ΚΕΦΑΛΑΙΟ 3

Ομάδες

Η αλγεβρική δομή *τής ομάδας* καθορίζεται μέσω τού εφοδιασμού ενός μη κενού συνόλου με μία και μόνον εσωτερική πράξη, η οποία πληροί κάποιες «χαρακτηριστικές συνθήκες». Τα *ομαδοειδή*, οι *ημιομάδες* και τα *μονοειδή* υπάγονται στους «προπομπούς» της.

Θα μπορούσε κανείς να ισχυρισθεί με βάσιμα επιχειρήματα ότι η έννοια τής *ομάδας* «ενυπήρχε» ήδη (εμμέσως πλην σαφώς) σε διάφορες εργασίες των μαθηματικών τής αρχαιότητας. Ως *αλγεβρική δομή* πρωτοπαρουσιάσθηκε σε αριθμοθεωρητικές εργασίες των L. Euler (1707-1783), C.-F. Gauss (1777-1855) κ.ά. κατά τα τέλη τού 18ου και τις αρχές τού 19ου αιώνα, και, εν συνεχεία, στη θεωρία μετατάξεων των θέσεων μηδενισμού αλγεβρικών εξισώσεων των J.-L. Lagrange (1736-1813), E. Galois (1811-1832) κ.ά. Ωστόσο, ο τελικώς καθιερωθείς «ορισμός» της, όπως τον αντιλαμβανόμαστε στις ημέρες μας, αποκρυσταλλώθηκε σε ένα άρθρο[1] τού A. Cayley (1821-1895) το οποίο δημοσιεύθηκε το 1854, καθώς και σε κατοπινές δημοσιεύσεις[2] του περί τα μέσα τής δεκαετίας τού 1870. (Αρκετοί ιστορικοί υπογραμμίζουν και την πολύτιμη συμβολή των R. Dedekind (1831-1916), C. Jordan (1838-1922) και W. van Dyck (1856-1934) στην παγίωση αυτού τού ορισμού.)

[1] Cayley A.: *On the theory of groups, as depending in the symbolic equation* $\Theta^n = 1$, Phil. Magazine, Vol. **7** (1854).

[2] Πρβλ. Scholz E. (Hrsg.): *Geschichte der Algebra*, B.I., Mannheim, 1990, σελ. 309.

3.1 ΟΜΑΔΟΕΙΔΗ, ΗΜΙΟΜΑΔΕΣ ΚΑΙ ΜΟΝΟΕΙΔΗ

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

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

επί τού A, ονομάζεται **ομαδοειδές**[3]. (Το A καλείται **υποκείμενο σύνολο** τού ομαδοειδούς $(A, \circledcirc)$.)

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

(i) **προσεταιριστικό ομαδοειδές** ή **ημιομάδα** όταν η πράξη "$\circledcirc$" είναι *προσεταιριστική* (βλ. 1.5.3 (i)),

(ii) **μεταθετικό ομαδοειδές** ή **αβελιανό ομαδοειδές** όταν η πράξη "$\circledcirc$" είναι *μεταθετική* (βλ. 1.5.3 (ii)), και

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

3.1.3 Ορισμός. Κάθε ημιομάδα (και αντιστοίχως, κάθε αβελιανή ημιομάδα) η οποία διαθέτει *ουδέτερο στοιχείο* ως προς την πράξη την ορισθείσα επ' αυτής (βλ. 1.5.6 (iii)) ονομάζεται **μονοειδές** (και αντιστοίχως, **αβελιανό μονοειδές**).

3.1.4 Σημείωση. Εάν μια ημιομάδα (ή, γενικότερα, ένα ομαδοειδές) διαθέτει ουδέτερο στοιχείο, τότε αυτό, σύμφωνα με την πρόταση 1.5.8, είναι μονοσημάντως ορισμένο.

3.1.5 Παραδείγματα. (i) Εάν $A \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, τότε το ζεύγος $(A, -)$, όπου "$-$" η πράξη τής αφαιρέσεως, είναι ένα *μη προσεταιριστικό*, *μη μεταθετικό* ομαδοειδές.

(ii) Παρομοίως, εάν το Ω είναι ένα σύνολο, τότε το ζεύγος $(\mathfrak{P}(\Omega), \smallsetminus)$ είναι (εν γένει) ένα *μη προσεταιριστικό*, *μη μεταθετικό* ομαδοειδές (βλ. 1.5.5(iv)).

(iii) Το ζεύγος $(\mathbb{Z}, \circledcirc)$, όπου

$$\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, \ \ (a, b) \longmapsto a \circledcirc b := b,$$

αποτελεί μια *μη αβελιανή* ημιομάδα, διότι $a \circledcirc b \neq b \circledcirc a$ όταν $a \neq b$, ενώ για οιαδήποτε $a, b, c \in \mathbb{Z}$ ισχύουν οι ισότητες

$$(a \circledcirc b) \circledcirc c = b \circledcirc c = c = a \circledcirc c = a \circledcirc (b \circledcirc c).$$

Επιπροσθέτως, είναι προφανές ότι το $(\mathbb{Z}, \circledcirc)$ δεν είναι μονοειδές.

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

(iv) Το ζεύγος $(\mathbb{Z}, \circledast)$, όπου

$$\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, \ \ (a, b) \longmapsto a \circledast b := a^2 + b^2,$$

αποτελεί ένα αβελιανό ομαδοειδές που *δεν είναι ημιομάδα*, διότι $a \circledast b = b \circledast a$ για οιαδήποτε $a, b \in \mathbb{Z}$ και

$$(2 \circledast 1) \circledast 1 = 26 \neq 8 = 2 \circledast (1 \circledast 1)\,.$$

(v) Έστω A ένα μη κενό σύνολο. Το σύνολο $A^A = \text{ΑΠ}(A, A)$ των απεικονίσεων από το A στο A, εφοδιασμένο με την εσωτερική πράξη

$$A^A \times A^A \longrightarrow A^A, \ (g, f) \longmapsto g \circ f,$$

είναι ένα (εν γένει *μη αβελιανό*) μονοειδές με την ταυτοτική απεικόνιση id_A ως ουδέτερο στοιχείο του (βλ. 1.5.12).

(vi) Το ζεύγος $(\mathbb{N}, +)$, όπου "$+$" η συνήθης πρόσθεση φυσικών αριθμών, είναι μια αβελιανή ημιομάδα που δεν είναι μονοειδές.

(vii) Εάν $A \in \{\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ και $B \in \{\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, τότε τα ζεύγη $(A, +)$ και $(B, \cdot)$ (ως προς τις συνήθεις πράξεις προσθέσεως και πολλαπλασιασμού) αποτελούν αβελιανά μονοειδή με ουδέτερά τους στοιχεία τα 0 και 1, αντιστοίχως.

(viii) Τα ζεύγη $(\mathbb{Z}_m, +), m \in \mathbb{N}$, και $(\mathbb{Z}_m, \cdot), m \in \mathbb{N}$, $m \geq 2$, ως προς τις πράξεις προσθέσεως και πολλαπλασιασμού τις ορισθείσες μέσω τού θεωρήματος 2.4.28, είναι αβελιανά μονοειδή με ουδέτερά τους στοιχεία τα $[0]_m$ και $[1]_m$, αντιστοίχως.

(ix) Εάν το Ω είναι ένα σύνολο, τότε τα ζεύγη $(\mathfrak{P}(\Omega), \cup)$, $(\mathfrak{P}(\Omega), \cap)$ και $(\mathfrak{P}(\Omega), \triangle)$ είναι αβελιανά μονοειδή με ουδέτερά τους στοιχεία τα $\varnothing, \Omega$ και $\varnothing$, αντιστοίχως. (Βλ. 1.5.5 (i), (ii) και (iii), και 1.5.10.)

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

$$f : \{1, 2, \ldots, m\} \times \{1, 2, \ldots, n\} \longrightarrow A \tag{3.1}$$

ονομάζεται $(m \times n)$-**πίνακας** με τις «εγγραφές[4]» του ειλημμένες από το A. Αντί τού σχετικώς δύσχρηστου συμβολισμού (3.1) γράφουμε απλώς

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1\,n-1} & a_{1\,n} \\ a_{21} & a_{22} & \cdots & a_{2\,n-1} & a_{2\,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m-1\,1} & a_{m-1\,2} & \cdots & a_{m-1\,n-1} & a_{m-1\,n} \\ a_{m\,1} & a_{m\,2} & \cdots & a_{m\,n-1} & a_{m\,n} \end{pmatrix}$$

[4]Οι **εγγραφές** (αγγλ. entries) ενός πίνακα (3.1) είναι οι $m \times n$ εικόνες τής f.

ή $(a_{ij})_{1\leq i\leq m,1\leq j\leq n}$, όπου

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

Επίσης, ως $\mathrm{Mat}_{m\times n}(A)$ συμβολίζουμε το σύνολο όλων των $(m\times n)$-πινάκων 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

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

για κάθε $((a_{ij})_{1\leq i\leq m,1\leq j\leq n},(b_{ij})_{1\leq i\leq m,1\leq j\leq n})\in(\mathrm{Mat}_{m\times n}(A))^2$. Εάν το $(A,\circledcirc)$ είναι προσεταιριστικό (και αντιστοίχως, αβελιανό), τότε και το $(\mathrm{Mat}_{m\times n}(A),\widehat{\circledcirc}\,)$ είναι προσεταιριστικό (και αντιστοίχως, αβελιανό). Επιπροσθέτως, εάν το $(A,\circledcirc)$ είναι μονοειδές έχον το e_A ως ουδέτερο στοιχείο του, τότε και το $(\mathrm{Mat}_{m\times n}(A),\widehat{\circledcirc}\,)$ είναι μονοειδές με ουδέτερο στοιχείο του τον $(m\times n)$-πίνακα, όλες οι εγγραφές τού οποίου είναι ίσες με το e_A. Επί παραδείγματι, εάν το $A\in\{\mathbb{N}_0,\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Z}_k\}$ (όπου $k\in\mathbb{N}$) εφοδιασθεί με την πράξη τής προσθέσεως "$+$", τότε είθισται να γράφουμε απλώς "$+$" αντί τού "$\widehat{+}$" για τον συμβολισμό τής επαγομένης πράξεως επί τού $\mathrm{Mat}_{m\times n}(A)$ και να την καλούμε **πρόσθεση πινάκων**. Εν προκειμένω, το $(\mathrm{Mat}_{m\times n}(A),+)$ είναι *αβελιανό μονοειδές*.

3.2 ΟΜΑΔΕΣ ΚΑΙ ΥΠΟΟΜΑΔΕΣ

► **Ομάδες**. Αυτές 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.

3.2.1 Ορισμός. Ένα μονοειδές $(G,\circledcirc)$ (με το G ως υποκείμενο σύνολό του) καλείται **ομάδα**[5] όταν για κάθε στοιχείο τού G υπάρχει το συμμετρικό του ως προς την $\circledcirc$ (πρβλ. πρόταση 1.5.8). Η **τάξη** $|G|$ μιας ομάδας $(G,\circledcirc)$ είναι εξ ορισμού ο πληθικός αριθμός $\mathrm{card}(G)$ τού συνόλου G. Εάν η $|G|$ είναι πεπερασμένη, τότε λέμε ότι η G έχει **πεπερασμένη τάξη** ή απλώς ότι η G είναι μια **πεπερασμένη ομάδα** και γράφουμε $|G|<\infty$. (Ειδάλλως λέμε ότι η G είναι μια **άπειρη ομάδα** και γράφουμε $|G|=\infty$). Μια ομάδα G λέγεται **μεταθετική** ή **αβελιανή** (ή **ομάδα τού Abel**) όταν η πράξη, με την οποία είναι εφοδιασμένη, είναι μεταθετική.

[5] Σε πολλές περιπτώσεις όπου δεν υφίσταται κίνδυνος συγχύσεως (για το ποια πράξη υπονοείται) συμβολίζουμε τις ομάδες μόνον με ένα κεφαλαίο (λατινικό) γράμμα.

3.2.2 Παραδείγματα. (i) Τα ζεύγη $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$ των ακεραίων, των ρητών, των πραγματικών και των μιγαδικών αριθμών, αντιστοίχως, μαζί με τη συνήθη πρόσθεση, αποτελούν τα πιο οικεία παραδείγματα αβελιανών ομάδων. Το αβελιανό μονοειδές $(\mathbb{N}_0,+)$ δεν είναι ομάδα, διότι κανένας $n\in\mathbb{N}$ δεν διαθέτει αντίθετο (= συμμετρικό) στοιχείο *εντός* τού συνόλου $\mathbb{N}_0$.

(ii) Το μονοειδές $(\mathbb{Z}_m,+)$, $m\in\mathbb{N}$, (βλ. 3.1.5 (viii)) είναι μια αβελιανή ομάδα με ουδέτερό της στοιχείο το $[0]_m$ και αντίθετο στοιχείο καθενός $[k]_m\in\mathbb{Z}_m$ το $[-k]_m$.

(iii) Τα ζεύγη $(\mathbb{Q}\smallsetminus\{0\},\cdot),(\mathbb{R}\smallsetminus\{0\},\cdot),(\mathbb{Q}_{>0},\cdot),(\mathbb{R}_{>0},\cdot),(\mathbb{C}\smallsetminus\{0\},\cdot)$ 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 $(\mathbb{Z}\smallsetminus\{0\},\cdot)$ δεν είναι ομάδα, διότι μόνον οι ±1 διαθέτουν αντίστροφο (= συμμετρικό) στοιχείο εντός τού $\mathbb{Z}\smallsetminus\{0\}$ (βλ. πόρισμα 1.7.21).

(iv) Το ζεύγος $(\mathbb{Q}_{>0},\star)$, όπου

$$r\star s:=\frac{rs}{2},\quad \forall\,(r,s)\in\mathbb{Q}_{>0}\times\mathbb{Q}_{>0},$$

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 $(\mathbb{Z}_m,\cdot)$, $m\in\mathbb{N}$, $m\geq2$, (βλ. 3.1.5 (viii)), με ουδέτερό του στοιχείο το $[1]_m$, δεν είναι ομάδα, διότι (τουλάχιστον) το $[0]_m$ δεν διαθέτει αντίστροφο.

(vi) Εάν το Ω είναι ένα σύνολο, τότε το ζεύγος $(\mathfrak{P}(\Omega),\triangle)$ αποτελεί μια αβελιανή ομάδα. Αντιθέτως, για οιοδήποτε $\Omega\neq\varnothing$ τα αβελιανά μονοειδή $(\mathfrak{P}(\Omega),\cup)$ και $(\mathfrak{P}(\Omega),\cap)$ δεν είναι ομάδες. (Βλ. 1.5.15 και 3.1.5 (ix).)

(vii) Εάν $m,n\in\mathbb{N}$ και εάν το $A\in\{\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Z}_k\}$ (όπου $k\in\mathbb{N}$) εφοδιασθεί με την πράξη τής συνήθους προσθέσεως, τότε το αβελιανό μονοειδές $(\mathrm{Mat}_{m\times n}(A),+)$ το ορισθέν στο εδάφιο 3.1.6 αποτελεί μια ομάδα, καθότι κάθε

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

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

3.2.3 Σημείωση. Ορισμένες φορές, όταν μελετούμε μια πεπερασμένη ομάδα $(G,\circledcirc)$ που έχει είτε μικρή τάξη είτε στοιχεία διασυνδεόμενα μέσω ειδικών σχέσεων, είναι χρήσιμο να εργαζόμαστε με τον **πολλαπλασιαστικό κατάλογο τής** $(G,\circledcirc)$ (που ονομάζεται, εναλλακτικώς, και **κατάλογος τής πράξεως** "$\circledcirc$" ή **κατάλογος τού Cayley για την** $(G,\circledcirc)$). Εάν $G=\{g_1,\ldots,g_k\}$, $k\in\mathbb{N}$, τότε αυτός είναι ο

εξής:

$\circledcirc$	g_1	g_2	$\cdots$	$\cdots$	g_k
g_1	$g_1 \circledcirc g_1$	$g_1 \circledcirc g_2$	$\cdots$	$\cdots$	$g_1 \circledcirc g_k$
g_2	$g_2 \circledcirc g_1$	$g_2 \circledcirc g_2$	$\cdots$	$\cdots$	$g_2 \circledcirc g_k$
$\vdots$	$\vdots$	$\vdots$			$\vdots$
$\vdots$	$\vdots$	$\vdots$			$\vdots$
g_k	$g_k \circledcirc g_1$	$g_k \circledcirc g_2$	$\cdots$	$\cdots$	$g_k \circledcirc g_k$

Στην i-οστή γραμμή και στην j-οστή στήλη τού καταλόγου τοποθετείται το στοιχείο $g_i \circledcirc g_j$, $1 \leq i, j \leq k$. Κάθε στοιχείο τής ομάδας εμφανίζεται *μόνον μία φορά* σε κάθε γραμμή και κάθε στήλη.

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

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

Από τα προηγηθέντα παραδείγματα 3.1.5 και 3.3.2 καθίσταται σαφές ότι οι ανωτέρω εγκλεισμοί είναι *γνήσιοι*. Επιπροσθέτως, επισημαίνεται -ιδιαιτέρως- ότι, δοθέντος ενός *μονοειδούς*, υπάρχει πάντοτε η δυνατότητα σχηματισμού μιας *ομάδας*, όπως περιγράφεται στην πρόταση 3.2.6.

3.2.5 Ορισμός. Έστω $(M, \cdot)$ ένα μονοειδές έχον το e_M ως ουδέτερο στοιχείο του. Τότε συμβολίζουμε ως

$$\boxed{M^\times := \{x \in M \,|\exists y \in M : xy = e_M = yx\,\}}$$

το σύνολο όλων των $x \in M$ που διαθέτουν συμμετρικό στοιχείο ως προς την "$\cdot$".

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

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς, επειδή $e_M e_M = e_M$, έχουμε $e_M \in M^\times$. Εάν $x, x' \in M^\times$, τότε

$$[\exists y \in M : xy = e_M = yx] \text{ και } [\exists y' \in M : x'y' = e_M = y'x'],$$

οπότε $(y'y)(xx') = y'(yx)x' = y'e_M x' = y'x' = e_M$ και (παρομοίως διαπιστώνουμε ότι) $(xx')(y'y) = e_M$. Τούτο σημαίνει ότι $xx' \in M^\times$, δηλαδή ότι το $M^\times$ είναι κλειστό ως προς την "$\cdot$" (βλ. 1.5.2). Επιπροσθέτως, εάν το x είναι τυχόν στοιχείο τού $M^\times$ και το y συμμετρικό στοιχείο του, τότε το y (λόγω τής προτάσεως 1.

5.13) είναι το μόνο στοιχείο τού M με αυτήν ιδιότητα και (εξ ορισμού) $y \in M^\times$ (διότι το x είναι, με τη σειρά του, το συμμετρικό στοιχείο τού y). Κατά συνέπειαν, το ζεύγος $(M^\times, \cdot)$ αποτελεί μια ομάδα. □

3.2.7 Παραδείγματα. (i) Εάν $F \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, τότε μέσω τού αβελιανού μονοειδούς $(F, \cdot)$ (όπου "$\cdot$" ο συνήθης πολλαπλασιασμός) δημιουργείται η πολλαπλασιαστική ομάδα που έχει ως υποκείμενο σύνολό της το

$$\boxed{F^\times = F \setminus \{0_F\}.}$$

(ii) Μέσω τού αβελιανού μονοειδούς $(\mathbb{Z}, \cdot)$ (όπου "$\cdot$" ο συνήθης πολλαπλασιασμός) δημιουργείται η πολλαπλασιαστική ομάδα που έχει ως υποκείμενο σύνολό της το $\mathbb{Z}^\times = \{1, -1\}$ (βλ. πόρισμα 1.7.21).

(iii) Μέσω τού αβελιανού μονοειδούς $(\mathbb{Z}_m, \cdot)$, $m \in \mathbb{N}$, $m \geq 2$, (όπου "$\cdot$" ο πολλαπλασιασμός ο ορισθείς στο θεώρημα 2.4.28) δημιουργείται η πολλαπλασιαστική ομάδα που έχει ως υποκείμενο σύνολό της το

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

και τάξη $\varphi(m)$, όπου φ η συνάρτηση φι τού Euler. (Βλ. 2.4.16 και 2.4.32.) Η $(\mathbb{Z}_m^\times, \cdot)$ καλείται **ομάδα των αντιστρέψιμων κλάσεων υπολοίπων κατά μόδιο** m.

(iv) Έστω $F \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p\}$ (όπου p πρώτος αριθμός) και έστω $n \in \mathbb{N}$. Ας συμβολίσουμε ως 0_F το ουδέτερο στοιχείο τής ομάδας $(F, +)$ και ως 1_F το ουδέτερο στοιχείο τού μονοειδούς $(F, \cdot)$, όπου "$+$" και "$\cdot$" οι συνήθεις πράξεις προσθέσεως και πολλαπλασιασμού, αντιστοίχως. Επί τού $\text{Mat}_{n\times n}(F)$ ορίζεται *πολλαπλασιασμός πινάκων*:

$$\mathbf{AB} = (a_{i\,1}b_{1\,j} + a_{i\,2}b_{2\,j} + \cdots + a_{i\,n}b_{n\,j})_{1\leq i,j\leq n},$$

για οιουσδήποτε $\mathbf{A} = (a_{ij})_{1\leq i,j\leq n}$, $\mathbf{B} = (b_{ij})_{1\leq i,j\leq n} \in \text{Mat}_{n\times n}(F)$. Το ζεύγος $(\text{Mat}_{n\times n}(F), \cdot)$ είναι ένα μονοειδές με ουδέτερό του στοιχείο τον *μοναδιαίο* $(n \times n)$-πίνακα

$$\mathbf{I}_n := \begin{pmatrix} 1_F & 0_F & \cdots & 0_F & 0_F \\ 0_F & 1_F & \cdots & 0_F & 0_F \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0_F & 0_F & \cdots & 1_F & 0_F \\ 0_F & 0_F & \cdots & 0_F & 1_F \end{pmatrix}.$$

Από τη Γραμμική Άλγεβρα είναι γνωστή η **γενική γραμμική ομάδα**

$$\boxed{\text{GL}_n(F) := (\text{Mat}_{n\times n}(F))^\times = \{\mathbf{A} \in \text{Mat}_{n\times n}(F) \mid \det(\mathbf{A}) \neq 0_F\},}$$

όπου $\det(\mathbf{A})$ η *ορίζουσα* ενός $\mathbf{A} \in \text{Mat}_{n\times n}(F)$.

3.2.8 Σημείωση. (Χρηστικός τρόπος συμβολισμού ομάδων) Από εδώ και στο εξής, όταν αναφερόμαστε σε *τυχούσες* ομάδες, θα υιοθετούμε ως επί το πλείστον τον *πολλαπλασιαστικό* και (κάπως σπανιότερα) τον *προσθετικό* συμβολισμό για τις εκάστοτε θεωρούμενες πράξεις (γράφοντας π.χ. $g_1g_2, g_1 \cdot g_2$ ή $g_1 * g_2$ και, αντιστοίχως, g_1+g_2, αντί τού $g_1 \circledcirc g_2$, για δυο στοιχεία g_1, g_2 μιας ομάδας G, ακόμη και όταν οι πράξεις δεν υπονοούν κάποιους «οικείους» πολλαπλασιασμούς και προσθέσεις, αντιστοίχως) και θα συμβολίζουμε το ουδέτερο στοιχείο μιας ομάδας G ως e_G και το συμμετρικό στοιχείο ενός $g \in G$ ως g^{-1} («αντίστροφο» τού g) και, αντιστοίχως, $-g$ («αντίθετος» τού g).

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

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

(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

$$\left(g^{-1}\right)^{-1} g^{-1} = e_G = g^{-1}\left(g^{-1}\right)^{-1} \quad \text{και} \quad gg^{-1} = e_G = g^{-1}g,$$

έχουμε $\left(g^{-1}\right)^{-1} = g$, για κάθε $g \in G$, λόγω τής μονοσημαντότητας τού συμμετρικού στοιχείου (βλ. πρόταση 1.5.8).
(iii) Έστω $k = 2$. Αρκεί (και πάλι λόγω τής μονοσημαντότητας τού συμμετρικού στοιχείου) να δείξουμε ότι

$$(g_1g_2)\left(g_2^{-1}g_1^{-1}\right) = e_G = \left(g_2^{-1}g_1^{-1}\right)(g_1g_2).$$

Θέτοντας σε εφαρμογή τον γενικευμένο προσεταιριστικό νόμο 1.6.40 λαμβάνουμε

$$(g_1g_2)\left(g_2^{-1}g_1^{-1}\right) = \left(g_1\left(g_2g_2^{-1}\right)\right)g_1^{-1} = (g_1e_G)\, g_1^{-1} = g_1g_1^{-1} = e_G.$$

Αναλόγως δείχνουμε ότι $\left(g_2^{-1}g_1^{-1}\right)(g_1g_2) = e_G$. Για $k \geq 3$ 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 το μονοσήμαντο τής λύσεως τής 2ης εξισώσεως. □

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

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

εν είδει[6] «δυνάμεως».

3.2.11 Πρόταση. *Έστω $(G, \cdot)$ μια ομάδα. Τότε για κάθε στοιχείο $g \in G$ και κάθε $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ ισχύουν τα ακόλουθα*:

(i) $g^mg^n = g^{m+n} = g^ng^m$,

(ii) $(g^m)^n = g^{mn}$,

(iii) $g^{-m} = \left(g^{-1}\right)^m = (g^m)^{-1}$. (Το g^{-m} είναι το αντίστροφο τού g^m.)

ΑΠΟΔΕΙΞΗ. (i) Κατ' αρχάς υποθέτουμε ότι αμφότεροι οι m, n είναι θετικοί. Διατηρώντας τόν n παγιωμένο, θα εφαρμόσουμε κλασική μαθηματική επαγωγή ως προς τον m. (Αναλόγως επιχειρηματολογεί κανείς και με τον n). Εάν $m = 1$, τότε -εξ ορισμού- $gg^n = g^{1+n}$. Υποθέτοντας ότι $g^mg^n = g^{m+n}$, λαμβάνουμε

$$g^{m+1}g^n = (gg^m)\,g^n = g\,(g^mg^n) = gg^{m+n} = g^{m+n+1}.$$

Τώρα υποθέτουμε ότι ένας εκ των m, n είναι $= 0$. Εάν $m = 0$, τότε

$$g^0g^n = e_Gg^n = g^n = g^{0+n}.$$

[6] Όταν χρησιμοποιείται *προσθετικός συμβολισμός* για την G, τότε για κάθε $n \in \mathbb{Z}$ ορίζουμε κατ' αναλογίαν

$$ng := \begin{cases} \underbrace{g + g + \cdots + g}_{n \text{ φορές}}, & \text{όταν } n > 0, \\ -((-n)g), & \text{όταν } n < 0, \\ e_G\,, & \text{όταν } n = 0, \end{cases}$$

εν είδει «πολλαπλασίου».

(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. Τότε, σύμφωνα με τα 3.2.9 (ii) και (iii),

$$\begin{aligned} g^m g^n &= \left(g^{-m}\right)^{-1}\left(g^{-n}\right)^{-1} = \left(g^{-n}g^{-m}\right)^{-1} \\ &= \left(g^{-(n+m)}\right)^{-1} = \left(g^{-(m+n)}\right)^{-1} = g^{m+n}. \end{aligned}$$

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 (βλ. 1.7.28), 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 3.2.9 (ii). Έχοντας τις

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

ως επαγωγική μας υπόθεση, μέσω τού (i) και των 3.2.9 (ii), (iii) λαμβάνουμε

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

και

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

Τούτο ολοκληρώνει την απόδειξη. □

3.2.12 Παρατήρηση. Όταν ένα στοιχείο $g \in G$ γράφεται ως «γινόμενο» $g = xy$ δυο στοιχείων x, y τής G, το «τετράγωνό του» $g^2 = (xy)^2 = (xy)(xy)$ *δεν ισούται* κατ' ανάκην με το x^2y^2!

► **Υποομάδες**. Η υποδομή που αντιστοιχεί στην αλγεβρική δομή τής ομάδας είναι η *υποομάδα*.

3.2.13 Ορισμός. Ένα μη κενό υποσύνολο H (τού υποκειμένου συνόλου G) μιας ομάδας $(G, \cdot)$ καλείται **υποομάδα** τής G όταν το H είναι κλειστό ως προς την πράξη τής G (βλ. 1.5.2) και καθίσταται αφ' εαυτού μια ομάδα (ως προς τον περιορισμό της $\cdot|_H$ επ' αυτού). Όταν η H είναι υποομάδα μιας ομάδας G και $H \subsetneqq G$, τότε η H λέγεται, ιδιαιτέρως, **γνήσια υποομάδα** τής G.

3.2.14 Παρατήρηση. Για τον έλεγχο τού κατά πόσον ένα μη κενό υποσύνολο H μιας ομάδας $(G, \cdot)$ είναι ή δεν είναι υποομάδα τής $(G, \cdot)$ *δεν* απαιτείται ο έλεγχος τής ισχύος τής προσεταιριστικής ιδιότητας, διότι για κάθε τριάδα $(x, y, z) \in H^3$ έχουμε αυτομάτως $(x, y, z) \in G^3$, οπότε $x(yz) = (xy)z$. Η επόμενη 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 $(G, \cdot)$.

3.2.15 Πρόταση. *Έστω* $(G, \cdot)$ *μια ομάδα και έστω* $H \subseteq G$. *Τότε τα* (i), (ii) *και* (iii) *είναι ισοδύναμα*:

(i) *Το* H *είναι μια υποομάδα τής* G.

(ii) *Το* H *πληροί τις εξής συνθήκες*:

(a) *Το ουδέτερο στοιχείο τής G ανήκει στο H.*

(b) *Εάν $(x, y) \in H \times H$, τότε $xy \in H$.*

(c) *Εάν $h \in H$, τότε $h^{-1} \in H$.*

(iii) *Το H πληροί τις εξής συνθήκες*:

(a) *Το ουδέτερο στοιχείο τής G ανήκει στο H.*

(b) *Εάν $(a, b) \in H \times H$, τότε $ab^{-1} \in H$.*

ΑΠΟΔΕΙΞΗ. (i) $\Longrightarrow$ (ii). Εάν το H είναι μια υποομάδα τής 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. 3.2.9 (iv)) δίδει $e_G = e_H$.

(ii) $\Longrightarrow$ (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) $\Longrightarrow$ (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

$$\forall (x, y) \in H \times H \Longrightarrow xy \in H.$$

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 η H είναι μια υποομάδα τής G. □

3.2.16 Παρατήρηση. Οι συνθήκες (ii) (a) και (iii) (a) συμπεριελήφθησαν στην πρόταση 3.2.15 μόνον για να μας εγγυηθούν ότι το θεωρούμενο σύνολο H δεν είναι κενό. Επί παραδείγματι, εάν το H διαθέτει τουλάχιστον ένα στοιχείο, τότε εφαρμόζοντας την (iii) (b) με $a = b$, λαμβάνουμε $e_G \in H$.

3.2.17 Παραδείγματα. (i) Κάθε ομάδα έχει πάντοτε δύο προφανείς υποομάδες, ήτοι τον εαυτό της και την **τετριμμένη υποομάδα** που αποτελείται -εξ ορισμού- μόνον από το ουδέτερο στοιχείο της.

(ii) Η ομάδα $(\mathbb{Z}^{\times} = \{1, -1\}, \cdot)$ είναι υποομάδα τής $(\mathbb{Q}\setminus\{0\}, \cdot)$ (όπως έπεται άμεσα από την πρόταση 3.2.15).

(iii) Έστω $n \in \mathbb{Z}$ και έστω $n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\}$ το σύνολο όλων των ακεραίων πολλαπλασίων του. Τότε, εφαρμόζοντας την πρόταση 3.2.15, διαπιστώνουμε ότι το $(n\mathbb{Z}, +)$ είναι μια υποομάδα τής $(\mathbb{Z}, +)$.

(iv) Οι εγκλεισμοί $\mathbb{Z} \subsetneqq \mathbb{Q}$, $\mathbb{Z} \subsetneqq \mathbb{R}$, $\mathbb{Z} \subsetneqq \mathbb{C}$, $\mathbb{Q} \subsetneqq \mathbb{R}$, $\mathbb{Q} \subsetneqq \mathbb{C}$ και $\mathbb{R} \subsetneqq \mathbb{C}$ καθιστούν αυτά τα υποσύνολα υποομάδες ως προς την πράξη τής συνήθους προσθέσεως.

(v) Οι εγκλεισμοί $\mathbb{Q}\setminus\{0\} \subsetneqq \mathbb{R}\setminus\{0\}$, $\mathbb{Q}\setminus\{0\} \subsetneqq \mathbb{C}\setminus\{0\}$ και $\mathbb{R}\setminus\{0\} \subsetneqq \mathbb{C}\setminus\{0\}$ καθιστούν αυτά τα υποσύνολα υποομάδες ως προς την πράξη τού συνήθους πολλαπλασιασμού.

(vi) Ο **μοναδιαίος κύκλος**

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

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

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

είναι υποομάδα τής $(\mathbb{S}^1, \cdot)$, καθότι $1 \in \mathcal{E}_n$ και για οιαδήποτε $z_1, z_2 \in \mathcal{E}_n$ έχουμε

$$\left(z_1 z_2^{-1}\right)^n = z_1^n z_2^{-n} = 1 \Rightarrow z_1 z_2^{-1} \in \mathcal{E}_n.$$

(vii) Έστω $F \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p\}$ (όπου p πρώτος αριθμός) και έστω $n \in \mathbb{N}$. Το σύνολο

$$\boxed{\mathrm{SL}_n(F) := \{\mathbf{A} \in \mathrm{GL}_n(F) \mid \det(\mathbf{A}) = 1_F\},}$$

εφοδιασμένο με τον πολλαπλασιασμό $(n \times n)$-πινάκων, αποτελεί υποομάδα τής $(\mathrm{GL}_n(F), \cdot)$ (βλ. 3.2.7 (iv)), διότι $\mathbf{I}_n \in \mathrm{SL}_n(F)$ και για οιουσδήποτε πίνακες $\mathbf{A}, \mathbf{B} \in \mathrm{SL}_n(F)$ έχουμε

$$\det\left(\mathbf{A}\mathbf{B}^{-1}\right) = \det(\mathbf{A}) \det\left(\mathbf{B}^{-1}\right) = \det(\mathbf{A}) \det(\mathbf{B})^{-1} = 1_F.$$

Η $(\mathrm{SL}_n(F), \cdot)$ καλείται **ειδική γραμμική ομάδα** (υπεράνω τού F).

(viii) Από τη θεωρία πινάκων με τις εγγραφές τους ειλημμένες από τους πραγματικούς αριθμούς προκύπτει ο ακόλουθος «πύργος» πολλαπλασιαστικών υποομάδων

$$\boxed{\begin{array}{ccc} \mathrm{GL}_n(\mathbb{R}) = \{\mathbf{A} \in \mathrm{Mat}_{n\times n}(\mathbb{R}) \mid \det(\mathbf{A}) \neq 0\} & \supsetneqq & \mathrm{SL}_n(\mathbb{R}) \\ \cup & & \\ \mathrm{O}_n(\mathbb{R}) := \left\{\mathbf{A} \in \mathrm{GL}_n(\mathbb{R}) \;\middle|\; \mathbf{A}^t = \mathbf{A}^{-1}\right\} & & \\ \cup & & \\ \mathrm{SO}_n(\mathbb{R}) := \mathrm{O}_n(\mathbb{R}) \cap \mathrm{SL}_n(\mathbb{R}), & & \end{array}}$$

όπου $\mathbf{A}^t$ ο ανάστροφος[7] ενός $\mathbf{A} \in \mathrm{GL}_n(\mathbb{R})$. Η $\mathrm{O}_n(\mathbb{R})$ 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

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

όπου $\overline{\mathbf{A}}^t$ ο αναστροφοσυζυγής[8] ενός $\mathbf{A} \in \mathrm{GL}_n(\mathbb{C})$. Η $\mathrm{U}_n(\mathbb{C})$ καλείται **μοναδιακή** και η $\mathrm{SU}_n(\mathbb{C})$ **ειδική μοναδιακή ομάδα**.

3.2.18 Πρόταση. *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.

ΑΠΟΔΕΙΞΗ. Επειδή $e_G \in H_j$ για κάθε $j \in J$, έχουμε $e_G \in \bigcap\limits_{j\in J} H_j$, οπότε η τομή αυτή δεν είναι κενή. Εάν $h_1, h_2 \in \bigcap\limits_{j\in J} H_j$, 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 η $\bigcap\limits_{j\in J} H_j$ είναι όντως μια υποομάδα τής G (βλ. 3.2.15 (iii)). □

3.2.19 Σημείωση. Η ένωση δυο υποομάδων μιας δεδομένης ομάδας G δεν είναι πάντοτε υποομάδα τής G. (Βλ. άσκηση ??)

► **Υποομάδες παραγόμενες από σύνολα**. 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.

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

[8] Ο **συζυγής** ενός πίνακα (με τις εγγραφές του ειλημμένες από το $\mathbb{C}$) είναι αυτός που προκύπτει ύστερα από αντικατάσταση καθεμιάς των εγγραφών του με τον συζυγή της μιγαδικό αριθμό. Ο **αναστροφοσυζυγής** ενός πίνακα (με τις εγγραφές του ειλημμένες από το $\mathbb{C}$) είναι εξ ορισμού ο ανάστροφος τού συζυγούς του.

3.2.20 Ορισμός. Για *τυχόν υποσύνολο* X τού υποκειμένου συνόλου G μιας ομάδας $(G,\cdot)$, χαρακτηρίζουμε την τομή[9]

$$\boxed{\langle X\rangle := \bigcap \{\text{υποομάδες } H \text{ τής } G \mid X \subseteq H\},} \tag{3.2}$$

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

3.2.21 Πρόταση. *Εάν*[10] $X \neq \varnothing$, *τότε η υποομάδα* (3.2)*, για την οποία λέμε ότι έχει το* X *ως* ***το σύνολο ή το σύστημα γεννητόρων*** *της, ισούται με*

$$\langle X\rangle = \left\{ g = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k} \;\middle|\; (x_1,..,x_k) \in X^k \text{ και } \varepsilon_j \in \mathbb{Z},\ \forall j, 1 \leq j \leq k,\ k \in \mathbb{N} \right\}.$$

ΑΠΟΔΕΙΞΗ. Το σύνολο

$$K := \left\{ g = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k} \;\middle|\; (x_1,\ldots,x_k) \in X^k \text{ και } \varepsilon_j \in \mathbb{Z},\ \forall j,\ 1 \leq j \leq k,\ k \in \mathbb{N} \right\}$$

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

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

(πρβλ. 3.2.9 (iii) και 3.2.15 (iii)). Επειδή $x = x^1 \in K$ για *κάθε* $x \in X$, λαμβάνουμε $X \subseteq K$. Αρκεί λοιπόν να αποδειχθεί ότι το K είναι η ελαχίστη 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 K, έχουμε

$$(x_j \in B \text{ και } \varepsilon_j \in \mathbb{Z},\ \forall j \in \{1,...,k\}) \Longrightarrow x_j^{\varepsilon_j} \in B,$$

οπότε $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k} \in B$. Εξ αυτού συνάγουμε ότι το K είναι υποομάδα τής B, ήτοι ότι $\langle X\rangle = K$. □

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

3.2.23 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 σύνολο των πρώτων αριθμών αποτελεί ένα σύνολο γεννητόρων τής ομάδας $(\mathbb{Q}_{>0},\cdot)$ (βλ. παρατήρηση 2.3.9).

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

[10] Εάν $X = \varnothing$, τότε η $\langle X\rangle$ είναι η *τετριμμένη* υποομάδα τής G (αποτελούμενη μόνον από το ουδέτερο στοιχείο της).

3.2.24 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

$$\boxed{\mathbf{Q} := \langle \mathbf{j}, \mathbf{k} \rangle \subset \mathrm{SU}_2(\mathbb{C})}$$

η παραγόμενη από τους πίνακες $\mathbf{j}$ και $\mathbf{k}$, καλείται **ομάδα των τετρανίων** και (όπως διαπιστώνεται εύκολα) έχει τάξη 8, καθότι

$$\mathbf{Q} = \left\{ \begin{array}{c} \mathbf{j},\, \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{I}_2,\, \mathbf{j}^3 = -\mathbf{j},\, \mathbf{j}^4 = \mathbf{k}^4 = \mathbf{I}_2,\, \mathbf{k}, \\ \mathbf{k}^3 = -\mathbf{k},\ \mathbf{jk} = \mathbf{i},\ \ \mathbf{jk}^3 = \mathbf{kj} = -\mathbf{jk} = -\mathbf{i} \end{array} \right\}.$$

Σημειωτέον ότι η $\mathbf{Q}$ δεν είναι αβελιανή (αφού $\mathbf{kj} \neq \mathbf{jk}$) και ότι ο πολλαπλασιαστικός της κατάλογος (όπου $\mathbf{I} := \mathbf{I}_2$) είναι ο εξής:

$\cdot$	$\mathbf{I}$	$-\mathbf{I}$	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{j}$	$-\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$
$\mathbf{I}$	$\mathbf{I}$	$-\mathbf{I}_2$	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{j}$	$-\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$
$-\mathbf{I}$	$-\mathbf{I}$	$\mathbf{I}$	$-\mathbf{i}$	$\mathbf{i}$	$-\mathbf{j}$	$\mathbf{j}$	$-\mathbf{k}$	$\mathbf{k}$
$\mathbf{i}$	$\mathbf{i}$	$-\mathbf{i}$	$-\mathbf{I}$	$\mathbf{I}$	$\mathbf{k}$	$-\mathbf{k}$	$-\mathbf{j}$	$\mathbf{j}$
$-\mathbf{i}$	$-\mathbf{i}$	$\mathbf{i}$	$\mathbf{I}$	$-\mathbf{I}$	$-\mathbf{k}$	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{j}$
$\mathbf{j}$	$\mathbf{j}$	$-\mathbf{j}$	$-\mathbf{k}$	$\mathbf{k}$	$-\mathbf{I}$	$\mathbf{I}$	$\mathbf{i}$	$-\mathbf{i}$
$-\mathbf{j}$	$-\mathbf{j}$	$\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$	$\mathbf{I}$	$-\mathbf{I}$	$-\mathbf{i}$	$\mathbf{i}$
$\mathbf{k}$	$\mathbf{k}$	$-\mathbf{k}$	$\mathbf{j}$	$-\mathbf{j}$	$-\mathbf{i}$	$\mathbf{i}$	$-\mathbf{I}$	$\mathbf{I}$
$-\mathbf{k}$	$-\mathbf{k}$	$\mathbf{k}$	$-\mathbf{j}$	$\mathbf{j}$	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{I}$	$-\mathbf{I}$

3.2.25 Ορισμός. Μια ομάδα καλείται **κυκλική** (ή **μονογενής**) όταν μπορεί να παραχθεί (υπό την έννοια τού 3.2.20) από ένα *μονοσύνολο*.

3.2.26 Παραδείγματα. (i) $\mathrm{H}(\mathbb{Z}, +)$ (όπως προαναφέραμε στο 3.2.23) είναι κυκλική. Το ίδιο ισχύει και για την $(n\mathbb{Z}, +)$, για οιονδήποτε $n \in \mathbb{Z}$.

(ii) $\mathrm{H}(\mathbb{Z}_m, +)$ είναι κυκλική, αφού παράγεται από την κλάση ισοτιμίας $[1]_m$.

(iii) $\mathrm{H}(\mathbb{Q}, +)$ δεν είναι κυκλική, καθότι για κάθε $r \in \mathbb{Q} \setminus \{0\}$ η $\{nr \mid n \in \mathbb{Z}\}$ είναι μια *γνήσια* υποομάδα τής $(\mathbb{Q}, +)$. Πράγματι· εάν η $(\mathbb{Q}, +)$ παρήγετο από κάποιον $r \in \mathbb{Q} \setminus \{0\}$, όπου $r = \frac{a}{b}$, $a, b \in \mathbb{Z} \setminus \{0\}$, τότε κάθε ρητός αριθμός s θα όφειλε να γράφεται υπό τη μορφή $s = nr$, για κάποιον $n \in \mathbb{Z}$. Π.χ., για τον $s = \frac{1}{2b}$ θα υπήρχε κάποιος $n \in \mathbb{Z}$ για τον οποίο θα ίσχυε η ισότητα $\frac{1}{2b} = n\frac{a}{b}$, πράγμα άτοπο, καθότι δεν υφίσταται $a \in \mathbb{Z} \setminus \{0\}$ με $2na = 1$.

3.2.27 Πρόταση. *Κάθε κυκλική ομάδα είναι αβελιανή.*

ΑΠΟΔΕΙΞΗ. Έστω $(G,\cdot)$ μια ομάδα. Εάν $G=\langle g\rangle$ (για κάποιο $g\in G$), και εάν $(x,y)\in G^2$, τότε $x=g^m$ και $y=g^n$, για κάποιους ακεραίους αριθμούς m και n. Ως εκ τούτου, βάσει τού (i) τής προτάσεως 3.2.11 λαμβάνουμε

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

οπότε η G είναι όντως αβελιανή. □

3.2.28 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» $g^n, n=0,\pm1,\pm2,\dots$ 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,*

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

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 $g^\nu,\nu\in\mathbb{N}$, ένα τυχόν στοιχείο τής $\langle g\rangle$. Δυνάμει τής ταυτότητας (2.1) τής ευκλείδειας διαιρέσεως υπάρχουν μοναδικοί ακέραιοι q,r με $0\le r<l$, τέτοιοι ώστε να ισχύει $\nu=ql+r$. Κατά συνέπειαν,

$$g^\nu=g^{ql+r}=g^{ql}g^r=g^{lq}g^r=\left(g^l\right)^q g^r=e_G^qg^r=e_Gg^r=g^r.$$

Απομένει λοιπόν να αποδειχθεί ότι τα στοιχεία $e_G,g,g^2,\dots,g^{l-1}$ είναι σαφώς διακεκριμένα. Εάν υποτεθεί ότι υπάρχουν $\mu,\nu\in\{0,1,\dots,l-1\}$, για τους οποίους ισχύει $\mu>\nu$ και

$$g^\mu=g^\nu,$$

τότε $g^{\mu-\nu}=e_G$, $1\le\mu-\nu\le l-1$, πράγμα που αντίκειται στην επιλογή τού l ως τού ελαχίστου εκθέτη με αυτήν την ιδιότητα. □

3.2.29 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.*

ΑΠΟΔΕΙΞΗ. (i) Έστω H μια υποομάδα τής ομάδας $(\mathbb{Z},+)$. Εάν η H είναι τετριμμένη, τότε είναι προφανώς κυκλική. Εάν η H δεν είναι τετριμμένη, τότε περιέχει έναν ακέραιο x διάφορο τού μηδενός και, επειδή η H είναι μια υποομάδα, θα

έχουμε και $-x \in H$. 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 $n = qd + m$, όπου οι q και m είναι ακέραιοι και $0 \leq m < d$, ήτοι $m \equiv n \,(\mathrm{mod}\, d)$. Γνωρίζουμε ότι $n \in H$ και $d \in H$. Επειδή η H είναι μια υποομάδα, έχουμε $qd \in H$, οπότε $-qd \in H$, απ' όπου συμπεραίνουμε ότι

$$m = n - qd = n + (-qd) \in H.$$

Αυτό όμως αντιφάσκει προς την επιλογή τού d, εκτός και εάν ο m 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. □

3.2.30 Ορισμός. Έστω $(G, \cdot)$ μια ομάδα. Τότε **η τάξη** $\mathrm{ord}(g)$ **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**). Όταν η ίδια η G είναι μια *πεπερασμένη* ομάδα, τότε προφανώς όλα της τα στοιχεία έχουν πεπερασμένη τάξη.

3.2.31 Παρατήρηση. Εάν $g \in G$, τότε, σύμφωνα με την πρόταση 3.2.28, έχουμε:

$$\boxed{\mathrm{ord}\,(g) = |\langle g \rangle|\,.} \tag{3.3}$$

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

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

ΑΠΟΔΕΙΞΗ. Εάν η G είναι κυκλική, τότε υπάρχει ένα $g \in G$ με $G = \langle g \rangle$, οπότε -βάσει τής (3.3)-

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

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

$$\left.\begin{array}{c} |\langle g \rangle| = |G| \\ \langle g \rangle \subseteq G \end{array}\right\} \Longrightarrow G = \langle g \rangle \,,$$

πρβλ. λήμμα 1.12.5 και παρατήρηση 1.12.6. □

3.2.34 Πρόταση. *Έστω $(G, \cdot)$ μια ομάδα. Εάν $g \in G$ και $\text{ord}(g) = n \in \mathbb{N}$, 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 $\exists\,(q, r) \in \mathbb{Z}^2$:

$$m = nq + r, \quad 0 \leq r < n.$$

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 $n \,|m$. □

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

(iii) $\text{ord}(gh) = \text{ord}(hg)\,, \forall (g, h) \in G \times G.$

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

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

$$\begin{array}{l} \left(g^{-1}\right)^m = e_G \Longrightarrow g^{-m} = e_G \Longrightarrow (g^{-m})^{-1} = e_G^{-1} = e_G \\ \Longrightarrow g^m = e_G \underset{\text{(βλ. 3.2.34)}}{\Longrightarrow} n \,|m \Longrightarrow n \leq m. \end{array}$$

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

$$\text{ord}\left(g^{-1}\right) = n \Longrightarrow \text{ord}\left(\left(g^{-1}\right)^{-1}\right) = \text{ord}\left(g\right) = n.$$

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

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

(ii) Έστω $(g, h) \in G^2$ με $\text{ord}(g) = n \in \mathbb{N}$. Κατά την άσκηση ?? ισχύει η ισότητα

$$\left(h^{-1}gh\right)^n = h^{-1}g^n h,$$

και επειδή -εξ υποθέσεως- $g^n = e_G$, έχουμε

$$\left(h^{-1}gh\right)^n = h^{-1}e_G h = h^{-1}h = e_G.$$

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

$$\left(h^{-1}gh\right)^m = h^{-1}g^m h = e_G \Longrightarrow hh^{-1}g^m hh^{-1} = he_G h^{-1} \Longrightarrow g^m = e_G,$$

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

$$\text{ord}\left(h^{-1}gh\right) = n \Longrightarrow \text{ord}\left(h\left(h^{-1}gh\right)h^{-1}\right) = \text{ord}\left(g\right) = n.$$

Εν συνεχεία, υποθέτουμε ότι $\text{ord}(g) = \infty$. Εάν $\text{ord}\left(h^{-1}gh\right) \neq \infty$, τότε θα υπήρχε ένας φυσικός αριθμός n με $n = \text{ord}\left(h^{-1}gh\right)$, πράγμα αδύνατο, διότι σε αυτήν την περίπτωση θα είχαμε κατ' ανάγκην και $\text{ord}(g) = n$ (βάσει των όσων προαναφέραμε). Και αντιστρόφως· εάν $\text{ord}\left(h^{-1}gh\right) = \infty$, τότε, με εκ νέου εφαρμογή τής ήδη αποδειχθείσας συνεπαγωγής (και εναλλαγή των ρόλων των g και $h^{-1}gh$, καθώς και των h και h^{-1}) λαμβάνουμε

$$\text{ord}\left(h^{-1}gh\right) = \infty \Longrightarrow \text{ord}\left(h\left(h^{-1}gh\right)h^{-1}\right) = \text{ord}\left(g\right) = \infty.$$

(iii) Επειδή $hg = g^{-1}\left(gh\right)g$, τα hg και gh 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. □

3.2.36 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 3.2.29 η $H = \langle a \rangle$ είναι μια κυκλική υποομάδα τής G. Αρκεί λοιπόν να προσδιορίσουμε την τάξη της. Σύμφωνα με την πρόταση 3.2.34, εάν $k \in \mathbb{N}$, τότε $a^k = e_G \iff g^{nk} = e_G \iff m\,|nk$. Άρα

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

Έστω $d := \text{μκδ}(m,n)$. Τότε, επί τη βάσει τού θεωρήματος 2.2.5 υπάρχουν $\mu, \nu \in \mathbb{Z}$, τέτοιοι ώστε

$$d = \mu m + \nu n \iff 1 = \mu\left(\frac{m}{d}\right) + \nu\left(\frac{n}{d}\right). \tag{3.4}$$

Από την τελευταία ισότητα συνάγουμε ότι οι $\frac{m}{d}$ και $\frac{n}{d}$ είναι σχετικώς πρώτοι. Το ζητούμενο είναι ο προσδιορισμός τού ελαχίστου φυσικού αριθμού k, για τον οποίο

$$\frac{nk}{m} = \frac{k\left(\frac{n}{d}\right)}{\left(\frac{m}{d}\right)} \in \mathbb{Z}.$$

Επειδή $\text{μκδ}(\frac{n}{d}, \frac{m}{d}) = 1$, η ανωτέρω συνθήκη ισοδυναμεί με την: $\frac{m}{d} \big|\, k$ (βλ. πόρισμα 2.2.10). Κατά συνέπειαν,

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

(ii) Επειδή $a = g^n = g^{d\left(\frac{n}{d}\right)} = \left(g^d\right)^{\frac{n}{d}} \Longrightarrow g^n \in \left\langle g^d \right\rangle$, η H είναι μια υποομάδα τής $\left\langle g^d \right\rangle$. Από την άλλη μεριά, λόγω τής (3.4),

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

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

3.2.37 Πόρισμα. *Έστω $(G,\cdot)$ μια ομάδα και έστω $(m,n) \in \mathbb{N}^2$. Τότε*

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

ΑΠΟΔΕΙΞΗ. Προφανής βάσει τής προτάσεως 3.2.36 και τού (3.3). □

3.2.38 Πόρισμα. *Έστω $(G,\cdot)$ μια ομάδα και έστω $(m,n)\in\mathbb{N}^2$. Τότε*

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

3.2.39 Παραδείγματα. (i) Εάν η $(G,\cdot)$ είναι μια ομάδα, $g\in G$ και $\text{ord}(g)=12$, 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 $\text{ord}([4]_{48})=12$, 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:

3.2.40 Πόρισμα. *Έστω m ένας φυσικός αριθμός ≥ 2. Τότε για κάθε $n\in\mathbb{Z}$ η τάξη τού στοιχείου $[n]_m$ τής ομάδας $(\mathbb{Z}_m,+)$ δίδεται από τον τύπο*:

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

ΑΠΟΔΕΙΞΗ. Επειδή $|\mathbb{Z}_m|=m$,

$$\mathbb{Z}_m=\langle[1]_m\rangle\Longrightarrow\ \text{ord}\,([1]_m)=|\langle[1]_m\rangle|=m,$$

και $[n]_m=n\,[1]_m$, συνάγουμε την ισότητα

$$\text{ord}\,([n]_m)=\text{ord}\,(n\,[1]_m)=\frac{m}{\text{μκδ}\,(m,n)}$$

μέσω εφαρμογής τού πορίσματος 3.2.37. □

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

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

ΑΠΟΔΕΙΞΗ. Εάν $\langle g^k\rangle = \langle g^l\rangle$, τότε $\left|\langle g^k\rangle\right| = \left|\langle g^l\rangle\right|$, και από την πρόταση 3.2.36 (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 μκδ$(k,m) = $ μκδ$(l,m) =: d$, τότε, βάσει τής 3.2.36 (ii), ισχύει η ισότητα $\langle g^k\rangle = \langle g^d\rangle = \langle g^l\rangle$. □

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

$$\text{card}\,(\{\text{γεννήτορες τής } G\}) = \varphi\,(m)\,,$$

όπου φ *η συνάρτηση τού Euler (βλ.* 2.4.16*).*

3.2.43 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:

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

Η εύρεση των υποομάδων μιας δεδομένης ομάδας -*όταν* είναι εφικτή- μας επιφυλάσσει μια ως επί το πλείστον επίπονη διαδικασία. Ωστόσο, στην ειδική περίπτωση κατά την οποία θεωρούμε μόνον *κυκλικές ομάδες*, το θεώρημα 3.2.44 και τα συνακόλουθα πορίσματα 3.2.45 και 3.3.16 μας παρέχουν μια πλήρη (και αρκετά εύκολη) περιγραφή τόσον τού τρόπου σχηματισμού όσον και τού πλήθους των διαθέσιμων υποομάδων.

3.2.44 Θεώρημα. *Έστω* $G = \{e, g, g^2, \ldots, g^{m-1}\}$ *μια πεπερασμένη κυκλική ομάδα τάξεως* $m \geq 2$ *(όπου* $e = e_G$*). Τότε ισχύουν τα εξής:*

(i) *Όταν* $n \in \mathbb{N}$*, 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 3.2.38-

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

δηλαδή η $\left\langle g^{\frac{m}{n}} \right\rangle$ έχει τάξη ίση με n. Και αντιστρόφως· εάν η H είναι μια μη τετριμμένη[11] υποομάδα τής G τάξεως n και $H = \left\langle g^k \right\rangle$, για κάποιον $k \in \{1, \dots, m-1\}$ (πρβλ. 3.2.29 (ii)), τότε (λόγω τής 3.2.36 (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 (μη τετριμμένες) υποομάδες τής G τάξεως n και ότι

$$H_1 = \left\langle g^{k_1} \right\rangle, \quad H_2 = \left\langle g^{k_2} \right\rangle,$$

για κάποιους $k_1, k_2 \in \{1, \dots, m-1\}$. Τότε

$$|H_1| = \frac{m}{\text{μκδ}\,(m,k_1)} = n = \frac{m}{\text{μκδ}\,(m,k_2)} = |H_2| \Longrightarrow \text{μκδ}\,(m,k_1) = \text{μκδ}\,(m,k_2)\,.$$

Όμως -κατά την πρόταση 3.2.36 (ii)- τούτο σημαίνει ότι $H_1 = H_2$. □

3.2.45 Πόρισμα. *Έστω ότι η* $G = \{e, g, g^2, \dots, g^{m-1}\}$ *είναι μια πεπερασμένη κυκλική ομάδα τάξεως* $m \geq 2$ (*όπου* $e = e_G$) *και ότι οι*[12]

$$d_1, d_2, \dots, d_\nu$$

είναι οι θετικοί διαιρέτες τού m. *Τότε οι*

$$\left\langle g^{d_1} \right\rangle, \left\langle g^{d_2} \right\rangle, \dots, \left\langle g^{d_\nu} \right\rangle$$

είναι όλες οι σαφώς διακεκριμένες (*ήτοι διαφορετικές μεταξύ τους ανά ζεύγη*) *υποομάδες τής* G.

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

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

απ' όπου έπεται ότι $j = j'$. □

3.2.46 Παράδειγμα. Οι υποομάδες τής (προσθετικής) ομάδας

$$\mathbb{Z}_8 = \{[0]_8, [1]_8, [2]_8, [3]_8, [4]_8, [5]_8, [6]_8, [7]_8\}$$

είναι η τετριμμένη $\{[0]_8\}$, ολόκληρη η $\mathbb{Z}_8$, καθώς και οι

$$\langle [2]_8 \rangle = \{[0]_8, [2]_8, [4]_8, [6]_8\}, \quad \langle [4]_8 \rangle = \{[0]_8, [4]_8\}.$$

[11] Εάν η H είναι τετριμμένη, τότε ο ισχυρισμός είναι προφανής.

[12] Στη Στοιχειώδη Θεωρία Αριθμών αυτός ο πληθικός αριθμός ν όλων των θετικών διαιρετών τού m συμβολίζεται συνήθως ως $\tau\,(m)$.

3.3 ΟΜΟΜΟΡΦΙΣΜΟΙ, ΙΣΟΜΟΡΦΙΣΜΟΙ ΚΑΙ ΑΥΤΟΜΟΡΦΙΣΜΟΙ ΟΜΑΔΩΝ

3.3.1 Ορισμός. Έστω ότι οι $(G,\cdot)$ και $(H,*)$ είναι δυο ομάδες. Μια απεικόνιση[13] $f: G \longrightarrow H$ καλείται **ομομορφισμός (ομάδων)** όταν για οιαδήποτε $x, y \in G$ ισχύει η ισότητα

$$\boxed{f(x\cdot y) = f(x) * f(y)} \tag{3.5}$$

3.3.2 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

$$(\mathbb{R},+) \longrightarrow (\mathbb{R}\setminus\{0\},\cdot)\,,\quad x \longmapsto \exp(x)\,,$$

αποτελεί έναν ομομορφισμό ομάδων.

3.3.3 Πρόταση. *Εάν η $f : (G,\cdot) \longrightarrow (H,*)$ είναι ένας ομομορφισμός ομάδων, τότε ισχύουν τα εξής*:
(i) $f(e_G) = e_H$.
(ii) $f(g)^{-1} = f\left(g^{-1}\right),\ \forall g \in G$.
(iii) $f(g)^n = f(g^n),\ \forall g \in G$ *και* $\forall n \in \mathbb{Z}$.

ΑΠΟΔΕΙΞΗ. (i) Επειδή λόγω τής (3.5), $f(e_G) * f(e_G) = f(e_G\cdot e_G) = f(e_G)$, έχουμε

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

(ii) Για κάθε $g \in G$,

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

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

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 $n < 0$, τότε $-n > 0$, οπότε εφαρμόζοντας το ανωτέρω αποδειχθέν για τον $-n$, το (ii), καθώς και το (iii) τής προτάσεως 3.2.11, λαμβάνουμε

$$f(g)^n = (f(g)^{-1})^{-n} = f(g^{-1})^{-n} = f((g^{-1})^{-n}) = f(g^n).$$

Τελικώς λοιπόν, $f(g)^n = f(g^n)$, $\forall g \in G$ και $\forall n \in \mathbb{Z}$. □

3.3.4 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 3.3.3 (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,

$$h * h'^{-1} = f(g) * f(g')^{-1} = f(g) * f(g^{-1}) = f(g \cdot g^{-1}) \in f(G),$$

οπότε η $f(G)$ είναι μια υποομάδα τής H δυνάμει τού (iii) τής προτάσεως 3.2.15.

(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

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

Συνεπώς $g \cdot g'^{-1} \in \mathrm{Ker}(f)$ και αρκεί να εφαρμόσουμε εκ νέου το (iii) τής προτάσεως 3.2.15. □

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

(i) *Η εικόνα $f(K)$ οιασδήποτε υποομάδας K τής G μέσω τής f είναι μια υποομάδα*

τής $f\,(G)$.

(ii) *Η αντίστροφη εικόνα* $f^{-1}\,(L) = \{\, g \in G \mid f(g) \in L\}$ *οιασδήποτε υποομάδας* L *τής* H *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 3.3.4 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 $e_G \in f\,(K)$. Εξάλλου, εάν $u, v \in f\,(K)$, τότε υπάρχουν στοιχεία $x, y \in K$ με $f(x) = u$ και $f(y) = v$. Κατά συνέπειαν,

$$u * v^{-1} = f(x) * f(y)^{-1} = f(x) * f(y^{-1}) = f(x \cdot y^{-1}) \in f(K),$$

οπότε η $f\,(K)$ είναι μια υποομάδα τής H δυνάμει τού (iii) τής προτάσεως 3.2.15.

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

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

διότι η L είναι υποομάδα τής G. Συνεπώς $x \cdot y^{-1} \in f^{-1}\,(L)$ και αρκεί να εφαρμόσουμε εκ νέου το (iii) τής προτάσεως 3.2.15. □

3.3.6 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 επιριπτική,
ισομορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι αμφιριπτική,
ενδομορφισμός (**τής** G)	$\underset{\text{ορσ}}{\Longleftrightarrow}$	$G = H$ και $\text{“}\cdot\text{”} = \text{“}*\text{”}$,
αυτομορφισμός (**τής** G)	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η f είναι αμφιριπτικός ενδομορφισμός τής G.

3.3.7 Παραδείγματα. (i) Η απεικόνιση

$$(\mathbb{R}, +) \longrightarrow (\mathbb{R}_{>0}, \cdot)\,, \quad x \longmapsto \exp(x)\,,$$

αποτελεί έναν ισομορφισμό ομάδων με αντίστροφό του τον $x \longmapsto \ln(x)$.

(ii) Οι ομομορφισμοί μ_a οι ορισθέντες στο 3.3.2 (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) Για κάθε $m \in \mathbb{N}$ υφίσταται ισομορφισμός

$$(\mathbb{Z}_m, +) \longrightarrow (\mathcal{E}_m, \cdot)\,, \quad [k]_m \longmapsto \exp(\frac{2\pi ik}{m}).$$

(v) 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:

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

3.3.8 Πρόταση. *Εάν οι $f : (G, \cdot) \longrightarrow (H, *)$ και $g : (H, *) \longrightarrow (K, \star)$ είναι δυο ομομορφισμοί ομάδων, τότε ισχύουν τα ακόλουθα*:

(i) *Η σύνθεση $g \circ f : G \longrightarrow K$ είναι ομομορφισμός ομάδων.*

(ii) *Εάν οι f και g είναι μονομορφισμοί (και αντιστοίχως, επιμορφισμοί/ισομορφισμοί), τότε και η σύνθεσή τους $g \circ f : G \longrightarrow K$ είναι μονομορφισμός (και αντιστοίχως, επιμορφισμός/ισομορφισμός).*

ΑΠΟΔΕΙΞΗ. (i) Για οιαδήποτε $x, y \in G$ έχουμε

$$\begin{aligned} (g \circ f)(x \cdot y) &= g(f(x \cdot y)) = g(f(x) * f(y)) \\ &= g(f(x)) \star g(f(y)) = (g \circ f)(x) \star (g \circ f)(y). \end{aligned}$$

(ii) Τούτο έπεται άμεσα από τα (i) και (ii) τής προτάσεως 1.2.15. □

3.3.9 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

$$f(g) = e_H = f(e_G) \underset{f\ 1\text{-}1}{\Longrightarrow} g = e_G.$$

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

$$f\left(g_2^{-1} \cdot g_1\right) = (f(g_2))^{-1} * f(g_1) = (f(g_2))^{-1} * f(g_2) = e_H,$$

οπότε $g_2^{-1} \cdot g_1 = e_G \Longrightarrow g_1 = g_2$. Άρα ο ομομορφισμός f είναι όντως ένας μονομορφισμός. □

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

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

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

(iii) *Η* G *είναι κυκλική εάν και μόνον εάν η* H *είναι κυκλική.*

(iv) $\text{ord}(g) = \text{ord}(f(g)), \forall g \in G$.

(v) *Εάν κάθε στοιχείο τής* G *έχει πεπερασμένη τάξη, τότε και κάθε στοιχείο τής* H *έχει πεπερασμένη τάξη (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,

$$\begin{aligned} h * h' &= f(g) * f(g') = f(g \cdot g') = f(g' \cdot g) \\ &= f(g') * f(g) = h' * h, \end{aligned}$$

και η H είναι, ως εκ τούτου, αβελιανή. Το αντίστροφο αποδεικνύεται παρομοίως.

(iii) Εάν $\exists g \in G : G = \langle g \rangle$, τότε, λόγω τής επιρριπτικότητας τής f, για *κάθε* $h \in H$ υπάρχει $\nu \in \mathbb{Z}$ με $h = f(g^\nu)$, οπότε από το (iii) τής προτάσεως 3.3.3 συμπεραίνουμε ότι

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

Το αντίστροφο αποδεικνύεται παρομοίως.

(iv) Έστω $g \in G$ τάξεως $\text{ord}(g) = n \in \mathbb{N}$. Τότε $g^n = e_G$, οπότε τα (i) και (iii) τής προτάσεως 3.3.3 μας δίδουν

$$f(g^n) = f(g)^n = f(e_G) = e_H \underset{3.2.34}{\Longrightarrow} \text{ord}(f(g)) = m \in \mathbb{N} \text{ και } m \mid n.$$

Επειδή $f(g)^m = f(g^m) = e_H \underset{3.2.34}{\Longrightarrow} g^m \in \text{Ker}(f) = \{e_G\} \Rightarrow g^m = e_G \Rightarrow n \mid m$, 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 $\exists n_g \in \mathbb{N} : g^{n_g} = e_G$. Έστω *τυχόν* στοιχείο $h \in H$. Τότε $\exists x \in G : h = f(x)$, οπότε μέσω των (i) και (iii) τής προτάσεως 3.3.3 συνάγουμε 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. □

3.3.11 Παράδειγμα. Είναι αδύνατον να υφίσταται ισομορφισμός μεταξύ των ομάδων $(\mathbb{Z},+)$ και $(\mathbb{Q},+)$, διότι η πρώτη εξ αυτών είναι κυκλική και η δεύτερη μη κυκλική (βλ. 3.2.26 (i) και (iii)).

3.3.12 Ορισμός. Έστω ότι οι $(G,\cdot)$ και $(H,*)$ είναι δυο ομάδες. Λέμε ότι η G είναι **ισόμορφη με την** H ή απλώς ότι είναι **ισόμορφη τής** H (και σημειώνουμε: $G\cong H$) όταν υπάρχει κάποιος ισομορφισμός ομάδων $f: G\longrightarrow H$.

3.3.13 Πρόταση. *Για οιεσδήποτε ομάδες* $(G,\cdot),(G',\cdot'),(G'',\cdot'')$ *ισχύουν τα εξής*:

(i) $G\cong G$,

(ii) $G\cong G'\Rightarrow G'\cong G$,

(iii) $[G\cong G'$ *και* $G'\cong G'']\Rightarrow G\cong G''$.

ΑΠΟΔΕΙΞΗ. (i) Η ταυτοτική απεικόνιση $\mathrm{id}_G: G\longrightarrow G$ είναι προφανώς ένας ισομορφισμός ομάδων.

(ii) Εάν ο $f: G\longrightarrow G'$ είναι ένας ισομορφισμός ομάδων, τότε, ως αμφιριπτική απεικόνιση, διαθέτει μια (μονοσημάντως ορισμένη, αμφιριπτική) αντίστροφο f^{-1}. Αρκεί λοιπόν να αποδειχθεί ότι η f^{-1} αποτελεί ομομορφισμό ομάδων. Εάν $x,y\in G'$, τότε υπάρχουν $a,b\in G$ με $x=f(a)$ και $y=f(b)$. Επομένως,

$$f^{-1}(x\cdot' y)=f^{-1}(f(a)\cdot' f(b))=f^{-1}(f(a\cdot b))=a\cdot b=f^{-1}(x)\cdot f^{-1}(y),$$

(αφού οι f, f^{-1} είναι αμφιριπτικές) και η f^{-1} αποτελεί ομομορφισμό ομάδων.

(iii) Εάν οι $f: G\longrightarrow G'$ και $g: G'\longrightarrow G''$ είναι δυο ισομορφισμοί ομάδων, τότε, σύμφωνα με το (ii) τής προτάσεως 3.3.8, *και* η σύνθεσή τους $g\circ f$ είναι ένας ισομορφισμός ομάδων. □

3.3.14 Σημείωση. Σύμφωνα με την πρόταση 3.3.13, η διμελής σχέση "$\cong$" ορίζει μια σχέση ισοδυναμίας επί οιουδήποτε συνόλου απαρτιζομένου από ομάδες (ή επί τής NBG-«κλάσεως» όλων των ομάδων). Ως εκ τούτου, δυο ομάδες λογίζονται ως (ομαδοθεωρητικώς) *ταυτιζόμενες* όταν είναι μεταξύ τους ισόμορφες. Το ακόλουθο θεώρημα μας παρέχει τη δυνατότητα πλήρους *ταξινομήσεως* των κυκλικών ομάδων *μέχρις ισομορφισμού.*

3.3.15 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 τής* $(\mathbb{Z},+)$.

(ii) *Εάν η* $(G,\cdot)$ *είναι πεπερασμένη ομάδα τάξεως* m, *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

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

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 $g^{\max\{n,n'\}-\min\{n,n'\}}=e_G$ (όπου e_G το ουδέτερο στοιχείο τής G), απ' όπου θα συνάγετο ότι η G είναι πεπερασμένη ομάδα (βλ. πρόταση 3.2.28), κάτι που θα αντέφασκε προς την υπόθεσή μας. Επιπροσθέτως, η εν λόγω απεικόνιση είναι και *ομομορφισμός ομάδων*, διότι (σύμφωνα με το 3.2.11 (i)) έχουμε

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

(ii) Εάν η $(G,\cdot)$ είναι πεπερασμένη ομάδα τάξεως m, τότε $G=\{e,g,g^2,...,g^{m-1}\}$ (όπου $e=e_G$) και η επιρριπτική απεικόνιση[14]

$$(\mathbb{Z}_m,+)\longrightarrow(G,\cdot),\ \ [n]_m\longmapsto g^n,\ \forall n\in\{0,1,...,m-1\},$$

είναι ένας ισομορφισμός ομάδων. Πράγματι· επειδή η εικόνα (μέσω τής ανωτέρω απεικονίσεως) τού $[n]_m+[n']_m=[n+n']_m=[n'']_m$ (όπου $n''\in\{0,1,...,m-1\}$ το υπόλοιπο που αφήνει το $n+n'$ διαιρούμενο διά τού m) είναι το

$$g^{n''}=g^{n+n'}=g^ng^{n'},\ \forall(n,n')\in\{0,1,...,m-1\}\times\{0,1,...,m-1\}$$

(βλ. 3.2.11 (i)), αυτή είναι *ομομορφισμός ομάδων*. Επιπροσθέτως, η εν λόγω απεικόνιση είναι και *μονομορφισμός ομάδων*, διότι ο πυρήνας της είναι (προφανώς) η τετριμμένη υποομάδα $\{[0]_m\}$ τής $(\mathbb{Z}_m,+)$ (βλ. πρόταση 3.3.9). □

3.3.16 Πόρισμα. (Ταξινόμηση υποομάδων κυκλικών ομάδων) *Έστω $(G,\cdot)$ μια κυκλική ομάδα. Τότε ισχύουν τα εξής*:

(i) *Εάν η G είναι άπειρη ομάδα και $G=\langle g\rangle$, για κάποιο $g\in G$, τότε, σύμφωνα με τα* 3.3.15 (i) *και* 3.2.29 (i), *οι υποομάδες της είναι ακριβώς οι κυκλικές ομάδες*[15] $\left\langle g^d\right\rangle$, *όπου $d\in\mathbb{N}_0$.*

(ii) *Εάν η G είναι πεπερασμένη ομάδα τάξεως $m\geq 2$, τότε οι υποομάδες της είναι ακριβώς αυτές που περιεγράφησαν στο πόρισμα* 3.2.45. (*Εάν $|G|=1$, τότε η G είναι η τετριμμένη ομάδα.*)

---

[14] Το ότι η απεικόνιση αυτή είναι *καλώς ορισμένη* αποδεικνύεται ως εξής: Εάν $n,n'\in\{0,1,...,m-1\}$, τέτοιοι ώστε να ισχύει η ισότητα $[n]_m=[n']_m$, τότε $\exists k\in\mathbb{Z}: n-n'=km$, οπότε $g^{n-n'}=(g^k)^m=e\Rightarrow g^n=g^{n'}$.

[15] 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 3.2.28.)

3.3.17 Πόρισμα. *Εάν μια ομάδα δεν διαθέτει άλλες υποομάδες πέραν τής τετριμμένης και τού εαυτού της, τότε είναι είτε κυκλική με τάξη της έναν πρώτο αριθμό είτε τετριμμένη.*

ΑΠΟΔΕΙΞΗ. Εάν μια ομάδα G με αυτήν την ιδιότητα δεν είναι τετριμμένη, τότε $\exists g \in G \setminus \{e_G\}$. Η κυκλική ομάδα $\langle g \rangle$ η παραγόμενη από αυτό το στοιχείο g είναι προφανώς μια μη τετριμμένη υποομάδα τής G, οπότε (εξ υποθέσεως) $G = \langle g \rangle$. Εάν η G ήταν είτε άπειρη κυκλική είτε πεπερασμένη κυκλική με τάξη της έναν *σύνθετο* φυσικό αριθμό, τότε θα όφειλε να διαθέτει και άλλες υποομάδες πέραν τής τετριμμένης και τού εαυτού της (λόγω των πορισμάτων 3.2.45 και 3.3.16). Άρα η G είναι κατ' ανάγκην μια πεπερασμένη κυκλική ομάδα με τάξη της έναν πρώτο αριθμό. □

3.3.18 Σημείωση. Εάν η G είναι μια τυχούσα ομάδα, τότε το σύνολο $\mathrm{Aut}(G)$ όλων των αυτομορφισμών τής G αποτελεί μια ομάδα ως προς την πράξη τής συνθέσεως απεικονίσεων[16]. Ας υποθέσουμε, επί παραδείγματι, ότι η G είναι η προσθετική ομάδα των ακεραίων αριθμών $\mathbb{Z}$. Κάθε αυτομορφισμός θ τής $\mathbb{Z}$ πρέπει να στέλνει το 1 να απεικονίζεται σε έναν ακέραιο αριθμό ο οποίος παράγει την $\mathbb{Z}$. Κατά συνέπειαν, $\theta(1) \in \{\pm 1\}$. Εάν $\theta(1) = 1$, τότε παίρνουμε τον ταυτοτικό αυτομορφισμό· ειδάλλως, $\theta(1) = -1$, και ο θ στέλνει κάθε ακέραιο αριθμό n να απεικονίζεται στον αντίθετό του $-n$. Βλέπουμε λοιπόν άμεσα ότι η $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

3.4 ΟΜΑΔΕΣ ΜΕΤΑΤΑΞΕΩΝ

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

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

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_G 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

$$\mathfrak{S}_A \longrightarrow \mathfrak{S}_B, \;\; \sigma \longmapsto f \circ \sigma \circ f^{-1},$$

[16] Αντιστοίχως, μπορούμε να εφοδιάσουμε και το σύνολο $\mathrm{End}(G)$ των *ενδομορφισμών* μιας ομάδας G με την ίδια εσωτερική πράξη. Εν προκειμένω, το ζεύγος $(\mathrm{End}(G), \circ)$ αποτελεί μόνον ένα μονοειδές (ήτοι μια ημιομάδα με ουδέτερο στοιχείο).

είναι ένας *ισομορφισμός ομάδων*). Τα στοιχεία τής ομάδας $\mathfrak{S}_A$ ονομάζονται **μεταττάξεις**[17]. Όταν $\sigma \in \mathfrak{S}_A \setminus \{\mathrm{id}_G\}$, η σ «μετατάσσει» *κυριολεκτικώς* τουλάχιστον ένα εκ των στοιχείων τού A, δηλαδή το απεικονίζει σε ένα άλλο (διαφορετικό) στοιχείο τού A. Εάν το θεωρούμενο A είναι ένα *πεπερασμένο* σύνολο και $n = \mathrm{card}(A)$, τότε μπορούμε δίχως βλάβη τής γενικότητας να υποθέσουμε ότι $A = \{1, ..., n\}$. Εν τοιαύτη περιπτώσει η $\mathfrak{S}_A$ συμβολίζεται ως $\mathfrak{S}_n$ και καλείται **συμμετρική ομάδα σε** n **σύμβολα**.

(ii) Συνήθως γράφουμε τις μετατάξεις $\sigma \in \mathfrak{S}_n$ υπό τη μορφή

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

ή

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ \sigma(x_1) & \sigma(x_2) & \cdots & \sigma(x_n) \end{bmatrix}$$

στην περίπτωση όπου τα $x_1, \ldots, x_n$ αποτελούν μια αναδιάταξη των αριθμών $1, 2, \ldots, n$. Αυτός ο τρόπος γραφής μάς διευκολύνει κατά τον υπολογισμό τής συνθέσεως δύο μετατάξεων. Π.χ.,

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{bmatrix}.$$

Θα πρέπει να επισημανθεί ότι κατά την εκτέλεση τής συνθέσεως *προηγείται* η εφαρμογή τής δεξιάς απεικονίσεως και *ακολουθεί* η εφαρμογή τής αριστεράς. Γενικότερα, για τυχούσες μετατάξεις τ και $\sigma \in \mathfrak{S}_n$ έχουμε

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

3.4.2 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

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

[17] 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.)

(ii) Για λόγους συντομίας, θα συμβολίζουμε το ουδέτερο στοιχείο $\mathrm{id}_{\{1,\ldots,n\}}$ της $\mathfrak{S}_n$ 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:

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

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

3.4.3 Πρόταση. *Η τάξη της ομάδας* $\mathfrak{S}_n$ *ισούται με*

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

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

Ισχυρισμός: *Εάν τα* $A = \{x_1, \ldots, x_n\}$ *και* $B = \{y_1, \ldots, y_n\}$ *είναι δυο σύνολα που περιέχουν* (*ακριβώς*) n *στοιχεία, τότε το σύνολο*

$$\mathbf{Bij}(A, B) := \{f : A \longrightarrow B \mid f \text{ αμφιρριπτική απεικόνιση}\}$$

έχει ακριβώς $n!$ *στοιχεία.*

Όταν $n = 1$, ο ισχυρισμός είναι προφανής. Ας υποθέσουμε πως για κάποιο $n > 1$ ισχύει η ισότητα

$$\mathrm{card}\,(\mathbf{Bij}(A', B')) = (n-1)!$$

για οιαδήποτε σύνολα A', B' που διαθέτουν (ακριβώς) $n-1$ στοιχεία. Έστω τώρα ότι τα $A = \{x_1, \ldots, x_n\}$ και $B = \{y_1, \ldots, y_n\}$ είναι δυο σύνολα που περιέχουν (ακριβώς) n στοιχεία. Για κάθε $i \in \{1, \ldots, n\}$ ορίζουμε το

$$\mathbf{Bij}(A, B)_i := \{f \in \mathbf{Bij}(A, B) \mid f(x_1) = y_i\}.$$

Προφανώς η απεικόνιση

$$\mathbf{Bij}(A, B)_i \longrightarrow \mathbf{Bij}(A \smallsetminus \{x_1\}, B \smallsetminus \{y_i\}), \quad f \longmapsto f|_{A \smallsetminus \{x_1\}},$$

είναι αμφιρριπτική. Επομένως, κατά την επαγωγική μας υπόθεση,

$$\mathrm{card}\,(\mathbf{Bij}(A, B)_i) = (n-1)!.$$

Επιπροσθέτως,

$$\mathbf{Bij}(A, B) = \coprod_{i=1}^{n} \mathbf{Bij}(A, B)_i.$$

Εξ αυτού συνάγουμε ότι

$$\text{card}\left(\mathbf{Bij}\left(A,B\right)\right)=\sum_{i=1}^{n}\text{card}\left(\mathbf{Bij}\left(A,B\right)_{i}\right)=n\cdot(n-1)!=n!.$$

(κατά το λήμμα 1.12.3). □

3.4.4 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 **ο φορέας τής** σ.

(ii) Λέμε ότι δυο μετατάξεις $\sigma,\tau\in\mathfrak{S}_n$ είναι **ξένες μεταξύ τους** όταν για οιουσδήποτε φυσικούς αριθμούς $j,k\in\{1,\ldots,n\}$ ισχύουν (ταυτοχρόνως) οι συνεπαγωγές

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

3.4.5 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 $\tau\left(k\right)\neq k$, 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. □

3.4.6 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.

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

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

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** (ή **αμοιβαίες μετατοπίσεις**).

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

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

και

$$[1\,3] \circ [1\,2] = [1\,2\,3], \qquad [2\,3] \circ [1\,2] = [1\,3\,2].$$

3.4.9 Πρόταση. *Οι k-κύκλοι (εντός τής $\mathfrak{S}_n$) έχουν τις ακόλουθες ιδιότητες*:

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

(ii) *Όταν $k \geq 3$, τότε*

$$[\alpha_1\ \alpha_2\ \dots\ \alpha_k] = [\alpha_1\ \ \dots\ \alpha_j] \circ [\alpha_j\ \alpha_{j+1}\ \dots\ \alpha_k],\ \ \forall j \in \{2, \dots, k\}$$

(iii) *Όταν $k \geq 3$, τότε*

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

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

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

όπου οι (υπο)δείκτες τής κάτω γραμμής οφείλουν να «διαβάζονται κατά μόδιο k», ήτοι

$$a_{k+1} = a_1,\ a_{k+2} = a_2, \dots\dots,\ a_{k+t} = a_l,\ \ \textit{όπου}\ \ t \equiv l (\mathrm{mod}\, k)\ \ (t, l \in \mathbb{N}).$$

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

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

ΑΠΟΔΕΙΞΗ. Το (i) είναι εξ ορισμού προφανές. Το (ii) είναι άμεση συνέπεια τού υπολογισμού τού γινομένου (= συνθέσεως).

(iii) Τούτο έπεται από το (ii) (για $j = 2$) και εφαρμογή τής πρώτης μορφής τής μαθηματικής επαγωγής ως προς τον k (βλ. 1.6.36), εκκινώντας από τον $k = 3$.

(iv) Εδώ εφαρμόζεται κλασική μαθηματική επαγωγή ως προς τον m (βλ. 1.6.34). Για $m = 1$ ο ισχυρισμός είναι προφανώς αληθής. Εάν υποθέσουμε ότι είναι αληθής για κάποιον $m \geq 1$, τότε

$$\begin{aligned}
[\alpha_1\ \alpha_2\ \ldots\ \alpha_k]^{m+1} &= [\alpha_1\ \alpha_2\ \ldots\ \alpha_k]^m \circ [\alpha_1\ \alpha_2\ \ldots\ \alpha_k] \\
&= \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_{m+1} & a_{m+2} & \cdots & a_{m+k} \end{bmatrix} \circ \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_2 & a_3 & \cdots & a_1 \end{bmatrix} \\
&= \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_{m+2} & a_{m+3} & \cdots & a_{m+1+k} \end{bmatrix},
\end{aligned}$$

όπου η δεύτερη ισότητα έπεται από την επαγωγική μας υπόθεση.

(v) Εάν $\sigma := [\alpha_1\ \alpha_2\ \ldots\ \alpha_k]$, τότε από το (iv) λαμβάνουμε

$$\begin{aligned}
\sigma^k &= [\alpha_1\ \alpha_2\ \ldots\ \alpha_k]^k \\
&= \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_{k+1} & a_{k+2} & \cdots & a_{k+k} \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_1 & a_2 & \cdots & a_k \end{bmatrix} = \mathrm{id}.
\end{aligned}$$

Εάν $\varrho \in \{1, ..., k-1\}$, τότε $\sigma^\varrho(a_j) = a_{j+\varrho}$, $\forall j \in \{1, ..., k\}$, οπότε

$$j + \varrho \not\equiv j (\mathrm{mod}\, k), \forall j \in \{1, ..., k\} \Longrightarrow \sigma^\varrho \neq \mathrm{id} \Longrightarrow \mathrm{ord}\,([\alpha_1\ \alpha_2\ \ldots\ \alpha_k]) = k.$$

(vi) Για $k = 1$ τούτο είναι προφανές. Για $k \geq 2$ έχουμε

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

όπου η πρώτη ισότητα έπεται από το (v), και η δεύτερη και η τρίτη από το (iv), καθόσον το $2k-1$ γράφεται ως $(k-1)+k$. □

3.4.10 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. Εάν οι κύκλοι σ, τ είναι ξένοι μεταξύ τους, αρκεί θα δείξουμε ότι

$$(\sigma \circ \tau)(j) = (\tau \circ \sigma)(j), \ \ \forall j \in \{1, ..., n\}. \tag{3.6}$$

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

$$(\sigma \circ \tau)(j) = \sigma(\tau(j)) = \sigma(j) = j \ \text{ και } \ (\tau \circ \sigma)(j) = \tau(\sigma(j)) = \tau(j) = j.$$

Κατά συνέπειαν, απομένει να αποδειχθεί ότι ισχύει η (3.6) 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 ξένοι μεταξύ τους συνάγουμε 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

$$(\sigma \circ \tau)(j) = \sigma(\tau(j)) = \sigma(j) = \tau(\sigma(j)) = (\tau \circ \sigma)(j), \ \ \forall j \in \text{supp}(\sigma).$$

Με ανάλογη επιχειρηματολογία (ύστερα από εναλλαγή των ρόλων των σ και τ) αποδεικνέται ότι η (3.6) είναι αληθής ακόμη και για τους φυσικούς j τους ανήκοντες στον φορέα τής τ. □

3.4.11 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 $c_1, c_2, \ldots, c_\nu \in \mathfrak{S}_n$, 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 $c_1, c_2, \ldots, c_\nu$ είναι ανά δύο ξένοι μεταξύ τους κύκλοι, το λήμμα 3.4.10 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 3.4.5) και

$$\check{\sigma} \circ c_s = c_s \circ \check{\sigma} \tag{3.7}$$

(και πάλι λόγω τού λήμματος 3.4.10). Κάνοντας χρήση τής κλασικής μαθηματικής επαγωγής ως προς τον κ (βλ. 1.6.34) και τής ισότητας (3.7) 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,

$$\sigma^\kappa(j) = (c_s \circ \check{\sigma})^\kappa\,(j) = c_s^\kappa(\check{\sigma}^\kappa(j)) = c_s^\kappa(\check{\sigma}^{k-1}(j)) = \cdots = c_s^\kappa(j),\ \forall \kappa \in \mathbb{N}.$$

και η απόδειξη περατούται. □

3.4.12 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 3.4.9 μπορούμε δίχως βλάβη τής γενικότητας να υποθέσουμε ότι

$$\sigma = [\alpha_1\ \alpha_2\ \ldots\ \alpha_\nu],\ \tau = \left[\beta_1\ \beta_2\ \ldots\ \beta_\xi\right],\ \text{όπου}\ \ \alpha_1 = \beta_1 = j.$$

Κατά το 3.4.9 (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 3.4.9 (v)), οπότε έχουμε κατ' ανάγκην $\xi = \nu$ και $\sigma = \tau$. □

3.4.13 Θεώρημα. *Κάθε (μη ταυτοτική) μετάταξη ανήκουσα στην $\mathfrak{S}_n$, $n \geq 2$, 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. Όταν $n = 2$, τότε έχουμε $\mathfrak{S}_2 \setminus \{\text{id}\} = \{[1\ 2]\}$, οπότε ο ισχυρισμός είναι αληθής. Θα εφαρμόσουμε την πρώτη μορφή τής μαθηματικής επαγωγής ως προς τον n (βλ. 1.6.36), θεωρώντας ως αφετηρία μας τον $n = 2$. Υποθέτοντας ότι ο ισχυρισμός είναι αληθής για κάποιον

$n \geq 2$, αρκεί να αποδείξουμε την ορθότητά του και για τον $n+1$. Έστω τυχούσα $\sigma \in \mathfrak{S}_{n+1} \setminus \{\mathrm{id}\}$. Διαχωρίζουμε δύο περιπτώσεις:

Περίπτωση πρώτη. Εάν $\sigma(n+1) = n+1$, τότε η

$$\sigma' := \sigma|_{\{1,2,\ldots,n\}} : \{1,2,...,n\} \longrightarrow \{1,2,...,n\}$$

είναι ένα στοιχείο τής ομάδας $\mathfrak{S}_n$. Σύμφωνα με την επαγωγική υπόθεσή μας υπάρχουν $\nu \in \mathbb{N}$ και ανά δύο ξένοι μεταξύ τους κύκλοι $\tau'_1, \ldots, \tau'_\nu$ μήκους ≥ 2, ούτως ώστε να ισχύει η ισότητα

$$\sigma' = \tau'_1 \circ \tau'_2 \circ \cdots \circ \tau'_\nu.$$

Έστω $\tau_j : \{1,2,...,n+1\} \longrightarrow \{1,2,...,n+1\}$ η επέκταση τού κύκλου τ'_j που ορίζεται μέσω τού τύπου

$$\tau_j(l) := \begin{cases} \tau'_j(l), & \text{όταν } l \in \{1,...,n\}, \\ n+1, & \text{όταν } l = n+1, \end{cases}$$

για κάθε $j \in \{1,...,\nu\}$. Τότε

$$\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_\nu,$$

οπότε ο ισχυρισμός είναι αληθής και για τον $n+1$.

Περίπτωση δεύτερη. Έστω ότι $\sigma(n+1) \neq n+1$. Λόγω τού εγκλεισμού

$$\left\{n+1, \sigma\left(n+1\right), \sigma^2\left(n+1\right), ..., \sigma^{n+1}\left(n+1\right)\right\} \subseteq \{1,2,...,n+1\}$$

υπάρχουν κάποιοι

$$k, l \in \{0,1,...,n+1\},\ k < l : \sigma^k\left(n+1\right) = \sigma^l\left(n+1\right).$$

Θέτοντας $m := l - k \in \{1,...,n+1\}$, έχουμε $\sigma^m\left(n+1\right) = n+1$. Εξ υποθέσεως, $m \geq 2$. Επειδή το

$$\{q \in \{2,...,n+1\} \,|\sigma^q\left(n+1\right) = n+1\,\}$$

είναι ένα μη κενό υποσύνολο τού $\mathbb{N}$ (καθότι περιέχει τουλάχιστον το m ως στοιχείο του), θα περιέχει (σύμφωνα με την αρχή 1.6.32 τής καλής διατάξεως τού $\mathbb{N}$) ελάχιστο στοιχείο, ας το πούμε μ ($\mu \geq 2$). Σημειωτέον ότι

$$\mathrm{card}(\left\{n+1, \sigma\left(n+1\right), \sigma^2\left(n+1\right), ..., \sigma^{\mu-1}\left(n+1\right)\right\}) = \mu.$$

Πράγματι· εάν οι μ φυσικοί αριθμοί $n+1, \sigma\left(n+1\right), ..., \sigma^{\mu}\left(n+1\right)$ δεν ήταν σαφώς διακεκριμένοι, τότε θα υπήρχαν κάποιοι

$$\xi, \varrho \in \{0,1,...,\mu-1\},\ \xi < \varrho : \sigma^\xi\left(n+1\right) = \sigma^\varrho\left(n+1\right),$$

οπότε θα είχαμε $\sigma^{\varrho-\xi}(n+1) = n+1$, κάτι που θα αντέκειτο προς την επιλογή τού μ (διότι $\varrho - \xi \leq \mu - 1$). Θέτοντας $\tau := \left[n+1\ \sigma(n+1)\ \ldots\ \sigma^{\mu-1}(n+1)\right]$ και $\widetilde{\sigma} := \tau^{-1} \circ \sigma \in \mathfrak{S}_{n+1} \setminus \{\mathrm{id}\}$, διαπιστώνουμε ότι

$$\widetilde{\sigma}(n+1) = \tau^{-1}(\sigma(n+1)) = n+1,$$

οπότε εμπίπτουμε στην πρώτη περίπτωση (για την $\widetilde{\sigma}$). Ως εκ τούτου, υπάρχουν ανά δύο ξένοι μεταξύ τους κύκλοι $\tau_1, \ldots, \tau_\nu$ μήκους ≥ 2, ούτως ώστε

$$\widetilde{\sigma} = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_\nu \Rightarrow \sigma = \tau \circ \widetilde{\sigma} = \tau \circ \tau_1 \circ \tau_2 \circ \cdots \circ \tau_\nu.$$

Επειδή $\widetilde{\sigma}(n+1) = n+1$ και

$$\widetilde{\sigma}(\sigma(n+1)) = \tau^{-1}(\sigma^2(n+1)) = \sigma(n+1), ..., \ \widetilde{\sigma}(\sigma^{\mu-1}(n+1)) = \sigma^{\mu-1}(n+1),$$

έχουμε

$$\left(\bigcup_{j=1}^{\nu} \mathrm{supp}(\tau_j)\right) \cap \left\{n+1, \sigma(n+1), \sigma^2(n+1), ..., \sigma^{\mu-1}(n+1)\right\} = \varnothing,$$

οπότε οι μετατάξεις $\widetilde{\sigma}$ και τ είναι ξένες μεταξύ τους και, κατ' επέκτασιν, και οι κύκλοι $\tau, \tau_1, \tau_2, ..., \tau_\nu$ είναι ανά δύο ξένοι μεταξύ τους. Άρα *και σε αυτήν την περίπτωση* ο (πρώτος) ισχυρισμός είναι αληθής και για τον $n+1$.

2) ΕΠΑΛΗΘΕΥΣΗ ΔΕΥΤΕΡΟΥ ΙΣΧΥΡΙΣΜΟΥ. Έστω $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{id}\}$. Υποθέτουμε ότι η σ γράφεται υπό τη μορφή

$$\sigma = c_1 \circ c_2 \circ \cdots \circ c_\nu = d_1 \circ d_2 \circ \cdots \circ d_{\nu'}, \ \ \nu, \nu' \in \mathbb{N},$$

όπου οι $c_1, c_2, \ldots, c_\nu$ (και, αντιστοίχως, οι $d_1, d_2, \ldots, d_{\nu'}$) είναι κύκλοι ανά δύο ξένοι μεταξύ τους μήκους ≥ 2. Θα εφαρμόσουμε τη δεύτερη μορφή τής μαθηματικής επαγωγής ως προς τον $\ell := \max\{\nu, \nu'\}$ (βλ. 1.6.38). 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 $\sigma \neq \mathrm{id}$,

$$\exists j \in \{1, ..., n\} : \sigma(j) \neq j$$

και $\exists s \in \{1, ..., \nu\}$, $s' \in \{1, ..., \nu'\} : j \in \mathrm{supp}(c_s) \cap \mathrm{supp}(d_{s'})$. Κατά το λήμμα 3.4.11,

$$\sigma^\kappa(j) = c_s^\kappa(j) = d_{s'}^\kappa(j), \ \ \forall \kappa \in \mathbb{N},$$

οπότε το λήμμα 3.4.12 μας πληροφορεί ότι $c_s = d_{s'}$. Εξάλλου, δυνάμει τού λήμματος 3.4.10 και τού νόμου τής διαγραφής 3.2.9 (i) συνάγουμε ότι

$$c_1 \circ \cdots \circ c_{s-1} \circ c_s \circ c_{s+1} \circ \cdots \circ c_\nu = d_1 \circ \cdots \circ d_{s'-1} \circ d_{s'} \circ d_{s'+1} \circ \cdots \circ d_{\nu'}$$

$$\Rightarrow (c_1 \circ \cdots \circ c_{s-1} \circ c_{s+1} \circ \cdots \circ c_\nu) \circ c_s = (d_1 \circ \cdots \circ d_{s'-1} \circ d_{s'+1} \circ \cdots \circ d_{\nu'}) \circ d_{s'}$$

$$\Rightarrow c_1 \circ \cdots \circ c_{s-1} \circ c_{s+1} \circ \cdots \circ c_\nu = d_1 \circ \cdots \circ d_{s'-1} \circ d_{s'+1} \circ \cdots \circ d_{\nu'}$$

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 $c_x = d_{\psi(x)}$, για κάθε $x \in \{1, ..., s-1, s+1, ..., \nu\}$. Επειδή $c_s = d_{s'}$, 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, $c_x = d_{\vartheta(x)}$, για κάθε $x \in \{1, ..., \nu\}$, και η απόδειξη λήγει εδώ. □

3.4.14 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 3.4.13 με το (iii) τής προτάσεως 3.4.9. 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 3.4.9. □

3.4.15 Πόρισμα. *Όταν $n \geq 2$, τότε η συμμετρική ομάδα $\mathfrak{S}_n$ παράγεται από το σύνολο των αντιμεταθέσεών της.*

3.4.16 Παράδειγμα. Έστω τυχούσα $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{id}\}$ (όπου $n \geq 2$). Αυτή, σύμφωνα με το θεώρημα 3.4.13, 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 3.4.14) *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

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

Ωστόσο, αξίζει να επισημανθεί ότι περισώζεται μια λίαν σημαντική ιδιότητα: *το πλήθος των εμφανιζομένων αντιμεταθέσεων είναι ή πάντοτε ένας άρτιος ή πάντοτε ένας περιττός φυσικός αριθμός* (βλ. 3.4.21 (iv)).

3.4.17 Ορισμός. (i) Έστω $\sigma \in \mathfrak{S}_n$ μια μετάταξη. Ορίζουμε ως **παραβατικό ζεύγος**[18] (για την σ) κάθε διατεταγμένο ζεύγος

$$(i,j) \in \{1,\dots,n\} \times \{1,\dots,n\}$$

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

$$\operatorname{sgn} : (\mathfrak{S}_n, \circ) \longrightarrow (\{1,-1\}, \cdot) \tag{3.8}$$

μέσω τού τύπου[19]:

$$\operatorname{sgn}(\sigma) := \begin{cases} 1, & \text{όταν η } \sigma \text{ διαθέτει έναν άρτιο αριθμό παραβατικών ζευγών,} \\ -1, & \text{όταν η } \sigma \text{ διαθέτει έναν περιττό αριθμό παραβατικών ζευγών,} \end{cases}$$

για κάθε $\sigma \in \mathfrak{S}_n$.

(iii) Μια μετάταξη $\sigma \in \mathfrak{S}_n$ ονομάζεται **άρτια** (και αντιστοίχως, **περιττή**) όταν $\operatorname{sgn}(\sigma) = 1$ (και αντιστοίχως, όταν $\operatorname{sgn}(\sigma) = -1$).

3.4.18 Παράδειγμα. Τα παραβατικά ζεύγη τής μετατάξεως

$$\begin{bmatrix} 1\,2\,3\,4 \\ 2\,1\,4\,3 \end{bmatrix}$$

είναι τα $(1,2)$ και $(3,4)$.

3.4.19 Λήμμα. *Κάθε αντιμετάθεση $\tau \in \mathfrak{S}_n$, $n \geq 2$, είναι περιττή μετάταξη, δηλαδή έχουμε*

$$\operatorname{sgn}(\tau) = -1.$$

[18] 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).

[19] Η τιμή $\operatorname{sgn}(\sigma)$ ονομάζεται **προσημασμένος άσος** (ή -πιο σύντομα, αλλά όχι ακριβολογημένα- **πρόσημο**) τής σ.

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

$$\begin{bmatrix} 1 & \dots & i-1 & \boxed{i} & i+1 & \dots & j-1 & \boxed{j} & j+1 & \dots & n \\ 1 & \dots & i-1 & \boxed{j} & i+1 & \dots & j-1 & \boxed{i} & j+1 & \dots & n \end{bmatrix}.$$

Προφανώς, τα παραβατικά ζεύγη -πέραν τού ιδίου τού (i, j)- ανήκουν στην ένωση δύο συνόλων:

$$\{(i,k) \mid i+1 \leq k \leq j-1\} \cup \{(l,j) \mid i+1 \leq l \leq j-1\}.$$

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 $\operatorname{sgn}(\tau) = -1$. □

3.4.20 Λήμμα. *Η τιμή που λαμβάνει οιαδήποτε μετάταξη $\sigma \in \mathfrak{S}_n$ μέσω τής απεικονίσεως προσημάνσεως μπορεί να εκφρασθεί με τη βοήθεια τού ακολούθου «κλειστού» τύπου*:

$$\boxed{\operatorname{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j-i}.}$$

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

$$\prod_{1 \leq i < j \leq n} (\sigma(j) - \sigma(i)) = \left(\prod_{\substack{1 \leq i < j \leq n \\ \sigma(i) < \sigma(j)}} \sigma(j) - \sigma(i) \right) \cdot (-1)^s \prod_{\substack{1 \leq i < j \leq n \\ \sigma(i) > \sigma(j)}} |\sigma(j) - \sigma(i)|$$

$$= (-1)^s \prod_{1 \leq i < j \leq n} |\sigma(j) - \sigma(i)| = (-1)^s \prod_{1 \leq i < j \leq n} (j-i).$$

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 αμφιριπτικότητα τής σ. □

3.4.21 Θεώρημα. (i) *Για τυχούσες* $\sigma, \tau \in \mathfrak{S}_n$ *έχουμε*

$$\boxed{\operatorname{sgn}(\tau \circ \sigma) = \operatorname{sgn}(\tau) \cdot \operatorname{sgn}(\sigma).}$$

οπότε η απεικόνιση προσημάνσεως (3.8) *είναι ένας ομομορφισμός ομάδων.*
(ii) *Για κάθε* $\sigma \in \mathfrak{S}_n$ *έχουμε*

$$\boxed{\operatorname{sgn}(\sigma) = \operatorname{sgn}\left(\sigma^{-1}\right).}$$

(iii) *Εάν η μετάταξη* $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k \in \mathfrak{S}_n$ *συντίθεται από* k *αντιμεταθέσεις* $\tau_1, \tau_2, \ldots, \tau_k$, *τότε*

$$\boxed{\operatorname{sgn}(\sigma) = (-1)^k.}$$

Ιδιαιτέρως, αυτή η ισότητα ισχύει για κάθε $(k+1)$*-κύκλο* $\sigma \in \mathfrak{S}_n$ $(0 \leq k \leq n-1)$.
(iv) *Εάν μια μετάταξη* $\sigma \in \mathfrak{S}_n$ *γράφεται υπό τη μορφή επαλλήλων συνθέσεων*

$$\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k = \tau'_1 \circ \tau'_2 \circ \cdots \circ \tau'_l$$

k *αντιμεταθέσεων* $\tau_1, \ldots, \tau_k$ *και -ταυτοχρόνως-* l *αντιμεταθέσεων* $\tau'_1, \ldots, \tau'_l$, *τότε τόσον το* k *όσον και το* l *είναι ή πάντοτε ένας άρτιος ή πάντοτε ένας περιττός φυσικός αριθμός.*

ΑΠΟΔΕΙΞΗ. (i) Σύμφωνα με το λήμμα 3.4.20 έχουμε

$$\begin{aligned}\operatorname{sgn}(\tau \circ \sigma) &= \prod_{1 \leq i < j \leq n} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{j - i} \\ &= \prod_{1 \leq i < j \leq n} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)} \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}.\end{aligned}$$

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

$$\prod_{1 \leq i < j \leq n} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)}$$

γράφεται ως ακολούθως:

$$\begin{aligned}&\prod_{\substack{1 \leq i < j \leq n \\ \sigma(i) < \sigma(j)}} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)} \prod_{\substack{1 \leq i < j \leq n \\ \sigma(i) > \sigma(j)}} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)} \\ = &\prod_{\substack{1 \leq i < j \leq n \\ \sigma(i) < \sigma(j)}} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)} \prod_{\substack{1 \leq j < i \leq n \\ \sigma(i) < \sigma(j)}} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)} \\ = &\prod_{\sigma(i) < \sigma(j)} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)}.\end{aligned}$$

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 *τανάπαλιν*). Επομένως, το τελευταίο αυτό γινόμενο περιέχει (ενδεχομένως παρατεταγμένους κατά έναν διαφορετικό τρόπο, πράγμα ουσιαστικώς αδιάφορο) *τους ίδιους παράγοντες* με το γινόμενο

$$\prod_{\lambda<\mu} \frac{\tau(\lambda) - \tau(\mu)}{\lambda - \mu} = \text{sgn}(\tau).$$

(ii) Άμεσο επί τη βάσει τού (i), καθόσον ισχύει: $\sigma \circ \sigma^{-1} = \text{id}$ και $\text{sgn}(\text{id}) = 1$.

(iii) Τούτο έπεται από το (i), το λήμμα 3.4.19 και το (iii) τής προτάσεως 3.4.9.

(iv) Προφανώς,

$$\begin{aligned}
&\tau_1 \circ \tau_2 \circ \cdots \circ \tau_k = \tau'_1 \circ \tau'_2 \circ \cdots \circ \tau'_l \\
&\Longrightarrow (\tau_1 \circ \tau_2 \circ \cdots \circ \tau_k) \circ (\tau'_1 \circ \tau'_2 \circ \cdots \circ \tau'_l)^{-1} = \text{id} \\
&\underset{\text{(ii)}}{\overset{\text{(i)}}{\Longrightarrow}} \text{sgn}(\tau_1 \circ \tau_2 \circ \cdots \circ \tau_k) \cdot \text{sgn}(\tau'_1 \circ \tau'_2 \circ \cdots \circ \tau'_l) = 1 \\
&\underset{\text{(iii)}}{\Longrightarrow} (-1)^k \cdot (-1)^l = 1 \Longrightarrow (-1)^{k+l} = 1,
\end{aligned}$$

οπότε το άθροισμα $k + l$ οφείλει να είναι ένας άρτιος φυσικός αριθμός. □

3.4.22 Ορισμός. Έστω n ένας φυσικός αριθμός ≥ 2. Ο πυρήνας

$$\boxed{\mathfrak{A}_n := \text{Ker}(\text{sgn}) = \{\sigma \in \mathfrak{S}_n \mid \text{sgn}(\sigma) = 1\}}$$

τού ομομορφισμού (3.8) είναι μια υποομάδα τής συμμετρικής ομάδας $\mathfrak{S}_n$ (κατά το (ii) τού λήμματος 3.3.4), απαρτίζεται από όλες τις άρτιες μετατάξεις τής $\mathfrak{S}_n$ και καλείται **εναλλάσσουσα ομάδα** (σε n σύμβολα). Σημειωτέον ότι το σύνολο $\{\sigma \in \mathfrak{S}_n \mid \text{sgn}(\sigma) = -1\}$ *δεν* είναι υποομάδα τής $\mathfrak{S}_n$, διότι δεν περιέχει το ουδέτερο στοιχείο id τής $\mathfrak{S}_n$.

3.4.23 Πρόταση. *Η τάξη τής* $\mathfrak{A}_n$ *ισούται με*

$$|\mathfrak{A}_n| = \frac{n!}{2}.$$

ΑΠΟΔΕΙΞΗ. Έστω μια μετάταξη $\tau \in \mathfrak{S}_n$ και έστω

$$\mathfrak{A}_n\tau := \{\sigma \circ \tau \mid \sigma \in \mathfrak{A}_n\}.$$

Εάν $\text{sgn}(\tau) = 1$, τότε $\mathfrak{A}_n\tau = \mathfrak{A}_n$. Ας παγιώσουμε τώρα μια $\tau \in \mathfrak{S}_n$ για την οποία $\text{sgn}(\tau) = -1$. Για κάθε $\sigma \in \mathfrak{S}_n$ με $\text{sgn}(\sigma) = -1$ έχουμε $\text{sgn}\big(\sigma \circ \tau^{-1}\big) = 1$ (βάσει τού (i) τού θεωρήματος 3.4.21), οπότε $\sigma \in \mathfrak{A}_n\tau$, διότι $\sigma = \big(\sigma \circ \tau^{-1}\big) \circ \tau$. Τούτο σημαίνει ότι $\{\sigma \in \mathfrak{S}_n \mid \text{sgn}(\sigma) = -1\} \subseteq \mathfrak{A}_n\tau$, οπότε τελικώς

$$\{\sigma \in \mathfrak{S}_n \mid \text{sgn}(\sigma) = -1\} = \mathfrak{A}_n\tau$$

(διότι ο αντίστροφος εγκλεισμός είναι προφανής) και $\mathfrak{A}_n\tau \cap \mathfrak{A}_n = \varnothing$. Επειδή η απεικόνιση $\mathfrak{A}_n \longrightarrow \mathfrak{A}_n\tau,\ \ \sigma \longmapsto \sigma \circ \tau$, είναι αμφιρριπτική, λαμβάνουμε (βάσει τού 1.12.3 και τής προτάσεως 3.4.3)

$$\mathfrak{S}_n = \mathfrak{A}_n \coprod \mathfrak{A}_n\tau \Rightarrow n! = |\mathfrak{S}_n| = |\mathfrak{A}_n| + \mathrm{card}(\mathfrak{A}_n\tau) = 2\,|\mathfrak{A}_n|\,,$$

οπότε $|\mathfrak{A}_n| = \frac{n!}{2}$. □

3.4.24 Παρατήρηση. Από το (i) τού θεωρήματος 3.8 και την πρόταση 3.4.23 έπεται άμεσα ότι για $n \geq 2$ η απεικόνιση προσημάνσεως (3.8) είναι *επιμορφισμός* ομάδων.

3.4.25 Ορισμός. Κάθε υποομάδα τής $\mathfrak{S}_A$ (όπου A ένα μη κενό σύνολο) ή τής $\mathfrak{S}_n$ (όπου $n \in \mathbb{N}$) καλείται **ομάδα μετατάξεων**.

3.4.26 Παραδείγματα. (i) Η εναλλάσσουσα ομάδα $\mathfrak{A}_n$ είναι μια ομάδα μετατάξεων.

(ii) Έστω $\mathbf{V}$ το ακόλουθο υποσύνολο τής $\mathfrak{A}_4$:

$$\boxed{\mathbf{V} := \{\mathrm{id}, [1\,2] \circ [3\,4]\,, [1\,3] \circ [2\,4]\,, [1\,4] \circ [2\,3]\}\,.}$$

Είναι εύκολο να διαπιστωθεί ότι το $\mathbf{V}$ είναι κλειστό ως προς την πράξη τής συνθέσεως και ότι αποτελεί μια αβελιανή υποομάδα τής $\mathfrak{A}_4$. Η ομάδα μετατάξεων[20] $(\mathbf{V}, \circ)$ καλείται **ομάδα των τεσσάρων στοιχείων τού Klein**.

(iii) Έστω $n \in \mathbb{N}$, $n \geq 3$. Ορίζουμε τις ακόλουθες μετατάξεις $\sigma, \tau \in \mathfrak{S}_n$:

$$\sigma := [1\,2\ \ldots\ n],\ \ \tau := \begin{bmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{bmatrix}.$$

Η υποομάδα τής $\mathfrak{S}_n$

$$\boxed{\mathbf{D}_n := \langle \sigma, \tau \rangle}$$

η παραγόμενη από τις σ και τ είναι μια ομάδα μετατάξεων που επιδέχεται μια ειδική «γεωμετρική ερμηνεία» και καλείται, ιδιαιτέρως, n-**οστή διεδρική ομάδα** έχουσα τάξη $|\mathbf{D}_n| = 2n$, καθότι

$$\mathbf{D}_n = \left\{\sigma^j \tau^k \,|j \in \{0, 1, ..., n-1\}\ ,\ k \in \{0, 1\}\right\}.$$

Για περισσότερες λεπτομέρειες βλ. άσκηση ??.

[20] 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.

Η σημασία των ομάδων μετατάξεων στη Θεωρία Ομάδων παρεμφαίνεται από το ακόλουθο:

3.4.27 Θεώρημα. (Cayley, 1878) *Κάθε ομάδα* $(G,\cdot)$ *είναι ισόμορφη με μια υποομάδα τής ομάδας* $(\mathfrak{S}_G,\circ)$.

ΑΠΟΔΕΙΞΗ. Έστω $(G,\cdot)$ τυχούσα ομάδα (με ουδέτερό της στοιχείο το e_G). Σε κάθε στοιχείο g τής G αντιστοιχούμε μια μετάταξη L_g οριζόμενη ως εξής:

$$L_g : G \longrightarrow G, \quad L_g(x) = gx.$$

(Η απεικόνιση L_g είναι ενριπτική, διότι

$$L_g(x) = L_g(y) \Longrightarrow gx = gy \Longrightarrow g^{-1}gx = g^{-1}gy \Longrightarrow e_G x = e_G y \Longrightarrow x = y,$$

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 G' το υποσύνολο $\{L_g \mid g \in G\}$ τής $\mathfrak{S}_G$. Η πράξη με την οποία είναι εφοδιασμένη η $\mathfrak{S}_G$ είναι η σύνθεση απεικονίσεων. Ως εκ τούτου, έχουμε

$$(L_g \circ L_h)(x) = L_g(L_h(x)) = L_g(hx) = ghx = L_{gh}(x), \quad \forall x \in G.$$

Κατά συνέπειαν, το γινόμενο δυο τυχόντων στοιχείων τού G' ανήκει στο G'. Το ταυτοτικό στοιχείο id_G τής $\mathfrak{S}_G$ ανήκει στο 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 G'. Τούτο σημαίνει ότι το σύνολο G' αποτελεί μια *υποομάδα* τής $\mathfrak{S}_G$ δυνάμει τού (ii) τής προτάσεως 3.2.15. Η απεικόνιση

$$G \longrightarrow G', \quad g \longmapsto L_g,$$

είναι προφανώς επιριπτική και μεταφέρει τον πολλαπλασιασμό τής G στη σύνθεση απεικονίσεων τής 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 G' τής ομάδας $\mathfrak{S}_G$. □

3.4.28 Σημείωση. Η ανωτέρω κατασκευασθείσα ομάδα μετατάξεων G' καλείται ενίοτε και **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** $\breve{G}' := \{R_g \mid g \in G\}$ **τής** G **εντός τής** $\mathfrak{S}_G$, όπου

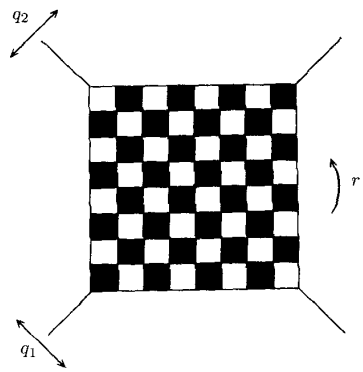
$$R_g : G \longrightarrow G, \quad R_g(x) = xg.$$

Προφανώς, $G' \cong G \cong \breve{G}'$.

3.4.29 Πόρισμα. *Εάν η G είναι μια πεπερασμένη ομάδα τάξεως n, τότε η G είναι ισόμορφη με μια υποομάδα τής $\mathfrak{S}_n$.*

ΑΠΟΔΕΙΞΗ. Εάν, κατά κάποιον τρόπο, αριθμήσουμε τα στοιχεία τής G ως $1, 2, \ldots, n$, τότε κάθε μετάταξη τής G επάγει μια μετάταξη των $1, 2, \ldots, n$. Ως εκ τούτου, δημιουργείται ένας ισομορφισμός μεταξύ τής $\mathfrak{S}_G$ και τής $\mathfrak{S}_n$, και επομένως η υποομάδα G' τής $\mathfrak{S}_G$ είναι ισόμορφη με μια υποομάδα G'' τής $\mathfrak{S}_n$. Επειδή η G είναι ισόμορφη τής G' και επειδή η σύνθεση δύο ισομορφισμών είναι ένας ισομορφισμός, η G είναι ισόμορφη τής G''. □

3.4.30 Παράδειγμα. (Επίπεδες συμμετρίες μιας σκακιέρας) Μια σκακιέρα διαθέτει τέσσερεις επίπεδες συμμετρίες[21]: την ταυτοτική e, τη στροφή r περί το κέντρο της κατά 180° και τους κατοπτρισμούς q_1 και q_2 ως προς τις δύο διαγωνίους της.



Αυτές οι συμμετρίες συγκροτούν μια ομάδα $G = \{e, r, q_1, q_2\}$ με πράξη της τη σύνθεση απεικονίσεων. Ο κατάλογος τής πράξεως 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 3.4.27 τού Cayley, $G \cong G'$, όπου

$$G' = \{L_e, L_r, L_{q_1}, L_{q_2}\} \subsetneqq \mathfrak{S}_G.$$

[21] Ως *συμμετρίες* ενός υποσυνόλου A τού ευκλειδείου επιπέδου ορίζονται εκείνες οι αμφιρρίψεις από το ευκλείδειο επίπεδο στον εαυτό του, οι οποίες διατηρούν τις αποστάσεις και στέλνουν το A να απεικονισθεί στο ίδιο το A.

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 $G' \cong G''$, όπου $G'' := \Phi_f(G')$. Προφανώς, $\Phi_f(L_e) = \mathrm{id}$ και $\Phi_f(L_r) = f \circ L_r \circ f^{-1}$, οπότε

$$\Phi_f(L_r)(1) = f(L_r(f^{-1}(1))) = f(L_r(e)) = f(r) = 2,$$
$$\Phi_f(L_r)(2) = f(L_r(f^{-1}(2))) = f(L_r(r)) = f(e) = 1,$$
$$\Phi_f(L_r)(3) = f(L_r(f^{-1}(3))) = f(L_r(q_1)) = f(q_2) = 4,$$
$$\Phi_f(L_r)(4) = f(L_r(f^{-1}(4))) = f(L_r(q_2)) = f(q_1) = 3,$$

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, $G'' = \mathbf{V}$, όπου η $\mathbf{V}$ είναι η ομάδα 3.4.26 (ii) των τεσσάρων στοιχείων τού Klein και $G \cong \mathbf{V}$.

3.5 ΠΛΕΥΡΙΚΕΣ ΚΛΑΣΕΙΣ ΚΑΙ ΔΕΙΚΤΕΣ ΥΠΟΟΜΑΔΩΝ

Σε αυτήν την ενότητα θα αποδείξουμε ένα από τα σημαντικότερα θεωρήματα που αφορούν στις πεπερασμένες ομάδες, το λεγόμενο *θεώρημα τού Lagrange* 3.5.18,

μέσω ενός γενικότερου θεωρήματος που συνδέει την τάξη *οιασδήποτε* ομάδας με την τάξη μιας υποομάδας της (βλ. θεώρημα 3.5.16). Προς τούτο προαπαιτείται η παράθεση των ορισμών των *πλευρικών κλάσεων* και τού *δείκτη* υποομάδων δοθείσας ομάδας.

3.5.1 Ορισμός. Έστω $(G, \cdot)$ μια ομάδα. Εάν $A \subseteq G$ και $B \subseteq G$, τότε ορίζουμε ως AB το σύνολο

$$\boxed{AB := \{xy \mid x \in A \ \text{ και } \ y \in B\}.}$$

3.5.2 Πρόταση. *Έστω $(G, \cdot)$ μια ομάδα. Εάν τα A, B, C είναι τρία υποσύνολα τού υποκειμένου συνόλου της G, 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,

$$\exists y \in B \ \text{ και } \ \exists z \in C : g = xy = xz \underset{\text{3.2.9 (i)}}{\Longrightarrow} y = z \in B \cap C,$$

οπότε $g \in A(B \cap C)$. Αυτό σημαίνει ότι $A(B \cap C) \supseteq AB \cap AC$.

(iii) Τούτο είναι άμεσο από τον ορισμό 3.5.1 και την προσεταιριστικότητα τής πράξεως "$\cdot$". □

3.5.3 Πρόταση. *Έστω ότι τα H και K είναι δυο υποομάδες μιας ομάδας $(G, \cdot)$. Τότε*

$$[\textit{το σύνολο } HK \textit{ είναι υποομάδα τής } G] \Longleftrightarrow HK = KH.$$

ΑΠΟΔΕΙΞΗ. "⇒": Έστω τυχόν $x \in HK$. Τότε $x = hk$ για κάποια $h \in H$ και $k \in K$. Επειδή το HK είναι εξ υποθέσεως υποομάδα τής G, έχουμε $x^{-1} \in HK$ (βλ. το (ii) (c) τής προτάσεως 3.2.15). Άρα $x^{-1} = h'k'$ για κάποια $h' \in H$ και $k' \in K$, και

$$\left.\begin{array}{r} x = \left(x^{-1}\right)^{-1} \Rightarrow x = (h'k')^{-1} = (k')^{-1}(h')^{-1} \\ k' \in K \Rightarrow (k')^{-1} \in K \ \text{ και } \ h' \in H \Rightarrow (h')^{-1} \in H \end{array}\right\} \Rightarrow x = (k')^{-1}(h')^{-1} \in KH.$$

Τούτο σημαίνει ότι $HK \subseteq KH$. Για την απόδειξη τού αντιστρόφου εγκλεισμού θεωρούμε τυχόν $y \in KH$. Προφανώς, $y = kh$ για κάποια $k \in K$ και $h \in H$, και

$$\left.\begin{array}{r} h \in H \Rightarrow h^{-1} \in H \ \text{ και } \ k \in K \Rightarrow k^{-1} \in K \\ y^{-1} = (kh)^{-1} = h^{-1}k^{-1} \end{array}\right\} \Rightarrow y^{-1} \in HK.$$

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 τα H και K είναι υποομάδες τής 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 $h_1, h_2 \in H$ και $k_1, k_2 \in K$, τέτοια ώστε να ισχύουν οι ισότητες $x_1 = h_1k_1$ και $x_2 = h_2k_2$. Επιπροσθέτως,

$$k_1h_2 \in KH = HK \Rightarrow \exists h_3 \in H \ \text{ και } \ \exists k_3 \in K : k_1h_2 = h_3k_3.$$

Κατά συνέπειαν,

$$\begin{aligned} x_1x_2 &= (h_1k_1)(h_2k_2) \underset{1.6.40}{=} h_1(k_1h_2)k_2 \\ &= h_1(h_3k_3)k_2 \underset{1.6.40}{=} \underbrace{(h_1h_3)}_{\in H}\underbrace{(k_3k_2)}_{\in K} \in HK. \end{aligned}$$

Τέλος, για οιοδήποτε $x \in HK$ υπάρχουν $h \in H$ και $k \in K$, τέτοια ώστε να ισχύει η ισότητα $x = hk$, οπότε

$$x^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH = HK.$$

Σύμφωνα με το (ii) τής προτάσεως 3.2.15 το σύνολο HK είναι υποομάδα τής G. □

3.5.4 Παράδειγμα. Εάν $G := \mathfrak{S}_3$ και $H := \langle [1\,2] \rangle$, $K := \langle [2\,3] \rangle$, τότε

$$\{\mathrm{id},\ [1\,2],\ [2\,3],\ [1\,2\,3]\} = HK \neq KH = \{\mathrm{id},\ [1\,2],\ [2\,3],\ [1\,3\,2]\},$$

οπότε κανένα εκ των συνόλων HK, KH δεν είναι υποομάδα τής $\mathfrak{S}_3$.

3.5.5 Ορισμός. Εάν η H είναι μια υποομάδα μιας ομάδας $(G, \cdot)$, τότε κάθε σύνολο τής μορφής

$$Hg := H\{g\} = \{\, hg \mid h \in H\}$$

(και αντιστοίχως, κάθε σύνολο τής μορφής

$$gH := \{g\}H = \{\, gh \mid h \in H\} \,)$$

όπου $g \in G$, καλείται **δεξιά** (και αντιστοίχως, **αριστερή**) **πλευρική κλάση**[22] **τής** H **εντός τής** G .

3.5.6 Ορισμός. Έστω ότι η $(G, \cdot)$ είναι μια ομάδα και η H μια υποομάδα της. Επί τού συνόλου G ορίζουμε τις διμελείς σχέσεις

$$\boxed{x \sim_\delta y \underset{\text{ορσ}}{\iff} yx^{-1} \in H} \tag{3.9}$$

και

$$\boxed{x \sim_\alpha y \underset{\text{ορσ}}{\iff} y^{-1}x \in H.} \tag{3.10}$$

3.5.7 Πρόταση. *Οι* (3.9) *και* (3.10) *αποτελούν σχέσεις ισοδυναμίας επί τού* G.

ΑΠΟΔΕΙΞΗ. Η (3.9) είναι *ανακλαστική*, διότι

$$(e_G = xx^{-1} \in H \Longrightarrow x \sim_\delta x), \quad \forall x \in G,$$

συμμετρική, διότι εάν $x \sim_\delta y$, τότε

$$yx^{-1} \in H \Longrightarrow \left(yx^{-1}\right)^{-1} = xy^{-1} \in H \Longrightarrow y \sim_\delta x,$$

και, τέλος, *μεταβατική*, διότι εάν $x \sim_\delta y$ και $y \sim_\delta z$, τότε

$$\left(yx^{-1} \in H \text{ και } zy^{-1} \in H\right) \Longrightarrow \left(zy^{-1}\right)\left(yx^{-1}\right) = zx^{-1} \in H \Longrightarrow x \sim_\delta z.$$

Κατά συνέπειαν, η "$\sim_\delta$" είναι μια σχέση ισοδυναμίας επί τού συνόλου G. Παρομοίως αποδεικνύεται ότι το ίδιο ισχύει και για την (3.10). □

3.5.8 Πρόταση. *Έστω* H *μια υποομάδα μιας ομάδας* $(G, \cdot)$. *Τότε ισχύουν τα εξής*:
(i) H *κλάση ισοδυναμίας* $[g]_\delta := \{\, y \in G \mid g \sim_\delta y\}$ *οιουδήποτε στοιχείου* $g \in G$ (*ως προς τη σχέση ισοδυναμίας* (3.9)) *ισούται με τη δεξιά πλευρική κλάση*

$$[g]_\delta = Hg$$

[22] 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).

τής H εντός τής G την οριζόμενη μέσω τού g.

(ii) *Η κλάση ισοδυναμίας* $[g]_\alpha := \{y \in G \mid g \sim_\alpha y\}$ *οιουδήποτε στοιχείου* $g \in G$ (*ως προς τη σχέση ισοδυναμίας* (3.10)) *ισούται με την αριστερή πλευρική κλάση*

$$[g]_\alpha = gH$$

τής H εντός τής G την οριζόμενη μέσω τού g.

ΑΠΟΔΕΙΞΗ. (i) Η $[g]_\delta$ ισούται πράγματι με

$$\{y \in G \mid g \sim_\delta y\} = \{y \in G \mid yg^{-1} \in H\}$$
$$= \{y \in G \mid yg^{-1} = h \in H\}$$
$$= \{y \in G \mid y = hg,\ h \in H\} = \{hg \mid h \in H\}$$

ήτοι με τη δεξιά πλευρική κλάση Hg τής H εντός τής G την οριζόμενη μέσω τού στοιχείου g. Η απόδειξη τού (ii) είναι παρόμοια. □

3.5.9 Πόρισμα. *Εάν η H είναι μια υποομάδα μιας ομάδας $(G, \cdot)$, τότε*

$$\boxed{G = \bigcup_{Hg \in (G/\sim_\delta)} Hg = \bigcup_{gH \in (G/\sim_\alpha)} gH} \tag{3.11}$$

και ισχύουν οι αμφίπλευρες συνεπαγωγές

$$Hg_1 \cap Hg_2 \neq \varnothing \Leftrightarrow Hg_1 = Hg_2 \Leftrightarrow g_2 \in Hg_1 \Leftrightarrow g_2 g_1^{-1} \in H,\ \forall (g_1, g_2) \in G \times G,$$

καθώς και οι

$$g_1 H \cap g_2 H \neq \varnothing \Leftrightarrow g_1 H = g_2 H \Leftrightarrow g_2 \in g_1 H \Leftrightarrow g_1^{-1} g_2 \in H,\ \forall (g_1, g_2) \in G \times G.$$

Ιδιαιτέρως δε, για ένα $g \in G$, $g \in H \Leftrightarrow Hg = H \Leftrightarrow H = gH$.

ΑΠΟΔΕΙΞΗ. Αυτή έπεται άμεσα από το γεγονός ότι τα σύνολα

$$G/\sim_\delta = \{Hg \mid g \in G\} \quad \text{και} \quad G/\sim_\alpha = \{gH \mid g \in G\}$$

των κλάσεων ισοδυναμίας ως προς τις "$\sim_\delta$" και "$\sim_\alpha$" είναι διαμελισμοί τού υποκειμένου συνόλου G τής ομάδας $(G, \cdot)$. Βλ. προτάσεις 1.3.14, 3.5.7 και 3.5.8. Οι αμφίπλευρες συνεπαγωγές

$$Hg_1 = Hg_2 \Leftrightarrow g_2 \in Hg_1 \Leftrightarrow g_2 g_1^{-1} \in H$$

αποδεικνύονται στοιχειωδώς: Εάν $Hg_1 = Hg_2$, τότε προφανώς $g_2 \in Hg_2 = Hg_1$. Εάν $g_2 \in Hg_1$, τότε $\exists h \in H$:$g_2 = hg_1$, οπότε $g_2 g_1^{-1} = h \in H$. Τέλος, εάν υποθέσουμε ότι $g_2 g_1^{-1} \in H$, τότε $g_2 g_1^{-1} = h$ για κάποιο $h \in H$, οπότε

$$g_2 = hg_1 \Rightarrow Hg_2 = H(hg_1) = (Hh)g_1 = Hg_1.$$

Οι λοιπές αμφίπλευρες συνεπαγωγές αποδεικνύονται παρομοίως. □

3.5.10 Πρόταση. *Εάν η H είναι μια υποομάδα μιας ομάδας $(G,\cdot)$, τότε για κάθε στοιχείο $g\in G$ οι απεικονίσεις*

$$\left\{\begin{array}{c}\vartheta_g^{[\delta]}:H\longrightarrow Hg\\ h\longmapsto hg\end{array}\right\},\ \left\{\begin{array}{c}\vartheta_g^{[\alpha]}:H\longrightarrow gH\\ h\longmapsto gh\end{array}\right\}$$

είναι αμφιρριπτικές. Ως εκ τούτου,

$$|H|=\operatorname{card}(Hg)=\operatorname{card}(gH),\ \ \forall g\in G. \tag{3.12}$$

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

$$\vartheta_g^{[\delta]}\circ\psi_g^{[\delta]}=\mathrm{id}_{Hg}\ \ \text{και}\ \ \psi_g^{[\delta]}\circ\vartheta_g^{[\delta]}=\mathrm{id}_H.$$

Κατά το (iii) τής προτάσεως 1.2.17 η $\vartheta_g^{[\delta]}$ είναι αμφιρριπτική απεικόνιση έχουσα την $\psi_g^{[\delta]}$ ως αντίστροφό της. Παρομοίως αποδεικνύεται ότι η $\vartheta_g^{[\alpha]}$ είναι ωσαύτως αμφιρριπτική έχουσα την απεικόνιση

$$\psi_g^{[\alpha]}:gH\longrightarrow H,\quad \psi_g^{[\alpha]}(x):=g^{-1}x,\ \forall x\in gH.$$

ως αντίστροφό της. □

3.5.11 Ορισμός. Εάν η H είναι μια υποομάδα μιας ομάδας $(G,\cdot)$, τότε κάθε πλήρες σύστημα εκπροσώπων τού συνόλου G ως προς την "$\sim_\delta$", ήτοι κάθε $\Delta\subseteq G$, τέτοιο ώστε[23] για οιαδήποτε $x,y\in\Delta$ να ισχύει η συνεπαγωγή

$$x\neq y\Longrightarrow Hx\neq Hy \tag{3.13}$$

(βλ. 1.3.19) 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,

$$\boxed{G=\coprod_{g\in\Delta}[g]_\delta=\coprod_{g\in\Delta}Hg.}$$

Κατ' αναλογίαν, κάθε πλήρες σύστημα εκπροσώπων τού συνόλου G ως προς την "$\sim_\alpha$" καλείται **σύστημα αριστερών εκπροσώπων τής H εντός τής G**.

[23] Προφανώς, η συνθήκη (3.13) ισοδυναμεί με την: $\operatorname{card}(\Delta\cap Hg)=1,\forall g\in G$.

3.5.12 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*

$$\mathrm{card}\left(\{Hg\,|g\in\Delta\}\right)=\mathrm{card}\left(\Delta\right)=\mathrm{card}\left(\mathrm{A}\right)=\mathrm{card}\left(\{gH\,|g\in\mathrm{A}\}\right). \tag{3.14}$$

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. □

3.5.13 Ορισμός. Εάν η H είναι μια υποομάδα μιας ομάδας $(G,\cdot)$, τότε ο πληθικός αριθμός (3.14) 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, $|G:H|=\infty$).

3.5.14 Παραδείγματα. (i) Προφανώς, $|G:\{e_G\}|=|G|$, $|G:G|=1$, όπου $\{e_G\}$ η τετριμμένη υποομάδα τής G, για οιαδήποτε ομάδα G.

(ii) Εάν ως G θεωρήσουμε την προσθετική ομάδα $\mathbb{Z}$ των ακεραίων και $H=n\,\mathbb{Z}$, για κάποιον $n\in\mathbb{N}$, $n\geq 2$, τότε $|\mathbb{Z}:n\,\mathbb{Z}|=n$, διότι το σύνολο

$$\mathrm{A}:=\{n\,\mathbb{Z},1+n\,\mathbb{Z},...,(n-1)+n\,\mathbb{Z}\}$$

(όπου $k+n\,\mathbb{Z}:=\{k+nl\,|l\in\mathbb{Z}\},\forall k\in\mathbb{Z}$) αποτελεί ένα σύστημα αριστερών εκπροσώπων τής H εντός τής $\mathbb{Z}$.

(iii) Εάν ως G θεωρήσουμε την προσθετική ομάδα $\mathbb{Q}$ των ρητών αριθμών, τότε οιαδήποτε γνήσια υποομάδα της H έχει δείκτη $|\mathbb{Q}:H|=\infty$ εντός αυτής.

3.5.15 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

$$G = Hg_1 \coprod Hg_2 \coprod Hg_3 = g_1H \coprod g_2H \coprod g_3H \Rightarrow |G : H| = 3.$$

Ωστόσο, συνολοθεωρητικώς, $Hg_2 \neq g_2H$ και $Hg_3 \neq g_3H$. 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 επόμενη ενότητα[24].)

3.5.16 Θεώρημα. *Εάν η H είναι μια υποομάδα μιας ομάδας $(G, \cdot)$, τότε*

$$\boxed{|G| = |G : H|\ |H|\,.} \tag{3.15}$$

ΑΠΟΔΕΙΞΗ. Έστω Δ ένα σύστημα δεξιών εκπροσώπων τής H εντός τής G. Τότε

$$|G| := \mathrm{card}(G) = \mathrm{card}(\coprod_{g \in \Delta} Hg). \tag{3.16}$$

Η απεικόνιση

$$f : H \times \Delta \longrightarrow \coprod_{g \in \Delta} Hg, \quad f(h, g) := hg \in Hg,\ \forall (h, g) \in H \times \Delta, \tag{3.17}$$

[24]Κάθε υποομάδα μιας *αβελιανής* ομάδας είναι ορθόθετη (βλ. 3.6.14). 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*.

είναι αμφίρριψη. Ως εκ τούτου, μέσω των (3.16) και (3.17) ή, εναλλακτικώς, μέσω των (3.16) και (3.12) συνάγουμε ότι

$$|G| = \text{card}\,(H \times \Delta) = |H| \cdot \text{card}(\Delta) = \text{card}(\Delta) \cdot |H| = |G : H|\ |H|\,,$$

οπότε η (3.15) είναι αληθής. □

3.5.17 Σημείωση. Εάν δύο εκ των πληθικών αριθμών $|G|\,,\ |H|\,,\ |G : H|$ είναι πεπερασμένοι, τότε και ο τρίτος είναι πεπερασμένος.

3.5.18 Πόρισμα. (Θεώρημα τού Lagrange, 1770) *Εάν η G 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[25]. 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 (3.15) έχουμε $m\,|n$ και $|G : H| = \frac{n}{m}$. □

3.5.19 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, $|\mathbb{Z}_{12} : H| = 4 = \frac{12}{3} = \frac{|\mathbb{Z}_{12}|}{|H|}$.

3.5.20 Πόρισμα. *Εάν η G είναι μια πεπερασμένη ομάδα, τότε η τάξη οιουδήποτε στοιχείου της είναι διαιρέτης τής $|G|$.*

ΑΠΟΔΕΙΞΗ. Εάν $g \in G$, τότε $\text{ord}(g) = |\langle g\rangle|$ (βλ. (3.3)), οπότε η τάξη $\text{ord}(g)$ τού g είναι διαιρέτης τής $|G|$ επί τη βάσει τού θεωρήματος 3.5.18 τού Lagrange. □

3.5.21 Πόρισμα. *Εάν μια ομάδα G έχει ως τάξη της έναν πρώτο αριθμό $p \geq 2$, τότε η G είναι κυκλική* [26].

[25] Παρότι ο Joseph-Louis Lagrange (1736-1813) ήταν ο πρώτος που διετύπωσε ένα θεώρημα ισοδύναμο τού 3.5.18 το 1770, η πρώτη ολοκληρωμένη απόδειξη εδόθη τριάντα έτη αργότερα από τον Pietro Abbatti (1768-1842).

[26] Βεβαίως, και κάθε ομάδα τάξεως 1 είναι *προφανώς* κυκλική.

ΑΠΟΔΕΙΞΗ. Επειδή $p = |G| \geq 2$, υπάρχει κάποιο $g \in G$ με $g \neq e_G$. Συνεπώς, $\text{ord}(g) \geq 2$ και $\text{ord}(g)\,|p$ (δυνάμει τού πορίσματος 3.5.20). Και επειδή ο p είναι εξ υποθέσεως πρώτος, έχουμε $\text{ord}(g) = p$. Αυτό όμως σημαίνει ότι η G είναι κυκλική δυνάμει τής προτάσεως 3.2.33. □

3.5.22 Πόρισμα. *Εάν η $(G, \cdot)$ είναι μια πεπερασμένη ομάδα, τότε*

$$\boxed{g^{|G|} = e_G, \quad \forall g \in G.} \tag{3.18}$$

ΑΠΟΔΕΙΞΗ. Έστω τυχόν $g \in G$. Εάν $m := \text{ord}(g)$, τότε $g^m = e_G$ και, σύμφωνα με το πόρισμα 3.5.20, 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 (3.18) είναι αληθής. □

3.5.23 Σημείωση. (Νέα απόδειξη τού θεωρήματος τού Euler περί ισοτιμιών) Έστω m ένας φυσικός αριθμός ≥ 2 και έστω a ένας ακέραιος με μκδ$(a, m) = 1$. Θεωρούμε την πολλαπλασιαστική ομάδα $(\mathbb{Z}_m^\times, \cdot)$,

$$\mathbb{Z}_m^\times = \{[k]_m \in \mathbb{Z}_m \,|k \in \{1, ..., m-1\} : \text{ μκδ } (k, m) = 1\},$$

η τάξη τής οποίας ισούται με $|\mathbb{Z}_m^\times| = \varphi(m)$, όπου φ η συνάρτηση φι τού Euler (βλ. 2.4.16 και 3.2.7 (iii)). Ας υποθέσουμε ότι ο a διαιρούμενος διά τού m αφήνει υπόλοιπο r. Προφανώς, $[a]_m = [r]_m$ με $r \in \{1, ..., m-1\}$ και μκδ$(r, m) = 1$. Από το (iii) τής προτάσεως 2.4.5 και από το πόρισμα 3.5.22 συνάγουμε ότι

$$[r]_m \in \mathbb{Z}_m^\times \Rightarrow [a^{\varphi(m)}]_m = ([a]_m)^{\varphi(m)} = ([r]_m)^{\varphi(m)} = [1]_m\,,$$

οπότε καταλήγουμε σε μια (απλούστατη, ομαδοθεωρητική) απόδειξη τής ισοτιμίας (2.28). Εν προκειμένω, κατά την αποδεικτική πορεία δεν έγινε χρήση τού «μικρού θεωρήματος» τού Fermat 2.4.14 (κάτι *που συνέβη* στην απόδειξη που είχε δοθεί για το θεώρημα 2.4.21). Πρέπει, λοιπόν, να επισημανθεί, ότι έχοντας αποδείξει κατ' αυτόν τον τρόπο την ισχύ τής ισοτιμίας

$$a^{\varphi(m)} \equiv 1 (\text{mod } m), \tag{3.19}$$

έχουμε τη δυνατότητα τής απευθείας αποδείξεως τού «μικρού θεωρήματος» τού Fermat 2.4.14 *μέσω αυτής* και -κατόπιν τούτου- και τής κατά τι γενικότερης ισοτιμίας (2.22) που είχαμε παραθέσει στο πόρισμα 2.4.13. Πράγματι· εάν ο a είναι ένας ακέραιος αριθμός και ο p ένας πρώτος αριθμός, τότε, στην περίπτωση κατά

την οποία $p \nmid a$, η ισοτιμία (3.19), η ισότητα $\varphi(p) = p-1$ (βλ. 2.4.18) και το (ii) τής προτάσεως 2.4.5 μας δίδουν

$$a^{p-1} \equiv 1(\mathrm{mod}\ p) \Longrightarrow a^p \equiv a(\mathrm{mod}\, p),$$

ενώ στην περίπτωση κατά την οποία $\exists l \in \mathbb{Z} : a = lp$, λαμβάνουμε

$$a^p - a = (lp)^p - lp = p(l^p p^{p-1} - l) \equiv 0(\mathrm{mod}\, p) \Rightarrow a^p \equiv a(\mathrm{mod}\, p).$$

Το θεώρημα 3.5.16 γενικεύεται ως εξής:

3.5.24 Θεώρημα. *Εάν οι H και K είναι δυο υποομάδες μιας ομάδας $(G,\cdot)$ και ισχύει ο εγκλεισμός $K \subseteq H$, τότε*

$$\boxed{|G:K| = |G:H|\ |H:K|\,.} \tag{3.20}$$

ΑΠΟΔΕΙΞΗ. Έστω A ένα σύστημα αριστερών εκπροσώπων *τής H εντός τής G* και έστω A′ ένα σύστημα αριστερών εκπροσώπων *τής K εντός τής H*. Τότε

$$\mathrm{card}(\mathrm{A}) = |G:H| \quad \text{και} \quad \mathrm{card}(\mathrm{A}') = |H:K|\,. \tag{3.21}$$

Θα αποδείξουμε ότι το $\mathrm{AA}' \subseteq G$ αποτελεί ένα σύστημα αριστερών εκπροσώπων *τής K εντός τής G*. Κατ' αρχάς,

$$G = \bigcup_{g\in \mathrm{A}} gH = \bigcup_{g\in \mathrm{A}} g\left(\bigcup_{h\in \mathrm{A}'} hK\right) = \bigcup_{g\in \mathrm{A},\, h\in \mathrm{A}'} (gh)\,K,$$

όπου η τελευταία ισότητα έπεται από το (i) τής προτάσεως 3.5.2. Η τελευταία ένωση είναι *αποσυνδετή*. Πράγματι· εάν $g_1, g_2 \in \mathrm{A}$ και $h_1, h_2 \in \mathrm{A}'$, τέτοια ώστε να ισχύει η ισότητα $(g_1h_1)\,K = (g_2h_2)\,K$, τότε

$$\left.\begin{array}{r}(g_1h_1)\,KH = (g_2h_2)\,KH\\ K \subseteq H \Rightarrow KH = H\end{array}\right\} \Rightarrow \left.\begin{array}{r}g_1h_1H = g_2h_2H\\ h_j \in H \Rightarrow h_jH = H, \forall j \in \{1,2\}\end{array}\right\} \Rightarrow g_1H = g_2H,$$

οπότε $g_1 = g_2$ (διότι το A είναι εξ υποθέσεως ένα σύστημα αριστερών εκπροσώπων τής H εντός τής G). Τούτο σημαίνει ότι το σύνολο AA' είναι όντως (εκ κατασκευής) ένα σύστημα αριστερών εκπροσώπων τής K εντός τής G. Άρα $\mathrm{card}(\mathrm{AA}') = |G:K|$. Εν συνεχεία, παρατηρούμε ότι για οιαδήποτε $g_1, g_2 \in \mathrm{A}$ και $h_1, h_2 \in \mathrm{A}'$, για τα οποία $g_1h_1 = g_2h_2$, ισχύουν οι συνεπαγωγές

$$g_1h_1 = g_2h_2 \Rightarrow (g_1h_1)\,KH = (g_2h_2)\,KH \Rightarrow g_1 = g_2 \Rightarrow h_1 = h_2,$$

όπου η πρώτη είναι προφανής, η δεύτερη απόρροια των όσων έχουμε ήδη προαναφέρει και η τρίτη έπεται από τον νόμο τής διαγραφής 3.2.9 (i). Από το γεγονός τού ότι τελικώς ισχύει $g_1h_1 = g_2h_2 \Rightarrow [g_1 = g_2 \ \text{ και } \ h_1 = h_2]$ συμπεραίνουμε ότι

$$|G:K| = \mathrm{card}(\mathrm{AA}') = \mathrm{card}(\mathrm{A}\times\mathrm{A}') = \mathrm{card}(\mathrm{A})\cdot\mathrm{card}(\mathrm{A}'). \tag{3.22}$$

Ο συνδυασμός των (3.21) και (3.22) δίδει την (3.20). □

3.5.25 Παρατήρηση. Η ισότητα (3.15) έπεται άμεσα από την (3.20) εάν ως K θεωρήσουμε την τετριμμένη υποομάδα τής G (βλ. 3.5.14 (i)).

3.5.26 Ορισμός. Κάθε υποομάδα H μιας ομάδας $(G,\cdot)$ με $|G:H|<\infty$ καλείται **υποομάδα πεπερασμένου δείκτη** (εντός τής G).

3.5.27 Θεώρημα. (H. Poincaré) *Εάν οι H και K είναι δυο υποομάδες μιας ομάδας $(G,\cdot)$, τότε ισχύουν τα ακόλουθα*:

(i) *Ο δείκτης τής $H\cap K$ εντός τής G πληροί την ανισοϊσότητα*

$$|G:H\cap K|\le |G:H|\,|G:K|\,. \tag{3.23}$$

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 ισχύει η συνεπαγωγή*

$$\text{μκδ}\,(|G:H|\,,|G:K|)=1\Longrightarrow |G:H\cap K|=|G:H|\,|G:K|\,.$$

ΠΡΩΤΗ ΑΠΟΔΕΙΞΗ ΤΟΥ (i). Κατ' αρχάς, εάν $x,y\in G$, τότε το σύνολο $(xH)\cap(yK)$ είναι είτε το κενό σύνολο είτε μια αριστερή πλευρική κλάση τής $H\cap K$ εντός τής G. Πράγματι· εάν $g\in(xH)\cap(yK)$, τότε $g\in xH$ και $g\in yK$, οπότε $gH=xH$ και $gK=yK$ (βλ. πρόταση 3.5.9). Από το (ii) τής προτάσεως 3.5.2 συνάγουμε 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

$$\begin{aligned}\mathrm{card}(\{(xH)\cap(yK)\,|x\in\mathrm{A},y\in\mathrm{A}'\}) &= \mathrm{card}(\mathrm{A})\cdot\mathrm{card}(\mathrm{A}')\\ &= |G:H|\,|G:K|\end{aligned}$$

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 (3.23).

ΔΕΥΤΕΡΗ ΑΠΟΔΕΙΞΗ ΤΟΥ (i). Εφαρμόζοντας το θεώρημα 3.5.24 (με την $H\cap K$ στη θέση τής εκεί παρατιθέμενης 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 $m := |G : H|$, $n := |G : K|$, $k := |G : H \cap K|$ και $l := |H : H \cap K|$, η (3.23) μας πληροφορεί ότι

$$|G : H \cap K| =: k \leq mn. \tag{3.24}$$

Εκ παραλλήλου, διπλή εφαρμογή τού θεωρήματος 3.5.24 μας δίδει

$$k = ml, \quad k = n \,|K : H \cap K| \Longrightarrow n \mid k = ml.$$

Επειδή μκδ$(m, n) = 1$, βάσει τού πορίσματος 2.2.10 συμπεραίνουμε ότι $n \mid l$, οπότε

$$\left.\begin{array}{r} \exists \nu \in \mathbb{N} : l = \nu n \Rightarrow k = ml = m\nu n = \nu(mn) \geq mn \\ (3.24) \Longrightarrow k \leq mn \end{array}\right\} \Rightarrow k = mn,$$

και η απόδειξη λήγει εδώ. □

3.5.28 Πόρισμα. *Εάν οι* $H_1, \ldots, H_k$ *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 οι $H_1, \ldots, H_k$ *είναι υποομάδες πεπερασμένου δείκτη, τότε και η* $\bigcap_{j=1}^{k} H_j$ *είναι υποομάδα πεπερασμένου δείκτη.*

ΑΠΟΔΕΙΞΗ. Άμεση κατόπιν εφαρμογής τού (i) τού θεωρήματος 3.5.27 και μαθηματικής επαγωγής ως προς τον k. □

3.6 ΠΗΛΙΚΟΟΜΑΔΕΣ ΚΑΙ ΘΕΩΡΗΜΑΤΑ ΙΣΟΜΟΡΦΙΣΜΩΝ

► **Ορθόθετες υποομάδες.** Μεταξύ των υποομάδων μιας ομάδας συγκαταλέγονται πάντοτε κάποιες οι οποίες είναι «ορθώς τιθέμενες» (= *ορθόθετες*), υπό την έννοια ότι κάθε αριστερή πλευρική τους κλάση τους είναι και δεξιά και τανάπαλιν.

3.6.1 Πρόταση. *Έστω $(G,\cdot)$ μια ομάδα και έστω H μια υποομάδα της. Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες* :

(i) *Οι σχέσεις ισοδυναμίας "$\sim_\delta$" και "$\sim_\alpha$" 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 "$\sim_\delta$" και "$\sim_\alpha$" είναι συμβατές με την πράξη "$\cdot$"* (βλ. 1.5.19).

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. 3.5.9). Άρα $gH = Hg,\ \forall g \in G.$

(iii)⇔(iv). Προφανώς, $gH = Hg \Leftrightarrow gHg^{-1} = Hgg^{-1} = He_G = H,\ \forall g \in G.$

(v)⇒(iv). Εξ υποθέσεως, $gHg^{-1} \subseteq H,\ \forall g \in G.$ Κατά συνέπειαν, για το αντίστροφο g^{-1} *οιουδήποτε* στοιχείου $g \in G$, έχουμε $g^{-1}H\left(g^{-1}\right)^{-1} = g^{-1}Hg \subseteq H$. Για κάθε $g \in G$, ύστερα από «πολλαπλασιασμό» τού $g^{-1}Hg$ με το g εξ αριστερών και με το g^{-1} εκ δεξιών λαμβάνουμε $g\left(g^{-1}Hg\right)g^{-1} \subseteq gHg^{-1} \subseteq H$, οπότε

$$H = e_GHe_G = (gg^{-1})H(gg^{-1}) = g\left(g^{-1}Hg\right)g^{-1} \subseteq gHg^{-1},$$

απ' όπου έπεται ότι $gHg^{-1} = H,\ \forall g \in G.$

(v)⇒(vi). Ας υποθέσουμε ότι $g_1, g_2, g_1', g_2' \in G$ με $g_1 \sim_\delta g_2$ και $g_1' \sim_\delta g_2'$. Τότε $g_2g_1^{-1} \in H$ και $g_2'g_1'^{-1} \in H$, και (εξ υποθέσεως) $g_1(g_2'g_1'^{-1})g_1^{-1} \in H$. Άρα

$$\left.\begin{matrix} g_2g_1^{-1} \in H \\ g_1(g_2'g_1'^{-1})g_1^{-1} \in H \end{matrix}\right\} \Rightarrow \left(g_2g_1^{-1}\right)\left(g_1(g_2'g_1'^{-1})g_1^{-1}\right) = (g_2g_2')(g_1'^{-1}g_1^{-1}) \in H,$$

οπότε $(g_2g_2')(g_1'^{-1}g_1^{-1}) = (g_2g_2')(g_1g_1')^{-1} \in H \Rightarrow g_1g_1' \sim_\delta g_2g_2'$. Η απόδειξη τής συμβατότητας τής "$\sim_\alpha$" με την "$\cdot$" είναι παρόμοια.

(vi)⇒(v). Για κάθε $h \in H$ και κάθε $g \in G$ έχουμε

$$\left.\begin{array}{c} g \sim_\delta g \\ h \sim_\delta e_G \end{array}\right\} \Longrightarrow gh \sim_\delta ge_G = g \Rightarrow g \sim_\delta gh,$$

οπότε

$$\left.\begin{array}{c} g \sim_\delta gh \\ g^{-1} \sim_\delta g^{-1} \end{array}\right\} \Rightarrow e_G = gg^{-1} \sim_\delta ghg^{-1} \underset{\text{ορσ}}{\Longleftrightarrow} ghg^{-1}e_G = ghg^{-1} \in H.$$

Άρα $gHg^{-1} \subseteq H,\ \forall g \in G$. (Τούτο αποδεικνύεται παρομοίως εάν εργασθούμε με την "$\sim_\alpha$" στη θέση τής "$\sim_\delta$".) □

3.6.2 Ορισμός. Έστω $(G, \cdot)$ μια ομάδα. Μια υποομάδα H τής G ονομάζεται **ορθόθετη**[27] (σημειούμενη συνήθως ως[28] $H \lhd G$) όταν πληρούται μία (και, κατ' επέκτασιν, και οιαδήποτε άλλη) εκ των συνθηκών (i)-(vi) τής προτάσεως 3.6.1.

3.6.3 Πρόταση. *Η τετριμμένη υποομάδα μιας ομάδας G και η ίδια η G αποτελούν πάντοτε ορθόθετες υποομάδες τής G.*

ΑΠΟΔΕΙΞΗ. Προφανώς, $G \lhd G$. Εξάλλου, $\forall g \in G$ έχουμε $ge_G = g = e_G g$, οπότε $\{e_G\} \lhd G$. □

3.6.4 Πρόταση. *Εάν οι H και K είναι δυο υποομάδες μιας ομάδας $(G, \cdot)$, τέτοιες ώστε $K \subseteq H$ και $K \lhd G$, τότε $K \lhd H$.*

ΑΠΟΔΕΙΞΗ. Θεωρούμε τυχόντα στοιχεία $k \in K$ και $h \in H$. Προφανώς,

$$\left.\begin{array}{c} h \in G \\ K \lhd G \end{array}\right\} \Rightarrow hkh^{-1} \in K,$$

οπότε $hKh^{-1} \subseteq K \Rightarrow K \lhd H$. □

3.6.5 Παρατήρηση. (i) Με τα δεδομένα τής προτάσεως 3.6.4 δεν μπορούμε να συμπεράνουμε ότι θα ισχύει κατ' ανάγκην $H \lhd G$. Επί παραδείγματι, θέτοντας $G := \mathfrak{S}_3$, $H := \langle [1\,2] \rangle = \{\mathrm{id},\ [1\,2]\}$ και $K := \{\mathrm{id}\}$ έχουμε $H \not\lhd G$ (βλ. 3.5.15).

(ii) Έστω $(G, \cdot)$ μια ομάδα. Η διμελής σχέση «$K \backsim H \underset{\text{ορσ}}{\Longleftrightarrow} K$ υποομάδα τής H» επί τού συνόλου όλων των υποομάδων τής $(G, \cdot)$ είναι προφανώς ανακλαστική, αντισυμμετρική και μεταβατική (ήτοι μια σχέση μερικής διατάξεως, βλ. 1.4.1). Αντιθέτως, η διμελής σχέση «$K \backsim H \underset{\text{ορσ}}{\Longleftrightarrow} K \lhd H$» επί τού ιδίου συνόλου *δεν είναι*

[27] 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.

[28] Κατ' αναλογίαν, το σύμβολο $H \not\lhd G$ σημαίνει ότι η H δεν είναι ορθόθετη υποομάδα τής G.

μεταβατική. Επί παραδείγματι, θέτοντας $G := \mathfrak{A}_4$, $H := \mathbf{V}$ (ομάδα των τεσσάρων στοιχείων τού Klein, βλ. 3.4.26 (ii)) και $K := \langle [1\,2] \circ [3\,4] \rangle$, έχουμε $K \lhd H$, $H \lhd G$ αλλά $K \not\lhd G$ (βλ. άσκηση ??).

3.6.6 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 3.2.18 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 $H_j \lhd G$ 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, $g(\bigcap\limits_{j\in J} H_j)g^{-1} \subseteq \bigcap\limits_{j\in J} H_j \Rightarrow \bigcap\limits_{j\in J} H_j \lhd G$. □

3.6.7 Πρόταση. *Έστω H μια υποομάδα μιας ομάδας $(G,\cdot)$. Εάν ο δείκτης τής G εντός τής H είναι $|G:H| = 2$, τότε $H \lhd G$.*

ΑΠΟΔΕΙΞΗ. Εξ υποθέσεως,

$$\exists g \in G \smallsetminus H : G = H \coprod gH \ \text{ και } \ \exists g' \in G \smallsetminus H : G = H \coprod Hg'.$$

Επομένως, $gH = Hg' = G \smallsetminus H$. Ως εκ τούτου, κάθε αριστερή πλευρική κλάση τής H εντός τής G είναι και δεξιά πλευρική κλάση και τανάπαλιν. Αυτό όμως σημαίνει ότι $H \lhd G$. □

3.6.8 Παράδειγμα. Έστω n ένας φυσικός αριθμός ≥ 2. Επειδή, σύμφωνα με τις προτάσεις 3.4.3 και 3.4.23, $|\mathfrak{S}_n| = n!$ και $|\mathfrak{A}_n| = \frac{n!}{2}$, το θεώρημα 3.5.18 τού Lagrange μας πληροφορεί ότι $|\mathfrak{S}_n : \mathfrak{A}_n| = \frac{|\mathfrak{S}_n|}{|\mathfrak{A}_n|} = 2$. Άρα $\mathfrak{A}_n \lhd \mathfrak{S}_n$.

3.6.9 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 $ge_Gg^{-1} = e_G \in gHg^{-1}$. Εν συνεχεία θεωρούμε τυχόντα στοιχεία gh_1g^{-1} και gh_2g^{-1} τού gHg^{-1}. Προφανώς,

$$\left(gh_1g^{-1}\right)\left(gh_2g^{-1}\right)^{-1} = \left(gh_1g^{-1}\right)\left(gh_2^{-1}g^{-1}\right) = g(\underbrace{h_1h_2^{-1}}_{\in H})g^{-1} \in gHg^{-1},$$

οπότε το gHg^{-1} είναι πράγματι μια υποομάδα τής G δυνάμει τού (iii) τής προτάσεως 3.2.15. Επιπροσθέτως, η απεικόνιση $H \ni h \longmapsto ghg^{-1} \in gHg^{-1}$ είναι αμφιρριπτική. Άρα $\left|gHg^{-1}\right| = |H|$. □

3.6.10 Πρόταση. *Έστω H είναι μια πεπερασμένη υποομάδα μιας ομάδας $(G,\cdot)$ τάξεως $|H|=m\in\mathbb{N}$. Εάν η H είναι η μοναδική υποομάδα τής $(G,\cdot)$ τάξεως m, τότε $H\lhd G$.*

ΑΠΟΔΕΙΞΗ. Έστω τυχόν στοιχείο $g\in G$. Σύμφωνα με το λήμμα 3.6.9 το σύνολο gHg^{-1} αποτελεί μια υποομάδα τής G τάξεως $\left|gHg^{-1}\right|=|H|=m$. Εξ υποθέσεως, $gHg^{-1}=H\Rightarrow H\lhd G$. □

3.6.11 Πρόταση. *Εάν η $f:(G,\cdot)\longrightarrow(H,*)$ είναι ένας ομομορφισμός ομάδων, τότε ισχύουν τα ακόλουθα*:

(i) *Η εικόνα $f(K)$ οιασδήποτε ορθόθετης υποομάδας K τής G μέσω τής f είναι μια ορθόθετη υποομάδα τής $f(G)$.*

(ii) *Η αντίστροφη εικόνα $f^{-1}(L)=\{g\in G\mid f(g)\in L\}$ οιασδήποτε ορθόθετης υποομάδας L τής H μέσω τού f είναι μια ορθόθετη υποομάδα τής G.*

ΑΠΟΔΕΙΞΗ. (i) Κατά το 3.3.5 (i) η εικόνα $f(K)$ οιασδήποτε υποομάδας K τής G μέσω τής f είναι μια υποομάδα τής $f(G)$. Εάν υποθέσουμε ότι $K\lhd G$, 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

$$\left.\begin{array}{r} h*v*h^{-1}=f(g)*f(u)*f(g)^{-1}=f(gug^{-1})\\ u\in K,\ K\lhd G\Rightarrow gug^{-1}\in K\end{array}\right\}\Rightarrow h*v*h^{-1}\in f(K).$$

Κατά συνέπειαν, $f(K)\lhd f(G)$.

(ii) Κατά το 3.3.5 (ii) η αντίστροφη εικόνα $f^{-1}(L)$ οιασδήποτε υποομάδας L τής H μέσω τής f είναι μια υποομάδα τής G. Εάν υποθέσουμε ότι $L\lhd H$, 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, $f^{-1}(L)\lhd G$. □

3.6.12 Πόρισμα. *Ο πυρήνας οιουδήποτε ομομορφισμού ομάδων $f:(G,\cdot)\to(H,*)$ είναι ορθόθετη υποομάδα τής G.*

ΑΠΟΔΕΙΞΗ. Άμεση από τα 3.3.4 (ii), 3.6.3 και 3.6.11 (ii), καθόσον ο πυρήνας $\mathrm{Ker}(f)$ είναι εξ ορισμού η αντίστροφη εικόνα τής τετριμμένης υποομάδας τής H μέσω τής απεικονίσεως f. □

3.6.13 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 (3.8). Κατά το (i) τού

θεωρήματος 3.4.21 και την παρατήρηση 3.4.24 η sgn είναι ένας επιμορφισμός ομάδων. Εφαρμόζοντας το πόρισμα 3.6.12 διαπιστώνουμε εκ νέου ότι $\mathfrak{A}_n \lhd \mathfrak{S}_n$ (πρβλ. 3.6.8).

(ii) Έστω $F \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p\}$ (όπου p πρώτος αριθμός). Τότε ο ομομορφισμός ομάδων

$$\det : \mathrm{GL}_n(F) \longrightarrow F^\times,\ \mathbf{A} \longmapsto \det(\mathbf{A}),$$

είναι επιμορφισμός, διότι

$$\det \begin{pmatrix} x & 0_F & \cdots & 0_F \\ \vdots & 1_F & & \vdots \\ \vdots & & \ddots & 0_F \\ 0_F & \cdots & 0_F & 1_F \end{pmatrix} = x,\ \ \forall x \in F^\times,$$

και έχει ως πυρήνα του την $\mathrm{SL}_n(F)$, οπότε $\mathrm{SL}_n(F) \lhd \mathrm{GL}_n(F)$ (βλ. 3.2.17 (vii)).

(iii) Ο επιμορφισμός ομάδων

$$\det : \mathrm{O}_n(\mathbb{R}) \longrightarrow \{1, -1\},\ \mathbf{A} \longmapsto \det(\mathbf{A}),$$

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

$$\det : \mathrm{U}_n(\mathbb{C}) \longrightarrow \mathbb{S}^1,\ \mathbf{A} \longmapsto \det(\mathbf{A}),$$

έχει ως πυρήνα του την $\mathrm{SU}_n(\mathbb{C})$, οπότε $\mathrm{SU}_n(\mathbb{C}) \lhd \mathrm{U}_n(\mathbb{C})$.

3.6.14 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 $H \lhd G$. □

► **Απλές ομάδες**. Ένα σημαντικό τμήμα τής Θεωρίας Ομάδων συναρτάται με τη μελέτη εκείνων των ομάδων που διαθέτουν *τον ελάχιστο δυνατό αριθμό* ορθόθετων υποομάδων.

3.6.15 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 δομής των *μη αβελιανών*.

3.6.16 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 3.6.14, οι μόνες υποομάδες της είναι η τετριμμένη και ο εαυτός της. Αρκεί λοιπόν η εφαρμογή τού πορίσματος 3.3.17. □

3.6.17 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[29]. Ο πλήρης κατάλογος των μη αβελιανών, απλών πεπερασμένων ομάδων υποδιαιρείται, σε αδρές γραμμές, σε τρεις κλάσεις ομάδων. Αυτές είναι οι εξής:

(i) Οι *εναλλάσσουσες ομάδες*[30] $\mathfrak{A}_n$, $n \geq 5$.

(ii) Διάφορες οικογένειες ομάδων *τύπου Lie*[31].

(iii) Οι *σποραδικές ομάδες*[32] (ήτοι 26 ειδικές απλές ομάδες που δεν εντάσσονται στις (i)-(ii)).]

► **Πηλικοομάδες**. 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.

3.6.18 Ορισμός. Εάν η H είναι μια ορθόθετη υποομάδα μιας ομάδας $(G, \cdot)$, τότε συμβολίζουμε ως

$$\boxed{G/H := G/\sim_{\alpha} \ (= G/\sim_{\delta})}$$

[29] 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. Ashbacher: *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).

[30] Η απόδειξη τού ότι οι $\mathfrak{A}_n$, $n \geq 5$, είναι απλές είναι κατά τι μακροσκελής, αλλ' εντούτοις εφικτή με τα τεχνικά μέσα που διαθέτουμε εδώ· είθισται, ωστόσο, λόγω των υφιστάμενων χρονικών περιορισμών, να παρατίθεται μόνον στις παραδόσεις τού μαθήματος τής «αμιγούς» Θεωρίας Ομάδων.

[31] Βλ. R.W. Carter: *Finite Groups of Lie Type*, Wiley, (1985).

[32] Βλ. M. Ashbacher: *Sporadic Groups*, Cambridge Tracts in Math., Vol. **104**, Cambridge University Press, (1994).

το αντίστοιχο σύνολο των κλάσεων ισοδυναμίας και ως $\pi_H : G \longrightarrow G/H$ τη φυσική επίρριψη $\pi_{\sim_\alpha}$ (δηλαδή $\pi_H(g) := gH, \forall g \in G$, βλ. 1.3.3, 1.3.4 και 3.5.8).

3.6.19 Πρόταση. *Έστω $(G, \cdot)$ μια ομάδα και έστω H μια ορθόθετη υποομάδα της. Τότε υφίσταται μία και μόνον απεικόνιση*

$$(G/H) \times (G/H) \longrightarrow G/H, \;\; (gH, g'H) \longmapsto gH \odot g'H,$$

ήτοι μία και μόνον εσωτερική πράξη "$\odot$" επί τού G/H, η οποία καθιστά το διάγραμμα

$$\begin{array}{ccc} G \times G & \xrightarrow{\quad\cdot\quad} & G \\ \Big\downarrow{\scriptstyle \pi_H \times \pi_H} & & \Big\downarrow{\scriptstyle \pi_H} \\ (G/H) \times (G/H) & \xrightarrow[\quad\odot\quad]{} & G/H \end{array}$$

μεταθετικό. Συγκεκριμένα,

$$\boxed{gH \odot g'H := (g \cdot g')\, H, \;\; \forall (g, g') \in G \times G,}$$

και το ζεύγος $(G/H, \odot)$ αποτελεί μια ομάδα τάξεως $|G/H| = |G : H|$ έχουσα το $e_G H \,(= H)$ 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.*

ΑΠΟΔΕΙΞΗ. Επειδή η "$\sim_\alpha$" είναι συμβατή με την "$\cdot$" (βλ. 3.6.1), η απόδειξη τής προτάσεως έπεται άμεσα κατόπιν εφαρμογής τού θεωρήματος 1.5.20. □

3.6.20 Ορισμός. Η ομάδα $(G/H, \odot)$ η ορισθείσα μέσω τής προτάσεως 3.6.19 καλείται **πηλικοομάδα** (ή **ομάδα πηλίκων**) τής G ως προς την H. (Επειδή έχουμε $x \sim_\alpha y \underset{\text{ορσ}}{\iff} y^{-1}x \in H$, 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».)

3.6.21 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 $(gH)\,(g'H)$ 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 3.6.19 (και που απλώς *επάγεται* μέσω τού «πολλαπλασιασμού» τού ορισμένου επί τού G).

3.6.22 Πρόταση. *Έστω H μια ορθόθετη υποομάδα μιας ομάδας $(G,\cdot)$. Η φυσική επίρριψη*

$$\pi_H : G \longrightarrow G/H,\ \ g \longmapsto \pi_H(g) := gH,$$

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 είναι ομομορφισμός ομάδων και ότι $\mathrm{Ker}(\pi_H) = H$. Για οιαδήποτε στοιχεία $g, g' \in G$ έχουμε

$$\pi_H(gg') = (gg')H = (gH)\,(g'H) = \pi_H(g)\pi_H(g').$$

Εξάλλου, $\mathrm{Ker}(\pi_H) = \{g \in G \,|\pi_H(g) = H\,\} = \{g \in G\,|gH = H\,\} = H$. □

3.6.23 Πόρισμα. *Μια υποομάδα H μιας ομάδας $(G,\cdot)$ είναι ορθόθετη εάν και μόνον εάν αποτελεί τον πυρήνα ενός ομομορφισμού ομάδων $f : (G,\cdot) \longrightarrow (G',*)$.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από την πρόταση 3.6.22 και το πόρισμα 3.6.12. □

3.6.24 Πρόταση. *Έστω H μια υποομάδα μιας κυκλικής ομάδας $(G,\cdot)$. Τότε η G/H είναι κυκλική.*

ΑΠΟΔΕΙΞΗ. Η G ως κυκλική είναι αβελιανή (βλ. 3.2.27), οπότε η H είναι ορθόθετη (βλ. 3.6.14). Ως εκ τούτου, ορίζεται η πηλικομάδα G/H. Εάν θεωρήσουμε κάποιον γεννήτορα $g \in G$ τής G, τότε τα στοιχεία τής G/H είναι τής μορφής $g^nH = (gH)^n$, όπου $n \in \mathbb{Z}$. Κατά συνέπειαν, $G/H = \langle gH \rangle$. □

3.6.25 Πρόταση. *Έστω H μια ορθόθετη υποομάδα μιας ομάδας $(G,\cdot)$. Για οιοδήποτε $g \in G$ η τάξη τού στοιχείου gH τής G/H ισούται με*

$$\mathrm{ord}(gH) = \begin{cases} \infty, & \text{όταν } g^k \notin H,\ \forall k \in \mathbb{N}, \\ \min\{\,k \in \mathbb{N} \mid\ g^k \in H\}, & \text{στην αντίθετη περίπτωση.} \end{cases}$$

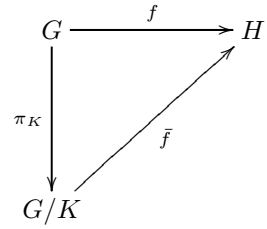
ΑΠΟΔΕΙΞΗ. Έστω τυχόν στοιχείο $g \in G$. Εάν $g^k \notin H,\ \forall k \in \mathbb{N}$, τότε προφανώς $g^kH = (gH)^k \neq H,\ \forall k \in \mathbb{N}$, οπότε $\mathrm{ord}(gH) = \infty$. Εάν $\{\,k \in \mathbb{N} \mid\ g^k \in H\} \neq \varnothing$ και $m := \min\{\,k \in \mathbb{N} \mid\ g^k \in H\}$, τότε $m = \min\{\,k \in \mathbb{N} \mid\ (gH)^k = H\} = \mathrm{ord}(gH)$. □

► **Θεωρήματα ισομορφισμών ομάδων**. Αυτά είναι ορισμένα χαρακτηριστικά θεωρήματα που περιγράφουν τον τρόπο διασυνδέσεως των ομομορφισμών ομάδων, των ορθόθετων υποομάδων και των πηλικοομάδων.

3.6.26 Θεώρημα. (Θεμελιώδες θεώρημα περί πηλικοομάδων) *Έστω*

$$f : (G, \cdot) \longrightarrow (H, *)$$

ένας ομομορφισμός ομάδων και έστω $K \lhd G$. *Εάν* $K \subseteq \mathrm{Ker}(f)$, *τότε υφίσταται μία και μόνον απεικόνιση* $\bar{f} : G/K \longrightarrow H$, *τέτοια ώστε να ισχύει* $f = \bar{f} \circ \pi_K$, *δηλαδή τέτοια ώστε το διάγραμμα*



(3.25)

να καθίσταται μεταθετικό. Η απεικόνιση αυτή ορίζεται μέσω τού τύπου

$$\boxed{\bar{f}(gK) := f(g), \ \ \forall g \in G,} \tag{3.26}$$

και αποτελεί ομομορφισμό ομάδων. Επιπροσθέτως, ισχύουν τα ακόλουθα:

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

(ii) $\mathrm{Ker}(\bar{f}) = \mathrm{Ker}(f)/K$.

(iii) *Η* $\bar{f}$ *είναι μονομορφισμός εάν και μόνον εάν* $K = \mathrm{Ker}(f)$.

ΑΠΟΔΕΙΞΗ. Έστω $\mathcal{R}_f$ η σχέση ισοδυναμίας η επαγομένη μέσω τού f επί τής G (βλ. 1.3.22). Η σχέση ισοδυναμίας "$\sim_\alpha$" η οριζόμενη επί τής G *μέσω τής υποομάδας* K (βλ. (3.10)) περιέχεται σε αυτήν, δηλαδή $\sim_\alpha \subseteq \mathcal{R}_f$. Πράγματι· εάν $g_1, g_2 \in G$, τότε

$$g_1 \sim_\alpha g_2 \underset{\text{ορσ}}{\Longleftrightarrow} g_2^{-1} g_1 \in K \subseteq \mathrm{Ker}(f) \Rightarrow f(g_2^{-1} g_1) = f(g_2)^{-1} * f(g_1) = e_H.$$

Κατόπιν «πολλαπλασιασμού» αμφοτέρων των μελών τής τελευταίας ισότητας εξ αριστερών με το $f(g_2)$ λαμβάνουμε

$$g_1 \sim_\alpha g_2 \Rightarrow f(g_1) = f(g_2) \underset{\text{ορσ}}{\Longleftrightarrow} (g_1, g_2) \in \mathcal{R}_f.$$

Εφαρμόζοντας το θεμελιώδες θεώρημα 1.3.25 (περί συνόλων κλάσεων ισοδυναμίας) κατασκευάζουμε τη μοναδική απεικόνιση $\bar{f} : G/K \longrightarrow H$ που καθιστά το διάγραμμα (3.25) μεταθετικό. Αυτή ορίζεται μέσω τού τύπου (3.26) και αποτελεί ομομορφισμό ομάδων, διότι για οιαδήποτε $g_1, g_2 \in G$ έχουμε

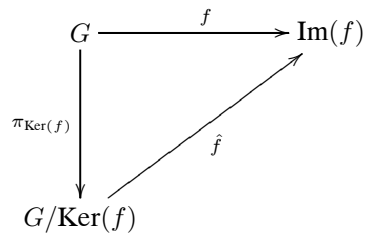
$$\begin{aligned} \bar{f}(g_1 K) * \bar{f}(g_2 K) &= f(g_1) * f(g_2) = f(g_1 g_2) \\ &= \bar{f}((g_1 g_2)\, K) = \bar{f}((g_1 K)(g_2 K)). \end{aligned}$$

(i) Εκ κατασκευής, $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f)$ (βλ. 1.3.25 (b)).
(ii) Επειδή εξ υποθέσεως $K \lhd G$ και $K \subseteq \mathrm{Ker}(f)$, η πρόταση 3.6.4 μας πληροφορεί ότι $K \lhd \mathrm{Ker}(f)$. Κατά συνέπειαν, ορίζεται η πηλικομάδα $\mathrm{Ker}(f)/K$. Προφανώς,

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

(iii) Τούτο είναι άμεση συνέπεια τού (ii) και τής προτάσεως 3.3.9. □

3.6.27 Πρώτο Θεώρημα Ισομορφισμών. *Έστω $f : (G, \cdot) \to (H, *)$ 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 3.6.26 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* $\mathrm{Im}(f) \subseteq H$. (Πρβλ. 1.3.26.) □

3.6.28 Παραδείγματα. (i) Εάν $m \in \mathbb{N}$, τότε η απεικόνιση

$$(\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_m, +), \;\; n \longmapsto [n]_m$$

είναι ένας επιμορφισμός ομάδων με πυρήνα του την υποομάδα $m\mathbb{Z}$ τής ομάδας $\mathbb{Z}$ (βλ. 3.2.17 (iii)). Συνεπώς,

$$\boxed{\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m.}$$

(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 στον ισομορφισμό

$$\boxed{\mathbb{S}^1/\{\pm 1\} \cong \mathbb{S}^1.}$$

(v) Μέσω τού επιμορφισμού 3.6.13 (i) κατασκευάζεται ο ισομορφισμός

$$\boxed{\mathfrak{S}_n/\mathfrak{A}_n \cong \{\pm 1\}.}$$

(vi) Μέσω τού επιμορφισμού 3.6.13 (ii) κατασκευάζεται ο ισομορφισμός

$$\boxed{\mathbf{GL}_n(F)/\mathbf{SL}_n(F) \cong F^\times.}$$

(vii) Μέσω τού επιμορφισμού 3.6.13 (iii) κατασκευάζεται ο ισομορφισμός

$$\boxed{\mathbf{O}_n(\mathbb{R})/\mathbf{SO}_n(\mathbb{R}) \cong \{\pm 1\}.}$$

(viii) Μέσω τού επιμορφισμού 3.6.13 (iv) κατασκευάζεται ο ισομορφισμός

$$\boxed{\mathbf{U}_n(\mathbb{C})/\mathbf{SU}_n(\mathbb{C}) \cong \mathbb{S}^1.}$$

(ix) Έστω ότι η G είναι μια ομάδα και $\mathrm{Aut}(G)$ η ομάδα των αυτομορφισμών της (βλ. 3.3.18). Το υποσύνολο $\mathrm{Inn}(G)$ τής $\mathrm{Aut}(G)$ το αποτελούμενο από όλους τους αυτομορφισμούς τής μορφής

$$\phi_h : G \longrightarrow G, \quad \phi_h(g) = h^{-1}gh, \ \forall g, \ g \in G,$$

όπου $h \in G$, είναι μια ορθόθετη υποομάδα τής $\mathrm{Aut}(G)$. Τα στοιχεία τού $\mathrm{Inn}(G)$ ονομάζονται **εσωτερικοί αυτομορφισμοί** τής G. Η απεικόνιση

$$f : G \longrightarrow \mathrm{Inn}(G), \quad f(h) = \phi_h, \ \forall h, \ h \in G,$$

είναι ένας επιμορφισμός ομάδων με πυρήνα του τον $\mathrm{Ker}(f) = Z(G)$, όπου

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

είναι το λεγόμενο **κέντρο** τής ομάδας G. Επομένως,

$$\boxed{G/Z(G) \cong \mathrm{Inn}(G).}$$

3.6.29 Πόρισμα. (Φυσική «παραγοντοποίηση» ομομορφισμών) *Κάθε ομομορφισμός ομάδων $f : (G, \cdot) \longrightarrow (H, *)$ γράφεται ως σύνθεση τριών απεικονίσεων*

$$\boxed{f = (\mathrm{id}_H|_{\mathrm{Im}(f)}) \circ \hat{f} \circ \pi_{\mathrm{Ker}(f)},}$$

τού φυσικού επιμορφισμού $\pi_{\mathrm{Ker}(f)}$, τού ισομορφισμού $\hat{f}$ τού κατασκευασθέντος στο θεώρημα 3.6.27 *και τού μονομορφισμού $\mathrm{id}_H|_{\mathrm{Im}(f)}$.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το πόρισμα 1.3.27 και το θεώρημα 3.6.27. □

3.6.30 Πόρισμα. *Έστω $(G, \cdot)$ μια πεπερασμένη ομάδα και έστω $f : (G, \cdot) \to (H, *)$ ένας ομομορφισμός ομάδων. Εάν η K είναι μια υποομάδα τής ομάδας $(G, \cdot)$, τότε ισχύουν τα ακόλουθα:*

(i) $|K| = |f(K)| \, |\mathrm{Ker}(f|_K)|$.

(ii) $|G : K| = |f(G) : f(K)| \, |\mathrm{Ker}(f) : \mathrm{Ker}(f|_K)|$.

ΑΠΟΔΕΙΞΗ. (i) Ύστερα από περιορισμό τού πεδίου τιμών τής $f|_K$ στο $f(K)$ προκύπτει ένας επιμορφισμός ομάδων $f|_K : K \longrightarrow f(K)$. Κατά το θεώρημα 3.6.27,

$$K/\mathrm{Ker}(f|_K) \cong \mathrm{Im}(f|_K) = f(K),$$

όπου $\mathrm{Ker}(f|_K) = \mathrm{Ker}(f) \cap K$,οπότε ο ισχυρισμός είναι αληθής επί τη βάσει τού θεωρήματος 3.5.18 τού Lagrange.

(ii) Δυνάμει τού (i) (στην ειδική περίπτωση όπου $K = G$) ισχύει η ισότητα

$$|G| = |f(G)|\ |\mathrm{Ker}(f)|\,.$$

Κατά συνέπειαν,

$$\left.\begin{array}{r} |G| = |f(G)|\ |\mathrm{Ker}(f)| \\ |K| = |f(K)|\ \left|\mathrm{Ker}(f|_K)\right| \end{array}\right\} \Rightarrow |G:K| = |f(G):f(K)|\ \left|\mathrm{Ker}(f):\mathrm{Ker}(f|_K)\right|,$$

κατόπιν εφαρμογής τού θεωρήματος 3.5.18 τού Lagrange. □

3.6.31 Θεώρημα. (Τύπος γινομένου) *Εάν οι H, K είναι πεπερασμένες υποομάδες μιας ομάδας $(G,\cdot)$, τότε*

$$\boxed{\mathrm{card}(HK) = \frac{|H|\ |K|}{|H\cap K|}.} \tag{3.27}$$

ΑΠΟΔΕΙΞΗ. Ορίζουμε την επιρριπτική απεικόνιση

$$\vartheta : H\times K \longrightarrow HK,\ \ (h,k)\longmapsto \vartheta(h,k) := hk.$$

Αρκεί να αποδείξουμε ότι

$$\mathrm{card}(\vartheta^{-1}(x)) = |H\cap K|\,,\ \ \forall x\in HK,$$

διότι[33] $H\times K = \coprod\limits_{x\in HK} \vartheta^{-1}(x)$ και $\mathrm{card}(H\times K) = |H|\ |K|$. Έστω τυχόν $x\in HK$. Τότε $\exists h\in H, k\in K$: $x = hk$ και

$$\vartheta^{-1}(x) = \{(hr, r^{-1}k)\,|r\in H\cap K\,\}. \tag{3.28}$$

Πράγματι· κάθε διατεταγμένο ζεύγος ειλημμένο από το $H\times K$ και έχον τη μορφή $(hr, r^{-1}k)$, για κάποιο $r\in H\cap K$, ανήκει στην ίνα $\vartheta^{-1}(x)$ τής ϑ υπεράνω τού x, διότι

$$\vartheta(hr, r^{-1}k) = (hr)(r^{-1}k) = h(rr^{-1})k = he_Gk = hk = x.$$

Για την απόδειξη τού αντιστρόφου εγκλεισμού θεωρούμε τυχόν διατεταγμένο ζεύγος $(h',k')\in\vartheta^{-1}(x)$. Τότε

$$\vartheta(h',k') = h'k' = x = hk \Rightarrow h^{-1}h' = kk'^{-1} =: r\in H\cap K.$$

Για το κατ' αυτόν τον τρόπο ορισθέν r έχουμε $h' = hr$ και $k' = r^{-1}k$, οπότε η (3.28) είναι αληθής. Επομένως,

$$\mathrm{card}(\vartheta^{-1}(x)) = \mathrm{card}(\{(hr, r^{-1}k)\,|r\in H\cap K\,\}) = |H\cap K|\,,$$

καθότι η απεικόνιση $H\cap K\ni r\longmapsto (hr, r^{-1}k)\in\vartheta^{-1}(x)$ είναι αμφιρριπτική. □

[33] Εάν $x, x'\in HK$ με $x\neq x'$, τότε $f^{-1}(x)\cap f^{-1}(x') = \varnothing$, διότι εάν υπήρχε $z\in f^{-1}(x)\cap f^{-1}(x')$, τότε θα συμπεραίναμε ότι $x = f(z) = x'$.

3.6.32 Λήμμα. *Εάν οι H, K είναι υποομάδες μιας ομάδας $(G, \cdot)$ και $H \lhd \langle H, K\rangle$, όπου $\langle H, K\rangle := \langle H \cup K\rangle$ (βλ. 3.2.20), τότε ισχύουν τα εξής:*

(i) $HK = \langle H, K\rangle = KH$.

(ii) $H \cap K \lhd K$.

ΑΠΟΔΕΙΞΗ. (i) Θεωρούμε τυχόντα στοιχεία $h \in H$ και $k \in K$. Επειδή

$$\left.\begin{array}{r} h \in H \lhd \langle H, K\rangle \\ k \in \langle H, K\rangle \end{array}\right\} \Rightarrow hkh^{-1} \in \langle H, K\rangle \Rightarrow hkh^{-1} = x^m,$$

για κάποιο $x \in H \cup K$ και κάποιον $m \in \mathbb{Z}$, έχουμε $hk = x^m h$. Εάν $x \in H$, τότε $hk \in H \subseteq KH$. Εάν $x \in K$, τότε $hk \in KH$. Άρα σε κάθε περίπτωση $hk \in KH$. Εξ αυτού έπεται ότι $HK \subseteq KH$. Επιπροσθέτως, επειδή $h \in H \Rightarrow h^{-1} \in H$, έχουμε

$$\left.\begin{array}{r} h^{-1} \in H \lhd \langle H, K\rangle \\ k \in \langle H, K\rangle \end{array}\right\} \Rightarrow h^{-1}k(h^{-1})^{-1} = h^{-1}kh \in \langle H, K\rangle \Rightarrow h^{-1}kh = y^n,$$

για κάποιο $y \in H \cup K$ και κάποιον $n \in \mathbb{Z}$, οπότε $kh = hy^n$. Εάν $y \in H$, τότε $kh \in H \subseteq HK$. Εάν $y \in K$, τότε $kh \in HK$. Άρα σε κάθε περίπτωση $kh \in HK$. Εξ αυτού έπεται ότι $KH \subseteq HK$. Τελικώς λοιπόν, $HK = KH$ και το HK (σύμφωνα με την πρόταση 3.5.3) είναι μια *υποομάδα* της G η οποία περιέχεται στην υποομάδα $\langle H, K\rangle$. Επειδή η $\langle H, K\rangle$ είναι η *ελαχίστη* υποομάδα της G (ως προς τον συνολοθεωρητικό εγκλεισμό) η οποία περιέχει την ένωση $H \cup K \subseteq HK$, ισχύει κατ' ανάγκην η ισότητα $HK = \langle H, K\rangle$.

(ii) Εάν $f := \pi_H \circ \iota_K$, όπου $\pi_H : HK \longrightarrow HK/H$ ο φυσικός επιμορφισμός και

$$\iota_K : K \longrightarrow KH, \;\; k \longmapsto \iota_K(k) := k,$$

τότε η f δίδεται από τον τύπο

$$f(k) := \pi_H(\iota_K(k)) = \pi_H(k) = kH, \;\; \forall k \in K,$$

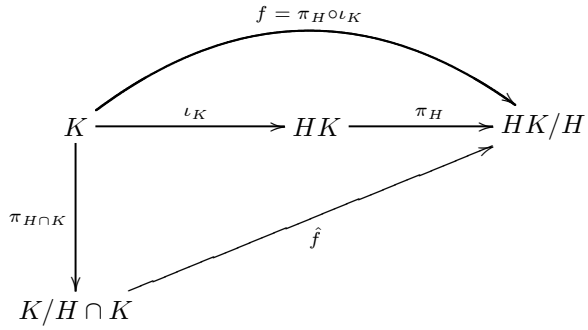
και (ούσα σύνθεση δύο ομομορφισμών ομάδων) είναι ομομορφισμός ομάδων με πυρήνα του τον

$$\mathrm{Ker}(f) = \{\, k \in K \mid kH = H\} = \{\, k \in K \mid k \in H\} = H \cap K.$$

Άρα $H \cap K \lhd K$ (σύμφωνα με το πόρισμα 3.6.12). □

3.6.33 Δεύτερο Θεώρημα Ισομορφισμών. *Έστω ότι οι H, K είναι δυο υποομάδες μιας ομάδας $(G, \cdot)$ με $H \lhd \langle H, K\rangle$. Εάν $f := \pi_H \circ \iota_K$, όπου $\pi_H : HK \longrightarrow HK/H$*

ο φυσικός επιμόρφισμός και $\iota_K : K \longrightarrow KH,\ k \longmapsto \iota_K(k) := k$, *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 ομάδων. Ως εκ τούτου,

$$\boxed{K/\,H \cap K \cong HK/\,H\ (= \langle H, K\rangle\ /\,H)} \tag{3.29}$$

ΑΠΟΔΕΙΞΗ. Κατά το λήμμα 3.6.32, $HK = \langle H, K\rangle = KH$ και $\mathrm{Ker}(f) = H \cap K \lhd K$. Επομένως ορίζονται οι πηλικοομάδες $HK/\,H$ και $K/\,H \cap K$. Έστω $(hk)H$ τυχόν στοιχείο τής πηλικοομάδας $HK/\,H$ (όπου $h \in H$ και $k \in K$). Τότε

$$(hk)H = (hH)(kH) = H(kH) = (e_G H)(kH) = (e_G k)H = kH = f(k),$$

οπότε ο f είναι *επιμορφισμός* ομάδων. Εφαρμόζοντας γι' αυτόν το 1ο θεώρημα ισομορφισμών 3.6.27 κατασκευάζουμε τον ισομορφισμό

$$\hat{f} : K/\,H \cap K \longrightarrow HK/\,H,\ \ k(H \cap K) \longmapsto f(k) = kH,$$

με τις επιθυμητές ιδιότητες. □

3.6.34 Παρατήρηση. (i) Σε ορισμένα συγγράμματα, στη διατύπωση τού 2ου θεωρήματος ισομορφισμών, αντί τής συνθήκης "$H \lhd \langle H, K\rangle$" παρατίθεται η συνθήκη "$H \lhd G$". Ωστόσο, η πρώτη είναι ασθενέστερη τής δεύτερης, διότι κατόπιν εφαρμογής τής προτάσεως 3.6.4 συμπεραίνουμε ότι $H \lhd G \ \Rightarrow\ H \lhd \langle H, K\rangle$ (αφού $H \subseteq \langle H, K\rangle$).

(ii) Στην περίπτωση όπου οι H και K πεπερασμένες υποομάδες τής G και $H \lhd \langle H, K\rangle$, ο τύπος τού γινομένου (3.27) έπεται άμεσα από τον ισομορφισμό (3.29), τη σημείωση 3.5.17 και το θεώρημα 3.5.18 τού Lagrange. Ωστόσο, το θεώρημα 3.6.31 μας πληροφορεί ότι ο εν λόγω τύπος εξακολουθεί να ισχύει *ακόμη και όταν το σύνολο* HK *δεν είναι υποομάδα τής* G.

3.6.35 Παράδειγμα. Θεωρούμε τις υποομάδες $H := 3\mathbb{Z}$ και $K := 4\mathbb{Z}$ τής (αβελιανής, προσθετικής) ομάδας $(\mathbb{Z}, +)$. Επειδή $H \cap K = 12\mathbb{Z}$ και $HK = \mathbb{Z}$, το θεώρημα 3.6.33 μας παρέχει τον ισομορφισμό

$$\mathbb{Z} \,/\, 4\mathbb{Z} \cong 3\mathbb{Z} \,/\, 12\mathbb{Z}.$$

3.6.36 Παράδειγμα. Έστω $\mathbf{V}$ η ομάδα των τεσσάρων στοιχείων τού Klein (βλ. το (ii) τού εδαφίου 3.4.26) και έστω $\sigma \in \mathfrak{S}_4$. Επειδή

$$\sigma \circ ([1\,2] \circ [3\,4]) \circ \sigma^{-1} = [\sigma(1)\,\sigma(2)] \circ [\sigma(3)\,\sigma(4)]$$

και $\{\sigma(1), \sigma(2), \sigma(3), \sigma(4)\} = \{1, 2, 3, 4\}$, έχουμε $\sigma \circ ([1\,2] \circ [3\,4]) \circ \sigma^{-1} \in \mathbf{V}$. Κατ' αναλογίαν,

$$\sigma \circ ([1\,3] \circ [2\,4]) \circ \sigma^{-1} \in \mathbf{V} \;\text{ και }\; \sigma \circ ([1\,4] \circ [2\,3]) \circ \sigma^{-1} \in \mathbf{V}.$$

Επομένως, $\mathbf{V} \lhd \mathfrak{S}_4$. Έστω $K := \{\sigma \in \mathfrak{S}_4 \,|\, \sigma\,(4) = 4\}$. Προφανώς, $K \cong \mathfrak{S}_3$. Θα δείξουμε ότι $\mathbf{V}K = \mathfrak{S}_4$. Έστω τυχούσα μετάταξη $\sigma \in \mathfrak{S}_4$. Εάν $\sigma\,(4) = 4$, τότε έχουμε $\sigma \in K \subseteq \mathbf{V}K$. Εάν $\sigma\,(4) = j$, για κάποιον $j \in \{1, 2, 3\}$, τότε η συντιθέμενη μετάταξη $\tau := [j\ 4] \circ \sigma$ ανήκει στην K (διότι αφήνει το 4 αμετάβλητο). Θεωρώντας τήν αντιμετάθεση $[l\ m]$, όπου $\{l, m\} = \{1, 2, 3\} \smallsetminus \{j\}$, $l \neq m$, συμπεραίνουμε (μέσω των (i), (v) και (vi) τής προτάσεως 3.4.9) ότι

$$\sigma = [j\ 4]^{-1} \circ \tau = [j\ 4] \circ \tau = (\underbrace{[j\ 4] \circ [l\ m]}_{\in \mathbf{V}})(\underbrace{[l\ m] \circ \tau}_{\in K}) \in \mathbf{V}K.$$

Άρα όντως $\mathbf{V}K = \mathfrak{S}_4$. 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, το θεώρημα 3.6.33 μας παρέχει τον ισομορφισμό

$$\mathfrak{S}_3 \cong K \cong K/\{\mathrm{id}\} \cong \mathfrak{S}_4/\,\mathbf{V}.$$

3.6.37 Τρίτο Θεώρημα Ισομορφισμών. *Εάν οι H, K είναι ορθόθετες υποομάδες μιας ομάδας $(G, \cdot)$ και $K \subseteq H$, τότε $H/K \lhd G/K$ και υφίσταται μία και μόνον απεικόνιση $\tilde{\pi}_K : G/H \longrightarrow (G/K) \,/\, (H/K)$, τέτοια ώστε το διάγραμμα*

$$\begin{array}{ccc} G & \xrightarrow{\ \pi_K\ } & G/K \\ \Big\downarrow{\scriptstyle \pi_H} & & \Big\downarrow{\scriptstyle \pi_{H/K}} \\ G/H & \xrightarrow[\ \tilde{\pi}_K\ ]{} & (G/K)/(H/K) \end{array} \tag{3.30}$$

να καθίσταται μεταθετικό. Η απεικόνιση αυτή ορίζεται μέσω τού τύπου

$$\boxed{\check{\pi}_K(gH) := (gK)(H/K),\ \ \forall g \in G,} \tag{3.31}$$

και αποτελεί ισομορφισμό ομάδων. Ως εκ τούτου,

$$\boxed{G/H \cong (G/K)\ /\ (H/K)\,.} \tag{3.32}$$

ΑΠΟΔΕΙΞΗ. Επειδή $K \subseteq H$ και και $K \lhd G$, έχουμε $K \lhd H$ (βλ. πρόταση 3.6.4). Ως εκ τούτου, ορίζεται η πηλικομάδα H/K. Επειδή $H \lhd G$, έχουμε για κάθε $g \in G$ και για κάθε $h \in H$,

$$ghg^{-1} \in H \Rightarrow (ghg^{-1})K \in H/K,$$

οπότε

$$(ghg^{-1})K = (gK)(hK)(g^{-1}K) = (gK)(hK)(gK)^{-1} \in H/K,$$

πράγμα που σημαίνει ότι $H/K \lhd G/H$ και ότι ορίζεται η πηλικοομάδα $(G/K)\ /\ (H/K)$. Έστω $\mathcal{R}_{\pi_{H/K}\circ\pi_K}$ η σχέση ισοδυναμίας η επαγομένη μέσω τής συνθέσεως $\pi_{H/K} \circ \pi_K$ επί τής G (βλ. 1.3.22), όπου

$$\pi_K : G \longrightarrow G/K,\ \ g \longmapsto gK,$$

και

$$\pi_{H/K} : G/K \longrightarrow (G/K)\ /\ (H/K)\,,\ \ gK \longmapsto (gK)(H/K),$$

οι αντίστοιχοι φυσικοί επιμορφισμοί. Αυτή ισούται με τη σχέση ισοδυναμίας "$\sim_\alpha$" την οριζόμενη επί τής G *μέσω τής υποομάδας* H (βλ. (3.10)). Πράγματι· εάν θεωρήσουμε τυχόντα στοιχεία $g_1, g_2 \in G$, τότε

$$\begin{aligned}
&g_1 \sim_\alpha g_2 \underset{\text{ορσ}}{\Longleftrightarrow} g_2^{-1}g_1 \in H \Leftrightarrow (g_2^{-1}g_1)K \in H/K\\
&\Leftrightarrow (g_2^{-1}K)(g_1K) \in H/K \Leftrightarrow (g_1K)\,(H/K) = (g_2K)\,(H/K)\\
&\Leftrightarrow (\pi_{H/K} \circ \pi_K)(g_1) = (\pi_{H/K} \circ \pi_K)(g_2).
\end{aligned}$$

Εν συνεχεία, εφαρμόζοντας το πόρισμα 1.3.29 κατασκευάζουμε τη μοναδική απεικόνιση $\check{\pi}_K : G/H \longrightarrow (G/K)\ /\ (H/K)$ που καθιστά το διάγραμμα (3.30) μεταθετικό. Αυτή ορίζεται μέσω τού τύπου (3.31) και είναι ενριπτική. Επιπροσθέτως, είναι και επιρριπτική, διότι $\mathrm{Im}(\check{\pi}_K) = \mathrm{Im}(\pi_{H/K}\circ\pi_K) = (G/K)\ /\ (H/K)\,$. Υπολείπεται να ελεγχθεί ότι η $\check{\pi}_K$ είναι ομομορφισμός ομάδων. Για οιαδήποτε στοιχεία $g_1, g_2 \in G$ έχουμε

$$\begin{aligned}
\check{\pi}_K(g_1H)\check{\pi}_K(g_2H) &= ((g_1K)(H/K))\,((g_2K)(H/K))\\
&= ((g_1K)(g_2K))\,(H/K) = ((g_1g_2)K)(H/K)\\
&= \check{\pi}_K((g_1g_2)\,H) = \check{\pi}_K((g_1H)(g_2H)),
\end{aligned}$$

οπότε η απόδειξη λήγει εδώ. □

3.6.38 Σημείωση. Ένας εναλλακτικός τρόπος αποδείξεως τής υπάρξεως ενός ισομορφισμού (3.32) είναι ο εξής: Θεωρούμε την

$$f : G/K \longrightarrow G/H, \quad f(gK) := gH, \ \forall g \in G.$$

Η f είναι καλώς ορισμένη απεικόνιση, διότι για οιαδήποτε $g_1, g_2 \in G$ για τα οποία $g_1K = g_2K$ έχουμε $g_2^{-1}g_1 \in K \subseteq H$, οπότε $g_1H = g_2H$. Επιπροσθέτως, η f είναι (εκ κατασκευής) επιριπτική και μάλιστα επιμορφισμός ομάδων, διότι για οιαδήποτε $g_1, g_2 \in G$ έχουμε

$$\begin{aligned} f((g_1K)(g_2K)) &= f((g_1g_2)K) = (g_1g_2)H \\ &= (g_1H)(g_2H) = f(g_1K)f(g_2K). \end{aligned}$$

Προφανώς, $\mathrm{Ker}(f) = \{\, gK \in G/K \mid gH = H\} = H/K$. Επομένως, είναι δυνατόν να εφαρμόσουμε το 1ο θεώρημα ισομορφισμών 3.6.27 και να κατασκευάσουμε τον ισομορφισμό

$$\hat{f} : (G/K) \ / \ (H/K) \longrightarrow G/\,H, \ \ (gK)(H/K) \longmapsto f(gK) = gH.$$

Είναι πλέον πρόδηλο ότι ο ισομορφισμός $\hat{f}$ είναι ο αντίστροφος τού ανωτέρω κατασκευασθέντος ισομορφισμού $\tilde{\pi}_K$.

3.6.39 Παράδειγμα. Εάν $m, n \in \mathbb{N}$, τότε οι $m\mathbb{Z}$ και $n\mathbb{Z}$ είναι ορθόθετες υποομάδες τής $(\mathbb{Z}, +)$. Υποθέτοντας ότι η $m\mathbb{Z}$ είναι υποομάδα τής $n\mathbb{Z}$ (που ισοδυναμεί με το ότι $n \mid m$), έχουμε $(\mathbb{Z}/m\mathbb{Z}) \ / \ (n\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$.

3.7 ΚΛΑΣΕΙΣ ΣΥΖΥΓΙΑΣ

3.7.1 Ορισμός. Έστω $(G, \cdot)$ μια ομάδα. Δυο στοιχεία $x, y \in G$ καλούνται **συζυγή στοιχεία** εντός τής G (σημειούμενα ως $x \underset{\text{συζ.}}{\sim} y$) όταν υπάρχει κάποιο $g \in G$, ούτως ώστε να ισχύει η ισότητα $y = gxg^{-1}$. Είναι εύκολο να ελεγχθεί ότι η κατ' αυτόν τον τρόπο οριζόμενη διμελής σχέση "$\underset{\text{συζ.}}{\sim}$" είναι μια σχέση ισοδυναμίας επί τού υποκειμένου συνόλου G τής θεωρούμενης ομάδας. Η κλάση ισοδυναμίας ενός στοιχείου $x \in G$ ως προς την "$\underset{\text{συζ.}}{\sim}$" καλείται **κλάση συζυγίας** τού x (εντός τής G) και συμβολίζεται ως εξής:

$$\boxed{\mathrm{ΚΛΣ}_G(x) := \{y \in G \,|\, x \underset{\text{συζ.}}{\sim} y\}.}$$

3.7.2 Σημείωση. Η κλάση συζυγίας ενός $x \in G$ είναι μονοσύνολο εάν και μόνον εάν το x ανήκει στο κέντρο $Z(G)$ τής G (βλ. 3.6.28 (ix)). Πράγματι·

$$\begin{aligned} \text{ΚΛΣ}_G(x) = \{x\} \quad &\Leftrightarrow \quad gxg^{-1} = x, \forall g \in G \\ &\Leftrightarrow \quad gx = xg, \forall g \in G \Leftrightarrow x \in Z(G). \end{aligned}$$

3.7.3 Πρόταση. *Συζυγή στοιχεία εντός μιας ομάδας $(G, \cdot)$ έχουν την ίδια τάξη.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το (ii) τής προτάσεως 3.2.35. □

3.7.4 Πρόταση. *Έστω H μια υποομάδα μιας ομάδας $(G, \cdot)$. Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) $H \lhd G$.

(ii) *H υποομάδα H είναι ένωση κάποιων κλάσεων συζυγίας εντός τής G.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii). Για κάθε $h \in H$ έχουμε $ghg^{-1} \in H$, οπότε $\text{ΚΛΣ}_G(h) \subseteq H$.

(ii)⇒(i). Επειδή η H είναι ένωση κάποιων κλάσεων συζυγίας εντός τής G, τα στοιχεία τής G που είναι συζυγή οιουδήποτε στοιχείου $h \in H$ θα περιέχονται κατ' ανάγκην στην H, οπότε $gHg^{-1} \subseteq H$ για κάθε $g \in G$. □

3.7.5 Ορισμός. Έστω $(G, \cdot)$ μια ομάδα και έστω $g \in G$. Το σύνολο

$$\boxed{C_G(g) := \{x \in G \,|gx = xg\}}$$

όλων των στοιχείων τής $(G, \cdot)$ που μετατίθενται αμοιβαίως με το g καλείται **κεντροποιητής τού** g εντός τής G. Προφανώς,

$$Z(G) = \bigcap_{g \in G} C_G(g).$$

Σημειωτέον ότι η $(G, \cdot)$ είναι αβελιανή $\Leftrightarrow G = Z(G)$.

3.7.6 Λήμμα. *Έστω $(G, \cdot)$ μια ομάδα και έστω $g \in G$. Τότε ισχύουν τα ακόλουθα*:

(i) *Ο κεντροποιητής $C_G(g)$ τού g είναι μια υποομάδα τής G.*

(ii) *Το πλήθος των στοιχείων μιας ομάδας $(G, \cdot)$ που είναι συζυγή τού g ισούται με τον δείκτη $|G : C_G(g)|$ τού $C_G(g)$ εντός τής G.*

ΑΠΟΔΕΙΞΗ. (i) Προφανώς, $e_G \in C_G(g)$. Επιπροσθέτως, εάν $x, y \in C_G(g)$, τότε

$$\left.\begin{aligned} gx = xg \\ gy = yg \Rightarrow g = y^{-1}gy \end{aligned}\right\} \Rightarrow gx = xy^{-1}gy \Rightarrow gxy^{-1} = xy^{-1}g,$$

οπότε $xy^{-1} \in C_G(g)$. Βάσει τού (iii) τής προτάσεως 3.2.15 ο κεντροποιητής $C_G(g)$ τού g είναι μια υποομάδα τής G.

(ii) Έστω A ένα σύστημα αριστερών εκπροσώπων τού $C_G(g)$ εντός τής G. Ορίζουμε την β μέσω τού τύπου

$$\{xC_G(g)\,|x \in \mathrm{A}\} \ni xC_G(g) \overset{\beta}{\longmapsto} xgx^{-1} \in \text{ΚΛΣ}_G(g).$$

Αυτή είναι καλώς ορισμένη απεικόνιση, διότι για $x, y \in \mathrm{A}$ με $xC_G(g) = yC_G(g)$ έχουμε

$$x^{-1}y \in C_G(g) \Rightarrow gx^{-1}y = x^{-1}yg \Rightarrow xgx^{-1} = ygy^{-1}.$$

Η β είναι ενριπτική, καθότι ισχύουν οι συνεπαγωγές

$$\begin{aligned} \beta\left(xC_G(g)\right) &= \beta\left(yC_G(g)\right) \Rightarrow xgx^{-1} = ygy^{-1} \\ &\Rightarrow x^{-1}y \in C_G(g) \Rightarrow xC_G(g) = yC_G(g). \end{aligned}$$

Τέλος, η β είναι και επιριπτική, αφού για κάθε $z \in \text{ΚΛΣ}_G(g)$ υπάρχει κάποιο στοιχείο $x \in G : z = xgx^{-1}$, οπότε $\beta\left(xC_G(g)\right) = z$. □

3.7.7 Πρόταση. (Εξίσωση κλάσεων συζυγίας) *Έστω $(G, \cdot)$ μια μη αβελιανή πεπερασμένη ομάδα. Εάν τα $g_1, \ldots, g_m$ 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*

$$\boxed{|G| = |Z(G)| + \sum_{j=1}^{m} |G : C_G(g_j)|\,.} \tag{3.33}$$

ΑΠΟΔΕΙΞΗ. Εάν $Z(G) = \{e_G = z_1, z_2, ..., z_k\}$ και εάν οι $\mathcal{C}_1, \ldots, \mathcal{C}_m$ είναι οι σαφώς διακεκριμένες κλάσεις συζυγίας που δεν περιέχονται στο $Z(G)$ με $g_j \in \mathcal{C}_j$ για κάθε $j \in \{1, ..., m\}$, τότε το

$$\{e_G = z_1, z_2, ..., z_k, \mathcal{C}_1 = \text{ΚΛΣ}_G(g_1), \ldots, \mathcal{C}_m = \text{ΚΛΣ}_G(g_m)\}$$

αποτελεί ένα πλήρες σύστημα εκπροσώπων τής G ως προς την "$\underset{\text{συζ.}}{\sim}$". Επομένως,

$$G = \left(\coprod_{\varrho=1}^{k} \{z_\varrho\}\right) \coprod \left(\coprod_{j=1}^{m} \text{ΚΛΣ}_G(g_j)\right) \Rightarrow |G| = k + \sum_{j=1}^{m} \text{card}(\text{ΚΛΣ}_G(g_j)).$$

Η (3.33) έπεται θέτοντας $|Z(G)| = k$ και

$$\text{card}(\text{ΚΛΣ}_G(g_j)) = |G : C_G(g_j)|\,,\ \forall j \in \{1, ..., m\},$$

επί τη βάσει τού λήμματος 3.7.6. □

3.7.8 Θεώρημα. *Έστω $(G,\cdot)$ μια πεπερασμένη 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 $G=Z(G)$, οπότε

$$|G|=|Z(G)|=p^\nu>1.$$

Εάν η $(G,\cdot)$ δεν είναι αβελιανή, τότε, θεωρώντας εκπροσώπους $g_1,\ldots,g_m$ εκείνων των σαφώς διακεκριμένων κλάσεων συζυγίας που δεν περιέχονται στο κέντρο $Z(G)$ τής G, έχουμε (εκ κατασκευής) $|G:C_G(g_j)|>1$ για κάθε $j\in\{1,...,m\}$ και η (3.33) γράφεται ως εξής:

$$p^\nu=|Z(G)|+\sum_{j=1}^{m}|G:C_G(g_j)|\,.$$

Κατά το θεώρημα 3.5.18 τού Lagrange, $|G:C_G(g_j)|\mid p^\nu$ για κάθε $j\in\{1,...,m\}$, οπότε

$$\exists\xi_j\in\{1,...,\nu\}:|G:C_G(g_j)|=p^{\xi_j},\ \forall j\in\{1,...,m\},$$

(πρβλ. 2.3.10). Επομένως,

$$|Z(G)|=p\left(p^{\nu-1}-\sum_{j=1}^{m}p^{\xi_j-1}\right),$$

απ' όπου έπεται ότι $p\mid|Z(G)|\Rightarrow 1<p\le|Z(G)|$. □

3.7.9 Σημείωση. Λόγω τού θεωρήματος 3.5.18 τού Lagrange, το κέντρο $Z(G)$ τής G οφείλει να έχει τάξη $|Z(G)|=p^\kappa$, όπου $\kappa\in\{1,...,\nu\}$ (με $\kappa=\nu$ εάν και μόνον εάν η G είναι αβελιανή).

3.8 ΕΥΘΕΑ ΓΙΝΟΜΕΝΑ ΟΜΑΔΩΝ

Το **ευθύ γινόμενο** $G\times H$ δυο ομάδων $(G,\cdot)$ και $(H,*)$ κατασκευάζεται ως ακολούθως: τα στοιχεία τού $G\times H$ είναι διατεταγμένα ζεύγη (g,h), όπου $g\in G$ και $h\in H$, ενώ ο πολλαπλασιασμός επ' αυτού ορίζεται μέσω τής

$$(g,h)\circledcirc(g',h')=(g\cdot g',h*h').$$

Αμφότερα τα g,g' είναι στοιχεία τής G και, πολλαπλασιαζόμενα εντός τής G, δίδουν την πρώτη «συντεταγμένη» αυτού τού γινομένου. Η δεύτερη «συντεταγμένη» προέρχεται από τον πολλαπλασιασμό τού h με το h' εντός τής H. Επομένως, το

$(g \cdot g', h * h')$ είναι ένα στοιχείο τού καρτεσιανού γινομένου $G \times H$. Η προσεταιριστικότητα έπεται άμεσα από την προσεταιριστικότητα των πολλαπλασιαστικών πράξεων των G και H. Επίσης, το (e_G, e_H) είναι το ουδέτερο στοιχείο, ενώ το (g^{-1}, h^{-1}) είναι το αντίστροφο τού στοιχείου (g, h). (Από εδώ και στο εξής θα απλουστεύσουμε εκ νέου τον συμβολισμό μας και αντί των "$\circledcirc$" και "$*$" θα γράφουμε απλώς "$\cdot$", γνωρίζοντας τι εννοούμε κατά περίπτωση.)

3.8.1 Θεώρημα. $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ *εάν και μόνον εάν* μκδ$(m, n) = 1$.

ΑΠΟΔΕΙΞΗ. Έστω k η τάξη τού στοιχείου $([1]_m, [1]_n)$ εντός τής $\mathbb{Z}_m \times \mathbb{Z}_n$ (βλ. 3.2.30). Αθροίζοντας το $([1]_m, [1]_n)$ με τον εαυτό του k φορές λαμβάνουμε το $([0]_m, [0]_n)$, οπότε έχουμε

$$[k]_m = [0]_m \ \text{ και } \ [k]_n = [0]_n \Rightarrow m \mid k \ \text{ και } \ n \mid k.$$

Εάν μκδ$(m, n) = 1$, τότε, κατά το πόρισμα 2.3.15, $mn \mid k$, οπότε $mn \leq k$. Επειδή $k \leq mn = |\mathbb{Z}_m \times \mathbb{Z}_n|$ (βλ. 3.5.22), έχουμε τελικώς $k = mn$ και η $\mathbb{Z}_m \times \mathbb{Z}_n$ (σύμφωνα με την πρόταση 3.2.33) είναι κυκλική με το $([1]_m, [1]_n)$ ως γεννήτορά της. Επιπροσθέτως, κατά το (ii) τού θεωρήματος 3.3.15,

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}.$$

Ας υποθέσουμε τώρα ότι $d := \text{μκδ}(m, n) > 1$. Αρκεί να δείξουμε ότι η $\mathbb{Z}_m \times \mathbb{Z}_n$ δεν είναι κυκλική. Προς τούτο ορίζουμε τους $m' := \frac{m}{d}$ και $n' := \frac{n}{d}$. Για οιοδήποτε στοιχείο $([l]_m, [l']_n)$ τής $\mathbb{Z}_m \times \mathbb{Z}_n$ έχουμε

$$\begin{aligned} m'dn'([l]_m, [l']_n) &= (m'dn'[l]_m, m'dn'[l']_n) \\ &= ([mn'l]_m, [m'nl']_n) \\ &= ([0]_m, [0]_n), \end{aligned}$$

οπότε

$$\text{ord}(([l]_m, [l']_n)) \leq m'dn' < mn.$$

Επομένως, η ομάδα $\mathbb{Z}_m \times \mathbb{Z}_n$ δεν είναι κυκλική, διότι δεν περιέχει κανένα στοιχείο τάξεως mn (βλ. πρόταση 3.2.33). □

3.8.2 Θεώρημα. *Εάν οι H και K είναι υποομάδες μιας ομάδας $(G, \cdot)$, για τις οποίες πληρούνται οι εξής συνθήκες*:

(i) $HK = G$,

(ii) $H \cap K = \{e_G\}$, *και*

(iii) $hk = kh$, $\forall h \in H$ *και* $\forall k \in K$, *τότε*

$$\boxed{G \cong H \times K.}$$

ΑΠΟΔΕΙΞΗ. Ορίζουμε την απεικόνιση

$$\vartheta : H \times K \longrightarrow G, \quad (x,y) \longmapsto \vartheta(x,y) := xy.$$

Για οιαδήποτε $(x,y)(x',y') \in H \times K$ έχουμε

$$\begin{aligned} \vartheta((x,y)(x',y')) &= \vartheta(xx',yy') = xx'yy' \\ &= xyx'y' \left(\begin{array}{c} \text{επειδή κάθε στοιχείο τής } H \\ \text{μετατίθεται με κάθε στοιχείο τής } K \end{array} \right) \\ &= \vartheta(x,y)\,\vartheta(x',y'). \end{aligned}$$

Τούτο σημαίνει ότι η ϑ είναι ομομορφισμός ομάδων. Εάν $\vartheta(x,y) = \vartheta(x',y')$, τότε

$$xy = x'y' \Longrightarrow (x')^{-1} x = y'y^{-1}.$$

Επειδή το αριστερό μέλος αυτής τής τελευταίας εξισώσεως ανήκει στην H και το δεξιό στην K, *και* τα δύο μέλη θα ανήκουν στην τομή $H \cap K = \{e_G\}$. Άρα

$$(x')^{-1} x = e_G = y'y^{-1} \Longrightarrow x = x', y = y',$$

οπότε η ϑ είναι ενριπτική. Η ϑ είναι και επιριπτική, καθότι η ισότητα $HK = G$ σημαίνει ότι κάθε στοιχείο τής G γράφεται ως ένα γινόμενο xy, όπου $x \in H$ και $y \in K$. Άρα η ϑ είναι *ισομορφισμός ομάδων*. □

3.8.3 Θεώρημα. *Εάν η $(G,\cdot)$ είναι μια ομάδα τάξεως $|G| = p^2$, όπου p πρώτος αριθμός, τότε είτε*

$$\boxed{G \cong \mathbb{Z}_{p^2}} \quad \textit{είτε} \quad \boxed{G \cong \mathbb{Z}_p \times \mathbb{Z}_p.}$$

ΑΠΟΔΕΙΞΗ. Έστω G μια ομάδα με ακριβώς p^2 στοιχεία. Εάν υπάρχει ένα στοιχείο τής G τάξεως p^2, τότε $G \cong \mathbb{Z}_{p^2}$ (βλ. 3.2.33 και 3.3.15 (ii)). Εάν δεν υπάρχει κανένα στοιχείο G τάξεως p^2, τότε (σύμφωνα με το θεώρημα 3.5.18 τού Lagrange) *κάθε στοιχείο* διαφορετικό τού ουδετέρου *οφείλει να έχει τάξη* p. Εν τοιαύτη περιπτώσει, το κέντρο $Z(G)$ τής G είναι μη τετριμμένο κατά το θεώρημα 3.7.8. Ως εκ τούτου, μπορούμε να επιλέξουμε ένα $x \in Z(G) \setminus \{e_G\}$ και ένα $y \in G \setminus \langle x \rangle$. Τα p^2 στοιχεία $x^i y^j, 1 \leq i,j \leq p$, είναι σαφώς διακεκριμένα, καθότι $\langle x \rangle \cap \langle y \rangle = \{e_G\}$. Επομένως, $\langle x \rangle \langle y \rangle = G$. Κάθε στοιχείο τής $\langle x \rangle$ μετατίθεται με κάθε στοιχείο τής $\langle y \rangle$, διότι $x \in Z(G)$. Κατά συνέπειαν, σύμφωνα με το θεώρημα 3.8.2, η G είναι ισόμορφη με την $\langle x \rangle \times \langle y \rangle$, οπότε $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ (βλ. 3.2.33 και 3.3.15 (ii)).

3.8.4 Σημείωση. Κατά το θεώρημα 3.8.1, $\mathbb{Z}_p \times \mathbb{Z}_p \ncong \mathbb{Z}_{p^2}$.

3.9 ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΟΜΑΔΩΝ ΤΑΞΕΩΣ ≤ 11

Κλείνουμε αυτό το κεφάλαιο ταξινομώντας *μέχρις ισομορφισμού* όλες τις πεπερασμένες ομάδες G με $|G| \leq 11$.

3.9.1 Θεώρημα. *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. Έστω G μια ομάδα με ακριβώς $2p$ στοιχεία. Εάν υπάρχει ένα στοιχείο τής G τάξεως $2p$, τότε $G \cong \mathbb{Z}_{2p}$ (βλ. 3.2.33 και 3.3.15 (ii)). Εάν υποθέσουμε ότι οι τάξεις όλων των στοιχείων τής G είναι $< 2p$, τότε $G \cong \mathbf{D}_p$. Πράγματι· σύμφωνα με το θεώρημα 3.5.18 τού Lagrange κάθε στοιχείο διαφορετικό τού ουδετέρου οφείλει να έχει τάξη είτε 2 είτε p. Εάν όλα τα $g \in G \smallsetminus \{e_G\}$ είχαν τάξη 2, τότε η G θα ήταν αβελιανή (βλ. 3.2.35 (iv)). Εν τοιαύτη περιπτώσει, για οιαδήποτε $a, b \in G \smallsetminus \{e_G\}$, $a \neq b$, το σύνολο $\{e_G, a, b, ab\}$ θα ήταν κλειστό ως προς την πράξη τής G, οπότε θα αποτελούσε υποομάδα τής G τάξεως 4, πράγμα που θα μας οδηγούσε σε άτοπο λόγω τού θεωρήματος 3.5.18 τού Lagrange (καθότι $4 \nmid 2p$). *Άρα η G διαθέτει κατ' ανάγκην κάποιο στοιχείο*, ας πούμε x, *τάξεως p.* Έστω τυχόν στοιχείο $y \in G \smallsetminus \langle x \rangle$. Επειδή $y\langle x \rangle \neq \langle x \rangle$ και $|G : \langle x \rangle| = 2$, έχουμε

$$G = \langle x \rangle \coprod y\langle x \rangle .$$

Επειδή οι $\langle x \rangle$ και $y\langle x \rangle$ είναι οι μόνες (ξένες) πλευρικές κλάσεις τής $\langle x \rangle$ εντός τής G, για το $y^2\langle x \rangle = (y\langle x \rangle)^2$ έχουμε

$$\text{είτε} \quad y^2\langle x \rangle = y\langle x \rangle \quad \text{είτε} \quad y^2\langle x \rangle = \langle x \rangle .$$

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,

$$y^2\langle x \rangle = \langle x \rangle \Rightarrow y^2 \in \langle x \rangle \Rightarrow \text{ είτε } \operatorname{ord}(y^2) = 1 \text{ είτε } \operatorname{ord}(y^2) = p.$$

Εξ υποθέσεως, $\operatorname{ord}(y^2) \neq p$ (διότι η $\operatorname{ord}(y^2) = p$ θα σήμαινε ότι $\operatorname{ord}(y) = 2p$). Άρα $\operatorname{ord}(y^2) = 1$, οπότε $\operatorname{ord}(y) = 2$. Ως εκ τούτου, *κάθε στοιχείο $y \in G \smallsetminus \langle x \rangle$ έχει τάξη 2*. Για οιοδήποτε $y \in G \smallsetminus \langle x \rangle$ έχουμε $xy \notin \langle x \rangle$, οπότε μέσω τού ανωτέρω επιχειρήματος συνάγουμε ότι

$$\operatorname{ord}(xy) = 2 \Rightarrow xyxy = e_G \Rightarrow yx = x^{-1}y^{-1} = x^{-1}y.$$

Αυτές οι σχέσεις καθορίζουν πλήρως τον πολλαπλασιαστικό κατάλογο τής G. Επειδή ο πολλαπλασιαστικός κατάλογος όλων των μη κυκλικών ομάδων τάξεως

$2p$ καθορίζονται πλήρως από την εξίσωση $yx = x^{-1}y$, όλες οι μη κυκλικές ομάδες τάξεως $2p$ είναι μεταξύ τους ισόμορφες. Βεβαίως, η $\mathbf{D}_p$ είναι (εκ κατασκευής) μία εξ αυτών. Άρα $G \cong \mathbf{D}_p$. □

3.9.2 Θεώρημα. (Cayley, 1859) *Έστω $(G, \cdot)$ μια ομάδα τάξεως $|G| = 8$. Τότε αυτή οφείλει να είναι ισόμορφη με μία εκ των ακολούθων ομάδων*:

$$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbf{D}_4, \mathbf{Q} \text{ (βλ. 3.2.24).}$$

ΑΠΟΔΕΙΞΗ. Έστω G μια ομάδα με ακριβώς οκτώ στοιχεία. Εάν υπάρχει ένα στοιχείο τής G τάξεως 8, τότε $G \cong \mathbb{Z}_8$ (βλ. 3.2.33 και 3.3.15 (ii)). Γι' αυτόν τον λόγο μπορούμε, από εδώ και στο εξής, να υποθέτουμε ότι οι τάξεις όλων των στοιχείων τής G είναι ≤ 4. Διακρίνουμε δύο περιπτώσεις:

► *Περίπτωση πρώτη.* Υποθέτουμε ότι *υπάρχει κάποιο στοιχείο*, έστω x, τής G *τάξεως* 4. Τότε επιλέγουμε ένα στοιχείο $y \in G \smallsetminus \{x\}$. Οι δεξιές πλευρικές κλάσεις $\langle x \rangle$ και $\langle x \rangle\, y$ μας παρέχουν τα οκτώ στοιχεία τής G υπό τη μορφή

$$e_G, x, x^2, x^3, y, xy, x^2y, x^3y.$$

Προφανώς, $yx \notin \langle x \rangle$, $yx \neq y$ (ειδάλλως θα είχαμε $yx = y \Rightarrow x = e_G$) και $yx \neq x^2y$ (διότι η ισότητα $yx = x^2y$ θα οδηγούσε στην $x = y^{-1}x^2y$, η οποία, με τη σειρά της, θα έδιδε $x^2 = y^{-1}x^2yy^{-1}x^2y = e_G$). Άρα $yx \in \{xy, x^3y\}$. Επιπροσθέτως, η τάξη τού y είναι είτε 2 είτε 4. Παρατηρούμε ότι $y^2 \notin \langle x \rangle\, y$ (διότι $y \notin \langle x \rangle$) και ότι $y^2 \notin \{x, x^3\}$ (διότι η τάξη τού y είναι διάφορη τού 8). Επομένως, εάν το y έχει τάξη 4, τότε $y^2 = x^2$. Υπάρχουν τέσσερα εν συνόλω ενδεχόμενα:

(i) Εάν $yx = xy$ και $y^2 = e_G$, τότε η G είναι αβελιανή και μέσω τής απεικονίσεως

$$x^j \longmapsto ([j]_4, [0]_2), \quad x^jy \longmapsto ([j]_4, [1]_2), \ \ \forall j \in \{0,1,2,3\},$$

κατακευάζεται ένας ισομορφισμός $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

(ii) Εάν $yx = x^3y$ και $y^2 = e_G$, και εάν χρησιμοποιήσουμε τον συμβολισμό τον εισαχθέντα στο (iii) τού εδαφίου 3.4.26, τότε διαπιστώνουμε ότι η απεικόνιση

$$x^j \longmapsto \sigma^j, \quad x^jy \longmapsto \sigma^j \circ \tau, \ \ \forall j \in \{0,1,2,3\},$$

προσδιορίζει έναν ισομορφισμό μεταξύ τής G και τής $\mathbf{D}_4$.

(iii) Εάν $yx = xy$ και $y^2 = x^2$, τότε η G είναι αβελιανή, το xy^{-1} έχει τάξη 2 και η απεικόνιση

$$x^j \longmapsto ([j]_4, [0]_2), \quad x^jy \longmapsto ([j+1]_4, [1]_2), \ \ \forall j \in \{0,1,2,3\},$$

μας οδηγεί στον καθορισμό ενός ισομορφισμού μεταξύ τής G και τής $\mathbb{Z}_4 \times \mathbb{Z}_2$.

(iv) Τέλος, εάν $yx = x^3y$ και $y^2 = x^2$, και εάν χρησιμοποιήσουμε τον συμβολισμό τον εισαχθέντα στο εδάφιο 3.2.24, τότε διαπιστώνουμε ότι η απεικόνιση

$$x^\nu \longmapsto \mathbf{j}^\nu, \quad x^\nu y \longmapsto \mathbf{j}^\nu \mathbf{k}, \ \ \forall \nu \in \{0,1,2,3\},$$

προσδιορίζει έναν ισομορφισμό μεταξύ τής G και τής ομάδας $\mathbf{Q}$ των τετρανίων.

► *Περίπτωση δεύτερη.* Υποθέτουμε ότι *κάθε στοιχείο που ανήκει στη διαφορά* $G \smallsetminus \{e_G\}$ *έχει τάξη* 2. Εν τοιαύτη περιπτώσει η G είναι *αβελιανή* ομάδα (βλ. το (iv) τής προτάσεως 3.2.35). Επιλέγουμε τρία στοιχεία $x, y, z \in G \smallsetminus \{e_G\}$, ούτως ώστε να ισχύει $xy \neq z$. Η υποομάδα $H = \{e_G, x, y, xy\}$ είναι ισόμορφη με την $\mathbb{Z}_2 \times \mathbb{Z}_2$ μέσω τής

$$x^j y^k \longmapsto ([j]_2\,, [k]_2), \ \ j,k \in \{0,1\},$$

και, εάν $K := \langle z \rangle$, τότε εύκολα διαπιστώνουμε ότι $HK = G$ και $H \cap K = \{e_G\}$. Επομένως,

$$G \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

επί τη βάσει τού θεωρήματος 3.8.2. □

3.9.3 Θεώρημα. (Ταξινομήσεως) *Η ταξινόμηση των ομάδων* $(G, \cdot)$ *με* $|G| \leq 11$ *μέχρις ισομορφισμού είναι αυτή που καταχωρίζεται στον ακόλουθο κατάλογο*:

τάξη	G
1	τετριμμένη
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ \mathbf{D}_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8,\ \mathbb{Z}_4 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ \mathbf{D}_4,\ \mathbf{Q}$
9	$\mathbb{Z}_9,\ \mathbb{Z}_3 \times \mathbb{Z}_3$
10	$\mathbb{Z}_{10},\ \mathbf{D}_5$
11	$\mathbb{Z}_{11}$

Οι ομάδες οι εμφανιζόμενες σε αυτόν τον κατάλογο είναι ανά δύο μη ισόμορφες.

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς θα εξηγήσουμε το πώς σχηματίζεται ο ανωτέρω κατάλογος. Όταν $|G| = 1$, τότε η G είναι τετριμμένη. Όταν $|G| \in \{2,3,5,7,11\}$, το συμπέρασμα εξάγεται από το πόρισμα 3.5.21 και το (ii) τού θεωρήματος 3.3.15. Όταν

$|G| \in \{4, 9\}$, αρκεί κανείς να εφαρμόσει το θεώρημα 3.8.3. Όταν $|G| \in \{6, 10\}$, τότε τίθεται σε εφαρμογή το θεώρημα 3.9.1. Τέλος, όταν $|G| = 8$, η ταξινόμηση μέχρις ισομορφισμού έχει γίνει στο θεώρημα 3.9.2. Εν συνεχεία, θα δείξουμε ότι οι ομάδες οι εμφανιζόμενες στον κατάλογο είναι ανά δύο μη ισόμορφες. Είναι προφανές ότι δυο ομάδες διαφορετικής τάξεως δεν είναι ισόμορφες (βλ. 3.3.10 (i)). Εξάλλου, κατά το θεώρημα 3.8.1, $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_8 \ncong \mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_9 \ncong \mathbb{Z}_3 \times \mathbb{Z}_3$. Επίσης, η $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ δεν μπορεί να είναι ισόμορφη με μία εκ των $\mathbb{Z}_4 \times \mathbb{Z}_2$ και $\mathbb{Z}_8$, διότι δεν διαθέτει κανένα στοιχείο τάξεως 4 ή 8 (βλ. 3.3.10 (iv)). Από την άλλη μεριά, η $\mathbf{D}_3$ δεν μπορεί να είναι ισόμορφη τής $\mathbb{Z}_6$, διότι δεν είναι αβελιανή (βλ. το (ii) τής προτάσεως 3.3.10) και, για τον ίδιο λόγο, η $\mathbf{D}_5$ δεν μπορεί να είναι ισόμορφη τής $\mathbb{Z}_{10}$ αλλά ούτε και η $\mathbf{D}_4$ να είναι ισόμορφη με μία εκ των $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Απομένει λοιπόν να δειχθεί ότι $\mathbf{D}_4 \ncong \mathbf{Q}$. Τούτο έπεται εύκολα από το γεγονός ότι η $\mathbf{Q}$ διαθέτει μόνον ένα στοιχείο τάξεως 2 (συγκεκριμένα το $\mathbf{j}^2 = -\mathbf{I}_2$), ενώ η $\mathbf{D}_4$ έχει εν συνόλω πέντε στοιχεία τάξεως 2. □