρατεθέντος b) λαμβάνουμε

$$(1+ap)^{p^{\nu-1}} = \left((1+ap)^{p^{\nu-2}}\right)^p \equiv \left(1+ap^{\nu-1}\right)^p (\mathrm{mod}\, p^{\nu+1}).$$

Επειδή

$$\left(1+ap^{\nu-1}\right)^p = \sum_{j=0}^{p} \tbinom{p}{j}(ap^{\nu-1})^j$$

$$= 1 + ap^\nu + p^{\nu+1}\left(\tfrac{1}{2}a^2(p-1)p^{\nu-2} + \sum_{j=3}^{p}\tbinom{p}{j}a^j p^{\nu(j-1)-(j+1)}\right)$$

με $\nu(j-1)-(j+1) \geq 0$ για κάθε $j \in \{3,...,p\}$, έχουμε

$$(1+ap)^{p^{\nu-1}} \equiv (1+ap^\nu)(\mathrm{mod}\, p^{\nu+1}),$$

οπότε η ισοτιμία είναι αληθής και για τον $\nu+1$.
(iv) Εάν $\nu \geq 2$, τότε εφαρμόζοντας το (iii) για τον $\nu+1$ λαμβάνουμε

$$(1+ap)^{p^{\nu-1}} \equiv (1+ap^\nu)(\mathrm{mod}\, p^{\nu+1}) \Rightarrow p^{\nu+1} \mid (1+ap)^{p^{\nu-1}} - (1+ap^\nu),$$

οπότε

$$\left.\begin{array}{r} p^\nu \mid (1+ap)^{p^{\nu-1}} - 1 - ap^\nu \\ p^\nu \mid ap^\nu \end{array}\right\} \underset{\text{B.1.5 (vi)}}{\Longrightarrow} p^\nu \mid (1+ap)^{p^{\nu-1}} - 1.$$

Τέλος, $(1+ap)^{p^{\nu-2}} \underset{\text{(iii)}}{\equiv} (1+ap^{\nu-1})(\mathrm{mod}\, p^\nu) \not\equiv 1(\mathrm{mod}\, p^\nu)$, διότι $p \nmid a$. □

7.3.9 Πρόταση. *Εάν $\nu \in \mathbb{N}$, $\nu \geq 2$, και εάν ο p είναι ένας περιττός πρώτος αριθμός, τότε η ομάδα $(\mathbb{Z}_{p^\nu}^\times, \cdot)$ είναι κυκλική.*

ΑΠΟΔΕΙΞΗ. Επειδή $\left|\mathbb{Z}_{p^\nu}^\times\right| = \phi(p^\nu) = p^{\nu-1}(p-1)$ και[56] μκδ$(p^{\nu-1}, p-1) = 1$, το θεώρημα 7.1.49 μας πληροφορεί ότι υπάρχει μία και μόνον υποομάδα H τής $\mathbb{Z}_{p^\nu}^\times$ τάξεως $p^{\nu-1}$ και μία και μόνον υποομάδα K τής $\mathbb{Z}_{p^\nu}^\times$ τάξεως $p-1$, ούτως ώστε να ισχύει

$$\mathbb{Z}_{p^\nu}^\times = H \times_{\text{εσ.}} K \cong H \times K.$$

Αρκεί λοιπόν (λόγω τού πορίσματος 7.1.66) να αποδείξουμε ότι αμφότερες οι H, K είναι κυκλικές. Για την κλάση ισοτιμίας $[1+p]_{p^\nu}$ έχουμε (μέσω τού (iv) τού λήμματος 7.3.8 για $a=1$)

$$([1+p]_{p^\nu})^{p^{\nu-1}} = [1]_{p^\nu} \quad \text{και} \quad ([1+p]_{p^\nu})^{p^{\nu-2}} \neq [1]_{p^\nu}.$$

Από την ανωτέρω ισότητα προκύπτει (λόγω τής προτάσεως 2.3.8) ότι η τάξη $\mathrm{ord}([1+p]_{p^\nu})$ τού στοιχείου $[1+p]_{p^\nu}$ τής $\mathbb{Z}_{p^\nu}^\times$ διαιρεί τον $p^{\nu-1}$. Κατά συνέπειαν, κατά το λήμμα B.3.14, $\exists \xi \in \{0,1,...,\nu-1\} : \mathrm{ord}([1+p]_{p^\nu}) = p^\xi$. Υποθέτοντας ότι $\xi < \nu-1$, καταλήγουμε σε άτοπο, καθόσον

$$([1+p]_{p^\nu})^{p^\xi} = [1]_{p^\nu} \Rightarrow ([1+p]_{p^\nu})^{p^{\nu-2}} = (([1+p]_{p^\nu})^{p^\xi})^{p^{\nu-2-\xi}} = [1]_{p^\nu}.$$

[56] Κατά το (iii) τής προτάσεως B.2.14, μκδ$(p, p-1)$ = μκδ$(p-(p-1), p-1)$ = μκδ$(1, p-1) = 1$, απ' όπου έπεται ότι μκδ$(p^{\nu-1}, p-1) = 1$ (μέσω τού πορίσματος B.2.13).

Ως εκ τούτου, $\mathrm{ord}([1+p]_{p^\nu}) = p^{\nu-1}$ και η H είναι κυκλική (βλ. 2.3.7). Επιπροσθέτως, το 1ο θεώρημα ισομορφισμών 4.5.2, εφαρμοζόμενο για τον επιμορφισμό ομάδων $f : (\mathbb{Z}_{p^\nu}^\times, \cdot) \longrightarrow (\mathbb{Z}_p^\times, \cdot)$, $[l]_{p^\nu} \longmapsto f([l]_{p^\nu}) := [l]_p$, δίδει $\mathbb{Z}_{p^\nu}^\times/\mathrm{Ker}(f) \cong \mathbb{Z}_p^\times$, οπότε

$$\frac{\left|\mathbb{Z}_{p^\nu}^\times\right|}{|\mathrm{Ker}(f)|} = \frac{p^{\nu-1}(p-1)}{|\mathrm{Ker}(f)|} = \left|\mathbb{Z}_p^\times\right| = p-1 \Rightarrow |\mathrm{Ker}(f)| = p^{\nu-1}.$$

Επειδή η H είναι η μόνη υποομάδα τής $\mathbb{Z}_{p^\nu}^\times$ τάξεως $p^{\nu-1}$, έχουμε κατ' ανάγκην $\mathrm{Ker}(f) = H$. Δυνάμει τής προτάσεως 7.1.29,

$$\mathbb{Z}_{p^\nu}^\times = H \times_{\text{εσ.}} K \Rightarrow K \cong \mathbb{Z}_{p^\nu}^\times/H = \mathbb{Z}_{p^\nu}^\times/\mathrm{Ker}(f) \cong \mathbb{Z}_p^\times.$$

Επειδή η $\mathbb{Z}_p^\times$ (κατά την πρόταση 7.3.7) είναι κυκλική, η K είναι ωσαύτως κυκλική. (Βλ. 2.4.19 (iii).) □

7.3.10 Πρόταση. *Εάν $\nu \in \mathbb{N}$ και εάν ο p είναι ένας περιττός πρώτος αριθμός, τότε η ομάδα $(\mathbb{Z}_{2p^\nu}^\times, \cdot)$ είναι κυκλική.*

ΑΠΟΔΕΙΞΗ. Επειδή $\text{μκδ}(2, p) = \text{μκδ}(2, p^\nu) = 1$, έχουμε $\mathbb{Z}_{2p^\nu} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{p^\nu}$ (μέσω τού θεωρήματος 7.1.64), οπότε το πόρισμα 7.3.3 δίδει $\mathbb{Z}_{2p^\nu}^\times \cong \mathbb{Z}_2^\times \times \mathbb{Z}_{p^\nu}^\times \cong \mathbb{Z}_{p^\nu}^\times$. Ο τελευταίος ισομορφισμός οφείλεται στο ότι η $\mathbb{Z}_2^\times$ είναι τετριμμένη. (Βλ. 7.1.55 (iv).) Λόγω τής προτάσεως 7.3.9 η $\mathbb{Z}_{2p^\nu}^\times$ είναι κυκλική. (Βλ. 2.4.19 (iii)). □

7.3.11 Λήμμα. *Εάν $k \in \mathbb{N}$, $k \geq 2$, τότε ισχύουν τα εξής:*

(i) *Εντός τής $(\mathbb{Z}_{2^k}^\times, \cdot)$ έχουμε* $\mathrm{ord}([5]_{2^k}) = 2^{k-2}$.

(ii) *Για οιουσδήποτε $i, j \in \mathbb{N}_0$, $0 \leq i, j < 2^{k-2}$, $i \neq j$, ισχύει (εντός τής $(\mathbb{Z}_{2^k}^\times, \cdot)$)*

$$\left[\pm 5^i\right]_{2^k} \neq \left[\pm 5^j\right]_{2^k} \quad (\Longleftrightarrow \pm 5^i \not\equiv \pm 5^j (\mathrm{mod}\, 2^k)).$$

ΑΠΟΔΕΙΞΗ. (i) Για $k = 2$ έχουμε $5 \equiv 1 (\mathrm{mod}\, 4)$, οπότε ο ισχυρισμός είναι αληθής. Από εδώ και στο εξής θα υποθέσουμε ότι $k \geq 3$. Αρκεί να αποδείξουμε ότι

$$5^{2^{k-3}} \equiv (1 + 2^{k-1}) (\mathrm{mod}\, 2^k), \tag{7.54}$$

διότι τότε (προφανώς) $5^{2^{k-3}} \not\equiv 1 (\mathrm{mod}\, 2^k)$ και

$$5^{2^{k-2}} = (5^{2^{k-3}})^2 \equiv (1 + 2^{k-1})^2 \equiv 1 (\mathrm{mod}\, 2^k), \tag{7.55}$$

οπότε[57] $\mathrm{ord}([5]_{2^k}) = 2^{k-2}$. Για την απόδειξη τής (7.54) θα εργασθούμε με τη βοήθεια τής μαθηματικής επαγωγής ως προς τον k. Για $k = 3$ η ισοτιμία (7.54) είναι

[57] Από την (7.55) προκύπτει (λόγω τής προτάσεως 2.3.8) ότι $\mathrm{ord}([5]_{2^k}) \mid 2^{k-2}$. Επομένως $\exists \xi \in \{0, 1, \ldots, k-2\}$: $\mathrm{ord}([5]_{2^k}) = 2^\xi$. Υποθέτοντας ότι $\xi < k-2$, καταλήγουμε σε άτοπο, καθόσον

$$([5]_{2^k})^{2^{k-2}} = [1]_{2^k} \Rightarrow ([5]_{2^k})^{2^{k-3}} = (([5]_{2^k})^{2^\xi})^{2^{k-3-\xi}} = [1]_{2^k}.$$

προδήλως αληθής. Υποθέτουμε ότι είναι αληθής για κάποιον $k \geq 3$. Η επαγωγική υπόθεση δίδει $5^{2^{k-3}} \equiv (1+2^{k-1}) (\mathrm{mod}\, 2^k)$. Κατόπιν εφαρμογής τού (ii) τού λήμματος 7.3.8 (με το $5^{2^{k-3}}$ ως a και με το $1+2^{k-1}$ ως b) λαμβάνουμε

$$5^{2^{(k+1)-3}} = 5^{2^{k-2}} = (5^{2^{k-3}})^2 \equiv (1+2^{k-1})^2 (\mathrm{mod}\, 2^{k+1}).$$

Σημειωτέον ότι

$$2k-2 \geq k+1 \geq 4 \Rightarrow (1+2^{k-1})^2 = 1+2^k+2^{2k-2} \equiv \left(1+2^k\right) (\mathrm{mod}\, 2^{k+1}).$$

Εξ αυτού έπεται ότι η (7.54) είναι αληθής και για τον $k+1$.

(ii) Ας υποθέσουμε ότι[58] $\exists i, j \in \mathbb{N}_0, 0 \leq i < j < 2^{k-2} : \left[\pm 5^i\right]_{2^k} = \left[\pm 5^j\right]_{2^k}$. Επειδή $5 \equiv 1 (\mathrm{mod}\, 4)$, οι θεωρηθείσες κλάσεις ισοτιμίας οφείλουν να έχουν το ίδιο πρόσημο[59]. Επομένως,

$$\left.\begin{array}{r} 5^j \equiv 5^i (\mathrm{mod}\, 2^k) \Rightarrow 5^{j-i} \cdot 5^i \equiv 1 \cdot 5^i (\mathrm{mod}\, 2^k) \\ \text{μκδ}(5,2) = 1 \underset{\text{B.2.13}}{\Longrightarrow} \text{μκδ}(5^i, 2) = 1 \end{array}\right\} \underset{\text{B.4.4 (v)}}{\Longrightarrow} 5^{j-i} \equiv 1 (\mathrm{mod}\, 2^k),$$

ήτοι $([5]_{2^k})^{j-i} = [1]_{2^k}$. Σύμφωνα με το (i) και την πρόταση 2.3.8,

$$2^{k-2} \mid j-i \Rightarrow \text{ είτε } j-i = 0 \text{ είτε } 2^{k-2} \leq j-i.$$

Τούτο μας οδηγεί σε άτοπο: Το μεν πρώτο ενδεχόμενο αποκλείεται διότι $i < j$, το δε δεύτερο διότι $j-i < 2^{k-2}$. □

7.3.12 Πρόταση. *Εάν $k \in \mathbb{N}, k \geq 3$, τότε η $(\mathbb{Z}_{2^k}^\times, \cdot)$ δεν είναι κυκλική. Συγκεκριμένα, υφίσταται ένας ισομορφισμός $\mathbb{Z}_{2^k}^\times \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{k-2}}$.*

ΑΠΟΔΕΙΞΗ. Θέτοντας $H := \langle [-1]_{2^k} \rangle$ και $K := \langle [5]_{2^k} \rangle$, παρατηρούμε ότι $|H| = 2$ και $|K| = 2^{k-2}$ (με την τελευταία ισότητα οφειλόμενη στο (i) τού λήμματος 7.3.11). Επειδή έχουμε $\left|\mathbb{Z}_{2^k}^\times\right| = \phi(2^k) = 2^{k-1}$, από το (ii) τού λήμματος 7.3.11 έπεται ότι

$$\mathbb{Z}_{2^k}^\times = \left\{ \left[\pm 5^i\right]_{2^k} \middle| i \in \mathbb{N}_0, i < 2^{k-2} \right\}.$$

Κατά συνέπειαν, $\mathbb{Z}_{2^k}^\times = HK$ και $H \cap K = \{[1]_{2^k}\} \underset{101}{\Longrightarrow} \mathbb{Z}_{2^k}^\times \cong H \times K$, όπου $H \cong \mathbb{Z}_2$ και $K \cong \mathbb{Z}_{2^{k-2}}$ (βλ. 2.4.23 (ii)). Άρα $\mathbb{Z}_{2^k}^\times \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{k-2}}$ (βλ. 7.1.55 (v)). □

7.3.13 Θεώρημα. (Συνθήκες «κυκλικότητας» τής $\mathbb{Z}_m^\times$. C.F. Gauss, 1801) *Έστω $m \in \mathbb{N}, m \geq 2$. Τα ακόλουθα είναι ισοδύναμα*:

(i) *Η ομάδα $(\mathbb{Z}_m^\times, \cdot)$ είναι κυκλική.*

(ii) $m \in \{2, 4\} \cup \{p^\nu \,|\nu \in \mathbb{N},\ p \text{ πρώτος } \geq 3\} \cup \{2p^\nu \,|\nu \in \mathbb{N},\ p \text{ πρώτος } \geq 3\}$.

[58] Η απόδειξη είναι πανομοιότυπη εάν υποθέσουμε ότι $j < i$. (Αρκεί η εναλλαγή των ρόλων των i και j εντός αυτής.)

[59] Σημειωτέον ότι μκδ$(5, 2) = 1$ και, ως εκ τούτου, μκδ$(5^i, 2^k) = 1$ (βλ. B.2.13 για $i > 0$). Εάν λοιπόν ίσχυε $\left[5^i\right]_{2^k} = \left[-5^j\right]_{2^k}$ ή $\left[-5^i\right]_{2^k} = \left[5^j\right]_{2^k}$, τότε $2^k \mid 5^i(5^{j-i}+1) \Rightarrow 2^k \mid 5^i+1$ (βλ. B.2.9). Επιπροσθέτως, επειδή $5 \equiv 1 (\mathrm{mod}\, 4) \Rightarrow 5^i \equiv 1 (\mathrm{mod}\, 4)$ (βλ. B.4.4 (iii)), θα είχαμε $5^i + 1 \equiv 2 (\mathrm{mod}\, 4)$ (βλ. B.4.4 (ii)), ήτοι $4 \nmid 5^i+1$, και θα καταλήγαμε *σε άτοπο*. ($4 \mid 2^k, 2^k \mid 5^i+1$, αλλά $4 \nmid 5^i+1$, βλ. B.1.5 (v).)

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Έστω $m \in \mathbb{N}$, $m \geq 2$. Υποθέτοντας ότι

$$m \notin \{2,4\} \cup \{p^\nu \,|\nu \in \mathbb{N},\ p \text{ πρώτος } \geq 3\} \cup \{2p^\nu \,|\nu \in \mathbb{N},\ p \text{ πρώτος } \geq 3\},$$

αρκεί να αποδείξουμε ότι η ομάδα $(\mathbb{Z}_m^\times, \cdot)$ δεν είναι κυκλική. Προφανώς, υπό την ανωτέρω υπόθεση το m θα γράφεται (λόγω τού θεμελιώδους θεωρήματος Β.3.7 τής Αριθμητικής) υπό τη μορφή

$$m = \begin{cases} 2^k,\ (k \in \mathbb{N},\ k \geq 3) & \text{εάν } \nexists p \text{ πρώτος } \geq 3 : p \mid m, \\ \\ 2^k p_1^{\nu_1} p_2^{\nu_2} \cdots p_\kappa^{\nu_\kappa},\ (k \in \mathbb{N}_0, \kappa \in \mathbb{N}) & \text{εάν } \exists p \text{ πρώτος } \geq 3 : p \mid m, \end{cases}$$

όπου οι $p_1,...,p_\kappa$ είναι περιττοί πρώτοι αριθμοί με $p_1 < \cdots < p_\kappa$ (όταν $\kappa \geq 2$) και $\nu_1,...,\nu_\kappa \in \mathbb{N}$, με την ακόλουθη συνεπαγωγή ως επιπρόσθετο περιορισμό στη δεύτερη περίπτωση:

$$\kappa = 1 \Longrightarrow k \geq 2.$$

Περίπτωση πρώτη. Εάν $\nexists p$ περιττός πρώτος με $p \mid m$, τότε $m = 2^k$, $k \geq 3$, οπότε η $\mathbb{Z}_m^\times = \mathbb{Z}_{2^k}^\times$ δεν είναι κυκλική επί τη βάσει τής προτάσεως 7.3.12.

Περίπτωση δεύτερη. Εάν $\exists p$ περιττός πρώτος με $p \mid m$ και $k \in \{0,1,2\}$, $\kappa \geq 2$, τότε (λόγω τού πορίσματος 7.3.3) έχουμε

$$\mathbb{Z}_m^\times \cong \begin{cases} \mathbb{Z}_{p_1^{\nu_1}}^\times \times \mathbb{Z}_{p_2^{\nu_2}}^\times \times \cdots \times \mathbb{Z}_{p_\kappa^{\nu_\kappa}}^\times, & \text{όταν } k \in \{0,1\}, \\ \\ \mathbb{Z}_4^\times \times \mathbb{Z}_{p_1^{\nu_1}}^\times \times \mathbb{Z}_{p_2^{\nu_2}}^\times \times \cdots \times \mathbb{Z}_{p_\kappa^{\nu_\kappa}}^\times, & \text{όταν } k = 2. \end{cases}$$

Λαμβάνοντας υπ' όψιν την πρόταση 7.3.9, το (ii) τού θεωρήματος 2.4.23, τον ισομορφισμό $\left(\mathbb{Z}_4^\times, \cdot\right) \cong (\mathbb{Z}_2, +)$ και το (v) τής προτάσεως 7.1.55 συμπεραίνουμε ότι

$$\mathbb{Z}_m^\times \cong \begin{cases} \mathbb{Z}_{(p_1-1)p_1^{\nu_1-1}} \oplus \cdots \oplus \mathbb{Z}_{(p_\kappa-1)p_\kappa^{\nu_\kappa-1}}, & \text{όταν } k \in \{0,1\}, \\ \\ \mathbb{Z}_2 \oplus \mathbb{Z}_{(p_1-1)p_1^{\nu_1-1}} \oplus \cdots \oplus \mathbb{Z}_{(p_\kappa-1)p_\kappa^{\nu_\kappa-1}}, & \text{όταν } k = 2, \end{cases}$$

οπότε η $(\mathbb{Z}_m^\times, \cdot)$ δεν είναι κυκλική λόγω τού θεωρήματος 7.1.64, αφού καθένας εκ των ευθέων προσθετέων έχει ως τάξη του έναν άρτιο αριθμό. Εάν, από την άλλη μεριά, $k \geq 3$ και $\kappa \geq 1$, τότε (λόγω τού πορίσματος 7.3.3) έχουμε

$$\mathbb{Z}_m^\times \cong \mathbb{Z}_{2^k}^\times \times \mathbb{Z}_{p_1^{\nu_1}}^\times \times \cdots \times \mathbb{Z}_{p_\kappa^{\nu_\kappa}}^\times.$$

Από τις προτάσεις 7.3.9 και 7.3.12 προκύπτει ένας ισομορφισμός

$$\mathbb{Z}_m^\times \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{k-2}} \oplus \mathbb{Z}_{(p_1-1)p_1^{\nu_1-1}} \oplus \cdots \oplus \mathbb{Z}_{(p_\kappa-1)p_\kappa^{\nu_\kappa-1}},$$

οπότε και σε αυτήν την περίπτωση συμπεραίνουμε ότι η $(\mathbb{Z}_m^\times, \cdot)$ δεν είναι κυκλική (εκ νέου λόγω τού θεωρήματος 7.1.64).

(ii)⇒(i) Η $\left(\mathbb{Z}_2^\times, \cdot\right)$ είναι τετριμμένη και η $\left(\mathbb{Z}_4^\times, \cdot\right)$ κυκλική τάξεως 2. Το ότι η $(\mathbb{Z}_m^\times, \cdot)$ είναι κυκλική και στις λοιπές περιπτώσεις (ήτοι όταν $m = p^\nu$ ή $m = 2p^\nu$, όπου p περιττός πρώτος) έχει αποδειχθεί στις προτάσεις 7.3.9 και 7.3.10. □

7.4 ΠΟΤΕ ΕΙΝΑΙ Η $\mathbb{Z}_n$ Η ΜΟΝΗ ΟΜΑΔΑ ΤΑΞΕΩΣ n;

Το ερώτημα είναι εύλογο και λίαν ενδιαφέρον: *Για ποιους φυσικούς αριθμούς n είναι όλες οι ομάδες τάξεως n κυκλικές* (ήτοι ισόμορφες με την $(\mathbb{Z}_n, +)$); Ως γνωστόν, *όλες* οι πεπερασμένες ομάδες που έχουν ως τάξη τους έναν *πρώτο αριθμό* p είναι κυκλικές (βλ. πόρισμα 4.1.33). Ωστόσο, όταν $n = pq$, όπου p, q πρώτοι αριθμοί, η $(\mathbb{Z}_n, +)$ άλλοτε *είναι* και άλλοτε *δεν είναι* (μέχρις ισομορφισμού) η μόνη ομάδα τάξεως n. Επί παραδείγματι, η $(\mathbb{Z}_{15}, +)$ είναι (μέχρις ισομορφισμού) *η μόνη* ομάδα τάξεως $15 = 3 \cdot 5$ (βλ. 5.7.16 (i), καθόσον $5 \not\equiv 1 (\mathrm{mod}\, 3)$), αλλά για $n = 3 \cdot 7$ υπάρχουν *δύο* (μη ισόμορφες) ομάδες τάξεως 21. (Συγκεκριμένα, οι $(\mathbb{Z}_{21}, +)$ και $(\mathbf{L}_{21}, \cdot)$, διότι $7 \equiv 1 (\mathrm{mod}\, 3)$, βλ. 5.7.16 (ii).) Επίσης, όταν $p = q$, τότε υπάρχουν *δύο* (μη ισόμορφες) ομάδες τάξεως pq (οι $\mathbb{Z}_{p^2}$ και $\mathbb{Z}_p \oplus \mathbb{Z}_p$, βλ. θεώρημα 7.1.46).

Πιθανολογείται ότι αυτό το πρόβλημα θα πρέπει να είχε διατυπωθεί ήδη κατά τα μέσα τού 19ου αιώνα. Η πρώτη ευρέως γνωστή λύση ενός γενικότερου προβλήματος που το περιέχει (ως υποπρόβλημα, βλ. θεώρημα 9.1.39) οφείλεται στον L.E. Dickson[60] (1874-1954). Έκτοτε έχει αποδειχθεί πολλάκις στη συναφή αρθρογραφία (με διαφορετικές μεθόδους, από πληθώρα μαθηματικών). Η κατωτέρω παρατιθέμενη λύση του (που βασίζεται σε δημοσιεύσεις των D. Jungnickel[61] και J.A. Gallian και D. Moulton[62], βλ. θεώρημα 7.4.2) χρησιμοποιεί μόνον τεχνικά μέσα που μας είναι οικεία, εκκινώντας από το ακόλουθο:

7.4.1 Λήμμα. *Κάθε πεπερασμένη μη κυκλική ομάδα, οι γνήσιες υποομάδες τής οποίας είναι κυκλικές, διαθέτει (τουλάχιστον) μία μη τετριμμένη γνήσια ορθόθετη υποομάδα.*

ΑΠΟΔΕΙΞΗ. Θα υποθέσουμε ότι υπάρχει κάποια πεπερασμένη μη κυκλική ομάδα $(G, \cdot)$, με όλες τις γνήσιες υποομάδες της κυκλικές, η οποία δεν διαθέτει καμία μη τετριμμένη γνήσια ορθόθετη υποομάδα, και θα καταλήξουμε σε άτοπο.

Βήμα 1ο. Εάν H και K είναι δυο μεγιστικές υποομάδες[63] τής G (βλ. 2.1.34 (i)) και $H \neq K$, τότε $H \cap K = \{e_G\}$. Πράγματι· επειδή οι H και K (ως γνήσιες υποομάδες τής G) είναι (εξ υποθέσεως) κυκλικές, δηλαδή $H = \langle x \rangle$, $K = \langle y \rangle$, για κάποια $x, y \in G$, για κάθε στοιχείο x^k ($k \in \mathbb{Z}$) τής H, για κάθε στοιχείο y^l ($l \in \mathbb{Z}$) τής K και για κάθε στοιχείο $z \in H \cap K$ με $z = x^m = y^n$ (για κάποιους $m, n \in \mathbb{Z}$) έχουμε

$$\left\{ \begin{array}{l} x^k(H \cap K)(x^k)^{-1} \ni x^k z x^{-k} = x^k x^m x^{-k} = x^m = z \in H \cap K, \\ y^l(H \cap K)(y^l)^{-1} \ni y^l z y^{-l} = y^l y^n y^{-l} = y^n = z \in H \cap K. \end{array} \right\}$$

[60] L.E. Dickson: *Definitions of a group and a field by independent postulates*, Trans. A.M.S. **6** (1905), 198-204. [Βλ., ιδιαιτέρως, σελ. 200.]

[61] D. Jungnickel: *On the Uniqueness of the Cyclic Group of Order n*, The American Math. Monthly **99** (1992), 545-547.

[62] J.A. Gallian & D. Moulton: *When is $\mathbb{Z}_n$ the only group of order n?*, Elem. Math. **48** (1993), 117-119.

[63] Επειδή η G είναι μη κυκλική, έχουμε $|G| \geq 4$, οπότε υπάρχει κάποιος πρώτος διαιρέτης $p \geq 2$ τής $|G|$ και, κατ' επέκταση, τουλάχιστον μία υποομάδα τής G τάξεως p (βλ. 5.7.1). Αυτό σημαίνει ότι *όλες* οι μεγιστικές της υποομάδες είναι *μη τετριμμένες*.

Επομένως, $H \sqsubseteq \mathrm{N}_G(H\cap K) \sqsubseteq G$ και $K \sqsubseteq \mathrm{N}_G(H\cap K) \sqsubseteq G$. Τούτο έχει ως συνέπεια (λόγω τής μεγιστικότητας των H και K) ότι *είτε* $\mathrm{N}_G(H\cap K) \sqsubset G$ και $\mathrm{N}_G(H\cap K) = H = K$ *είτε* $\mathrm{N}_G(H\cap K) = G$. Το πρώτο ενδεχόμενο είναι εξ υποθέσεως αποκλεισθέν. Άρα (λόγω τού (iii) τής προτάσεως 5.2.4 και τού ότι η G δεν διαθέτει -εξ υποθέσεως- καμία μη τετριμμένη γνήσια ορθόθετη υποομάδα) ισχύει η συνεπαγωγή $H\cap K \trianglelefteq \mathrm{N}_G(H\cap K) = G \Longrightarrow H\cap K = \{e_G\}$.

Βήμα 2ο. Θεωρούμε μια μεγιστική υποομάδα H τής G. Επειδή (εξ υποθέσεως) η H είναι κυκλική και δεν είναι ορθόθετη, έχουμε

$$\left.\begin{array}{r}\text{5.2.2 (ii)}\\ \text{5.2.4 (vi)}\end{array}\right\} \Longrightarrow H \sqsubseteq \mathrm{C}_G(H) \sqsubseteq \mathrm{N}_G(H) \sqsubseteq G \underset{\text{5.2.4 (iii)}}{\Longrightarrow} H = \mathrm{C}_G(H) = \mathrm{N}_G(H).$$

Κατά συνέπειαν[64],

$$\left.\begin{array}{r}\mathrm{N}_G(H) := \left\{g\in G \,\middle|\, gHg^{-1} = H\right\} = H\\ \text{4.2.16} \Rightarrow |H| = \left|gHg^{-1}\right|,\ \forall g\in G\end{array}\right\} \underset{\text{(από το 1ο βήμα)}}{\Longrightarrow} \left[\begin{array}{c} H\cap gHg^{-1} = \{e_G\},\\ \forall g\in G\smallsetminus H.\end{array}\right]$$

Το πλήθος των στοιχείων τής G που είναι $\neq e_G$ και ανήκουν στην H και στις συζυγείς υποομάδες της (εντός τής G) οι οποίες είναι $\neq H$ ισούται με

$$\begin{aligned}(|H|-1)\,|G:\mathrm{N}_G(H)| &= (|H|-1)\,|G:H|\\ &= |G| - |G:H| = (1-\tfrac{1}{|H|})\,|G| \geq \tfrac{1}{2}\,|G|\,.\end{aligned}$$

(Βλ. εδ. 5.2.8, 4.1.20 και 4.1.22.) Επειδή $|G:H|\geq 2$ και το πλήθος των στοιχείων των ανηκόντων στην H και στις (λοιπές) συζυγείς υποομάδες της ισούται με $|G| - |G:H| + 1$, το σύνολο $G\smallsetminus(H\cup \bigcup\limits_{g\in G\smallsetminus H} gHg^{-1})$ είναι μη κενό. Έστω u ένα στοιχείο αυτού και έστω K μια μεγιστική υποομάδα τής G που το περιέχει[65]. Επαναλαμβάνοντας τα ανωτέρω επιχειρήματα για την K διαπιστώνουμε ότι το πλήθος των στοιχείων τής G που είναι $\neq e_G$ και ανήκουν στην K και στις (λοιπές) συζυγείς υποομάδες της (εντός τής G) είναι $\geq \frac{1}{2}\,|G|$. Επειδή $H\cap K = \{e_G\}$ (από το 1ο βήμα), αυτό σημαίνει ότι η G διαθέτει *τουλάχιστον* $\frac{1}{2}\,|G| + \frac{1}{2}\,|G| + 1 = |G| + 1$ στοιχεία. Άτοπο! □

7.4.2 Θεώρημα. *Δοθέντος ενός $n\in\mathbb{N}$, $n\geq 2$, οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) $\mu\kappa\delta(n,\phi(n)) = 1$, *όπου ϕ η συνάρτηση φι τού Euler* (βλ. Β.4.15).

(ii) $n = p_1\cdots p_k$, $k\in\mathbb{N}$, *όπου p_1,...,p_k είναι σαφώς διακεκριμένοι πρώτοι αριθμοί για τους οποίους ισχύει $p_i \not\equiv 1 (\mathrm{mod}\, p_j)$ για οιουσδήποτε $i,j\in\{1,...,k\}$, $i\neq j$, όταν $k\geq 2$.*

(iii) H *$(\mathbb{Z}_n,+)$ είναι (μέχρις ισομορφισμού) η μοναδική ομάδα τάξεως n.* (*Ισοδυνάμως*: *Όλες οι ομάδες τάξεως n είναι ισόμορφες με την $(\mathbb{Z}_n,+)$.*)

[64] Είναι φανερό ότι οι υποομάδες gHg^{-1}, $g\in G\smallsetminus H$, είναι ωσαύτως μεγιστικές.

[65] Προφανώς, $K\neq H$ και $K\neq gHg^{-1}$, $\forall g\in G\smallsetminus H$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν υποθέσουμε ότι ο n γράφεται υπό τη μορφή $n = p^\nu m$ για κάποιους φυσικούς αριθμούς m, ν με $\nu \geq 2$, όπου ο p είναι τυχών πρώτος αριθμός για τον οποίο ισχύει $p \nmid m$, τότε

$$\left.\begin{array}{r} p \mid p^\nu m\,(=n) \\ p \mid p^{\nu-1}(p-1)\phi\,(m)\ (=\phi\,(n)) \\ \text{(βλ. 7.3.2 και 7.3.3 ή (B.38))} \end{array}\right\} \underset{\text{B.2.6}}{\Longrightarrow} p \mid \text{μκδ}(n, \phi(n)) \Rightarrow \text{μκδ}(n, \phi(n)) > 1.$$

Άτοπο! Άρα $n = p_1 \cdots p_k$, $k \in \mathbb{N}$, όπου $p_1, ..., p_k$ είναι πρώτοι αριθμοί και μάλιστα σαφώς διακεκριμένοι όταν $k \geq 2$. Εξάλλου, εάν υποθέσουμε ότι $k \geq 2$ και ότι υπάρχουν $i_0, j_0 \in \{1,...,k\}$, $i_0 \neq j_0$, τέτοιοι ώστε να ισχύει η ισοτιμία

$$p_{i_0} \equiv 1 (\mathrm{mod}\, p_{j_0}),$$

τότε

$$\left.\begin{array}{r} p_{j_0} \mid n \\ p_{j_0} \mid (p_1 - 1) \cdots (p_k - 1)\,(=\phi\,(n)) \\ \text{(βλ. 7.3.3 ή (B.38))} \end{array}\right\} \underset{\text{B.2.6}}{\Longrightarrow} p \mid \text{μκδ}(n, \phi(n)) \Rightarrow \text{μκδ}(n, \phi(n)) > 1.$$

Άτοπο! Άρα $p_i \not\equiv 1 (\mathrm{mod}\, p_j)$ για οιουσδήποτε $i, j \in \{1,...,k\}$, $i \neq j$, όταν $k \geq 2$.

(ii)⇒(i) Τούτο είναι προδήλως αληθές.

(ii)⇒(iii) Θα εργασθούμε εκ νέου με «εις άτοπον απαγωγή». Υποθέτουμε ότι υπάρχουν φυσικοί αριθμοί που ικανοποιούν *τις ως άνω* (αριθμητικές) *συνθήκες* (τού (ii)) και είναι τέτοιοι, ώστε να υφίστανται *μη κυκλικές* πεπερασμένες ομάδες έχουσες αυτούς ως τάξεις τους. Έστω n_* το *ελάχιστο* στοιχείο τού συνόλου των φυσικών αριθμών με την εν λόγω ιδιότητα. (Εξ υποθέσεως,

$$n_* = p_1 \cdots p_k \ \text{ όπου } \ p_i \not\equiv 1 (\mathrm{mod}\, p_j)$$

για κατάλληλους σαφώς διακεκριμένους πρώτους αριθμούς $p_1,...,p_k$. Επιπροσθέτως, λόγω αυτής τής επιλογής τού n_*, κάθε ομάδα τάξεως $< n_*$ είναι *κατ' ανάγκην* κυκλική.) Θεωρούμε τυχούσα μη κυκλική ομάδα $(G, \cdot)$ τάξεως n_*. Κάθε *γνήσια* υποομάδα τής G είναι κατ' ανάγκην κυκλική. Σύμφωνα με το λήμμα 7.4.1 η G διαθέτει (τουλάχιστον) μία μη τετριμμένη γνήσια ορθόθετη υποομάδα H. Προφανώς, εξαιτίας τού ορισμού τού n_*,

$$\left.\begin{array}{r} 1 < |H| < |G| = n_* \\ |G/H| = \frac{n_*}{|H|} < n_* \end{array}\right\} \Longrightarrow [\text{αμφότερες οι } H \text{ και } G/H \text{ είναι κυκλικές}].$$

Θέτοντας $m := |H|$ λαμβάνουμε $m = p_{\varrho_1} \cdots p_{\varrho_s}$, όπου $\{\varrho_1, ..., \varrho_s\} \subsetneqq \{1,...,k\}$, $s \in \mathbb{N}$ και $s < k$ (βλ. 4.1.22 και B.3.14). Βάσει τού (ii) τού θεωρήματος 2.4.32,

$$\mathrm{Aut}(H) \cong \mathrm{Aut}(\mathbb{Z}_m) \cong \mathbb{Z}_m^\times \Longrightarrow |\mathrm{Aut}(H)| = \phi\,(m) = (p_{\varrho_1} - 1) \cdots (p_{\varrho_s} - 1).$$

Από την άλλη μεριά, το θεώρημα 5.4.26 μας πληροφορεί ότι η πηλικοομάδα $\mathrm{N}_G(H)/\mathrm{C}_G(H)$ είναι εμφυτεύσιμη στην $\mathrm{Aut}(H)$ (ήτοι ισόμορφη με μια υποομάδα τής $\mathrm{Aut}(H)$). Επομένως,

$$\left.\begin{array}{r} 4.1.22 \Longrightarrow |\mathrm{N}_G(H)/\mathrm{C}_G(H)| \mid \phi(m) \\ m \mid n \underset{\text{B.4.22}}{\Longrightarrow} \phi(m) \mid (p_1-1)\cdots(p_k-1) = \phi(n_*) \\ H \lhd G \underset{\text{5.2.4 (iii)}}{\Longrightarrow} \mathrm{N}_G(H) = G \\ |G/\mathrm{C}_G(H)| = |\mathrm{N}_G(H)/\mathrm{C}_G(H)| = \frac{n_*}{|C_G(H)|} \end{array}\right\} \Rightarrow \left[\begin{array}{l} |G/\mathrm{C}_G(H)| \mid \phi(n_*) \\ \text{και } |G/\mathrm{C}_G(H)| \mid n_* \end{array}\right].$$

Αυτό σημαίνει ότι

$$|G/\mathrm{C}_G(H)| \mid \text{μκδ}(n_*, \phi(n_*)) = 1 \Rightarrow |G/\mathrm{C}_G(H)| = 1,$$

ήτοι ότι η $G = \mathrm{C}_G(H)$ είναι αβελιανή[66]. Εάν $k = 1$, τότε $|G| = n_* = p_1$, οπότε η G (κατά το πόρισμα 4.1.33) είναι κυκλική. Άτοπο! Εάν $k \geq 2$, τότε μκδ$(p_1, p_2 \cdots p_k) = 1$ και το θεώρημα 7.1.49 μας διασφαλίζει την ύπαρξη μίας και μόνον υποομάδας K_1 τής G τάξεως $|K_1| = p_1$ και μίας και μόνον υποομάδας K_1' τής G τάξεως $|K_1'| = p_2 \cdots p_k$, ούτως ώστε να ισχύει $G \cong K_1 \times K_1'$. Εφαρμόζοντας και πάλι το θεώρημα 7.1.49 (με την K_1' στη θέση τής G) λαμβάνουμε έναν ισομορφισμό $K_1' \cong K_2 \times K_2'$, όπου $|K_2| = p_2$ και $|K_2'| = p_3 \cdots p_k$ (για $k \geq 3$). Ύστερα από επανάληψη αυτής τής διαδικασίας (όσες φορές απαιτείται από το μέγεθος τού k) καταλήγουμε σε έναν ισομορφισμό

$$\left.\begin{array}{r} G \cong K_1 \times K_2 \times \cdots \times K_k, \text{ όπου } K_j \text{ ομ. τάξεως} \\ |K_j| = p_j \underset{\text{4.1.33}}{\Longrightarrow} K_j \cong \mathbb{Z}_{p_j},\ \forall j \in \{1,...,k\} \end{array}\right\} \underset{\text{7.1.55 (v)}}{\Longrightarrow} G \cong \mathbb{Z}_{p_1} \oplus \mathbb{Z}_{p_2} \oplus \cdots \oplus \mathbb{Z}_{p_k}.$$

Επειδή μκδ$(p_i, p_j) = 1$ για οιουσδήποτε $i, j \in \{1,...,k\}$, $i \neq j$, συμπεραίνουμε (μέσω τού θεωρήματος 7.1.62) ότι $G \cong \mathbb{Z}_{n_*}$, ήτοι ότι η G είναι (και σε αυτήν την περίπτωση) κυκλική. Άτοπο!

(iii)⇒(ii) Υποθέτουμε ότι όλες οι ομάδες που έχουν τάξη ίση με τον δοθέντα n είναι κυκλικές (και, ως εκ τούτου, ισόμορφες με την $(\mathbb{Z}_n, +)$) και ότι τουλάχιστον μία εκ των ως άνω (αριθμητικών) συνθηκών (τού (ii)) δεν ικανοποιείται. (Φυσικά, εξ αυτού έπεται ότι ο ίδιος ο n δεν είναι πρώτος αριθμός.) Εάν υπήρχε πρώτος αριθμός p, τέτοιος ώστε να ισχύει $p^2 \mid n$, τότε θα καταλήγαμε σε άτοπο, καθόσον η ομάδα $\mathbb{Z}_p \oplus \mathbb{Z}_{\frac{n}{p}}$ θα είχε τάξη n χωρίς να είναι κυκλική[67] (βλ. θεώρημα 7.1.64). Άρα ο n γράφεται ως γινόμενο (τουλάχιστον δύο) *σαφώς διακεκριμένων* πρώτων. Επειδή μκδ$(n, \phi(n)) > 1$, υπάρχουν πρώτοι αριθμοί p, q διαιρούντες τον n με $p < q$ και $q \equiv 1 (\mathrm{mod}\, p)$. Εν τοιαύτη περιπτώσει, το ευθύ γινόμενο $\mathbf{L}_{pq} \times \mathbb{Z}_{\frac{n}{pq}}$ (όπου $\mathbf{L}_{pq}$ είναι η μη αβελιανή ομάδα η ορισθείσα στο εδάφιο 5.7.13) έχει τάξη n χωρίς να είναι αβελιανή (πόσω δε μάλλον κυκλική) ομάδα (βλ. 7.1.57 (ii)). Άτοπο! □

[66] Η ισότητα $G = \mathrm{C}_G(H)$ ισοδυναμεί με το ότι $H \sqsubseteq Z(G)$ (βλ. πρόταση 5.4.3). Επειδή η G/H είναι κυκλική, η πρόταση 5.4.20 μας πληροφορεί ότι η G είναι αβελιανή.

[67] Προφανώς, $p^2 \mid n \Rightarrow \exists \lambda \in \mathbb{Z} : n = \lambda p^2 \Rightarrow$ μκδ$(p, \frac{n}{p})$ = μκδ$(p, \lambda p) = p > 1$.

7.5 ΧΑΜΙΛΤΟΝΙΑΝΕΣ ΟΜΑΔΕΣ

Ως γνωστόν, κάθε υποομάδα μιας αβελιανής ομάδας είναι ορθόθετη. (Βλ. πρόταση 4.2.6.) Επίσης, υπάρχουν *μη αβελιανές* ομάδες, όπως π.χ. η ομάδα $\mathbf{Q}$ των τετρανίων, κάθε υποομάδα των οποίων είναι ορθόθετη. (Βλ. εδ. 4.2.18.) Ένας πλήρης χαρακτηρισμός αυτών των (όχι κατ' ανάγκην πεπερασμένων) ομάδων δίδεται στο θεώρημα 7.5.3, το οποίο οφείλεται στον Reinhold Baer[68] (1902-1979) και το οποίο γενικεύει προγενέστερα σχετικά αποτελέσματα των Richard Dedekind[69] (1831-1916), George Abram Miller[70] (1863-1951) και Ernst Wendt[71] (1872-1946).

7.5.1 Ορισμός. Μια μη αβελιανή ομάδα καλείται **ομάδα τού Hamilton**[72] ή **χαμιλτονιανή ομάδα** όταν *κάθε* υποομάδα της είναι ορθόθετη.

7.5.2 Λήμμα. *Εάν $(G,\cdot)$ είναι μια μη αβελιανή ομάδα, κάθε κυκλική υποομάδα τής οποίας είναι ορθόθετη, τότε ισχύουν τα εξής*:

(i) *Η G είναι περιοδική ομάδα.*

(ii) *Κάθε μη αβελιανή υποομάδα τής G περιέχει μια υποομάδα που είναι $\cong \mathbf{Q}$.*

ΑΠΟΔΕΙΞΗ. (i) Έστω τυχόν $x \in G$. Θα αποδείξουμε ότι $\mathrm{ord}(x) < \infty$.

Περίπτωση πρώτη. Εάν $x \notin Z(G)$, τότε υπάρχει $y \in G$, τέτοιο ώστε να ισχύει $xy \neq yx$. Θέτοντας $w := [x,y] \neq e_G$ και λαμβάνοντας υπ' όψιν ότι $\langle x\rangle \trianglelefteq G$ και $\langle y\rangle \trianglelefteq G$, παρατηρούμε ότι

$$\left.\begin{aligned} w &= \underbrace{(xyx^{-1})}_{\in\langle y\rangle}\underbrace{y^{-1}}_{\in\langle y\rangle} \in \langle y\rangle \\ w &= \underbrace{x}_{\in\langle x\rangle}\underbrace{(yx^{-1}y^{-1})}_{\in\langle x\rangle} \in \langle x\rangle \end{aligned}\right\} \Rightarrow w \in \langle x\rangle \cap \langle y\rangle\,,$$

απ' όπου έπεται ότι $\exists (m,n) \in (\mathbb{Z}\setminus\{0\}) \times (\mathbb{Z}\setminus\{0\})$: $w = x^m = y^n$. Επομένως,

$$\left.\begin{aligned} wx = x^{m+1} = xw \Rightarrow w \in \mathbf{C}_G(x) \\ wy = y^{n+1} = yw \Rightarrow w \in \mathbf{C}_G(y) \end{aligned}\right\} \Rightarrow w \in \mathbf{C}_G(x) \cap \mathbf{C}_G(y)$$

και η ισότητα (5.43) τού (ix) τής προτάσεως 5.5.2 δίδει

$$e_G = [w,w] = [x^m, y^n] = [x,y]^{mn} = w^{mn} \Rightarrow \mathrm{ord}(w) = |\langle w\rangle| \leq mn < \infty,$$

οπότε $\mathrm{ord}(x) = |\langle x\rangle| \leq m^2 n < \infty$ (διότι $(x^m)^{mn} = e_G$).

[68] R. Baer: *Situation der Untergruppen und Struktur der Gruppe*, S.-B. Heidelberg. Akad. Wiss. **2** (1933), 12-17.

[69] R. Dedekind: *Über Gruppen, deren sämmtliche Theiler Normaltheiler sind*, Mathematische Annalen **48** (1897), 548-561.

[70] G.A. Miller: *On the Hamilton groups*, Bulletin of the American Mathematical Society **4** (1898), 510-515.

[71] E. Wendt: *Hamiltonsche Gruppen*, Mathematische Annalen **59** (1904), 187-192.

[72] Προς τιμήν τού William Rowan Hamilton (1805-1865) που ανακάλυψε το 1843 *το στρεβλό σώμα των τετρανίων* (μέσω τού οποίου ορίζεται *η ομάδα των τετρανίων*).

Περίπτωση δεύτερη. Εάν $x \in Z(G)$, τότε θεωρώντας ένα $y \notin Z(G)$, παρατηρούμε ότι[73] $xy \notin Z(G)$. Κατά τα προαναφερθέντα (στην πρώτη περίπτωση) υπάρχουν $\kappa, \lambda \in \mathbb{N}$, τέτοιοι ώστε

$$\mathrm{ord}(y) = \kappa \ \text{και} \ \mathrm{ord}(xy) = \lambda.$$

Συνεπώς, $x \in Z(G) \Rightarrow xy = yx \underset{2.1.12}{\Longrightarrow} e_G = (xy)^\lambda = x^\lambda y^\lambda \Rightarrow x^\lambda = y^{-\lambda}$, απ' όπου έπεται ότι $\mathrm{ord}(x^\lambda) = \mathrm{ord}((y^{-1})^\lambda) \underset{2.3.11}{=} \frac{\kappa}{\text{μκδ}(\kappa,\lambda)}$ (καθόσον $\mathrm{ord}(y^{-1}) \underset{2.3.9\,(i)}{=} \kappa$) και, κατ' επέκταση, ότι $x^{\frac{\kappa\lambda}{\text{μκδ}(\kappa,\lambda)}} \underset{B.2.29}{=} x^{\text{εκπ}(\kappa,\lambda)} = e_G \Rightarrow \mathrm{ord}(x) \leq \text{εκπ}(\kappa,\lambda) < \infty$.

(ii) Έστω M μια μη αβελιανή υποομάδα τής G και έστω

$$\mathcal{A} := \{\, (g_1, g_2) \in M \times M |\ g_1 g_2 \neq g_2 g_1 \,\}.$$

Επιλέγουμε ένα ζεύγος $(x, y) \in \mathcal{A}$ με την ιδιότητα

$$\mathrm{ord}(x) + \mathrm{ord}(y) = \min\{\, \mathrm{ord}(g_1) + \mathrm{ord}(g_2) |\ (g_1, g_2) \in \mathcal{A} \}.$$

Επειδή $x \notin Z(G) \Rightarrow x \neq e_G \Rightarrow \mathrm{ord}(x) \geq 2$, υπάρχει κάποιος πρώτος αριθμός p, τέτοιος ώστε $p \mid \mathrm{ord}(x)$. Εάν θέσουμε $w := [x, y] = x^m = y^n$ (όπως πράξαμε στην πρώτη περίπτωση τού (i)), τότε

$$\mathrm{ord}(x^p) \underset{2.3.11}{=} \tfrac{\mathrm{ord}(x)}{\text{μκδ}(\mathrm{ord}(x),p)} = \tfrac{\mathrm{ord}(x)}{p} < \mathrm{ord}(x)$$

$$\Longrightarrow \mathrm{ord}(x^p) + \mathrm{ord}(y) < \mathrm{ord}(x) + \mathrm{ord}(y) \Longrightarrow (x^p, y) \notin \mathcal{A}$$

$$\Longrightarrow x^p y = y x^p \underset{5.5.2\,(ix)}{\Longrightarrow} e_G = [x^p, y] = [x, y]^p = w^p,$$

οπότε $[\mathrm{ord}(w) = |\langle w \rangle| \leq p \ \text{και} \ |\langle w \rangle| = |\langle x^m \rangle| \mid |\langle x \rangle| = \mathrm{ord}(x)] \Rightarrow \mathrm{ord}(w) = p$. Κατά συνέπειαν,

$$p = \mathrm{ord}(w) = \mathrm{ord}(x^m) \underset{2.3.11}{=} \tfrac{\mathrm{ord}(x)}{\text{μκδ}(\mathrm{ord}(x),|m|)}, \tag{7.56}$$

οπότε ο p είναι ο *μόνος*[74] πρώτος αριθμός ο οποίος διαιρεί την τάξη $\mathrm{ord}(x)$ τού x. Επειδή[75] $p \mid \mathrm{ord}(y)$, επαναλαμβάνοντας την ίδια επιχειρηματολογία (με το y στη

[73] Εάν ίσχυε $xy \in Z(G)$, τότε θα είχαμε $x^{-1}(xy) = y \in Z(G)$.

[74] Έστω ότι οι $\mathrm{ord}(x) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ και $|m| = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ είναι παραστάσεις των $\mathrm{ord}(x)$ και $|m|$ ως γινομένων (κατάλληλων δυνάμεων) πρώτων αριθμών $p_1, p_2, \ldots, p_k$, $k \in \mathbb{N}$, οι οποίοι είναι σαφώς διακεκριμένοι (όταν $k > 1$) και $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k \in \mathbb{N}_0$ (με τουλάχιστον έναν εκ των $\alpha_1, \ldots, \alpha_k$ κατ' ανάγκην διάφορο τού μηδενός). Τότε η (7.56), σε συνδυασμό με την πρόταση B.3.16, δίδει

$$p = \prod_{j=1}^{k} p_j^{\alpha_j - \min\{\alpha_j, \beta_j\}} \underset{B.3.7}{\Longrightarrow} \left[\begin{array}{c} \exists \ell \in \{1, \ldots, k\} : \alpha_j \leq \beta_j,\ \forall j \in \{1, \ldots, k\} \setminus \{\ell\}, \\ \text{με } \beta_\ell = \alpha_\ell - 1 \ \text{και} \ p_\ell = p \end{array} \right].$$

[75] Η συνεπαγωγή $p \mid \mathrm{ord}(x) \Longrightarrow p \mid \mathrm{ord}(y)$ έπεται από το ότι

$$\mathrm{ord}(w) = \mathrm{ord}(x^m) = \mathrm{ord}(y^n) \Longrightarrow \tfrac{\mathrm{ord}(x)}{\text{μκδ}(\mathrm{ord}(x),|m|)} = \tfrac{\mathrm{ord}(y)}{\text{μκδ}(\mathrm{ord}(y),|n|)}.$$

θέση τού x και το n στη θέση τού m) αποδεικνύουμε ότι ο p είναι ο *μόνος* πρώτος αριθμός ο οποίος διαιρεί την τάξη $\mathrm{ord}(y)$ τού y. Επομένως,

$$\exists (i,j) \in \mathbb{N}_0 \times \mathbb{N}_0 : \mathrm{ord}(x) = p^{i+1} \ \text{ και } \ \mathrm{ord}(y) = p^{j+1}.$$

Προφανώς,

$$p = \tfrac{p^{i+1}}{\mu\kappa\delta(p^{i+1},|m|)} \Rightarrow p^i = \mu\kappa\delta(p^{i+1},|m|) \Rightarrow \left[|m| = p^i c, \ \text{για κάποιον } c \in \mathbb{N} : p \nmid c\right]$$

και

$$p = \tfrac{p^{j+1}}{\mu\kappa\delta(p^{j+1},|n|)} \Rightarrow p^j = \mu\kappa\delta(p^{j+1},|n|) \Rightarrow \left[|n| = p^i d, \ \text{για κάποιον } d \in \mathbb{N} : p \nmid d\right].$$

Επειδή $[c]_p \in \mathbb{Z}_p^{\times}$ (και αντιστοίχως, $[d]_p \in \mathbb{Z}_p^{\times}$), υπάρχει $b \in \{1,...,p-1\}$ (και αντιστοίχως, $a \in \{1,...,p-1\}$) με

$$[c]_p [b]_p = [1]_p \Leftrightarrow cb \equiv 1 (\mathrm{mod}\, p) \Leftrightarrow [\exists \nu \in \mathbb{N}_0 : cb - 1 = p\nu],$$

και αντιστοίχως, με $[d]_p [a]_p = [1]_p \Leftrightarrow da \equiv 1 (\mathrm{mod}\, p) \Leftrightarrow [\exists \xi \in \mathbb{N}_0 : da - 1 = p\xi]$. Προφανώς,

$$\begin{aligned} w^{ab} &= (x^m)^{ab} = (x^{\mathrm{sign}(m)})^{p^i cab} = (x^{\mathrm{sign}(m)})^{p^i \left(\frac{p\nu+1}{b}\right)ab} = (x^{\mathrm{sign}(m)})^{p^i a(p\nu+1)} \\ &= (\underbrace{(x^{\mathrm{sign}(m)})^{p^{i+1}}}_{=e_G})^{a\nu} (x^{\mathrm{sign}(m)})^{p^i a} = ((x^{\mathrm{sign}(m)})^a)^{p^i}, \end{aligned}$$

και αντιστοίχως,

$$\begin{aligned} w^{ab} &= (y^n)^{ab} = (y^{\mathrm{sign}(n)})^{p^j dab} = (y^{\mathrm{sign}(n)})^{p^j \left(\frac{p\xi+1}{a}\right)ab} = (y^{\mathrm{sign}(n)})^{p^j b(p\xi+1)} \\ &= (\underbrace{(y^{\mathrm{sign}(n)})^{p^{j+1}}}_{=e_G})^{b\xi} (y^{\mathrm{sign}(n)})^{p^j b} = ((y^{\mathrm{sign}(n)})^b)^{p^j}. \end{aligned}$$

Θέτοντας $\widetilde{x} := (x^{\mathrm{sign}(m)})^a$, $\widetilde{y} := (y^{\mathrm{sign}(n)})^b$ και $\widetilde{w} := w^{(\mathrm{sign}(m)a)(\mathrm{sign}(n)b)}$ λαμβάνουμε

$$\widetilde{x}^{p^i} = w^{ab} = [x,y]^{ab} = \widetilde{y}^{p^j} \tag{7.57}$$

και $\widetilde{w} = [x,y]^{(\mathrm{sign}(m)a)(\mathrm{sign}(n)b)} = [\widetilde{x},\widetilde{y}] \neq e_G$, όπου

$$\left\{ \begin{array}{l} p \nmid a \Rightarrow \mathrm{ord}(\widetilde{x}) = \mathrm{ord}(x^a) = \frac{p^{i+1}}{\mu\kappa\delta(p^{i+1},a)} = p^{i+1}, \\ p \nmid b \Rightarrow \mathrm{ord}(\widetilde{y}) = \mathrm{ord}(y^b) = \frac{p^{j+1}}{\mu\kappa\delta(p^{j+1},b)} = p^{j+1}, \\ p \nmid ab \Rightarrow \mathrm{ord}(\widetilde{w}) = \mathrm{ord}(w^{ab}) = \frac{p}{\mu\kappa\delta(p,ab)} = p. \end{array} \right\} \tag{7.58}$$

Θα αποδείξουμε ότι η $H := \langle \widetilde{x}, \widetilde{y} \rangle \sqsubseteq M$ είναι ισόμορφη με την ομάδα $\mathbf{Q}$ των τετρανίων. Κατ' αρχάς, σημειώνουμε ότι κανένας εκ των i, j δεν μπορεί να ισούται με 0. Εάν, π.χ., $j = 0$, τότε θα ίσχυε $\widetilde{y} = w^{ab} = \widetilde{w}^{\mathrm{sign}(m)\mathrm{sign}(n)} = [\widetilde{x}^{\mathrm{sign}(m)}, \widetilde{y}^{\mathrm{sign}(n)}]$, οπότε

$$\widetilde{y}^{1+\mathrm{sign}(n)} = \widetilde{x}^{\mathrm{sign}(m)} \widetilde{y}^{\mathrm{sign}(n)} \widetilde{x}^{-\mathrm{sign}(m)}. \tag{7.59}$$

Εάν $\text{sign}(n) = -1$, τότε η (7.59) θα έδιδε $\widetilde{y} = e_G$, κάτι που είναι αδύνατο. Εάν $\text{sign}(n) = 1$, τότε τα $\widetilde{y}^2$ και $\widetilde{y}$ θα ήταν συζυγή, οπότε θα είχαμε κατ' ανάγκην

$$p = \text{ord}(\widetilde{y}) = \text{ord}(\widetilde{y}^{\,2}) = \tfrac{p}{\text{μκδ}(p,2)} \Rightarrow \text{μκδ}(p,2) = 1 \Rightarrow p = 2,$$

δηλαδή $\text{ord}(\widetilde{y}) = 2 \Rightarrow \widetilde{y}^2 = e_G$ και η (7.59) θα έδιδε εκ νέου $\widetilde{y} = e_G$. (Παρομοίως αποδεικνύεται ότι $i \neq 0$.) Επομένως, δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $i \geq j \geq 1$. Για οιονδήποτε $l \in \mathbb{Z}$ τα $\widetilde{x}$ και $\widetilde{x}^l\widetilde{y}$ δεν μετατίθενται αμοιβαίως[76], οπότε $(\widetilde{x}, \widetilde{x}^l\widetilde{y}) \in \mathcal{A}$ και

$$\text{ord}(x) + \text{ord}(y) \underset{(7.58)}{=} \text{ord}(\widetilde{x}) + \text{ord}(\widetilde{y}) \leq \text{ord}(\widetilde{x}) + \text{ord}(\widetilde{x}^l\widetilde{y})$$

$$\Longrightarrow \text{ord}(\widetilde{x}^l\widetilde{y}) \geq \text{ord}(\widetilde{y}) = p^{j+1}. \tag{7.60}$$

Στην περίπτωση όπου *είτε* ο p είναι περιττός *είτε* $p = 2$ και $j \geq 2$, έχουμε

$$\text{ord}(\widetilde{w}^{-1}) \underset{2.3.9\ (\text{i})}{=} \text{ord}(\widetilde{w}) \underset{(7.58)}{=} p \mid \tbinom{p^j}{2} = \tfrac{p^j(p^j-1)}{2},$$

οπότε

$$\left\{ \begin{array}{l} e_G \underset{(7.60)}{\neq} (\widetilde{x}^l\widetilde{y})^{p^j} \underset{5.5.2\ (\text{x})}{=} [\widetilde{y}, \widetilde{x}^l]^{\binom{p^j}{2}} \widetilde{x}^{lp^j}\widetilde{y}^{p^j} \underset{5.5.2\ (\text{ix})}{=} [\widetilde{y}, \widetilde{x}]^{l\binom{p^j}{2}} \widetilde{x}^{lp^j}\widetilde{y}^{p^j} \\ = \underbrace{(\widetilde{w}^{-1})^{l\binom{p^j}{2}}}_{=e_G} \widetilde{x}^{lp^j}\widetilde{y}^{p^j} \underset{(7.57)}{=} \widetilde{x}^{lp^j} w^{ab}, \end{array} \right\} \tag{7.61}$$

και η (7.61) μας οδηγεί σε άτοπο εφαρμοζόμενη για $l = -p^{i-j}$, καθώς

$$\widetilde{x}^{-p^i} w^{ab} \underset{(7.57)}{=} e_G.$$

Άρα $p = 2$ και $j = 1$. Παρομοίως αποδεικνύεται ότι $i = 1$. Τελικώς λοιπόν $p = 2$, $i = j = 1$ και οι (7.58) και (7.57) δίδουν $\text{ord}(\widetilde{x}) = \text{ord}(\widetilde{y}) = 4$, $\text{ord}(\widetilde{w}) = \text{ord}(u) = 2$, με $\widetilde{x}^{\,2} = u = \widetilde{y}^{\,2}$, όπου $u := \widetilde{w}^{\,\text{sign}(m)\text{sign}(n)}$. Σημειωτέον ότι[77] $u = \widetilde{w}\,(= [\widetilde{x}, \widetilde{y}])$ (ασχέτως με το ποια είναι τα $\text{sign}(m)$ και $\text{sign}(n)$) και ότι για το γινόμενο $v := \widetilde{x}\,\widetilde{y}$ ισχύει

$$\begin{aligned} v^2 &= (\widetilde{x}\,\widetilde{y})(\widetilde{x}\,\widetilde{y}) = u\widetilde{y}\,\widetilde{x}(\widetilde{x}\,\widetilde{y}) = (u\widetilde{y})(\widetilde{x}^{\,2}\widetilde{y}) \\ &= (u\widetilde{y})^2 \underset{u \in \text{C}_M(\widetilde{y})}{=} u^2\widetilde{y}^{\,2} = e_G\widetilde{y}^{\,2} = \widetilde{y}^{\,2} = u. \end{aligned}$$

Επιπροσθέτως, $\widetilde{y}\,\widetilde{x} = u^2\widetilde{y}\,\widetilde{x} = u(u\widetilde{y}\,\widetilde{x}) = u(\widetilde{x}\,\widetilde{y}) = \widetilde{x}^{\,2}(\widetilde{x}\,\widetilde{y}) = \widetilde{x}^{\,3}\,\widetilde{y} = \widetilde{x}^{\,-1}\,\widetilde{y}$. Επομένως, $H = \{e_G, u, v, v^{-1}, \widetilde{x}, \widetilde{x}^{\,-1}, \widetilde{y}, \widetilde{y}^{\,-1}\}$, έχουσα ως πολλαπλασιαστικό κατάλογό

[76] Προφανώς, $[\widetilde{x}, \widetilde{y}] \neq e_G \Rightarrow \widetilde{y}\widetilde{x} \neq \widetilde{x}\widetilde{y} \Rightarrow (\widetilde{x}^l\widetilde{y})\widetilde{x} = \widetilde{x}^l(\widetilde{y}\widetilde{x}) \neq \widetilde{x}^l(\widetilde{x}\widetilde{y}) = \widetilde{x}(\widetilde{x}^l\widetilde{y})$.

[77] Επειδή $\text{ord}(u) = 2$, έχουμε $u = u^{-1}$.

της τον

$\cdot$	e_G	u	v	v^{-1}	$\widetilde{x}$	$\widetilde{x}^{-1}$	$\widetilde{y}$	$\widetilde{y}^{-1}$
e_G	e_G	u	v	v^{-1}	$\widetilde{x}$	$\widetilde{x}^{-1}$	$\widetilde{y}$	$\widetilde{y}^{-1}$
u	u	e_G	v^{-1}	v	$\widetilde{x}^{-1}$	$\widetilde{x}$	$\widetilde{y}^{-1}$	$\widetilde{y}$
v	v	v^{-1}	u	e_G	$\widetilde{y}$	$\widetilde{y}^{-1}$	$\widetilde{x}^{-1}$	$\widetilde{x}$
v^{-1}	v^{-1}	v	e_G	u	$\widetilde{y}^{-1}$	$\widetilde{y}$	$\widetilde{x}$	$\widetilde{x}^{-1}$
$\widetilde{x}$	$\widetilde{x}$	$\widetilde{x}^{-1}$	$\widetilde{y}^{-1}$	$\widetilde{y}$	u	e_G	v	v^{-1}
$\widetilde{x}^{-1}$	$\widetilde{x}^{-1}$	$\widetilde{x}$	$\widetilde{y}$	$\widetilde{y}^{-1}$	e_G	u	v^{-1}	v
$\widetilde{y}$	$\widetilde{y}$	$\widetilde{y}^{-1}$	$\widetilde{x}$	$\widetilde{x}^{-1}$	v^{-1}	v	u	e_G
$\widetilde{y}^{-1}$	$\widetilde{y}^{-1}$	$\widetilde{y}$	$\widetilde{x}^{-1}$	$\widetilde{x}$	v	v^{-1}	e_G	u

Είναι άμεσος ο έλεγχος τού ότι η απεικόνιση

$$e_G \longmapsto \mathbf{I}_2, \quad u \longmapsto -\mathbf{I}_2, \qquad v \longmapsto \mathbf{i}, \quad v^{-1} \longmapsto -\mathbf{i},$$

$$\widetilde{x} \longmapsto \mathbf{j}, \qquad \widetilde{x}^{-1} \longmapsto -\mathbf{j}, \quad \widetilde{y} \longmapsto \mathbf{k}, \quad \widetilde{y}^{-1} \longmapsto -\mathbf{k},$$

από την H επί τής $\mathbf{Q}$ αποτελεί έναν ισομορφισμό ομάδων. □

7.5.3 Θεώρημα. (R. Baer, 1933) *Για μια ομάδα $(G,\cdot)$ τα ακόλουθα είναι ισοδύναμα*:

(i) *H G είναι χαμιλτονιανή ομάδα.*

(ii) *$G = H \times_{\text{εσ.}} K \times_{\text{εσ.}} L$, όπου $H \cong \mathbf{Q}$, K μια περιοδική αβελιανή ομάδα έχουσα εκθέτη ≤ 2 και L μια περιοδική αβελιανή ομάδα, κάθε στοιχείο τής οποίας έχει ως τάξη του κάποιον περιττό φυσικό αριθμό.*

ΑΠΟΔΕΙΞΗ ΤΗΣ ΣΥΝΕΠΑΓΩΓΗΣ (i)⇒(ii). Έστω G μια χαμιλτονιανή ομάδα. Σύμφωνα με το (i) τού λήμματος 7.5.2, αυτή είναι περιοδική.

Βήμα 1ο. Για *οιαδήποτε* $x, y \in G$, το ότι (εξ υποθέσεως) ισχύει $\langle x\rangle \trianglelefteq G$ και $\langle y\rangle \trianglelefteq G$ έχει ως επακόλουθο ότι $\langle x, y\rangle = \langle x\rangle\,\langle y\rangle$ και ότι

$$\left.\begin{array}{r} xy \in \langle x,y\rangle \underset{4.1.22}{\Longrightarrow} \operatorname{ord}(xy) = |\langle xy\rangle| \,|\, |\langle x,y\rangle| \\ |\langle x,y\rangle|\,|\langle x\rangle \cap \langle y\rangle| \underset{(4.35)}{=} |\langle x\rangle|\,|\langle y\rangle| = \operatorname{ord}(x)\operatorname{ord}(y) \end{array}\right\} \Rightarrow \operatorname{ord}(xy) \mid \operatorname{ord}(x)\operatorname{ord}(y). \quad (7.62)$$

Θέτοντας $M := \{\, g \in G \mid \exists j \in \mathbb{N}_0\colon \operatorname{ord}(g) = 2^j\}$ και $L := \{\, g \in G \mid \operatorname{ord}(g) \equiv 1 (\operatorname{mod} 2)\}$ παρατηρούμε ότι $M \cap L = \{e_G\}$ και ότι $M \trianglelefteq G$ και $L \trianglelefteq G$ (λόγω τής ιδιότητας (7.62)). Από την άλλη μεριά, επειδή η τάξη $\operatorname{ord}(g)$ *οιουδήποτε* στοιχείου $g \in G$ γράφεται υπό τη μορφή $\operatorname{ord}(g) = 2^j\lambda$, για κάποιον $j \in \mathbb{N}_0$ και κάποιον $\lambda \in \mathbb{N}$ με $\lambda \equiv 1 (\operatorname{mod} 2)$, το πόρισμα 2.3.15 μας πληροφορεί ότι υπάρχουν $g_1 \in \langle g\rangle \cap M$ και $g_2 \in \langle g\rangle \cap L$, τέτοια ώστε να ισχύει $g = g_1 g_2$, όπου $\operatorname{ord}(g_1) = 2^j$ και $\operatorname{ord}(g_2) = \lambda$. Κατά συνέπειαν,

$$G = ML \Rightarrow G = M \times_{\text{εσ.}} L, \quad (7.63)$$

όπου η L είναι κατ' ανάγκην[78] *αβελιανή* και η M *μη αβελιανή* (αφού η ίδια η G είναι μη αβελιανή). Επιπροσθέτως, η M οφείλει να περιέχει μια υποομάδα $H \cong \mathbf{Q}$. (Βλ. 7.5.2 (ii).)

[78] Εάν η L ήταν μη αβελιανή υποομάδα τής G, τότε θα έπρεπε (σύμφωνα με το (ii) τού λήμματος 7.5.2) να περιέχει μια υποομάδα $\cong \mathbf{Q}$. Τούτο όμως είναι αδύνατο, καθόσον κάθε στοιχείο τής $\mathbf{Q}$ διαφορετικό τού ουδετέρου έχει άρτια τάξη.

Βήμα 2ο. Για διευκόλυνσή μας επιλέγουμε έναν ισομορφισμό $f : \mathbf{Q} \xrightarrow{\cong} H$ και θέτουμε $s := f(\mathbf{j})$ και $t := f(\mathbf{k})$. Προφανώς, $H = f(\mathbf{Q}) = \langle s, t\rangle$ (αφού $\mathbf{Q} = \langle \mathbf{j}, \mathbf{k}\rangle$) και $s^4 = t^4 = e_H = e_G$, $s^2 = t^2 (= f(-\mathbf{I}_2))$, $ts = s^{-1}t = st^{-1} (= f(-\mathbf{i}))$. Ο κεντροποιητής $\mathrm{C}_M(H) = \mathrm{C}_M(s) \cap \mathrm{C}_M(t)$ τής H εντός τής M είναι μια ορθόθετη υποομάδα τής M, αφού

$$H \sqsubseteq M \trianglelefteq G \text{ και (εξ υπ.) } H \trianglelefteq G \underset{4.2.19}{\Longrightarrow} H \trianglelefteq M \underset{5.2.2\,(\mathrm{iii})}{\Longrightarrow} \mathrm{C}_M(H) \trianglelefteq M,$$

οπότε ορίζεται η πηλικοομάδα $M/\mathrm{C}_M(H)$. Επίσης,

$$\mathrm{C}_M(s) \sqsubseteq M \trianglelefteq G \text{ και (εξ υποθ.) } \mathrm{C}_M(s) \trianglelefteq G \underset{4.2.19}{\Longrightarrow} \mathrm{C}_M(s) \trianglelefteq M.$$

Εάν $u \in M \smallsetminus \mathrm{C}_M(s)$, τότε

$$\left.\begin{array}{r} s \in H \trianglelefteq M \Rightarrow usu^{-1} \in H \\ usu^{-1} \in \mathrm{K\Lambda\Sigma}_M(s) \end{array}\right\} \Rightarrow usu^{-1} \in \mathrm{K\Lambda\Sigma}_M(s) \cap H = \mathrm{K\Lambda\Sigma}_H(s) = \{s, s^{-1}\},$$

οπότε

$$u \notin \mathrm{C}_M(s) \Rightarrow usu^{-1} \neq s \Longrightarrow usu^{-1} = s^{-1} \Rightarrow usu^{-1}t = s^{-1}t = ts$$
$$\Rightarrow s(u^{-1}t) = (u^{-1}t)s \Rightarrow u^{-1}t \in \mathrm{C}_M(s) \Rightarrow u \in t\mathrm{C}_M(s).$$

Άρα $M/\mathrm{C}_M(s) = \{\mathrm{C}_M(s), t\mathrm{C}_M(s)\}$ και $|M : \mathrm{C}_M(s)| = 2$. Κατ' αναλογίαν,

$$\mathrm{C}_M(t) \sqsubseteq M \trianglelefteq G \text{ και (εξ υποθ.) } \mathrm{C}_M(t) \trianglelefteq G \underset{4.2.19}{\Longrightarrow} \mathrm{C}_M(t) \trianglelefteq M$$

και εάν $w \in M \smallsetminus \mathrm{C}_M(t)$, τότε

$$\left.\begin{array}{r} t \in H \trianglelefteq M \Rightarrow wtw^{-1} \in H \\ wtw^{-1} \in \mathrm{K\Lambda\Sigma}_M(t) \end{array}\right\} \Rightarrow wtw^{-1} \in \mathrm{K\Lambda\Sigma}_M(t) \cap H = \mathrm{K\Lambda\Sigma}_H(t) = \{t, t^{-1}\},$$

οπότε

$$w \notin \mathrm{C}_M(t) \Rightarrow wtw^{-1} \neq t \Longrightarrow wtw^{-1} = t^{-1} = s^{-1}ts \Rightarrow swtw^{-1} = ts$$
$$\Rightarrow (sw)\,t = t\,(sw) \Rightarrow sw \in \mathrm{C}_M(t) \Rightarrow w \in s^{-1}\mathrm{C}_M(t).$$

Επομένως, $M/\mathrm{C}_M(t) = \{\mathrm{C}_M(t), s^{-1}\mathrm{C}_M(t)\}$ και $|M : \mathrm{C}_M(t)| = 2$. Εξάλλου, είναι άμεσος ο έλεγχος τού ότι οι πλευρικές κλάσεις $\mathrm{C}_M(H)$, $s\,\mathrm{C}_M(H)$, $t\mathrm{C}_M(H)$, $st\,\mathrm{C}_M(H)$ είναι τέσσερα *σαφώς διακεκριμένα* στοιχεία τής $M/\mathrm{C}_M(H)$. Τούτο, σε συνδυασμό με το ότι ισχύει

$$|M : \mathrm{C}_M(H)| = |M : \mathrm{C}_M(s) \cap \mathrm{C}_M(t)| \underset{(4.23)}{\leq} |M : \mathrm{C}_M(s)|\,|M : \mathrm{C}_M(t)| = 4,$$

σημαίνει ότι $M/\mathrm{C}_M(H) = \{\mathrm{C}_M(H), s\,\mathrm{C}_M(H), t\,\mathrm{C}_M(H), st\,\mathrm{C}_M(H)\}$. Έστω $\iota : H \hookrightarrow M$ η συνήθης εμφύτευση ($\iota(h) := h, \forall h \in H$). Επειδή

$$\iota(Z(H)) = Z(H) \subseteq \mathrm{C}_M(H),$$

όπου $Z(H) = Z(f(\mathbf{Q})) = f(Z(\mathbf{Q})) = f(\{\pm\mathbf{I}_2\})$ και

$$H/Z(H) = \{Z(H), s\,Z(H), t\,Z(H), st\,Z(H)\} \cong \mathrm{Inn}(H) \cong \mathbf{V},$$

ορίζεται (σύμφωνα με το θεώρημα 4.5.5) ο κανονιστικός ομομορφισμός

$$\iota^{\pi\eta\lambda\cdot} : H/Z(H) \longrightarrow M/\mathrm{C}_M(H)$$

σε επίπεδο πηλικοομάδων ως ακολούθως:

$$\begin{aligned} Z(H) &\overset{\iota^{\pi\eta\lambda\cdot}}{\longmapsto} \mathrm{C}_M(H), \qquad s\,Z(H) \quad \overset{\iota^{\pi\eta\lambda\cdot}}{\longmapsto} s\,\mathrm{C}_M(H), \\ t\,Z(H) &\overset{\iota^{\pi\eta\lambda\cdot}}{\longmapsto} t\,\mathrm{C}_M(H), \quad st\,Z(H) \quad \overset{\iota^{\pi\eta\lambda\cdot}}{\longmapsto} st\,\mathrm{C}_M(H). \end{aligned}$$

Επειδή, εν προκειμένω, ο $\iota^{\pi\eta\lambda\cdot}$ είναι *ισομορφισμός*, λαμβάνουμε[79]

$$M = \mathrm{Im}(\iota)\,\mathrm{C}_M(H) = H\,\mathrm{C}_M(H). \tag{7.64}$$

Βήμα 3ο. Έστω τυχόν $z \in \mathrm{C}_M(H)$. Επειδή $z \in M$, υπάρχει κάποιος $i \in \mathbb{N}_0$, τέτοιος ώστε να ισχύει $\mathrm{ord}(z) = 2^i$. Εάν υποθέσουμε ότι $i = 2$, ήτοι ότι $\mathrm{ord}(z) = 4$, τότε

$$zs = sz \underset{2.1.12}{\Longrightarrow} (zs)^4 = z^4 s^4 = e_G \underset{2.3.8}{\Longrightarrow} \mathrm{ord}(zs) = |\langle zs\rangle| \mid 4 \Rightarrow \mathrm{ord}(zs) \in \{1, 2, 4\}.$$

Επειδή $t\,(zs)\,t^{-1} = (tz)st^{-1} = (zt)st^{-1} = z(tst^{-1}) = zs^{-1}$, τα zs και zs^{-1} είναι συζυγή, οπότε $\mathrm{ord}(zs) = \mathrm{ord}(zs^{-1})$. Το ενδεχόμενο να ισχύει $\mathrm{ord}(zs) = 1$ αποκλείεται (διότι εν τοιαύτη περιπτώσει $z = s^{-1}$, ενώ το $zs^{-1} = s^{-2}$ έχει τάξη 2). Εάν ίσχυε $\mathrm{ord}(zs) = 2$, τότε θα είχαμε $\langle zs\rangle = \{e_G, zs\}$ και

$$\left.\begin{aligned} \mathrm{ord}(zs) = \mathrm{ord}(zs^{-1}) \Rightarrow z \neq s \Rightarrow zs^{-1} \neq e_G \\ s^2 \neq e_G \Rightarrow s^{-1} \neq s \Rightarrow zs^{-1} \neq zs \\ t(\underbrace{zs}_{\in\langle zs\rangle})t^{-1} = zs^{-1} \notin \langle zs\rangle \end{aligned}\right\} \Rightarrow \langle zs\rangle \not\trianglelefteq G,$$

πράγμα άτοπο, διότι η G είναι χαμιλτονιανή. Επίσης, εάν $\mathrm{ord}(zs) = 4$, τότε θα είχαμε $\langle zs\rangle = \{e_G, zs, (zs)^2, (zs)^3\}$ και

$$\left.\begin{aligned} \mathrm{ord}(zs) = \mathrm{ord}(zs^{-1}) \Rightarrow z \neq s \Rightarrow zs^{-1} \neq e_G \\ s^2 \neq e_G \Rightarrow s^{-1} \neq s \Rightarrow zs^{-1} \neq zs \\ z \neq s = s^{-3} \Rightarrow zs^{-1} \neq z^2 s^2 = (zs)^2 \\ \mathrm{ord}(z) = 4 \Rightarrow z^2 \neq e_G = s^{-4} \Rightarrow zs^{-1} \neq z^3 s^3 = (zs)^3 \\ t(\underbrace{zs}_{\in\langle zs\rangle})t^{-1} = zs^{-1} \notin \langle zs\rangle \end{aligned}\right\} \Rightarrow \langle zs\rangle \not\trianglelefteq G,$$

[79] Βλ. το (b) στη διατύπωση τού θεωρήματος 4.5.5.

πράγμα άτοπο, διότι η G είναι χαμιλτονιανή. Άρα $i \neq 2$. Εν συνεχεία, εάν υποθέσουμε ότι $i \geq 3$, τότε καταλήγουμε εκ νέου σε άτοπο, καθώς

$$z^{i-2} \in \mathrm{C}_M(H) \text{ και } \mathrm{ord}(z^{i-2}) = \tfrac{2^i}{\mu\kappa\delta(2^i, 2^{i-2})} = \tfrac{2^i}{2^{i-2}} = 4.$$

(Αρκεί να επαναληφθεί η προηγούμενη επιχειρηματολογία με το z^{i-2} στη θέση τού z.) Επομένως, $i \in \{0, 1\} \Rightarrow \mathrm{ord}(z) \in \{1, 2\}$, απ' όπου έπεται ότι η $\mathrm{C}_M(H)$ *είναι αβελιανή.* (Βλ. 2.3.9 (iv).)

Βήμα 4ο. Το s^2 είναι το μόνο στοιχείο τής H τάξεως 2. Προφανώς, $s^2 \in \mathrm{C}_M(s)$. Επιπροσθέτως, $s^4 = e_G \Rightarrow s^2 = s^{-2}$, οπότε

$$s^2 t = s^{-2} t = s^{-1}(s^{-1} t) = s^{-1}(ts) = (s^{-1}t)s = (ts)s = ts^2 \Rightarrow s^2 \in \mathrm{C}_M(t)$$

και, ως εκ τούτου,

$$s^2 \in \mathrm{C}_M(s) \cap \mathrm{C}_M(t) = \mathrm{C}_M(H).$$

Άρα $\mathrm{C}_M(H) \cap H = \langle s^2 \rangle$ και $\exp(\mathrm{C}_M(H)) = 2$. (Βλ. 2.3.24.) Επειδή υπάρχει μια υποομάδα[80] K τής $\mathrm{C}_M(H)$, τέτοια ώστε να ισχύει

$$\mathrm{C}_M(H) = \langle s^2 \rangle \times_{\text{εσ.}} K,$$

έχουμε προφανώς

$$M \underset{(7.64)}{=} H\,\mathrm{C}_M(H) = H(\langle s^2 \rangle \times_{\text{εσ.}} K) = HK.$$

Λαμβανομένου υπ' όψιν ότι $H \trianglelefteq M$,

$$K \sqsubseteq M \trianglelefteq G \text{ και (εξ υποθ.) } K \trianglelefteq G \underset{4.2.19}{\Longrightarrow} K \trianglelefteq M$$

και $\langle s^2 \rangle \cap K = \{e_G\} \Rightarrow H \cap K = \{e_G\}$ (διότι τα στοιχεία τού K έχουν τάξη ≤ 2), συμπεραίνουμε τελικώς ότι[81]

$$\left.\begin{array}{r} M = H \times_{\text{εσ.}} K \\ G \underset{(7.63)}{=} M \times_{\text{εσ.}} L \end{array}\right\} \Longrightarrow G = H \times_{\text{εσ.}} K \times_{\text{εσ.}} L.$$

ΑΠΟΔΕΙΞΗ ΤΗΣ ΣΥΝΕΠΑΓΩΓΗΣ (ii)⇒(i). Έστω N *τυχούσα* υποομάδα τής ομάδας $G = H \times_{\text{εσ.}} K \times_{\text{εσ.}} L$ και έστω $f : \mathbf{Q} \xrightarrow{\cong} H$ ένας ισομορφισμός.

Περίπτωση πρώτη. Εάν $N \sqsubseteq K \times_{\text{εσ.}} L$, τότε $N \trianglelefteq K \times_{\text{εσ.}} L$ (διότι η $K \times_{\text{εσ.}} L$ είναι μια αβελιανή υποομάδα τής G), οπότε $N \trianglelefteq G$. (Βλ. 4.2.6 και 7.1.39 (i).)

[80] Εάν εκλάβουμε την αβελιανή ομάδα $\mathrm{C}_M(H)$ ως έναν $\mathbb{Z}_2$-διανυσματικό χώρο και την $\langle s^2 \rangle$ ως γραμμικό υπόχωρό του, τότε (όπως είναι γνωστό από τη Γραμμική Άλγεβρα) υφίσταται κάποιο (μέχρις ισομορφισμού διανυσματικών χώρων μονοσημάντως ορισμένο) συμπλήρωμά του K. Θεωρώντας το (απλώς) ως αβελιανή ομάδα, λαμβάνουμε $\mathrm{C}_M(H) = \langle s^2 \rangle \times_{\text{εσ.}} K$.

[81] Προφανώς, $K = \{e_G\} \Leftrightarrow \mathrm{C}_M(H) = \langle s^2 \rangle$.

Περίπτωση δεύτερη. Ας υποθέσουμε ότι $N \in \mathbf{Subg}(G) \setminus \mathbf{Subg}(K \times_{\text{εσ.}} L)$. Κάθε στοιχείο $x \in N$ γράφεται υπό τη μορφή

$$x = abc, \tag{7.65}$$

για κάποια μονοσημάντως ορισμένα στοιχεία $a \in H$, $b \in K$ και $c \in L$. Επιπροσθέτως, για οιουσδήποτε $\kappa, \lambda \in \mathbb{Z}$ ισχύει

$$\left\{ \begin{array}{c} [7.1.25\text{ (b) (i)} \Rightarrow]\ a(bc) = (bc)a \underset{2.1.12}{\Longrightarrow} a^\kappa (bc)^\kappa = (bc)^\kappa a^\kappa \\ [K \times_{\text{εσ.}} L \text{ αβελιανή}] \Rightarrow bc = cb \underset{2.1.12}{\Longrightarrow} (bc)^\lambda = b^\lambda c^\lambda \end{array} \right\}. \tag{7.66}$$

Επειδή $\mathrm{ord}(c) = 2\nu + 1$ για κάποιον $\nu \in \mathbb{N}_0$, από τις (7.65) και (7.66) προκύπτει ότι[82]

$$\left. \begin{array}{r} x^{2\,\mathrm{ord}(c)} = x^{4\nu+2} = (a^4)^\nu a^2 (b^2)^{2\nu+1} \left(c^{2\nu+1}\right)^2 = a^2 \\ x \in N \Rightarrow x^{2\,\mathrm{ord}(c)} \in N \end{array} \right\} \Rightarrow a^2 \in N. \tag{7.67}$$

Πρώτη υποπερίπτωση. Εάν για κάποιο $x \in N$ το a στην (7.65) έχει τάξη 4, τότε έχουμε κατ' ανάγκην $a \in f(\{\mathbf{i}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\})$, οπότε (μέσω τής (7.67)) συμπεραίνουμε ότι[83] $f(-\mathbf{I}_2) \in N$. Εξ αυτού έπεται ότι

$$\begin{aligned} G' &\underset{7.1.83}{=} H' \times_{\text{εσ.}} K' \times_{\text{εσ.}} L' \underset{5.5.6}{=} H' = f(\mathbf{Q})' \\ &\underset{5.5.10}{=} f(\mathbf{Q}') \underset{5.5.13}{=} f(\{\pm \mathbf{I}_2\}) = \{e_G, f(-\mathbf{I}_2)\} \subseteq N \\ &\underset{2.1.20}{\Longrightarrow} G' \sqsubseteq N \underset{5.5.11}{\Longrightarrow} N \trianglelefteq G. \end{aligned}$$

Δεύτερη υποπερίπτωση. Εάν το a στην (7.65) έχει τάξη ≤ 2 *για κάθε* $x \in N$, τότε

$$a \in f(\{\pm \mathbf{I}_2\}) \underset{5.4.7}{=} f(Z(\mathbf{Q})) \underset{5.4.5}{=} Z(f(\mathbf{Q})) = Z(H),$$

οπότε

$$N \sqsubseteq Z(H) \times_{\text{εσ.}} K \times_{\text{εσ.}} L = Z(H) \times_{\text{εσ.}} Z(K) \times_{\text{εσ.}} Z(L) \underset{7.1.82}{=} Z(G) \underset{5.4.19\text{ (i)}}{\Longrightarrow} N \trianglelefteq G.$$

Τελικό συμπέρασμα: Σε όλες τις περιπτώσεις η N είναι ορθόθετη υποομάδα τής G, οπότε η G είναι χαμιλτονιανή ομάδα. □

7.5.4 Σημείωση. Μεταξύ όλων των πεπερασμένων ομάδων τάξεως ≤ 100 υφίστανται ακριβώς 13 χαμιλτονιανές ομάδες[84].

---

[82] Σημειωτέον ότι, υψώνοντας *οιοδήποτε* στοιχείο τής $\mathbf{Q}$ (και, κατ' επέκταση, και τής H) στη δύναμη 4, λαμβάνουμε το ουδέτερο στοιχείο.

[83] Εάν $a = f(\mathbf{i})$, τότε $a^2 = f(\mathbf{i})^2 = f(\mathbf{i}^2) = f(-\mathbf{I}_2) \in N$. Παρομοίως ισχύει $a^2 = f(-\mathbf{I}_2) \in N$ και για $a \in f(\{-\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\})$. (Βλ. τον πολλαπλασιαστικό κατάλογο τής $\mathbf{Q}$ στο εδ. 2.2.11.)

[84] Βλ. B. Horvat, G. Jaklic & T. Pisanski: *On the number of hamiltonian groups*, Mathematical Communications **10** (2005), 89-94.

7.6 ΗΜΙΕΥΘΕΑ ΓΙΝΟΜΕΝΑ

Το ευθύ γινόμενο δύο ομάδων γενικεύεται κατά τρόπο φυσικό (τόσον στην «εξωτερική» όσον και στην «εσωτερική» του εκδοχή) μέσω τής εννοίας τού *ημιευθέος γινομένου*. (Βλ. 7.6.4 και 7.6.44 (i).)

► **«Εξωτερικό» ημιευθύ γινόμενο δύο ομάδων**. Έστω ότι οι $(G_1, \circledast)$ και $(G_2, \circledcirc)$ είναι τυχούσες ομάδες και ότι η απεικόνιση[85]

$$\varphi : (G_2, \circledcirc) \longrightarrow (\mathrm{Aut}(G_1), \circ)\,,\ x \longmapsto \varphi_x,$$

είναι ένας ομομορφισμός ομάδων, ήτοι[86] $\varphi_{a \circledcirc b} = \varphi_a \circ \varphi_b,\ \forall\,(a,b) \in G_2 \times G_2$. Εφοδιάζουμε το καρτεσιανό γινόμενο $G_1 \times G_2$ των υποκειμένων συνόλων των θεωρουμένων ομάδων με την εσωτερική πράξη

$$\boxed{\begin{array}{c}(G_1 \times G_2) \times (G_1 \times G_2) \longrightarrow G_1 \times G_2 \\ ((x_1, x_2)\,, (y_1, y_2)) \longmapsto (x_1, x_2) \boxtimes_\varphi (y_1, y_2) := \big(x_1 \circledast \varphi_{x_2}(y_1), x_2 \circledcirc y_2\big)\,.\end{array}}$$

7.6.1 Πρόταση. *Το ζεύγος $(G_1 \times G_2, \boxtimes_\varphi)$ αποτελεί ομάδα έχουσα* (*ως προς την ορισθείσα πράξη "$\boxtimes_\varphi$"*) *το (e_{G_1}, e_{G_2}) ως ουδέτερο στοιχείο της και το $(\varphi_{x_2}^{-1}(x_1^{-1}), x_2^{-1})$ ως αντίστροφο* (= *συμμετρικό*) *στοιχείο οιουδήποτε $(x_1, x_2) \in G_1 \times G_2$, όπου x_1^{-1} το αντίστροφο στοιχείο τού $x_1 \in G_1$ ως προς την " $\circledast$ " και x_2^{-1} το αντίστροφο στοιχείο τού $x_2 \in G_2$ ως προς την " $\circledcirc$ "*.

ΑΠΟΔΕΙΞΗ. Εάν $(x_1, x_2)\,, (y_1, y_2)\,, (z_1, z_2) \in G_1 \times G_2$, τότε

$$\begin{aligned}
&[(x_1, x_2) \boxtimes_\varphi (y_1, y_2)] \boxtimes_\varphi (z_1, z_2) = \big(x_1 \circledast \varphi_{x_2}(y_1), x_2 \circledcirc y_2\big) \boxtimes_\varphi (z_1, z_2) \\
&= \big(\big(x_1 \circledast \varphi_{x_2}(y_1)\big) \circledast \varphi_{x_2 \circledcirc y_2}(z_1), (x_2 \circledcirc y_2) \circledcirc z_2\big) \\
&= \big(x_1 \circledast \big(\varphi_{x_2}(y_1) \circledast \varphi_{x_2 \circledcirc y_2}(z_1)\big)\,, (x_2 \circledcirc y_2) \circledcirc z_2\big) \\
&= \big(x_1 \circledast \big(\varphi_{x_2}(y_1) \circledast \big(\varphi_{x_2} \circ \varphi_{y_2}\big)(z_1)\big)\big), x_2 \circledcirc (y_2 \circledcirc z_2)\big) \\
&= \big(x_1 \circledast \big(\varphi_{x_2}(y_1) \circledast \varphi_{x_2}\big(\varphi_{y_2}(z_1)\big)\big)\big), x_2 \circledcirc (y_2 \circledcirc z_2)\big) \\
&= \big(x_1 \circledast \varphi_{x_2}(y_1 \circledast \varphi_{y_2}(z_1)), x_2 \circledcirc (y_2 \circledcirc z_2)\big) \\
&= (x_1, x_2) \boxtimes_\varphi \big(y_1 \circledast \varphi_{y_2}(z_1), y_2 \circledcirc z_2\big) = (x_1, x_2) \boxtimes_\varphi [(y_1, y_2) \boxtimes_\varphi (z_1, z_2)],
\end{aligned}$$

όπου η τρίτη ισότητα έπεται από την προσεταιριστικότητα τής " $\circledast$ ", η τέταρτη ισότητα από το ότι η φ είναι ομομορφισμός και από την προσεταιριστικότητα τής " $\circledcirc$ ", και η έκτη ισότητα από το ότι η φ_{x_2} είναι αυτομορφισμός τής G_1. Κατά συνέπειαν, η εσωτερική πράξη "$\boxtimes_\varphi$" είναι προσεταιριστική. Επίσης, για οιοδήποτε στοιχείο $(x_1, x_2) \in G_1 \times G_2$ έχουμε

$$\begin{aligned}
&(x_1, x_2) \boxtimes_\varphi (e_{G_1}, e_{G_2}) = \big(x_1 \circledast \varphi_{x_2}(e_{G_1}), x_2 \circledcirc e_{G_2}\big) \\
&= (x_1 \circledast e_{G_1}, x_2 \circledcirc e_{G_2}) = (x_1, x_2) = (e_{G_1} \circledast x_1, e_{G_2} \circledcirc x_2) \\
&= (e_{G_1} \circledast \mathrm{id}_{G_1}(x_1), e_{G_2} \circledcirc x_2) = (e_{G_1} \circledast \varphi_{e_{G_2}}(x_1), e_{G_2} \circledcirc x_2) \\
&= (e_{G_1}, e_{G_2}) \boxtimes_\varphi (x_1, x_2)
\end{aligned}$$

[85] Εν προκειμένω, είναι προσφορότερο (για ευνόητους λόγους) να χρησιμοποιούμε το σύμβολο φ_x αντί τού $\varphi(x)$.

[86] Σημειωτέον ότι $\varphi_{e_{G_2}} = e_{\mathrm{Aut}(G_1)} = \mathrm{id}_{G_1}$ και ότι $\varphi_a^j = \varphi_{aj}$ για κάθε $(a, j) \in G_2 \times \mathbb{Z}$.

και

$$\begin{aligned}&(x_1,x_2)\boxtimes_\varphi(\varphi_{x_2}^{-1}(x_1^{-1}),x_2^{-1})=\big(x_1\circledast\varphi_{x_2}(\varphi_{x_2}^{-1}(x_1^{-1})),x_2\circledcirc x_2^{-1}\big)\\&=\big(x_1\circledast x_1^{-1},x_2\circledcirc x_2^{-1}\big)=(e_{G_1},e_{G_2})=(\varphi_{x_2^{-1}}(e_{G_1}),e_{G_2})\\&=(\varphi_{x_2^{-1}}(x_1^{-1})\circledast\varphi_{x_2^{-1}}(x_1),e_{G_2})=(\varphi_{x_2}^{-1}(x_1^{-1})\circledast\varphi_{x_2^{-1}}(x_1),x_2^{-1}\circledcirc x_2)\\&=(\varphi_{x_2}^{-1}(x_1^{-1}),x_2^{-1})\boxtimes_\varphi(x_1,x_2)\,.\end{aligned}$$

Άρα το ζεύγος $(G_1\times G_2,\boxtimes_\varphi)$ αποτελεί όντως ομάδα έχουσα το (e_{G_1},e_{G_2}) ως ουδέτερο στοιχείο της και το $(\varphi_{x_2}^{-1}(x_1^{-1}),x_2^{-1})$ ως το αντίστροφο στοιχείο οιουδήποτε $(x_1,x_2)\in G_1\times G_2$. □

7.6.2 Ορισμός. Λέμε ότι η ομάδα $(G_1\times G_2,\boxtimes_\varphi)$ είναι το **εξωτερικό ημιευθύ γινόμενο των** $(G_1,\circledast)$ **και** $(G_2,\circledcirc)$ **το καθοριζόμενο μέσω τού** φ. Για το υποκείμενο σύνολο αυτής θα χρησιμοποιούμε εφεξής τον (πλέον καθιερωμένο) συμβολισμό

$$\boxed{G_1\rtimes_\varphi G_2}$$

(μέσω τού οποίου διασφαλίζεται τόσον η διάκρισή της από το *σύνηθες* εξωτερικό ευθύ γινόμενο[87] των G_1 και G_2 όσον και η απαραίτητη αναγραφή τού φ).

7.6.3 Πρόταση. *Για την $G_1\rtimes_\varphi G_2$ ισχύουν τα ακόλουθα*:
(i) $G_1\cong\overline{G}_1:=G_1\rtimes_\varphi\{e_{G_2}\}\trianglelefteq G_1\rtimes_\varphi G_2$.
(ii) *Η (δεύτερη φυσική) προβολή*

$$\mathrm{pr}_2:G_1\rtimes_\varphi G_2\longrightarrow G_2,\ (x_1,x_2)\longmapsto x_2,$$

είναι ένας επιμορφισμός έχων ως πυρήνα του την $\overline{G}_1$, οπότε $(G_1\rtimes_\varphi G_2)/\overline{G}_1\cong G_2$.
(iii) $G_2\cong\overline{G}_2:=\{e_{G_1}\}\rtimes_\varphi G_2\sqsubseteq G_1\rtimes_\varphi G_2$.
(iv) $G_1\rtimes_\varphi G_2=\overline{G}_1\boxtimes_\varphi\overline{G}_2$.
(v) $\overline{G}_1\cap\overline{G}_2=\{(e_{G_1},e_{G_2})\}$.

ΑΠΟΔΕΙΞΗ. (i) Η απεικόνιση $G_1\ni x_1\mapsto(x_1,e_{G_2})\in\overline{G}_1$ είναι ένας ισομορφισμός ομάδων. Επιπλέον, $(e_{G_1},e_{G_2})\in\overline{G}_1$ και για οιαδήποτε στοιχεία $(x_1,e_{G_2}),(x_1',e_{G_2})\in\overline{G}_1$ και $(y_1,y_2)\in G_1\rtimes_\varphi G_2$ έχουμε αφ' ενός μεν

$$\begin{aligned}&(x_1,e_{G_2})\boxtimes_\varphi(x_1',e_{G_2})^{-1}=(x_1,e_{G_2})\boxtimes_\varphi(\varphi_{e_{G_2}}^{-1}((x_1')^{-1}),e_{G_2}^{-1})\\&=(x_1\circledast\varphi_{e_{G_2}}(\varphi_{e_{G_2}}^{-1}((x_1')^{-1})),e_{G_2}\circledcirc e_{G_2}^{-1})\\&=(x_1\circledast(x_1')^{-1},e_{G_2})\in\overline{G}_1\underset{\text{2.1.16 (iii)}}{\Longrightarrow}\overline{G}_1\sqsubseteq G_1\rtimes_\varphi G_2,\end{aligned}$$

αφ' ετέρου δε

$$\begin{aligned}&(y_1,y_2)\boxtimes_\varphi(x_1,e_{G_2})\boxtimes_\varphi(y_1,y_2)^{-1}=(y_1,y_2)\boxtimes_\varphi(x_1,e_{G_2})\boxtimes_\varphi(\varphi_{y_2}^{-1}(y_1^{-1}),y_2^{-1})\\&=\big(y_1\circledast\varphi_{y_2}(x_1),y_2\circledcirc e_{G_2}\big)\boxtimes_\varphi(\varphi_{y_2}^{-1}(y_1^{-1}),y_2^{-1})\\&=\big(y_1\circledast\varphi_{y_2}(x_1),y_2\big)\boxtimes_\varphi(\varphi_{y_2}^{-1}(y_1^{-1}),y_2^{-1})\\&=(y_1\circledast\varphi_{y_2}(x_1)\circledast\varphi_{y_2}(\varphi_{y_2}^{-1}(y_1^{-1})),y_2\circledcirc y_2^{-1})\\&=(y_1\circledast\varphi_{y_2}(x_1\circledast\varphi_{y_2}^{-1}(y_1^{-1})),e_{G_2})\in\overline{G}_1\Rightarrow\overline{G}_1\trianglelefteq G_1\rtimes_\varphi G_2.\end{aligned}$$

[87] Σημειωτέον ότι, εν αντιθέσει προς ό,τι συμβαίνει με το εξωτερικό *ευθύ* γινόμενο, ο ορισμός τού εξωτερικού *ημιευθέος* γινομένου *εξαρτάται* από το ποιον εκ δύο «παραγόντων» αναφέρουμε ως πρώτο και ποιον ως δεύτερο.

(ii) Αρκεί να εφαρμοσθεί το θεώρημα 4.5.2 λαμβάνοντας υπ' όψιν ότι

$$\mathrm{Ker}(\mathrm{pr}_2) = \{\,(x_1, x_2) \in G_1 \rtimes_\varphi G_2 |\, x_2 = e_{G_2}\} = \overline{G}_1.$$

(iii) Η απεικόνιση $G_2 \ni x_2 \mapsto (e_{G_1}, x_2) \in \overline{G}_2$ είναι ένας ισομορφισμός ομάδων. Προφανώς, $(e_{G_1}, e_{G_2}) \in \overline{G}_2$. Επίσης, για οιαδήποτε $(e_{G_1}, x_2), (e_{G_1}, x_2') \in \overline{G}_2$ λαμβάνουμε

$$\begin{aligned}
&(e_{G_1}, x_2) \boxtimes_\varphi (e_{G_1}, x_2')^{-1} = (e_{G_1}, x_2) \boxtimes_\varphi (\varphi_{x_2}^{-1}(e_{G_1}^{-1}), (x_2')^{-1}) \\
&= (e_{G_1}, x_2) \boxtimes_\varphi (\varphi_{x_2}^{-1}(e_{G_1}), (x_2')^{-1}) = (e_{G_1}, x_2) \boxtimes_\varphi (e_{G_1}, (x_2')^{-1}) \\
&= (e_{G_1} \circledast \varphi_{x_2}(e_{G_1}), x_2 \circledcirc (x_2')^{-1}) = (\varphi_{x_2}(e_{G_1}), x_2 \circledcirc (x_2')^{-1}) \\
&= (e_{G_1}, x_2 \circledcirc (x_2')^{-1}) \in \overline{G}_2 \underset{2.1.16\,(\mathrm{iii})}{\Longrightarrow} \overline{G}_2 \sqsubseteq G_1 \rtimes_\varphi G_2.
\end{aligned}$$

(iv) Προφανώς, $\overline{G}_1 \boxtimes_\varphi \overline{G}_2 \subseteq G_1 \rtimes_\varphi G_2$. Από την άλλη μεριά, για οιοδήποτε στοιχείο $(x_1, x_2) \in G_1 \rtimes_\varphi G_2$ έχουμε

$$\begin{aligned}
&(x_1, x_2) = (x_1 \circledast e_{G_1}, e_{G_2} \circledcirc x_2) = (x_1 \circledast \varphi_{e_{G_2}}(e_{G_1}), e_{G_2} \circledcirc x_2) \\
&= (x_1, e_{G_2}) \boxtimes_\varphi (e_{G_1}, x_2) \in \overline{G}_1 \boxtimes_\varphi \overline{G}_2 \Rightarrow G_1 \rtimes_\varphi G_2 \subseteq \overline{G}_1 \boxtimes_\varphi \overline{G}_2.
\end{aligned}$$

(v) Τούτο είναι προφανές. □

7.6.4 Πρόταση. *Οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Η ταυτοτική απεικόνιση από το εξωτερικό ημιευθύ γινόμενο $G_1 \rtimes_\varphi G_2$ επί τού εξωτερικού ευθέος γινομένου $G_1 \times G_2$ είναι ομομορφισμός ομάδων.*

(ii) *Ο $\varphi : G_2 \longrightarrow \mathrm{Aut}(G_1),\ x \longmapsto \varphi_x$, είναι ο τετριμμένος ομομορφισμός, ήτοι ισχύει $\varphi_x = e_{\mathrm{Aut}(G_1)} = \mathrm{id}_{G_1}$ για κάθε $x \in G_2$.*

(iii) *Το εξωτερικό ημιευθύ γινόμενο $G_1 \rtimes_\varphi G_2$ συμπίπτει με το εξωτερικό ευθύ γινόμενο $G_1 \times G_2$.*

(iv) $\overline{G}_2 \trianglelefteq G_1 \rtimes_\varphi G_2$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Για οιαδήποτε στοιχεία $(x_1, x_2), (y_1, y_2) \in G_1 \rtimes_\varphi G_2$ έχουμε (εξ υποθέσεως) $(x_1, x_2) \boxtimes_\varphi (y_1, y_2) := \big(x_1 \circledast \varphi_{x_2}(y_1), x_2 \circledcirc y_2\big) = (x_1 \circledast y_1, x_2 \circledcirc y_2)$, οπότε $x_1 \circledast \varphi_{x_2}(y_1) = x_1 \circledast y_1 \Rightarrow \varphi_{x_2}(y_1) = y_1$ και, κατ' επέκταση, $\varphi_{x_2} = \mathrm{id}_{G_1}$.

(ii)⇒(i) Και αντιστρόφως, για οιαδήποτε $(x_1, x_2), (y_1, y_2) \in G_1 \rtimes_\varphi G_2$,

$$\big(x_1 \circledast \varphi_{x_2}(y_1), x_2 \circledcirc y_2\big) = (x_1 \circledast y_1, x_2 \circledcirc y_2).$$

(ii)⇒(iii) Για οιαδήποτε στοιχεία $(x_1, x_2), (y_1, y_2) \in G_1 \rtimes_\varphi G_2$ έχουμε

$$\begin{aligned}
&(x_1, x_2) \boxtimes_\varphi (y_1, y_2) := \big(x_1 \circledast \varphi_{x_2}(y_1), x_2 \circledcirc y_2\big) \\
&= (x_1 \circledast \mathrm{id}_{G_1}(y_1), x_2 \circledcirc y_2) = (x_1 \circledast y_1, x_2 \circledcirc y_2) \\
&= (x_1, x_2) \boxdot (y_1, y_2)
\end{aligned}$$

(βλ. 7.1.1), οπότε $G_1 \rtimes_\varphi G_2 = G_1 \times G_2$.

(iii)⇒(iv) Επειδή $G_1 \rtimes_\varphi G_2 = G_1 \times G_2$, τούτο έπεται από το 7.1.4 (ii).

(iv)⇒(ii) Επειδή $\overline{G}_2 \trianglelefteq G_1 \rtimes_\varphi G_2$, για οιαδήποτε $x \in G_2$ και $(y_1, y_2) \in G_1 \rtimes_\varphi G_2$ ισχύει

$$\begin{aligned}
&(y_1, y_2) \boxtimes_\varphi (e_{G_1}, x) \boxtimes_\varphi (y_1, y_2)^{-1} = (y_1 \circledast \varphi_{y_2}(e_{G_1}), y_2 \circledcirc x) \boxtimes_\varphi (y_1, y_2)^{-1} \\
&= (y_1 \circledast e_{G_1}, y_2 \circledcirc x) \boxtimes_\varphi (\varphi_{y_2}^{-1}(y_1^{-1}), y_2^{-1}) = (y_1, y_2 \circledcirc x) \boxtimes_\varphi (\varphi_{y_2}^{-1}(y_1^{-1}), y_2^{-1}) \\
&= (y_1 \circledast \varphi_{y_2 \circledcirc x}(\varphi_{y_2}^{-1}(y_1^{-1})), y_2 \circledcirc x \circledcirc y_2^{-1}) = (y_1 \circledast \varphi_{y_2 \circledcirc x}(\varphi_{y_2^{-1}}(y_1^{-1})), y_2 \circledcirc x \circledcirc y_2^{-1}) \\
&= (y_1 \circledast (\varphi_{y_2 \circledcirc x \circledcirc y_2^{-1}}(y_1))^{-1}, y_2 \circledcirc x \circledcirc y_2^{-1}) \in \overline{G}_2,
\end{aligned}$$

οπότε $y_1 \circledast (\varphi_{y_2 \circledcirc x \circledcirc y_2^{-1}}(y_1))^{-1} = e_{G_1} \Rightarrow \varphi_{y_2 \circledcirc x \circledcirc y_2^{-1}}(y_1) = y_1$ και, κατ' επέκταση,

$$\begin{aligned}
&\mathrm{id}_{G_1} = \varphi_{y_2 \circledcirc x \circledcirc y_2^{-1}} = \varphi_{y_2} \circ \varphi_x \circ \varphi_{y_2^{-1}} = \varphi_{y_2} \circ \varphi_x \circ \varphi_{y_2}^{-1} \\
&\Rightarrow \varphi_{y_2} \circ \varphi_x = \varphi_{y_2} \Rightarrow \varphi_x = \mathrm{id}_{G_1}.
\end{aligned}$$

Άρα ο $\varphi : G_2 \longrightarrow \mathrm{Aut}(G_1)$ είναι όντως ο τετριμμένος ομομορφισμός. □

7.6.5 Πόρισμα. *Οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Η ομάδα $G_1 \rtimes_\varphi G_2$ είναι αβελιανή.*

(ii) *Αμφότερες οι G_1 και G_2 είναι αβελιανές ομάδες και το εξωτερικό ημιευθύ γινόμενο $G_1 \rtimes_\varphi G_2$ συμπίπτει με το εξωτερικό ευθύ γινόμενο $G_1 \times G_2$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν η $G_1 \rtimes_\varphi G_2$ είναι αβελιανή, τότε $\overline{G}_2 \trianglelefteq G_1 \rtimes_\varphi G_2$. (Βλ. πρόταση 4.2.6.) Από την πρόταση 7.6.4 συνάγεται ότι $G_1 \rtimes_\varphi G_2 = G_1 \times G_2$ και από το (ii) τής προτάσεως 7.1.57 ότι αμφότερες οι G_1 και G_2 είναι αβελιανές.

(ii)⇒(i) Εάν αμφότερες οι G_1 και G_2 είναι αβελιανές και $G_1 \rtimes_\varphi G_2 = G_1 \times G_2$, τότε και η $G_1 \times G_2$ είναι αβελιανή δυνάμει τού (ii) τής προτάσεως 7.1.57. □

► **Κριτήρια υπάρξεως ισομορφισμού μεταξύ εξωτερικών ημιευθέων γινομένων**. Εάν $\varphi, \psi \in \mathrm{Hom}(G_2, \mathrm{Aut}(G_1))$, τότε τα εξωτερικά ημιευθέα γινόμενα $G_1 \rtimes_\varphi G_2$ και $G_1 \rtimes_\psi G_2$ έχουν ίσες τάξεις αλλά δεν είναι κατ' ανάγκην ισόμορφα. Κάποιες *ικανές* συνθήκες για να είναι ισόμορφα δίδονται στις προτάσεις 7.6.6, 7.6.7 και 7.6.9. Επίσης, μια *αναγκαία* συνθήκη (υπό ειδικές προϋποθέσεις) δίδεται στην πρόταση 7.6.12.

7.6.6 Πρόταση. *Για κάθε $\varphi \in \mathrm{Hom}(G_2, \mathrm{Aut}(G_1))$ και κάθε $\vartheta \in \mathrm{Aut}(G_2)$ υφίσταται (κανονιστικός) ισομορφισμός*

$$\boxed{G_1 \rtimes_\varphi G_2 \xrightarrow{\cong} G_1 \rtimes_{\varphi \circ \vartheta} G_2.}$$

ΑΠΟΔΕΙΞΗ. Το εξωτερικό ημιευθύ γινόμενο $G_1 \rtimes_{\varphi\circ\vartheta} G_2$ ορίζεται, καθώς είναι πρόδηλο ότι η σύνθεση $\varphi \circ \vartheta : G_2 \longrightarrow \mathrm{Aut}(G_1)$ αποτελεί ομομορφισμό ομάδων. Η απεικόνιση $f : G_1 \rtimes_\varphi G_2 \to G_1 \rtimes_{\varphi\circ\vartheta} G_2,\ (x_1, x_2) \mapsto f((x_1, x_2)) := (x_1, \vartheta^{-1}(x_2))$ είναι τόσον ενριπτική (διότι η ϑ^{-1} είναι ενριπτική) όσον και επιριπτική (διότι για κάθε $(z_1, z_2) \in G_1 \rtimes_{\varphi\circ\vartheta} G_2$ ισχύει η ισότητα $f((z_1, \vartheta(z_2))) = (z_1, z_2)$). Επιπροσθέτως, η f είναι *και* ομομορφισμός ομάδων, καθόσον για οιαδήποτε στοιχεία

$(x_1, x_2), (y_1, y_2) \in G_1 \rtimes_\varphi G_2$ έχουμε

$$\begin{aligned}
&f((x_1, x_2) \boxtimes_\varphi (y_1, y_2)) = f(x_1 \circledast \varphi_{x_2}(y_1), x_2 \circledcirc y_2) \\
&= (x_1 \circledast \varphi_{x_2}(y_1), \vartheta^{-1}(x_2 \circledcirc y_2)) = (x_1 \circledast \varphi_{x_2}(y_1), \vartheta^{-1}(x_2) \circledcirc \vartheta^{-1}(y_2)) \\
&= (x_1 \circledast (\varphi \circ \vartheta)_{\vartheta^{-1}(x_2)}(y_1), \vartheta^{-1}(x_2) \circledcirc \vartheta^{-1}(y_2)) \\
&= \left(x_1, \vartheta^{-1}(x_2)\right) \boxtimes_{\varphi\circ\vartheta} \left(y_1, \vartheta^{-1}(y_2)\right) = f((x_1, x_2)) \boxtimes_{\varphi\circ\vartheta} f((y_1, y_2)),
\end{aligned}$$

διότι $(\varphi \circ \vartheta)_{\vartheta^{-1}(x_2)} = \varphi_{\vartheta(\vartheta^{-1}(x_2))} = \varphi_{x_2},\ \forall x_2 \in G_2$. Άρα η f είναι *ισομορφισμός* ομάδων. □

7.6.7 Πρόταση. *Εάν* $\varphi, \psi \in \mathrm{Hom}(G_2, \mathrm{Aut}(G_1))$ *και εάν*

$$\exists \vartheta \in \mathrm{Aut}(G_1) \text{ και } \exists \omega \in \mathrm{Aut}(G_2) : \psi_{\omega(x)} = \vartheta \circ \varphi_x \circ \vartheta^{-1},\ \forall x \in G_2,$$

δηλαδή εάν το διάγραμμα

$$\begin{array}{ccc}
G_2 & \xrightarrow{\ \varphi\ } & \mathrm{Aut}(G_1) \\
{\scriptstyle\omega}\downarrow & \circlearrowleft & \downarrow{\scriptstyle \text{συζυγία } \vartheta\circ-\circ\vartheta^{-1}} \\
G_2 & \xrightarrow[\ \psi\ ]{} & \mathrm{Aut}(G_1)
\end{array}$$

είναι μεταθετικό, τότε υφίσταται (κανονιστικός) ισομορφισμός

$$\boxed{G_1 \rtimes_\varphi G_2 \xrightarrow{\cong} G_1 \rtimes_\psi G_2.}$$

ΑΠΟΔΕΙΞΗ. Η απεικόνιση

$$f : G_1 \rtimes_\varphi G_2 \longrightarrow G_1 \rtimes_\psi G_2,\ (x_1, x_2) \longmapsto f\left((x_1, x_2)\right) := (\vartheta(x_1), \omega(x_2))$$

είναι ομομορφισμός ομάδων, καθόσον για οιαδήποτε $(x_1, x_2), (y_1, y_2) \in G_1 \rtimes_\varphi G_2$ έχουμε

$$\begin{aligned}
&f((x_1, x_2) \boxtimes_\varphi (y_1, y_2)) = f(x_1 \circledast \varphi_{x_2}(y_1), x_2 \circledcirc y_2) \\
&= (\vartheta(x_1 \circledast \varphi_{x_2}(y_1)), \omega(x_2 \circledcirc y_2)) = (\vartheta(x_1) \circledast \vartheta(\varphi_{x_2}(y_1)), \omega(x_2 \circledcirc y_2)) \\
&= (\vartheta(x_1) \circledast (\vartheta \circ \varphi_{x_2} \circ \vartheta^{-1})(\vartheta(y_1)), \omega(x_2 \circledcirc y_2)) \\
&= (\vartheta(x_1) \circledast \psi_{\omega(x_2)}(\vartheta(y_1)), \omega(x_2) \circledcirc \omega(y_2)) \\
&= (\vartheta(x_1), \omega(x_2)) \boxtimes_\psi (\vartheta(y_1), \omega(y_2)) = f((x_1, x_2)) \boxtimes_\psi f((y_1, y_2)).
\end{aligned}$$

Παρομοίως αποδεικνύεται ότι *και* η απεικόνιση

$$f' : G_1 \rtimes_\psi G_2 \longrightarrow G_1 \rtimes_\varphi G_2,\ (x_1, x_2) \longmapsto f'\left((x_1, x_2)\right) := \left(\vartheta^{-1}(x_1), \omega^{-1}(x_2)\right)$$

είναι ομομορφισμός ομάδων. Επειδή $f \circ f' = \mathrm{id}_{G_1 \rtimes_\psi G_2}$ και $f' \circ f = \mathrm{id}_{G_1 \rtimes_\varphi G_2}$, η f είναι ισομορφισμός και $f' = f^{-1}$. □

7.6.8 Λήμμα. *Εάν $a \in \mathbb{Z}$ και $m, n \in \mathbb{N}$, $n \geq 2$, είναι τέτοιοι, ώστε να ισχύει $m \mid n$ και $\mu\kappa\delta(a, m) = 1$, τότε $\exists a' \in \mathbb{Z} : [a]_m = [a']_m$ και $\mu\kappa\delta(a', n) = 1$. Κατά συνέπειαν, η απεικόνιση $\mathbb{Z}_n^\times \ni [k]_n \longmapsto [k]_m \in \mathbb{Z}_m^\times$ $(k \in \mathbb{Z})$ είναι επιρριπτική.*

ΑΠΟΔΕΙΞΗ. Εξ υποθέσεως, $\exists q \in \mathbb{N} : n = mq$. Εάν θέσουμε $d := \mu\kappa\delta(a, n)$, τότε

$$\mu\kappa\delta(m, d) = \mu\kappa\delta(m, \mu\kappa\delta(a, n)) \underset{\text{B.2.16}}{=} \mu\kappa\delta(m, a, n) = \mu\kappa\delta(a, m) = 1$$

(διότι $m \mid n$), απ' όπου έπεται ότι

$$\left.\begin{array}{l} n = mq,\ d \mid n \\ \mu\kappa\delta(m, d) = 1 \end{array}\right\} \underset{\text{B.2.9}}{\Longrightarrow} d \mid q \Rightarrow \exists q' \in \mathbb{N} : q = q'd.$$

Έστω t το γινόμενο όλων των πρώτων διαιρετών τού q' που δεν διαιρούν το d όταν $q' \geq 2$ και $t := 1$ όταν $q' = 1$. Θέτουμε $a' := a + tm$, παρατηρούμε ότι $[a]_m = [a']_m$, θεωρούμε τυχόντα πρώτο διαιρέτη p τού n και εξετάζουμε 4 περιπτώσεις χωριστά.

Περίπτωση πρώτη. Εάν $p \mid m$, τότε $\mu\kappa\delta(a, m) = 1 \Rightarrow p \nmid a \Rightarrow p \nmid a'$.

Περίπτωση δεύτερη. Εάν $p \nmid m$, $p \mid q'$ και $p \mid d$, τότε $p \nmid t$ (εξ ορισμού τού t), οπότε

$$[p \mid d \ \text{ και } \ d \mid a] \Rightarrow p \mid a \ \text{ και } \ [p \mid a \ \text{ και } \ p \nmid tm] \Rightarrow p \nmid a'.$$

Περίπτωση τρίτη. Εάν $p \nmid m$, $p \mid q'$ και $p \nmid d$, τότε $[p \mid t \ \text{ και } \ p \nmid a] \Rightarrow p \nmid a'$.

Περίπτωση τέταρτη. Εάν $p \nmid m$ και $p \nmid q'$, τότε $p \mid d$ (διότι $n = mq'd$), οπότε έχουμε $[p \mid a \ \text{ και } \ p \nmid t] \Rightarrow p \nmid a'$. Επειδή κανένας εκ των πρώτων διαιρετών τού n δεν διαιρεί το a', έχουμε $\mu\kappa\delta(a', n) = 1$ και, κατ' επέκταση, $[a']_n \in \mathbb{Z}_n^\times$. □

7.6.9 Πρόταση. *Εάν η G_1 είναι τυχούσα ομάδα, η G_2 κυκλική ομάδα και*

$$\varphi : G_2 \longrightarrow \mathrm{Aut}(G_1),\ \psi : G_2 \longrightarrow \mathrm{Aut}(G_1)$$

δυο ομομορφισμοί, οι εικόνες των οποίων είναι συζυγείς υποομάδες εντός τής $\mathrm{Aut}(G_1)$, τότε υφίσταται (κανονιστικός) ισομορφισμός

$$\boxed{G_1 \rtimes_\varphi G_2 \overset{\cong}{\longrightarrow} G_1 \rtimes_\psi G_2}$$

στις ακόλουθες δύο περιπτώσεις:

(i) *Όταν η G_2 είναι πεπερασμένη.*

(ii) *Όταν η G_2 είναι άπειρη και οι φ, ψ είναι μονομορφισμοί.*

ΑΠΟΔΕΙΞΗ. Εάν η G_2 είναι τετριμμένη, τότε ο ισχυρισμός είναι προδήλως αληθής. Έστω ότι $|G_2| \geq 2$ και ότι z είναι ένας γεννήτορας τής ομάδας G_2. Προφανώς,

$$G_2 = \langle z \rangle \underset{\text{2.4.9 (i)}}{\Longrightarrow} [\mathrm{Im}(\varphi) = \varphi(\langle z \rangle) = \langle \varphi_z \rangle \ \text{ και } \ \mathrm{Im}(\psi) = \psi(\langle z \rangle) = \langle \psi_z \rangle].$$

Επειδή

$$(\mathrm{Im}(\varphi), \mathrm{Im}(\psi)) \in \left.\mathcal{R}_{\text{συζ.}}^{\mathrm{Aut}(G_1)}\right|_{\mathbf{Subg}(\mathrm{Aut}(G_1))^2} \Rightarrow [\exists \vartheta \in \mathrm{Aut}(G_1) : \vartheta \circ \mathrm{Im}(\varphi) \circ \vartheta^{-1} = \mathrm{Im}(\psi)],$$

έχουμε $\vartheta \circ \varphi_z \circ \vartheta^{-1} = \psi_{z'}$ για κάποιο $z' \in G_2\,(= \langle z \rangle)$, οπότε $\exists a \in \mathbb{Z} : z' = z^a$. Έστω τώρα τυχόν $x \in G_2$. Αυτό γράφεται υπό τη μορφή $x = z^c$ για κάποιον $c \in \mathbb{Z}$. Τούτο σημαίνει ότι

$$\begin{aligned} \vartheta \circ \varphi_x \circ \vartheta^{-1} &= \vartheta \circ \varphi_{z^c} \circ \vartheta^{-1} = (\vartheta \circ \varphi_z \circ \vartheta^{-1})^c \\ &= \psi^c_{z'} = \psi^c_{z^a} = \psi^{ca}_z = (\psi^c_z)^a = \psi^a_{z^c} = \psi^a_x. \end{aligned} \tag{7.68}$$

(i) Όταν η G_2 είναι *πεπερασμένη*, τότε είναι ισόμορφη με την $(\mathbb{Z}_n, +)$ για κάποιον $n \in \mathbb{N}$, $n \geq 2$. Εξάλλου,

$$G_2/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi) \Longrightarrow n = |\mathrm{Ker}(\varphi)|\,|\mathrm{Im}(\varphi)|\,.$$

(Βλ. 4.5.2, 4.4.2 (iii) και 2.4.19 (i).) Θέτοντας $m := |\mathrm{Im}(\varphi)|$ λαμβάνουμε

$$\mathrm{Im}(\varphi) = \langle \varphi_z \rangle = \left\{ \varphi_z^j \middle|\, j \in \{0, 1, ..., m-1\} \right\} = \{\, \varphi_{z^j} \,|\, j \in \{0, 1, ..., m-1\} \}\,.$$

Λόγω τού ισομορφισμού

$$\mathrm{Im}(\varphi) \xrightarrow{\cong} \mathrm{Im}(\psi),\ \varphi_{z^j} \longmapsto \vartheta \circ \varphi_{z^j} \circ \vartheta^{-1} = \psi^a_{z^j} = (\psi^a_z)^j,\ \forall j \in \{0, 1, ..., m-1\},$$

η $\mathrm{Im}(\psi) = \langle \psi_z \rangle$ έχει τον αυτομορφισμό ψ^a_z τής G_1 ως (άλλον) έναν γεννήτορά της. Δυνάμει τού πορίσματος 2.3.17 έχουμε μκδ$(a, m) = 1$. Κατά το προηγηθέν λήμμα 7.6.8, $\exists a' \in \mathbb{Z} : [a]_m = [a']_m$ και μκδ$(a', n) = 1$. Κατά συνέπειαν, $[a']_n \in \mathbb{Z}_n^\times$. Έστω $[b]_n$ το (πολλαπλασιαστικό) αντίστροφο τού $[a']_n$ εντός τής $\mathbb{Z}_n^\times$ (για κατάλληλον $b \in \mathbb{Z}$). Η απεικόνιση $\omega : G_2 \longrightarrow G_2,\ x \longmapsto \omega(x) := x^{a'}$, είναι ένας αυτομορφισμός τής G_2, καθόσον είναι εμφανώς ενδομορφισμός τής G_2 και η σύνθεσή της (τόσον εκ δεξιών όσον και εξ αριστερών) με τον ενδομορφισμό $G_2 \longrightarrow G_2,\ x \longmapsto x^b$, ισούται με id_{G_2}. Επιπροσθέτως,

$$m \mid a' - a \Rightarrow [\psi_x^{a'-a} = \mathrm{id}_{G_1} \Rightarrow \psi^a_x = \psi^{a'}_x = \psi_{x^{a'}} = \psi_{\omega(x)}, \forall x \in G_2]. \tag{7.69}$$

Από τις (7.68) και (7.69) συνάγεται ότι $\psi_{\omega(x)} = \vartheta \circ \varphi_x \circ \vartheta^{-1},\ \forall x \in G_2$. Επομένως, σύμφωνα με την πρόταση 7.6.7, η απεικόνιση

$$f : G_1 \rtimes_\varphi G_2 \longrightarrow G_1 \rtimes_\psi G_2,\ (x_1, x_2) \longmapsto f\,((x_1, x_2)) := (\vartheta(x_1), \omega(x_2))$$

αποτελεί έναν (κανονιστικό) ισομορφισμό ομάδων.

(ii) Όταν η G_2 είναι *άπειρη* και *οι* φ, ψ *μονομορφισμοί*, η G_2 είναι ισόμορφη με την $(\mathbb{Z}, +)$ και έχουμε (για κάθε $x \in G_2$) $\vartheta \circ \varphi_x \circ \vartheta^{-1} = \psi^a_x$ και (κατ' αναλογίαν) $\vartheta^{-1} \circ \psi_x \circ \vartheta = \varphi^b_x$ (για κάποιον $b \in \mathbb{Z}$). Εξ αυτών των ισοτήτων έπεται ότι

$$\psi_{x^{ab}} = \psi^{ab}_x = (\psi^a_x)^b = (\vartheta \circ \varphi_x \circ \vartheta^{-1})^b = \vartheta \circ \varphi^b_x \circ \vartheta^{-1} = \psi_x$$

και η ενριπτικότητα τού ψ δίδει $x^{ab} = x \Rightarrow x^{ab-1} = e_{G_2} \Rightarrow ab = 1 \Rightarrow a = b \in \{\pm 1\}$ (διότι αλλιώς η G_2 δεν θα ήταν άπειρη, βλ. 2.2.18). Η απεικόνιση

$$f : G_1 \rtimes_\varphi G_2 \longrightarrow G_1 \rtimes_\psi G_2,\ (x_1, x_2) \longmapsto f\,((x_1, x_2)) := (\vartheta(x_1), x_2^a)$$

είναι ομομορφισμός ομάδων, καθόσον για οιαδήποτε $(x_1, x_2), (y_1, y_2) \in G_1 \rtimes_\varphi G_2$ έχουμε

$$\begin{aligned}
&f((x_1, x_2) \boxtimes_\varphi (y_1, y_2)) = f(x_1 \circledast \varphi_{x_2}(y_1), x_2 \circledcirc y_2) \\
&= (\vartheta(x_1 \circledast \varphi_{x_2}(y_1)), (x_2 \circledcirc y_2)^a) = (\vartheta(x_1) \circledast \vartheta(\varphi_{x_2}(y_1)), (x_2 \circledcirc y_2)^a) \\
&= (\vartheta(x_1) \circledast (\vartheta \circ \varphi_{x_2} \circ \vartheta^{-1})(\vartheta(y_1)), x_2^a \circledcirc y_2^a) = (\vartheta(x_1) \circledast \psi^a_{x_2}(\vartheta(y_1)), x_2^a \circledcirc y_2^a) \\
&= (\vartheta(x_1), x_2^a) \boxtimes_\psi (\vartheta(y_1), y_2^a) = f((x_1, x_2)) \boxtimes_\psi f((y_1, y_2)).
\end{aligned}$$

Παρομοίως αποδεικνύεται ότι *και* η απεικόνιση

$$f' : G_1 \rtimes_\psi G_2 \longrightarrow G_1 \rtimes_\varphi G_2,\ (x_1, x_2) \longmapsto f'((x_1, x_2)) := \left(\vartheta^{-1}(x_1), x_2^a\right)$$

είναι ομομορφισμός ομάδων. Επειδή $f \circ f' = \mathrm{id}_{G_1 \rtimes_\psi G_2}$ και $f' \circ f = \mathrm{id}_{G_1 \rtimes_\varphi G_2}$, ο f είναι ισομορφισμός και $f' = f^{-1}$. □

7.6.10 Λήμμα. *Για τυχούσες ομάδες G_1, G_2 και τυχόντα $\varphi \in \mathrm{Hom}(G_2, \mathrm{Aut}(G_1))$ ισχύουν τα εξής*:
(i) $\mathrm{C}_{G_1 \rtimes_\varphi G_2}(\overline{G}_1) \cap \overline{G}_2 = \{e_{G_1}\} \rtimes_\varphi \mathrm{Ker}(\varphi)$.
(ii) $\mathrm{C}_{G_1 \rtimes_\varphi G_2}(\overline{G}_2) \cap \overline{G}_1 = \mathrm{N}_{G_1 \rtimes_\varphi G_2}(\overline{G}_2) \cap \overline{G}_1$.

ΑΠΟΔΕΙΞΗ. (i) Προφανώς, $(e_{G_1}, x_2) \in \mathrm{C}_{G_1 \rtimes_\varphi G_2}(\overline{G}_1) \cap \overline{G}_2$ εάν και μόνον εάν

$$(x_1, e_{G_2}) = (e_{G_1}, x_2) \boxtimes_\varphi (x_1, e_{G_2}) \boxtimes_\varphi (e_{G_1}, x_2)^{-1} = (\varphi_{x_2}(x_1), e_{G_2})$$

για κάθε $x_1 \in G_1$, δηλαδή εάν και μόνον εάν $\varphi_{x_2} = \mathrm{id}_{G_1}$ ($\Leftrightarrow x_2 \in \mathrm{Ker}(\varphi)$).
(ii) Εάν $(x_1, e_{G_2}) \in \mathrm{N}_{G_1 \rtimes_\varphi G_2}(\overline{G}_2) \cap \overline{G}_1$ και $x_2 \in G_2$, τότε

$$\exists x_2' \in G_2 : (x_1, e_{G_2}) \boxtimes_\varphi (e_{G_1}, x_2) \boxtimes_\varphi (x_1, e_{G_2})^{-1} = (e_{G_1}, x_2'). \tag{7.70}$$

Επειδή $(x_1, e_{G_2}) \boxtimes_\varphi (e_{G_1}, x_2) \boxtimes_\varphi (x_1, e_{G_2})^{-1} = (x_1 \circledast \varphi_{x_2}(x_1^{-1}), x_2)$, η ισότητα (7.70) δίδει $\varphi_{x_2} = \mathrm{id}_{G_1}$ και $x_2 = x_2'$. Επομένως,

$$\mathrm{N}_{G_1 \rtimes_\varphi G_2}(\overline{G}_2) \cap \overline{G}_1 \subseteq \mathrm{C}_{G_1 \rtimes_\varphi G_2}(\overline{G}_2) \cap \overline{G}_1.$$

Ο αντίστροφος εγκλεισμός "$\supseteq$" είναι προφανής. □

7.6.11 Λήμμα. *Εάν η G_1 είναι αβελιανή και η G_2 τυχούσα, τότε για οιονδήποτε ομομορφισμό $\varphi : G_2 \longrightarrow \mathrm{Aut}(G_1)$ ισχύει η ισότητα*

$$\mathrm{C}_{G_1 \rtimes_\varphi G_2}(\overline{G}_1) = \overline{G}_1 \boxtimes_\varphi (\{e_{G_1}\} \rtimes_\varphi \mathrm{Ker}(\varphi)).$$

ΑΠΟΔΕΙΞΗ. Κατά το (iv) τής προτάσεως 7.6.3,

$$G_1 \rtimes_\varphi G_2 = \overline{G}_1 \boxtimes_\varphi \overline{G}_2 = \bigcup_{x \in G_2} \overline{G}_1 \boxtimes_\varphi (e_{G_1}, x).$$

Επειδή η $G_1 \cong \overline{G}_1$ είναι αβελιανή, έχουμε $\overline{G}_1 \sqsubseteq \mathrm{C}_{G_1 \rtimes_\varphi G_2}(\overline{G}_1)$. (Βλ. 5.2.2 (ii).) Αυτό σημαίνει ότι ο κεντροποιητής $\mathrm{C}_{G_1 \rtimes_\varphi G_2}(\overline{G}_1)$ τής $\overline{G}_1$ είναι η ένωση κάποιων

πλευρικών κλάσεων τής $\overline{G}_1$ εντός τής $G_1 \rtimes_\varphi G_2$. Η πλευρική κλάση $\overline{G}_1 \boxtimes_\varphi (e_{G_1}, x)$ ανήκει στον $\mathrm{C}_{G_1 \rtimes_\varphi G_2}(\overline{G}_1)$ εάν και μόνον εάν $(e_{G_1}, x) \in \mathrm{C}_{G_1 \rtimes_\varphi G_2}(\overline{G}_1)$. Επομένως,

$$\begin{aligned} \mathrm{C}_{G_1 \rtimes_\varphi G_2}(\overline{G}_1) &= \bigcup_{(e_{G_1}, x) \in \mathrm{C}_{G_1 \rtimes_\varphi G_2}(\overline{G}_1) \cap \overline{G}_2} \overline{G}_1 \boxtimes_\varphi (e_{G_1}, x) \\ &= \overline{G}_1 \boxtimes_\varphi (\mathrm{C}_{G_1 \rtimes_\varphi G_2}(\overline{G}_1) \cap \overline{G}_2). \end{aligned}$$

Αρκεί λοιπόν να εφαρμοσθεί το (i) τού λήμματος 7.6.10. □

7.6.12 Πρόταση. *Εάν οι ομάδες G_1, G_2 είναι πεπερασμένες, η G_1 αβελιανή και* $\mu\kappa\delta(|G_1|, |G_2|) = 1$, *τότε ισχύουν τα εξής*:

(i) *Για οιονδήποτε ομομορφισμό $\varphi \in \mathrm{Hom}(G_2, \mathrm{Aut}(G_1))$ δεν υπάρχει, πέραν τής ιδίας τής $\overline{G}_1 := G_1 \rtimes_\varphi \{e_{G_2}\}$, καμία άλλη υποομάδα τού εξωτερικού ημιευθέος γινομένου $G_1 \rtimes_\varphi G_2$ που να έχει τάξη ίση με $\left|\overline{G}_1\right|$.*

(ii) *Για οιουσδήποτε $\varphi, \psi \in \mathrm{Hom}(G_2, \mathrm{Aut}(G_1))$ ισχύει η συνεπαγωγή*

$$G_1 \rtimes_\varphi G_2 \cong G_1 \rtimes_\psi G_2 \Longrightarrow \mathrm{Ker}(\varphi) \cong \mathrm{Ker}(\psi).$$

ΑΠΟΔΕΙΞΗ. (i) Ας υποθέσουμε ότι $\exists H \in \mathbf{Subg}(G_1 \rtimes_\varphi G_2) \setminus \{\overline{G}_1\} : |H| = \left|\overline{G}_1\right|$. Θεωρούμε τυχόν στοιχείο $(x_1, x_2) \in H \setminus \overline{G}_1$ και τον φυσικό επιμορφισμό

$$\pi_{\overline{G}_1}^{G_1 \rtimes_\varphi G_2} : G_1 \rtimes_\varphi G_2 \longrightarrow (G_1 \rtimes_\varphi G_2)/\overline{G}_1 \cong \overline{G}_2.$$

Προφανώς, $\mathrm{ord}((x_1, x_2)) \geq 2$. Ως γνωστόν,

$$\mathrm{ord}((x_1, x_2)) \mid |G_1 \rtimes_\varphi G_2| = |G_1|\,|G_2| = \left|\overline{G}_1\right| \left|\overline{G}_2\right|.$$

(Βλ. πόρισμα 4.1.27.) Από την άλλη μεριά, $\mathrm{ord}(\pi_{\overline{G}_1}^{G_1 \rtimes_\varphi G_2}(x_1, x_2)) \geq 2$,

$$\mathrm{ord}(\pi_{\overline{G}_1}^{G_1 \rtimes_\varphi G_2}(x_1, x_2)) \mid \left|(G_1 \rtimes_\varphi G_2)/\overline{G}_1\right| = \left|\overline{G}_2\right|$$

και (λόγω τού (iv) τής προτάσεως 2.4.3) $\mathrm{ord}(\pi_{\overline{G}_1}^{G_1 \rtimes_\varphi G_2}(x_1, x_2)) \mid \mathrm{ord}((x_1, x_2))$. Έστω p ένας πρώτος διαιρέτης τής τάξεως $\mathrm{ord}(\pi_{\overline{G}_1}^{G_1 \rtimes_\varphi G_2}(x_1, x_2))$. Επειδή

$$\left.\begin{aligned} p \mid \mathrm{ord}((x_1, x_2)) \mid \left|\overline{G}_1\right| \left|\overline{G}_2\right| \\ \mu\kappa\delta(\left|\overline{G}_1\right|, \left|\overline{G}_2\right|) = \mu\kappa\delta(|G_1|, |G_2|) = 1 \\ p \mid \left|\overline{G}_2\right| \end{aligned}\right\} \Rightarrow p \nmid \left|\overline{G}_1\right| = |H|,$$

έχουμε $\mathrm{ord}((x_1, x_2)) \nmid \left|\overline{G}_1\right| = |H|$, πράγμα *αδύνατο*, διότι

$$(x_1, x_2) \in H \Rightarrow \mathrm{ord}((x_1, x_2)) = |\langle (x_1, x_2) \rangle| \mid |H|.$$

(ii) Εάν $\varphi, \psi \in \mathrm{Hom}(G_2, \mathrm{Aut}(G_1))$ και εάν υπάρχει κάποιος ισομορφισμός

$$f : G_1 \rtimes_\varphi G_2 \xrightarrow{\cong} G_1 \rtimes_\psi G_2,$$

τότε από το (i) έπεται ότι $f(G_1 \rtimes_\varphi \{e_{G_2}\}) = G_1 \rtimes_\psi \{e_{G_2}\}$ και

$$f(\mathrm{C}_{G_1 \rtimes_\varphi G_2}(G_1 \rtimes_\varphi \{e_{G_2}\})) = \mathrm{C}_{G_1 \rtimes_\psi G_2}(G_1 \rtimes_\psi \{e_{G_2}\}).$$

Ως εκ τούτου, μέσω τού ισομορφισμού

$$f|_{\mathrm{C}_{G_1 \rtimes_\varphi G_2}(\overline{G}_1)} : \mathrm{C}_{G_1 \rtimes_\varphi G_2}(G_1 \rtimes_\varphi \{e_{G_2}\}) \xrightarrow{\cong} \mathrm{C}_{G_1 \rtimes_\psi G_2}(G_1 \rtimes_\psi \{e_{G_2}\})$$

επάγεται, σε επίπεδο πηλικοομάδων, ο ισομορφισμός

$$\begin{array}{c} \mathrm{C}_{G_1 \rtimes_\varphi G_2}(G_1 \rtimes_\varphi \{e_{G_2}\})/G_1 \rtimes_\varphi \{e_{G_2}\} \\ \Big\downarrow {\scriptstyle (f|_{\mathrm{C}_{G_1 \rtimes_\varphi G_2}(G_1 \rtimes_\varphi \{e_{G_2}\})})^{\pi\eta\lambda.}} \quad \cong \\ \mathrm{C}_{G_1 \rtimes_\psi G_2}(G_1 \rtimes_\psi \{e_{G_2}\})/G_1 \rtimes_\psi \{e_{G_2}\} \end{array} \tag{7.71}$$

(Βλ. θεώρημα 4.5.5.) Από το λήμμα 7.6.11 γνωρίζουμε ότι

$$\mathrm{C}_{G_1 \rtimes_\varphi G_2}(G_1 \rtimes_\varphi \{e_{G_2}\}) = G_1 \rtimes_\varphi \{e_{G_2}\} \boxtimes_\varphi (\{e_{G_1}\} \rtimes_\varphi \mathrm{Ker}(\varphi)).$$

Κατά το 2ο θεώρημα ισομορφισμών 4.5.13,

$$\mathrm{C}_{G_1 \rtimes_\varphi G_2}(G_1 \rtimes_\varphi \{e_{G_2}\})/G_1 \rtimes_\varphi \{e_{G_2}\} \cong \{e_{G_1}\} \rtimes_\varphi \mathrm{Ker}(\varphi) \tag{7.72}$$

(διότι $(\{e_{G_1}\} \rtimes_\varphi \mathrm{Ker}(\varphi)) \cap (G_1 \rtimes_\varphi \{e_{G_2}\}) = \{(e_{G_1}, e_{G_2})\}$). Κατ' αναλογίαν,

$$\mathrm{C}_{G_1 \rtimes_\psi G_2}(G_1 \rtimes_\psi \{e_{G_2}\})/G_1 \rtimes_\psi \{e_{G_2}\} \cong \{e_{G_1}\} \rtimes_\psi \mathrm{Ker}(\psi). \tag{7.73}$$

Από τους ισομορφισμούς (7.71), (7.72) και (7.73) συμπεραίνουμε τελικώς ότι υφίσταται ισομορφισμός $\mathrm{Ker}(\varphi) \xrightarrow{\cong} \mathrm{Ker}(\psi)$. □

7.6.13 Σημείωση. (Απλούστευση συμβολισμού.) Μέχρι στιγμής χρησιμοποιήσαμε τα σύμβολα "$\circledast$", "$\circledcirc$", "$\boxtimes_\varphi$" για τη σήμανση των εσωτερικών πράξεων επί των ομάδων G_1, G_2 και $G_1 \rtimes_\varphi G_2$, αντιστοίχως, προκειμένου να περιγράψουμε επακριβώς τους μεταξύ τους υφιστάμενους συσχετισμούς στις αποδείξεις των προτάσεων 7.6.1, 7.6.3, 7.6.4, 7.6.6, 7.6.7, 7.6.9 και 7.6.12. Από εδώ, όμως, και στο εξής, θα μεταβούμε στον *απλουστευμένο πολλαπλασιαστικό* συμβολισμό των πράξεων *και των τριών* ομάδων G_1, G_2 και $G_1 \rtimes_\varphi G_2$ (μέσω τού dot[88] "$\cdot$").

► **Περιοριστικές συνθήκες προκύπτουσες από τον ορισμό.** Το εξωτερικό *ευθύ* γινόμενο $G_1 \times G_2$ ορίζεται για *τυχούσες* ομάδες G_1, G_2. Αντιθέτως, η δόμηση τού εξωτερικού *ημιευθέος* γινομένου $G_1 \rtimes_\varphi G_2$ δυο ομάδων G_1, G_2 είναι (εξ ορισμού) εφικτή μόνον όταν για αυτές πληρούνται κάποιες περιοριστικές συνθήκες, ακόμη και όταν αμφότερες τυγχάνει να είναι *κυκλικές*! Τούτο παρεμφαίνεται μέσω των προτάσεων 7.6.14, 7.6.16 και 7.6.17.

[88] Είναι βεβαίως αυτονόητο ότι σε ορισμένες εφαρμογές και σε ορισμένα παραδείγματα, στα οποία μία εκ των υπεισερχομένων ομάδων έχει ως πράξη της τη σύνθεση ή τη (συνήθη) πρόσθεση, το dot (ή το νοερό dot) υποκαθίσταται αυτομάτως από τα "$\circ$" και "$+$".

7.6.14 Πρόταση. *Έστω p ένας πρώτος αριθμός. Εάν G_1 είναι μια κυκλική ομάδα τάξεως p^m και G_2 μια κυκλική ομάδα τάξεως p^n με $m,n\in\mathbb{N}$, τότε το εξωτερικό ημιευθύ γινόμενο $G_1\rtimes_\varphi G_2$ (ως προς κάποιον $\varphi\in\mathrm{Hom}(G_2,\mathrm{Aut}(G_1))$) ορίζεται εάν και μόνον εάν*

$$\exists k\in\{1,...,p^m-1\}: p\nmid k \text{ και } k^{p^n}\equiv 1(\mathrm{mod}\,p^m). \tag{7.74}$$

ΑΠΟΔΕΙΞΗ. Εξ υποθέσεως, υπάρχουν $a\in G_1$ και $b\in G_2$ (τάξεως p^m και p^n, αντιστοίχως), τέτοια ώστε $G_1=\langle a\rangle$ και $G_2=\langle b\rangle$. Επειδή $\mathrm{Aut}(G_1)\cong\mathrm{Aut}(\mathbb{Z}_{p^m})\cong\mathbb{Z}_{p^m}^\times$ και, συγκεκριμένα, βάσει των προαναφερθέντων στην απόδειξη τού θεωρήματος 2.4.32, ισχύει

$$\begin{aligned}\mathrm{Aut}(G_1) &= \{\vartheta_k|\, k\in\{1,...,p^m-1\}: \text{μκδ}(k,p^m)=1\}\\ &= \{\vartheta_k|\, k\in\{1,...,p^m-1\}: p\nmid k\},\end{aligned}$$

όπου $\vartheta_k(a^i):=a^{ik}$, $\forall i\in\{0,1,...,p^n-1\}$, οι όποιοι υφιστάμενοι ομομορφισμοί

$$G_2=\langle b\rangle\ni b^j\overset{\varphi}{\longmapsto}\varphi_{b^j}\in\mathrm{Aut}(G_1),\ j\in\{0,1,...,p^m-1\}, \tag{7.75}$$

θα καθορίζονται πλήρως από την τιμή φ_b που θα λαμβάνουν στον γεννήτορα b τής G_2. Έτσι λοιπόν, μια απεικόνιση (7.75) είναι ομομορφισμός ομάδων από την G_2 στην $\mathrm{Aut}(G_1)$ εάν και μόνον εάν

$$\exists\, k\in\{1,...,p^m-1\}: p\nmid k \text{ με } \varphi_b=\vartheta_k \text{ και } \mathrm{ord}(\vartheta_k)\mid p^n\,(=\mathrm{ord}(b)).$$

(Βλ. 2.4.3 (iv).) Η τελευταία συνθήκη διαιρετότητας πληρούται εάν και μόνον εάν[89] $\vartheta_k^{p^n}=\mathrm{id}_{G_1}\Leftrightarrow a^{k^{p^n}}=a\Leftrightarrow a^{k^{p^n}-1}=e_{G_1}\Leftrightarrow\mathrm{ord}(a)=p^m\mid k^{p^n}-1$, όπου η τελευταία αμφίπλευρη συνεπαγωγή έπεται από την πρόταση 2.3.8. □

7.6.15 Παραδείγματα. (i) Στην ειδική περίπτωση όπου $m=1$, έχουμε κατ' ανάγκην $k=1$. Πράγματι· εάν υποθέσουμε ότι $k\geq 2$, το «μικρό» θεώρημα τού Fermat (βλ. Β.4.13 ή 4.1.31) και η ισοτιμία (7.74) δίδουν

$$\left.\begin{array}{r} p\mid k^{p-1}-1\\ \text{και } p\mid k^{p^n}-1\end{array}\right\}\underset{\text{Β.2.6}}{\Longrightarrow} p\mid \text{μκδ}(k^{p-1}-1,k^{p^n}-1)\underset{\text{Β.2.15}}{=}k^{\text{μκδ}(p-1,p^n)}-1$$

με $(-1)(p-1)+p=1\underset{\text{Β.2.8}}{\Longrightarrow}\text{μκδ}(p-1,p)=1\underset{\text{Β.2.13}}{\Longrightarrow}\text{μκδ}(p-1,p^n)=1$, ήτοι $p\mid k-1$, πράγμα *άτοπο*, διότι $1<k<p$. Άρα για $m=1$ ισχύει $k=1\Rightarrow\varphi_b=\vartheta_1=\mathrm{id}_{G_1}$, ο φ είναι ο τετριμμένος ομομορφισμός και $G_1\rtimes_\varphi G_2=\langle a\rangle\times\langle b\rangle\cong\mathbb{Z}_p\oplus\mathbb{Z}_{p^n}$.

(ii) Στην περίπτωση όπου $n=1$, η (7.74) γράφεται $k^p\equiv 1(\mathrm{mod}\,p^m)$. Κάθε k τής μορφής $k=1+lp^{m-1}$, όπου $l\in\mathbb{N}_0$, $l<p$, την ικανοποιεί, αφού

$$k^p=(1+lp^{m-1})^p=1+\sum_{i=1}^{p}\tbinom{p}{i}(lp^{m-1})^i\equiv 1(\mathrm{mod}\,p^m).$$

[89] Προφανώς, $\vartheta_k^{p^n}(a)=\vartheta_k^{p^n-1}(a^k)=(\vartheta_k^{p^n-1}(a))^k=(\vartheta_k^{p^n-2}(a^k))^k=\vartheta_k^{p^n-2}((a^k)^k)=\vartheta_k^{p^n-2}(a^{k^2})$. Επομένως, επαναλαμβάνοντας την ίδια διαδικασία, καταλήγουμε στο ότι $\vartheta_k^{p^n}(a)=a^{k^{p^n}}$.

(Βλ. λήμμα Β.4.10.) Άρα για κάθε $l < p$ ορίζεται το εξωτερικό ημιευθύ γινόμενο $G_1 \rtimes_\varphi G_2$ και υπάρχουν δύο ενδεχόμενα:

α) $l = 0$ και ο φ είναι τετριμμένος (με $G_1 \rtimes_\varphi G_2 = \langle a\rangle \times \langle b\rangle \cong \mathbb{Z}_{p^m} \oplus \mathbb{Z}_p$),

β) $l \in \{1, ..., p-1\}$ και ο φ δεν είναι τετριμμένος, ενώ η εσωτερική πράξη («πολλαπλασιασμός») επί τού $G_1 \rtimes_\varphi G_2$ μπορεί να γραφεί ως

$$(x_1, x_2)\,(y_1, y_2) := \left(x_1 \varphi_{x_2}(y_1), x_2 y_2\right),$$

οπότε οι γεννήτορες $\overline{a} := (a, e_{G_2})$ και $\overline{b} := (e_{G_1}, b)$ των $\overline{G}_1 \cong G_1$ και $\overline{G}_2 \cong G_2$, αντιστοίχως, υπόκεινται (εντός αυτού) στη σχέση $\overline{b}\,\overline{a} = \overline{a}^{1+lp^{m-1}}\,\overline{b}$, διότι

$$\begin{aligned} \overline{b}\,\overline{a} &= (e_{G_1}, b)(a, e_{G_2}) = (e_{G_1}\varphi_b(a), be_{G_2}) \\ &= \left(\vartheta_{1+lp^{m-1}}(a), b\right) = (a^{1+lp^{m-1}}, b) = \overline{a}^{1+lp^{m-1}}\,\overline{b}. \end{aligned}$$

7.6.16 Πρόταση. *Εάν $G_1 = \langle a\rangle$, $G_2 = \langle b\rangle$ είναι δυο άπειρες κυκλικές ομάδες, τότε ορίζεται πάντοτε το εξωτερικό ημιευθύ γινόμενο $G_1 \rtimes_\varphi G_2$ και υπάρχουν δύο ενδεχόμενα: Είτε ο φ είναι τετριμμένος και $G_1 \rtimes_\varphi G_2 = \langle a\rangle \times \langle b\rangle$ είτε ο φ είναι μη τετριμμένος και $\overline{b}\,\overline{a} = \overline{a}^{-1}\,\overline{b}$ (όπου $\overline{a} := (a, e_{G_2})$ και $\overline{b} := (e_{G_1}, b)$).*

ΑΠΟΔΕΙΞΗ. Επειδή $\mathrm{Aut}(G_1) \cong \mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$ και, βάσει των προαναφερθέντων στην απόδειξη τού 2.4.32, ισχύει $\mathrm{Aut}(G_1) = \{\mathrm{id}_{G_1}, \vartheta\}$, όπου $\vartheta(a^i) := a^{-i}$, $\forall i \in \mathbb{Z}$, ένας ομομορφισμός $G_2 = \langle b\rangle \ni b^j \overset{\varphi}{\longmapsto} \varphi_{b^j} = \varphi_b^j \in \mathrm{Aut}(G_1)$, $j \in \mathbb{Z}$, είναι είτε ο τετριμμένος (με $\varphi_{b^j} = \mathrm{id}_{G_1}$ για κάθε $j \in \mathbb{Z}$) είτε ο $\varphi_{b^j} = \vartheta$ (για κάθε $j \in \mathbb{Z}$). Στην πρώτη περίπτωση, $G_1 \rtimes_\varphi G_2 = \langle a\rangle \times \langle b\rangle \cong \mathbb{Z} \oplus \mathbb{Z}$. Στη δεύτερη περίπτωση,

$$\overline{b}\,\overline{a} = (e_{G_1}, b)(a, e_{G_2}) = (e_{G_1}\varphi_b(a), be_{G_2}) = (\vartheta(a), b) = (a^{-1}, b) = \overline{a}^{-1}\,\overline{b},$$

οπότε $G_1 \rtimes_\varphi G_2 = \left\{ \overline{a}^i\,\overline{b}^j \,\middle|\, (i, j) \in \mathbb{Z} \times \mathbb{Z} \text{ και } \overline{b}\,\overline{a} = \overline{a}^{-1}\,\overline{b} \right\}$. □

7.6.17 Πρόταση. *Εάν $G_1 = \langle a\rangle$ είναι μια κυκλική ομάδα τάξεως $n \in \mathbb{N}$, $n \geq 2$, και $G_2 = \langle b\rangle$ είναι μια άπειρη κυκλική ομάδα, τότε το εξωτερικό ημιευθύ γινόμενο $G_1 \rtimes_\varphi G_2$ (ως προς κάποιον $\varphi \in \mathrm{Hom}(G_2, \mathrm{Aut}(G_1))$) ορίζεται εάν και μόνον εάν*

$$\exists k \in \{1, ..., n-1\} : \mu\kappa\delta(k, n) = 1.$$

Εν τοιαύτη περιπτώσει, $\overline{b}\,\overline{a} = \overline{a}^k\,\overline{b}$ (όπου $\overline{a} := (a, e_{G_2})$ και $\overline{b} := (e_{G_1}, b)$).

ΑΠΟΔΕΙΞΗ. Επειδή $\mathrm{Aut}(G_1) \cong \mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$ και, συγκεκριμένα,

$$\mathrm{Aut}(G_1) = \{\, \vartheta_k \,|\, k \in \{1, ..., n-1\} : \mu\kappa\delta(k, n) = 1\},$$

όπου $\vartheta_k(a^i) := a^{ik}$, $\forall i \in \{0, 1, ..., n-1\}$, για κάθε ομομορφισμό

$$G_2 = \langle b\rangle \ni b^j \overset{\varphi}{\longmapsto} \varphi_{b^j} \in \mathrm{Aut}(G_1),\ j \in \{0, 1, ..., n-1\},$$

θα υπάρχει κάποιος $k \in \{1, ..., n-1\} : \mu\kappa\delta(k, n) = 1$ με $\varphi_b = \vartheta_k$. Εάν $k = 1$, τότε $G_1 \rtimes_\varphi G_2 = \langle a\rangle \times \langle b\rangle \cong \mathbb{Z}_n \oplus \mathbb{Z}$. Εάν $k \geq 2$, τότε το εξωτερικό ημιευθύ γινόμενο $G_1 \rtimes_\varphi G_2$ δεν είναι ευθύ. Σε αμφότερες τις περιπτώσεις,

$$\overline{b}\,\overline{a} = (e_{G_1}, b)(a, e_{G_2}) = (e_{G_1}\varphi_b(a), be_{G_2}) = (\vartheta_k(a), b) = (a^k, b) = \overline{a}^k\,\overline{b},$$

οπότε $G_1 \rtimes_\varphi G_2 = \left\{ \overline{a}^i \, \overline{b}^j \,\middle|\, (i,j) \in \{0,1,...,n-1\} \times \mathbb{Z} \text{ και } \overline{b}\,\overline{a} = \overline{a}^k \, \overline{b} \right\}$. □

► **Γνωστές ομάδες παριστώμενες ως εξωτερικό ημιευθύ γινόμενο δύο ομάδων**. Στα θεωρήματα 7.6.19 και 7.6.20 αποδεικνύεται ότι οι ομάδες $\mathbf{V}, \mathbf{D}_n, \mathbf{D}_\infty$ και $\mathbf{L}_{pq}$ είναι ισόμορφες με εξωτερικά ημιευθέα γινόμενα δύο *κυκλικών* ομάδων.

7.6.18 Ορισμός. Έστω $(G,\cdot)$ μια αβελιανή ομάδα. Η **γενικευμένη διεδρική ομάδα** (τάξεως $2\,|G|$) **η επαγόμενη από την** G (ή απλώς **η διεδρικοποίηση τής** G) είναι το εξωτερικό ημιευθύ γινόμενο

$$\boxed{\mathbf{Dih}(G) := G \rtimes_\varphi \{\pm 1\}}$$

των $(G,\cdot)$ και $(\{\pm 1\},\cdot)$, όπου

$$\varphi : (\{\pm 1\},\cdot) \longrightarrow (\mathbf{Aut}(G),\circ)\,,\ x \longmapsto \varphi_x,$$

ο ομομορφισμός ο απεικονίζων το x στον αυτομορφισμό

$$\varphi_x : G \longrightarrow G,\ y \longmapsto \varphi_x(y) := y^x.$$

Κατά συνέπειαν, η εσωτερική πράξη τής $\mathbf{Dih}(G)$ είναι η

$$((x_1,x_2),(y_1,y_2)) \longmapsto (x_1 y_1^{x_2}, x_2 y_2)\,.$$

Σημειωτέον ότι όταν η G είναι *είτε* άπειρη μη περιοδική *είτε* άπειρη περιοδική χωρίς πεπερασμένο εκθέτη *είτε* περιοδική (πεπερασμένη ή άπειρη) πεπερασμένου εκθέτη με $\exp(G) \geq 3$, ο ομομορφισμός φ δεν είναι τετριμμένος, οπότε η $\mathbf{Dih}(G)$ (σύμφωνα με την πρόταση 7.6.4) δεν είναι αβελιανή!

7.6.19 Θεώρημα. *Έστω $(G,\cdot)$ μια ομάδα που είναι είτε τετριμμένη είτε ισόμορφη με μία εκ των $(\mathbb{Z}_2,+)$, $(\mathbb{Z}_n,+)$, $n \geq 3$, $(\mathbb{Z},+)$. Τότε η γενικευμένη διεδρική ομάδα $\mathbf{Dih}(G)$ η επαγόμενη από αυτήν είναι ισόμορφη με την (αντίστοιχη) ομάδα την καταχωριζόμενη στη δεξιά στήλη τού ακόλουθου καταλόγου*:

	G	$\mathbf{Dih}(G)$
(i)	τετριμμένη	$\mathbb{Z}_2$
(ii)	$\mathbb{Z}_2$	$\mathbf{V}$
(iii)	$\mathbb{Z}_n,\ n \geq 3$	$\mathbf{D}_n$
(iv)	$\mathbb{Z}$	$\mathbf{D}_\infty$

ΑΠΟΔΕΙΞΗ. Επειδή $(\{\pm 1\},\cdot) \cong (\mathbb{Z}_2,+)$, το ότι ισχύει $\mathbf{Dih}(G) \cong \mathbb{Z}_2$ στην περίπτωση (i) έπεται άμεσα από τον ορισμό 7.6.18. Στην περίπτωση (ii) έχουμε $\mathbf{Dih}(\mathbb{Z}_2) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong \mathbf{V}$ (βλ. 7.1.67). Στην περίπτωση (iii) η εσωτερική πράξη, με την οποία είναι εφοδιασμένη η $\mathbf{Dih}(\mathbb{Z}_n)$, είναι η

$$(([x_1]_n, x_2), ([y_1]_n, y_2)) \longmapsto ([x_1 + x_2 y_1]_n, x_2 y_2)\,,$$

όπου $x_1, y_1 \in \{0, 1, ..., n-1\}$ και $x_2, y_2 \in \{\pm 1\}$. Κάθε $([x_1]_n, x_2) \in \mathbf{Dih}(\mathbb{Z}_n)$ γράφεται υπό τη μορφή

$$([x_1]_n, x_2) = \begin{cases} ([0]_n, -1)\,([1]_n, 1)^{-x_1}, & \text{όταν } x_2 = -1, \\ ([1]_n, 1)^{x_1}, & \text{όταν } x_2 = 1. \end{cases}$$

όπου $([1]_n, 1)^{x_1} = ([x_1]_n, 1^{x_1}) = ([x_1]_n, 1)$ και $([1]_n, 1)^{-x_1} = (-[x_1]_n, 1)$. Κατά συνέπειαν, $\mathbf{Dih}(\mathbb{Z}_n) = \langle ([0]_n, -1), ([1]_n, 1) \rangle$. Επειδή $([0]_n, -1) \neq ([0]_n, 1)$,

$$([0]_n, -1)^2 = ([0 + (-1) \cdot 0]_n, (-1)(-1)) = ([0]_n, 1) = e_{\mathbf{Dih}(\mathbb{Z}_n)}$$

και $([1]_n, 1)^n = ([n \cdot 1]_n, 1^n) = ([0]_n, 1), ([1]_n, 1)^k = ([k]_n, 1) \neq ([0]_n, 1)$, για κάθε $k \in \{1, ..., n-1\}$, το στοιχείο $([0]_n, -1)$ έχει τάξη 2 και το στοιχείο $([1]_n, 1)$ έχει τάξη $n \geq 3$. Επιπροσθέτως,

$$\begin{aligned} ([1]_n, 1)\,([0]_n, -1) &= ([1 + 1 \cdot 0]_n, 1 \cdot (-1)) = ([1]_n, -1) \\ &= ([0]_n, -1)\,([n-1]_n, 1) = ([0]_n, -1)\,([1]_n, 1)^{-1} \end{aligned}$$

Σύμφωνα με την πρόταση 3.4.7, $\mathbf{Dih}(\mathbb{Z}_n) \cong \mathbf{D}_n$. Στην περίπτωση (iv) η εσωτερική πράξη, με την οποία είναι εφοδιασμένη η $\mathbf{Dih}(\mathbb{Z})$, είναι η

$$((x_1, x_2), (y_1, y_2)) \longmapsto (x_1 + x_2 y_1, x_2 y_2),$$

όπου $x_1, y_1 \in \mathbb{Z}$ και $x_2, y_2 \in \{\pm 1\}$. Χρησιμοποιώντας επιχειρήματα ανάλογα εκείνων που επικαλεσθήκαμε στην (iii) δείχνουμε ότι $\mathbf{Dih}(\mathbb{Z}) = \langle (0, -1), (1, 1) \rangle$ και ότι ισχύει $(1, 1)\,(0, -1) = (0, -1)\,(1, 1)^{-1}$, όπου το στοιχείο $(0, -1)$ έχει τάξη 2. Η μόνη διαφορά έγκειται στο ότι, εν προκειμένω, το στοιχείο $(1, 1)$ είναι άπειρης τάξεως. Επομένως, $\mathbf{Dih}(\mathbb{Z}) \cong \mathbf{D}_\infty$ (επί τη βάσει τής προτάσεως 3.4.17). □

7.6.20 Θεώρημα. *Έστω ότι p, q είναι πρώτοι αριθμοί με $p < q$ και $q \equiv 1 (\mathrm{mod}\, p)$, και έστω*

$$\mathbf{L}_{pq} := \left\{ \begin{pmatrix} [a]_q & [b]_q \\ [0]_q & [1]_q \end{pmatrix} \in \mathbf{GL}_2(\mathbb{Z}_q) \,\middle|\, a, b \in \mathbb{Z} \text{ και } a^p \equiv 1 (\mathrm{mod}\, q) \right\}$$

η μοναδική (μέχρις ισομορφισμού) μη αβελιανή ομάδα τάξεως pq. (Βλ. πρόταση 5.7.15.) *Τότε*

$$\boxed{\mathbf{L}_{pq} \cong \mathbb{Z}_q \rtimes_\varphi \mathbb{Z}_p,}$$

όπου

$$\varphi : (\mathbb{Z}_p, +) \longrightarrow (\mathbf{Aut}(\mathbb{Z}_q), \circ), \; [x]_p \longmapsto \varphi_{[x]_p},$$

είναι ο ομομορφισμός ο απεικονίζων την κλάση ισοτιμίας $[x]_p$ οιουδήποτε $x \in \mathbb{Z}$ στον αυτομορφισμό

$$\varphi_{[x]_p} : \mathbb{Z}_q \longrightarrow \mathbb{Z}_q, \; [y]_q \longmapsto \varphi_{[x]_p}([y]_q) := [\xi^x y]_q \quad (y \in \mathbb{Z}), \tag{7.76}$$

και $\xi := \min \left\{ \lambda \in \{2, ..., q-1\} \,\middle|\, \mathrm{ord}([\lambda]_q) = p \text{ εντός τής } \mathbb{Z}_q^\times \right\}$.

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς, επειδή ο q είναι πρώτος έχουμε $\left|\mathbb{Z}_q^\times\right| = q-1$. Επειδή εξ υποθέσεως $p \mid q-1$, το θεώρημα 4.4.21 τού Cauchy μάς πληροφορεί ότι το σύνολο $\left\{\lambda \in \{2,...,q-1\} \,\middle|\, \mathrm{ord}([\lambda]_q) = p \text{ εντός τής } \mathbb{Z}_q^\times\right\}$ είναι *μη κενό* και, κατ' επέκταση, ο φυσικός αριθμός ξ καλώς ορισμένος. Επιπροσθέτως, οι (7.76) και είναι *καλώς ορισμένες* απεικονίσεις, διότι για οιουσδήποτε $x, x' \in \mathbb{Z}$ με $[x]_p = [x']_p$ και οιουσδήποτε $y, y' \in \mathbb{Z}$ με $[y]_q = [y']_q$έχουμε

$$\left.\begin{array}{r} [x]_p = [x']_p \Rightarrow p \mid x-x' \\ \mathrm{ord}([\xi]_q) = p \text{ (εντός τής } \mathbb{Z}_q^\times) \end{array}\right\} \underset{2.3.8}{\Longrightarrow} [\xi]_q^{x-x'} = [1]_q \Rightarrow [\xi^x]_q = [\xi^{x'}]_q,$$

οπότε

$$[\xi^x y]_q = [\xi^x]_q\,[y]_q = [\xi^{x'}]_q\,[y]_q = [\xi^{x'}]_q [y']_q = [\xi^{x'} y']_q.$$

Η $\varphi_{[x]_p}$ είναι ένας ενδομορφισμός τής $\mathbb{Z}_q$, καθότι για $x, x', y, y' \in \mathbb{Z}$ έχουμε

$$(\varphi_{[x]_p} \circ \varphi_{[x']_p})([y]_q) = \varphi_{[x]_p}([\xi^{x'} y]_q) = [\xi^x \xi^{x'} y]_q = [\xi^{x+x'} y]_q = \varphi_{[x]_p + [x']_p}([y]_q).$$

Εξάλλου, επειδή $[\xi^x]_q \neq [0]_q$ (q πρώτος), ισχύει

$$\mathrm{Ker}(\varphi_{[x]_p}) = \{[y]_q \in \mathbb{Z}_q \,|\, [\xi^x y]_q = [0]_q\} = \{[0]_q\}.$$

Η $\varphi_{[x]_p}$ είναι ενριπτική και, κατ' επέκταση, αμφιριπτική, οπότε $\varphi_{[x]_p} \in \mathrm{Aut}(\mathbb{Z}_q)$. Κατά συνέπειαν, *ορίζεται* το εξωτερικό ημιευθύ γινόμενο $\mathbb{Z}_q \rtimes_\varphi \mathbb{Z}_p$ με την πράξη

$$(([x_1]_q, [x_2]_p), ([y_1]_q, [y_2]_p)) \longmapsto ([x_1 + \xi^{x_2} y_1]_q, [x_2 + y_2]_p).$$

Σημειωτέον ότι $([1]_q, [0]_p)([0]_q, [1]_p) = ([1]_q, [1]_p)$ και

$$([0]_q, [1]_p)([1]_q, [0]_p) = ([\xi]_q, [1]_p),$$

οπότε $\mathrm{ord}([\xi]_q) = p > 1$ (εντός τής $\mathbb{Z}_q^\times$)$\Rightarrow ([1]_q, [1]_p) \neq ([\xi]_q, [1]_p)$. Αυτό σημαίνει ότι η $\mathbb{Z}_q \rtimes_\varphi \mathbb{Z}_p$ είναι μια μη αβελιανή ομάδα τάξεως pq. Άρα η $\mathbb{Z}_q \rtimes_\varphi \mathbb{Z}_p$ είναι κατ' ανάγκην ισόμορφη με την $\mathbf{L}_{pq}$ (επί τη βάσει τής προτάσεως 5.7.15). □

► **Μη αβελιανές ομάδες τάξεως** p^3. Έστω p τυχών πρώτος αριθμός. Ως γνωστόν, οι ομάδες τάξεως p είναι κατ' ανάγκην κυκλικές και οι ομάδες τάξεως p^2 αβελιανές. (Βλ. πορίσματα 4.1.33 και 5.6.7.) Ωστόσο, υπάρχουν ομάδες τάξεως p^3 *που δεν είναι αβελιανές*[90]. Έχουμε ήδη αποδείξει ότι για $p = 2$ υπάρχουν (μέχρις ισομορφισμού) *ακριβώς δύο* μη αβελιανές ομάδες τάξεως 8: οι $\mathbf{Q}$ και $\mathbf{D}_4$. (Βλ. 4.1.39.) Το θεώρημα 7.6.24 επεκτείνει αυτήν την ταξινόμηση για μη αβελιανές ομάδες τάξεως p^3, όπου $p \geq 3$, ενώ το θεώρημα 7.6.25 μας πληροφορεί ότι οι εν λόγω ομάδες είναι ισόμορφες με (κατάλληλα) εξωτερικά ημιευθέα γινόμενα.

[90] Αργότερα, θα αποδείξουμε ότι υπάρχουν (μέχρις ισομορφισμού) *ακριβώς τρεις* αβελιανές ομάδες τάξεως p^3, ήτοι οι $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$, $\mathbb{Z}_p \oplus \mathbb{Z}_{p^2}$ και $\mathbb{Z}_{p^3}$. (Βλ. εδάφιο 9.1.13.)

7.6.21 Συμβολισμός. Εάν p είναι τυχών περιττός πρώτος αριθμός, τότε θέτουμε

$$\boxed{\mathbf{Heis}(\mathbb{Z}_p) := \mathbf{UT}_3^{[1]}(\mathbb{Z}_p) = \left\{ \left(\begin{array}{ccc} [1]_p & [a]_p & [c]_p \\ [0]_p & [1]_p & [b]_p \\ [0]_p & [0]_p & [1]_p \end{array} \right) \middle| \, a,b,c \in \mathbb{Z} \right\}}$$

(για να συμβολίσουμε την κλασική *ομάδα τού Heisenberg υπεράνω τού σώματος* $\mathbb{Z}_p$, βλ. D.2.24) και

$$\boxed{\mathbb{G}_p := \left\{ \left(\begin{smallmatrix} [a]_{p^2} & [b]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{smallmatrix} \right) \in \mathbf{GL}_2(\mathbb{Z}_{p^2}) \middle| \, a,b \in \mathbb{Z} \text{ και } a \equiv 1 (\mathrm{mod}\, p) \right\}.}$$

Είναι άμεσος ο έλεγχος τού ότι το σύνολο $\mathbb{G}_p$, εφοδιασμένο με την πράξη πολλαπλασιασμού πινάκων, αποτελεί μια υποομάδα τής γενικής γραμμικής ομάδας $\mathbf{GL}_2(\mathbb{Z}_{p^2})$ βαθμού 2 υπεράνω τού δακτυλίου $\mathbb{Z}_{p^2}$. (Βλ. D.2.18.)

7.6.22 Πρόταση. *Αμφότερες οι* $\mathbf{Heis}(\mathbb{Z}_p)$ *και* $\mathbb{G}_p$ *είναι μη αβελιανές ομάδες τάξεως* p^3, *και* $\mathbf{Heis}(\mathbb{Z}_p) \ncong \mathbb{G}_p$.

ΑΠΟΔΕΙΞΗ. Επειδή (προφανώς) ισχύει

$$\mathbf{Heis}(\mathbb{Z}_p) = \left\{ \left(\begin{array}{ccc} [1]_p & [a]_p & [c]_p \\ [0]_p & [1]_p & [b]_p \\ [0]_p & [0]_p & [1]_p \end{array} \right) \middle| \, a,b,c \in \{0,1,...,p-1\} \right\}$$

και

$$\left(\begin{array}{ccc} [1]_p & [1]_p & [0]_p \\ [0]_p & [1]_p & [0]_p \\ [0]_p & [0]_p & [1]_p \end{array} \right) \left(\begin{array}{ccc} [1]_p & [0]_p & [0]_p \\ [0]_p & [1]_p & [1]_p \\ [0]_p & [0]_p & [1]_p \end{array} \right) = \left(\begin{array}{ccc} [1]_p & [1]_p & [1]_p \\ [0]_p & [1]_p & [1]_p \\ [0]_p & [0]_p & [1]_p \end{array} \right)$$

$$\neq \left(\begin{array}{ccc} [1]_p & [1]_p & [0]_p \\ [0]_p & [1]_p & [1]_p \\ [0]_p & [0]_p & [1]_p \end{array} \right) = \left(\begin{array}{ccc} [1]_p & [0]_p & [0]_p \\ [0]_p & [1]_p & [1]_p \\ [0]_p & [0]_p & [1]_p \end{array} \right) \left(\begin{array}{ccc} [1]_p & [1]_p & [0]_p \\ [0]_p & [1]_p & [0]_p \\ [0]_p & [0]_p & [1]_p \end{array} \right),$$

η $\mathbf{Heis}(\mathbb{Z}_p)$ είναι μη αβελιανή τάξεως p^3. Από την άλλη μεριά, η κλάση ισοτιμίας $[b]_{p^2}$ στον ορισμό τής $\mathbb{G}_p$ μπορεί να λάβει (προφανώς) οιαδήποτε εκ των p^2 σαφώς διακεκριμένων τιμών $[0]_{p^2}, [1]_{p^2}, ..., \left[p^2-1\right]_{p^2}$, ενώ η κλάση ισοτιμίας $[a]_{p^2}$ μπορεί να λάβει μόνον p σαφώς διακεκριμένες τιμές. Πράγματι· εάν $a_1, a_2 \in \mathbb{Z}$ με

$$a_1 \equiv 1 (\mathrm{mod}\, p), a_2 \equiv 1 (\mathrm{mod}\, p) \text{ και } [a_1]_{p^2} = [a_2]_{p^2},$$

τότε $a_1 = 1 + pm_1$ και $a_2 = 1 + pm_2$, για κάποιους $m_1, m_2 \in \mathbb{Z}$, οπότε

$$\begin{aligned} &[a_1]_{p^2} = [a_2]_{p^2} \Leftrightarrow [pm_1]_{p^2} = [pm_2]_{p^2} \Leftrightarrow p^2 \mid p(m_1 - m_2) \\ &\Leftrightarrow p \mid m_1 - m_2 \Leftrightarrow [m_1]_p = [m_2]_p. \end{aligned}$$

Επειδή λοιπόν

$$\mathbb{G}_p = \left\{ \left(\begin{smallmatrix} [1+pm]_{p^2} & [b]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{smallmatrix} \right) \middle| \, m \in \{0,1,...,p-1\} \text{ και } b \in \{0,1,...,p^2-1\} \right\}$$

και

$$\begin{pmatrix} [1+p]_{p^2} & [0]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{pmatrix}\begin{pmatrix} [1]_{p^2} & [1]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{pmatrix} = \begin{pmatrix} [1+p]_{p^2} & [1+p]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{pmatrix}$$

$$\neq \begin{pmatrix} [1+p]_{p^2} & [1]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{pmatrix} = \begin{pmatrix} [1]_{p^2} & [1]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{pmatrix}\begin{pmatrix} [1+p]_{p^2} & [0]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{pmatrix},$$

η $\mathbb{G}_p$ είναι ωσαύτως μη αβελιανή τάξεως p^3. Τέλος, παρατηρούμε ότι για οιουσδήποτε ακεραίους αριθμούς a, b, c ισχύει

$$\begin{pmatrix} [1]_p & [a]_p & [c]_p \\ [0]_p & [1]_p & [b]_p \\ [0]_p & [0]_p & [1]_p \end{pmatrix}^p = \begin{pmatrix} [1]_p & [0]_p & \left[\frac{p(p-1)}{2}ab\right]_p \\ [0]_p & [1]_p & [0]_p \\ [0]_p & [0]_p & [1]_p \end{pmatrix} = \mathbf{I}_3$$

(διότι $\frac{p(p-1)}{2} \equiv 0 (\mathrm{mod}\, p)$, αφού ο p είναι περιττός), πράγμα που σημαίνει ότι κάθε στοιχείο τής $\mathbf{Heis}(\mathbb{Z}_p)$ διάφορο τού μοναδιαίου πίνακα $\mathbf{I}_3$ έχει τάξη p. Αντιθέτως, το $\begin{pmatrix} [1]_{p^2} & [1]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{pmatrix} \in \mathbb{G}_p$ έχει τάξη p^2, διότι

$$\begin{pmatrix} [1]_{p^2} & [1]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{pmatrix}^k = \begin{pmatrix} [1]_{p^2} & [k]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{pmatrix}$$

για κάθε $k \in \mathbb{Z}$. Επομένως, σύμφωνα με το 2.4.19 (iv), $\mathbf{Heis}(\mathbb{Z}_p) \ncong \mathbb{G}_p$. □

7.6.23 Παρατήρηση. (i) Θέτοντας

$$\mathbf{A} := \begin{pmatrix} [1]_p & [0]_p & [0]_p \\ [0]_p & [1]_p & [1]_p \\ [0]_p & [0]_p & [1]_p \end{pmatrix},\ \mathbf{B} := \begin{pmatrix} [1]_p & [1]_p & [0]_p \\ [0]_p & [1]_p & [0]_p \\ [0]_p & [0]_p & [1]_p \end{pmatrix}, \tag{7.77}$$

παρατηρούμε ότι για οιουσδήποτε $a, b, c \in \mathbb{Z}$ ισχύουν οι ισότητες

$$\begin{pmatrix} [1]_p & [a]_p & [c]_p \\ [0]_p & [1]_p & [b]_p \\ [0]_p & [0]_p & [1]_p \end{pmatrix} = \mathbf{A}^b\mathbf{B}^a[\mathbf{B}, \mathbf{A}]^c = \mathbf{A}^b\mathbf{B}^a[\mathbf{A}, \mathbf{B}]^{-c}, \tag{7.78}$$

όπου $[\mathbf{A}, \mathbf{B}]$ είναι ο μεταθέτης των $\mathbf{A}$ και $\mathbf{B}$. Εξ αυτών έπεται ότι

$$\mathbf{Heis}(\mathbb{Z}_p) = \langle \mathbf{A}, \mathbf{B}, [\mathbf{A}, \mathbf{B}] \rangle = \langle \mathbf{A}, \mathbf{B} \rangle .$$

Οι ανωτέρω γεννήτορες τής $\mathbf{Heis}(\mathbb{Z}_p)$ υπόκεινται στις σχέσεις

$$\mathbf{A}^p = \mathbf{B}^p = [\mathbf{A}, \mathbf{B}]^p = \mathbf{I}_3,\ \ \mathbf{A}[\mathbf{A}, \mathbf{B}]\mathbf{A}^{-1} = \mathbf{B}[\mathbf{A}, \mathbf{B}]\mathbf{B}^{-1} = [\mathbf{A}, \mathbf{B}].$$

(ii) Θέτοντας

$$\mathbf{C} := \begin{pmatrix} [1]_{p^2} & [1]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{pmatrix},\ \mathbf{D} := \begin{pmatrix} [1+p]_{p^2} & [0]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{pmatrix}, \tag{7.79}$$

παρατηρούμε ότι για οιουσδήποτε $m, b \in \mathbb{Z}$ ισχύουν οι ισότητες

$$\begin{pmatrix} [1+pm]_{p^2} & [b]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{pmatrix} = \mathbf{C}^b\mathbf{D}^m,\ \ [\mathbf{C}, \mathbf{D}] = \mathbf{C}^{-p} = \begin{pmatrix} [1]_{p^2} & [-p]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{pmatrix}, \tag{7.80}$$

όπου $[\mathbf{C},\mathbf{D}]$ είναι ο μεταθέτης των $\mathbf{C}$ και $\mathbf{D}$. Εξ αυτών έπεται ότι

$$\mathbb{G}_p = \langle \mathbf{C},\mathbf{D},[\mathbf{C},\mathbf{D}]\rangle = \langle \mathbf{C},\mathbf{D}\rangle\,.$$

Οι ανωτέρω γεννήτορες τής $\mathbb{G}_p$ υπόκεινται στις σχέσεις

$$\mathbf{C}^{2p} = \mathbf{D}^p = [\mathbf{C},\mathbf{D}]^p = \mathbf{I}_3,\ \ \mathbf{D}\,\mathbf{C}\,\mathbf{D}^{-1} = \mathbf{C}^{p+1}.$$

7.6.24 Θεώρημα. (Ταξινόμηση μη αβελιανών ομάδων τάξεως p^3, $p\neq 2$.) *Εάν η $(G,\cdot)$ είναι μια μη αβελιανή ομάδα τάξεως $|G|=p^3$, όπου p περιττός πρώτος αριθμός, τότε είτε*

$$\boxed{G\cong \mathbf{Heis}(\mathbb{Z}_p)} \quad \textit{είτε} \quad \boxed{G\cong \mathbb{G}_p.}$$

ΑΠΟΔΕΙΞΗ. Έστω $(G,\cdot)$ μια μη αβελιανή ομάδα με ακριβώς p^3 στοιχεία.

Βήμα 1ο. Σύμφωνα με το πόρισμα 5.6.8, $|Z(G)|=p$ και $G'=Z(G)$. Το κέντρο $Z(G)$ τής G αποτελεί μια κυκλική υποομάδα τής G. Ταυτοχρόνως, η πηλικοομάδα $G/Z(G)$ έχει τάξη p^2 και είναι, ως εκ τούτου, αβελιανή μη κυκλική και ισόμορφη τής $\mathbb{Z}_p\oplus\mathbb{Z}_p$. (Βλ., κατά σειράν, τα πορίσματα 4.1.33 και 4.1.22, το θεώρημα 7.1.46 και την πρόταση 5.4.17.) Ειδικότερα, $Z(G)=\langle z\rangle\,,\ \forall z\in Z(G)\smallsetminus\{e_G\}$ (βλ. 4.1.34 (iii)⇔(ii)) και υπάρχουν στοιχεία $xZ(G)$ και $yZ(G)$ τής $G/Z(G)$ (για κατάλληλα $x,y\in G\smallsetminus\{e_G\}$), καθένα εκ των οποίων έχει τάξη p (εντός τής $G/Z(G)$), και για τα οποία ισχύει[91]

$$G/Z(G)=\langle xZ(G)\rangle\times_{\text{εσ.}}\langle yZ(G)\rangle=\langle xZ(G)\rangle\,\langle yZ(G)\rangle=\langle xZ(G),yZ(G)\rangle\,. \quad (7.81)$$

Ισχυρισμός πρώτος: $xy\neq yx$. Αυτός θα επαληθευθεί κάνοντας χρήση τής «εις άτοπον απαγωγής». Εάν υποθέσουμε ότι $xy=yx$ και ότι z είναι τυχών γεννήτορας τού κέντρου $Z(G)$ τής G, τότε (λόγω τής (7.81)) για κάθε $g\in G$ θα υπάρχουν $k,l\in\mathbb{Z}$, τέτοιοι ώστε να ισχύει

$$gZ(G)=(xZ(G))^k(yZ(G))^l=(x^ky^l)Z(G)\Rightarrow g^{-1}(x^ky^l)\in Z(G)\ (=\langle z\rangle)\,.$$

Επομένως, $\exists m\in\mathbb{Z}: g^{-1}(x^ky^l)=z^{-m}$ ή, ισοδυνάμως, $g=x^ky^lz^m$. Θεωρώντας, εν συνεχεία, *τυχόντα* $g_1,g_2\in G$, και γράφοντας $g_1=x^{k_1}y^{l_1}z^{m_1}$ και $g_2=x^{k_2}y^{l_2}z^{m_2}$ για κατάλληλους ακεραίους k_1,k_2,l_1,l_2,m_1,m_2, παρατηρούμε ότι

$$g_1g_2=\left(x^{k_1}y^{l_1}\right)\underbrace{z^{m_1}}_{\in Z(G)}\left(\left(x^{k_2}y^{l_2}\right)z^{m_2}\right)=x^{k_1}(y^{l_1}x^{k_2})y^{l_2}z^{m_1+m_2}$$

$$=x^{k_1}(x^{k_2}y^{l_1})y^{l_2}z^{m_1+m_2}=x^{k_1+k_2}y^{l_1+l_2}z^{m_1+m_2}$$

και

$$g_2g_1=\left(x^{k_2}y^{l_2}\right)\underbrace{z^{m_2}}_{\in Z(G)}\left(\left(x^{k_1}y^{l_1}\right)z^{m_1}\right)=x^{k_2}(y^{l_2}x^{k_1})y^{l_1}z^{m_1+m_2}$$

$$=x^{k_2}(x^{k_1}y^{l_2})y^{l_1}z^{m_1+m_2}=x^{k_1+k_2}y^{l_1+l_2}z^{m_1+m_2},$$

[91] Αρκεί κανείς να ακολουθήσει το δεύτερο σκέλος τής αποδείξεως τού θεωρήματος 7.1.46 (με την $G/Z(G)$ στη θέση τής εκεί παρατεθείσας ομάδας G και με τα $xZ(G)$, $yZ(G)$ στη θέση των εκεί παρατεθέντων x και y, αντιστοίχως) και να λάβει υπ' όψιν την πρόταση 4.2.24.

όπου οι προτελευταίες ισότητες έπονται από την $xy = yx$ (βλ. 2.1.12), οπότε $g_1g_2 = g_2g_1$ και η G είναι αβελιανή. Άτοπο!

Ισχυρισμός δεύτερος: $[x,y] \in Z(G)\setminus\{e_G\}$. Ο μεταθέτης $[x,y] := xyx^{-1}y^{-1} \in G'$ των x και y ανήκει στο κέντρο $Z(G)$ τής G, διότι $G' = Z(G)$. Επίσης, βάσει των προαναφερθέντων, $xy \neq yx \Rightarrow [x,y] \neq e_G$. Άρα και ο δεύτερος ισχυρισμός είναι αληθής και $Z(G) = \langle [x,y] \rangle$. (Βλ. 4.1.34 (iii)⇔(ii).)

Ισχυρισμός τρίτος: $G = \langle x, y, [x,y] \rangle = \langle x, y \rangle$. Έστω τυχόν $g \in G$. Από την (7.81) έπεται ότι υπάρχουν $k, l \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει

$$gZ(G) = (xZ(G))^k (yZ(G))^l = (x^k y^l)Z(G) \Rightarrow g^{-1}(x^k y^l) \in Z(G)\ (= \langle [x,y] \rangle)\,.$$

Επομένως, $\exists m \in \mathbb{Z} : g^{-1}(x^k y^l) = [x,y]^{-m}$ ή, ισοδυνάμως,

$$g = x^k y^l\, [x,y]^m \in \langle x, y, [x,y] \rangle\,.$$

(Η ισότητα $G = \langle x, y \rangle$ προκύπτει από το ότι $[x,y] \in \langle x, y \rangle$.)

Βήμα 2ο. Κάθε στοιχείο τής G έχει ως τάξη του έναν θετικό διαιρέτη τού p^3. (Βλ. 4.1.27.) Το μόνο στοιχείο τής G τάξεως 1 είναι το e_G. Εξάλλου, δεν υφίσταται κανένα στοιχείο τής G έχον ως τάξη του τον ίδιον τον p^3. (Αλλιώς η G θα έπρεπε να είναι κυκλική. Βλ. πρόταση 2.3.7.) Κατά συνέπειαν, για κάθε $g \in G\setminus\{e_G\}$ έχουμε $\mathrm{ord}(g) \in \{p, p^2\}$. Εξετάζουμε τα τρία ενδεχόμενα χωριστά.

Περίπτωση πρώτη: $\mathrm{ord}(x) = \mathrm{ord}(y) = p$. Εν προκειμένω, έχοντας ως κίνητρό μας τις ισότητες (7.78) θεωρούμε την

$$\mathbf{Heis}(\mathbb{Z}_p) \ni \begin{pmatrix} [1]_p & [a]_p & [c]_p \\ [0]_p & [1]_p & [b]_p \\ [0]_p & [0]_p & [1]_p \end{pmatrix} \longmapsto x^b y^a\, [x,y]^{-c} \in G \tag{7.82}$$

για οιαδήποτε τριάδα $(a,b,c) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$. Η (7.82) είναι καλώς ορισμένη απεικόνιση, διότι εάν $(a_1,b_1,c_1) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ και $(a_2,b_2,c_2) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ με $([a_1]_p,[b_1]_p,[c_1]_p) = ([a_2]_p,[b_2]_p,[c_2]_p)$, τότε

$$\exists(\nu,\xi,\varrho) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z} : a_1 = p\nu + a_2,\ b_1 = p\xi + b_2,\ c_1 = p\varrho + c_2,$$

οπότε (λόγω των $x^p = y^p = e_G$ και $[[x,y] \in Z(G)\ \text{και}\ |Z(G)| = p] \Rightarrow [x,y]^p = e_G$)

$$x^{b_1}y^{a_1}\,[x,y]^{-c_1} = (x^p)^{\xi}x^{b_2}(y^p)^{\nu}y^{a_2}([x,y]^p)^{-\varrho}\,[x,y]^{-c_2} = x^{b_2}y^{a_2}\,[x,y]^{-c_2}\,.$$

Η (7.82) είναι προφανώς επιρριπτική (απεικονίζουσα τον πίνακα **A** στο x και τον **B** στο y), αποτελεί δε και *ομομορφισμό ομάδων*, καθόσον για οιεσδήποτε τριάδες $(a_1,b_1,c_1) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ και $(a_2,b_2,c_2) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ λαμβάνουμε

$$\begin{pmatrix} [1]_p & [a_1]_p & [c_1]_p \\ [0]_p & [1]_p & [b_1]_p \\ [0]_p & [0]_p & [1]_p \end{pmatrix}\begin{pmatrix} [1]_p & [a_2]_p & [c_2]_p \\ [0]_p & [1]_p & [b_2]_p \\ [0]_p & [0]_p & [1]_p \end{pmatrix} = \begin{pmatrix} [1]_p & [a_1+a_2]_p & [a_1b_2+c_1+c_2]_p \\ [0]_p & [1]_p & [b_1+b_2]_p \\ [0]_p & [0]_p & [1]_p \end{pmatrix}$$

και[92]

$$\begin{aligned} &[x,y] \in Z(G) \Rightarrow [x,y]^{-1} = [y,x] \in Z(G) \underset{(5.43)}{\Longrightarrow} \left[y^{a_1}, x^{b_2}\right] = [y,x]^{a_1b_2} \\ &\Rightarrow y^{a_1}x^{b_2} = [y,x]^{a_1b_2}\,x^{b_2}y^{a_1} = [x,y]^{-a_1b_2}\,x^{b_2}y^{a_1} \end{aligned}$$

[92]Επειδή $[y,x] \in Z(G) = \bigcap\limits_{g\in G} \mathrm{C}_G(g) \subseteq \mathrm{C}_G(y) \cap \mathrm{C}_G(x)$, έχουμε τη δυνατότητα εφαρμογής τής ισότητας (5.43) τής αποδειχθείσας στο (ix) τής προτάσεως 5.5.2.

και, ως εκ τούτου,

$$\left(x^{b_1}y^{a_1}\,[x,y]^{-c_1}\right)\left(x^{b_2}y^{a_2}\,[x,y]^{-c_2}\right) = (x^{b_1}y^{a_1})\underbrace{[x,y]^{-c_1}}_{\in Z(G)}\left(x^{b_2}y^{a_2}\,[x,y]^{-c_2}\right)$$
$$= x^{b_1}(y^{a_1}x^{b_2})y^{a_2}\,[x,y]^{-(c_1+c_2)} = x^{b_1}([x,y]^{-a_1b_2}\,x^{b_2}y^{a_1})y^{a_2}\,[x,y]^{-(c_1+c_2)}$$
$$= x^{b_1}(\underbrace{[x,y]^{-a_1b_2}}_{\in Z(G)}(x^{b_2}y^{a_1+a_2}\,[x,y]^{-(c_1+c_2)})) = x^{b_1+b_2}y^{a_1+a_2}\,[x,y]^{-(a_1b_2+c_1+c_2)}\,.$$

Επειδή $|\mathbf{Heis}(\mathbb{Z}_p)| = |G|$, ο επιμορφισμός (7.82) είναι κατ' ανάγκην ισομορφισμός.

Περίπτωση δεύτερη: $(\mathrm{ord}(x),\mathrm{ord}(y)) \in \{(p^2,p),(p,p^2)\}$. Δίχως βλάβη τής γενικότητας (ήτοι μέχρις εναλλαγής των ρόλων των x και y) αρκεί να υποθέσουμε ότι $\mathrm{ord}(x) = p^2$ και $\mathrm{ord}(y) = p$. Επειδή (*και* από τα προαναφερθέντα στο 1ο βήμα)

$$\left.\begin{array}{r}(xZ(G))^p = e_{G/Z(G)} = Z(G) \Rightarrow x^p \in Z(G)\\ \mathrm{ord}(x) = p^2 > p \Rightarrow x^p \neq e_G\end{array}\right\} \Rightarrow x^p \in Z(G)\smallsetminus\{e_G\}$$
$$\underset{4.1.34}{\Longrightarrow} Z(G) = \langle x^p\rangle = \langle x^{-p}\rangle$$

και $Z(G) = \langle [x,y]\rangle$, υπάρχει ακέραιος k, $k \not\equiv 0(\mathrm{mod}\,p)$, τέτοιος ώστε να ισχύει $[x,y] = (x^{-p})^k$. Κι επειδή $[k]_p \in \mathbb{Z}_p^\times$, υπάρχει $l \in \mathbb{Z}$, $l \not\equiv 0(\mathrm{mod}\,p)$, τέτοιος ώστε η κλάση ισοτιμίας $[l]_p$ να αποτελεί το αντίστροφο τής κλάσεως ισοτιμίας $[k]_p$ εντός τής $\mathbb{Z}_p^\times$. Προφανώς,

$$p \mid kl-1 \Rightarrow [\exists\lambda \in \mathbb{Z} : kl-1 = p\lambda]\,.$$

Από την άλλη μεριά,

$$[x,y] \in Z(G) \underset{(5.43)}{\Longrightarrow} [x,y^l] = [x,y]^l = x^{-pkl} = x^{-p(1+p\lambda)} = x^{-p}(x^{p^2})^{(-\lambda)} = x^{-p},$$

διότι $x^{p^2} = e_G$. Θέτοντας $\hat{y} := y^l$, παρατηρούμε ότι

$$l \not\equiv 0(\mathrm{mod}\,p) \Rightarrow \mu\kappa\delta(p,l) = 1 \underset{2.3.17}{\Longrightarrow} [\langle y\rangle = \langle\hat{y}\rangle \ \text{ και } \mathrm{ord}(\hat{y}) = p]\,,$$

απ' όπου προκύπτει ότι

$$G = \langle x,y\rangle = \langle x,\hat{y}\rangle \ \text{ με } [x,\hat{y}] = x^{-p} \in Z(G). \tag{7.83}$$

Έχοντας ως κίνητρό μας την πρώτη εκ των ισοτήτων (7.80) θεωρούμε την

$$\mathbb{G}_p \ni \begin{pmatrix} [1+pm]_{p^2} & [b]_{p^2} \\ [0]_{p^2} & [1]_{p^2}\end{pmatrix} \longmapsto x^b\hat{y}^m \in G \tag{7.84}$$

για κάθε ζεύγος $(b,m) \in \mathbb{Z}\times\mathbb{Z}$. Η (7.84) είναι καλώς ορισμένη απεικόνιση, διότι εάν $(b_1,m_1) \in \mathbb{Z}\times\mathbb{Z}$ και $(b_2,m_2) \in \mathbb{Z}\times\mathbb{Z}$ με $([b_1]_{p^2},[m_1]_p,) = ([b_2]_{p^2},[m_2]_p)$, τότε

$$\exists(\nu,\xi) \in \mathbb{Z}\times\mathbb{Z} : b_1 = p^2\nu + b_2,\ m_1 = p\xi + m_2,$$

οπότε (λόγω των $x^{p^2} = \hat{y}^p = e_G$) ισχύει $x^{b_1}\hat{y}^{m_1} = (x^{p^2})^\nu x^{b_2}(\hat{y}^p)^\xi\hat{y}^{m_2} = x^{b_2}\hat{y}^{m_2}$. Η (7.84) είναι προφανώς επιρριπτική (απεικονίζουσα τον πίνακα $\mathbf{C}$ στο x και τον

D στο y), αποτελεί δε και *ομομορφισμό ομάδων*, καθόσον για οιαδήποτε ζεύγη $(b_1, m_1) \in \mathbb{Z} \times \mathbb{Z}$ και $(b_2, m_2) \in \mathbb{Z} \times \mathbb{Z}$ λαμβάνουμε

$$\begin{pmatrix} [1+pm_1]_{p^2} & [b_1]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{pmatrix} \begin{pmatrix} [1+pm_2]_{p^2} & [b_2]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{pmatrix} = \begin{pmatrix} [1+p(m_1+m_2)]_{p^2} & [pm_1b_2+b_1+b_2]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{pmatrix}$$

και

$$\begin{aligned} &[x, \hat{y}] \in Z(G) \Rightarrow [x, \hat{y}]^{-1} = [\hat{y}, x] \in Z(G) \underset{(5.43)}{\Longrightarrow} [\hat{y}^{m_1}, x^{b_2}] = [\hat{y}, x]^{m_1 b_2} \\ &\Rightarrow \hat{y}^{m_1} x^{b_2} = [\hat{y}, x]^{m_1 b_2} x^{b_2} \hat{y}^{m_1} = [x, \hat{y}]^{-m_1 b_2} x^{b_2} \hat{y}^{m_1} \\ &\underset{(7.83)}{=} (x^{-p})^{(-m_1 b_2)} x^{b_2} \hat{y}^{m_1} = x^{pm_1 b_2 + b_2} \end{aligned}$$

και, ως εκ τούτου,

$$\left(x^{b_1} \hat{y}^{m_1}\right)\left(x^{b_2} \hat{y}^{m_2}\right) = x^{b_1}\left(\hat{y}^{m_1} x^{b_2}\right)\hat{y}^{m_2} = x^{b_1} x^{pm_1 b_2 + b_2} \hat{y}^{m_2} = x^{pm_1 b_2 + b_1 + b_2}\, \hat{y}^{m_1 + m_2}.$$

Επειδή $|\mathbb{G}_p| = |G|$, ο επιμορφισμός (7.84) είναι κατ' ανάγκην ισομορφισμός.

Περίπτωση τρίτη: $\text{ord}(x) = \text{ord}(y) = p^2$. Επειδή η $G/Z(G)$ έχει τάξη p^2 και είναι *μη κυκλική*, έχουμε για κάθε $g \in G$

$$g^p Z(G) = (gZ(G))^p = e_{G/Z(G)} = Z(G) \Rightarrow g^p \in Z(G).$$

Εξάλλου,

$$\left.\begin{aligned} x^p \in Z(G) \\ \text{ord}(x) = p^2 > p \Rightarrow x^p \neq e_G \end{aligned}\right\} \Rightarrow x^p \in Z(G) \setminus \{e_G\} \underset{4.1.34}{\Longrightarrow} Z(G) = \langle x^p \rangle .$$

Επομένως, $y^p \in Z(G) \Rightarrow \exists r \in \mathbb{Z} : y^p = (x^p)^r$. Σημειωτέον ότι η απεικόνιση

$$G \ni g \longmapsto g^p \in G$$

αποτελεί έναν *ενδομορφισμό* της ομάδας G. [Πράγματι· εάν $(g_1, g_2) \in G \times G$, τότε $[g_1, g_2] \in G' = Z(G)$, οπότε $[g_1, g_2]^p = e_G$, διότι $|Z(G)| = p$. Επιπλέον, επειδή $[g_1, g_2] \in Z(G)$, έχουμε τη δυνατότητα εφαρμογής της ισότητας (5.44) της αποδειχθείσας στο (x) της προτάσεως 5.5.2 (για την p-οστή δύναμη του γινομένου $g_1 g_2$):

$$(g_1 g_2)^p = [g_2, g_1]^{\frac{p(p-1)}{2}} g_1^p g_2^p = ([g_1, g_2]^p)^{\frac{1-p}{2}} g_1^p g_2^p = (e_G)^{\frac{1-p}{2}} g_1^p g_2^p = g_1^p g_2^p,$$

απ' όπου προκύπτει ότι $(g_1 g_2)^p = g_1^p g_2^p$.] Κατά συνέπειαν,

$$\left.\begin{aligned} y^p = (x^p)^r \Rightarrow (yx^{-r})^p = y^p (x^{-r})^p = e_G \\ [\text{η } G \text{ δεν είναι αβελιανή}] \Rightarrow y \notin \langle x \rangle \Rightarrow yx^{-r} \neq e_G \end{aligned}\right\} \Longrightarrow \text{ord}(yx^{-r}) = p.$$

Θέτοντας λοιπόν $\widetilde{y} := yx^{-r}$, λαμβάνουμε

$$G = \langle x, y \rangle = \langle x, \widetilde{y} \rangle \;\text{ με }\; \text{ord}(\widetilde{y}) = p.$$

Στο σημείο αυτό, αντικαθιστώντας το σύστημα γεννητόρων $\{x, y\}$ της G με το $\{x, \widetilde{y}\}$, εμπίπτουμε σε ό,τι εξετάσαμε προηγουμένως στη δεύτερη περίπτωση, οπότε η G είναι κατ' ανάγκην ισόμορφη με την $\mathbb{G}_p$. □

7.6.25 Θεώρημα. *Για κάθε περιττό πρώτο αριθμό p έχουμε*

$$\boxed{\mathbf{Heis}(\mathbb{Z}_p) \cong (\mathbb{Z}_p \oplus \mathbb{Z}_p) \rtimes_{\varphi} \mathbb{Z}_p,}$$

όπου $\varphi : \mathbb{Z}_p \longrightarrow \mathrm{Aut}(\mathbb{Z}_p \oplus \mathbb{Z}_p) \underset{7.1.74}{\cong} \mathbf{GL}_2(\mathbb{Z}_p),\ [j]_p \longmapsto \varphi_{[j]_p}$, *είναι ο ομομορφισμός ο απεικονίζων την κλάση ισοτιμίας* $[j]_p$ *καθενός* $j \in \mathbb{Z}$ *στον αυτομορφισμό*

$$\varphi_{[j]_p} : \mathbb{Z}_p \oplus \mathbb{Z}_p \longrightarrow \mathbb{Z}_p \oplus \mathbb{Z}_p,$$
$$[j]_q \longmapsto \varphi_{[j]_p}([k]_p, [l]_p) := ([k]_p, [l]_p) \begin{pmatrix} [1]_p & [j]_p \\ [0]_p & [1]_p \end{pmatrix},\ \forall (k,l) \in \mathbb{Z} \times \mathbb{Z},$$

οπότε η εσωτερική πράξη επί τής $(\mathbb{Z}_p \oplus \mathbb{Z}_p) \rtimes_{\varphi} \mathbb{Z}_p$ *είναι η*

$$(([k_1]_p, [l_1]_p), [j_1]_p) \cdot (([k_2]_p, [l_2]_p), [j_2]_p) := (([k_1 + k_2]_p, [k_2 j_1 + l_1 + l_2]_p), [j_1 + j_2]_p)$$

για οιουσδήποτε $k_1, k_2, l_1, l_2, j_1, j_2 \in \mathbb{Z}$. *Επιπροσθέτως,*

$$\boxed{\mathbb{G}_p \cong \mathbb{Z}_{p^2} \rtimes_{\psi} \mathbb{Z}_p,}$$

όπου $\psi : \mathbb{Z}_p \longrightarrow \mathrm{Aut}(\mathbb{Z}_{p^2}) \underset{2.4.32\,(ii)}{\cong} \mathbb{Z}_{p^2}^{\times},\ [j]_p \longmapsto \psi_{[j]_p}$, *είναι ο ομομορφισμός ο απεικονίζων την κλάση ισοτιμίας* $[j]_p$ *καθενός* $j \in \mathbb{Z}$ *στον αυτομορφισμό*

$$\psi_{[j]_p} : \mathbb{Z}_{p^2} \longrightarrow \mathbb{Z}_{p^2},\ [k]_{p^2} \longmapsto \psi_{[j]_p}([k]_{p^2}) := [(jp+1)k]_{p^2},\ \forall k \in \mathbb{Z},$$

οπότε η εσωτερική πράξη επί τής $\mathbb{Z}_{p^2} \rtimes_{\psi} \mathbb{Z}_p$ *είναι η*

$$([k_1]_{p^2}, [j_1]_p) \cdot ([k_2]_{p^2}, [j_2]_p) := ([k_1 + (j_1 p + 1)k_2]_{p^2}, [j_1 + j_2]_p)$$

για οιουσδήποτε $k_1, k_2, j_1, j_2 \in \mathbb{Z}$.

ΑΠΟΔΕΙΞΗ. Είναι άμεσος ο έλεγχος τού ότι οι απεικονίσεις

$$\mathbf{Heis}(\mathbb{Z}_p) \ni \begin{pmatrix} [1]_p & [a]_p & [c]_p \\ [0]_p & [1]_p & [b]_p \\ [0]_p & [0]_p & [1]_p \end{pmatrix} \longmapsto (([a]_p, [c]_p), [b]_p) \in (\mathbb{Z}_p \oplus \mathbb{Z}_p) \rtimes_{\varphi} \mathbb{Z}_p$$

(για κάθε τριάδα $(a,b,c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$) και

$$\mathbb{G}_p \ni \begin{pmatrix} [1+pm]_{p^2} & [b]_{p^2} \\ [0]_{p^2} & [1]_{p^2} \end{pmatrix} \longmapsto ([b]_{p^2}, [m]_p) \in \mathbb{Z}_{p^2} \rtimes_{\psi} \mathbb{Z}_p$$

(για κάθε ζεύγος $(b,m) \in \mathbb{Z} \times \mathbb{Z}$) αποτελούν *ισομορφισμούς ομάδων*. □

► **Οικογένειες «νέων» ομάδων δημιουργούμενες μέσω εξωτερικών ημιευθέων γινομένων.** Το εξωτερικό ημιευθύ γινόμενο (ή κάποια κατάλληλη πηλικοομάδα αυτού) είναι δυνατόν να χρησιμοποιηθεί για να ορισθούν ολόκληρες *οικογένειες* «νέων» *μη αβελιανών* ομάδων. Δειγματοληπτικώς, θα αναφερθούν οι οικογένειες των *ημιδιεδρικών* και των *δικυκλικών ομάδων*.

7.6.26 Ορισμός. Έστω $n \in \mathbb{N}$, $n \geq 4$, και έστω $(G,\cdot) \cong (\mathbb{Z}_{2^{n-1}},+)$ μια κυκλική ομάδα τάξεως 2^{n-1}. Παγιώνουμε έναν γεννήτορα g τής G. Η απεικόνιση

$$\vartheta : G \longrightarrow G,\ g^j \longmapsto \vartheta(g^j) := g^{\left(2^{n-2}-1\right)j},\ \forall j \in \{0,1,...,2^{n-1}-1\},$$

αποτελεί έναν αυτομορφισμό τής G τάξεως 2, διότι $\mu\kappa\delta(2^{n-2}-1, 2^{n-1}) = 1$ και

$$\left(2^{n-2}-1\right)^2 = 2^{2(n-2)} - 2^{n-1} + 1 = (2^{n-3}-1)2^{n-1} + 1 \equiv 1 (\mathrm{mod}\, 2^{n-1}).$$

Ορίζουμε ως (n-οστή) **ημιδιεδρική** (ή **σχεδόν διεδρική**) ομάδα το εξωτερικό ημιευθύ γινόμενο[93]

$$\boxed{\mathbf{SD}_n := \quad G \rtimes_\iota \langle\vartheta\rangle\,,}$$

τής G και τής $\langle\vartheta\rangle = \{\mathrm{id}_G, \vartheta\}$, όπου $\iota : \langle\vartheta\rangle \hookrightarrow \mathrm{Aut}(G)$ είναι η συνήθης ένθεση[94]. Προφανώς, η $\mathbf{SD}_n$ είναι μη αβελιανή[95], έχει τάξη $|\mathbf{SD}_n| = 2^n$ και η εσωτερική της πράξη είναι η

$$(g^j, \vartheta^l)\cdot(g^k, \vartheta^m) := (g^j \vartheta^l(g^k), \vartheta^{l+m}), \tag{7.85}$$

$\forall (j,k) \in \{0,1,...,2^{n-1}-1\} \times \{0,1,...,2^{n-1}-1\}$ και $\forall (l,m) \in \{0,1\}\times\{0,1\}$.

7.6.27 Πρόταση. *Θέτοντας* $\mathfrak{a} := (e_G, \vartheta)$ *και* $\mathfrak{b} := (g^{-1}, \mathrm{id}_G)$ *λαμβάνουμε*

$$\mathbf{SD}_n = \langle \mathfrak{a}, \mathfrak{b}\rangle\,,\ \text{όπου}\ \mathrm{ord}(\mathfrak{a}) = 2,\ \mathrm{ord}(\mathfrak{b}) = 2^{n-1}\ \text{και}\ \mathfrak{b}\mathfrak{a} = \mathfrak{a}\mathfrak{b}^{2^{n-2}-1}.$$

ΑΠΟΔΕΙΞΗ. Προφανώς, $\mathbf{SD}_n = \{(g^j,\vartheta^l)\,\big|\, l \in \{0,1\},\ j \in \{0,1,...,2^{n-1}-1\}\}$. Επειδή η (7.85) δίδει

$$\begin{aligned}
&(g^j, \mathrm{id}_G)\cdot(g^k, \mathrm{id}_G) := (g^{j+k}, \mathrm{id}_G), \quad &&(g^j, \vartheta)\cdot(g^k, \mathrm{id}_G) := (g^{j+(2^{n-2}-1)k}, \vartheta),\\
&(g^j, \mathrm{id}_G)\cdot(g^k, \vartheta) := (g^{j+k}, \vartheta), &&(g^j, \vartheta)\cdot(g^k, \vartheta) := (g^{j+(2^{n-2}-1)k}, \mathrm{id}_G),
\end{aligned}$$

για κάθε $(j,k) \in \{0,1,...,2^{n-1}-1\}\times\{0,1,...,2^{n-1}-1\}$, έχουμε

$$(g^j,\vartheta^l) = (e_G,\vartheta)^l\cdot(g^{-1},\mathrm{id}_G)^j = (e_G,\vartheta)^l\cdot(g^{2^{n-1}-1},\mathrm{id}_G)^j = \mathfrak{a}^l\mathfrak{b}^j$$

για κάθε $(l,j) \in \{0,1\}\times\{0,1,...,2^{n-1}-1\}$, οπότε

$$\mathbf{SD}_n = \langle \mathfrak{a},\mathfrak{b}\rangle = \left\{\mathfrak{a}^l\mathfrak{b}^j\,\big|\, l\in\{0,1\},\ j\in\{0,1,...,2^{n-1}-1\}\right\}.$$

---

[93] Η διαφορά μεταξύ τής $\mathbf{SD}_n$ και τής διεδρικής ομάδας $\mathbf{D}_{2^{n-1}} := \langle\alpha,\beta\rangle$ (τάξεως $\left|\mathbf{D}_{2^{n-1}}\right| = 2^n = |\mathbf{SD}_n|$) έγκειται στο ότι οι γεννήτορες τής $\mathbf{D}_{2^{n-1}}$ υπόκεινται στη σχέση $\beta\circ\alpha = \alpha\circ\beta^{2^{n-1}-1}$ (βλ. (3.16)). Παρά το γεγονός ότι (σύμφωνα με την πρόταση 7.6.27) ισχύει $\mathbf{SD}_n = \langle\mathfrak{a},\mathfrak{b}\rangle$ με $\mathrm{ord}(\mathfrak{a}) = \mathrm{ord}(\alpha) = 2$ και $\mathrm{ord}(\mathfrak{b}) = \mathrm{ord}(\beta) = 2^{n-1}$, η αντίστοιχη σχέση μεταξύ των $\mathfrak{a}$ και $\mathfrak{b}$ είναι η $\mathfrak{b}\mathfrak{a} = \mathfrak{a}\mathfrak{b}^{2^{n-2}-1}$. (Μολαταύτα, αξίζει να επισημανθεί ότι η ημιδιεδρική ομάδα $\mathbf{SD}_n$ τάξεως 2^n περιέχει την $\langle\mathfrak{a},\mathfrak{b}^2\rangle \cong \mathbf{D}_{2^{n-2}}$ τάξεως 2^{n-1} ως μια μεγιστική ορθόθετη υποομάδα της, καθώς έχουμε $\mathfrak{b}^2\mathfrak{a} = \mathfrak{a}(\mathfrak{b}^2)^{(2^{n-2}-1)}$.)

[94] Ως γνωστόν, $\mathrm{Aut}(G) \cong \mathrm{Aut}(\mathbb{Z}_{2^{n-1}}) \underset{2.4.32\,\text{(ii)}}{\cong} \mathbb{Z}_{2^{n-1}}^\times$ (που είναι $\underset{7.3.12}{\cong} \mathbb{Z}_2\oplus\mathbb{Z}_{2^{n-3}}$ αφού $n\geq 4$).

[95] Επειδή η συνήθης ένθεση $\iota : \langle\vartheta\rangle \hookrightarrow \mathrm{Aut}(G)$ είναι *μη τετριμμένος* ομομορφισμός, τούτο έπεται από την πρόταση 7.6.4 και το πόρισμα 7.6.5.

Εν συνεχεία, παρατηρούμε ότι $\mathrm{ord}(\mathfrak{a}) = 2$ (καθόσον $\mathfrak{a} \neq (e_G, \mathrm{id}_G)$, $\mathfrak{a}^2 = (e_G, \mathrm{id}_G)$) και

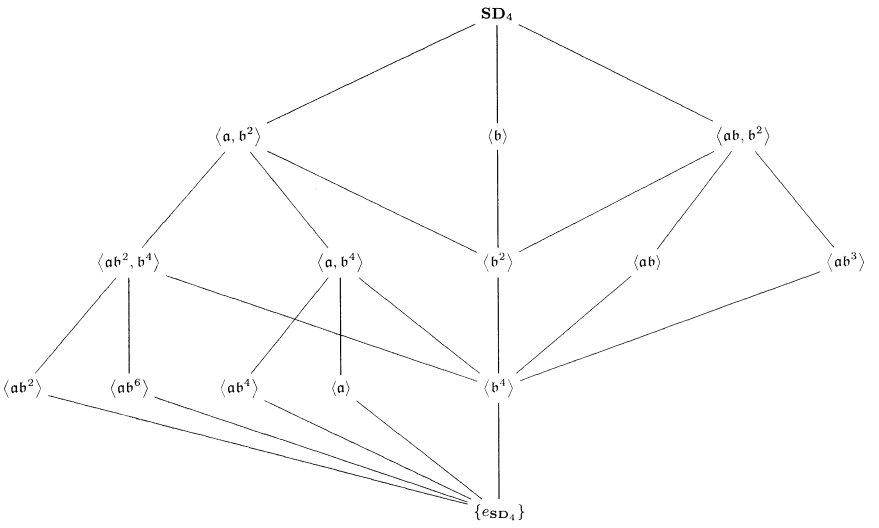
$$\mathfrak{b}^{2^{n-1}} = (g^{2^{n-1}-1}, \mathrm{id}_G)^{2^{n-1}} = (g^{(2^{n-1}-1)2^{n-1}}, \mathrm{id}_G) = (e_G, \mathrm{id}_G),$$

ενώ $\mathfrak{b}^j = (g^{(2^{n-1}-1)j}, \mathrm{id}_G) \neq (e_G, \mathrm{id}_G)$, $\forall j \in \{1, ..., 2^{n-1}-1\}$. Άρα $\mathrm{ord}(\mathfrak{b}) = 2^{n-1}$. Τέλος,

$$\begin{aligned}\mathfrak{a}\mathfrak{b}^{2^{n-2}-1} &= (e_G, \vartheta) \cdot (g^{2^{n-1}-1}, \mathrm{id}_G)^{2^{n-2}-1} = (e_G, \vartheta) \cdot (g^{\left(2^{n-1}-1\right)\left(2^{n-2}-1\right)}, \mathrm{id}_G) \\ &= (\vartheta(g^{\left(2^{n-1}-1\right)\left(2^{n-2}-1\right)}), \vartheta) = (g^{\left(2^{n-1}-1\right)\left(2^{n-2}-1\right)^2}, \vartheta) = (g^{-1}, \vartheta) = (g^{2^{n-1}-1}, \vartheta) \\ &= (g^{2^{n-1}-1}\mathrm{id}_G(e_G), \vartheta) = (g^{2^{n-1}-1}, \mathrm{id}_G) \cdot (e_G, \vartheta) = (g^{-1}, \mathrm{id}_G) \cdot (e_G, \vartheta) = \mathfrak{b}\mathfrak{a},\end{aligned}$$

διότι $\left(2^{n-1}-1\right)\left(2^{n-2}-1\right)^2 \equiv -\left(2^{n-2}-1\right)^2 (\mathrm{mod}\, 2^{n-1}) \equiv -1 (\mathrm{mod}\, 2^{n-1})$. □

7.6.28 Παράδειγμα. Το διάγραμμα τού Hasse για τον σύνδεσμο $(\mathbf{SD}_4, \sqsubseteq)$ (όπου $\mathbf{SD}_4 = \langle \mathfrak{a}, \mathfrak{b} \rangle$ τάξεως 16) είναι το



και

$$\begin{array}{ccccc} & \langle \mathfrak{a}, \mathfrak{b}^2 \rangle \cong \mathbf{D}_4, & \langle \mathfrak{b} \rangle \cong \mathbb{Z}_8, & \langle \mathfrak{a}\mathfrak{b}, \mathfrak{b}^2 \rangle \cong \mathbf{Q}, & \\ \langle \mathfrak{a}\mathfrak{b}^2, \mathfrak{b}^4 \rangle \cong \mathbf{V}, & \langle \mathfrak{a}, \mathfrak{b}^4 \rangle \cong \mathbf{V}, & \langle \mathfrak{b}^2 \rangle \cong \mathbb{Z}_4, & \langle \mathfrak{a}\mathfrak{b} \rangle \cong \mathbb{Z}_4, & \langle \mathfrak{a}\mathfrak{b}^3 \rangle \cong \mathbb{Z}_4, \\ \langle \mathfrak{a}\mathfrak{b}^2 \rangle \cong \mathbb{Z}_2, & \langle \mathfrak{a}\mathfrak{b}^6 \rangle \cong \mathbb{Z}_2, & \langle \mathfrak{a}\mathfrak{b}^4 \rangle \cong \mathbb{Z}_2, & \langle \mathfrak{a} \rangle \cong \mathbb{Z}_2, & \langle \mathfrak{b}^4 \rangle \cong \mathbb{Z}_2. \end{array}$$

7.6.29 Ορισμός. Έστω $m \in \mathbb{N}$, $m \geq 2$. Ορίζουμε ως (m-οστή) **δικυκλική ομάδα** την πηλικοομάδα

$$\boxed{\mathbf{Dic}_m := \quad (\mathbb{Z}_{2m} \rtimes_\varphi \mathbb{Z}_4) / \langle ([m]_{2m}, [2]_4) \rangle}$$

τη δημιουργούμενη από το εξωτερικό ημιευθύ γινόμενο των κυκλικών ομάδων $(\mathbb{Z}_{2m},+)$ και $(\mathbb{Z}_4,+)$ (ύστερα από «διαίρεσή» του διά τής κυκλικής ορθόθετης[96] υποομάδας του που παράγεται από το στοιχείο $([m]_{2m},[2]_4)$), όπου

$$\varphi:\mathbb{Z}_4\longrightarrow \mathbf{Aut}(\mathbb{Z}_{2m})\cong\mathbb{Z}_{2m}^{\times},\ [j]_4\longmapsto\varphi_{[j]_4},$$

είναι ο ομομορφισμός ο απεικονίζων την κλάση ισοτιμίας $[j]_4$ οιουδήποτε $j\in\mathbb{Z}$ στον αυτομορφισμό

$$\varphi_{[j]_4}:\mathbb{Z}_{2m}\longrightarrow\mathbb{Z}_{2m},\ [k]_{2m}\longmapsto\varphi_{[j]_4}([k]_{2m}):=\left[(-1)^jk\right]_{2m},\ \forall k\in\mathbb{Z}. \tag{7.86}$$

Η εσωτερική πράξη επί τής $\mathbb{Z}_{2m}\rtimes_{\varphi}\mathbb{Z}_4$ είναι η

$$([k_1]_{2m},[j_1]_4)\cdot([k_2]_{2m},[j_2]_4):=(\left[k_1+(-1)^{j_1}k_2\right]_{2m},[j_1+j_2]_4)$$

και $([k]_{2m},[j]_4)^{-1}=(\left[(-1)^{j+1}k\right]_{2m},[-j]_4)$ για οιουσδήποτε $k_1,k_2,k,j_1,j_2,j\in\mathbb{Z}$. (Η (7.86) είναι *καλώς ορισμένη* απεικόνιση, διότι για οιουσδήποτε $j,j'\in\mathbb{Z}$ με $[j]_4=[j']_4$ και οιουσδήποτε $k,k'\in\mathbb{Z}$ με $[k]_{2m}=[k']_{2m}$ έχουμε

$$\left.\begin{array}{r}[j]_4=[j']_4\Rightarrow 4\mid j-j'\\ \mathrm{ord}([-1]_{2m})=2\ (\text{εντός τής }\mathbb{Z}_{2m}^{\times})\end{array}\right\}\underset{2.3.8}{\Longrightarrow}[-1]_{2m}^{j-j'}=[1]_{2m}\Rightarrow[(-1)^j]_{2m}=[(-1)^{j'}]_{2m},$$

οπότε

$$[(-1)^jk]_{2m}=[(-1)^j]_{2m}\,[k]_{2m}=[(-1)^{j'}]_{2m}\,[k]_{2m}=[(-1)^{j'}]_{2m}\,[k']_{2m}=[(-1)^{j'}k]_{2m}.$$

Η $\varphi_{[j]_4}$ είναι ένας ενδομορφισμός τής $\mathbb{Z}_{2m}$, καθότι για $k,j,j'\in\mathbb{Z}$ έχουμε

$$(\varphi_{[j]_4}\circ\varphi_{[j']_4})([k]_{2m})=\varphi_{[j]_4}([(-1)^{j'}k]_{2m})=[(-1)^{j+j'}k]_{2m}=\varphi_{[j]_4+[j']_4}([k]_{2m}).$$

Εξάλλου,

$$\left.\begin{array}{r}\mathbf{Ker}(\varphi_{[j]_4})=\left\{[k]_{2m}\in\mathbb{Z}_{2m}\,\middle|\,\left[(-1)^jk\right]_{2m}=[0]_{2m}\right\}\\ \left[(-1)^j\right]_{2m}\neq[0]_{2m}\end{array}\right\}\Rightarrow\mathbf{Ker}(\varphi_{[j]_4})=\{[0]_{2m}\}.$$

Η $\varphi_{[j]_4}$ είναι ενριπτική και, κατ' επέκταση, αμφιριπτική, οπότε $\varphi_{[j]_4}\in\mathbf{Aut}(\mathbb{Z}_{2m})$.) Η $\mathbf{Dic}_m$ έχει τάξη $|\mathbf{Dic}_m|=4m$ (διότι $|\langle([m]_{2m},[2]_4)\rangle|=2$). Στην ειδική περίπτωση όπου $m=2^{n-2}$, για κάποιον $n\in\mathbb{N}$, $n\geq 3$, η δικυκλική ομάδα

$$\boxed{\mathbf{Q}_n:=\mathbf{Dic}_{2^{n-2}}}$$

(τάξεως $|\mathbf{Q}_n|=2^n$) καλείται, ιδιαιτέρως, (n-οστή) **γενικευμένη ομάδα τετρανίων**.

[96] Επειδή $([m]_{2m},[2]_4)\in Z(\mathbb{Z}_{2m}\rtimes_{\varphi}\mathbb{Z}_4)=\langle[m]_{2m}\rangle\oplus\langle[2]_4\rangle$, έχουμε

$$\langle([m]_{2m},[2]_4)\rangle\sqsubseteq Z(\mathbb{Z}_{2m}\rtimes_{\varphi}\mathbb{Z}_4)\underset{5.4.19\,\text{(i)}}{\Longrightarrow}\langle([m]_{2m},[2]_4)\rangle\trianglelefteq\mathbb{Z}_{2m}\rtimes_{\varphi}\mathbb{Z}_4.$$

7.6.30 Πρόταση. *Εάν* $\mathfrak{x} := ([0]_{2m}, [1]_4) \cdot (\mathbb{Z}_{2m} \rtimes_\varphi \mathbb{Z}_4)$ *και* $\mathfrak{y} := ([-1]_{2m}, [0]_4) \cdot (\mathbb{Z}_{2m} \rtimes_\varphi \mathbb{Z}_4)$, *τότε λαμβάνουμε*

$$\mathbf{Dic}_m = \langle \mathfrak{x}, \mathfrak{y} \rangle, \text{ όπου } \operatorname{ord}(\mathfrak{x}) = 4, \operatorname{ord}(\mathfrak{y}) = 2m \text{ και } \mathfrak{y}^m = \mathfrak{x}^2, \ \mathfrak{y}\mathfrak{x} = \mathfrak{x}\mathfrak{y}^{-1}.$$

ΑΠΟΔΕΙΞΗ. Επειδή $\langle ([-1]_{2m}, [0]_4) \rangle = \overline{\mathbb{Z}_{2m}}$ και $\langle ([0]_{2m}, [1]_4) \rangle = \overline{\mathbb{Z}_4}$, το δισύνολο $\{\mathfrak{x}, \mathfrak{y}\}$ παράγει την $\mathbf{Dic}_m$. Εξάλλου, από τις ισότητες

$$\begin{aligned}
&([-1]_{2m}, [0]_4) \cdot ([0]_{2m}, [1]_4) = ([-1 + (-1)^0 0]_{2m}, [1]_4) = ([-1]_{2m}, [1]_4) \\
&([0]_{2m}, [1]_4) \cdot ([-1]_{2m}, [0]_4)^{-1} = ([0]_{2m}, [1]_4) \cdot ([1]_{2m}, [0]_4) = ([-1]_{2m}, [1]_4) \\
&([-1]_{2m}, [1]_4) \cdot ([-1]_{2m}, [1]_4)^{-1} = ([0]_{2m}, [0]_4) \in \langle ([m]_{2m}, [2]_4) \rangle
\end{aligned}$$

έπεται ότι $\mathfrak{y}\mathfrak{x} = \mathfrak{x}\mathfrak{y}^{-1}$. Εν συνεχεία, παρατηρούμε ότι για κάθε $\nu \in \mathbb{Z}$ ισχύει

$$([0]_{2m}, [1]_4)^\nu = ([0]_{2m}, [\nu]_4) \text{ και } ([-1]_{2m}, [0]_4)^\nu = ([-\nu]_{2m}, [0]_4).$$

Επομένως, $\operatorname{ord}(\mathfrak{x}) = 4$, $\operatorname{ord}(\mathfrak{y}) = 2m$ και

$$\begin{aligned}
&([-1]_{2m}, [0]_4)^m \cdot ([0]_{2m}, [1]_4)^{-2} = ([m]_{2m}, [0]_4) \cdot ([0]_{2m}, [2]_4) \\
&= ([m]_{2m}, [2]_4) \in \langle ([m]_{2m}, [2]_4) \rangle \Rightarrow \mathfrak{y}^m = \mathfrak{x}^2.
\end{aligned}$$

Σημειωτέον ότι

$$\begin{aligned}
\mathbf{Dic}_m = \langle \mathfrak{x}, \mathfrak{y} \rangle &= \left\{ \mathfrak{y}^{-\lambda} \mathfrak{x}^\kappa \,|\kappa \in \{0,1\}, \ \lambda \in \{0,1,...,2m-1\} \right\} \\
&= \left\{ \mathfrak{x}^\kappa \mathfrak{y}^{(-1)^{\kappa+1}\lambda} \,|\kappa \in \{0,1\}, \ \lambda \in \{0,1,...,2m-1\} \right\},
\end{aligned}$$

διότι

$$([k]_{2m}, [j]_4) = ([-1]_{2m}, [0]_4)^{-k} \cdot ([0]_{2m}, [1]_4)^j = ([0]_{2m}, [1]_4)^j \cdot ([-1]_{2m}, [0]_4)^{(-1)^{j+1}k}$$

για κάθε ζεύγος $(k, j) \in \mathbb{Z} \times \mathbb{Z}$. □

7.6.31 Σημείωση. Επειδή $\operatorname{ord}(\mathfrak{y}) = 2m \geq 4 > 2$, έχουμε $\mathfrak{y}\mathfrak{x} = \mathfrak{x}\mathfrak{y}^{-1} \neq \mathfrak{x}\mathfrak{y}$, απ' όπου έπεται ότι η $\mathbf{Dic}_m$ δεν είναι αβελιανή.

7.6.32 Πρόταση. $Z(\mathbf{Dic}_m) = \{e_{\mathbf{Dic}_m}, \mathfrak{y}^m\}$ *και* $\mathbf{Dic}_m / Z(\mathbf{Dic}_m) \cong \mathbf{D}_m$.

ΑΠΟΔΕΙΞΗ. Επειδή $\mathfrak{y}^m = \mathfrak{x}^2$, το $\mathfrak{y}^m$ μετατίθεται αμοιβαίως με αμφότερους τους γεννήτορες $\mathfrak{x}$ και $\mathfrak{y}$ τής $\mathbf{Dic}_m$ και, κατ' επέκταση, με όλα τα στοιχεία τής $\mathbf{Dic}_m$. Άρα $\mathfrak{y}^m = \mathfrak{x}^2 \in Z(\mathbf{Dic}_m)$. Έστω τώρα τυχούσα δύναμη $\mathfrak{y}^\nu$ τού $\mathfrak{y}$ ($\nu \in \mathbb{Z}$) ανήκουσα στο $Z(\mathbf{Dic}_m)$. Επειδή

$$\mathfrak{y} = \mathfrak{x}\mathfrak{y}^{-1}\mathfrak{x}^{-1} \Rightarrow \mathfrak{y}^\nu = \left(\mathfrak{x}\mathfrak{y}^{-1}\mathfrak{x}^{-1}\right)^\nu = \mathfrak{x}\mathfrak{y}^{-\nu}\mathfrak{x}^{-1} \tag{7.87}$$

και (ταυτοχρόνως) $\mathfrak{y}^\nu \in Z(\mathbf{Dic}_m) \Rightarrow \mathfrak{x}\mathfrak{y}^\nu = \mathfrak{y}^\nu\mathfrak{x} \Rightarrow \mathfrak{x}\mathfrak{y}^\nu\mathfrak{x}^{-1} = \mathfrak{y}^\nu \underset{(7.87)}{=} \mathfrak{x}\mathfrak{y}^{-\nu}\mathfrak{x}^{-1}$, λαμβάνουμε $\mathfrak{y}^\nu = \mathfrak{y}^{-\nu} \Rightarrow \mathfrak{y}^{2\nu} = e_{\mathbf{Dic}_m} \Longrightarrow 2m \mid 2\nu \Rightarrow m \mid \nu$, οπότε ο ν οφείλει να είναι κάποιο πολλαπλάσιο τού m. (Αυτό σημαίνει ότι $\mathfrak{y}^\nu \in \{e_{\mathbf{Dic}_m}, \mathfrak{y}^m\}$.) Από

την άλλη μεριά, κανένα από τα υπολειπόμενα $2m$ στοιχεία τής $\mathbf{Dic}_m$ δεν ανήκει στο κέντρο της. Πράγματι· υποθέτοντας ότι $\exists \nu \in \mathbb{Z} : \mathfrak{y}^\nu \mathfrak{x} \in Z(\mathbf{Dic}_m)$, θα έπρεπε να ισχύει $\mathfrak{y}\left(\mathfrak{y}^\nu \mathfrak{x}\right)\mathfrak{y}^{-1} = \mathfrak{y}^\nu \mathfrak{x}$. Ωστόσο, $\mathfrak{x}^2 \neq e_{\mathbf{Dic}_m}$ και

$$\mathfrak{y}\left(\mathfrak{y}^\nu \mathfrak{x}\right)\mathfrak{y}^{-1} = \mathfrak{y}^{\nu+1}(\mathfrak{x}\mathfrak{y}^{-1}) = \mathfrak{y}^{\nu+1}(\mathfrak{y}\mathfrak{x}) = \mathfrak{y}^{\nu+2}\mathfrak{x} \neq \mathfrak{y}^\nu \mathfrak{x}.$$

Τελικώς λοιπόν, $Z(\mathbf{Dic}_m) = \{e_{\mathbf{Dic}_m}, \mathfrak{y}^m\}$. Επιπροσθέτως,

$$\mathbf{Dic}_m = \langle \mathfrak{x}, \mathfrak{y} \rangle \underset{4.4.18}{\Longrightarrow} \mathbf{Dic}_m / Z(\mathbf{Dic}_m) = \langle \mathfrak{x} \cdot Z(\mathbf{Dic}_m), \mathfrak{y} \cdot Z(\mathbf{Dic}_m) \rangle$$

και $\mathfrak{x} \notin Z(\mathbf{Dic}_m)$, $\mathfrak{x}^2 \in Z(\mathbf{Dic}_m) \Rightarrow (\mathfrak{x} \cdot Z(\mathbf{Dic}_m))^2 = \mathfrak{x}^2 \cdot Z(\mathbf{Dic}_m) = Z(\mathbf{Dic}_m)$,

$$\begin{aligned} &\mathfrak{y}\mathfrak{x}\left(\mathfrak{x}\mathfrak{y}^{-1}\right)^{-1} = e_{\mathbf{Dic}_m} \in Z(\mathbf{Dic}_m) \Rightarrow (\mathfrak{y}\mathfrak{x} \cdot Z(\mathbf{Dic}_m)) = \left(\mathfrak{x}\mathfrak{y}^{-1} \cdot Z(\mathbf{Dic}_m)\right) \\ &\Rightarrow (\mathfrak{y} \cdot Z(\mathbf{Dic}_m))\,(\mathfrak{x} \cdot Z(\mathbf{Dic}_m)) = (\mathfrak{x} \cdot Z(\mathbf{Dic}_m))\,(\mathfrak{y} \cdot Z(\mathbf{Dic}_m))^{-1}, \end{aligned}$$

ενώ $\exists \nu \in \mathbb{Z} : \mathfrak{y}^\nu \in Z(\mathbf{Dic}_m) \Leftrightarrow m \mid \nu$, οπότε η τάξη τής πλευρικής κλάσεως $\mathfrak{y} \cdot Z(\mathbf{Dic}_m)$ ισούται με m. Εφαρμόζοντας την πρόταση 3.4.7 διαπιστώνουμε ότι η $\mathbf{Dic}_m / Z(\mathbf{Dic}_m)$ είναι ισόμορφη με τη διεδρική ομάδα $\mathbf{D}_m$ (τάξεως $2m$). □

7.6.33 Πρόταση. *Έστω $m \in \mathbb{N}$, $m \geq 2$. Εάν $G = \langle \mathfrak{s}, \mathfrak{t} \rangle$ είναι μια ομάδα παραγόμενη από δύο στοιχεία της $\mathfrak{s}$ και $\mathfrak{t}$, για τα οποία ισχύουν οι σχέσεις*[97]

$$\mathfrak{s}^4 = \mathfrak{t}^{2m} = e_G,\ \mathfrak{t}^m = \mathfrak{s}^2 \text{ και } \mathfrak{t}\mathfrak{s} = \mathfrak{s}\mathfrak{t}^{-1}, \tag{7.88}$$

τότε υφίσταται ένας και μόνον ομομορφισμός ομάδων $\bar{f} : \mathbf{Dic}_m \longrightarrow G$ με $\bar{f}(\mathfrak{x}) = \mathfrak{s}$ και $\bar{f}(\mathfrak{y}) = \mathfrak{t}$. Αυτός είναι κατ' ανάγκην επιμορφισμός. Μάλιστα, στην περίπτωση όπου $|G| = 4m$, ο $\bar{f}$ είναι ισομορφισμός.

ΑΠΟΔΕΙΞΗ. Εάν υπάρχει ομομορφισμός $\bar{f} : \mathbf{Dic}_m \longrightarrow G$ με $\bar{f}(\mathfrak{x}) = \mathfrak{s}$ και $\bar{f}(\mathfrak{y}) = \mathfrak{t}$, τότε αυτός είναι πλήρως καθορισμένος (και, ως εκ τούτου, ο μοναδικός ομομορφισμός με αυτήν την ιδιότητα), καθώς $\mathbf{Dic}_m = \langle \mathfrak{x}, \mathfrak{y} \rangle$. (Βλ. 2.4.9.) Θεωρούμε την

$$f : \mathbb{Z}_{2m} \rtimes_\varphi \mathbb{Z}_4 \longrightarrow G,\ f([k]_{2m}, [j]_4) := \mathfrak{t}^{-k}\mathfrak{s}^j = \mathfrak{s}^j \mathfrak{t}^{(-1)^{j+1}k},\ \forall (k, j) \in \mathbb{Z} \times \mathbb{Z}.$$

Αυτή είναι *καλώς ορισμένη* απεικόνιση, διότι $\mathfrak{s}^4 = \mathfrak{t}^{2m} = e_G$. Επίσης, είναι *επιρριπτική*, διότι $G = \langle \mathfrak{s}, \mathfrak{t} \rangle$, $\mathfrak{s} = f([0]_{2m}, [1]_4)$ και $\mathfrak{t} = f([-1]_{2m}, [0]_4)$. Τέλος, η f είναι *και ομομορφισμός*, διότι για οιουσδήποτε $k_1, k_2, j_1, j_2 \in \mathbb{Z}$ έχουμε[98]

$$\begin{aligned} &f(([k_1]_{2m}, [j_1]_4) \cdot ([k_2]_{2m}, [j_2]_4)) = f(\left[k_1 + (-1)^{j_1} k_2\right]_{2m}, [j_1 + j_2]_4) \\ &= \mathfrak{t}^{-(k_1 + (-1)^{j_1} k_2)} \mathfrak{s}^{j_1 + j_2} = \mathfrak{t}^{-k_1} (\mathfrak{s}^{j_1} \mathfrak{t}^{-k_2} \mathfrak{s}^{-j_1}) \mathfrak{s}^{j_1 + j_2} = (\mathfrak{t}^{-k_1} \mathfrak{s}^{j_1})(\mathfrak{t}^{-k_2} \mathfrak{s}^{-j_1} \mathfrak{s}^{j_1 + j_2}) \\ &= (\mathfrak{t}^{-k_1} \mathfrak{s}^{j_1})(\mathfrak{t}^{-k_2} \mathfrak{s}^{j_2}) = f(([k_1]_{2m}, [j_1]_4)) f(([k_2]_{2m}, [j_2]_4)). \end{aligned}$$

[97] Προσοχή! Δεν προαπαιτείται από την G να είναι μη αβελιανή ούτε να έχουμε κατ' ανάγκην $\mathfrak{s} \neq \mathfrak{t}$. Επίσης, οι πρώτες δύο εκ των ισοτήτων (7.88) δεν σημαίνουν απαραιτήτως ότι $\operatorname{ord}(\mathfrak{s}) = 4$ ή/και $\operatorname{ord}(\mathfrak{t}) = 2m$. (Στην G επιτρέπεται να είναι ακόμη και η τετριμμένη, εάν $\mathfrak{s} = \mathfrak{t} = e_G$!) Εδώ κατασκευάζουμε τον ομομορφισμό $\bar{f}$ (δείχνοντας, μάλιστα, ότι είναι και επιμορφισμός). *Μόνον στην περίπτωση* κατά την οποία συμβαίνει να έχουμε $|G| = 4m$, ο $\bar{f}$ καθίσταται ισομορφισμός και η G έχει τις προαναφερθείσες ιδιότητες.

[98] Προφανώς, για κάθε $k \in \mathbb{Z}$ ισχύει $\mathfrak{t} = \mathfrak{s}\mathfrak{t}^{-1}\mathfrak{s}^{-1} \Rightarrow \mathfrak{t}^k = (\mathfrak{s}\mathfrak{t}^{-1}\mathfrak{s}^{-1})^k = \mathfrak{s}\mathfrak{t}^{-k}\mathfrak{s}^{-1}$. Σημειωτέον ότι

$$\mathfrak{s}^2 \mathfrak{t}^{-k} \mathfrak{s}^{-2} = \mathfrak{s}(\mathfrak{s}\mathfrak{t}^{-k}\mathfrak{s}^{-1})\mathfrak{s}^{-1} = \mathfrak{s}\mathfrak{t}^k\mathfrak{s}^{-1} = \mathfrak{t}^{-k} = \mathfrak{t}^{(-1)^{2+1}k}.$$

Γενικότερα, επαγωγικώς αποδεικνύεται ότι $\mathfrak{s}^j \mathfrak{t}^{-k} \mathfrak{s}^{-j} = \mathfrak{t}^{(-1)^{j+1}k}$ για κάθε $j \in \mathbb{Z}$.

Επειδή $f([m]_{2m},[2]_4)=\mathfrak{t}^{-m}\mathfrak{s}^2=(\mathfrak{s}^{-2}\mathfrak{t}^m)^{-1}=(\mathfrak{s}^{-2}\mathfrak{s}^2)^{-1}=e_G^{-1}=e_G$,

$$([m]_{2m},[2]_4)\in \mathrm{Ker}(f)\Rightarrow \langle([m]_{2m},[2]_4)\rangle\subseteq \mathrm{Ker}(f),$$

το θεμελιώδες θεώρημα 4.5.1 περί πηλικοομάδων μάς πληροφορεί ότι υφίσταται ένας και μόνον επιμορφισμός $\bar{f}:\mathbf{Dic}_m\longrightarrow G$, τέτοιος ώστε $f=\bar{f}\circ\pi^{\mathbf{Dic}_m}_{\langle([m]_{2m},[2]_4)\rangle}$. Στην περίπτωση όπου $|G|=4m=|\mathbf{Dic}_m|$, ο πυρήνας τού $\bar{f}$ είναι η τετριμμένη υποομάδα τής $\mathbf{Dic}_m$, οπότε ο $\bar{f}$ είναι *ισομορφισμός*. □

7.6.34 Πόρισμα. $\mathbf{Dic}_m\cong\langle\mathfrak{s},\mathfrak{t}\rangle\sqsubset \mathrm{SU}_2(\mathbb{C})$, *όπου*

$$\mathfrak{s}:=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\ \mathfrak{t}:=\begin{pmatrix}\zeta_{2m}&0\\0&\overline{\zeta_{2m}}\end{pmatrix},\ \zeta_{2m}:=\exp(\tfrac{\pi i}{m}),\ \overline{\zeta_{2m}}:=\exp(\tfrac{-\pi i}{m}).$$

ΑΠΟΔΕΙΞΗ. Μπορεί να ελεγχθεί εύκολα ότι για τους ανωτέρω πίνακες $\mathfrak{s}$ και $\mathfrak{t}$ ισχύουν οι σχέσεις (7.88). Άρα υφίσταται επιμορφισμός $\bar{f}:\mathbf{Dic}_m\longrightarrow\langle\mathfrak{s},\mathfrak{t}\rangle$ με $\bar{f}(\mathfrak{x})=\mathfrak{s}$, $\bar{f}(\mathfrak{y})=\mathfrak{t}$ και $|\langle\mathfrak{s},\mathfrak{t}\rangle|\mid 4m$. Επειδή $\langle\mathfrak{t}\rangle\sqsubset\langle\mathfrak{s},\mathfrak{t}\rangle$ με $|\langle\mathfrak{t}\rangle|=2m$, λαμβάνουμε

$$\left.\begin{array}{c}|\langle\mathfrak{s},\mathfrak{t}\rangle|\mid 4m\\ 2m\mid|\langle\mathfrak{s},\mathfrak{t}\rangle|\\ |\langle\mathfrak{s},\mathfrak{t}\rangle|>2m\end{array}\right\}\Longrightarrow|\langle\mathfrak{s},\mathfrak{t}\rangle|=4m.$$

Κατά συνέπειαν, ο $\bar{f}$ είναι ισομορφισμός. □

7.6.35 Πόρισμα. *Η ομάδα των τετρανίων* $\mathbf{Q}$ (*η ορισθείσα στο εδάφιο* 2.2.11) *είναι ισόμορφη με την* $\mathbf{Q}_3:=\mathbf{Dic}_2$.

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμοσθεί το πόρισμα 7.6.34 για την $\mathbf{Q}:=\langle\mathbf{k},\mathbf{j}\rangle$. □

► **Ομάδες αυτομορφισμών παριστώμενες ως εξωτερικά ημιευθέα γινόμενα.** Το εξωτερικό ημιευθύ γινόμενο δεν χρησιμοποιείται μόνον για την κατασκευή οικογενειών «νέων» ομάδων αλλά και για την (μέχρις ισομορφισμού) περιγραφή τής *ομάδας αυτομορφισμών* κάποιων ομάδων, όπως αυτής των $\mathbf{D}_n$, $\mathbf{L}_{pq}$ και $\mathbf{Dic}_m$, $m\geq 3$.

7.6.36 Θεώρημα. (Ομάδα αυτομορφισμών των διεδρικών ομάδων) *Έστω* $n\in\mathbb{N}$, $n\geq 3$. *Η ομάδα αυτομορφισμών τής* n*-οστής διεδρικής ομάδας* $\mathbf{D}_n=\langle\alpha,\beta\rangle$ (*τής ορισθείσας στο εδάφιο* 3.4.4) *είναι η*

$$\boxed{\mathrm{Aut}(\mathbf{D}_n)=\{\,\vartheta_{k,l}\,|\,(k,l)\in\{0,1,...,n-1\}\times\{1,...,n-1\}\text{ και }\mu\kappa\delta(l,n)=1\}}$$

τάξεως $|\mathrm{Aut}(\mathbf{D}_n)|=n\phi(n)$, *όπου* ϕ *η συνάρτηση φι τού Euler* (βλ. B.4.15) *και*

$$\vartheta_{k,l}(\beta^j):=\beta^{jl},\ \vartheta_{k,l}(\alpha\circ\beta^j):=\alpha\circ\beta^{jl+k},\ \forall j\in\{0,1,...,n-1\}.$$

Επιπροσθέτως,

$$\boxed{\mathrm{Aut}(\mathbf{D}_n)\cong\mathbb{Z}_n\rtimes_\psi\mathbb{Z}_n^\times\cong\left\{\left.\begin{pmatrix}[1]_n&[k]_n\\[0]_n&[l]_n\end{pmatrix}\in\mathbf{GL}_2(\mathbb{Z}_n)\right|\begin{array}{c}k\in\{0,1,...,n-1\},\\ l\in\{1,...,n-1\}\\ \text{με }\mu\kappa\delta(l,n)=1\end{array}\right\},}$$

όπου $\psi : (\mathbb{Z}_n^\times, \cdot) \longrightarrow (\mathrm{Aut}(\mathbb{Z}_n), \circ)\,,\ [\lambda]_n \longmapsto \psi_{[\lambda]_n}$, *είναι ο ομομορφισμός ο απεικονίζων την κλάση ισοτιμίας* $[\lambda]_n$ *οιουδήποτε* $\lambda \in \{\, l \in \{1, ..., n-1\} | \text{μκδ}(l, n) = 1\}$ *στον αυτομορφισμό*

$$\psi_{[\lambda]_n} : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n,\ [k]_n \longmapsto \psi_{[\lambda]_n}([k]_n) := [\lambda]_n[k]_n.$$

Ως εκ τούτου, η εσωτερική πράξη επί τού $\mathbb{Z}_n \rtimes_\psi \mathbb{Z}_n^\times$ *είναι η*

$$(([\kappa]_n, [\lambda]_n), ([k]_n, [l]_n)) \longmapsto ([\kappa]_n + [\lambda]_n[k]_n, [\lambda]_n[l]_n).$$

Εξάλλου, $\mathrm{Aut}(\mathbf{D}_n) \cong \mathbf{D}_n \Leftrightarrow n \in \{3, 4, 6\}$.

ΑΠΟΔΕΙΞΗ. **Βήμα 1ο**. *Οι ανωτέρω ορισθείσες απεικονίσεις* $\vartheta_{k,l} : \mathbf{D}_n \longrightarrow \mathbf{D}_n$ *είναι ενδομορφισμοί*. Πράγματι· στηριζόμενοι στο ότι

$$\mathbf{D}_n = \left\{\, \beta^j \,\middle|\, j \in \{0, 1, ..., n-1\}\right\} \cup \left\{\, \alpha \circ \beta^j \,\middle|\, j \in \{0, 1, ..., n-1\}\right\}$$

ελέγχουμε απευθείας ότι για οιουσδήποτε $i, j \in \{0, 1, ..., n-1\}$ ισχύουν οι ισότητες

$$\begin{aligned}
&\vartheta_{k,l}(\beta^i \circ \beta^j) = \vartheta_{k,l}(\beta^{i+j}) = \beta^{(i+j)l} = \beta^{il} \circ \beta^{jl} = \vartheta_{k,l}(\beta^i) \circ \vartheta_{k,l}(\beta^j),\\
&\vartheta_{k,l}(\beta^i \circ \big(\alpha \circ \beta^j\big)) = \vartheta_{k,l}(\beta^i \circ \big(\alpha \circ \beta^j\big)) = \vartheta_{k,l}(\alpha \circ \beta^{j-i})\\
&= \alpha \circ \beta^{(j-i)l+k} = \beta^{il} \circ (\alpha \circ \beta^{jl+k}) = \vartheta_{k,l}(\beta^i) \circ \vartheta_{k,l}(\alpha \circ \beta^j),\\
&\vartheta_{k,l}(\big(\alpha \circ \beta^i\big) \circ \beta^j) = \vartheta_{k,l}(\big(\alpha \circ \beta^i\big) \circ \beta^j) = \vartheta_{k,l}(\alpha \circ \beta^{i+j})\\
&= \alpha \circ \beta^{(i+j)l+k} = (\alpha \circ \beta^{il+k}) \circ \beta^{jl} = \vartheta_{k,l}(\alpha \circ \beta^i) \circ \vartheta_{k,l}(\beta^j),\\
&\vartheta_{k,l}(\big(\alpha \circ \beta^i\big) \circ \big(\alpha \circ \beta^j\big)) = \vartheta_{k,l}(\alpha \circ (\beta^i \circ \alpha \circ \beta^j)) = \vartheta_{k,l}(\alpha^2 \circ \beta^{j-i})\\
&= \vartheta_{k,l}(\beta^{j-i}) = \beta^{(j-i)l+k} = \alpha^2 \circ \beta^{(j-i)l+k} = \alpha \circ (\beta^{il+k} \circ \alpha \circ \beta^{jl+k})\\
&= (\alpha \circ \beta^{il+k}) \circ (\alpha \circ \beta^{jl+k}) = \vartheta_{k,l}(\alpha \circ \beta^i) \circ \vartheta_{k,l}(\alpha \circ \beta^j).
\end{aligned}$$

Βήμα 2ο. *Οι ενδομορφισμοί* $\vartheta_{k,l} : \mathbf{D}_n \longrightarrow \mathbf{D}_n$ *είναι αυτομορφισμοί*. Κατ' αρχάς, για οιοδήποτε (άλλο) ζεύγος $(\kappa, \lambda) \in \{0, 1, ..., n-1\} \times \{1, ..., n-1\}$ με $\text{μκδ}(\lambda, n) = 1$ έχουμε

$$\begin{aligned}
&\left(\vartheta_{\kappa,\lambda} \circ \vartheta_{k,l}\right)(\beta^j) = \vartheta_{\kappa,\lambda}(\beta^{jl}) = \beta^{j\lambda l} = \vartheta_{k\lambda+\kappa,l\lambda}(\beta^j),\\
&\left(\vartheta_{\kappa,\lambda} \circ \vartheta_{k,l}\right)(\alpha \circ \beta^j) = \vartheta_{\kappa,\lambda}(\alpha \circ \beta^{jl+k}) = \alpha \circ \beta^{(jl+k)\lambda+\kappa}\\
&= \alpha \circ \beta^{j\lambda l+k\lambda+\kappa} = \vartheta_{k\lambda+\kappa,l\lambda}(\alpha \circ \beta^j),
\end{aligned}$$

για κάθε $j \in \{0, 1, ..., n-1\}$. Άρα $\vartheta_{\kappa,\lambda} \circ \vartheta_{k,l} = \vartheta_{k\lambda+\kappa,l\lambda}$. Από την άλλη μεριά,

$$\left.\begin{aligned}
\vartheta_{0,1}(\beta^j) &= \beta^{j\cdot 1} = \beta^j\\
\vartheta_{0,1}(\alpha \circ \beta^j) &= \alpha \circ \beta^{j\cdot 1+0} = \alpha \circ \beta^j\\
\forall j &\in \{0, 1, ..., n-1\}
\end{aligned}\right\} \Longrightarrow \vartheta_{0,1} = \mathrm{id}_{\mathbf{D}_n}.$$

Επειδή $\text{μκδ}(l, n) = 1$, (βάσει τού πορίσματος Β.2.8) υπάρχουν $\widetilde{l}, \widetilde{n} \in \mathbb{Z}$, τέτοιοι ώστε $l\widetilde{l} + n\widetilde{n} = 1$. (Η κλάση ισοτιμίας $[\widetilde{l}]_n$ είναι ίση με το αντίστροφο $[l]_n^{-1}$ τής $[l]_n$ εντός τής ομάδας $\mathbb{Z}_n^\times$. Βλ. απόδειξη τής προτάσεως Β.4.43.) Προφανώς,

$$\vartheta_{-k\widetilde{l},\widetilde{l}} \circ \vartheta_{k,l} = \vartheta_{0,1} = \mathrm{id}_{\mathrm{Aut}(\mathbf{D}_n)} = \vartheta_{k,l} \circ \vartheta_{-k\widetilde{l},\widetilde{l}},$$

οπότε οι $\vartheta_{k,l}$ είναι όντως αυτομορφισμοί (έχοντες τους $\vartheta_{-k\tilde{l},\tilde{l}}$ ως αντιστρόφους τους). Εάν υποθέσουμε ότι δύο εξ αυτών είναι ίσοι, ας πούμε $\vartheta_{k_1,l_1} = \vartheta_{k_2,l_2}$, τότε

$$\vartheta_{k_1,l_1}(\beta) = \vartheta_{k_2,l_2}(\beta) \Rightarrow \beta^{l_1-l_2} = \mathrm{id}_{\mathcal{E}_n} \Longrightarrow l_1 - l_2 \mid n$$
$$\Rightarrow [l_1]_n = [l_2]_n \Rightarrow l_1 = l_2 \text{ (διότι } l_1, l_2 \in \{1, ..., n-1\})$$

και

$$\vartheta_{k_1,l_1}(\alpha \circ \beta) = \vartheta_{k_2,l_2}(\alpha \circ \beta) \Rightarrow \alpha \circ \beta^{l_1+k_1} = \alpha \circ \beta^{l_2+k_2}$$
$$\Longrightarrow \beta^{l_1+k_1} = \beta^{l_2+k_2} \Longrightarrow \beta^{(l_1-l_2)+(k_1-k_2)} = \mathrm{id}_{\mathcal{E}_n} \underset{l_1-l_2 \mid n}{\Longrightarrow} \beta^{k_1-k_2} = \mathrm{id}_{\mathcal{E}_n}$$
$$\Longrightarrow k_1 - k_2 \mid n \Rightarrow [k_1]_n = [k_2]_n \Rightarrow k_1 = k_2 \text{ (διότι } k_1, k_2 \in \{0, 1, ..., n-1\}).$$

Συμπεραίνουμε λοιπόν ότι

$$\vartheta_{k_1,l_1} = \vartheta_{k_2,l_2} \Longleftrightarrow [l_1 = l_2 \text{ και } k_1 = k_2]. \tag{7.89}$$

Αυτό σημαίνει ότι το υποσύνολο αυτών των αυτομορφισμών τής $\mathbf{D}_n$ αποτελεί μία υποομάδα τής $\mathrm{Aut}(\mathbf{D}_n)$ τάξεως $n\phi(n)$. Κατά συνέπειαν, $n\phi(n) \leq |\mathrm{Aut}(\mathbf{D}_n)|$.

Βήμα 3ο. *Κάθε αυτομορφισμός τής $\mathbf{D}_n$ είναι τής ανωτέρω μορφής* (*και, ως εκ τούτου,* $|\mathrm{Aut}(\mathbf{D}_n)| = n\phi(n)$). Έστω *τυχών* αυτομορφισμός $\vartheta \in \mathrm{Aut}(\mathbf{D}_n)$. Επειδή $\langle\beta\rangle \sqsubset_{\chi\alpha\varrho.} \mathbf{D}_n$ (βλ. 6.1.4), έχουμε $\vartheta(\langle\beta\rangle) = \langle\beta\rangle$, οπότε η εικόνα $\vartheta(\beta)$ τού στοιχείου β μέσω τού ϑ είναι μια δύναμη $\vartheta(\beta) = \beta^l$ τού β για κάποιον $l \in \{0, 1, ..., n-1\}$. Το β^l απεικονίζεται μέσω τού αντιστρόφου ϑ^{-1} τού ϑ στο στοιχείο β, οπότε από το πόρισμα 2.3.11 και το (iv) τής προτάσεως 2.4.19 λαμβάνουμε

$$\frac{n}{\mu\kappa\delta(l,n)} = \mathrm{ord}(\beta^l) = \mathrm{ord}(\vartheta^{-1}(\beta^l)) = \mathrm{ord}(\beta) = n,$$

απ' όπου έπεται ότι $\mu\kappa\delta(l,n) = 1$. Από την άλλη μεριά, $\vartheta(\alpha) \notin \langle\beta\rangle$ (διότι αλλιώς το α θα ήταν η εικόνα κάποιας δυνάμεως τού β μέσω τού ϑ^{-1}, ήτοι εκ νέου μια δύναμη τού β, πράγμα αδύνατο). Άρα υπάρχει κατ' ανάγκην κάποιος $k \in \{0, 1, ..., n-1\}$, τέτοιος ώστε να ισχύει $\vartheta(\alpha) = \alpha \circ \beta^k$. Για τους άνωθι (μονοσημάντως ορισμένους) k και l ισχύει η ισότητα $\vartheta = \vartheta_{k,l}$, αφού

$$\left\{ \begin{array}{l} \vartheta(\beta^j) = \vartheta(\beta)^j = \beta^{jl} = \vartheta_{k,l}(\beta^j), \\ \vartheta(\alpha \circ \beta^j) = \vartheta(\alpha) \circ \vartheta(\beta)^j = (\alpha \circ \beta^k) \circ \beta^{jl} \\ = \alpha \circ \beta^{jl+k} = \vartheta_{k,l}(\alpha \circ \beta^j),\ \forall j \in \{0, 1, ..., n-1\}. \end{array} \right\}$$

Βήμα 4ο. Η απεικόνιση

$$\psi_{[\lambda]_n} : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n,\ [k]_n \longmapsto \psi_{[\lambda]_n}([k]_n) := [\lambda]_n[k]_n$$

είναι ενδομορφισμός τής $\mathbb{Z}_n$, διότι

$$\begin{array}{rcl} \psi_{[\lambda]_n}([k]_n + [l]_n) & = & [\lambda]_n([k]_n + [l]_n) \\ & = & [\lambda]_n[k]_n + [\lambda]_n[l]_n = \psi_{[\lambda]_n}([k]_n) + \psi_{[\lambda]_n}([l]_n) \end{array}$$

για οιεσδήποτε κλάσεις ισοτιμίας $[k]_n, [l]_n \in \mathbb{Z}_n$. Επειδή $[\lambda]_n \in \mathbb{Z}_n^\times$, ο ενδομορφισμός $\psi_{[\lambda]_n}$ τής *πεπερασμένης* ομάδας $\mathbb{Z}_n$ είναι αυτομορφισμός της, διότι

$$\mathbf{Ker}(\psi_{[\lambda]_n}) = \{\, [k]_n \in \mathbb{Z}_n |\, [\lambda]_n[k]_n = [0]_n\} = \{[0]_n\}.$$

(Προφανώς,

$$[\lambda]_n[k]_n = [\lambda k]_n = [0]_n \Rightarrow \lambda k \mid n \Rightarrow k \mid n \Rightarrow [k]_n = [0]_n,$$

διότι μκδ$(\lambda, n) = 1$. Βλ. πόρισμα Β.2.9.) Εν συνεχεία, παρατηρούμε ότι η

$$\psi : \left(\mathbb{Z}_n^\times, \cdot\right) \longrightarrow (\mathbf{Aut}(\mathbb{Z}_n), \circ)\,,\ [\lambda]_n \longmapsto \psi_{[\lambda]_n},$$

είναι καλώς ορισμένη απεικόνιση, διότι εάν ισχύει $[\lambda_1]_n = [\lambda_2]_n$, τότε

$$\psi_{[\lambda_1]_n}([k]_n) := [\lambda_1]_n[k]_n = [\lambda_2]_n[k]_n =: \psi_{[\lambda_2]_n}([k]_n)$$

για κάθε κλάση ισοτιμίας $[k]_n \in \mathbb{Z}_n$, ήτοι $\psi_{[\lambda_1]_n} = \psi_{[\lambda_2]_n}$. Επιπροσθέτως, η ψ είναι *και* ομομορφισμός ομάδων, αφού

$$\psi_{[\lambda_1]_n[\lambda_2]_n} = \psi_{[\lambda_1]_n} \circ \psi_{[\lambda_2]_n},\ \forall\, (\lambda_1, \lambda_2) \in \mathbb{Z} \times \mathbb{Z}.$$

Εκ των προαναφερθέντων συνάγεται ότι *ορίζεται* το εξωτερικό ημιευθύ γινόμενο $\mathbb{Z}_n \rtimes_\psi \mathbb{Z}_n^\times$ των $\mathbb{Z}_n$ και $\mathbb{Z}_n^\times$ μέσω τού ψ.

Βήμα 5ο. Θεωρούμε την απεικόνιση[99]

$$f : \mathbf{Aut}(\mathbf{D}_n) \longrightarrow \mathbb{Z}_n \rtimes_\psi \mathbb{Z}_n^\times,\ \vartheta_{k,l} \longmapsto ([k]_n, [l]_n).$$

Αυτή είναι ομομορφισμός, διότι

$$f(\vartheta_{\kappa,\lambda})f(\vartheta_{k,l}) = ([\kappa]_n, [\lambda]_n)([k]_n, [l]_n) = ([\kappa]_n + [\lambda]_n[k]_n, [\lambda]_n[l]_n)$$
$$= ([k\lambda + \kappa]_n, [l\lambda]_n) = f(\vartheta_{k\lambda+\kappa,l\lambda}) = f(\vartheta_{\kappa,\lambda} \circ \vartheta_{k,l}).$$

Επειδή

$$\mathbf{Ker}(f) = \{\, \vartheta_{k,l} \in \mathbf{Aut}(\mathbf{D}_n) |\, f(\vartheta_{k,l}) = ([0]_n, [1]_n)\}$$
$$= \{\, \vartheta_{k,l} \in \mathbf{Aut}(\mathbf{D}_n) |\, ([k]_n, [l]_n) = ([0]_n, [1]_n)\} = \{\vartheta_{0,1}\} = \{\mathrm{id}_{\mathbf{D}_n}\}$$

και $|\mathbf{Aut}(\mathbf{D}_n)| = |\mathbb{Z}_n \rtimes_\psi \mathbb{Z}_n^\times|$, ο ομομορφισμός f είναι ισομορφισμός. Ο δεύτερος ισομορφισμός είναι ο

$$\mathbb{Z}_n \rtimes_\psi \mathbb{Z}_n^\times \ni ([k]_n, [l]_n) \longmapsto \begin{pmatrix} [1]_n & [k]_n \\ [0]_n & [l]_n \end{pmatrix}.$$

Βήμα 6ο. Εάν υφίστατο ισομορφισμός $\mathbf{Aut}(\mathbf{D}_n) \cong \mathbf{D}_n$, τότε θα έπρεπε να ισχύει

$$n\phi\,(n) = 2n \Longrightarrow \phi\,(n) = 2 \underset{\text{B.4.27}}{\Longrightarrow} n \in \{3, 4, 6\}.$$

[99] Το ότι η f είναι *καλώς ορισμένη* απεικόνιση έπεται από τη συνεπαγωγή "$\Rightarrow$" στην (7.89).

Ερώτημα: Υφίσταται όντως ένας τέτοιος ισομορφισμός για αυτές τις τρεις τιμές τού n; Η απάντηση είναι καταφατική. Στην πραγματικότητα, ισχύει κάτι ισχυρότερο: Ας θεωρήσουμε τους αυτομορφισμούς $\omega_1, \omega_2 \in \mathbf{Aut}(\mathbf{D}_n)$ τους οριζόμενους επί των γεννητόρων α, β τής $\mathbf{D}_n$ ως εξής:

$$\omega_1(\alpha) := \beta \circ \alpha = \alpha \circ \beta^{-1},\ \omega_1(\beta) := \beta,\ \omega_2(\alpha) := \alpha,\ \omega_2(\beta) := \beta^{-1}.$$

Για τον πρώτο εξ αυτών έχουμε

$$\omega_1(\beta^j) = \omega_1(\beta)^j = \beta^j,\ \omega_1(\alpha \circ \beta^j) = \omega_1(\alpha) \circ \omega_1(\beta^j) = \alpha \circ \beta^{-1} \circ \beta^j = \alpha \circ \beta^{j-1},$$
$$\omega_1^\nu(\beta^j) = \beta^j,\ \omega_1^\nu(\alpha \circ \beta^j) = \omega_1^{\nu-1}(\alpha \circ \beta^{j-1}) = \cdots = \omega_1^0(\alpha \circ \beta^{j-\nu}) = \alpha \circ \beta^{j-\nu}$$

για κάθε $j \in \{0, 1, ..., n-1\}$ και $\nu \in \{1, ..., n\}$, και για τον δεύτερο

$$\omega_2(\beta^j) = \omega_2(\beta)^j = \beta^{-j},\ \omega_2(\alpha \circ \beta^j) = \omega_2(\alpha) \circ \omega_2(\beta^j) = \alpha \circ \beta^{-j}$$

και $\omega_2^2(\beta^j) = \omega_2((\beta^{-1})^j) = \omega_2(\beta^{-1})^j = ((\beta^{-1})^{-1})^j = \beta^j$,

$$\omega_2^2(\alpha \circ \beta^j) = \omega_2(\alpha \circ (\beta^{-1})^j) = \alpha \circ ((\beta^{-1})^{-1})^j = \alpha \circ \beta^j,\ \forall j \in \{0, 1, ..., n-1\}.$$

Άρα $\omega_1^\nu \neq \mathrm{id}_{\mathbf{D}_n}$ για $\nu \in \{1, ..., n-1\}$ και

$$\omega_1^n = \omega_2^2 = \mathrm{id}_{\mathbf{D}_n}.$$

Έτσι λοιπόν (εντός τής $\mathbf{Aut}(\mathbf{D}_n)$) ο ω_1 έχει τάξη n και ο ω_2 τάξη 2. Επιπλέον, για κάθε $j \in \{0, 1, ..., n-1\}$ ισχύουν οι ισότητες

$$(\omega_1 \circ \omega_2)(\beta^j) = \omega_1(\beta^{-j}) = \omega_1(\beta)^{-j} = \beta^{-j} = \omega_2(\beta^j) = \left(\omega_2 \circ \omega_1^{-1}\right)(\beta^j),$$
$$(\omega_1 \circ \omega_2)(\alpha \circ \beta^j) = \omega_1(\alpha \circ \beta^{-j}) = \omega_1(\alpha) \circ \omega_1(\beta)^{-j} = (\alpha \circ \beta^{-1}) \circ \beta^{-j}$$
$$= \alpha \circ \beta^{-(j+1)} = \omega_2(\alpha) \circ \omega_2(\beta)^{j+1} = \omega_2(\alpha \circ \beta^{j+1}) = \left(\omega_2 \circ \omega_1^{-1}\right)(\alpha \circ \beta^j).$$

Εξ αυτών έπεται ότι $\omega_1 \circ \omega_2 = \omega_2 \circ \omega_1^{-1}$. Εάν θέσουμε

$$H := \langle \omega_1, \omega_2 \rangle \sqsubseteq \mathbf{Aut}(\mathbf{D}_n)$$

και λάβουμε υπ' όψιν ότι

$$(\omega_1 \circ \omega_2)(\alpha) = \omega_1(\alpha) = \beta \circ \alpha \neq \beta^{-1} \circ \alpha = \omega_2(\beta) \circ \omega_2(\alpha) = \omega_2(\beta \circ \alpha) = (\omega_2 \circ \omega_1)(\alpha)$$

(ήτοι ότι η ομάδα H είναι *μη αβελιανή,* αφού $\omega_1 \circ \omega_2 \neq \omega_2 \circ \omega_1$), συμπεραίνουμε ότι $H \cong \mathbf{D}_n$ μέσω τής προτάσεως 3.4.7. Άρα η $\mathbf{Aut}(\mathbf{D}_n)$ περιέχει *πάντοτε* ένα «αντίτυπο» τής $\mathbf{D}_n$ και

$$H = \mathbf{Aut}(\mathbf{D}_n) \Leftrightarrow n\phi(n) = 2n \Leftrightarrow \phi(n) = 2 \Leftrightarrow n \in \{3, 4, 6\}.$$

(Βλ. πρόταση Β.4.27.) □

7.6.37 Παρατήρηση. Μέσω τού θεωρήματος 7.6.36 και των προαναφερθέντων στα εδάφια 5.4.8 και 5.4.30 (ii) καταλήγουμε στον ακόλουθο ολοκληρωμένο κατάλογο:

n	$Z(\mathbf{D}_n)$	$\mathrm{Aut}(\mathbf{D}_n)$	$\mathrm{Inn}(\mathbf{D}_n)$	$\mathrm{Out}(\mathbf{D}_n)$
3	$\{\mathrm{id}_{\mathcal{E}_3}\}$	$\mathbf{D}_3\ (\cong \mathfrak{S}_3)$	$\mathbf{D}_3$	τετριμμένη
4	$\{\mathrm{id}_{\mathcal{E}_4}, \beta^2\}$	$\mathbf{D}_4$	$\mathbf{V}$	$\mathbb{Z}_2$
6	$\{\mathrm{id}_{\mathcal{E}_6}, \beta^3\}$	$\mathbf{D}_6$	$\mathbf{D}_3$	$\mathbb{Z}_2$
περιττός ≥ 5	$\{\mathrm{id}_{\mathcal{E}_n}\}$	$\mathbb{Z}_n \rtimes_\psi \mathbb{Z}_n^\times$	$\mathbf{D}_n$	$(\mathbb{Z}_n \rtimes_\psi \mathbb{Z}_n^\times)/\mathbf{D}_n$
άρτιος ≥ 8	$\{\mathrm{id}_{\mathcal{E}_n}, \beta^{\frac{n}{2}}\}$	$\mathbb{Z}_n \rtimes_\psi \mathbb{Z}_n^\times$	$\mathbf{D}_{\frac{n}{2}}$	$(\mathbb{Z}_n \rtimes_\psi \mathbb{Z}_n^\times)/\mathbf{D}_{\frac{n}{2}}$

7.6.38 Θεώρημα. (Ομάδα αυτομορφισμών των ομάδων $\mathbf{L}_{pq}$) *Έστω ότι p, q είναι πρώτοι αριθμοί με $p < q$ και $q \equiv 1(\mathrm{mod}\, p)$, και έστω*

$$\mathbf{L}_{pq} := \left\{ \begin{pmatrix} [a]_q & [b]_q \\ [0]_q & [1]_q \end{pmatrix} \in \mathbf{GL}_2(\mathbb{Z}_q) \,\middle|\, a, b \in \mathbb{Z} \text{ και } a^p \equiv 1(\mathrm{mod}\, q) \right\}$$

η μοναδική (μέχρις ισομορφισμού) μη αβελιανή ομάδα τάξεως pq. (Βλ. πρόταση 5.7.15). *Ως γνωστόν,*

$$\mathbf{L}_{pq} = \langle t \rangle \langle s \rangle = \left\{ t^i s^j \,\middle|\, (i,j) \in \{0,1,...,q-1\} \times \{0,1,...,p-1\} \right\},$$

όπου

$$s := \begin{pmatrix} [c]_q & [0]_q \\ [0]_q & [1]_q \end{pmatrix},\ t := \begin{pmatrix} [1]_q & [1]_q \\ [0]_q & [1]_q \end{pmatrix},\ sts^{-1} = t^c,$$

(με $\mathrm{ord}(s) = p$, $\mathrm{ord}(t) = q$) και $[c]_q$ μια κλάση ισοτιμίας (ενός $c \in \mathbb{Z}$) έχουσα τάξη p εντός τής $\mathbb{Z}_q^\times$. Η ομάδα αυτομορφισμών τής $\mathbf{L}_{pq}$ έχει τάξη $q(q-1)$ και είναι η

$$\boxed{\mathrm{Aut}(\mathbf{L}_{pq}) = \{\, \vartheta_{k,l} |\, (k,l) \in \{0,1,...,q-1\} \times \{1,...,q-1\}\}\,,}$$

όπου $\vartheta_{k,l}(s) := st^k = t^{ck}s$, $\vartheta_{k,l}(t) := t^l$, και, γενικότερα,

$$\vartheta_{k,l}(t^i s^j) := t^{li}(st^k)^j = t^{li}(t^{ck}s)^j,\ \forall (i,j) \in \{0,1,...,q-1\} \times \{0,1,...,p-1\}.$$

Επιπροσθέτως,

$$\boxed{\mathrm{Aut}(\mathbf{L}_{pq}) \cong \mathbb{Z}_q \rtimes_\psi \mathbb{Z}_q^\times \cong \mathrm{Aut}(\mathbf{D}_q),}$$

όπου $\psi : \left(\mathbb{Z}_q^\times, \cdot\right) \longrightarrow (\mathrm{Aut}(\mathbb{Z}_q), \circ)\,,\ [\lambda]_q \longmapsto \psi_{[\lambda]_q}$, είναι ο ομομορφισμός ο απεικονίζων την κλάση ισοτιμίας $[\lambda]_q$ οιουδήποτε $\lambda \in \{1,...,q-1\}$ στον αυτομορφισμό $\psi_{[\lambda]_q} : \mathbb{Z}_q \longrightarrow \mathbb{Z}_q,\ [k]_q \longmapsto \psi_{[\lambda]_q}([k]_q) := [\lambda]_q[k]_q$.

ΑΠΟΔΕΙΞΗ. **Βήμα 1ο**. *Οι ανωτέρω ορισθείσες απεικονίσεις* $\vartheta_{k,l} : \mathbf{L}_{pq} \longrightarrow \mathbf{L}_{pq}$ *είναι ενδομορφισμοί*. Πράγματι· κάνοντας χρήση μαθηματικής επαγωγής (συνήθους και με οπισθοπορεία, ως προς τον μ και ως προς τον ν) αποδεικνύουμε εν πρώτοις (μέσω τής σχέσεως $sts^{-1} = t^c$) ότι

$$s^\mu t^\nu = t^{c^\mu \nu} s^\mu,\ \forall (\mu, \nu) \in \mathbb{Z} \times \mathbb{Z}. \tag{7.90}$$

Για $(i, j) \in \{0, 1,..., q-1\} \times \{0, 1,..., p-1\}$, $(i', j') \in \{0, 1,..., q-1\} \times \{0, 1,..., p-1\}$ και $(k, l) \in \{0, 1, ..., q-1\} \times \{1, ..., q-1\}$ έχουμε

$$(t^i s^j)(t^{i'} s^{j'}) = t^i (s^j t^{i'}) s^{j'} = t^i (t^{c^j i'} s^j) s^{j'} = t^{i + c^j i'} s^{j+j'} \tag{7.91}$$

και (εξ ορισμού)

$$\vartheta_{k,l}(t^{i+c^j i'} s^{j+j'}) = t^{l(i+c^j i')} (st^k)^{j+j'} = t^{li} ((t^{li'})^{c^j} (st^k)^j)(st^k)^{j'}. \tag{7.92}$$

Εν συνεχεία, αποδεικνύουμε (επαγωγικώς, ως προς τον j) ότι

$$(t^{li'})^{c^j} (st^k)^j = (st^k)^j t^{li'}. \tag{7.93}$$

Η (7.93) είναι αληθής τόσον για $j = 0$ (προδήλως) όσον και για $j = 1$, διότι

$$(t^{li'})^c (st^k) = (t^{li'})^c (t^{ck} s) = t^{c(k+li')} s = st^{k+li'} = (st^k) t^{li'}$$

(λόγω τής (7.90)). Εάν υποθέσουμε ότι η (7.93) είναι αληθής για κάποιον εκθέτη $j \in \{1, ..., p-2\}$, τότε

$$\begin{aligned} (t^{li'})^{c^{j+1}} (st^k)^{j+1} &= ((t^{li'})^{c^j})^c (st^k)^j (st^k) \\ &= ((st^k)^j t^{li'} ((st^k)^j)^{-1})^c (st^k)^j (st^k) \\ &= (st^k)^j (t^{li'})^c ((st^k)^j)^{-1}) (st^k)^j (st^k) \\ &= (st^k)^j (t^{li'})^c (st^k). \end{aligned} \tag{7.94}$$

Επειδή

$$(t^{li'})^c (st^k) = (t^{li'})^c (t^{ck} s) = t^{c(li'+k)} s = st^{li'+k} = (st^k) t^{li'}, \tag{7.95}$$

οι (7.94) και (7.95) δίδουν

$$(t^{li'})^{c^{j+1}} (st^k)^{j+1} = (st^k)^j (t^{li'})^c (st^k) = (st^k)^{j+1} t^{li'},$$

οπότε η (7.93) είναι αληθής *και* για τον $j + 1$. Από τις (7.91), (7.92) και (7.93) προκύπτει ότι

$$\begin{aligned} \vartheta_{k,l}((t^i s^j)(t^{i'} s^{j'})) &= \vartheta_{k,l}(t^{i+c^j i'} s^{j+j'}) = t^{li} ((st^k)^j t^{li'}) (st^k)^{j'} \\ &= (t^{li} (st^k)^j)(t^{li'} (st^k)^{j'}) = \vartheta_{k,l}(t^i s^j) \vartheta_{k,l}(t^{i'} s^{j'}). \end{aligned}$$

Βήμα 2ο. *Οι ενδομορφισμοί* $\mathbf{L}_{pq} \longrightarrow \mathbf{L}_{pq}$ *είναι αυτομορφισμοί*. Κατ' αρχάς, για οιοδήποτε (άλλο) ζεύγος $(\kappa, \lambda) \in \{0, 1, ..., q-1\} \times \{1, ..., q-1\}$ έχουμε

$$(\vartheta_{\kappa,\lambda} \circ \vartheta_{k,l})(t^i s^j) = \vartheta_{\kappa,\lambda}(t^{li} (st^k)^j) = t^{\lambda li} ((st^\kappa) t^{\lambda k})^j = t^{\lambda li} (st^{k\lambda + \kappa})^j = \vartheta_{k\lambda+\kappa, l\lambda}(t^i s^j),$$

για κάθε $(i,j) \in \{0,1,...,q-1\} \times \{0,1,...,p-1\}$. Άρα $\vartheta_{\kappa,\lambda} \circ \vartheta_{k,l} = \vartheta_{k\lambda+\kappa,l\lambda}$. Από την άλλη μεριά, $\vartheta_{0,1} = \mathrm{id}_{\mathbf{L}_{pq}}$. Επειδή μκδ$(l,q) = 1$, υπάρχουν $\widetilde{l}, \widetilde{q} \in \mathbb{Z}$, τέτοιοι ώστε $l\widetilde{l} + q\widetilde{q} = 1$. (Η κλάση ισοτιμίας $[\widetilde{l}]_q$ είναι ίση με το αντίστροφο $[l]_q^{-1}$ τής $[l]_q$ εντός τής ομάδας $\mathbb{Z}_q^\times$.) Προφανώς, $\vartheta_{-k\widetilde{l},\widetilde{l}} \circ \vartheta_{k,l} = \vartheta_{0,1} = \mathrm{id}_{\mathrm{Aut}(\mathbf{L}_{pq})} = \vartheta_{k,l} \circ \vartheta_{-k\widetilde{l},\widetilde{l}}$, οπότε οι $\vartheta_{k,l}$ είναι όντως αυτομορφισμοί (έχοντες τους $\vartheta_{-k\widetilde{l},\widetilde{l}}$ ως αντιστρόφους τους). Εάν υποθέσουμε ότι δύο εξ αυτών είναι ίσοι, ας πούμε $\vartheta_{k_1,l_1} = \vartheta_{k_2,l_2}$, τότε

$$\vartheta_{k_1,l_1}(s) = \vartheta_{k_2,l_2}(s) \Rightarrow st^{k_1} = st^{k_2} \Rightarrow t^{k_1-k_2} = \mathbf{I}_2 \Rightarrow k_1 - k_2 \mid q \Rightarrow k_1 = k_2$$

(διότι $k_1, k_2 \in \{0,1,...,q-1\}$) και

$$\begin{aligned}&\vartheta_{k_1,l_1}(t) = \vartheta_{k_2,l_2}(t) \Rightarrow t^{l_1} = t^{l_2} \Rightarrow t^{l_1-l_2} = \mathbf{I}_2\\ &\Rightarrow l_1 - l_2 \mid q \Rightarrow l_1 = l_2 \text{ (διότι } l_1, l_2 \in \{1,...,q-1\})\end{aligned}$$

Συμπεραίνουμε λοιπόν ότι $\vartheta_{k_1,l_1} = \vartheta_{k_2,l_2} \Longleftrightarrow [l_1 = l_2 \text{ και } k_1 = k_2]$. Αυτό σημαίνει ότι το υποσύνολο αυτών των αυτομορφισμών τής $\mathbf{L}_{pq}$ αποτελεί μια υποομάδα τής $\mathrm{Aut}(\mathbf{L}_{pq})$ τάξεως $q(q-1)$. Κατά συνέπειαν, $q(q-1) \leq |\mathrm{Aut}(\mathbf{L}_{pq})|$.

Βήμα 3ο. *Κάθε αυτομορφισμός τής* $\mathbf{L}_{pq}$ *είναι τής ανωτέρω μορφής* (*και, ως εκ τούτου,* $|\mathrm{Aut}(\mathbf{L}_{pq})| = q(q-1)$). Η κυκλική ομάδα $\langle t \rangle$ (τάξεως q) είναι μια ορθόθετη υποομάδα τής $\mathbf{L}_{pq}$, διότι για οιουσδήποτε $i, \kappa \in \{0,1,...,q-1\}$ και $j \in \{0,1,...,p-1\}$ η (7.90) δίδει $(t^i s^j) t^\kappa (t^i s^j)^{-1} = t^{c^j \kappa} \in \langle t \rangle$, ήτοι

$$\langle t \rangle \lhd \mathbf{L}_{pq} \underset{4.2.24}{\Longrightarrow} \mathbf{L}_{pq} = \langle t \rangle \langle s \rangle = \langle s \rangle \langle t \rangle .$$

Επιπροσθέτως, η $\langle t \rangle$ είναι *και χαρακτηριστική* υποομάδα τής $\mathbf{L}_{pq}$, διότι

$$\text{μκδ}(|\langle t \rangle|, |\mathbf{L}_{pq} : \langle t \rangle|) = \text{μκδ}(q,p) = 1.$$

(Βλ. πρόταση 6.1.9.) Έστω τώρα *τυχόν* αυτομορφισμός $\vartheta \in \mathrm{Aut}(\mathbf{L}_{pq})$. Επειδή $\vartheta(\langle t \rangle) = \langle t \rangle$, η εικόνα $\vartheta(t)$ τού στοιχείου t μέσω τού ϑ είναι μια δύναμη t^l τού t για κάποιον $l \in \{0,1,...,q-1\}$. Το t^l απεικονίζεται μέσω τού αντιστρόφου ϑ^{-1} τού ϑ στο t, οπότε από το πόρισμα 2.3.11 και το (iv) τής προτάσεως 2.4.19 λαμβάνουμε

$$\frac{q}{\text{μκδ}(l,q)} = \mathrm{ord}(t^l) = \mathrm{ord}(\vartheta^{-1}(t^l)) = \mathrm{ord}(t) = q,$$

απ' όπου έπεται ότι μκδ$(l,q) = 1 \Rightarrow l \neq 0$. Από την άλλη μεριά, $\vartheta(s) \notin \langle t \rangle$ (διότι αλλιώς το στοιχείο s θα ήταν η εικόνα κάποιας δυνάμεως τού στοιχείου t μέσω τού ϑ^{-1}, ήτοι εκ νέου μια δύναμη τού t, πράγμα αδύνατο). Άρα υπάρχει κατ' ανάγκην κάποιος $k \in \{0,1,...,q-1\}$ και κάποιος $\varrho \in \{1,...,p-1\}$, ούτως ώστε να ισχύει $(\langle s \rangle \langle t \rangle) \smallsetminus \langle t \rangle \ni \vartheta(s) = s^\varrho t^k$. Επειδή

$$\begin{aligned}&sts^{-1} = t^c \Rightarrow \vartheta(s)\vartheta(t)\vartheta(s)^{-1} = \vartheta(t)^c \Rightarrow (s^\varrho t^k) t^l (s^\varrho t^k)^{-1} = t^{cl}\\ &\Rightarrow s^\varrho t^k t^l t^{-k} s^{-\varrho} = t^{cl} \Rightarrow s^\varrho t^l s^{-\varrho} = t^{cl} \underset{(7.90)}{\Longrightarrow} t^{c^\varrho l} = t^{cl} \Rightarrow t^{lc(c^{\varrho-1}-1)} = \mathbf{I}_2\\ &\underset{2.3.8}{\Longrightarrow} q \mid lc(c^{\varrho-1}-1) \underset{1 \leq l < q}{\Longrightarrow} q \mid c(c^{\varrho-1}-1).\end{aligned}$$

Εξ ορισμού (τού c), $([c]_q)^p = [c^p]_q = [1]_q \Rightarrow q \mid c^p - 1$. Εάν το q ήταν διαιρέτης τού c, τότε θα ήταν διαιρέτης και τού c^p και, κατ' επέκταση, και τού $c^p - (c^p - 1) = 1$,

πράγμα αδύνατο. Επομένως, $[q \mid c(c^{\varrho-1}-1) \text{ και } q \nmid c] \Rightarrow q \mid c^{\varrho-1}-1$. Επειδή όμως $\min\{\xi \in \mathbb{N} : q \mid c^{\xi}-1\} = p$ και $0 \leq \varrho - 1 < \varrho < p$, συμπεραίνουμε τελικώς ότι $\varrho = 1$ και $\vartheta(s) = st^k$. Για τους άνωθι (μονοσημάντως ορισμένους) k και l ισχύει η ισότητα $\vartheta = \vartheta_{k,l}$, αφού

$$\left\{ \begin{array}{l} \vartheta(t^i s^j) = \vartheta(t)^i \vartheta(s)^j = t^{li}(st^k)^j = \vartheta_{k,l}(t^i s^j), \\ \forall (i,j) \in \{0,1,...,q-1\} \times \{0,1,...,p-1\}. \end{array} \right\}$$

Βήμα 4ο. Η απεικόνιση $\psi_{[\lambda]_q}$ είναι ενδομορφισμός τής $\mathbb{Z}_q$ και η ψ ομομορφισμός ομάδων. (Πρβλ. με το 4ο βήμα τής αποδείξεως τού θεωρήματος 7.6.36.) Άρα *ορίζεται* το εξωτερικό ημιευθύ γινόμενο $\mathbb{Z}_q \rtimes_{\psi} \mathbb{Z}_q^{\times}$.

Βήμα 5ο. Η απεικόνιση $f : \mathrm{Aut}(\mathbf{L}_{pq}) \longrightarrow \mathbb{Z}_q \rtimes_{\psi} \mathbb{Z}_q^{\times}$, $\vartheta_{k,l} \longmapsto ([k]_q, [l]_q)$, είναι ισομορφισμός ομάδων. (Το εν λόγω εξωτερικό ημιευθύ γινόμενο ταυτίζεται με εκείνο τού θεωρήματος 7.6.36 στην περίπτωση κατά την οποία $n = q$.) □

Παρομοίως αποδεικνύεται και το ακόλουθο:

7.6.39 Θεώρημα. (Ομάδα αυτομορφισμών των $\mathbf{Dic}_m$ για $m \geq 3$)
Έστω $m \in \mathbb{N}$, $m \geq 3$, και έστω

$$\mathbf{Dic}_m = \langle \mathfrak{x}, \mathfrak{y} \rangle = \left\{ \mathfrak{y}^{-j} \middle| \, j \in \{0,1,...,2m-1\} \right\} \cup \left\{ \mathfrak{x}\mathfrak{y}^j \, | j \in \{0,1,...,2m-1\} \right\}$$

η m-οστή δικυκλική ομάδα, όπου $\mathfrak{x}$ και $\mathfrak{y}$ όπως στην πρόταση 7.6.30, με

$$\mathrm{ord}(\mathfrak{x}) = 4, \ \mathrm{ord}(\mathfrak{y}) = 2m \text{ και } \mathfrak{y}^m = \mathfrak{x}^2, \ \mathfrak{y}\mathfrak{x} = \mathfrak{x}\mathfrak{y}^{-1}.$$

Η ομάδα των αυτομορφισμών τής $\mathbf{Dic}_m$ είναι η

$$\boxed{\mathrm{Aut}(\mathbf{Dic}_m) = \{ \vartheta_{k,l} | \, (k,l) \in \{0,1,...,2m-1\} \times \{1,...,2m-1\} \text{ και } \mu\kappa\delta(l,2m) = 1\}}$$

τάξεως $|\mathrm{Aut}(\mathbf{Dic}_m)| = 2m\phi(2m)$, όπου ϕ η συνάρτηση φι τού Euler και

$$\vartheta_{k,l}(\mathfrak{y}^{-j}) := \mathfrak{y}^{-jl}, \ \vartheta_{k,l}(\mathfrak{x}\mathfrak{y}^j) := \mathfrak{x}\mathfrak{y}^{jl-k} = \mathfrak{y}^{k-jl}\mathfrak{x}, \ \forall j \in \{0,1,...,2m-1\}.$$

Επιπροσθέτως,

$$\boxed{\mathrm{Aut}(\mathbf{Dic}_m) \cong \mathbb{Z}_{2m} \rtimes_{\psi} \mathbb{Z}_{2m}^{\times} \cong \mathrm{Aut}(\mathbf{D}_{2m}),}$$

όπου $\psi : \left(\mathbb{Z}_{2m}^{\times}, \cdot\right) \longrightarrow \left(\mathrm{Aut}(\mathbb{Z}_{2m}), \circ\right), [\lambda]_{2m} \longmapsto \psi_{[\lambda]_{2m}}$, είναι ο ομομορφισμός ο απεικονίζων την κλάση $[\lambda]_{2m}$ οιουδήποτε $\lambda \in \{l \in \{1,...,2m-1\} | \mu\kappa\delta(l,2m) = 1\}$ στον αυτομορφισμό $\psi_{[\lambda]_{2m}} : \mathbb{Z}_{2m} \longrightarrow \mathbb{Z}_{2m}, [k]_{2m} \longmapsto \psi_{[\lambda]_{2m}}([k]_{2m}) := [\lambda]_{2m}[k]_{2m}$.

7.6.40 Σημείωση. Στην ειδική περίπτωση όπου $m = 2$, η ομάδα αυτομορφισμών τής $\mathbf{Dic}_2 \cong \mathbf{Q}$ (μη εμπίπτουσα στην ανωτέρω μέθοδο υπολογισμού) δίδεται στην άσκηση **7-78**.

► **«Εσωτερικό» ημιευθύ γινόμενο δύο υποομάδων μιας ομάδας**. Ως αφετηρία μας θα θεωρήσουμε την έννοια τού *συμπληρώματος*.

7.6.41 Ορισμός. Έστω $(G,\cdot)$ μια ομάδα. Όταν, δοθείσας μιας $H\in\mathbf{Subg}(G)$, υφίστανται κάποια $K\in\mathbf{Subg}(G)$, ούτως ώστε να ισχύει $G=HK$ και $H\cap K=\{e_G\}$, τότε λέμε ότι η K αποτελεί ένα **συμπλήρωμα τής** H (εντός τής G).

7.6.42 Σημείωση. (i) Ακόμη και μια *ορθόθετη* υποομάδα H τής G δεν διαθέτει κατ' ανάγκην κάποιο συμπλήρωμα. Αλλά και όταν διαθέτει, αυτό δεν είναι κατ' ανάγκην ένα και μόνο. (Επί παραδείγματι, εντός τής $\mathfrak{S}_3$, κάθε υποομάδα τάξεως 2 αποτελεί συμπλήρωμα τής $\mathfrak{A}_3$.) Ωστόσο, δυο τυχόντα συμπληρώματα K_1,K_2 μιας $H\trianglelefteq G$ είναι πάντοτε *ισόμορφα* μεταξύ τους, αφού

$$K_1\underset{4.4.5}{\cong}K_1/\{e_{K_1}\}\underset{2.1.18}{=}K_1/\{e_G\}=K_1/H\cap K_1\underset{4.5.13}{\cong}HK_1/H=G/H$$
$$=HK_2/H\underset{4.5.13}{\cong}K_2/H\cap K_2=K_2/\{e_G\}\underset{2.1.18}{=}K_2/\{e_{K_2}\}\underset{4.4.5}{\cong}K_2.$$

(ii) Εάν $H\trianglelefteq G$ και $K\trianglelefteq G$, τότε η K αποτελεί συμπλήρωμα τής H εντός τής G εάν και μόνον εάν $G=H\times_{\text{εσ.}}K$. Ωστόσο, όπως θα δούμε ευθύς αμέσως, εξίσου (αν όχι περισσότερο) σημαντική είναι και η μελέτη των συμπληρωμάτων μιας $H\trianglelefteq G$ που δεν είναι απαραιτήτως ορθόθετα.

Ο ορισμός 7.1.21 γενικεύεται ως ακολούθως:

7.6.43 Ορισμός. Έστω ότι η $(G,\cdot)$ είναι μια ομάδα και ότι $H\sqsubseteq G$ και $K\sqsubseteq G$. Λέμε ότι η G είναι το **εσωτερικό ημιευθύ γινόμενο των υποομάδων** H **και** K (και γράφουμε $G=H\rtimes K$) όταν πληρούνται οι ακόλουθες συνθήκες:

(i) $H\trianglelefteq G$,

(ii) $G=\langle H,K\rangle$ $(\underset{4.2.24}{=}HK=KH)$, και

(iii) $H\cap K=\{e_G\}$.

7.6.44 Σημείωση. (i) Προφανώς, $K\trianglelefteq G\iff G=H\times_{\text{εσ.}}K$. (Όταν $K\not\trianglelefteq G$, η $G=H\rtimes K$ καλείται, ιδιαιτέρως, **μη τετριμμένο εσωτερικό ημιευθύ γινόμενο των** H **και** K.)

(ii) Από τις συνθήκες (ii) και (iii) τού ορισμού 7.6.43 έπεται ότι η K αποτελεί συμπλήρωμα τής H εντός τής G και ότι κάθε $g\in G$ γράφεται ως $g=hk$ για κάποια *μονοσημάντως ορισμένα*[100] στοιχεία $h\in H$ και $k\in K$. Επίσης, αξίζει να τονισθεί ότι όταν η $G=H\rtimes K$ είναι *μη τετριμμένο* εσωτερικό ημιευθύ γινόμενο των H και K (και *παρά το γεγονός* ότι $G=HK=KH$), υπάρχουν *πάντοτε* κάποια $a\in H,b\in K$ με[101] $ab\neq ba$.

7.6.45 Θεώρημα. *Έστω $(G,\cdot)$ μια ομάδα και έστω $H\trianglelefteq G$. Τότε τα ακόλουθα είναι ισοδύναμα*:

(i) *Η ομάδα H διαθέτει κάποιο συμπλήρωμα $K\sqsubseteq G$ εντός τής G (ήτοι $G=H\rtimes K$*

[100] Εάν $g=h'k'$ για κάποια $h'\in H$ και $k'\in K$, τότε $hk=h'k'\Rightarrow H\ni h^{-1}h'=k'k^{-1}\in K$ και επειδή $H\cap K=\{e_G\}$ έχουμε $h=h'$ και $k=k'$.

[101] Εάν $xy=yx,\ \forall x\in H$ και $\forall y\in K$, τότε $G=H\times_{\text{εσ.}}K$. (Βλ. 7.1.26 (b)⇒(a).)

με $K \cong G/H$).

(ii) *Υπάρχει μια* $K \sqsubseteq G$, *τέτοια ώστε κάθε* $g \in G$ *να γράφεται ως* $g = hk$ *για κάποια μονοσημάντως ορισμένα στοιχεία* $h \in H$ *και* $k \in K$.

(iii) *Υπάρχει ομομορφισμός* $f : G/H \longrightarrow G$ *για τον οποίο ισχύει* $\pi_H^G \circ f = \mathrm{id}_{G/H}$, *όπου* $\pi_H^G : G \longrightarrow G/H$ *ο φυσικός επιμορφισμός.*

(iv) *Υπάρχει ένας* $\vartheta \in \mathrm{End}(G)$ *με* $\mathrm{Ker}(\vartheta) = H$ *και* $\vartheta(x) = x, \forall x \in \mathrm{Im}(\vartheta)$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Βλ. 7.6.44 (ii).

(ii)⇒(iii) Έστω τυχόν $g \in G$. Αυτό γράφεται εξ υποθέσεως ως $g = hk$ για κάποια μονοσημάντως ορισμένα στοιχεία $h \in H$ και $k \in K$. Άρα για την πλευρική του κλάση Hg εντός τής πηλικοομάδας G/H έχουμε $Hg = Hhk = Hk$. Θεωρούμε την

$$f : G/H \longrightarrow G,\ Hg \longmapsto k.$$

Η f είναι *καλώς ορισμένη* απεικόνιση (διότι προφανώς για $g_1 = h_1k_1$, $g_2 = h_2k_2$ με $Hg_1 = Hg_2$ λαμβάνουμε $Hk_1 = Hk_2$, οπότε $k_1k_2^{-1} \in H \cap K = \{e_G\}$, ήτοι $k_1 = k_2$). Επιπλέον, είναι και ομομορφισμός, καθόσον για $g_1 = h_1k_1$, $g_2 = h_2k_2$,

$$f(Hg_1)f(Hg_2) = k_1k_2 = f(Hg_1g_2) = f((Hg_1)(Hg_2)) = f(Hg_1g_2).$$

Τέλος, $(\pi_H^G \circ f)(Hg) = \pi_H^G(k) = Hk = Hhk = Hg$ για κάθε $g = hk \in G$.

(iii)⇒(iv) Ορίζουμε τον ενδομορφισμό $\vartheta := f \circ \pi_H^G$ τής G. Έστω τυχόν στοιχείο $x \in \mathrm{Im}(\vartheta)$. Τότε $\exists g \in G : x = \vartheta(g)$. Προφανώς,

$$\begin{aligned}\vartheta(x) &= \vartheta(\vartheta(g)) = (\vartheta \circ \vartheta)(g) = \left(\left(f \circ \pi_H^G\right) \circ \left(f \circ \pi_H^G\right)\right)(g)\\ &= (f \circ (\underbrace{\pi_H^G \circ f}_{=\mathrm{id}_{G/H}}) \circ \pi_H^G)(g) = \left(f \circ \pi_H^G\right)(g) = \vartheta(g) = x.\end{aligned}$$

Εάν $h \in H$, τότε ισχύει $\vartheta(h) = (f \circ \pi_H^G)(h) = f(hH) = f(H) = f(e_{G/H}) = e_G$, οπότε $h \in \mathrm{Ker}(\vartheta)$. Άρα $H \subseteq \mathrm{Ker}(\vartheta)$. Και αντιστρόφως· εάν $g \in \mathrm{Ker}(\vartheta)$, τότε έχουμε $f(H) = f(e_{G/H}) = e_G = \vartheta(g) = (f \circ \pi_H^G)(g) = f(gH)$. Επειδή $\pi_H^G \circ f = \mathrm{id}_{G/H}$, η f είναι *ενριπτική* απεικόνιση. Κατά συνέπειαν, $H = gH \Rightarrow g \in H$. Ως εκ τούτου, ισχύει και ο αντίστροφος εγκλεισμός $\mathrm{Ker}(\vartheta) \subseteq H$.

(iv)⇒(i) Θέτουμε $K := \mathrm{Im}(\vartheta)$. Εάν $g \in H \cap K$, τότε $\vartheta(g) = e_G$ και (ταυτοχρόνως) $\vartheta(g) = g$. Επομένως, $g = e_G$ και $H \cap K = \{e_G\}$. Εξάλλου, εάν $g \in G$, τότε

$$\vartheta(g\vartheta(g^{-1})) = \vartheta(g)\vartheta(\underbrace{\vartheta(g^{-1})}_{\in \mathrm{Im}(\vartheta)}) = \vartheta(g)\vartheta(g^{-1}) = \vartheta(\underbrace{gg^{-1}}_{=e_G}) = e_G,$$

οπότε $g\vartheta(g^{-1}) \in \mathrm{Ker}(\vartheta) = H$. Το g γράφεται ως ακολούθως:

$$g = ge_G = g\vartheta(e_G) = g\vartheta(g^{-1}g) = \underbrace{(g\vartheta(g^{-1}))}_{\in H}\ \underbrace{\vartheta(g)}_{\in K}.$$

Άρα $G = HK$ και η K αποτελεί ένα συμπλήρωμα τής H εντός τής G. □

7.6.46 Θεώρημα. *Έστω ότι η* $(G, \cdot)$ *είναι μια πεπερασμένη ομάδα και ότι* $H \trianglelefteq G$ *και* $K \sqsubseteq G$. *Εάν* $|G| = mn$ *και* $|H| = m, |K| = n$, *όπου* $m, n \in \mathbb{N}$ *με* μκδ$(m, n) = 1$, *τότε* $G = H \rtimes K$.

ΑΠΟΔΕΙΞΗ. Πανομοιότυπη εκείνης τού θεωρήματος 7.1.48. □

7.6.47 Παράδειγμα. Έστω $n \in \mathbb{N}$, $n \geq 3$. Η εναλλάσσουσα ομάδα $\mathfrak{A}_n$ είναι μια ορθόθετη υποομάδα τής $\mathfrak{S}_n$. (Βλ. 4.2.14 ή 4.2.32 (i)). Έστω K η κυκλική υποομάδα $\langle [1\ 2] \rangle = \{\mathrm{id}, [1\ 2]\}$ τής $\mathfrak{S}_n$ η παραγόμενη από την αντιμετάθεση $[1\ 2]$. Κατά το θεώρημα 7.6.46,

$$\boxed{\mathfrak{S}_n = \mathfrak{A}_n \rtimes \langle [1\ 2] \rangle .}$$

Αυτό το εσωτερικό ημιευθύ γινόμενο *δεν είναι ευθύ*, καθότι έχουμε $K \not\trianglelefteq \mathfrak{S}_n$. (Βλ. θεώρημα 4.3.12.)

7.6.48 Παράδειγμα. Εάν $K := \{\sigma \in \mathfrak{S}_4 \,|\, \sigma(4) = 4\}$, τότε $K \cong \mathfrak{S}_3$, $\mathbf{V} \lhd \mathfrak{S}_4$ και (σύμφωνα με το θεώρημα 7.6.46)

$$\boxed{\mathfrak{S}_4 = \mathbf{V} \rtimes K.}$$

Αυτό το εσωτερικό ημιευθύ γινόμενο *δεν είναι ευθύ*, δηλαδή είναι *μη τετριμμένο*, καθότι έχουμε $K \not\trianglelefteq \mathfrak{S}_4$. (Βλ. εδάφιο 7.1.28 (iii).)

7.6.49 Παράδειγμα. Έστω $K := \langle [1\ 2\ 3] \rangle$ η κυκλική υποομάδα (τάξεως 3) τής $\mathfrak{A}_4$ η παραγόμενη από τον 3-κύκλο $[1\ 2\ 3]$. Επειδή $\mathbf{V} \lhd \mathfrak{A}_4$ (βλ. 4.2.21), μέσω τού θεωρήματος 7.6.46 συμπεραίνουμε ότι

$$\boxed{\mathfrak{A}_4 = \mathbf{V} \rtimes \langle [1\ 2\ 3] \rangle .}$$

Αυτό το εσωτερικό ημιευθύ γινόμενο *είναι μη τετριμμένο*, καθόσον

$$([1\ 2] \circ [3\ 4]) \circ [1\ 2\ 3] \circ ([1\ 2] \circ [3\ 4])^{-1} = [2\ 4\ 3] \circ ([1\ 2] \circ [3\ 4])$$
$$= [1\ 4\ 2] \notin K\ (= \{\mathrm{id}, [1\ 2\ 3], [1\ 3\ 2]\}) \Rightarrow K \not\trianglelefteq \mathfrak{A}_4.$$

7.6.50 Παράδειγμα. Έστω ότι p, q είναι πρώτοι αριθμοί με $p < q$ και $q \equiv 1 (\mathrm{mod}\, p)$, και έστω $\mathbf{L}_{pq}$ η μοναδική (μέχρις ισομορφισμού) μη αβελιανή ομάδα τάξεως pq. (Βλ. πρόταση 5.7.15.) Σύμφωνα με το θεώρημα 7.6.20, η $\mathbf{L}_{pq}$ είναι ισόμορφη με ένα (κατάλληλο) εξωτερικό ημιευθύ γινόμενο των κυκλικών ομάδων $\mathbb{Z}_q$ και $\mathbb{Z}_p$. Από την άλλη μεριά, επειδή $\mathbf{L}_{pq} = \langle t \rangle \langle s \rangle$ και $\langle t \rangle \cap \langle s \rangle = \{\mathbf{I}_2\}$, όπου

$$s := \begin{pmatrix} [c]_q & [0]_q \\ [0]_q & [1]_q \end{pmatrix}, \quad t := \begin{pmatrix} [1]_q & [1]_q \\ [0]_q & [1]_q \end{pmatrix}$$

(με $\mathrm{ord}([c]_q) = p$ εντός τής $\mathbb{Z}_q^\times$) και $\langle t \rangle \lhd \mathbf{L}_{pq}$, έχουμε $\langle t \rangle \cong \mathbb{Z}_q$, $\langle s \rangle \cong \mathbb{Z}_p$ και (μέσω τού θεωρήματος 7.6.46)

$$\boxed{\mathbf{L}_{pq} = \langle t \rangle \rtimes \langle s \rangle .}$$

7.6.51 Παράδειγμα. Έστω p τυχών περιττός πρώτος αριθμός. Σύμφωνα με το θεώρημα 7.6.25, οι ομάδες $\mathbf{Heis}(\mathbb{Z}_p)$ και $\mathbb{G}_p$ (ήτοι οι -μέχρις ισομορφισμού- μοναδικές μη αβελιανές ομάδες τάξεως p^3) είναι ισόμορφες με (κατάλληλα) εξωτερικά ημιευθέα γινόμενα αβελιανών ομάδων. Από την άλλη μεριά, κάνοντας χρήση των γεννητόρων αυτών $\mathbf{A}, \mathbf{B}, \mathbf{C}$ και $\mathbf{D}$ (των ορισθέντων στις (7.77) και (7.79)), είναι εύκολο να ελέγξει κανείς ότι

$$\boxed{\mathbf{Heis}(\mathbb{Z}_p) = \langle \mathbf{A}, [\mathbf{A}, \mathbf{B}] \rangle \rtimes \langle \mathbf{B} \rangle = \langle \mathbf{B}, [\mathbf{A}, \mathbf{B}] \rangle \rtimes \langle \mathbf{A} \rangle} \quad \text{και} \quad \boxed{\mathbb{G}_p = \langle \mathbf{C} \rangle \rtimes \langle \mathbf{D} \rangle},$$

παρότι, εν προκειμένω, δεν μπορεί να εφαρμοσθεί το θεώρημα 7.6.46!

7.6.52 Παράδειγμα. Έστω $n \in \mathbb{N}, n \geq 2$. Θεωρούμε τις (άπειρες) ομάδες[102]

$$\mathbf{GL}_n^+(\mathbb{R}) := \{\mathbf{A} \in \mathbf{GL}_n(\mathbb{R}) \mid \det(\mathbf{A}) > 0\} \lhd \mathbf{GL}_n(\mathbb{R}),$$

$$\mathbf{SO}_n(\mathbb{R}) := \{\mathbf{A} \in \mathbf{O}_n(\mathbb{R}) \mid \det(\mathbf{A}) = 1\} \lhd \mathbf{O}_n(\mathbb{R}) \sqsubset \mathbf{GL}_n(\mathbb{R}),$$

καθώς και την (κυκλική υποομάδα τής $\mathbf{O}_n(\mathbb{R})$ τάξεως 2)

$$K_n := \begin{cases} \{\mathbf{I}_n, -\mathbf{I}_n\}, & \text{όταν ο } n \text{ είναι περιττός,} \\ \{\mathbf{I}_n, \mathbf{J}_n\}, & \text{όταν ο } n \text{ είναι άρτιος,} \end{cases}$$

όπου

$$\mathbf{I}_n := \begin{pmatrix} 1 & & & & \\ & 1 & & \mathbf{0} & \\ & & \ddots & & \\ & \mathbf{0} & & 1 & \\ & & & & 1 \end{pmatrix}, \quad \mathbf{J}_n := \begin{pmatrix} 1 & & & & \\ & 1 & & \mathbf{0} & \\ & & \ddots & & \\ & \mathbf{0} & & 1 & \\ & & & & -1 \end{pmatrix}.$$

Προφανώς, $\mathbf{GL}_n^+(\mathbb{R}) \cap K_n = \mathbf{SO}_n(\mathbb{R}) \cap K_n = \{\mathbf{I}_n\}$. Επίσης,

$$\left|\mathbf{GL}_n(\mathbb{R}) : \mathbf{GL}_n^+(\mathbb{R})\right| = 2 = \left|\mathbf{O}_n(\mathbb{R}) : \mathbf{SO}_n(\mathbb{R})\right|,$$

με

$$\mathbf{GL}_n(\mathbb{R}) = \begin{cases} \mathbf{GL}_n^+(\mathbb{R}) \coprod ((-\mathbf{I}_n)\, \mathbf{GL}_n^+(\mathbb{R})), & \text{όταν ο } n \text{ είναι περιττός,} \\ \mathbf{GL}_n^+(\mathbb{R}) \coprod (\mathbf{J}_n\, \mathbf{GL}_n^+(\mathbb{R})), & \text{όταν ο } n \text{ είναι άρτιος,} \end{cases}$$

και, κατ' αναλογίαν,

$$\mathbf{O}_n(\mathbb{R}) = \begin{cases} \mathbf{SO}_n(\mathbb{R}) \coprod ((-\mathbf{I}_n)\, \mathbf{SO}_n(\mathbb{R})), & \text{όταν ο } n \text{ είναι περιττός,} \\ \mathbf{SO}_n(\mathbb{R}) \coprod (\mathbf{J}_n\, \mathbf{SO}_n(\mathbb{R})), & \text{όταν ο } n \text{ είναι άρτιος,} \end{cases}$$

[102] Επειδή $\det(\mathbf{I}_n) = 1 > 0$ και $\det(\mathbf{AB}^{-1}) = \det(\mathbf{A})\det(\mathbf{B}^{-1}) = \frac{\det(\mathbf{A})}{\det(\mathbf{B})} > 0$ για κάθε $\mathbf{A}, \mathbf{B} \in \mathbf{GL}_n^+(\mathbb{R})$, έχουμε $\mathbf{GL}_n^+(\mathbb{R}) \sqsubset \mathbf{GL}_n(\mathbb{R})$ (βλ. 2.1.16 (iii)). Επίσης, επειδή $\det(\mathbf{BAB}^{-1}) = \det(\mathbf{A})$ για κάθε $\mathbf{A} \in \mathbf{GL}_n^+(\mathbb{R})$ και κάθε $\mathbf{B} \in \mathbf{GL}_n(\mathbb{R})$, έχουμε $\mathbf{GL}_n^+(\mathbb{R}) \lhd \mathbf{GL}_n(\mathbb{R})$. Το ότι $\mathbf{SO}_n(\mathbb{R}) \lhd \mathbf{O}_n(\mathbb{R})$ έχει ήδη αποδειχθεί στο εδάφιο 4.2.32 (iii).

οπότε $\mathrm{GL}_n(\mathbb{R}) = \mathrm{GL}_n^+(\mathbb{R})\, K_n$ και $\mathrm{O}_n(\mathbb{R}) = \mathrm{SO}_n(\mathbb{R})\, K_n$. Εν συνεχεία, εξετάζουμε τις δύο περιπτώσεις χωριστά:

(i) Εάν ο n είναι *περιττός*, τότε

$$\left.\begin{array}{r} \mathbf{A}\mathbf{I}_n\mathbf{A}^{-1} = \mathbf{I}_n \in K_n \\ \text{και } \mathbf{A}(-\mathbf{I_n})\mathbf{A}^{-1} = -\mathbf{I}_n \in K_n \\ \forall\ \mathbf{A} \in \mathrm{GL}_n(\mathbb{R}) \text{ (και αντ., } \forall \mathbf{A} \in \mathrm{O}_n(\mathbb{R})) \end{array}\right\} \Rightarrow K_n \lhd \mathrm{GL}_n(\mathbb{R}) \text{ και } K_n \lhd \mathrm{O}_n(\mathbb{R}),$$

οπότε (βάσει των 7.1.21 και 7.1.43 (ii)) έχουμε

$$\boxed{\mathrm{GL}_n(\mathbb{R}) = \mathrm{GL}_n^+(\mathbb{R}) \times_{\varepsilon\sigma.} K_n \cong \mathrm{GL}_n^+(\mathbb{R}) \times K_n}$$

και

$$\boxed{\mathrm{O}_n(\mathbb{R}) = \mathrm{SO}_n(\mathbb{R}) \times_{\varepsilon\sigma.} K_n \cong \mathrm{SO}_n(\mathbb{R}) \times K_n.}$$

(ii) Εάν ο n είναι *άρτιος*, τότε

$$\boxed{\mathrm{GL}_n(\mathbb{R}) = \mathrm{GL}_n^+(\mathbb{R}) \rtimes K_n} \quad \text{και} \quad \boxed{\mathrm{O}_n(\mathbb{R}) = \mathrm{SO}_n(\mathbb{R}) \rtimes K_n.}$$

Εν τοιαύτη περιπτώσει, τα ανωτέρω εσωτερικά ημιευθέα γινόμενα *δεν είναι ευθέα*, καθότι $K_n \not\trianglelefteq \mathrm{GL}_n(\mathbb{R})$ και $K_n \not\trianglelefteq \mathrm{O}_n(\mathbb{R})$. (Τούτο είναι αρκετό να αποδειχθεί για $n = 2$. Π.χ., για τον πίνακα $\mathbf{A} := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ έχουμε $\mathbf{A}\mathbf{J}_2\mathbf{A}^{-1} = -\mathbf{J}_2 \notin K_2$.)

7.6.53 Παράδειγμα. Από τα (i) και (iii) τού θεωρήματος 6.4.8 έπεται ότι το *ολόμορφο* $\mathrm{Hol}(G)$ οιασδήποτε ομάδας G είναι εσωτερικό ημιευθύ γινόμενο:

$$\boxed{\mathrm{Hol}(G) = L(G) \rtimes \mathrm{Aut}(G) = R(G) \rtimes \mathrm{Aut}(G).}$$

7.6.54 Παράδειγμα. Ως γνωστόν, για οιονδήποτε μη εσωτερικό αυτομορφισμό ϑ τής $\mathfrak{S}_6$ έχουμε

$$\boxed{\mathrm{Aut}(\mathfrak{A}_6) \cong \mathrm{Aut}(\mathfrak{S}_6) \cong \mathfrak{S}_6 \rtimes \langle\vartheta\rangle \cong \mathfrak{S}_6 \rtimes \mathbb{Z}_2.}$$

(Βλ. 6.3.9 και 6.3.19.)

7.6.55 Παράδειγμα. Έστω $s \in \mathbb{N}$, $s \geq 2$, και έστω G μια αναποσυνθέσιμη μη αβελιανή πεπερασμένη ομάδα. Ο J.N.S. Bidwell απέδειξε[103] ότι

$$\boxed{\mathrm{Aut}(G^s) \cong \mathcal{A} \rtimes \mathfrak{S}_s,}$$

όπου $\mathcal{A}$ η ομάδα η ορισθείσα στο θεώρημα 7.1.77 (με $G_1 = \cdots = G_s =: G$). Σημειωτέον ότι η τάξη τής $\mathrm{Aut}(G^s)$ ισούται με

$$\boxed{|\mathrm{Aut}(G^s)| = |\mathrm{Aut}(G)|^s\, |\mathrm{Hom}(G, Z(G))|^{s(s-1)}\, s!.}$$

Π.χ., επειδή $\mathrm{Aut}(\mathbf{D}_4) \cong \mathbf{D}_4$ και $\mathrm{Hom}(\mathbf{D}_4, Z(\mathbf{D}_4)) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$, έχουμε

$$|\mathrm{Aut}(\mathbf{D}_4 \times \mathbf{D}_4 \times \mathbf{D}_4)| = 8^3 4^6 3! = 12582912.$$

[103] Βλ. Thm. 3.1 στο άρθρο τού J.N.S. Bidwell: *Automorphisms of direct products of finite groups II*, Archiv der Math. (Basel) **91** (2008), 111-121.

► **Συσχετισμός εξωτερικού και εσωτερικού ημιευθέος γινομένου**. Αυτός αποσαφηνίζεται στο ακόλουθο:

7.6.56 Θεώρημα. (i) *Εάν G_1, G_2 είναι δυο ομάδες, $\varphi : G_2 \longrightarrow \mathrm{Aut}(G_1)$ ένας ομομορφισμός και $\overline{G}_1 := G_1 \rtimes_\varphi \{e_{G_2}\}$, $\overline{G}_2 := \{e_{G_1}\} \rtimes_\varphi G_2$, τότε*

$$\boxed{\overline{G}_1 \rtimes \overline{G}_2 = G_1 \rtimes_\varphi G_2.}$$

(ii) *Εάν H και K είναι υποομάδες μιας ομάδας $(G, \cdot)$ με $H \trianglelefteq G$, τέτοιες ώστε να ισχύει $G = H \rtimes K$, τότε*

$$\boxed{\exists\, \varphi \in \mathrm{Hom}(K, \mathrm{Aut}(H)) : H \rtimes_\varphi K \cong G = H \rtimes K.} \tag{7.96}$$

Μάλιστα, ως ένας τέτοιος $\varphi : K \longrightarrow \mathrm{Aut}(H),\ y \longmapsto \varphi_y$, μπορεί να επιλεγεί ο ομομορφισμός ο αντιστοιχίζων σε κάθε $y \in K$ τον αυτομορφισμό

$$\varphi_y = \boldsymbol{\gamma}_y\big|_H : H \longrightarrow H,\quad \boldsymbol{\gamma}_y(x) = yxy^{-1},\ \ \forall x \in H,$$

τής υποομάδας H που προκύπτει ως περιορισμός τού εσωτερικού αυτομορφισμού [104] *$\boldsymbol{\gamma}_y \in \mathrm{Inn}(G)$ τής G επί τής H και στέλνει κάθε στοιχείο τής H να απεικονισθεί στο συζυγές του το δημιουργούμενο μέσω τού y.* (Βλ. 5.4.21 και 5.4.23.)

ΑΠΟΔΕΙΞΗ. (i) Τούτο έπεται από τα (i), (iii), (iv) και (v) τής προτάσεως 7.6.3.
(ii) Εάν $G = H \rtimes K$, τότε για τον $\varphi : K \longrightarrow \mathrm{Aut}(H),\ y \longmapsto \varphi_y := \boldsymbol{\gamma}_y\big|_H$, η (προφανώς επιρριπτική) απεικόνιση

$$f : H \rtimes_\varphi K \longrightarrow G\,(= HK = H \rtimes K),\ (x, y) \longmapsto f((x, y)) := xy$$

είναι επιμορφισμός ομάδων, διότι για οιαδήποτε $(x_1, y_1), (x_2, y_2) \in H \rtimes_\varphi K$ ισχύει

$$f((x_1, y_1)(x_2, y_2)) = f(x_1\varphi_{y_1}(x_2), y_1y_2) = f(x_1\boldsymbol{\gamma}_{y_1}(x_2), y_1y_2) = (x_1\boldsymbol{\gamma}_{y_1}(x_2))(y_1y_2)$$
$$= (x_1y_1x_2y_1^{-1})(y_1y_2) = (x_1y_1)(x_2y_2) = f((x_1, y_1))f((x_2, y_2)),$$

και έχει ως πυρήνα τον

$$\begin{aligned}\mathrm{Ker}(f) &= \{(x, y) \in H \rtimes_\varphi K \,|\, xy = e_G\} \\ &= \{(x, y) \in H \rtimes_\varphi K \,|\, x = y = e_G\} = (e_G, e_G) = e_{H \rtimes_\varphi K}.\end{aligned}$$

(Η δεύτερη ισότητα έπεται από το ότι $xy = e_G = e_Ge_G \Rightarrow x = y = e_G$, ήτοι από τη μοναδικότητα τής παραστάσεως τού ουδετέρου στοιχείου e_G τής G ως γινομένου ενός στοιχείου τής H και ενός στοιχείου τής K. Βλ. 7.6.44 (ii).) Άρα η f είναι ισομορφισμός ομάδων. (Φυσικά, ο *συγκεκριμένος* φ, με $\varphi_y := \boldsymbol{\gamma}_y\big|_H, \forall y \in K$, μπορεί να είναι ο πλέον «κατάλληλος» ομομορφισμός από την K στην $\mathrm{Aut}(H)$ με αυτήν την ιδιότητα, αλλά δεν είναι κατ' ανάγκην και ο μόνος! Επί παραδείγματι,

[104] Για κάθε $g \in G$ έχουμε $\boldsymbol{\gamma}_g(H) = H$ (διότι, εξ υποθέσεως, $H \trianglelefteq G$, βλ. 5.4.24), οπότε μέσω τού $\boldsymbol{\gamma}_g$ επάγεται ο αυτομορφισμός $\boldsymbol{\gamma}_g\big|_H \in \mathrm{Aut}(H)$ τής H. Ωστόσο αυτός δεν είναι κατ' ανάγκην εσωτερικός αυτομορφισμός τής ίδιας τής H.

εάν η G_2 διαθέτει μη τετριμμένη ομάδα αυτομορφισμών, τότε *και όλες* οι συνθέσεις $\varphi \circ \vartheta$, $\vartheta \in \mathrm{Aut}(G_2) \smallsetminus \{\mathrm{id}_{G_2}\}$, έχουν την ίδια ιδιότητα[105]. Βλ. πρόταση 7.6.6.) $\square$

7.6.57 Σημείωση. (i) Το εσωτερικό ημιευθύ γινόμενο *εξαρτάται* (μέχρις ισομορφισμού) από τον ομομορφισμό (7.96) υπό την εξής έννοια: Έστω ότι η $(G, \cdot)$ είναι μια ομάδα για την οποία απλώς γνωρίζουμε *την ύπαρξη* μιας $H \lhd G$ και μιας $K \sqsubset G$, ούτως ώστε να ισχύει $G = H \rtimes K$. Ακόμη κι αν οι H και K είναι εύκολα (και, μέχρις ισομορφισμού, μονοσημάντως) περιγράψιμες (π.χ., κυκλικές), ο μέχρις ισομορφισμού προσδιορισμός τής G είναι εφικτός μόνον κατόπιν διεξοδικής μελέτης των ομομορφισμών $K \longrightarrow \mathrm{Aut}(H)$. Επί παραδείγματι, εάν υποθέσουμε ότι η H είναι κυκλική τάξεως 3 και η K κυκλική τάξεως 2, τότε $H \cong \mathbb{Z}_3$ και $K \cong \mathbb{Z}_2$ (βλ. 2.4.23 (ii)). Ωστόσο, αυτή η πληροφορία (από μόνη της) *δεν αρκεί* για τον μέχρις ισομορφισμού προσδιορισμό τής G, καθώς[106] $\mathrm{Hom}(K, \mathrm{Aut}(H)) \cong \mathbb{Z}_2$. Στην περίπτωση όπου $K \lhd G$, ο (αντίστοιχος) φ είναι (κατά την πρόταση 7.6.4) ο τετριμμένος ομομορφισμός και έχουμε

$$G = H \times_{\varepsilon\sigma.} K \underset{\text{7.1.43 (ii)}}{\cong} H \times K \underset{\text{7.1.55 (v)}}{\cong} \mathbb{Z}_3 \oplus \mathbb{Z}_2 \underset{\text{7.1.62}}{\cong} \mathbb{Z}_6,$$

οπότε και η ίδια η G είναι κυκλική. Όμως όταν $K \not\lhd G$, ο φ είναι ο (μοναδικός) *μη τετριμμένος* ομομορφισμός από την K στην $\mathrm{Aut}(H)$, οπότε η G (κατά την πρόταση 7.6.4 και το πόρισμα 7.6.5) είναι *μη αβελιανή* και, ως εκ τούτου, $G \cong \mathfrak{S}_3$.[107] (Βλ. θεώρημα 4.1.37.)

(ii) Από την άλλη μεριά, είναι αυτή ακριβώς η εξάρτηση (μόνον) από τους ομομορφισμούς φ που καθιστά το θεώρημα 7.6.56 αρκούντως βοηθητικό για την (μέχρις ισομορφισμού) *ταξινόμηση* ορισμένων *ειδικών* πεπερασμένων ομάδων: Ας υποθέσουμε ότι ένας $n \in \mathbb{N}$ είναι τέτοιος, ώστε για *οιαδήποτε* ομάδα $(G, \cdot)$ τάξεως $|G| = n$ υπάρχουν (όχι κατ' ανάγκην μονοσημάντως ορισμένες) $H \lhd G$ και $K \sqsubset G$ με τις ιδιότητες $H \lhd G$, $G = HK$ και $H \cap K = \{e_G\}$, ήτοι με τις K συμπληρώματα των H. Η ταξινόμηση επιτυγχάνεται ως εξής:

Βήμα 1ο. Επιλέγουμε κατάλληλους (βολικούς) εκπροσώπους όλων των (σαφώς διακεκριμένων) κλάσεων ισομορφίας των H και K.

Βήμα 2ο. Για κάθε ζεύγος $\hat{H}, \hat{K}$ (με $H \cong \hat{H}$ και $K \cong \hat{K}$) που έχουμε βρει στο 1ο βήμα προσδιορίζουμε όλους τους δυνατούς ομομορφισμούς $\varphi \in \mathrm{Hom}(\hat{K}, \mathrm{Aut}(\hat{H}))$.

Βήμα 3ο. Για κάθε τριάδα $\hat{H}, \hat{K}, \varphi$ που έχουμε βρει στο 2ο βήμα σχηματίζουμε τα εξωτερικά ημιευθέα γινόμενα $\hat{H} \rtimes_\varphi \hat{K}$ (οπότε κάθε ομάδα G τάξεως n είναι ισόμορφη με μία εξ αυτών των διεξοδικώς κατασκευαζόμενων ομάδων) και, εν συνεχεία, ελέγχουμε ποια από τα εν λόγω εξωτερικά ημιευθέα γινόμενα είναι μεταξύ

[105] Μολαταύτα, *για κάθε* $\varphi \in \mathrm{Hom}(K, \mathrm{Aut}(H))$ ο «κανόνας πολλαπλασιασμού στοιχείων» εντός τού $H \rtimes_\varphi K$ δίδει $(e_H, y)(x, e_K)(e_H, y)^{-1} \underset{\text{2.1.18}}{=} (e_G, y)(x, e_G)(e_G, y)^{-1} = (\varphi_y(x), y)(e_G, y^{-1}) = (\varphi_y(x), e_G)$, $\forall x \in H$ και $\forall y \in K$. Με άλλα λόγια, *για κάθε* $\varphi \in \mathrm{Hom}(K, \mathrm{Aut}(H))$ το στοιχείο $(\varphi_y(x), e_G) \in H \rtimes_\varphi K$ ισούται με την εικόνα $\gamma_{(e_G, y)}(x, e_G)$ τού (x, e_G) μέσω τού εσωτερικού αυτομορφισμού $\gamma_{(e_G, y)} \in \mathrm{Inn}(H \rtimes_\varphi K)$ *τού ιδίου τού* $H \rtimes_\varphi K$!

[106] Επειδή $\mathrm{Aut}(\mathbb{Z}_3) \underset{\text{2.4.32 (ii)}}{\cong} \mathbb{Z}_3^\times \underset{\text{4.1.33}}{\cong} \mathbb{Z}_2$, έχουμε $\mathrm{Hom}(K, \mathrm{Aut}(H)) \cong \mathrm{Hom}(\mathbb{Z}_2, \mathbb{Z}_2) \cong \mathbb{Z}_2$ (πρβλ. 2.4.13 (ii)), όπου $\mathrm{Hom}(\mathbb{Z}_2, \mathbb{Z}_2) = \{\varphi_1, \varphi_2\}$ με $\varphi_1([0]_2) = \varphi_1([1]_2) = [0]_2$ και $\varphi_2([0]_2) = [0]_2$, $\varphi_2([1]_2) = [1]_2$.

[107] Π.χ., $\mathfrak{S}_3 = \mathfrak{A}_3 \rtimes \langle [1\ 2] \rangle$, όπου $\mathfrak{A}_3 \cong \mathbb{Z}_3$ και $\langle [1\ 2] \rangle \cong \mathbb{Z}_2$. (Βλ. 7.6.47.)

τους ισόμορφα. Κατ' αυτόν τον τρόπο προκύπτει ο τελικός κατάλογος των (ανά ζεύγη μη ισομόρφων) ομάδων τάξεως n.

7.6.58 Παράδειγμα. Έστω G μια ομάδα τάξεως $18 = 2 \cdot 3^2$. Είναι εύκολο να δειχθεί[108] ότι η G περιέχει *μία και μόνον* ορθόθετη υποομάδα H τάξεως 9, καθώς και (κάποιες) υποομάδες τάξεως 2. Έστω K τυχούσα υποομάδα τάξεως 2. Επειδή $H \lhd G$, το HK αποτελεί μια υποομάδα τής G. (Βλ. πρόταση 4.2.24.) Από το θεώρημα 7.6.46 έπεται ότι $G = H \rtimes K$. Επειδή (δυνάμει τού θεωρήματος 7.1.46 και τού (ii) τού θεωρήματος 2.4.23) έχουμε *είτε* $H \cong \mathbb{Z}_9$ *είτε* $H \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$ και $K \cong \mathbb{Z}_2$, συνάγεται ότι

$$\begin{aligned} &\text{είτε } \exists\, \varphi \quad \in \quad \mathrm{Hom}(\mathbb{Z}_2,\, \mathrm{Aut}(\mathbb{Z}_9)) : G \cong \mathbb{Z}_9 \rtimes_\varphi \mathbb{Z}_2, \\ &\text{είτε } \exists\, \varphi \quad \in \quad \mathrm{Hom}(\mathbb{Z}_2,\, \mathrm{Aut}(\mathbb{Z}_3 \oplus \mathbb{Z}_3)) : G \cong (\mathbb{Z}_3 \oplus \mathbb{Z}_3) \rtimes_\varphi \mathbb{Z}_2. \end{aligned}$$

Στην πρώτη περίπτωση, $\mathrm{Aut}(\mathbb{Z}_9) \underset{\text{2.4.32 (ii)}}{\cong} \mathbb{Z}_9^\times \underset{\text{7.3.9}}{\cong} \mathbb{Z}_6$ και $\mathrm{Hom}(\mathbb{Z}_2, \mathbb{Z}_6) \cong \mathbb{Z}_2$, οπότε

$$\text{είτε } \; G \cong \mathbb{Z}_9 \oplus \mathbb{Z}_2 \; \text{ είτε } \; G \cong \mathbb{Z}_9 \rtimes_\varphi \mathbb{Z}_2 \underset{\text{7.6.19 (iii)}}{\cong} \mathbf{D}_9,$$

όπου φ ο (μοναδικός) μη μηδενικός ομομορφισμός. Στη δεύτερη περίπτωση έχουμε

$$\mathrm{Aut}(\mathbb{Z}_3 \oplus \mathbb{Z}_3) \underset{\text{7.1.74}}{\cong} \mathbf{GL}_2(\mathbb{Z}_3)$$

και εκπρόσωποι των ομομορφισμών $\mathbb{Z}_2 \longrightarrow \mathbf{GL}_2(\mathbb{Z}_3)$ που καθορίζουν (ανά δύο) μη ισόμορφα εξωτερικά ημιευθέα γινόμενα είναι οι εξής[109]:

$$[j]_2 \overset{\text{τετρ. ομ.}}{\longmapsto} \begin{pmatrix} [1]_3 & [0]_3 \\ [0]_3 & [1]_3 \end{pmatrix}, \;\; [j]_2 \overset{\varphi_1}{\longmapsto} \begin{pmatrix} [1]_3 & [0]_3 \\ [0]_3 & [-1]_3^j \end{pmatrix}, \;\; [j]_2 \overset{\varphi_2}{\longmapsto} \begin{pmatrix} [-1]_3^j & [0]_3 \\ [0]_3 & [-1]_3^j \end{pmatrix},$$

για κάθε $j \in \mathbb{Z}$. Ως εκ τούτου,

$$\text{είτε } \; G \cong (\mathbb{Z}_3 \oplus \mathbb{Z}_3) \oplus \mathbb{Z}_2 \; \text{ είτε } \; G \cong (\mathbb{Z}_3 \oplus \mathbb{Z}_3) \rtimes_{\varphi_1} \mathbb{Z}_2 \; \text{ είτε } \; G \cong (\mathbb{Z}_3 \oplus \mathbb{Z}_3) \rtimes_{\varphi_2} \mathbb{Z}_2.$$

(Σημειωτέον ότι το ευθύ γινόμενο $\mathfrak{S}_3 \times \mathbb{Z}_3$ είναι μια ομάδα τάξεως 18 μη περιέχουσα στοιχεία τάξεως 9, οπότε εμπίπτει στη δεύτερη περίπτωση. Επειδή δε, είναι μη αβελιανή και περιέχει 3 στοιχεία τάξεως 2, είναι κατ' ανάγκην ισόμορφη με την $(\mathbb{Z}_3 \oplus \mathbb{Z}_3) \rtimes_{\varphi_1} \mathbb{Z}_2$.) Συμπέρασμα: *Μέχρις ισομορφισμού υπάρχουν μόνον* 5 *ομάδες τάξεως* 18.

7.6.59 Σημείωση. (Περί των υποομάδων τού ημιευθέος γινομένου.)
(i) Για υποομάδες H και K μιας ομάδας $(G, \cdot)$ με $H \trianglelefteq G$, τέτοιες ώστε $G = H \rtimes K$, τα σύνολα $\mathbf{Subg}(G)$ και $\mathbf{NSubg}(G)$ των υποομάδων και των ορθόθετων υποομάδων τής G έχουν περιγραφεί (μέσω ειδικών συνθηκών που οφείλουν να πληρούνται από κατάλληλες πλευρικές κλάσεις) σε άρθρα των K. Rosenbaum[110] και L.

[108] Βλ. 11.1.2, 11.1.6, 11.1.15 και 11.1.18.

[109] Για την εύρεση αυτών χρησιμοποιείται η πρόταση 7.6.7.

[110] K. Rosenbaum: *Die Untergruppen von halbdirekten Produkten*, Rostock. Math. Kolloq. **35** (1988), 21-30.

Gutierrez-Barrios[111], αντιστοίχως.

(ii) Μια μερική γενίκευση των θεωρημάτων 7.1.10 και 7.1.14 των Goursat και Remak για το εξωτερικό ημιευθύ γινόμενο $G_1 \rtimes_\varphi G_2$ δυο τυχουσών ομάδων G_1 και G_2 (το καθοριζόμενο μέσω ενός $\varphi \in \mathrm{Hom}(G_2, \mathrm{Aut}(G_1))$) εδόθη το 1991 από τον V.M. Usenko[112]. Σε αυτήν γίνεται χρήση τής εννοίας τού λεγομένου «σταυρωτού ομομορφισμού» (crossed homomorphism).

► **Περί των $\mathbf{Aut}(H \rtimes K)$ και $\mathbf{Aut_c}(H \rtimes K)$.** Στην περίπτωση όπου η $G = H \rtimes K$ είναι πεπερασμένη και ικανοποιούνται κάποιες επιπρόσθετες συνθήκες, οι ομάδες των αυτομορφισμών και των κεντρικών αυτομορφισμών τής G είναι εύκολα προσδιορίσιμες, όπως δείχνουν τα ακόλουθα θεωρήματα[113]:

7.6.60 Θεώρημα. (F. Zhou και H. Liu, 2008) *Έστω ότι οι H και K είναι υποομάδες μιας πεπερασμένης ομάδας $(G, \cdot)$ με $H \trianglelefteq G$, τέτοιες ώστε να ισχύει $G = H \rtimes K$. Θεωρούμε τις υποομάδες*

$$\mathcal{C}_{\mathrm{Aut}(G)}(H) := \{\psi \in \mathrm{Aut}(G) \mid \psi(x) = x,\ \forall x \in H\}\,,$$
$$\mathcal{C}_{\mathrm{Aut}(G)}(K) := \{\chi \in \mathrm{Aut}(G) \mid \chi(y) = y,\ \forall y \in K\}$$

τής $\mathrm{Aut}(G)$. Τότε

$$\boxed{\mathrm{Aut}(G) = \mathcal{C}_{\mathrm{Aut}(G)}(H) \circ \mathcal{C}_{\mathrm{Aut(G)}}(K)}$$

εάν και μόνον εάν

$$H \cap \vartheta(K) = \{e_G\} \ \text{ και } \ \left\langle \left\{ y^{-1}\vartheta(y) \mid y \in K \right\} \right\rangle \sqsubseteq \mathrm{C}_G(H),\ \forall \vartheta \in \mathrm{Aut}(G).$$

7.6.61 Σημείωση. Στην περίπτωση όπου $G = H \rtimes K$ (όχι απαραιτήτως πεπερασμένη) είναι τέτοια, ώστε $H \sqsubseteq_{\chi\alpha\varrho.} G$, ο J.Dietz[114] περιέγραψε ορισμένες ενδιαφέρουσες ικανές συνθήκες προκειμένου η $\mathrm{Aut}(G)$ να είναι αφ' εαυτής ένα (εσωτερικό) ημιευθύ γινόμενο.

7.6.62 Θεώρημα. (H. Mousavi και A. Somali, 2013) *Έστω ότι οι H και K είναι υποομάδες μιας πεπερασμένης ομάδας $(G, \cdot)$ με $H \trianglelefteq G$, τέτοιες ώστε να ισχύει $G = H \rtimes K$. Εάν* μκδ$(|H|, |K|) = 1$, *τότε $\vartheta|_H \in \mathrm{Aut_c}(H)$ και $\vartheta|_K \in \mathrm{Aut_c}(K)$ για κάθε $\vartheta \in \mathrm{Aut_c}(G)$, και*

$$\boxed{\mathrm{Aut_c}(G) = \{\vartheta|_H : \vartheta \in \mathrm{Aut_c}(G)\} \times \{\vartheta|_K : \vartheta \in \mathrm{Aut_c}(G)\}\,.}$$

---

[111] L. Gutierrez-Barrios: *Die Normalteiler von halbdirekten Produkten*, Wiss. Z. Padagog. Hochsch. Erfurt/Muhlhausen Math.-Natur. Reihe, Bd. **25** (1989), No. 2, 108-114.

[112] Βλ. V.M. Usenko: *Subgroups of semidirect products*, Ukrainian Math. J. **43** (1991), No. 7-8, 982-988.

[113] Βλ. F. Zhou & H. Liu: *Automorphism groups of semidirect products*, Archiv der Math. **91** (2008), 193-198 και H. Mousavi & A. Somali: *Central automorphisms of semidirect products*, Bull. Malaysian Math. Sci. Soc. (2) **36** (2013), No. 3, 709-716.

[114] Βλ. J.Dietz: *Automorphism groups of semi-direct products*, Communications in Algebra **40** (2012), 3308-3316.

7.7 ΟΜΑΔΕΣ ΤΑΞΕΩΣ ≤ 15

Άπαξ και έχουμε στη διάθεσή μας τα τεχνικά μέσα τού ευθέος και ημιευθέος γινομένου, είναι δυνατόν να επεκτείνουμε την ταξινόμηση όλων των ομάδων τάξεως ≤ 7 (τού θεωρήματος 4.1.38) στην ταξινόμηση όλων των ομάδων τάξεως ≤ 15. Προς τούτο, λόγω τής προεργασίας που έχει μεσολαβήσει στα προηγούμενα κεφάλαια, αρκεί να συμπληρωθεί καταλλήλως η ταξινόμηση των ομάδων τάξεως 8 (που έχει ήδη ξεκινήσει με το θεώρημα 4.1.39) και να γίνει *καθ' ολοκληρίαν* η ταξινόμηση των ομάδων τάξεως 12. Σημειωτέον ότι για την ταξινόμηση των ομάδων τάξεως 12, που είναι, όπως θα δούμε ευθύς αμέσως, η πλέον σύνθετη, δεν είναι απαραίτητο να χρησιμοποιηθούν τα θεωρήματα τού Sylow τού κεφαλαίου 11. Αντ' αυτών είναι αρκετό να χρησιμοποιηθούν τα λήμματα 7.7.3, 7.7.4 και 7.7.5, οι αποδείξεις των οποίων στηρίζονται μόνον στην πρόταση 5.4.17, στην εξίσωση κλάσεων συζυγίας (5.64), στο θεώρημα 5.7.1 τού Cauchy και στο τέχνασμα 4.4.23 τού Poincaré.

► **Ομάδες τάξεως** 8. Για τον πλήρη προσδιορισμό αυτών αρκεί να λάβουμε υπ' όψιν το ακόλουθο λήμμα:

7.7.1 Λήμμα. (Ταξινόμηση αβελιανών ομάδων τάξεως 8.**)** *Κάθε αβελιανή ομάδα τάξεως* 8 *είναι είτε κυκλική είτε ισόμορφη με μία εκ των* $\mathbb{Z}_4 \oplus \mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

ΑΠΟΔΕΙΞΗ. Έστω $(G, \cdot)$ μια αβελιανή ομάδα τάξεως 8 και έστω $g \in G$. Από το πόρισμα 4.1.27 έπεται ότι $\text{ord}(g) = |\langle g \rangle| \in \{1, 2, 4, 8\}$. Εάν $\text{ord}(g) = 8$, τότε $G = \langle g \rangle \cong \mathbb{Z}_8$. (Βλ. 2.4.23 (ii).) Εάν αυτό δεν συμβαίνει, τότε οι τάξεις *όλων* των στοιχείων τής G είναι ≤ 4 και καταφεύγουμε στην ακόλουθη κατά περίπτωση εξέταση τής μορφής των στοιχείων τής G.

Περίπτωση πρώτη: $\exists x \in G \setminus \{e_G\} : \text{ord}(x) = 4$. 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 $y \in G \setminus \langle x \rangle$. 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 $yxy^{-1} \in \{x, x^3\}$.

(a) Το ενδεχόμενο να έχουμε $yxy^{-1} = x^3$ αποκλείεται, διότι η ισχύς αυτής τής ισότητας θα σήμαινε ότι

$$yxy^{-1} = x^3 = x^{-1} \Rightarrow yx^{-1}y^{-1} = (yxy^{-1})^{-1} = x \Rightarrow xy = yx^{-1}.$$

Επειδή η G είναι εξ υποθέσεως αβελιανή, $xy = yx^{-1} = yx \Rightarrow x^2 = e_G$, πράγμα αδύνατο, αφού $\text{ord}(x) = 4$.

(b) Η ισότητα $yxy^{-1} = x$ (ή, ισοδυνάμως, η $xy = yx$) είναι πάντοτε αληθής (διότι η G είναι εξ υποθέσεως αβελιανή) και η απεικόνιση

$$G \longrightarrow \mathbb{Z}_4 \oplus \mathbb{Z}_2,\ x^i y^j \longmapsto ([i]_4, [j]_2),\ \forall (i,j) \in \{0,1,2,3\} \times \{0,1\}$$

αποτελεί έναν ισομορφισμό ομάδων, οπότε $G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2$.

Περίπτωση δεύτερη: Όλα τα στοιχεία τα ανήκοντα στη διαφορά $G \smallsetminus \{e_G\}$ έχουν τάξη 2. Εν τοιαύτη περιπτώσει, επιλέγουμε τρία σαφώς διακεκριμένα στοιχεία $x, y, z \in G \smallsetminus \{e_G\}$, ούτως ώστε να ισχύει $xy \neq z$. Η υποομάδα $H := \{e_G, x, y, xy\}$ τής G είναι ισόμορφη τής $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, καθόσον η απεικόνιση

$$H \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2,\ x^i y^j \longmapsto ([i]_2, [j]_2),\ \forall (i,j) \in \{0,1\} \times \{0,1\}$$

είναι προδήλως ένας ισομορφισμός. Εν συνεχεία, θέτουμε $K := \langle z \rangle$ (με $K \cong \mathbb{Z}_2$) και παρατηρούμε ότι $H \cap K = \{e_G\}$ και[115]

$$G \smallsetminus H = \{z, xz, yz, xyz\} \Rightarrow G = \{e_G, x, y, xy, z, xz, yz, xyz\} = HK.$$

Σύμφωνα με το θεώρημα 7.1.26 και το (ii) τού θεωρήματος 7.1.43 έχουμε

$$G = H \times_{\text{εσ.}} K \cong H \times K \underset{\text{7.1.55 (v)}}{\cong} (\mathbb{Z}_2 \oplus \mathbb{Z}_2) \oplus \mathbb{Z}_2 \underset{\text{7.1.55 (iii)}}{\cong} \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

και η απόδειξη λήγει εδώ. □

7.7.2 Θεώρημα. (Ταξινόμηση ομάδων τάξεως 8.) *Κάθε ομάδα τάξεως* 8 *είναι ισόμορφη με μία εκ των* $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbf{D}_4$, $\mathbf{Q}$.

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το λήμμα 7.7.1 και το θεώρημα 4.1.39. □

► **Ομάδες τάξεως** 12. Για τον πλήρη προσδιορισμό αυτών (βλ. θεώρημα 7.7.6) αρκεί να λάβουμε υπ' όψιν ότι όχι μόνον η $\mathfrak{A}_4$ (βλ. 7.6.49) αλλά *και καθεμιά των υπολοίπων ομάδων* τάξεως 12 (που δεν είναι ισόμορφες με την $\mathfrak{A}_4$) μπορεί να παρασταθεί ως εσωτερικό ημιευθύ γινόμενο κατάλληλων υποομάδων της (και να εφαρμόσουμε τη μέθοδο την προταθείσα στο εδάφιο 7.6.57 (ii)).

7.7.3 Λήμμα. $|Z(G)| \in \{1,2,3\}$ *για κάθε μη αβελιανή ομάδα* G *τάξεως* 12.

ΑΠΟΔΕΙΞΗ. Έστω G τυχούσα μη αβελιανή ομάδα με ακριβώς 12 στοιχεία. Τότε $Z(G) \lhd G$ και (λόγω τού θεωρήματος 4.1.22 τού Lagrange) $|Z(G)| \in \{1,2,3,4,6\}$. Εάν ίσχυε $|Z(G)| \in \{4,6\}$, τότε η τάξη τής πηλικοομάδας $G/Z(G)$ θα ήταν ίση είτε με 3 είτε με 2, οπότε η $G/Z(G)$ θα ήταν κυκλική και η G αβελιανή (λόγω τής προτάσεως 5.4.17), και θα καταλήγαμε σε άτοπο. □

7.7.4 Λήμμα. *Κάθε ομάδα τάξεως* 12 *έχει τουλάχιστον μία υποομάδα τάξεως* 4.

[115] Εξ υποθέσεως, $z \notin H \cup \{xz, yz, xyz\}$ και η ισότητα $H \cap K = \{e_G\}$ είναι προφανής. Επιπλέον, έχουμε $z \neq x = x^{-1} \Rightarrow xz \neq e_G$, $z \neq e_G \Rightarrow xz \neq x$, $z \neq xy = x^{-1}y \Rightarrow xz \neq y$, $z \neq y \Rightarrow xz \neq xy$, $x \neq e_G \Rightarrow xz \neq z$, $x \neq y \Rightarrow xz \neq yz$, $e_G \neq y \Rightarrow x \neq xy \Rightarrow xz \neq xyz$, οπότε $xz \notin H \cup \{z, yz, xyz\}$. Παρομοίως, $yz \notin H \cup \{z, xz, xyz\}$ και $xyz \notin H \cup \{z, xz, yz\}$.

ΑΠΟΔΕΙΞΗ. Έστω $(G,\cdot)$ μια ομάδα με ακριβώς 12 στοιχεία.

Περίπτωση πρώτη. Εάν η G είναι αβελιανή, τότε ο ισχυρισμός είναι αληθής δυνάμει τού θεωρήματος 4.4.22 (διότι $4 \mid 12$).

Περίπτωση δεύτερη. Εάν η G είναι μη αβελιανή και τα $x_1,...,x_m$ είναι εκπρόσωποι εκείνων των σαφώς διακεκριμένων κλάσεων συζυγίας που δεν περιέχονται στο κέντρο της, τότε η εξίσωση κλάσεων συζυγίας (5.64) γράφεται ως εξής:

$$12 = |Z(G)| + \sum_{j=1}^{m} |G : \mathrm{C}_G(x_j)| = |Z(G)| + \sum_{j=1}^{m} \frac{12}{|\mathrm{C}_G(x_j)|},$$

απλοποιούμενη έτι περαιτέρω μέσω τού λήμματος 7.7.3:

$$\sum_{j=1}^{m} \frac{12}{|\mathrm{C}_G(x_j)|} = \begin{cases} 11, & \text{όταν } |Z(G)| = 1, \\ 10, & \text{όταν } |Z(G)| = 2, \\ 9, & \text{όταν } |Z(G)| = 3. \end{cases} \tag{7.97}$$

Σημειωτέον ότι $x_j \notin Z(G) \Rightarrow |G : \mathrm{C}_G(x_j)| > 1 \Rightarrow |\mathrm{C}_G(x_j)| < 12$, οπότε

$$|G : \mathrm{C}_G(x_j)| \in \{2,3,4,6,12\},\ \forall j \in \{1,...,m\}. \tag{7.98}$$

Εάν υποθέσουμε ότι για κάθε $j \in \{1,...,m\}$ ισχύει $2 \mid |G : \mathrm{C}_G(x_j)|$, τότε το άθροισμα τού αριστερού μέλους τής (7.97) (ως άρτιος θετικός ακέραιος) ισούται κατ' ανάγκην με 10 και $|Z(G)| = 2 \Rightarrow \mathbb{Z}_2 \cong Z(G) \lhd G$. Ως εκ τούτου, ορίζεται η πηλικοομάδα $G/Z(G)$ τάξεως $|G/Z(G)| = 6$. Μάλιστα[116], $G/Z(G) \cong \mathfrak{S}_3$. Προφανώς, υπάρχει κάποια υποομάδα L τής $G/Z(G)$ τάξεως 2. Το πόρισμα 4.4.15 μας πληροφορεί ότι η L οφείλει να είναι τής μορφής $L = K/Z(G)$, για κάποια υποομάδα K τής G που περιέχει την $Z(G)$. Επομένως,

$$2 = |L| = |K/Z(G)| = \frac{|K|}{|Z(G)|} = \frac{|K|}{2} \Rightarrow |K| = 4$$

και ο αρχικός ισχυρισμός είναι προδήλως αληθής. Από την άλλη μεριά, εάν

$$\exists j_0 \in \{1,...,m\} : 2 \nmid |G : \mathrm{C}_G(x_{j_0})|,$$

τότε η (7.98) δίδει $|G : \mathrm{C}_G(x_{j_0})| = 3 \Longrightarrow |\mathrm{C}_G(x_{j_0})| = 4$, και η (7.97) γράφεται ως ακολούθως:

$$\sum_{j \in \{1,...,m\} \setminus \{j_0\}} \frac{12}{|\mathrm{C}_G(x_j)|} = \begin{cases} 8, & \text{όταν } |Z(G)| = 1, \\ 7, & \text{όταν } |Z(G)| = 2, \\ 6, & \text{όταν } |Z(G)| = 3. \end{cases} \tag{7.99}$$

Η (7.99) είναι δυνατόν να διαθέτει λύσεις (π.χ., $2+2+2+2 = 8$ για $m = 5$ και $2+2+3 = 7$ και $2+2+2 = 6$ για $m = 4$), οπότε *και* σε αυτήν την περίπτωση η $K := \mathrm{C}_G(x_{j_0})$ είναι μια προσήκουσα υποομάδα τής G (τάξεως 4). □

[116] Υπάρχουν δύο ενδεχόμενα: Είτε $G/Z(G) \cong \mathfrak{S}_3$ είτε $G/Z(G) \cong \mathbb{Z}_6$. (Βλ. θεώρημα 4.1.37.) Το δεύτερο αποκλείεται, διότι η G υπετέθη ότι είναι μη αβελιανή. (Βλ. 5.4.17.)

7.7.5 Λήμμα. *Κάθε ομάδα τάξεως* 12 *που δεν είναι ισόμορφη με την* $\mathfrak{A}_4$ *περιέχει τουλάχιστον μία ορθόθετη υποομάδα τάξεως* 3.

ΑΠΟΔΕΙΞΗ. Έστω $(G,\cdot)$ μια ομάδα τάξεως 12 με $G \ncong \mathfrak{A}_4$. Κατά το θεώρημα τού Cauchy (βλ. 5.7.1), $\exists g \in G : |\langle g\rangle| = 3$ (διότι το 3 είναι πρώτος και διαιρεί το 12). Η ομάδα $H := \langle g\rangle$ είναι κυκλική και έχει δείκτη $|G:H| = 4$ εντός τής G. Έστω $\{g_1H, g_2H, g_3H, g_4H\}$ τυχόν σύστημα αριστερών εκπροσώπων τής H εντός τής G. Σύμφωνα με το θεώρημα 4.4.23, ορίζεται ένας ομομορφισμός

$$\Theta_H : G \longrightarrow \mathfrak{S}_{\{g_1H,g_2H,g_3H,g_4H\}} \cong \mathfrak{S}_4,\ \ x \longmapsto \Theta_H(x) := \sigma_x,$$

με $\sigma_x(g_jH) := xg_jH$, $\forall j \in \{1,2,3,4\}$, για τον οποίο ισχύει $\mathrm{Ker}(\Theta_H) \sqsubseteq H$. Επειδή η H έχει τάξη 3, έχουμε είτε $\mathrm{Ker}(\Theta_H) = \{e_G\}$ είτε $\mathrm{Ker}(\Theta_H) = H$. Εάν ίσχυε η ισότητα $\mathrm{Ker}(\Theta_H) = \{e_G\}$, τότε η Θ_H θα ήταν μονομορφισμός και η $G\,(\cong \mathrm{Im}(\Theta_H))$ θα εμφυτευόταν εντός τής $\mathfrak{S}_4$. Τούτο όμως θα οδηγούσε σε άτοπο, διότι ο δείκτης της εντός τής $\mathfrak{S}_4$ θα ήταν 2, οπότε αυτή (βάσει τής προτάσεως 4.2.13) θα όφειλε να είναι ορθόθετη υποομάδα. (Ως γνωστόν, η μόνη ορθόθετη υποομάδα τής $\mathfrak{S}_4$ τάξεως 12 είναι η $\mathfrak{A}_4$. Βλ. λήμμα 6.3.15.) Επομένως, $\mathrm{Ker}(\Theta_H) = H \underset{4.2.31}{\lhd} G$. □

7.7.6 Θεώρημα. (Ταξινόμηση ομάδων τάξεως 12.**)**
Έστω $(G,\cdot)$ *μια ομάδα τάξεως* 12. *Τότε ισχύουν τα εξής:*

(i) *Εάν η* G *είναι αβελιανή, τότε είτε* $G \cong \mathbb{Z}_{12}$ *είτε* $G \cong \mathbb{Z}_3 \times \mathbf{V} \cong \mathbb{Z}_3 \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_2)$.

(ii) *Εάν η* G *είναι μη αβελιανή, τότε είναι ισόμορφη είτε με την εναλλάσσουσα ομάδα* $\mathfrak{A}_4$ *είτε με τη διεδρική ομάδα* $\mathbf{D}_6$ *είτε με τη δικυκλική ομάδα* $\mathbf{Dic}_3$ (βλ. 7.6.29).
(Αυτές είναι ανά δύο μη ισόμορφες.)

ΑΠΟΔΕΙΞΗ. Έστω $(G,\cdot)$ μια ομάδα τάξεως 12 που *δεν είναι* ισόμορφη με την εναλλάσσουσα ομάδα $\mathfrak{A}_4$.Μέσω των λημμάτων 7.7.4 και 7.7.5 εξασφαλίζεται η ύπαρξη μιας $H \in \mathbf{NSubg}(G)$ τάξεως 3 και μιας $K \in \mathbf{Subg}(G)$ τάξεως 4. Από το θεώρημα 7.6.46 έπεται ότι $G = H \rtimes K$. Επειδή (δυνάμει τού (ii) τού θεωρήματος 2.4.23 και τού θεωρήματος 3.5.6) ισχύει $H \cong \mathbb{Z}_3$ και *είτε* $K \cong \mathbb{Z}_4$ *είτε* $K \cong \mathbf{V} \underset{7.1.67}{\cong} \mathbb{Z}_2 \oplus \mathbb{Z}_2$, συνάγεται ότι

$$\text{είτε } \exists\varphi \in \mathrm{Hom}(\mathbb{Z}_4,\ \mathrm{Aut}(\mathbb{Z}_3)) : G \cong \mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4,$$

$$\text{είτε } \exists\varphi \in \mathrm{Hom}(\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathrm{Aut}(\mathbb{Z}_3)) : G \cong \mathbb{Z}_3 \rtimes_\varphi (\mathbb{Z}_2 \oplus \mathbb{Z}_2),$$

όπου $\mathrm{Aut}(\mathbb{Z}_3) = \{\mathrm{id}_{\mathbb{Z}_3}, \vartheta\}$, με $\vartheta([0]_3) := [0]_3$, $\vartheta([1]_3) := [2]_3$, $\vartheta([2]_3) := [1]_3$. (Πρβλ. 7.6.57 (ii).) Στην πρώτη περίπτωση ο φ είναι *είτε* ο τετριμμένος ομομορφισμός ($\varphi_{[j]_4} = \mathrm{id}_{\mathbb{Z}_3}$, $\forall j \in \mathbb{Z}$), οπότε $G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_4 \cong \mathbb{Z}_{12}$, *είτε* αυτός για τον οποίο ισχύει $\varphi_{[j]_4} = \vartheta^j$, $\forall j \in \mathbb{Z}$, οπότε η εσωτερική πράξη επί τού $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$ είναι η

$$([i_1]_3,[j_1]_4)([i_2]_3,[j_2]_4) := ([i_1]_3 + \underbrace{\varphi_{[j_1]_4}([i_2]_3)}_{=\vartheta^{j_1}([i_2]_3)}, [j_1+j_2]_4)$$

για οιουσδήποτε $i_1, j_1, i_2, j_2 \in \mathbb{Z}$ και $G \cong \mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4 = \langle \mathfrak{u}\rangle\langle \mathfrak{s}\rangle = \langle \mathfrak{s}, \mathfrak{u}\rangle$, όπου $\mathfrak{u} := ([1]_3,[0]_4)$ και $\mathfrak{s} := ([0]_3,[1]_4)$. Σημειωτέον ότι

$$\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4 = \left\{\mathfrak{u}^i\,\mathfrak{s}^j \,\middle|\, (i,j) \in \{0,1,2\} \times \{0,1,2,3\} \text{ και } \mathfrak{s}\mathfrak{u} = \mathfrak{u}^2\mathfrak{s}\right\},$$

διότι $\mathfrak{s}^j = ([0]_3, [1]_4)^j = ([0]_3, [j]_4)$ και

$$\begin{aligned}
&\mathfrak{u}^2 = ([1]_3, [0]_4)([1]_3, [0]_4) = ([1]_3 + \vartheta^0([1]_3), [0]_4) = ([1]_3 + [1]_3, [0]_4) = ([2]_3, [0]_4),\\
&\mathfrak{u}^3 = ([2]_3, [0]_4)([1]_3, [0]_4) = ([2]_3 + \vartheta^0([1]_3), [0]_4) = ([3]_3, [0]_4) = ([0]_3, [0]_4) = e_{\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4},\\
&\mathfrak{su} = ([0]_3, [1]_4)([1]_3, [0]_4) = ([0]_3 + \vartheta([1]_3), [1]_4) = ([2]_3, [1]_4)\\
&= ([2]_3 + [0]_3, [1]_4) = ([2]_3 + \vartheta^0([0]_3), [1]_4) = ([2]_3, [0]_4)([0]_3, [1]_4) = \mathfrak{u}^2\mathfrak{s}.
\end{aligned}$$

Μεταβαίνοντας από το σύστημα γεννητόρων $\{\mathfrak{s}, \mathfrak{u}\}$ τής $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$ στο $\{\mathfrak{s}, \mathfrak{t}\}$, όπου $\mathfrak{t} := \mathfrak{us}^2$, λαμβάνουμε

$$\begin{aligned}
\mathfrak{t}^3 &= (\mathfrak{us}^2)^3 = \mathfrak{us}(\mathfrak{su})\mathfrak{s}^2\mathfrak{us}^2 = \mathfrak{us}(\mathfrak{u}^2\mathfrak{s})\mathfrak{s}^2\mathfrak{us}^2 = \mathfrak{u}(\mathfrak{su})\mathfrak{us}^3\mathfrak{us}^2\\
&= \mathfrak{u}(\mathfrak{u}^2\mathfrak{s})\mathfrak{us}^3\mathfrak{us}^2 = (\mathfrak{su})\mathfrak{s}^3\mathfrak{us}^2 = (\mathfrak{u}^2\mathfrak{s})\mathfrak{s}^3\mathfrak{us}^2 = \mathfrak{u}^2\mathfrak{us}^2 = \mathfrak{s}^2
\end{aligned}$$

και $\mathfrak{t}^6 = \left(\mathfrak{t}^3\right)^2 = (\mathfrak{s}^2)^2 = e_{\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4}$,

$$\begin{aligned}
&\mathfrak{tst} = (\mathfrak{us}^2)\mathfrak{s}(\mathfrak{us}^2) = (\mathfrak{us}^2)(\mathfrak{su})\mathfrak{s}^2 = (\mathfrak{us}^2)(\mathfrak{u}^2\mathfrak{s})\mathfrak{s}^2 = (\mathfrak{us})(\mathfrak{su})\mathfrak{us}^3\\
&= (\mathfrak{us})(\mathfrak{u}^2\mathfrak{s})\mathfrak{us}^3 = \mathfrak{u}(\mathfrak{su})(\mathfrak{us})\mathfrak{us}^3 = \mathfrak{u}(\mathfrak{u}^2\mathfrak{s})(\mathfrak{us})\mathfrak{us}^3 = (\mathfrak{su})\,(\mathfrak{su})\,\mathfrak{s}^3 = (\mathfrak{su})^2\mathfrak{s}^3\\
&= (\mathfrak{u}^2\mathfrak{s})^2\mathfrak{s}^3 = (\mathfrak{u}^2\mathfrak{s})(\mathfrak{u}^2\mathfrak{s})\mathfrak{s}^3 = (\mathfrak{u}^2\mathfrak{s})\mathfrak{u}^2 = (\mathfrak{su})\mathfrak{u}^2 = \mathfrak{s} \Longrightarrow \mathfrak{ts} = \mathfrak{st}^{-1},
\end{aligned}$$

οπότε η πρόταση 7.6.33 μας πληροφορεί ότι

$$G \cong \mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4 = \langle \mathfrak{s}, \mathfrak{t} \rangle \cong \mathbf{Dic}_3 \;\; (\text{αφού} \;\; |\langle \mathfrak{s}, \mathfrak{t} \rangle| = 12).$$

Στη δεύτερη περίπτωση,

$$\begin{aligned}
&\mathrm{Hom}(\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathrm{Aut}(\mathbb{Z}_3)) \cong \mathrm{Hom}(\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_2)\\
&\cong \mathrm{Hom}(\mathbb{Z}_2,\ \mathbb{Z}_2) \oplus \mathrm{Hom}(\mathbb{Z}_2,\ \mathbb{Z}_2) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2
\end{aligned}$$

και, συγκεκριμένα, $\mathrm{Hom}(\mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathrm{Aut}(\mathbb{Z}_3)) = \{\varphi, \varphi', \varphi'', \varphi'''\}$, όπου ο φ είναι ο τετριμμένος ομομορφισμός ($\varphi_{([j_1]_4, [j_2]_4)} = \mathrm{id}_{\mathbb{Z}_3}, \forall (j_1, j_2) \in \mathbb{Z} \times \mathbb{Z}$), οπότε

$$\mathbb{Z}_3 \rtimes_\varphi (\mathbb{Z}_2 \oplus \mathbb{Z}_2) = \mathbb{Z}_3 \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_2) \cong \mathbb{Z}_3 \times \mathbf{V},$$

και $\varphi'_{([0]_2, [0]_2)} = \varphi''_{([0]_2, [0]_2)} = \varphi'''_{([0]_2, [0]_2)} = \mathrm{id}_{\mathbb{Z}_3}$,

$$\begin{array}{l|l|l}
\varphi'_{([1]_2, [0]_2)} := \mathrm{id}_{\mathbb{Z}_3}, & \varphi''_{([1]_2, [0]_2)} := \vartheta, & \varphi'''_{([1]_2, [0]_2)} := \vartheta,\\
\varphi'_{([0]_2, [1]_2)} := \vartheta, & \varphi''_{([0]_2, [1]_2)} := \mathrm{id}_{\mathbb{Z}_3}, & \varphi'''_{([0]_2, [1]_2)} := \vartheta,\\
\varphi'_{([1]_2, [1]_2)} := \vartheta, & \varphi''_{([1]_2, [1]_2)} := \vartheta, & \varphi'''_{([1]_2, [1]_2)} := \mathrm{id}_{\mathbb{Z}_3}.
\end{array}$$

Ορίζουμε αυτομορφισμούς $\omega, \omega', \omega'' \in \mathrm{Aut}(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$ ως ακολούθως:

$$\begin{array}{l|l|l}
\omega([0]_2, [0]_2) := ([0]_2, [0]_2) & \omega'([0]_2, [0]_2) := ([0]_2, [0]_2), & \omega''([0]_2, [0]_2) := ([0]_2, [0]_2),\\
\omega([1]_2, [0]_2) := ([0]_2, [1]_2), & \omega'([1]_2, [0]_2) := ([1]_2, [0]_2), & \omega''([1]_2, [0]_2) := ([1]_2, [1]_2),\\
\omega([0]_2, [1]_2) := ([1]_2, [0]_2), & \omega'([0]_2, [1]_2) := ([1]_2, [1]_2), & \omega''([0]_2, [1]_2) := ([0]_2, [1]_2),\\
\omega([1]_2, [1]_2) := ([1]_2, [1]_2, & \omega'([1]_2, [1]_2) := ([0]_2, [1]_2), & \omega''([1]_2, [1]_2) := ([1]_2, [0]_2).
\end{array}$$

Εκ κατασκευής, $\varphi' \circ \omega = \varphi''$, $\varphi'' \circ \omega' = \varphi'''$ και $\varphi''' \circ \omega'' = \varphi'$.

Από την πρόταση 7.6.7 συμπεραίνουμε ότι

$$\mathbb{Z}_3 \rtimes_{\varphi'} (\mathbb{Z}_2 \oplus \mathbb{Z}_2) \cong \mathbb{Z}_3 \rtimes_{\varphi''} (\mathbb{Z}_2 \oplus \mathbb{Z}_2) \cong \mathbb{Z}_3 \rtimes_{\varphi'''} (\mathbb{Z}_2 \oplus \mathbb{Z}_2).$$

Επειδή η εσωτερική πράξη επί τής (μη αβελιανής) $\mathbb{Z}_3 \rtimes_{\varphi'} (\mathbb{Z}_2 \oplus \mathbb{Z}_2)$ είναι η

$$([i_1]_3, ([j_1]_2, [k_1]_2))([i_2]_3, ([j_2]_2, [k_2]_2)) := ([i_1]_3 + \varphi'_{([j_1]_2,[k_1]_2)}([i_2]_3), ([j_1 + j_2]_2, [k_1 + k_2]_2)),$$

για οιουσδήποτε $i_1, j_1, k_1, i_2, j_2, k_2 \in \mathbb{Z}$, θέτοντας

$$u := ([1]_3, ([0]_2, [0]_2)),\ s_1 := ([0]_3, ([1]_2, [0]_2)) \text{ και } s_2 := ([0]_3, ([0]_2, [1]_2))$$

διαπιστώνουμε ότι

$$\begin{aligned}\mathbb{Z}_3 \rtimes_{\varphi'} (\mathbb{Z}_2 \oplus \mathbb{Z}_2) &= \langle u, s_1, s_2\rangle = \langle u\rangle\langle s_1, s_2\rangle = \langle s_1, s_2\rangle\langle u\rangle\\ &= \left\{ s_1^\nu s_2^\xi u^\varrho \;\middle|\; \begin{array}{c}(\nu, \xi, \varrho) \in \{0,1\}\times\{0,1\}\times\{0,1,2,3\}\\ \text{και } s_1u = us_1,\ s_2u = u^2s_2\end{array} \right\},\end{aligned}$$

καθώς έχουμε

$$\begin{aligned}&s_1^2 = ([0]_3, ([1]_2, [0]_2))^2 = ([0]_3 + \varphi'_{([1]_2,[0]_2)}([0]_3), ([2]_2, [0]_2))\\ &= ([0]_3, ([0]_2, [0]_2)) = e_{\mathbb{Z}_3\rtimes_{\varphi'}(\mathbb{Z}_2\oplus\mathbb{Z}_2)} = s_2^2 = (s_1s_2)^2,\\ &u^2 = ([1]_3, ([0]_2, [0]_2))^2 = ([1]_3 + \varphi'_{([0]_2,[0]_2)}([1]_3), ([0]_2, [0]_2)) = ([2]_3, ([0]_2, [0]_2)),\\ &u^3 = ([1]_3, ([0]_2, [0]_2))([2]_3, ([0]_2, [0]_2)) = ([3]_3, ([0]_2, [0]_2)) = ([0]_3, ([0]_2, [0]_2)),\end{aligned}$$

και

$$\begin{aligned}&s_1u = ([0]_3, ([1]_2, [0]_2))([1]_3, ([0]_2, [0]_2)) = ([0]_3 + \varphi'_{([1]_2,[0]_2)}([1]_3), ([1]_2, [0]_2))\\ &= ([1]_3, ([1]_2, [0]_2)) = ([1]_3 + \varphi'_{([0]_2,[0]_2)}([0]_3), ([1]_2, [0]_2))\\ &= ([1]_3, ([0]_2, [0]_2))([0]_3, ([1]_2, [0]_2)) = us_1,\\ &s_2u = ([0]_3, ([0]_2, [1]_2))([1]_3, ([0]_2, [0]_2)) = ([0]_3 + \varphi'_{([0]_2,[1]_2)}([1]_3), ([0]_2, [1]_2))\\ &= ([2]_3, ([0]_2, [1]_2)) = ([2]_3 + \varphi'_{([0]_2,[0]_2)}([0]_3), ([0]_2, [1]_2))\\ &= ([2]_3, ([0]_2, [0]_2))([0]_3, ([0]_2, [1]_2)) = u^2s_2.\end{aligned}$$

Μεταβαίνοντας από το σύστημα γεννητόρων $\{s_1, s_2, u\}$ τής $\mathbb{Z}_3 \rtimes_{\varphi'} (\mathbb{Z}_2 \oplus \mathbb{Z}_2)$ στο[117] $\{s, t\}$, όπου $s := s_1s_2\ (= s_2s_1)$ και $t := us_1$, λαμβάνουμε $s^2 = e_{\mathbb{Z}_3\rtimes_{\varphi'}(\mathbb{Z}_2\oplus\mathbb{Z}_2)}$,

$$\begin{aligned}&t^2 = (us_1)^2 = u(s_1u)s_1 = u^2,\ t^3 = u^2(us_1) = s_1,\ t^4 = u^4 = u,\\ &t^5 = tu = (us_1)u = s_1u^2,\ t^6 = (t^3)^2 = s_1^2 = e_{\mathbb{Z}_3\rtimes_{\varphi'}(\mathbb{Z}_2\oplus\mathbb{Z}_2)},\\ &ts = (us_1)(s_1s_2) = us_1^2s_2 = us_2 = u(u^2s_2u^{-1}) = s_2u^{-1} = s_2u^2\\ &= s_1^2s_2u^2 = s_1(s_1s_2)u^2 = s_1(s_2s_1)u^2 = s(s_1u^2) = st^5 = st^{-1}.\end{aligned}$$

Κατά την πρόταση 3.4.7, $\mathbb{Z}_3 \rtimes_{\varphi'} (\mathbb{Z}_2 \oplus \mathbb{Z}_2) = \langle s, t\rangle \cong \mathbf{D}_6$. Άρα όταν η G είναι μη αβελιανή, *είτε* $G \cong \mathbf{Dic}_3$ *είτε* $G \cong \mathbf{D}_6$. Η απόδειξη λήγει παρατηρώντας ότι[118] $\mathbf{Dic}_3 \ncong \mathbf{D}_6$, καθόσον η $\langle \mathfrak{s}, \mathfrak{t}\rangle \cong \mathbf{Dic}_3$ διαθέτει 6 στοιχεία τάξεως 4 (συγκεκριμένα, τα $\mathfrak{s}, \mathfrak{s}^3, \mathfrak{ts}, \mathfrak{ts}^3, \mathfrak{t}^2\mathfrak{s}, \mathfrak{t}^2\mathfrak{s}^3$), ενώ η $\mathbf{D}_6$ δεν περιέχει κανένα στοιχείο[119] τάξεως 4. □

[117] Προφανώς, $s \in \langle u, s_1, s_2\rangle$ και $t \in \langle u, s_1, s_2\rangle$. Από την άλλη μεριά, $s_1 = t^3 \in \langle s, t\rangle$, $s_2 = st^3 \in \langle s, t\rangle$ και $u = t^4 \in \langle s, t\rangle$. Επομένως, $\langle u, s_1, s_2\rangle = \langle s, t\rangle = \mathbb{Z}_3 \rtimes_{\varphi'} (\mathbb{Z}_2 \oplus \mathbb{Z}_2)$.

[118] Το ότι καμία εκ των $\mathbf{Dic}_3, \mathbf{D}_6$ δεν είναι ισόμορφη με την $\mathfrak{A}_4$ είναι προφανές (αφού καμία εκ των τεσσάρων υποομάδων τής $\mathfrak{A}_4$ που έχουν τάξη 3 δεν είναι ορθόθετη).

[119] Ως γνωστόν, η $\mathbf{D}_6$ απαρτίζεται από το ουδέτερό της στοιχείο, 7 στοιχεία τάξεως 2, 2 στοιχεία τάξεως 3 και 2 στοιχεία τάξεως 6. (Πρβλ. τον κατάλογο στο εδ. 5.1.10 (ii).)

► **Ομάδες τάξεως** ≤ 15. Συλλέγοντας τώρα τα μέχρι στιγμής αποδειχθέντα, καταλήγουμε στο ακόλουθο:

7.7.7 Θεώρημα. (Ταξινόμηση ομάδων τάξεως ≤ 15.) *Η ταξινόμηση των ομάδων* G *με* $|G| \leq 15$ *μέχρις ισομορφισμού είναι αυτή που καταχωρίζεται στον εξής κατάλογο*:

Τάξη	Αβελιανές G	Μη αβελιανές G	Βλ. εδ.
1	τετριμμένη	——	2.4.24
2	$\mathbb{Z}_2$	——	4.1.33, 2.4.23
3	$\mathbb{Z}_3$	——	4.1.33, 2.4.23
4	$\mathbb{Z}_4$, $\mathbf{V}$ ($\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$)	——	3.5.6, 7.1.67
5	$\mathbb{Z}_5$	——	4.1.33, 2.4.23
6	$\mathbb{Z}_6$	$\mathbf{D}_3$ ($\cong \mathfrak{S}_3$)	4.1.37
7	$\mathbb{Z}_7$	——	4.1.33, 2.4.23
8	$\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	$\mathbf{D}_4$, $\mathbf{Q}$	7.7.2
9	$\mathbb{Z}_9$, $\mathbb{Z}_3 \oplus \mathbb{Z}_3$	——	7.1.46, 7.1.47
10	$\mathbb{Z}_{10}$	$\mathbf{D}_5$	5.7.18
11	$\mathbb{Z}_{11}$	——	4.1.33, 2.4.23
12	$\mathbb{Z}_{12}$, $\mathbb{Z}_3 \times \mathbf{V}$ ($\cong \mathbb{Z}_3 \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_2)$)	$\mathfrak{A}_4$, $\mathbf{D}_6$, $\mathbf{Dic}_3$	7.7.6
13	$\mathbb{Z}_{13}$	——	4.1.33, 2.4.23
14	$\mathbb{Z}_{14}$	$\mathbf{D}_7$	5.7.18
15	$\mathbb{Z}_{15}$	——	5.7.11, 2.4.23

7.8 ΣΤΕΦΑΝΙΑΙΑ ΓΙΝΟΜΕΝΑ

Έστω I ένα (όχι κατ' ανάγκην πεπερασμένο) σύνολο με $\mathrm{card}(I) \geq 2$ και έστω $(G, \cdot)$ τυχούσα ομάδα. Θεωρούμε τόσον το περιορισμένο εξωτερικό ευθύ γινόμενο $G^{(I)}$ όσον και το απεριόριστο εξωτερικό ευθύ γινόμενο G^I τής οικογενείας ομάδων με δείκτες ειλημμένους από το I, καθεμιά εκ των οποίων ισούται με την ίδια την G. (Βλ. 7.1.94 (ii).) Ταυτίζοντας κάθε στοιχείο τού $G^{(I)}$ (και αντιστοίχως, τού G^I) με μια απεικόνιση $f : I \longrightarrow G$ με πεπερασμένο φορέα (και αντιστοίχως, με μια απεικόνιση $f : I \longrightarrow G$) παρατηρούμε ότι κάθε μετάταξη $\sigma \in \mathfrak{S}_I$ τού I δίδει το έναυσμα για τον ορισμό ενός αυτομορφισμού $\vartheta_\sigma \in \mathrm{Aut}(G^{(I)})$ (και αντιστοίχως, ενός $\vartheta_\sigma \in \mathrm{Aut}(G^I)$) μέσω «μετατάξεως συντεταγμένων»[120]:

$$f \longmapsto \vartheta_\sigma(f) := f \circ \sigma^{-1}, \text{ όπου } \vartheta_\sigma(f)(i) := f(\sigma^{-1}(i)),\ \forall i \in I.$$

Για οιαδήποτε υποομάδα $K \sqsubseteq \mathfrak{S}_I$ η απεικόνιση $K \ni \sigma \overset{\vartheta}{\longmapsto} \vartheta_\sigma \in \mathrm{Aut}(G^{(I)})$ (και αντιστοίχως, η απεικόνιση $K \ni \sigma \overset{\vartheta}{\longmapsto} \vartheta_\sigma \in \mathrm{Aut}(G^I)$) αποτελεί *ομομορφισμό ομάδων*, διότι για $\sigma, \tau \in K$ και $f \in G^{(I)}$ (και αντιστοίχως, $f \in G^I$) λαμβάνουμε

$$\vartheta_{\sigma\circ\tau}(f) := f \circ (\sigma \circ \tau)^{-1} = (f \circ \tau^{-1}) \circ \sigma^{-1} = \vartheta_\tau(f) \circ \sigma^{-1} = \vartheta_\sigma(\vartheta_\tau(f)) = (\vartheta_\sigma \circ \vartheta_\tau)(f),$$

[120] Προφανώς, η ϑ_σ είναι αμφιριπτική και

$$\vartheta_\sigma(f_1 f_2) = (f_1 f_2) \circ \sigma^{-1} = (f_1 \circ \sigma^{-1})(f_2 \circ \sigma^{-1}) = \vartheta_\sigma(f_1) \circ \vartheta_\sigma(f_2)$$

για οιεσδήποτε $f_1, f_2 \in G^{(I)}$ (και αντιστοίχως, για οιεσδήποτε $f_1, f_2 \in G^I$).

οπότε $\vartheta(\sigma\circ\tau)=\vartheta_{\sigma\circ\tau}=\vartheta_\sigma\circ\vartheta_\tau=\vartheta(\sigma)\circ\vartheta(\tau)$.

7.8.1 Ορισμός. (i) Ως **περιορισμένο στεφανιαίο γινόμενο των** G **και** K (με **σύνολο δεικτών** I και **βάση** το $G^{(I)}$) ορίζεται το εξωτερικό ημιευθύ γινόμενο

$$\boxed{G\wr_I K:=G^{(I)}\rtimes_\vartheta K.}$$

(ii) Ως **απεριόριστο (ή πλήρες) στεφανιαίο γινόμενο των** G **και** K (με **σύνολο δεικτών** I και **βάση** το G^I) ορίζεται το εξωτερικό ημιευθύ γινόμενο

$$\boxed{G\wr\!\!\wr_I K:=G^I\rtimes_\vartheta K.}$$

7.8.2 Παρατήρηση. (i) Η εσωτερική πράξη επί τού $G\wr_I K$ (και αντιστοίχως, επί τού $G\wr\!\!\wr_I K$) είναι η

$$\boxed{(f_1,\sigma_1)(f_2,\sigma_2):=(f_1\vartheta_{\sigma_1}(f_2),\sigma_1\circ\sigma_2)=(f_1(f_2\circ\sigma_1^{-1}),\sigma_1\circ\sigma_2),}$$

για οιαδήποτε $\sigma_1,\sigma_2\in K$ και $f_1,f_2\in G^{(I)}$ (και αντιστοίχως, $f_1,f_2\in G^I$).

(ii) Προφανώς, $|G\wr\!\!\wr_I K|=|G|^{\mathrm{card}(I)}\,|K|$.

(ii) Εάν το I είναι πεπερασμένο, τότε $G\wr_I K=G\wr\!\!\wr_I K$.

7.8.3 Σημείωση. (Ειδική περίπτωση) Εάν ως σύνολο δεικτών θεωρήσουμε το υποκείμενο σύνολο H μιας *ομάδας* $(H,*)$, τότε ορίζουμε ως **κανονικό στεφανιαίο γινόμενο των** G **και** H το

$$\boxed{G\wr H:=G\wr_H L(H)}$$

και ως **κανονικό απεριόριστο στεφανιαίο γινόμενο των** G **και** H το

$$\boxed{G\wr\!\!\wr H:=G\wr\!\!\wr_H L(H),}$$

όπου $L(H):=\{L_h\mid h\in H\}\cong H$ η εξ αριστερών κανονική αναπαράσταση τής H εντός τής $\mathfrak{S}_H$ η εισαχθείσα στο θεώρημα 3.5.1 τού Cayley (με $L_h(x):=h*x$ για κάθε ζεύγος $(h,x)\in H\times H$). Η εσωτερική πράξη επί τού $G\wr H$ (και αντιστοίχως, επί τού $G\wr\!\!\wr H$) είναι η

$$\boxed{(f_1,L_{h_1})(f_2,L_{h_2}):=(f_1(f_2\circ L_{h_1^{-1}}),L_{h_1*h_2}),}$$

για οιαδήποτε $h_1,h_2\in H$ και $f_1,f_2\in G^{(I)}$ (και αντιστοίχως, $f_1,f_2\in G^I$).

7.8.4 Παράδειγμα. (Η $\mathbf{D_4}$ ως κανονικό στεφανιαίο γινόμενο.) Εάν $G=H=\mathbb{Z}_2$, τότε η ομάδα $\mathbb{Z}_2^{\mathbb{Z}_2}=\{f_1,f_2,f_3,f_4\}$, με $f_1:=\mathrm{id}_{\mathbb{Z}_2}$,

$$\begin{array}{c}\mathbb{Z}_2\xrightarrow{f_2}\mathbb{Z}_2,\\ [0]_2\mapsto[1]_2\\ [1]_2\mapsto[0]_2\end{array}\quad\left\|\quad\begin{array}{c}\mathbb{Z}_2\xrightarrow{f_3}\mathbb{Z}_2,\\ [0]_2\mapsto[0]_2\\ [1]_2\mapsto[0]_2\end{array}\quad\right\|\quad\begin{array}{c}\mathbb{Z}_2\xrightarrow{f_4}\mathbb{Z}_2,\\ [0]_2\mapsto[1]_2\\ [1]_2\mapsto[1]_2\end{array}$$

ως προς την πράξη $\mathbb{Z}_2^{\mathbb{Z}_2} \times \mathbb{Z}_2^{\mathbb{Z}_2} \ni (f_i, f_j) \longmapsto f_i f_j \in \mathbb{Z}_2^{\mathbb{Z}_2}$, $i, j \in \{1, 2, 3, 4\}$, όπου

$$f_i f_j([j]_2) := f_i([j]_2) + f_j([j]_2),\ \forall j \in \{0, 1\},$$

έχει ως ουδέτερο στοιχείο της $e_{\mathbb{Z}_2^{\mathbb{Z}_2}}$ την f_3, ενώ το κανονικό στεφανιαίο γινόμενο $\mathbb{Z}_2 \wr \mathbb{Z}_2$ έχει τάξη 8. Επειδή $L_{[0]_2} = \mathrm{id}_{\mathbb{Z}_2}$ και $L_{[-1]_2} = L_{[1]_2}$, για τον ομομορφισμό

$$\mathbb{Z}_2 \cong \mathfrak{S}_{\mathbb{Z}_2} \cong L(\mathbb{Z}_2) \xrightarrow{\vartheta} \mathrm{Aut}(\mathbb{Z}_2^{\mathbb{Z}_2}) \text{ με } \vartheta_{L_{[0]_2}} = \vartheta_{\mathrm{id}_{\mathbb{Z}_2}} = e_{\mathrm{Aut}(\mathbb{Z}_2^{\mathbb{Z}_2})} = \mathrm{id}_{\mathbb{Z}_2^{\mathbb{Z}_2}}$$

ισχύουν οι ισότητες

$$\vartheta_{L_{[1]_2}}(f_i)([0]_2) = (f_i \circ L_{[-1]_2})([0]_2) = (f_i \circ L_{[1]_2})([0]_2) = f_i([1]_2),$$
$$\vartheta_{L_{[1]_2}}(f_i)([1]_2) = (f_i \circ L_{[-1]_2})([1]_2) = (f_i \circ L_{[1]_2})([1]_2) = f_i([0]_2),$$

για κάθε $i \in \{1, 2, 3, 4\}$, οπότε η εσωτερική πράξη επί τού $\mathbb{Z}_2 \wr \mathbb{Z}_2$ καθορίζεται από τις

$$(f_i, L_{[0]_2})(f_j, L_{[0]_2}) := (f_i f_j, \mathrm{id}_{\mathbb{Z}_2}),$$
$$(f_i, L_{[0]_2})(f_j, L_{[1]_2}) := (f_i f_j, L_{[1]_2}),$$
$$(f_i, L_{[1]_2})(f_j, L_{[0]_2}) := (f_i(f_j \circ L_{[1]_2}), L_{[1]_2}),$$
$$(f_i, L_{[1]_2})(f_j, L_{[1]_2}) := (f_i(f_j \circ L_{[1]_2}), \mathrm{id}_{\mathbb{Z}_2}),$$

για οιουσδήποτε $i, j \in \{1, 2, 3, 4\}$, ενώ το ουδέτερο στοιχείο του είναι το

$$e_{\mathbb{Z}_2 \wr \mathbb{Z}_2} = (f_3, L_{[0]_2}) = (f_3, \mathrm{id}_{\mathbb{Z}_2}).$$

Επειδή για $i, j \in \{1, 2, 3, 4\}$ έχουμε

$$f_i f_j([0]_2) = f_i([0]_2) + f_j([0]_2),\ f_i f_j([1]_2) = f_i([1]_2) + f_j([1]_2),$$
$$f_i(f_j \circ L_{[1]_2})([0]_2) = f_i([0]_2) + f_j([1]_2),\ f_i(f_j \circ L_{[1]_2})([1]_2) = f_i([1]_2) + f_j([0]_2),$$

οι «πολλαπλασιασμοί» των απεικονίσεων f_i και $f_j, f_j \circ L_{[1]_2}$ *εντός τής* $\mathbb{Z}_2^{\mathbb{Z}_2}$ κατα-χωρίζονται στον κατάλογο[121]:

$\cdot$	f_1	f_2	f_3	f_4	$f_1 \circ L_{[1]_2}$	$f_2 \circ L_{[1]_2}$	$f_3 \circ L_{[1]_2}$	$f_4 \circ L_{[1]_2}$
f_1	f_3	f_4	f_1	f_2	f_4	f_3	f_1	f_2
f_2	f_4	f_3	f_2	f_1	f_3	f_4	f_2	f_1
f_3	f_1	f_2	f_3	f_4	f_2	f_1	f_3	f_4
f_4	f_2	f_1	f_4	f_3	f_1	f_2	f_4	f_3

[121] Αρκεί η εκτέλεση απλών πράξεων. Επί παραδείγματι, $f_2 f_1 = f_4$ και $f_2(f_1 \circ L_{[1]_2}) = f_3$, διότι

$$f_2 f_1([0]_2) = f_1([0]_2) + f_2([0]_2) = [0]_2 + [1]_2 = [1]_2 = f_4([0]_2),$$
$$f_2 f_1([1]_2) = f_1([1]_2) + f_2([1]_2) = [1]_2 + [0]_2 = [1]_2 = f_4([1]_2),$$

και

$$f_2(f_1 \circ L_{[1]_2})([0]_2) = f_2([0]_2) + f_1([1]_2) = [1]_2 + [1]_2 = [0]_2 = f_3([0]_2),$$
$$f_2(f_1 \circ L_{[1]_2})([1]_2) = f_2([1]_2) + f_1([0]_2) = [0]_2 + [0]_2 = [0]_2 = f_3([1]_2).$$

Μέσω αυτού σχηματίζουμε τον *πλήρη* πολλαπλασιαστικό κατάλογο τού κανονικού στεφανιαίου γινομένου $\mathbb{Z}_2 \wr \mathbb{Z}_2$ ως ακολούθως:

$\cdot$	$(f_1, L_{[0]_2})$	$(f_1, L_{[1]_2})$	$(f_2, L_{[0]_2})$	$(f_2, L_{[1]_2})$
$(f_1, L_{[0]_2})$	$(f_3,\mathrm{id}_{\mathbb{Z}_2})$	$(f_3, L_{[1]_2})$	$(f_4,\mathrm{id}_{\mathbb{Z}_2})$	$(f_4, L_{[1]_2})$
$(f_1, L_{[1]_2})$	$(f_4, L_{[1]_2})$	$(f_4,\mathrm{id}_{\mathbb{Z}_2})$	$(f_3, L_{[1]_2})$	$(f_3,\mathrm{id}_{\mathbb{Z}_2})$
$(f_2, L_{[0]_2})$	$(f_4,\mathrm{id}_{\mathbb{Z}_2})$	$(f_4, L_{[1]_2})$	$(f_3,\mathrm{id}_{\mathbb{Z}_2})$	$(f_3, L_{[1]_2})$
$(f_2, L_{[1]_2})$	$(f_3, L_{[1]_2})$	$(f_3,\mathrm{id}_{\mathbb{Z}_2})$	$(f_4, L_{[1]_2})$	$(f_4,\mathrm{id}_{\mathbb{Z}_2})$
$(f_3, L_{[0]_2})$	$(f_1,\mathrm{id}_{\mathbb{Z}_2})$	$(f_1, L_{[1]_2})$	$(f_2,\mathrm{id}_{\mathbb{Z}_2})$	$(f_2, L_{[1]_2})$
$(f_3, L_{[1]_2})$	$(f_2, L_{[1]_2})$	$(f_2,\mathrm{id}_{\mathbb{Z}_2})$	$(f_1, L_{[1]_2})$	$(f_1,\mathrm{id}_{\mathbb{Z}_2})$
$(f_4, L_{[0]_2})$	$(f_2,\mathrm{id}_{\mathbb{Z}_2})$	$(f_2, L_{[1]_2})$	$(f_1,\mathrm{id}_{\mathbb{Z}_2})$	$(f_1, L_{[1]_2})$
$(f_4, L_{[1]_2})$	$(f_1, L_{[1]_2})$	$(f_1,\mathrm{id}_{\mathbb{Z}_2})$	$(f_2, L_{[1]_2})$	$(f_2,\mathrm{id}_{\mathbb{Z}_2})$

$\cdot$	$(f_3, L_{[0]_2})$	$(f_3, L_{[1]_2})$	$(f_4, L_{[0]_2})$	$(f_4, L_{[1]_2})$
$(f_1, L_{[0]_2})$	$(f_1,\mathrm{id}_{\mathbb{Z}_2})$	$(f_1, L_{[1]_2})$	$(f_2,\mathrm{id}_{\mathbb{Z}_2})$	$(f_2, L_{[1]_2})$
$(f_1, L_{[1]_2})$	$(f_1, L_{[1]_2})$	$(f_1,\mathrm{id}_{\mathbb{Z}_2})$	$(f_2, L_{[1]_2})$	$(f_2,\mathrm{id}_{\mathbb{Z}_2})$
$(f_2, L_{[0]_2})$	$(f_2,\mathrm{id}_{\mathbb{Z}_2})$	$(f_2, L_{[1]_2})$	$(f_1,\mathrm{id}_{\mathbb{Z}_2})$	$(f_1, L_{[1]_2})$
$(f_2, L_{[1]_2})$	$(f_2, L_{[1]_2})$	$(f_2,\mathrm{id}_{\mathbb{Z}_2})$	$(f_1, L_{[1]_2})$	$(f_1,\mathrm{id}_{\mathbb{Z}_2})$
$(f_3, L_{[0]_2})$	$(f_3,\mathrm{id}_{\mathbb{Z}_2})$	$(f_3, L_{[1]_2})$	$(f_4,\mathrm{id}_{\mathbb{Z}_2})$	$(f_4, L_{[1]_2})$
$(f_3, L_{[1]_2})$	$(f_3, L_{[1]_2})$	$(f_3,\mathrm{id}_{\mathbb{Z}_2})$	$(f_4, L_{[1]_2})$	$(f_4,\mathrm{id}_{\mathbb{Z}_2})$
$(f_4, L_{[0]_2})$	$(f_4,\mathrm{id}_{\mathbb{Z}_2})$	$(f_4, L_{[1]_2})$	$(f_3,\mathrm{id}_{\mathbb{Z}_2})$	$(f_3, L_{[1]_2})$
$(f_4, L_{[1]_2})$	$(f_4, L_{[1]_2})$	$(f_4,\mathrm{id}_{\mathbb{Z}_2})$	$(f_3, L_{[1]_2})$	$(f_3,\mathrm{id}_{\mathbb{Z}_2})$

Εν συνεχεία, παρατηρούμε ότι $\mathbb{Z}_2 \wr \mathbb{Z}_2 = \big\langle (f_3, L_{[1]_2}), (f_1, L_{[1]_2}) \big\rangle$, όπου

$$(f_3, L_{[1]_2})^2 = (f_3, L_{[1]_2})(f_3, L_{[1]_2}) = (f_3, \mathrm{id}_{\mathbb{Z}_2}) = e_{\mathbb{Z}_2 \wr \mathbb{Z}_2},$$
$$(f_1, L_{[1]_2})^4 = (f_1, L_{[1]_2})^2 (f_1, L_{[1]_2})^2 = (f_4, \mathrm{id}_{\mathbb{Z}_2})(f_4, \mathrm{id}_{\mathbb{Z}_2}) = (f_3, \mathrm{id}_{\mathbb{Z}_2}) = e_{\mathbb{Z}_2 \wr \mathbb{Z}_2}$$

με $(f_1, L_{[1]_2})^\nu \neq e_{\mathbb{Z}_2 \wr \mathbb{Z}_2}$, $\forall \nu \in \{1, 2, 3\}$, και

$$(f_1, L_{[1]_2})(f_3, L_{[1]_2}) = (f_1, \mathrm{id}_{\mathbb{Z}_2}) \neq (f_2, \mathrm{id}_{\mathbb{Z}_2}) = (f_3, L_{[1]_2})(f_1, L_{[1]_2}),$$
$$(f_1, L_{[1]_2})(f_3, L_{[1]_2}) = (f_1, \mathrm{id}_{\mathbb{Z}_2}) = (f_2, \mathrm{id}_{\mathbb{Z}_2})(f_4, \mathrm{id}_{\mathbb{Z}_2})$$
$$= (f_3, L_{[1]_2})(f_1, L_{[1]_2})(f_4, \mathrm{id}_{\mathbb{Z}_2}) = (f_3, L_{[1]_2})(f_1, L_{[1]_2})^3 = (f_3, L_{[1]_2})(f_1, L_{[1]_2})^{-1}.$$

Από την πρόταση 3.4.7 συμπεραίνουμε ότι $\mathbb{Z}_2 \wr \mathbb{Z}_2 \cong \mathbf{D}_4$.

7.8.5 Παράδειγμα. (Η ομάδα τού φανανάφτη.) Εάν $G = \mathbb{Z}_2$, $H = \mathbb{Z}$, τότε η ομάδα $\mathbb{Z}_2^{(\mathbb{Z})}$ ως προς την πράξη

$$\mathbb{Z}_2^{(\mathbb{Z})} \times \mathbb{Z}_2^{(\mathbb{Z})} \ni (f_1, f_2) \longmapsto f_1 f_2 \in \mathbb{Z}_2^{(\mathbb{Z})}$$

με $f_1 f_2(m) := f_1(m) + f_2(m)$, $\forall m \in \mathbb{Z}$, έχει ως ουδέτερο στοιχείο της $e_{\mathbb{Z}_2^{(\mathbb{Z})}}$ την απεικόνιση που στέλνει κάθε ακέραιο αριθμό στο $[0]_2$. Άρα το κανονικό στεφανιαίο γινόμενο $\mathbb{Z}_2 \wr \mathbb{Z} := \mathbb{Z}_2 \wr_{\mathbb{Z}} L(\mathbb{Z})$ έχει άπειρη τάξη με εσωτερική πράξη την

$$(f_1, L_{k_1})(f_2, L_{k_2}) := (f_1(f_2 \circ L_{-k_1}), L_{k_1 + k_2}), \tag{7.100}$$

όπου $k_1, k_2 \in \mathbb{Z}$, και ουδέτερο στοιχείο το $e_{\mathbb{Z}_2 \wr \mathbb{Z}} = (e_{\mathbb{Z}_2^{(\mathbb{Z})}}, L_0)$. Κάθε στοιχείο $(f, L_k) \in \mathbb{Z}_2 \wr \mathbb{Z}$ διαθέτει ως «τετμημένη» του μια απεικόνιση $f \in \mathbb{Z}_2^{(\mathbb{Z})}$ που στέλνει

το πολύ πεπερασμένου πλήθους ακεραίους στο $[1]_2$ και τους υπολοίπους στο $[0]_2$ (και, ως εκ τούτου, προσδιορίζεται πλήρως όταν είναι γνωστός ο φορέας[122] αυτής) και ως «τεταγμένη» του την απεικόνιση $m \longmapsto k+m$. Η $\mathbb{Z}_2 \wr \mathbb{Z}$ καλείται **ομάδα τού φανανάφτη**[123] για τον εξής λόγο: Παρομοιάζοντας την πραγματική ευθεία με μια «απειρομήκη» οδό μιας πόλεως, στα ακέραια σημεία τής οποίας είναι τοποθετημένοι φανοί φωτισμού, υποθέτουμε ότι κάθε στοιχείο $(f, L_k) \in \mathbb{Z}_2 \wr \mathbb{Z}$ καθορίζει ποιοι εξ αυτών είναι αναμμένοι και μπροστά σε ποιον στέκεται ένας φανανάφτης ως ακολούθως: Οι μόνοι αναμμένοι φανοί είναι εκείνοι που βρίσκονται στα ακέραια σημεία τα ανήκοντα στον $\mathrm{supp}(f)$ και ο φανανάφτης βρίσκεται στη θέση k. (Ιδιαιτέρως, το $e_{\mathbb{Z}_2 \wr \mathbb{Z}}$ αντιστοιχεί σε παντελώς σβησμένους φανούς, με τον φανανάφτη ευρισκόμενον στο 0.) Επί παραδείγματι, το (f_1, L_1), όπου $\mathrm{supp}(f_1) = \{-3, -1, 1, 2\}$, μπορεί να εκφρασθεί σχηματικώς ως

$$\begin{array}{rcccccccccccc} & \cdots & \blacksquare & \square & \blacksquare & \square & \blacksquare & \square & \square & \blacksquare & \blacksquare & \cdots \\ (f_1, L_1): & & & & & & & \uparrow & & & & \\ & \cdots & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & \cdots \end{array}$$

με κάθε ■ να συμβολίζει έναν σβησμένο και κάθε □ έναν αναμμένο φανό, και με το βελάκι να δηλοί τη θέση τού φανανάφτη. Πολλαπλασιάζοντας αυτό (μέσω τής (7.100)) με το (f_2, L_{-3}), όπου $\mathrm{supp}(f_2) = \{-2, 0, 2\}$, ήτοι με το

$$\begin{array}{rcccccccccccc} & \cdots & \blacksquare & \blacksquare & \square & \blacksquare & \square & \blacksquare & \square & \blacksquare & \blacksquare & \cdots \\ (f_2, L_{-3}): & & & \uparrow & & & & & & & & \\ & \cdots & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & \cdots \end{array}$$

λαμβάνουμε «$\mathrm{mod}\, 2$»

$$\begin{array}{r|\!|cccccccccc} f_1 & \cdots & \blacksquare & \square & \blacksquare & \square & \blacksquare & \square & \square & \blacksquare & \blacksquare & \cdots \\ f_2 \circ L_{-1} & \cdots & \blacksquare & \blacksquare & \blacksquare & \square & \blacksquare & \square & \blacksquare & \square & \blacksquare & \cdots \\ \hline f_1(f_2 \circ L_{-1}) & \cdots & \blacksquare & \square & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \square & \square & \blacksquare & \cdots \end{array}$$

και τελικώς

$$\begin{array}{rcccccccccc} & \cdots & \blacksquare & \square & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \square & \square & \blacksquare & \cdots \\ (f_1, L_1)(f_2, L_{k_2}): & & & & \uparrow & & & & & & & \\ & \cdots & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & \cdots \end{array}$$

Σημειωτέον ότι

$$\boxed{\mathbb{Z}_2 \wr \mathbb{Z} = \langle \mathfrak{s}, \mathfrak{t} \rangle\,, \text{ όπου } \mathfrak{s} := (e_{\mathbb{Z}_2^{(\mathbb{Z})}}, L_1),\ \mathfrak{t} := (\widehat{f}, L_0)}$$

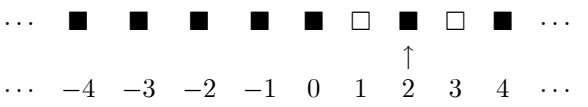
[122] Υπενθύμιση: $\mathrm{supp}(f) := \{\, m \in \mathbb{Z} |\, f(m) = [1]_2 \,\}$.

[123] Π.χ., στην παλαιά Αθήνα (κατά τον 19ο αιώνα) υπήρχαν δημοτικοί υπάλληλοι που ήταν επιτετραμμένοι για να ανάβουν τα βράδια τούς φανούς τού φωτισμού των δρόμων τής πόλεως (αρχικώς λαδοφάναρα και από το 1856 λάμπες φωταερίου) και κάποιοι άλλοι για να τους καθαρίζουν και να τους συντηρούν. Οι πρώτοι καλούντο *φανανάφτες* (το αντίστοιχο των *καντηλαναφτών* που εργάζονται στις εκκλησίες και στα κοιμητήρια) και οι δεύτεροι *φανοκόροι*. Η ηλεκτροδότηση, όπως ήταν φυσικό, οδήγησε στην εξαφάνιση των ειδικών αυτών ενασχολήσεων.

και $\widehat{f}(0) := [1]_2$, $\widehat{f}(m) := [0]_2$, $\forall m \in \mathbb{Z}\setminus\{0\}$. Πράγματι· για οιοδήποτε στοιχείο $(f, L_k) \in \mathbb{Z}_2 \wr \mathbb{Z}\setminus\{e_{\mathbb{Z}_2\wr\mathbb{Z}}\}$ με $\mathrm{supp}(f) = \{m_1, ..., m_l\}$ ισχύει η ισότητα

$$(f, L_k) = (\mathfrak{s}^{m_1}\mathfrak{t}\mathfrak{s}^{-m_1})\cdots(\mathfrak{s}^{m_l}\mathfrak{t}\mathfrak{s}^{-m_l})\mathfrak{s}^k.$$

Έχοντας αυτούς τους γεννήτορες στη διάθεσή μας μπορούμε να εκφράσουμε το στοιχείο τού $\mathbb{Z}_2 \wr \mathbb{Z}$ που αντιστοιχεί σε δοθέν σχήμα συναρτήσει αυτών *εκκινώντας από το* $e_{\mathbb{Z}_2\wr\mathbb{Z}} = (e_{\mathbb{Z}_2^{(\mathbb{Z})}}, L_0)$. Π.χ., εκκινώντας από σβησμένους φανούς και με τον φανανάφτη στο 0 καταλήγουμε στο



(με μόνον τους υπ. αρ. 1 και 3 φανούς αναμμένους) ως εξής:

(i) Κινούμε τον φανανάφτη κατά 3 θέσεις προς τα δεξιά.

(ii) Αυτός ανάβει τον φανό στη θέση 3.

(iii) Τον μετακινούμε κατά δύο θέσεις προς τα αριστερά.

(iv) Αυτός ανάβει τον φανό στη θέση 1.

(v) Τέλος, τον μεταφέρουμε κατά μία θέση προς τα δεξιά. Αυτή η διαδικασία μάς δίδει το $\mathfrak{s}^3\mathfrak{t}\mathfrak{s}^{-2}\mathfrak{t}\mathfrak{s}$. Φυσικά, τούτο θα μπορούσε να γίνει και με διαφορετικό τρόπο:

(i) Κινούμε τον φανανάφτη μία θέση προς τα δεξιά.

(ii) Αυτός ανάβει τον φανό στη θέση 1.

(iii) Τον μετακινούμε κατά δύο θέσεις προς τα δεξιά.

(iv) Αυτός ανάβει τον φανό στη θέση 3.

(v) Τέλος, τον μεταφέρουμε κατά μία θέση προς τα αριστερά. Αυτή η δεύτερη διαδικασία μάς δίδει το $\mathfrak{s}\mathfrak{t}\mathfrak{s}^2\mathfrak{t}\mathfrak{s}^{-1}$. Επομένως οι γεννήτορες υπόκεινται στη σχέση $\mathfrak{s}^3\mathfrak{t}\mathfrak{s}^{-2}\mathfrak{t}\mathfrak{s} = \mathfrak{s}\mathfrak{t}\mathfrak{s}^2\mathfrak{t}\mathfrak{s}^{-1}$.

Ασκήσεις

7-1. Να δειχθεί απευθείας ότι $\mathbb{Z}_8 \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_4$ και $\mathbb{Z}_8 \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

7-2. Να αποδειχθεί ότι $\mathbb{Z}_{m^2} \ncong \mathbb{Z}_m \oplus \mathbb{Z}_m$ για κάθε $m \in \mathbb{N}$, $m \geq 2$.

7-3. Να αποδειχθεί ότι $\mathbb{Z}_5 \times \mathbb{Z}_5^\times \cong \mathbb{Z}_{20}$.

7-4. Να αποδειχθεί ότι $\mathbb{Z}_{960}^\times \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{16}$.

7-5. Να αποδειχθεί ότι η υποομάδα $H := \langle 3, 6\rangle$ τής $(\mathbb{Q}\setminus\{0\}, \cdot)$ είναι ισόμορφη με την $\mathbb{Z} \oplus \mathbb{Z}$.

7-6. Ποια είναι η τάξη τού στοιχείου $([8]_{12}, [4]_{60}, [10]_{24}) \in \mathbb{Z}_{12} \oplus \mathbb{Z}_{60} \oplus \mathbb{Z}_{24}$;

7-7. Ποιο είναι το πλήθος των στοιχείων τής $\mathbb{Z}_5 \oplus \mathbb{Z}_{25}$ που έχουν τάξη 5;

7-8. Ποιο είναι το πλήθος των στοιχείων τής $\mathbb{Z}_{720}^{\times}$ που έχουν τάξη 12;

7-9. Πόσες κυκλικές υποομάδες τάξεως 10 διαθέτει η $\mathbb{Z}_{25} \oplus \mathbb{Z}_{100}$;

7-10. (i) Ποιος είναι ο εκθέτης τής ομάδας $G := \mathbb{Z}_{120} \times \mathbf{D}_9 \times \mathfrak{S}_7$;
(ii) Ποια είναι (εντός αυτής) η τάξη τού στοιχείου $([64]_{120}, \beta^6, [1\,2\,4]\circ[3\,7\,5\,6])$;
(iii) Πόσα στοιχεία τάξεως 3 διαθέτει η G;

7-11. Πόσες υποομάδες τάξεως 2 και πόσες τάξεως 4 διαθέτει η $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$;

7-12. Έστω p ένας πρώτος αριθμός. Πόσα στοιχεία τάξεως p, πόσα στοιχεία τάξεως p^2 και πόσα στοιχεία τάξεως p^3 διαθέτει η ομάδα $\mathbb{Z}_p \oplus \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^3}$;

7-13. Να προσδιορισθεί μια κυκλική υποομάδα H τού εξωτερικού ευθέος γινομένου $\mathbf{D}_5 \times \mathbb{Z}_2$ τάξεως $|H| = 10$.

7-14. Εάν G_1, G_2 είναι δυο ομάδες και $L_1, L_2 \in \mathbf{Subg}(G_1 \times G_2)$, να αποδειχθεί (με διατήρηση των συμβολισμών των εισαχθέντων στο θεώρημα 7.1.10) ότι ισχύει $L_1 \sqsubseteq L_2$ εάν και μόνον εάν ικανοποιούνται οι κάτωθι συνθήκες:
(i) $\mathrm{pr}_j(L_1) \sqsubseteq \mathrm{pr}_j(L_2)$ και $\mathrm{pr}_j(\overline{G}_j \cap L_1) \sqsubseteq \mathrm{pr}_j(\overline{G}_j \cap L_2)$ για $j = 1, 2$.
(ii) Ο ισομορφισμός f_{L_1} απεικονίζει την $\mathrm{pr}_1(L_1) \cap \mathrm{pr}_1(\overline{G}_1 \cap L_2)/\mathrm{pr}_1(\overline{G}_1 \cap L_1)$ στην

$$f_{L_1}(\mathrm{pr}_1(L_1) \cap \mathrm{pr}_1(\overline{G}_1 \cap L_2)/\mathrm{pr}_1(\overline{G}_1 \cap L_1)) = (\mathrm{pr}_2(L_1) \cap \mathrm{pr}_2(\overline{G}_2 \cap L_2))/\mathrm{pr}_2(\overline{G}_2 \cap L_1).$$

(iii) Ο ισομορφισμός f_{L_2} απεικονίζει την $(\mathrm{pr}_1(L_1)\mathrm{pr}_1(\overline{G}_1 \cap L_2))/\mathrm{pr}_1(\overline{G}_1 \cap L_2)$ στην

$$f_{L_2}((\mathrm{pr}_1(L_1)\mathrm{pr}_1(\overline{G}_1 \cap L_2))/\mathrm{pr}_1(\overline{G}_1 \cap L_2)) = (\mathrm{pr}_2(L_1)\mathrm{pr}_2(\overline{G}_2 \cap L_2))/\mathrm{pr}_2(\overline{G}_2 \cap L_2).$$

(iv) Εάν $\widetilde{f_{L_2}}$ είναι ο περιορισμός τού f_{L_2} στην $(\mathrm{pr}_1(L_1)\mathrm{pr}_1(\overline{G}_1 \cap L_2))/\mathrm{pr}_1(\overline{G}_1 \cap L_2)$, τότε το ακόλουθο διάγραμμα είναι μεταθετικό:

$$\begin{array}{ccc}
(\mathrm{pr}_1(L_1)\mathrm{pr}_1(\overline{G}_1 \cap L_2))/\mathrm{pr}_1(\overline{G}_1 \cap L_2) & \xrightarrow[\widetilde{f_{L_2}}]{\cong} & (\mathrm{pr}_2(L_1)\mathrm{pr}_2(\overline{G}_2 \cap L_2))/\mathrm{pr}_2(\overline{G}_2 \cap L_2) \\
\uparrow \cong & & \uparrow \cong \\
\mathrm{pr}_1(L_1)/(\mathrm{pr}_1(L_1) \cap \mathrm{pr}_1(\overline{G}_1 \cap L_2)) & \xrightarrow[\widetilde{f_{L_1}}]{\cong} & \mathrm{pr}_2(L_1)/(\mathrm{pr}_2(L_1) \cap \mathrm{pr}_2(\overline{G}_2 \cap L_2))
\end{array}$$

[*Σημείωση*. Εν προκειμένω, ο ισομορφισμός $\widetilde{f_{L_1}}$ ορίζεται ως εξής: Επειδή είναι προφανές ότι $\mathrm{pr}_1(\overline{G}_1 \cap L_1) \trianglelefteq \mathrm{pr}_1(L_1)$ και

$$\mathrm{pr}_1(\overline{G}_1 \cap L_1) \sqsubseteq \mathrm{pr}_1(L_1) \cap \mathrm{pr}_1(\overline{G}_1 \cap L_2) \trianglelefteq \mathrm{pr}_1(L_1),$$

ισχύει $(\mathrm{pr}_1(L_1) \cap \mathrm{pr}_1(\overline{G}_1 \cap L_2))/\mathrm{pr}_1(\overline{G}_1 \cap L_1) \trianglelefteq \mathrm{pr}_1(L_1)/\mathrm{pr}_1(\overline{G}_1 \cap L_1)$ (βλ. 4.4.15 (i)), οπότε υφίσταται ισομορφισμός

$$\mathrm{pr}_1(L_1)/(\mathrm{pr}_1(L_1) \cap \mathrm{pr}_1(\overline{G}_1 \cap L_2)) \xrightarrow{\cong}{}_{\eta_1} \left(\frac{\mathrm{pr}_1(L_1)}{\mathrm{pr}_1(\overline{G}_1 \cap L_1)}\right) / \left(\frac{\mathrm{pr}_1(L_1) \cap \mathrm{pr}_1(\overline{G}_1 \cap L_2)}{\mathrm{pr}_1(\overline{G}_1 \cap L_1)}\right)$$

βάσει τού θεωρήματος 4.5.21. Κατ' αναλογίαν, υφίσταται ισομορφισμός

$$\mathrm{pr}_2(L_1)/(\mathrm{pr}_2(L_1)\cap \mathrm{pr}_2(\overline{G}_2\cap L_2)) \xrightarrow[\eta_2]{\cong} \left(\tfrac{\mathrm{pr}_2(L_1)}{\mathrm{pr}_2(\overline{G}_2\cap L_1)}\right) / \left(\tfrac{\mathrm{pr}_2(L_1)\cap \mathrm{pr}_2(\overline{G}_2\cap L_2)}{\mathrm{pr}_2(\overline{G}_2\cap L_1)}\right).$$

Επιπροσθέτως, μέσω τού ισομορφισμού $f_{L_1} : \frac{\mathrm{pr}_1(L_1)}{\mathrm{pr}_1(\overline{G}_1\cap L_1)} \xrightarrow{\cong} \frac{\mathrm{pr}_2(L_1)}{\mathrm{pr}_2(\overline{G}_2\cap L_1)}$ επάγεται ισομορφισμός

$$\left(\tfrac{\mathrm{pr}_1(L_1)}{\mathrm{pr}_1(\overline{G}_1\cap L_1)}\right) / \left(\tfrac{\mathrm{pr}_1(L_1)\cap \mathrm{pr}_1(\overline{G}_1\cap L_2)}{\mathrm{pr}_1(\overline{G}_1\cap L_1)}\right) \xrightarrow[f_{L_1}^{\pi\eta\lambda\cdot}]{\cong} \left(\tfrac{\mathrm{pr}_2(L_1)}{\mathrm{pr}_2(\overline{G}_2\cap L_1)}\right) / \left(\tfrac{\mathrm{pr}_2(L_1)\cap \mathrm{pr}_2(\overline{G}_2\cap L_2)}{\mathrm{pr}_2(\overline{G}_2\cap L_1)}\right)$$

κατόπιν μεταφοράς σε «επίπεδο πηλικοομάδων». (Βλ. θεώρημα 4.5.5.) Εξ ορισμού, $\widetilde{f_{L_1}} := \eta_2^{-1}\circ f_{L_1}^{\pi\eta\lambda\cdot}\circ\eta_1$. Από την άλλη μεριά, οι δύο ισομορφισμοί οι υποδηλούμενοι στο διάγραμμα μέσω των κατακόρυφων βελών προκύπτουν από το θεώρημα 4.5.13.]

7-15. Ποιο είναι το σύνολο των υποομάδων τής ομάδας $\mathbb{Z}_4\times\mathbf{V}$ και ποιο το διάγραμμα τού Hasse για τον σύνδεσμο $(\mathbf{Subg}(\mathbb{Z}_4\times\mathbf{V}),\sqsubseteq)$;

7-16. Ποιο είναι το σύνολο των υποομάδων τής ομάδας $\mathbb{Z}_3\times\mathfrak{S}_3$ και ποιο το διάγραμμα τού Hasse για τον σύνδεσμο $(\mathbf{Subg}(\mathbb{Z}_3\times\mathfrak{S}_3),\sqsubseteq)$;

7-17. Εάν $m,n\in\mathbb{N}$ με $n\geq 3$, να προσδιορισθεί το σύνολο των υποομάδων τής ομάδας $\mathbb{Z}_{2m}\times\mathbf{D}_n$ και να σχεδιασθεί το διάγραμμα τού Hasse για τον σύνδεσμο $(\mathbf{Subg}(\mathbb{Z}_4\times\mathbf{D}_4),\sqsubseteq)$ (όταν $m=2$ και $n=4$).

7-18. Να προσδιορισθούν οι υποομάδες και οι ορθόθετες υποομάδες τής $\mathbf{D}_4\times\mathbf{D}_6$.

7-19. Έστω ότι p,q είναι δυο περιττοί πρώτοι αριθμοί και $m,n\in\mathbb{N}$. Για ποιον λόγο δεν είναι το εξωτερικό ευθύ γινόμενο $\mathbb{Z}_{p^m}^\times\times\mathbb{Z}_{q^n}^\times$ κυκλική ομάδα (παρά το γεγονός ότι καθεμιά εκ των $\mathbb{Z}_{p^m}^\times,\mathbb{Z}_{q^n}^\times$ είναι κυκλική βάσει τής προτάσεως 7.3.9);

7-20. Έστω $(F,+,\cdot)$ ένα σώμα και έστω

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

η ομάδα τού Heisenberg υπεράνω αυτού. (Βλ. εδ. D.2.24.) Να αποδειχθεί ότι η μεταθέτρια υποομάδα τής $\mathbf{Heis}(F)$ ισούται με το κέντρο $Z(\mathbf{Heis}(F))$ αυτής και ότι είναι ισόμορφη με την προσθετική ομάδα $(F,+)$, καθώς και το ότι υφίσταται ισομορφισμός

$$\mathbf{Heis}(F)/Z(\mathbf{Heis}(F))\cong F\oplus F.$$

7-21. Να αποδειχθεί ότι το σύνολο πινάκων

$$H := \left\{ \begin{pmatrix} [1]_3 & [a]_3 & [b]_3 \\ [0]_3 & [1]_3 & [0]_3 \\ [0]_3 & [0]_3 & [1]_3 \end{pmatrix} \middle| \, a,b\in\mathbb{Z} \right\}$$

αποτελεί μια αβελιανή υποομάδα τής $\mathbf{Heis}(\mathbb{Z}_3)$ τάξεως 9. Με ποια εκ των $\mathbb{Z}_9,\mathbb{Z}_3\oplus\mathbb{Z}_3$ είναι ισόμορφη η H; (Πρβλ. εδ. 7.1.46 και 7.1.47.)

7-22. Ποιο είναι το κέντρο και ποια η μεταθέτρια υποομάδα τής $\mathbf{D}_6 \times \mathfrak{S}_4$;

7-23. Να αποδειχθεί ότι για οιουσδήποτε $n_1, n_2 \in \mathbb{N}$ το εξωτερικό ευθύ γινόμενο $\mathfrak{S}_{n_1} \times \mathfrak{S}_{n_2}$ είναι εμφυτεύσιμο εντός τής $\mathfrak{S}_{n_1+n_2}$.

7-24. Είναι το εξωτερικό ευθύ γινόμενο $\mathfrak{S}_3 \times \mathfrak{S}_4$ εμφυτεύσιμο εντός τής $\mathfrak{S}_6$;

7-25. Έστω $(G, \cdot)$ μια ομάδα. Θέτοντας $\Delta_G := \{(g, g) | \, g \in G\} \subseteq G \times G$, να αποδειχθεί ότι $\Delta_G \sqsubseteq G \times G$. (Αυτή καλείται, ιδιαιτέρως, **διαγώνιος υποομάδα** τής $G \times G$.) Εν συνεχεία, να αποδειχθούν τα ακόλουθα:

(i) $\Delta_G \cong G$,

(ii) $\Delta_G \trianglelefteq G \times G \Leftrightarrow$ η G είναι αβελιανή.

(iii) $\mathrm{N}_{G\times G}(\Delta_G) = \Delta_G \Leftrightarrow Z(G) = \{e_G\}$.

7-26. Έστω ότι G_1, G_2 είναι δυο ομάδες και $G := G_1 \times G_2$. Να αποδειχθεί ότι μια απεικόνιση $f : G_1 \longrightarrow G_2$ είναι ομομορφισμός ομάδων εάν και μόνον εάν $\{(x, f(x)) | \, x \in G_1\} \sqsubseteq G$.

7-27. Εάν G_1, G_2 είναι δυο ομάδες και $G := G_1 \times G_2$, να αποδειχθούν τα εξής:

(i) Εάν αμφότερες οι G_1 και G_2 είναι περιοδικές, τότε και η G είναι περιοδική.

(ii) Εάν αμφότερες οι G_1 και G_2 στερούνται στρέψεως, τότε και η G στερείται στρέψεως.

7-28. Έστω ότι G_1, G_2 είναι δυο ομάδες και $G := G_1 \times G_2$. Να δειχθεί ότι ο κεντροποιητής $\mathrm{C}_G((g_1, g_2))$ κάθε στοιχείου $(g_1, g_2) \in G$ ισούται με το ευθύ εξωτερικό γινόμενο $\mathrm{C}_{G_1}(g_1) \times \mathrm{C}_{G_2}(g_2)$ των κεντροποιητών των «συντεταγμένων» του και ότι, ως εκ τούτου, ισχύει

$$\boxed{\mathfrak{K}(G) = \mathfrak{K}(G_1)\mathfrak{K}(G_2).}$$

7-29. Έστω ότι G_1, G_2 είναι δυο ομάδες, $G := G_1 \times G_2$ και $H \trianglelefteq G$.

(i) Να αποδειχθεί ότι είτε η H είναι αβελιανή είτε η τομή της με (τουλάχιστον) μία εκ των G_1, G_2 είναι μη τετριμμένη.

(ii) Εάν αμφότερες οι G_1 και G_2 είναι μη αβελιανές και απλές, να προσδιορισθούν οι ορθόθετες υποομάδες τής G.

7-30. Έστω ότι G_1, G_2 είναι ομάδες και $G := G_1 \times G_2$. Να αποδειχθούν τα εξής:

(i) Εάν $x_1, y_1 \in G_1$ και $x_2, y_2 \in G_2$, τότε εντός τής G ισχύει η ισότητα

$$[(x_1, x_2), (y_1, y_2)] = ([x_1, y_1], [x_2, y_2]).$$

(ii) Εάν $H_1, K_1 \in \mathbf{Subg}(G_1)$ και $H_2, K_2 \in \mathbf{Subg}(G_2)$, τότε

$$\boxed{[H_1 \times H_2, K_1 \times K_2] = [H_1, K_1] \times [H_2, K_2].}$$

7-31. Έστω ότι G_1, G_2 είναι δυο ομάδες και $G := G_1 \times G_2$. Μια $L \sqsubseteq G$ καλείται **υποευθύ γινόμενο των** G_1 **και** G_2 όταν $\mathrm{pr}_1(L) = G_1$ και $\mathrm{pr}_2(L) = G_2$. Να αποδειχθούν τα ακόλουθα:

(i) Μια υποομάδα L τής G είναι υποευθύ γινόμενο των G_1 και G_2 εάν και μόνον εάν $\overline{G}_1 L = G = L\overline{G}_2$, όπου $\overline{G}_1 := \mathrm{Im}(\iota_1)$ και $\overline{G}_2 := \mathrm{Im}(\iota_2)$.

(ii) Εάν $L \in \mathbf{Subg}(G)$ είναι ένα υποευθύ γινόμενο των G_1 και G_2, τότε

$$L \trianglelefteq G \Longleftrightarrow G' \sqsubseteq L.$$

7-32. Εάν $(G, \cdot)$ είναι μια ομάδα και $H, K \in \mathbf{NSubg}(G)$, να αποδειχθούν τα εξής:

(i) Η απεικόνιση

$$f : G \longrightarrow (G/H) \times (G/K)\,,\ g \longmapsto f(g) := (gH, gK),$$

είναι ομομορφισμός ομάδων και $\mathrm{Ker}(f) = H \cap K$.

(ii) Η $G/H \cap K$ είναι εμφυτεύσιμη στην $(G/H) \times (G/K)$ μέσω τού μονομορφισμού

$$\hat{f} : G/H \cap K \longrightarrow (G/H) \times (G/K)\,,\ g(H \cap K) \overset{\hat{f}}{\longmapsto} (gH, gK).$$

(ii) Η εικόνα $\mathrm{Im}(\hat{f})$ αποτελεί ένα υποευθύ γινόμενο των G/H και G/K.

(iii) Εάν αμφότερες οι G/H και G/K είναι αβελιανές, τότε και η $G/H \cap K$ είναι αβελιανή.

(iv) Εάν $H \neq K$ και $|G : H| = |G : K| = 2$, τότε ισχύει $|G : H \cap K| = 4$ και $G/H \cap K \cong \mathbf{V}$.

7-33. Εάν $(G, \cdot)$ είναι μια ομάδα, $s \in \mathbb{N}$, $s \geq 2$, και $H_1, ..., H_s \in \mathbf{NSubg}(G)$, να αποδειχθούν τα εξής για την απεικόνιση

$$f : G \longrightarrow \prod_{j=1}^{s} G/H_j,\ g \overset{f}{\longmapsto} (gH_1, ..., gH_s).$$

(i) Η f αποτελεί έναν ομομορφισμό ομάδων και $\mathrm{Ker}(f) = \bigcap_{j=1}^{s} H_j$.

(ii) Εάν $|G : H_j| < \infty,\ \forall j \in \{1, ..., s\}$, και

$$\text{μκδ}(|G : H_j|\,, |G : H_{j'}|) = 1,\ \forall (j, j') \in \{1, ..., s\} \times \{1, ..., s\} \ \text{ με } j \neq j',$$

τότε η f είναι επιμορφισμός και η

$$\hat{f} : G/\textstyle\bigcap_{j=1}^{s} H_j \longrightarrow \prod_{j=1}^{s} G/H_j,\ g(\textstyle\bigcap_{j=1}^{s} H_j) \overset{\hat{f}}{\longmapsto} (gH_1, ..., gH_s),$$

ισομορφισμός ομάδων.

7-34. Να αποδειχθούν τα εξής:

(i) $(\mathbb{Z}_2 \oplus \mathbb{Z}_4)/\langle([0]_2, [1]_4)\rangle \cong \mathbb{Z}_2$,

(ii) $(\mathbb{Z}_2 \oplus \mathbb{Z}_4)/\,\langle([0]_2, [2]_4)\rangle \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$,

(iii) $(\mathbb{Z}_2 \oplus \mathbb{Z}_4)/\,\langle([1]_2, [2]_4)\rangle \cong \mathbb{Z}_4$.

7-35. Να αποδειχθούν τα εξής:

(i) $(\mathbb{Z}_4 \oplus \mathbb{Z}_6)/\langle([0]_4, [1]_6)\rangle \cong \mathbb{Z}_4$,

(ii) $(\mathbb{Z}_4 \oplus \mathbb{Z}_6)/\langle([0]_4, [2]_6)\rangle \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2$,

(iii) $(\mathbb{Z}_4 \oplus \mathbb{Z}_6)/\langle([2]_4, [3]_6)\rangle \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.

7-36. Να αποδειχθεί ότι $(\mathbb{Z} \oplus \mathbb{Z})/(\langle(m, 0)\rangle \oplus \langle(0, n)\rangle) \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$, $\forall (m, n) \in \mathbb{N} \times \mathbb{N}$.

7-37. Να αποδειχθεί ότι $(\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}_8)/\langle(0, 4, [0]_8)\rangle \cong \mathbb{Z} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8$.

7-38. Είναι η πηλικοομάδα $(\mathbb{Z} \oplus \mathbb{Z})/\langle(4, 2)\rangle$ άπειρη; Κυκλική;

7-39. Να αποδειχθεί ότι για κάθε $n \in \mathbb{N}$, $n \geq 2$, υφίσταται ισομορφισμός

$$\underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n \text{ φορές}} \Big/ \left\langle \underbrace{(n, n, ..., n)}_{n \text{ φορές}} \right\rangle \cong \mathbb{Z}_n \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n-1 \text{ φορές}}.$$

7-40. Να προσδιορισθεί η τάξη τού στοιχείου

(i) $([2]_3, [1]_6) + \langle([1]_3, [1]_6)\rangle$ εντός τής $(\mathbb{Z}_3 \oplus \mathbb{Z}_6)/\langle([1]_4, [1]_6)\rangle$,

(ii) $([2]_6, [0]_8) + \langle([4]_6, [4]_8)\rangle$ εντός τής $(\mathbb{Z}_6 \oplus \mathbb{Z}_8)/\langle([4]_6, [4]_8)\rangle$.

7-41. Εάν $G := \mathbb{Z}_4 \oplus \mathbb{Z}_4$, $H := \{([0]_4, [0]_4), ([2]_4, [0]_4), ([0]_4, [2]_4), ([2]_4, [2]_4)\}$ και $K := \langle([1]_4, [2]_4)\rangle$, τότε (προφανώς) $|G/H| = |G/K| = 4$. Με ποια εκ των $\mathbb{Z}_4, \mathbb{Z}_2 \oplus \mathbb{Z}_2$ ($\cong \mathbf{V}$) είναι ισόμορφη η πηλικοομάδα G/H και με ποια η G/K; (Πρβλ. θεώρημα 7.1.46.)

7-42. Να ταξινομηθούν μέχρις ισομορφισμού οι αβελιανές ομάδες τάξεως p^2q^2, όπου p, q είναι δυο πρώτοι αριθμοί με $p \neq q$. [*Υπόδειξη*: Βλ. θεωρήματα 7.1.49 και 7.1.46.]

7-43. Να προσδιορισθεί μια μη ορθόθετη υποομάδα τού εξωτερικού ευθέος γινομένου $\mathbf{Q} \times \mathbb{Z}_4$. (Παρά το γεγονός ότι κάθε υποομάδα τόσον τής $\mathbf{Q}$ όσον και τής $\mathbb{Z}_4$ είναι ορθόθετη, η ομάδα $\mathbf{Q} \times \mathbb{Z}_4$ είναι μη χαμιλτονιανή. Πρβλ. θεώρημα 7.5.3.)

7-44. Έστω ότι G_1, G_2 είναι δυο ομάδες και $U_1 \sqsubseteq Z(G_1), U_2 \sqsubseteq Z(G_2)$. Υποτιθεμένου ότι υφίσταται ισομορφισμός $f : U_1 \xrightarrow{\cong} U_2$, ορίζεται η *ορθόθετη*[124] υποομάδα $\mathfrak{W} := \left\{ (x, f(x)^{-1}) \middle| \, x \in U_1 \right\}$ τού εξωτερικού ευθέος γινομένου $G_1 \times G_2$ των G_1 και G_2 και, ως εκ τούτου, η πηλικοομάδα

$$\boxed{G_1 \underset{\text{cent.}}{\overset{(U_1, U_2, f)}{\boxtimes}} G_2 := G_1 \times G_2/\mathfrak{W}}$$

η οποία καλείται, ιδιαιτέρως, **κεντρικό γινόμενο των** G_1 **και** G_2 **(ως προς την τριάδα** (U_1, U_2, f)**)**.

[124] Προφανώς, $\mathfrak{U} \sqsubseteq Z(G_1) \times Z(G_2) \underset{7.1.57\,(i)}{=} Z(G_1 \times G_2) \underset{5.4.19\,(i)}{\Longrightarrow} \mathfrak{U} \trianglelefteq G_1 \times G_2$.

(i) Εάν $\overline{G}_1 := \mathrm{Im}(\iota_1),\ \overline{G}_2 := \mathrm{Im}(\iota_2)$ και

$$\pi = \pi_{\mathfrak{M}}^{G_1 \times G_2} : G_1 \times G_2 \longrightarrow G_1 \overset{(U_1,U_2,f)}{\underset{\text{cent.}}{\boxtimes}} G_2$$

ο φυσικός επιμορφισμός, να αποδειχθεί ότι

$$U_1 \cong \pi(\overline{G}_1) \cap \pi(\overline{G}_2) \sqsubseteq Z(G_1 \overset{(U_1,U_2,f)}{\underset{\text{cent.}}{\boxtimes}} G_2),$$

καθώς και ότι

$$\boxed{\left| G_1 \overset{(U_1,U_2,f)}{\underset{\text{cent.}}{\boxtimes}} G_2 \right| = |G_1|\ |G_2 : U_2| = |G_2|\ |G_1 : U_1|\,.}$$

(ii) Να αποδειχθεί ότι

$$\mathbb{Z}_4 \overset{(\langle [2]_4\rangle, \langle -\mathbf{I}_2\rangle, f)}{\underset{\text{cent.}}{\boxtimes}} \mathbf{Q} \cong \mathbb{Z}_4 \overset{(\langle [2]_4\rangle, \langle \beta^2\rangle, f')}{\underset{\text{cent.}}{\boxtimes}} \mathbf{D}_4,$$

όπου $f([0]_4) := \mathbf{I}_2$, $f([2]_4) := -\mathbf{I}_2$, $f'([0]_4) := \mathrm{id}_{\mathcal{E}_4}$, $f'([2]_4) := \beta^2$.

(iii) Να αποδειχθεί ότι

$$\mathbf{D}_4 \overset{(\langle \beta^2\rangle, \langle -\mathbf{I}_2\rangle, f)}{\underset{\text{cent.}}{\boxtimes}} \mathbf{Q} \ncong \mathbf{D}_4 \overset{(\langle \beta^2\rangle, \langle \beta^2\rangle, \mathrm{id}_{\langle \beta^2\rangle})}{\underset{\text{cent.}}{\boxtimes}} \mathbf{D}_4,$$

όπου $f(\mathrm{id}_{\mathcal{E}_4}) := \mathbf{I}_2$, $f(\beta^2) := -\mathbf{I}_2$.

7-45. Εάν $s \in \mathbb{N}$, $s \geq 2$, και εάν οι $G_1, G_2, ..., G_s$ είναι s πεπερασμένες ομάδες με μκδ$(|G_i|\,, |G_j|) = 1$ για οιουσδήποτε $i, j \in \{1, ..., s\}$, $i \neq j$, να αποδειχθεί ότι για κάθε $L \sqsubseteq \prod_{j=1}^{s} G_j$ ισχύει

$$L = \prod_{j=1}^{s} \mathrm{pr}_j(\overline{G}_j \cap L),$$

όπου $\mathrm{pr}_i : \prod_{j=1}^{s} G_j \to G_i$ (και αντιστοίχως, $\iota_i : G_i \to \prod_{j=1}^{s} G_j$) η i-οστή φυσική προβολή (και αντιστοίχως, η i-οστή φυσική εμφύτευση) και $\overline{G}_i := \mathrm{Im}(\iota_i)$, απ' όπου έπεται ότι

$$\mathbf{Subg}(G_1) \times \mathbf{Subg}(G_2) \times \cdots \times \mathbf{Subg}(G_s) = \mathbf{Subg}(G_1 \times G_2 \times \cdots \times G_s).$$

7-46. Να αποδειχθεί ότι τα κάτωθι σύνολα

$$H_1 := \left\{ f \in \mathbb{Z}^{\mathbb{N}} \middle|\, f\,(j) \in m_j\mathbb{Z},\ \forall j \in \mathbb{N} \right\}\ (m_j \in \mathbb{N}_0 \text{ εξαρτώμενος από τον } j),$$

$$H_2 := \left\{ f \in \mathbb{Z}^{\mathbb{N}} \middle|\, f\,(i) \equiv f(j) (\mathrm{mod}\, 2),\ \forall (i,j) \in \mathbb{N} \times \mathbb{N} \right\},$$

$$H_3 := \left\{ f \in \mathbb{Z}^{\mathbb{N}} \middle|\, \exists k = k_f \in \mathbb{N} : f\,(i) = f(j) \text{ όταν } i \equiv j (\mathrm{mod}\, k) \right\},$$

είναι υποομάδες τής άπειρης ομάδας $\mathbb{Z}^{\mathbb{N}} = \{\text{απεικονίσεις } f : \mathbb{N} \longrightarrow \mathbb{Z}\}$.

7-47. Να δοθεί η απόδειξη τής προτάσεως 7.1.90.

7-48. Να δοθεί η απόδειξη τής προτάσεως 7.1.96.

7-49. Εάν $(G,\cdot)$ είναι μια ομάδα και I, J δύο μη κενά ισοπληθή σύνολα (όχι κατ' ανάγκην πεπερασμένα), να αποδειχθούν τα εξής:
(i) $G^I \cong G^J$. (Βλ. εδ. 7.1.94 (ii).) (ii) $G^{(I)} \cong G^{(J)}$.

7-50. Να αποδειχθεί ότι για τυχούσα ομάδα $(G,\cdot)$ ισχύουν τα ακόλουθα[125]:
(i) $G \times G^{(\mathbb{N}_0)} \cong G^{(\mathbb{N}_0)}$. (ii) $G^{(\mathbb{N}_0)} \times G^{(\mathbb{N}_0)} \cong G^{(\mathbb{N}_0)}$.

7-51. Να δοθεί παράδειγμα μιας άπειρης περιοδικής ομάδας, εντός τής οποίας για κάθε $k \in \mathbb{N}$ υφίσταται στοιχείο τάξεως k.

7-52. Υποτιθεμένου ότι I είναι ένα μη κενό σύνολο, $(G_i)_{i\in I}, (H_i)_{i\in I}$ οικογένειες ομάδων με τους δείκτες τους ειλημμένους από το I και $f_i : G_i \longrightarrow H_i$ ομομορφισμοί για κάθε $i \in I$, ορίζονται οι απεικονίσεις

$$\prod_{i\in I} f_i : \prod_{i\in I} G_i \longrightarrow \prod_{i\in I} H_i,\ x = (x_i)_{i\in I} \longmapsto (\prod_{i\in I} f_i)(x),$$

και

$$\prod_{i\in I}^{\text{περ.}} f_i : \prod_{i\in I}^{\text{περ.}} G_i \longrightarrow \prod_{i\in I}^{\text{περ.}} H_i,\ x = (x_i)_{i\in I} \longmapsto (\prod_{i\in I}^{\text{περ.}} f_i)(x),$$

όπου $(\prod_{i\in I} f_i)(x)(j) := f_j(x_j)$ και $(\prod_{i\in I}^{\text{περ.}} f_i)(x)(j) := f_j(x_j), \forall j \in I$. Να αποδειχθούν τα εξής:
(i) Αμφότερες οι $\prod_{i\in I} f_i$ και $\prod_{i\in I}^{\text{περ.}} f_i$ είναι ομομορφισμοί.
(ii) [Η $\prod_{i\in I} f_i$ είναι μονομορφισμός] $\Leftrightarrow$ [οι f_i είναι μονομορφισμοί, $\forall i \in I$].
(iii) [Η $\prod_{i\in I} f_i$ είναι επιμορφισμός] $\Leftrightarrow$ [οι f_i είναι επιμορφισμοί, $\forall i \in I$].
(iv) [Οι f_i είναι μονομορφισμοί, $\forall i \in I$] $\Rightarrow$ [η $\prod_{i\in I}^{\text{περ.}} f_i$ είναι μονομορφισμός].
(v) [Οι f_i είναι επιμορφισμοί, $\forall i \in I$] $\Rightarrow$ [η $\prod_{i\in I}^{\text{περ.}} f_i$ είναι επιμορφισμός].

7-53. Έστω I ένα μη κενό σύνολο και έστω $(G_i)_{i\in I}$ τυχούσα οικογένεια ομάδων με τους δείκτες της ειλημμένους από το I. Να αποδειχθούν τα εξής:
(i) $Z(\prod_{i\in I} G_i) = \prod_{i\in I} Z(G_i)$ και $Z(\prod_{i\in I}^{\text{περ.}} G_i) = \prod_{i\in I}^{\text{περ.}} Z(G_i)$.
(ii) $(\prod_{i\in I} G_i)' \sqsubseteq \prod_{i\in I} G_i'$ και $(\prod_{i\in I}^{\text{περ.}} G_i)' \sqsubseteq \prod_{i\in I}^{\text{περ.}} G_i'$.
(iii) Εάν η G_i στρείται στρέψεως για κάθε δείκτη $i \in I$, τότε αμφότερες οι $\prod_{i\in I} G_i$ και $\prod_{i\in I}^{\text{περ.}} G_i$ στερούνται στρέψεως.

[125] Για οιαδήποτε *πεπερασμένη* ομάδα H ισχύει προφανώς $H \times H \cong H$ εάν και μόνον εάν η H είναι *τετριμμένη*. Εντούτοις, υπάρχει *πληθώρα* απλών παραδειγμάτων (όπως αυτό τού (ii) τής παρούσας ασκήσεως, όταν η G είναι μη τετριμμένη) *άπειρων* ομάδων H για τις οποίες είναι δυνατόν να υφίσταται ισομορφισμός $H \times H \cong H$.

(iv) Εάν η G_i είναι περιοδική για κάθε $i \in I$, τότε και η $\prod_{i\in I}^{\text{περ.}} G_i$ είναι περιοδική.

(v) Εάν p είναι ένας πρώτος αριθμός και η G_i μια p-ομάδα για κάθε δείκτη $i \in I$, τότε και η $\prod_{i\in I}^{\text{περ.}} G_i$ είναι μια p-ομάδα.

(vi) Εάν $\exp(G_i) = n \in \mathbb{N}$ για κάθε δείκτη $i \in I$, τότε $\exp(\prod_{i\in I}^{\text{περ.}} G_i) = n$.

7-54. Εάν G, H είναι δυο αβελιανές ομάδες και $(G_i)_{i\in I}$, $(H_j)_{i\in J}$ δυο οικογένειες αβελιανών ομάδων (με $I \neq \varnothing$ και $J \neq \varnothing$), να δειχθεί ότι υφίστανται ισομορφισμοί[126]

$$\boxed{\text{Hom}(\prod_{i\in I}^{\text{περ.}} G_i, H) \cong \prod_{i\in I} \text{Hom}(G_i, H)}$$

και

$$\boxed{\text{Hom}(G, \prod_{j\in J} H_j) \cong \prod_{j\in J} \text{Hom}(G, H_j).}$$

7-55. Ποιες είναι οι ομάδες αυτομορφισμών $\text{Aut}(\mathbf{D}_{n_1} \times \mathbf{D}_{n_2})$ (όπου n_1, n_2 είναι θετικοί ακέραιοι ≥ 3) και $\text{Aut}(\mathbf{D}_{n_1} \times \mathfrak{S}_{n_2})$ (όπου n_1, n_2 είναι θετικοί ακέραιοι ≥ 3 και $n_2 \neq 6$) και ποιες οι τάξεις αυτών;

7-56. Έστω $(G, \cdot)$ μια κυκλική ομάδα τάξεως $|G| = mn$, όπου $m, n \in \mathbb{N}$ και μκδ$(m, n) = 1$. Εάν g είναι ένας γεννήτοράς της, να δειχθεί ότι αυτή παριστάται ως $G = \langle g^m \rangle \times_{\text{εσ.}} \langle g^n \rangle$.

7-57. Έστω $(F, +, \cdot)$ ένα σώμα και έστω $(\text{Mat}_{2\times 2}(F), +)$ η προσθετική ομάδα των 2×2-πινάκων με τις εγγραφές τους ειλημμένες από το F. Να αποδειχθεί ότι $\text{Mat}_{2\times 2}(F) = H \oplus_{\text{εσ.}} K$, όπου

$$H := \left\{ \begin{pmatrix} a & b \\ 0_F & 0_F \end{pmatrix} \middle| \, a, b \in F \right\} \text{ και } K := \left\{ \begin{pmatrix} 0_F & 0_F \\ c & d \end{pmatrix} \middle| \, c, d \in F \right\}.$$

7-58. Για τις υποομάδες $G := \langle 3, 6, 10 \rangle$ και $H := \langle 3, 6, 12 \rangle$ τής πολλαπλασιαστικής ομάδας $(\mathbb{Q}\setminus\{0\}, \cdot)$ να δειχθεί ότι

$$G = \langle 3 \rangle \times_{\text{εσ.}} \langle 6 \rangle \times_{\text{εσ.}} \langle 10 \rangle \text{ και } H \neq \langle 3 \rangle \times_{\text{εσ.}} \langle 6 \rangle \times_{\text{εσ.}} \langle 12 \rangle .$$

7-59. Έστω ότι οι H, K είναι δυο υποομάδες μιας ομάδας $(G, \cdot)$. Εάν υποτεθεί ότι $G = HK$ και ότι αμφότερες οι H, K είναι ορθόθετες, να αποδειχθεί ότι

$$G/H \cap K = (H/H \cap K) \times_{\text{εσ.}} (K/H \cap K).$$

Εν συνεχεία, να δειχθεί μέσω καταλλήλου παραδείγματος ότι τούτο μπορεί να μην ισχύει στην περίπτωση κατά την οποία η μία εκ των υποομάδων H, K είναι ορθόθετη και η άλλη δεν είναι.

[126] Ειδικώς, όταν $I = J = \{1, 2\}$, έχουμε $\text{Hom}(G_1 \times G_2, H) \cong \text{Hom}(G_1, H) \times \text{Hom}(G_2, H)$ και

$$\text{Hom}(G, H_1 \times H_2) \cong \text{Hom}(G, H_1) \times \text{Hom}(G, H_2).$$

7-60. Έστω $(G,\cdot)$ μια ομάδα και έστω $H \trianglelefteq G$. Εάν υποτεθεί ότι η H είναι πλήρης ομάδα, να αποδειχθεί ότι $G = H \times_{\text{εσ.}} \mathrm{C}_G(H)$.

7-61. (i) Εάν $(K,\cdot)$ είναι μια πλήρης ομάδα με την K^{ab} μη τετριμμένη, να δειχθεί ότι η K δεν μπορεί να είναι η μεταθέτρια υποομάδα μιας ομάδας.

(ii) Να δειχθεί ότι για οιονδήποτε $n \in \mathbb{N}$ με $n \geq 3$ και $n \neq 6$ η συμμετρική ομάδα $\mathfrak{S}_n$ δεν μπορεί να είναι η μεταθέτρια υποομάδα μιας ομάδας.

7-62. Έστω $(G,\cdot)$ μια ομάδα. Εάν υπάρχουν $H, K \in \mathbf{NSubg}(G)$, τέτοιες ώστε να ισχύει $G = H \times_{\text{εσ.}} K$ και εάν L είναι μια πλήρως αναλλοίωτη υποομάδα τής G, να αποδειχθούν τα ακόλουθα:

(i) $L = (L \cap H) \times_{\text{εσ.}} (L \cap K)$.

(ii) $G/L = (LH/L) \times_{\text{εσ.}} (LK/L)$.

7-63. Ένας ενδομορφισμός ϑ μιας ομάδας $(G,\cdot)$ καλείται **κεντρικός ενδομορφισμός** όταν $g^{-1}\vartheta(g) \in Z(G), \forall g \in G$. Να αποδειχθούν τα ακόλουθα:

(i) Κάθε κεντρικός ενδομορφισμός μιας ομάδας είναι ορθόθετος.

(ii) Κάθε επιρριπτικός ορθόθετος ενδομορφισμός μιας ομάδας είναι κεντρικός.

(iii) Κάθε ενδομορφισμός μιας αβελιανής ομάδας είναι κεντρικός.

(iv) Εάν υποτεθεί ότι ϑ είναι ένας κεντρικός ενδομορφισμός μιας ομάδας $(G,\cdot)$ και $\omega \in \mathbf{Aut}(G)$, τότε ο ενδομορφισμός $\omega \circ \vartheta \circ \omega^{-1}$ είναι κεντρικός.

(v) Ένας αυτομορφισμός μιας ομάδας είναι ορθόθετος εάν και μόνον εάν είναι κεντρικός.

7-64. Να αποδειχθεί ότι η $(\mathbb{Q},+)$ είναι αναποσυνθέσιμη ομάδα.

7-65. Να αποδειχθεί ότι τόσον η (άπειρη, αβελιανή) p-σχεδόν κυκλική ομάδα $\mathbb{Z}(p^\infty)$ (όπου p τυχών πρώτος αριθμός, βλ. άσκηση **4-41**) όσον και οι συμμετρικές ομάδες $\mathfrak{S}_n$, $n \geq 2$, είναι αναποσυνθέσιμες ομάδες.

7-66. Για ομάδες G, H, K, L να χρησιμοποιηθεί καταλλήλως το θεώρημα 7.2.25 των Krull, Remak και Schmidt, ούτως ώστε να αποδειχθούν τα ακόλουθα:

(i) Εάν η G πληροί τόσον τη **Σ.Α.Α.** όσον και τη **Σ.Κ.Α.** επί τού $\mathbf{NSubg}(G)$, και $G \times G \cong H \times H$, τότε $G \cong H$.

(ii) Εάν $G \cong H \times K$ και $G \cong H \times L$, και εάν η G πληροί τόσον τη **Σ.Α.Α.** όσον και τη **Σ.Κ.Α.** επί τού $\mathbf{NSubg}(G)$, τότε[127] $K \cong L$.

[127] Σημειωτέον ότι ο R. Hirshon απέδειξε (στο άρθρο του υπό τον τίτλο *On cancellation in groups*, The American Mathematical Monthly **76**, No. 9 (1969), 1037-1039) ότι για μια *πεπερασμένη* ομάδα H και *τυχούσες* ομάδες K, L ισχύει η συνεπαγωγή: $H \times K \cong H \times L \Rightarrow K \cong L$. Αργότερα ο ίδιος επεξέτεινε τα αποτελέσματά του επί τού προβλήματος τής *απαλοιφής σε ευθέα γινόμενα* και για άλλες (άπειρες) ομάδες (για τις οποίες δεν είναι δυνατόν να χρησιμοποιηθεί το θεώρημα 7.2.25) στα εξής άρθρα:

• *Cancellation of groups with maximal condition*, Proceedings of the American Math. Society **24**, (1970), 401-403.

• *Some new groups admitting essentially unique directly indecomposable decompositions*, Mathematische Annalen **194**, (1971), 123-125.

• *The cancellation of an infinite cyclic group in direct products*, Archiv der Mathematik **26** (1975), 134-138.

7-67. Έστω I ένα μη κενό σύνολο και έστω $(H_i)_{i\in I}$ μια οικογένεια υποομάδων μιας ομάδας $(G,\cdot)$ με τους δείκτες της ειλημμένους από το I, ούτως ώστε να ισχύει $G = \prod_{i\in I}^{\text{εσ.}} H_i$. Εάν $L \trianglelefteq H_j$ για κάποιον δείκτη $j \in I$, να αποδειχθεί ότι $L \trianglelefteq G$.

7-68. Υποτιθεμένου ότι μια μη τετριμμένη ομάδα $(G,\cdot)$ είναι τέτοια, ώστε να ισχύει $Z(G) = \{e_G\}$ και $G = H_1 \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_s$ ($s \in \mathbb{N}$, $s \geq 2$), όπου καθεμιά εξ αυτών των ορθόθετων υποομάδων της είναι απλή, να αποδειχθούν τα εξής:

(i) $\mathbf{Min\text{-}NSubg}(G) = \{H_1, ..., H_s\}$.

(ii) Για κάθε $\{e_G\} \neq K \trianglelefteq G$ υπάρχει ένα υποσύνολο $\{j_1, ..., j_r\} \subseteqq \{1, ..., s\}$ (με $1 \leq r \leq s$), ούτως ώστε να ισχύει $K = H_{j_1} \times_{\text{εσ.}} \cdots \times_{\text{εσ.}} H_{j_r}$.

7-69. Εάν p είναι ένας πρώτος αριθμός και $s \in \mathbb{N}$, να δειχθεί ότι η αβελιανή p-ομάδα $\underbrace{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p}_{s \text{ φορές}}$ είναι χαρακτηριστικώς απλή.

7-70. Να αποδειχθεί ότι για μια μη τετριμμένη πεπερασμένη ομάδα $(G,\cdot)$ οι ακόλουθες συνθήκες είναι ισοδύναμες:

(i) Η G είναι χαρακτηριστικώς απλή.

(ii) Η G είναι *είτε* αφ' εαυτής απλή *είτε* το εσωτερικό ευθύ γινόμενο s ορθόθετων υποομάδων της ($s \in \mathbb{N}$, $s \geq 2$), όπου καθεμιά εξ αυτών είναι απλή και ισόμορφη με οιαδήποτε εκ των υπολοίπων. [*Υπόδειξη*: Να χρησιμοποιηθούν καταλλήλως οι ασκήσεις **7-67**, **7-68** και **7-69**.]

7-71. Έστω $(F,+,\cdot)$ ένα σώμα. Θέτοντας

$$G := \left\{ \begin{pmatrix} a & b \\ 0_F & c \end{pmatrix} \middle| \, a, c \in F\smallsetminus\{0_F\}, b \in F \right\} \sqsubset \mathbf{GL}_2(F),$$

να αποδειχθεί ότι τα

$$H := \left\{ \begin{pmatrix} 1_F & b \\ 0_F & 1_F \end{pmatrix} \middle| \, b \in F \right\} \text{ και } K := \left\{ \begin{pmatrix} a & 0_F \\ 0_F & c \end{pmatrix} \middle| \, a, c \in F\smallsetminus\{0_F\} \right\}$$

αποτελούν υποομάδες τής G, ότι $H \lhd G$, $K \not\trianglelefteq G$ και ότι $G = H \rtimes K$.

7-72. Έστω $(F,+,\cdot)$ ένα σώμα και έστω $\mathbf{AGL}_n(F)$ η συσχετική (γενική γραμμική) ομάδα βαθμού n υπεράνω αυτού. (Βλ. άσκηση **4-53**.) Να αποδειχθεί ότι

$$\boxed{\mathbf{AGL}_n(F) = \mathbf{Trans}(F^n) \rtimes \mathbf{GL}_n(F).}$$

7-73. Εάν G_1, G_2 είναι δυο (πολλαπλασιαστικές) αβελιανές ομάδες με εκθέτες $\neq 2$ και $f : G_1 \longrightarrow G_2$ ένας ομομορφισμός, τότε ορίζεται μια απεικόνιση

$$f^* : \mathbf{Dih}(G_1) \longrightarrow \mathbf{Dih}(G_2),\ (g,\varepsilon) \longmapsto f^*(g,\varepsilon) := (f(g),\varepsilon)$$

(όπου $g \in G, \varepsilon \in \{\pm 1\}$) από τη διεδρικοποίηση τής πρώτης στη διεδρικοποίηση τής δεύτερης. (Βλ. εδ. 7.6.18.) Να αποδειχθούν τα ακόλουθα:

(i) Η f^* είναι ομομορφισμός.

(ii) Εάν ο f είναι μονομορφισμός, τότε και ο f^*είναι μονομορφισμός.

(iii) Εάν ο f είναι επιμορφισμός, τότε και ο f^*είναι επιμορφισμός.

7-74. Εάν $(G,\cdot)$ είναι μια αβελιανή ομάδα με $\exp(G)\neq 2$, να αποδειχθούν τα εξής:

(i) $Z(\mathbf{Dih}(G))=\left\{(g,1)|\, g\in G \text{ και } g^2=e_G\right\}$.

(ii) Εάν $H\sqsubseteq G$ με $\exp(G/H)\neq 2$, τότε

$$\mathbf{Dih}(G)/\left\{(h,1)|\, h\in H\right\}\cong \mathbf{Dih}(G/H).$$

(iii) $\mathbf{Subg}(\{(g,1)|\, g\in G\})\subseteq \mathbf{NSubg}(\mathbf{Dih}(G))$.

(iv) Εάν υποτεθεί ότι για κάθε $x\in G$ υπάρχει κάποιο $y\in G$ με $x=y^2$, τότε

$$\mathbf{Dih}(G)'=\left\{(g^2,1)\big|\, g\in G\right\}$$

και κάθε *γνήσια* ορθόθετη υποομάδα τής $\mathbf{Dih}(G)$ αποτελεί υποομάδα τής $\{(g,1)|\, g\in G\}$.

7-75. Να αποδειχθούν τα ακόλουθα:

(i) $Z(\mathbf{Dih}(\mathbb{Z}(2^\infty)))\cong\mathbb{Z}_2$ και $\mathbf{Dih}(\mathbb{Z}(2^\infty))/Z(\mathbf{Dih}(\mathbb{Z}(2^\infty)))\cong\mathbf{Dih}(\mathbb{Z}(2^\infty))$.

(ii) Η $\mathbf{D}_\infty$ είναι εμφυτεύσιμη εντός τής $\mathbf{Dih}(\mathbb{Q})$.

7-76. Να αποδειχθεί ότι $\mathrm{Aut}(\mathbf{D}_\infty)\cong\mathbf{D}_\infty$.

7-77. Να δοθεί διεξοδική απόδειξη τού θεωρήματος 7.6.39.

7-78. Να αποδειχθεί ότι $\mathrm{Aut}(\mathbf{Q})\cong\mathfrak{S}_4$.

7-79. Έστω $s\in\mathbb{N}$, $s\geq 2$, και έστω $n\in\mathbb{N}$, $n\geq 4$. Να προσδιορισθεί η τάξη τής ομάδας αυτομορφισμών

$$\mathrm{Aut}(\underbrace{\mathfrak{A}_n\times\mathfrak{A}_n\times\cdots\times\mathfrak{A}_n\times\mathfrak{A}_n}_{s\ \text{φορές}})$$

και να παρατεθεί ο κατάλογος των συγκεκριμένων τιμών που λαμβάνει αυτή όταν $(s,n)\in\{2,...,8\}\times\{4,...,10\}$. [*Υπόδειξη*: Βλ. εδ. 7.6.55.]

7-80. Να δειχθεί ότι το κανονικό στεφανιαίο γινόμενο πεπερασμένων ομάδων δεν είναι (εν γένει) «προσεταιριστικό» υπό την εξής έννοια: Εάν G,H,K είναι τρεις πεπερασμένες ομάδες, τότε το $G\wr(H\wr K)$ δεν ισούται κατ' ανάγκην με το $(G\wr H)\wr K$.