# ΚΕΦΑΛΑΙΟ 9

# Αβελιανές ομάδες

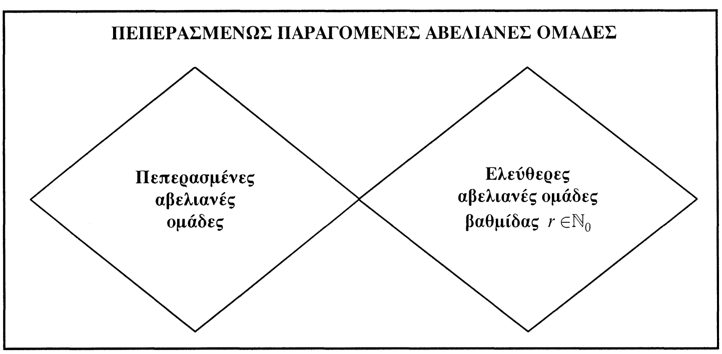
Το παρόν κεφάλαιο εστιάζεται αποκλειστικώς στην κλάση των *αβελιανών ομάδων*. Αυτή χωρίζεται σε τρεις υποκλάσεις:

(i) Πεπερασμένες αβελιανές ομάδες.

(ii) Άπειρες αλλά -ταυτοχρόνως- πεπερασμένως παραγόμενες αβελιανές ομάδες.

(iii) Μη πεπερασμένως παραγόμενες αβελιανές ομάδες.

Η μέχρις ισομορφισμού ταξινόμηση των *κυκλικών ομάδων* (πεπερασμένων και άπειρων) και η περιγραφή των υποομάδων τους και τής ομάδας των αυτομορφισμών τους έχουν ήδη παρουσιασθεί στο κεφάλαιο 2. (Βλ. θεώρημα 2.4.23, πόρισμα 2.4.26 και θεώρημα 2.4.32.) Τα εν λόγω θεωρητικά αποτελέσματα γενικεύονται καταλλήλως και για τις ανωτέρω υποκλάσεις (i) και (ii) τής κλάσεως των *αβελιανών ομάδων*, καθώς κάθε ομάδα ανήκουσα σε αυτές είναι ισόμορφη με το ευθύ άθροισμα πεπερασμένου πλήθους (προσθετικών) κυκλικών ομάδων. (Βλ. τα θεωρήματα 9.1.19, 9.1.25, 9.2.2, 9.2.4, 9.3.8 και 9.6.7, 9.6.10 και 9.6.11, αντιστοίχως.)

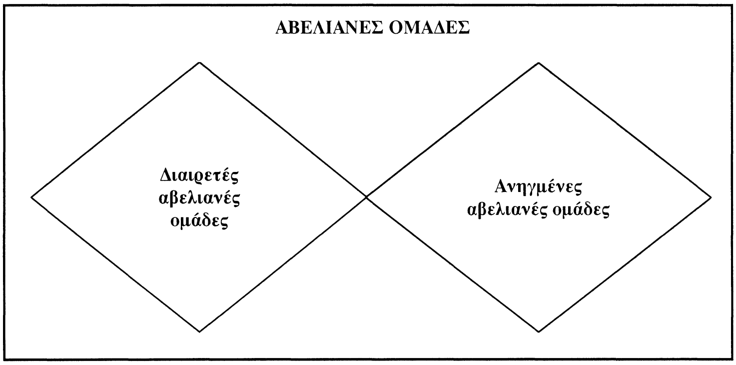



Ιδιαιτέρως, κάθε πεπερασμένως παραγόμενη αβελιανή ομάδα είναι ισόμορφη με το ευθύ άθροισμα δύο ομάδων: Η πρώτη εξ αυτών είναι *πεπερασμένη* και η δεύτερη *ελεύθερη πεπερασμένης βαθμίδας*. (Το σημείο συναντήσεως των δύο ρόμβων τού ανωτέρω σχήματος υποδηλοί την τετριμμένη.) Γενικότερα, για *τυχούσες* αβελιανές ομάδες αποδεικνύονται τα εξής:

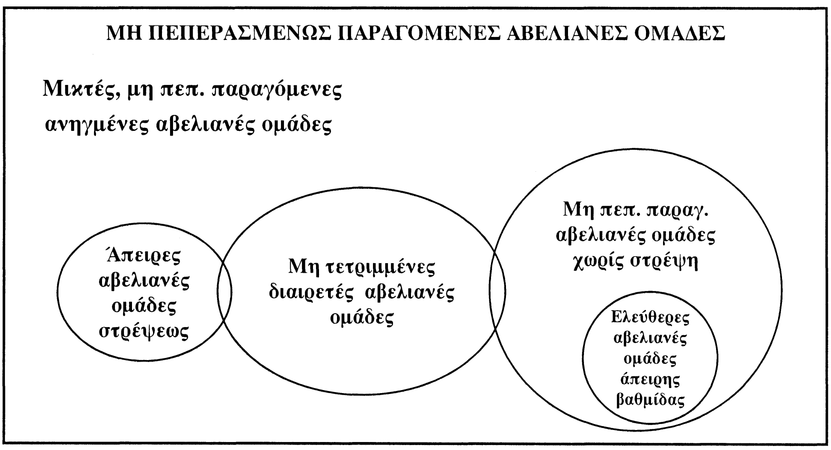
(α) Κάθε αβελιανή ομάδα είναι ισόμορφη με πηλικοομάδες που προκύπτουν ύστερα από «διαίρεση» *ελεύθερων* αβελιανών ομάδων διά καταλλήλων υποομάδων τους. (Βλ. θεώρημα 9.5.35.)

(β) Κάθε αβελιανή ομάδα είναι πάντοτε εμφυτεύσιμη εντός κάποιας *διαιρετής*. (Βλ. θεώρημα 9.7.19.)

(γ) Κάθε αβελιανή ομάδα είναι ισόμορφη με το ευθύ άθροισμα δύο ομάδων: Η πρώτη εξ αυτών είναι *διαιρετή* (για να κυριολεκτούμε, *η μέγιστη διαιρετή*) και η δεύτερη *ανηγμένη*. (Βλ. θεώρημα 9.7.40.) Σημειωτέον ότι το διαιρετό μέρος των ομάδων των ανηκουσών στις υποκλάσεις (i) και (ii) είναι τετριμμένο.




Ως εκ τούτου, οι μη τετριμμένες διαιρετές αβελιανές ομάδες ανήκουν στην υποκλάση (iii) των μη πεπερασμένως παραγομένων.




Οι διαιρετές αβελιανές ομάδες είναι πλήρως ταξινομήσιμες μέχρις ισομορφισμού. (Βλ. θεώρημα 9.7.35.) Από την άλλη μεριά, η μελέτη τής οικογενείας των ανηγμένων, μη πεπερασμένως παραγομένων αβελιανών ομάδων είναι απαιτητικότερη, καθώς προϋποθέτει εξοικείωση με τεχνικά μέσα προερχόμενα από την «προκεχωρημένη» Θεωρία Συνόλων, από την Ομολογική Άλγεβρα και από την Τοπολογία. Γι' αυτόν τον λόγο θα περιορισθούμε στην παράθεση μόνον κάποιων ενδεικτικών παραδειγμάτων, παραπέμποντας τους ενδιαφερόμενους αναγνώστες στο δίτομο έργο **[89]**-**[90]** τού László Fuchs για μια *κλασική* εισαγωγή στη Θεωρία Άπειρων Αβελιανών Ομάδων.

*Συμβολισμός*. Επειδή αρκετές σημαντικές αβελιανές ομάδες μπορούν να ταυτισθούν με τις προσθετικές ομάδες ορισμένων *διανυσματικών χώρων* και επειδή, γενικότερα, για την έκφραση ενός στοιχείου *τυχούσας* αβελιανής ομάδας συναρτήσει ενός συστήματος γεννητόρων της είναι προσφορότερη η θεώρηση «ακεραίων γραμμικών συνδυασμών», στο παρόν κεφάλαιο θα χρησιμοποιηθεί *κατά κανόνα* [1] ο *προσθετικός συμβολισμός*. Ο κάτωθι κατάλογος έχει ως στόχο την υπόμνηση των εκάστοτε ακολουθούμενων συμβολιστικών τροποποιήσεων.

| **Πολλαπλασιαστικός συμβολισμός** | **Προσθετικός συμβολισμός** |
|---|---|
| $(G, \cdot)$ | $(G, +)$ |
| $e_G$ | $0_G$ |
| $g^{-1}$ | $-g$ |
| $g_1 g_2$ | $g_1 + g_2$ |
| $g_1 g_2^{-1}$ | $g_1 - g_2$ |
| $\prod_{i=1}^{\kappa} g_i$ | $\sum_{i=1}^{\kappa} g_i$ |
| $g^n (n \in \mathbb{Z})$ | $ng \ (n \in \mathbb{Z})$ |
| $gH$ (και αντ., $Hg$) | $g + H$ (και αντ., $H + g$) |
| $HK$ | $H + K$ |
| $G_1 \times G_2$ | $G_1 \oplus G_2$ |
| $G = H \times_{\text{εσ.}} K$ | $G = H \oplus_{\text{εσ.}} K$ |
| $\prod_{i \in I} G_i$ (και αντ., $\prod_{i \in I}^{\text{περ.}} G_i$) | $\bigoplus_{i \in I} G_i$ (και αντ., $\bigoplus_{i \in I}^{\text{περ.}} G_i$) |
| $G = \prod_{i \in I}^{\text{εσ.}} H_i$ | $G = \bigoplus_{i \in I}^{\text{εσ.}} H_i$ |

[1] Φυσικά, θα εξαιρούνται (όταν παρατίθενται ως παραδείγματα) οι *συγκεκριμένες*, εκ κατασκευής *πολλαπλασιαστικές* αβελιανές ομάδες $(\mathbb{Z}_m^{\times}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q}_{>0}, \cdot)$, $(\mathbb{R}_{>0}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$, $(F^{\times}, \cdot)$ (όπου $(F, +, \cdot)$ σώμα) κ.ά.

# 9.1 ΤΑΞΙΝΟΜΗΣΗ ΠΕΠΕΡΑΣΜΕΝΩΝ ΑΒΕΛΙΑΝΩΝ ΟΜΑΔΩΝ

Η ταξινόμηση των πεπερασμένων αβελιανών ομάδων (μέχρις ισομορφισμού, με τη βοήθεια των λεγομένων *στοιχειωδών διαιρετών*, βλ. θεώρημα 9.1.19) επετεύχθη το 1879 σε μια κοινή εργασία[2] δύο μαθηματικών: τού Γερμανού Ferdinand Georg Frobenius (1849-1917) και τού Ελβετού Ludwig Stickelberger (1850-1936).

**9.1.1 Λήμμα.** *Έστω $p$ ένας πρώτος αριθμός και έστω $(G,+)$ μια πεπερασμένη μη τετριμμένη αβελιανή $p$-ομάδα. Εάν το $a \in G$ είναι ένα στοιχείο τάξεως*

$$\mathrm{ord}(a) = \max\{\,\mathrm{ord}(g) \,|\, g \in G\} \;\; (= \exp(G), \text{βλ. } 2.3.26),$$

*τότε*

$$\boxed{\exists H \in \mathbf{Subg}(G) : H \oplus_{\text{εσ.}} \langle a \rangle = G.}$$

Αποδειξη. Κατά το πόρισμα 5.7.3, $\exists \nu \in \mathbb{N} : |G| = p^{\nu}$. Θα χρησιμοποιήσουμε τη δεύτερη μορφή τής μαθηματικής επαγωγής ως προς τον $\nu$. Για $\nu = 1$ ο ισχυρισμός είναι αληθής, καθότι η $G$ είναι κυκλική (βλ. 4.1.33) και αρκεί να θέσουμε $H := \{0_G\}$. Για $\nu > 1$ υποθέτουμε ότι αυτός είναι αληθής για *κάθε μη τετριμμένη πεπερασμένη αβελιανή ομάδα τάξεως* $p^{\xi}$, όπου $\xi \in \mathbb{N}$, $\xi < \nu$. Η τάξη τού $a$ (λόγω τού θεωρήματος 4.1.22 τού Lagrange) ισούται με $p^{\lambda}$, για κάποιον $\lambda \in \{1, ..., \nu\}$. Επιπροσθέτως, $\mathrm{ord}(x) \le p^{\lambda}$ για κάθε $x \in G$. Εξετάζουμε δύο ενδεχόμενα χωριστά:

*Περίπτωση πρώτη*. Εάν $\lambda = \nu$, τότε $G = \langle a \rangle$, οπότε αρκεί να θέσουμε $H := \{0_G\}$.

*Περίπτωση δεύτερη*. Εάν $\lambda < \nu$, τότε θεωρούμε ένα $b \in G$, τέτοιο ώστε να ισχύει

$$\mathrm{ord}(b) = \min\{\,\mathrm{ord}(g) \,|\, g \in G \smallsetminus \langle a \rangle\}.$$

(Αυτό σημαίνει ότι για κάθε $y \in G$ με $\mathrm{ord}(y) < \mathrm{ord}(b)$ έχουμε $y \in \langle a \rangle$.) Κατ' αρχάς παρατηρούμε ότι

$$\langle a \rangle \cap \langle b \rangle = \{0_G\}. \tag{9.1}$$

Πράγματι· επειδή $\mathrm{ord}(pb) = \frac{\mathrm{ord}(b)}{p} < \mathrm{ord}(b) \Rightarrow pb \in \langle a \rangle$, υπάρχει κάποιος $m \in \mathbb{Z}$, τέτοιος ώστε να ισχύει η ισότητα $pb = ma$. Εξάλλου, επειδή $\mathrm{ord}(a) = p^{\lambda}$ και το $a$ διαθέτει εξ ορισμού τη μέγιστη δυνατή τάξη, έχουμε

$$0_G = p^{\lambda} b = p^{\lambda-1}(pb) = p^{\lambda-1}(ma) \Rightarrow \mathrm{ord}(ma) \le p^{\lambda-1}.$$

Κατά συνέπειαν, το $ma$ δεν παράγει την κυκλική ομάδα $\langle a \rangle$, απ' όπου έπεται ότι $\text{μκδ}(p^{\lambda}, m) > 1$ (λόγω τού πορίσματος 2.3.17) και, κατ' επέκταση, ότι $p \mid m$. Άρα $\exists \mu \in \mathbb{Z} : m = p\mu$ και

$$\left.\begin{array}{r} pb = ma = p\mu a \Rightarrow p(-\mu a + b) = 0_G \\ b \notin \langle a \rangle \Rightarrow -\mu a + b \notin \langle a \rangle \end{array}\right\} \Rightarrow \mathrm{ord}(-\mu a + b) = p.$$

[2] G. Frobenius & L. Stickelberger: *Über Gruppen von vertauschbaren Elementen*, Journal für die reine und angewandte Mathematik **86** (1879), 217-262.

Επειδή το $b$ επελέγη να έχει την ελάχιστη δυνατή τάξη μεταξύ των στοιχείων τού $G\diagdown \langle a\rangle$ , έχουμε κατ' ανάγκην $\mathrm{ord}(-\mu a+b)=p=\mathrm{ord}(b)$. Εξ αυτού έπεται η ισότητα[3] (9.1). Επανερχόμαστε τώρα στην κυρίως απόδειξη θεωρώντας τό στοιχείο $\widetilde{a}:=a+\langle b\rangle$ τής πηλικοομάδας $\widetilde{G}:=G/\langle b\rangle$ . Προφανώς,

$$\mathrm{ord}(\widetilde{a})=\min\{\,j\in\mathbb{N}|\,ja\in\langle b\rangle\}\underset{(9.1)}{\Longrightarrow}\mathrm{ord}(\widetilde{a})=\mathrm{ord}(a)=p^{\lambda}.$$

Κατόπιν εφαρμογής τού (iv) τής προτάσεως 2.4.3 για τον φυσικό επιμορφισμό

$$\pi^{G}_{\langle b\rangle}:G\longrightarrow\widetilde{G},\ a\longmapsto\widetilde{a},$$

συμπεραίνουμε ότι

$$\mathrm{ord}(\widetilde{g})\mid\mathrm{ord}(g),\ \forall g\in G\ (\widetilde{g}:=g+\langle b\rangle\,)\ \Rightarrow\mathrm{ord}(\widetilde{a})=\max\{\,\mathrm{ord}(\widetilde{g})|\,\widetilde{g}\in\widetilde{G}\}.$$

Ως εκ τούτου, έχουμε τη δυνατότητα εφαρμογής τής επαγωγικής υποθέσεως για την πηλικοομάδα $\widetilde{G}$ και το $\widetilde{a}$. Βάσει αυτής, $\exists\widetilde{H}\sqsubseteq\widetilde{G}:\widetilde{H}\oplus_{\text{εσ.}}\langle\widetilde{a}\rangle=\widetilde{G}$. Όμως η $\widetilde{H}$, ούσα υποομάδα τής $\widetilde{G}$, οφείλει να είναι τής μορφής $\widetilde{H}=H/\langle b\rangle$ , όπου $H$ κάποια υποομάδα τής $G$ με $\langle b\rangle\sqsubseteq H$. (Βλ. 4.4.15). Συνεπώς, $|H|=p\left|\widetilde{H}\right|$ και

$$|G|=|\langle b\rangle|\left|\widetilde{G}\right|=p\left|\widetilde{G}\right|=p\left|\widetilde{H}\right||\langle\widetilde{a}\rangle|=|H|\,p^{\lambda}=|H|\,|\langle a\rangle|\Rightarrow G=H+\langle a\rangle\,.$$

Απομένει λοιπόν να αποδειχθεί ότι $H\cap\langle a\rangle=\{0_G\}$. Έστω $x\in H\cap\langle a\rangle$ . Τότε

$$\left.\begin{array}{r}\widetilde{H}\oplus_{\text{εσ.}}\langle\widetilde{a}\rangle=\widetilde{G}\Rightarrow\widetilde{H}\cap\langle\widetilde{a}\rangle=\{0_{\widetilde{G}}\}=\{\langle b\rangle\}\\ x+\langle b\rangle\in\widetilde{H}\oplus_{\text{εσ.}}\langle\widetilde{a}\rangle\end{array}\right\}\Rightarrow\left.\begin{array}{c}x\in\langle b\rangle\,,x\in\langle a\rangle\\ \langle a\rangle\cap\langle b\rangle=\{0_G\}\end{array}\right\}\Rightarrow x=0_G.$$

Άρα τελικώς $H\oplus_{\text{εσ.}}\langle a\rangle=G$. □

**9.1.2 Λήμμα.** *Έστω $p$ ένας πρώτος αριθμός και έστω $(G,+)$ μια πεπερασμένη μη τετριμμένη αβελιανή $p$-ομάδα. Τότε*

$$\boxed{G=\bigoplus_{i=1}^{s}{}^{\text{εσ.}}G_i,}\tag{9.2}$$

*όπου $s\in\mathbb{N}$ και οι $G_1,G_2,...,G_s$ είναι μη τετριμμένες κυκλικές υποομάδες τής $G$ με*

$$\boxed{|G_1|\leq|G_2|\leq\cdots\leq|G_s|\,.}\tag{9.3}$$

ΑΠΟΔΕΙΞΗ. Θα χρησιμοποιήσουμε τη δεύτερη μορφή τής μαθηματικής επαγωγής ως προς την τάξη $|G|$ . Εάν $|G|\in\{2,3\}$, τότε ο ισχυρισμός είναι προδήλως αληθής. Για $|G|>3$ υποθέτουμε ότι αυτός είναι αληθής για *κάθε μη τετριμμένη πεπερασμένη αβελιανή ομάδα τάξεως* $<|G|$ . Μέσω τού λήμματος 9.1.1 διασφαλίζεται η ύπαρξη ενός στοιχείου $a\in G$ μεγίστης τάξεως και μιας υποομάδας $H$ τής $G$, ούτως ώστε να ισχύει $H\oplus_{\text{εσ.}}\langle a\rangle=G$. Εάν το $b$ είναι ένα στοιχείο μεγίστης τάξεως

[3]Επειδή $|\langle a\rangle\cap\langle b\rangle|\mid\mathrm{ord}(b)=|\langle b\rangle|=p$, έχουμε $|\langle a\rangle\cap\langle b\rangle|=1$ (διότι εάν ίσχυε $|\langle a\rangle\cap\langle b\rangle|=p$, τότε θα καταλήγαμε στο ότι $\langle a\rangle\cap\langle b\rangle=\langle b\rangle\Rightarrow\langle b\rangle\sqsubseteq\langle a\rangle$ , ήτοι σε κάτι που θα αντέκειτο στον ορισμό τού $b$).

*εντός τής* $H$, τότε $\mathrm{ord}(b) \leq \mathrm{ord}(a)$. Εάν $H = \{0_G\}$, τότε απλώς θέτουμε $s := 1$, $G_1 := G = \langle a \rangle$ . Εάν η $H$ είναι μη τετριμμένη, τότε κατά την επαγωγική υπόθεση $\exists s \in \mathbb{N}$, $s \geq 2$, καθώς και μη τετριμμένες κυκλικές υποομάδες $G_1$,..., $G_{s-1}$ τής $H$ με

$$H = G_1 \oplus_{\text{εσ.}} \cdots \oplus_{\text{εσ.}} G_{s-1} \;\; \text{και} \;\;\; |G_1| \leq \cdots \leq |G_{s-1}| \,.$$

Θέτοντας $G_s := \langle a \rangle$ λαμβάνουμε τη ζητουμένη έκφραση τής ομάδας $G$ ως εσωτερικού ευθέος αθροίσματος μη τετριμμένων κυκλικών υποομάδων της, καθόσον $|G_{s-1}| \leq |G_s|$ . □

**9.1.3 Συμβολισμός.** Για κάθε αβελιανή ομάδα $(G, +)$ και κάθε $m \in \mathbb{N}$ θέτουμε

$$\boxed{mG := \{mx \,|x \in G\}} \quad \text{και} \quad \boxed{G[m] := \{x \in G \,|mx = 0_G\} \,.}$$

**9.1.4 Πρόταση.** *Τα ανωτέρω* $mG$ *και* $G[m]$ *αποτελούν υποομάδες τής ομάδας* $G$ *και* $G/G[m] \cong mG$.

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς, $m0_G = 0_G$. Επειδή για οιαδήποτε στοιχεία $x_1, x_2 \in G$,

$$mx_1 + m(-x_2) = m\,(x_1 - x_2) \Rightarrow mx_1 + m(-x_2) \in mG$$

και για οιαδήποτε στοιχεία $y_1, y_2 \in G[m]$,

$$m\,(y_1 - y_2) = my_1 - my_2 = 0_G \Rightarrow y_1 - y_2 \in G[m],$$

έχουμε $mG \sqsubseteq G$ και $G[m] \sqsubseteq G$. (Βλ. 2.1.16 (iii)). Επιπροσθέτως, η απεικόνιση $G \ni x \longmapsto mx \in G$ είναι ένας ενδομορφισμός τής $G$ ομάδων έχων ως εικόνα του την $mG$ και ως πυρήνα του την $G[m]$. Άρα $G/G[m] \cong mG$ επί τη βάσει τού θεωρήματος 4.5.2. □

**9.1.5 Σημείωση.** Έστω $(G, +)$ μια αβελιανή ομάδα και έστω $p$ ένας πρώτος αριθμός.

(i) Επί τής $G[p] = \{0_G\} \cup \{x \in G\,|\mathrm{ord}(x) = p\}$ ορίζεται καλώς η απεικόνιση

$$\mathbb{Z}_p \times G[p] \longrightarrow G[p], \;\; ([\ell]_p, x) \longmapsto \ell x, \; \forall \ell \in \mathbb{Z}. \tag{9.4}$$

(Πράγματι· υποθέτοντας ότι $x \in G[p]$ και $\ell_1, \ell_2 \in \mathbb{Z}$ με $[\ell_1]_p = [\ell_2]_p$, έχουμε $p \mid \ell_1 - \ell_2$, οπότε $(\ell_1 - \ell_2)x = 0_G \Rightarrow \ell_1 x = \ell_2 x$. Βλ. 2.3.8.) Η $(G[p], +)$, μαζί με την επιπρόσθετη (εν γένει εξωτερική) πράξη (9.4) («αριθμητικό πολλαπλασιασμό»), καθίσταται διανυσματικός χώρος υπεράνω τού σώματος $\mathbb{Z}_p$. (Είναι άμεσος ο έλεγχος ότι πληρούνται τα αξιώματα τού ορισμού τού διανυσματικού χώρου). Στην *ειδική περίπτωση* όπου $pG = \{0_G\}$, έχουμε $G = G[p]$, οπότε τα προαναφερθέντα ισχύουν *για την ίδια την* $G$.

(ii) Γενικότερα, ακόμη και όταν $pG \neq \{0_G\}$, η

$$\mathbb{Z}_p \times G/pG \longrightarrow G/pG, \; ([\ell]_p, x + pG) \longmapsto [\ell]_p(x + pG) := \ell x + pG, \tag{9.5}$$

($\ell \in \mathbb{Z}$) είναι καλώς ορισμένη απεικόνιση. (Πράγματι· υποθέτοντας ότι $x_1, x_2 \in G$ και $\ell_1, \ell_2 \in \mathbb{Z}$ με $x_1 + pG = x_2 + pG$ και $[\ell_1]_p = [\ell_2]_p$, υπάρχουν $y \in G$ και $r \in \mathbb{Z}$, τέτοια ώστε $x_1 - x_2 = py$ και $\ell_1 - \ell_2 = pr$, οπότε

$$\begin{aligned} \ell_1 x_1 - \ell_2 x_2 &= p\ell_1 y + \ell_1 x_2 - \ell_2 x_2 = p\ell_1 y + (\ell_1 - \ell_2)x_2 \\ &= p\ell_1 y + prx_2 = p(\ell_1 y + rx_2) \in pG, \end{aligned}$$

απ' όπου έπεται ότι $\ell_1 x_1 + pG = \ell_2 x_2 + pG$.) Η $(G/pG, +)$, εφοδιαζόμενη με την επιπρόσθετη πράξη (9.5) («αριθμητικό πολλαπλασιασμό»), καθίσταται $\mathbb{Z}_p$-διανυσματικός χώρος.

**9.1.6 Λήμμα.** *Έστω $(G,+)$ μια αβελιανή ομάδα. Εάν $G \cong G_1 \oplus \cdots \oplus G_s$ (για κάποιες αβελιανές ομάδες $G_1, ..., G_s$, $s \in \mathbb{N}$) και $m \in \mathbb{N}$, τότε $mG \cong mG_1 \oplus \cdots \oplus mG_s$.*

ΑΠΟΔΕΙΞΗ. Έστω $f : G \xrightarrow{\cong} G_1 \oplus \cdots \oplus G_s$ ένας ισομορφισμός. Ορίζουμε ενδομορφισμούς $\vartheta_m^{[G]} \in \mathrm{End}(G)$ και $\vartheta_m^{[i]} \in \mathrm{End}(G_i)$ μέσω των τύπων

$$G \ni x \overset{\vartheta_m^{[G]}}{\longmapsto} mx \in G, \;\; G_i \ni x \overset{\vartheta_m^{[i]}}{\longmapsto} mx \in G_i, \; \forall i \in \{1, ..., s\},$$

(με $\mathrm{Ker}(\vartheta_m^{[G]}) = G[m]$ και $\mathrm{Ker}(\vartheta_m^{[i]}) = G_i[m]$) και παρατηρούμε ότι υφίσταται κανονιστικός ισομορφισμός

$$G/G[m] = G/\mathrm{Ker}(\vartheta_m^{[G]}) \xrightarrow[f^{\pi\eta\lambda.}]{\cong} (G_1 \oplus \cdots \oplus G_s)/f(G[m]). \tag{9.6}$$

(Βλ. 4.5.5 και 4.5.8 (ii).) Η εικόνα $f(x)$ οιουδήποτε στοιχείου $x \in G[m]$ μέσω τού $f$ γράφεται ως $f(x) = x_1 + x_2 + \cdots + x_s$ για κάποια (μονοσημάντως ορισμένα στοιχεία) $x_1 \in G_1,\ x_2 \in G_2, ...,\ x_s \in G_s$. Εξ αυτού έπεται ότι

$$0_G = mx \Rightarrow 0_{\mathrm{Im}(f^{\pi\eta\lambda.})} = f(0_G) = mx_1 + \cdots + mx_s \Rightarrow mx_1 = 0_{G_1}, ..., mx_s = 0_{G_s},$$

ήτοι ότι $x_i \in G_i[m]$ για κάθε $i \in \{1, ..., s\}$. Αυτό σημαίνει ότι η υποομάδα $f(G[m])$ εμπεριέχεται στην $G_1[m] \oplus \cdots \oplus G_s[m]$. Παρομοίως αποδεικνύεται και ο αντίστροφος εγκλεισμός. Άρα $f(G[m])) = G_1[m] \oplus \cdots \oplus G_s[m]$ και

$$\begin{aligned} (G_1 \oplus \cdots \oplus G_s)/f(G[m]) &= (G_1 \oplus \cdots \oplus G_s)/(G_1[m] \oplus \cdots \oplus G_s[m]) \\ &\underset{7.1.57\,\text{(iv)}}{\cong} (G_1/G_1[m]) \oplus \cdots \oplus (G_s/G_s[m]) \end{aligned} \tag{9.7}$$

Επειδή $G_i/G_i[m] \underset{9.1.4}{\cong} mG_i$ για κάθε $i \in \{1, ..., s\}$, οι (9.6) και (9.7) δίδουν

$$mG \underset{9.1.4}{\cong} G/G[m] \underset{7.1.55\,\text{(v)}}{\cong} mG_1 \oplus \cdots \oplus mG_s,$$

οπότε ο ισχυρισμός είναι αληθής. □

**9.1.7 Σημείωση.** Το λήμμα 9.1.2 γενικεύεται άμεσα και για *άπειρα* (απεριόστα ή περιορισμένα) ευθέα αθροίσματα αβελιανών ομάδων: Εάν $G \cong \bigoplus_{i \in I} G_i$ (και αντιστοίχως, $G \cong \bigoplus_{i \in I}^{\pi\varepsilon\rho.} G_i$), τότε $mG \cong \bigoplus_{i \in I} mG_i$ (και αντιστοίχως, $mG \cong \bigoplus_{i \in I}^{\pi\varepsilon\rho.} mG_i$).

**9.1.8 Πρόταση.** *Έστω $p$ ένας πρώτος αριθμός και έστω $(G,+)$ μια πεπερασμένη μη τετριμμένη αβελιανή $p$-ομάδα. Τότε $|G| = p^\nu$, για κάποιον $\nu \in \mathbb{N}$, και ισχύουν τα εξής:*

(i) *$\exists s \in \mathbb{N}$ και[4] $\exists\,(k_1, k_2, ..., k_s) \in \Pi_s(\nu)$, ούτως ώστε να υφίσταται ισομορφισμός*

$$\boxed{G \cong \mathbb{Z}_{p^{k_1}} \oplus \mathbb{Z}_{p^{k_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_s}}.} \tag{9.8}$$

(ii) *Η έκφραση (9.8) είναι μονοσημάντως ορισμένη υπό την εξής έννοια:*
*Εάν $\exists t \in \mathbb{N}$ και εάν $\exists\,(l_1, l_2, ..., l_t) \in \Pi_t(\nu)$, ούτως ώστε να υφίσταται ισομορφισμός*

$$G \cong \mathbb{Z}_{p^{l_1}} \oplus \mathbb{Z}_{p^{l_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{l_t}},$$

*τότε $t = s$ και $l_j = k_j$ για κάθε $j \in \{1, ..., s\}$.*

ΑΠΟΔΕΙΞΗ ΤΟΥ (i). Το λήμμα 9.1.2 μας πληροφορεί ότι η $G$ γράφεται υπό τη μορφή (9.2) υπό τη συνθήκη (9.3). Για κάθε $i \in \{1, ..., s\}$ η $G_i$, ως μη τετριμμένη υποομάδα τής $G$, έχει ως τάξη της έναν θετικό διαιρέτη τού $p^\nu$ που είναι $\geq 2$. (Βλ. 4.1.22.) Άρα $\exists k_i \in \mathbb{N} : k_i \leq \nu$, ούτως ώστε να ισχύει $|G_i| = p^{k_i}$. Επειδή $|G| = \prod_{i=1}^{s} |G_i|$, λαμβάνουμε $k_1 + \cdots + k_s = \nu$ και (λόγω τής (9.3)) $k_1 \leq k_2 \leq \cdots \leq k_s$. Κατά συνέπειαν, $(k_1, k_2, ..., k_s) \in \Pi_s(\nu)$. Τέλος, επειδή η $G_i$ είναι κυκλική ομάδα, έχουμε $G_i \cong \mathbb{Z}_{p^{k_i}}$ (βλ. 2.4.23 (ii)) και

$$G = \bigoplus_{i=1}^{s}{}^{\text{εσ.}} G_i \underset{7.1.85\text{ (ii)}}{\cong} \bigoplus_{i=1}^{s} G_i \underset{7.1.55\text{ (v)}}{\cong} \bigoplus_{i=1}^{s} \mathbb{Z}_{p^{k_i}}.$$

ΠΡΩΤΗ ΑΠΟΔΕΙΞΗ ΤΟΥ (ii). Θέτουμε $H := \mathbb{Z}_{p^{l_1}} \oplus \mathbb{Z}_{p^{l_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{l_t}}$. Θα χρησιμοποιήσουμε τη δεύτερη μορφή τής μαθηματικής επαγωγής ως προς τον $\nu$. Για $\nu = 1$ ο ισχυρισμός είναι αληθής, καθότι η $G$ είναι κυκλική. (Βλ. 4.1.33). Για $\nu > 1$ υποθέτουμε ότι αυτός είναι αληθής για *κάθε μη τετριμμένη πεπερασμένη αβελιανή ομάδα τάξεως* $p^\xi$, όπου $\xi \in \mathbb{N}$, $\xi < \nu$. Εν πρώτοις παρατηρούμε ότι για κάθε $j \in \{1, ..., s\}$ ισχύει

$$\mathbb{Z}_{p^{k_j}} = \left\langle [1]_{p^{k_j}} \right\rangle \Longrightarrow p\mathbb{Z}_{p^{k_j}} := \left\{ pu \,\middle|\, u \in \mathbb{Z}_{p^{k_j}} \right\} = \left\langle [p]_{p^{k_j}} \right\rangle,$$

οπότε η $p\mathbb{Z}_{p^{k_j}}$ είναι μια κυκλική ομάδα τάξεως $\frac{p^{k_j}}{\text{μκδ}(p^{k_j}, p)} = p^{k_j - 1}$, όταν $k_j > 1$ (βλ. 2.3.10 (i)), και τετριμμένη ομάδα όταν $k_j = 1$.

*Περίπτωση πρώτη.* Εάν $G[p] = G$, τότε[5] $k_1 = \cdots = k_s = 1$ και $s = \nu$. Επειδή (εξ υποθέσεως) $G \cong H$, κάθε στοιχείο τής $H$ διαφορετικό τού ουδετέρου οφείλει (σύμφωνα με το (iv) τής προτάσεως 2.4.19) να έχει τάξη $p$, οπότε $H[p] = H$ και $l_1 = \cdots = l_t = 1$, και, ως εκ τούτου, $|G| = p^s = p^t = |H| \Rightarrow s = t$.

[4] Υπενθύμιση συμβολισμού: $\Pi_s(\nu) := \left\{ (k_1, ..., k_s) \in \mathbb{N}^s \,\middle|\, k_1 \leq \cdots \leq k_s, \text{ με } \sum_{j=1}^{s} k_j = \nu \right\}$ (βλ. 5.3.1).

[5] Επειδή η ισότητα $G[p] = G$ σημαίνει ότι κάθε στοιχείο τής $G$ διαφορετικό τού ουδετέρου έχει τάξη $p$, και η τάξη οιουδήποτε στοιχείου τής $\mathbb{Z}_{p^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_s}}$ διαφορετικού τού ουδετέρου ισούται με το ελάχιστο κοινό πολλαπλάσιο των τάξεων των «συντεταγμένων» του (βλ. 7.1.59 (i)), έχουμε κατ' ανάγκην $k_1 = \cdots = k_s = 1$ (λόγω τής προτάσεως B.3.20).

*Περίπτωση δεύτερη.* Εάν η $G[p]$ είναι *γνήσια* υποομάδα τής $G$ (και, κατ' επέκταση, η $H[p]$ *γνήσια* υποομάδα τής $H$), τότε θέτουμε

$$m := \operatorname{card}\left(\{j \in \mathbb{N} \,|\, j \in \{1,...,s\} : k_j = 1\}\right), \; n := \operatorname{card}\left(\{j \in \mathbb{N} \,|\, j \in \{1,...,t\} : l_j = 1\}\right),$$

όπου $m \in \{0, 1, ..., s-1\}$ και $n \in \{0, 1, ..., t-1\}$. Επειδή $k_1 \leq \cdots \leq k_s$, έχουμε

$$\begin{aligned} pG &\underset{9.1.6}{\cong} (p\mathbb{Z}_{p^{k_1}}) \oplus (p\mathbb{Z}_{p^{k_2}}) \oplus \cdots \oplus (p\mathbb{Z}_{p^{k_s}}) \\ &\cong (p\mathbb{Z}_{p^{k_{m+1}}}) \oplus (p\mathbb{Z}_{p^{k_{m+2}}}) \oplus \cdots \oplus (p\mathbb{Z}_{p^{k_s}}) \cong \mathbb{Z}_{p^{k_{m+1}-1}} \oplus \mathbb{Z}_{p^{k_{m+2}-1}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_s-1}}, \end{aligned}$$

όπου κανείς εκ των ευθέων προσθετέων των δύο τελευταίων εκφράσεων δεν είναι τετριμμένος. Κατ' αναλογίαν, επειδή $l_1 \leq \cdots \leq l_t$,

$$pH \cong \mathbb{Z}_{p^{l_{n+1}-1}} \oplus \mathbb{Z}_{p^{l_{n+2}-1}} \oplus \cdots \oplus \mathbb{Z}_{p^{l_t-1}}.$$

Εξ υποθέσεως, υφίσταται ισομορφισμός $f : G \xrightarrow{\cong} H$. Προφανώς,

$$f(pG) = pf(G) = pH \Rightarrow pG \cong pH \Rightarrow |pG| = |pH|.$$

Επειδή $|pG| = p^{(k_{m+1}-1)+\cdots+(k_s-1)} = p^{(l_{n+1}-1)+\cdots+(l_t-1)} = |pH| < |G| = p^{\nu}$, έχουμε τη δυνατότητα εφαρμογής τής επαγωγικής υποθέσεως για τη μη τετριμμένη αβελιανή $p$-ομάδα $pG$. Αυτή δίδει

$$s - m = t - n, \; k_{m+1} = l_{n+1}, \; k_{m+2} = l_{n+2}, ..., \; k_s = l_t.$$

Από την άλλη μεριά, $|G| = p^{k_1+k_2+\cdots+k_s} = p^{l_1+l_2+\cdots+l_t} = |H|$, κι επειδή (εξ υποθέσεως) $k_1 = \cdots = k_m = 1 = l_1 = \cdots = l_n$, λαμβάνουμε

$$m + (k_{m+1} + \cdots + k_s) = n + (l_{n+1} + \cdots + l_t) \Rightarrow m = n,$$

οπότε $s = t$. Ως εκ τούτου, ο ισχυρισμός είναι αληθής *για κάθε* $\nu \geq 1$.

ΔΕΥΤΕΡΗ ΑΠΟΔΕΙΞΗ ΤΟΥ (ii). Εξ υποθέσεως, υπάρχουν ισομορφισμοί

$$f_1 : \mathbb{Z}_{p^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_s}} \xrightarrow{\cong} G \;\text{ και }\; f_2 : \mathbb{Z}_{p^{l_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{l_t}} \xrightarrow{\cong} G,$$

οπότε $G = f_1(\mathbb{Z}_{p^{k_1}}) \oplus \cdots \oplus f_1(\mathbb{Z}_{p^{k_s}}) = f_2(\mathbb{Z}_{p^{l_1}}) \oplus \cdots \oplus f_2(\mathbb{Z}_{p^{l_t}})$ και οι ομάδες $f_1(\mathbb{Z}_{p^{k_i}}) \cong \mathbb{Z}_{p^{k_i}}$ και $f_2(\mathbb{Z}_{p^{l_j}}) \cong \mathbb{Z}_{p^{l_j}}$ είναι *αναποσυνθέσιμες* υποομάδες τής $G$ (δυνάμει τής προτάσεως 7.1.34) για κάθε $i \in \{1, ..., s\}$ και για κάθε $j \in \{1,..., t\}$ Σύμφωνα με το θεώρημα 7.2.25 των Krull, Remak και Schmidt, $s = t$ και υπάρχει μετάταξη $\sigma \in \mathfrak{S}_s$, καθώς και αυτομορφισμός $\vartheta$ τής $G$ με $\vartheta(f_2(\mathbb{Z}_{p^{l_{\sigma(j)}}})) = f_1(\mathbb{Z}_{p^{k_j}})$ για κάθε $j \in \{1, ..., s\}$. Επομένως,

$$\begin{aligned} p^{l_{\sigma(j)}} &= \left|\mathbb{Z}_{p^{l_{\sigma(j)}}}\right| = \left|f_2(\mathbb{Z}_{p^{l_{\sigma(j)}}})\right| = \left|\vartheta(f_2(\mathbb{Z}_{p^{l_{\sigma(j)}}}))\right| \\ &= \left|f_1(\mathbb{Z}_{p^{k_j}})\right| = \left|\mathbb{Z}_{p^{k_j}}\right| = p^{k_j} \Rightarrow l_{\sigma(j)} = k_j, \; \forall j \in \{1, ..., s\}. \end{aligned}$$

Εν συνεχεία, λαμβάνουμε υπ' όψιν ότι $k_1 \leq k_2 \leq \cdots \leq k_s$ και $l_1 \leq l_2 \leq \cdots \leq l_s$.

*Περίπτωση πρώτη.* Εάν $k_1 = k_2 = \cdots = k_s$, τότε $l_1 = l_2 = \cdots = l_s$ και ο ισχυρισμός είναι προδήλως αληθής.

*Περίπτωση δεύτερη.* Εάν $s \geq 2$ και υπάρχουν $j, j' \in \{1, ..., s\}$ με $j < j'$ και $k_j < k_{j'}$, τότε $l_{\sigma(j)} < l_{\sigma(j')}$, οπότε (κατ' ανάγκην[6]) $l_j = k_j$ *για κάθε* $j \in \{1, ..., s\}$. □

**9.1.9 Ορισμός.** Κάθε αβελιανή ομάδα $(G, +)$ τάξεως $p^\nu$, όπου $p$ κάποιος πρώτος αριθμός και $\nu \in \mathbb{N}$, αποσυντιθέμενη ως ευθύ άθροισμα (9.8) κυκλικών ομάδων, ονομάζεται **αβελιανή $p$-ομάδα τύπου**[7] $(k_1, k_2, ..., k_s)$. Οι μονοσημάντως ορισμένοι (υπό την έννοια τού 9.1.8 (ii)) ευθείς προσθετέοι $\mathbb{Z}_{p^{k_1}}, \mathbb{Z}_{p^{k_2}}, ..., \mathbb{Z}_{p^{k_s}}$ τής εκφράσεως (9.8) καλούνται **στοιχειώδεις κυκλικοί προσθετέοι τής** $G$, οι δε τάξεις αυτών $p^{k_1}, p^{k_2}, ..., p^{k_s}$ **στοιχειώδεις διαιρέτες τής** $G$.

**9.1.10 Σημείωση.** Έστω $(G, +)$ είναι μια αβελιανή ομάδα τάξεως $p^\nu$, όπου $p$ κάποιος πρώτος αριθμός και $\nu \in \mathbb{N}$.

(i) Εάν η $G$ είναι τού τύπου $(\underbrace{k, k, ..., k}_{s \text{ φορές}})$, όπου $k = \frac{\nu}{s}$, τότε

$$\boxed{s = \dim_{\mathbb{Z}_p}(p^j G / p^{j+1} G), \ \forall j \in \{0, 1, ...., k-1\},}$$

δηλαδή το πλήθος των στοιχειωδών κυκλικών προσθετέων στην (9.8) ισούται με τη διάσταση τού $\mathbb{Z}_p$-διανυσματικού χώρου $p^j G / p(p^j G)$. (Βλ. 9.1.5 (ii).) Πράγματι· εν τοιαύτη περιπτώσει,

$$p^j G \cong \underbrace{p^j \mathbb{Z}_{p^k} \oplus p^j \mathbb{Z}_{p^k} \oplus \cdots \oplus p^j \mathbb{Z}_{p^k}}_{s \text{ φορές}},$$

$$p^{j+1} G \cong \underbrace{p^{j+1} \mathbb{Z}_{p^k} \oplus p^{j+1} \mathbb{Z}_{p^k} \oplus \cdots \oplus p^{j+1} \mathbb{Z}_{p^k}}_{s \text{ φορές}},$$

(βλ. 9.1.6), οπότε $p^j G / p^{j+1} G \underset{7.1.57\,(\text{iv})}{\cong} \underbrace{(p^j \mathbb{Z}_{p^k})/(p^{j+1} \mathbb{Z}_{p^k}) \oplus \cdots \oplus (p^j \mathbb{Z}_{p^k})/(p^{j+1} \mathbb{Z}_{p^k})}_{s \text{ φορές}}$.

Επειδή $p^j \mathbb{Z}_{p^k} = \left\langle [p^j]_{p^k} \right\rangle$ με $\left| p^j \mathbb{Z}_{p^k} \right| = \frac{p^k}{\text{μκδ}(p^k, p^j)} = p^{k-j}$ (βλ. 2.3.10 (i)), έχουμε $p^j \mathbb{Z}_{p^k} \cong \mathbb{Z}_{p^{k-j}}$ και, κατ' αναλογίαν, $p^{j+1} \mathbb{Z}_{p^k} \cong \mathbb{Z}_{p^{k-(j+1)}}$. Εξάλλου,

$$\frac{\left| \mathbb{Z}_{p^{k-j}} \right|}{\left| \mathbb{Z}_{p^{k-(j+1)}} \right|} = \frac{p^{k-j}}{p^{k-(j+1)}} = p \underset{4.1.33}{\Longrightarrow} (p^j \mathbb{Z}_{p^k})/(p^{j+1} \mathbb{Z}_{p^k}) \cong \mathbb{Z}_p,$$

οπότε $p^j G / p^{j+1} G \cong \underbrace{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{s \text{ φορές}}$.

(ii) Εάν η $G$ είναι τού τύπου $(k_1, k_2, ..., k_s)$, $s \geq 2$, και εάν τουλάχιστον δύο εκ

[6] Προφανώς, $\sigma(\{ j \in \{1, ..., s\} | \, k_j = \lambda \}) = \{ j \in \{1, ..., s\} | \, l_j = \lambda \}$ για κάθε (δυνατό) $\lambda \in \{1, ..., s\}$.

[7] Κάθε αβελιανή $p$-ομάδα τύπου $(1, 1, ..., 1)$ καλείται, ιδιαιτέρως, **στοιχειώδης αβελιανή $p$-ομάδα**.

των $k_1,\ldots,k_s$ είναι διαφορετικοί, τότε θεωρούμε εκείνο το (μονοσημάντως καθοριζόμενο) υποσύνολο δεικτών $\{\varrho_1,\ldots,\varrho_\xi\} \subseteq \{1,\ldots,s\}$ (με $\xi \geq 2$ και $\varrho_1 \geq 1$, $\varrho_\xi = s$) για το οποίο ισχύει

$$k_1 = \cdots = k_{\varrho_1} < k_{\varrho_1+1} = \cdots = k_{\varrho_2} < \cdots\cdots < k_{\varrho_{\xi-1}+1} = \cdots = k_{\varrho_\xi} = k_s,$$

και ορίζουμε τους $\varrho_0 := 0$ και $s_i := \varrho_i - \varrho_{i-1}$, $\forall i \in \{1,\ldots,\xi\}$, με $\sum_{i=1}^{\xi} s_i = s$. Θέτοντας $L_i := \underbrace{\mathbb{Z}_{p^{k_{\varrho_i}}} \oplus \mathbb{Z}_{p^{k_{\varrho_i}}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_{\varrho_i}}}}_{s_i \text{ φορές}}$, γνωρίζουμε (από το (i)) ότι ισχύει η ισότητα $s_i = \dim_{\mathbb{Z}_p}(p^{k_{\varrho_i}-1}L_i/p^{k_{\varrho_i}}L_i)$, $\forall i \in \{1,\ldots,\xi\}$. Επειδή

$$\begin{aligned}
&G \cong L_1 \oplus L_2 \oplus \cdots \oplus L_\xi \\
&\underset{9.1.6}{\Longrightarrow} p^{k_{\varrho_i}-1}G \cong p^{k_{\varrho_i}-1}L_1 \oplus p^{k_{\varrho_i}-1}L_2 \oplus \cdots \oplus p^{k_{\varrho_i}-1}L_\xi \\
&\cong p^{k_{\varrho_i}-1}L_i \oplus p^{k_{\varrho_i}-1}L_{i+1} \oplus \cdots \oplus p^{k_{\varrho_i}-1}L_\xi,
\end{aligned}$$

(αφού η $p^jL_i$ είναι τετριμμένη για $j \geq k_{\varrho_i}$) και, κατ' αναλογίαν,

$$p^{k_{\varrho_i}}G \cong p^{k_{\varrho_i}}L_{i+1} \oplus p^{k_{\varrho_i}}L_{i+2} \oplus \cdots \oplus p^{k_{\varrho_i}}L_\xi,$$

έχουμε[8] $p^{k_{\varrho_i}-1}G/p^{k_{\varrho_i}}G \cong \bigoplus_{\lambda=i}^{\xi}\left(p^{k_{\varrho_\lambda}-1}L_\lambda/p^{k_{\varrho_\lambda}}L_\lambda\right)$, απ' όπου έπεται ότι

$$\dim_{\mathbb{Z}_p}(p^{k_{\varrho_i}-1}G/p^{k_{\varrho_i}}G) = \sum_{\lambda=i}^{\xi} \dim_{\mathbb{Z}_p}(p^{k_{\varrho_\lambda}-1}L_\lambda/p^{k_{\varrho_\lambda}}L_\lambda) = \sum_{\lambda=i}^{\xi} s_\lambda \tag{9.9}$$

για $i \leq \xi$ και

$$\dim_{\mathbb{Z}_p}(p^{k_{\varrho_{i+1}}-1}G/p^{k_{\varrho_{i+1}}}G) = \sum_{\lambda=i+1}^{\xi} \dim_{\mathbb{Z}_p}(p^{k_{\varrho_\lambda}-1}L_\lambda/p^{k_{\varrho_\lambda}}L_\lambda) = \sum_{\lambda=i+1}^{\xi} s_\lambda \tag{9.10}$$

για $i \leq \xi - 1$ (με $k_{\varrho_{i+1}} = k_{\varrho_i+1}$). Αφαιρώντας για κάθε $i \in \{1,\ldots,\xi-1\}$ κατά μέλη την (9.10) από την (9.9) λαμβάνουμε

$$\boxed{s_i = \dim_{\mathbb{Z}_p}(p^{k_{\varrho_i}-1}G/p^{k_{\varrho_i}}G) - \dim_{\mathbb{Z}_p}(p^{k_{\varrho_i+1}-1}G/p^{k_{\varrho_i+1}}G),}$$

ενώ για $i = \xi$, $s_\xi = \dim_{\mathbb{Z}_p}(p^{k_s-1}G/p^{k_s}G)$.

**9.1.11 Πόρισμα.** *Έστω $p$ κάποιος πρώτος αριθμός και έστω $\nu \in \mathbb{N}$. Για δυο αβελιανές ομάδες $G_1, G_2$ τάξεως $p^\nu$ οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) $G_1 \cong G_2$.

(ii) *Οι $G_1, G_2$ διαθέτουν τους ίδιους στοιχειώδεις διαιρέτες.*

(iii) $d_p^{[j]}(G_1) = d_p^{[j]}(G_2)$ *για κάθε $j \in \mathbb{N}_0$, όπου*[9]

$$d_p^{[j]}(G_i) := \dim_{\mathbb{Z}_p}(p^jG_i/p^{j+1}G_i) - \dim_{\mathbb{Z}_p}(p^{j+1}G_i/p^{j+2}G_i), \quad i \in \{1,2\}.$$

[8] Η $p^{k_{\varrho_i}}L_i$ (για $\lambda = i$) είναι τετριμμένη.

[9] Η διαφορά $d_p^{[j]}(G_i) \in \mathbb{N}_0$ ισούται με το πλήθος των κυκλικών ομάδων τάξεως $p^{j+1}$ των εμφανιζομένων ως ευθείς προσθετέοι στην (9.8) για την $G_i$.

ΑΠΟΔΕΙΞΗ. Η αμφίπλευρη συνεπαγωγή (i)⇔(ii) έπεται άμεσα από την πρόταση 9.1.8.

(i)⇒(iii) Εξ υποθέσεως, υφίσταται ισομορφισμός $f : G_1 \xrightarrow{\cong} G_2$. Επειδή ισχύει $f(p^j G_1) = p^j G_2$, η απεικόνιση

$$p^j G_1/p^{j+1}G_1 \ni p^j x + p^{j+1}G_1 \longmapsto p^j f(x) + p^{j+1}G_2 \in p^j G_2/p^{j+1}G_2$$

αποτελεί τόσον ισομορφισμό ομάδων όσον και ισομορφισμό $\mathbb{Z}_p$-διανυσματικών χώρων, οπότε $d_p^{[j]}(G_1) = d_p^{[j]}(G_2)$ για κάθε $j \in \mathbb{N}_0$.

(iii)⇒(i) Εάν $d_p^{[j]}(G_1) = d_p^{[j]}(G_2)$, $\forall j \in \mathbb{N}_0$, τότε (σύμφωνα με τα προαναφεθέντα στη σημείωση 9.1.10) οι πληθικοί αριθμοί των κυκλικών ομάδων ίδιας τάξεως, οι οποίες εμφανίζονται ως ευθείς προσθετέοι στην (9.8) για την $G_1$ είναι ίσοι με τους αντίστοιχους για την $G_2$. Ως εκ τούτου, είναι πρόδηλος ο τρόπος κατασκευής ενός ισομορφισμού $f : G_1 \xrightarrow{\cong} G_2$. □

**9.1.12 Πόρισμα.** *Εάν $p$ είναι κάποιος πρώτος αριθμός και $\nu \in \mathbb{N}$, τότε το πλήθος των ανά ζεύγη μη ισομόρφων πεπερασμένων αβελιανών ομάδων τάξεως $p^\nu$ ισούται με τον πληθικό αριθμό $\varpi(\nu)$ των διαμερίσεων τού $\nu$* (βλ. 5.3.1).

**9.1.13 Παραδείγματα.** Έστω $p$ ένας πρώτος αριθμός. Οι ανά ζεύγη μη ισόμορφες $p$-αβελιανές ομάδες οι έχουσες τάξη $p^2$ είναι οι

| Τύποι | Αβελιανές ομάδες |
|---|---|
| $(1,1)$ | $\mathbb{Z}_p \oplus \mathbb{Z}_p$ |
| $(2)$ | $\mathbb{Z}_{p^2}$ |

οι έχουσες τάξη $p^3$ είναι οι

| Τύποι | Αβελιανές ομάδες |
|---|---|
| $(1,1,1)$ | $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$ |
| $(1,2)$ | $\mathbb{Z}_p \oplus \mathbb{Z}_{p^2}$ |
| $(3)$ | $\mathbb{Z}_{p^3}$ |

και οι έχουσες τάξη $p^4$ είναι οι

| Τύποι | Αβελιανές ομάδες |
|---|---|
| $(1,1,1,1)$ | $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$ |
| $(1,1,2)$ | $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_{p^2}$ |
| $(1,3)$ | $\mathbb{Z}_p \oplus \mathbb{Z}_{p^3}$ |
| $(2,2)$ | $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$ |
| $(4)$ | $\mathbb{Z}_{p^4}$ |

**9.1.14 Παραδείγματα.** Έστω $p$ ένας πρώτος αριθμός. Το πλήθος $\varpi(\nu)$ των ανά ζεύγη μη ισομόρφων $p$-αβελιανών ομάδων τάξεως $p^\nu$, όπου $\nu \in \{5, ..., 16\}$, δίδεται στους εξής καταλόγους:

| $\nu$ | $\varpi(\nu)$ |
|---|---|
| 5 | 7 |
| 6 | 11 |
| 7 | 15 |
| 8 | 22 |
| 9 | 30 |
| 10 | 42 |

| $\nu$ | $\varpi(\nu)$ |
|---|---|
| 11 | 56 |
| 12 | 77 |
| 13 | 101 |
| 14 | 135 |
| 15 | 176 |
| 16 | 231 |

**9.1.15 Πόρισμα.** *Έστω $(F, +, \cdot)$ τυχόν πεπερασμένο σώμα. Ως γνωστόν* (βλ. 5.7.6), *ισχύει* $\mathrm{card}(F) = p^\nu$ *για κάποιον πρώτο αριθμό $p$ και για κάποιον $\nu \in \mathbb{N}$. Επιπλέον, η προσθετική ομάδα $(F, +)$ τού $F$ είναι μια στοιχειώδης αβελιανή $p$-ομάδα, καθώς είναι ισόμορφη τής* $\underbrace{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{\nu \text{ φορές}}$.

ΑΠΟΔΕΙΞΗ. Η $(F, +)$ είναι μια αβελιανή $p$-ομάδα. Επομένως υπάρχουν $s \in \mathbb{N}$ και $(k_1, k_2, ..., k_s) \in \Pi_s(\nu)$, ούτως ώστε να υφίσταται ισομορφισμός

$$F \xrightarrow{\cong} \mathbb{Z}_{p^{k_1}} \oplus \mathbb{Z}_{p^{k_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_s}}. \tag{9.11}$$

Επειδή το σώμα $(F, +, \cdot)$ έχει χαρακτηριστική $p$ (βλ. C.2.16 (iv)), ισχύει

$$px = (p \cdot 1_F) \cdot x = 0_F \cdot x = 0_F, \ \forall x \in F,$$

οπότε κάθε στοιχείο $x \in F \smallsetminus \{0_F\}$ έχει τάξη $p$ εντός τής $(F, +)$ και απεικονίζεται μέσω τού ισομορφισμού (9.11) σε *ακριβώς ένα* στοιχείο

$$([a_1]_{p^{k_1}}, ..., [a_s]_{p^{k_s}}) \in \mathbb{Z}_{p^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_s}} \smallsetminus ([0]_{p^{k_1}}, ..., [0]_{p^{k_s}})$$

τάξεως $p$. (Βλ. 2.4.19 (iv).) Εάν υποθέσουμε ότι $\exists i_0 \in \{1, ..., s\} : k_{i_0} \geq 2$, τότε καταλήγουμε σε άτοπο, διότι εν τοιαύτη περιπτώσει το

$$y := \begin{cases} ([1]_{p^{k_1}}, [0]_{p^{k_2}}, ..., [0]_{p^{k_s}}), & \text{όταν } \ i_0 = 1, \\ ([0]_{p^{k_1}}, ..., [0]_{p^{k_{i_0 - 1}}}, [1]_{p^{k_{i_0}}}, [0]_{p^{k_{i_0+1}}}, ..., [0]_{p^{k_s}}), & \text{όταν } \ 2 \leq i_0 \leq s - 1, \\ ([0]_{p^{k_1}}, ..., [0]_{p^{k_{s-1}}}, [1]_{p^{k_s}}), & \text{όταν } \ i_0 = s, \end{cases}$$

θα έπρεπε να αποτελεί την εικόνα (ακριβώς) ενός $x \in F \smallsetminus \{0_F\}$ μέσω τού (9.11), πράγμα αδύνατο, καθόσον $p\,[1]_{p^{k_{i_0}}} = [p]_{p^{k_{i_0}}} \neq [0]_{p^{k_{i_0}}} \Rightarrow py \neq ([0]_{p^{k_1}}, ..., [0]_{p^{k_s}})$. Επομένως, $k_1 = \cdots = k_s = 1$ και $s = \nu$. □

**9.1.16 Λήμμα.** *Έστω $(G, +)$ μια αβελιανή ομάδα τάξεως $p^\nu m$, όπου $\nu, m \in \mathbb{N}$ και $p$ ένας πρώτος αριθμός με $p \nmid m$. Εάν*

$$H := \left\{ g \in G | \ \exists j \in \{0, 1, ..., \nu\} : \mathrm{ord}(g) = p^j \right\}, \ K := \{ g \in G | \ \mathrm{ord}(g) \mid m \},$$

*τότε ισχύουν τα ακόλουθα:*

(i) $H \sqsubseteq G$ *και* $K \sqsubseteq G$.

(ii) $G = H \oplus_{\text{εσ.}} K$.

(iii) $|H| = p^\nu$ *και* $|K| = m$.

ΑΠΟΔΕΙΞΗ. (i) Προφανώς, $0_G \in H$ και για οιαδήποτε $x, y \in H$ έχουμε

$$p^\nu(x-y) = p^\nu x - p^\nu y = 0_G \Rightarrow x - y \in H,$$

οπότε $H \sqsubseteq G$. (Βλ. 2.1.16 (iii)). Παρομοίως αποδεικνύουμε ότι $K \sqsubseteq G$.
(ii) Εν πρώτοις ισχύει η ισότητα $H + K = G$. Πράγματι· επειδή (κατά το πόρισμα B.2.8) από την ισότητα μκδ$(p^\nu, m) = 1$ συνάγεται ότι

$$\exists u, v \in \mathbb{Z} : up^\nu + vm = 1 \Rightarrow g = (up^\nu + vm)g = (up^\nu)g + (vm)g, \ \forall g \in G,$$

για κάθε στοιχείο $g \in G$ έχουμε

$$\left. \begin{array}{r} |G| = p^\nu m \Rightarrow p^\nu(vm)g = 0_G \Rightarrow (vm)g \in H \\ m(up^\nu)g = 0_G \Rightarrow (up^\nu)g \in K \end{array} \right\} \Rightarrow g \in H + K.$$

Εν συνεχεία, θεωρούμε τυχόν $x \in H \cap K$. Προφανώς, $\mathrm{ord}(x) \mid p^\nu$ και $\mathrm{ord}(x) \mid m$, και το πόρισμα B.2.6 δίδει $\mathrm{ord}(x) \mid$ μκδ$(p^\nu, m) = 1 \Rightarrow \mathrm{ord}(x) = 1 \Rightarrow x = 0_G$. Άρα $G = H \oplus_{\text{εσ.}} K$.
(iii) Επειδή η $K$ είναι αβελιανή, εάν ο $p$ διαιρούσε την τάξη της $|K|$, τότε, σύμφωνα με το θεώρημα 4.4.21, θα υπήρχε κάποιο στοιχείο τής $K$ τάξεως $p$, πράγμα αδύνατο, καθόσον μκδ$(p^\nu, m) = 1$. Εκ παραλλήλου, η τάξη $|H|$ τής $H$ είναι αδύνατο να έχει κάποιον πρώτο διαιρέτη διάφορο τού $p$. Επειδή λοιπόν $|G| = |H|\,|K|$, έχουμε κατ' ανάγκην $|H| = p^\nu$ και $|K| = m$. □

**9.1.17 Πρόταση.** *Έστω $(G, +)$ μια μη τετριμμένη πεπερασμένη αβελιανή ομάδα. Εάν $|G| = p_1^{\nu_1} p_2^{\nu_2} \cdots p_\kappa^{\nu_\kappa}$ ($\kappa \in \mathbb{N}$, $\nu_1, \ldots, \nu_\kappa \in \mathbb{N}$) είναι η κανονική παράσταση* (B.19) *τής τάξεώς της ως γινομένου (κατάλληλων δυνάμεων) πρώτων αριθμών $p_1, \ldots, p_\kappa$ με $p_1 < \cdots < p_\kappa$ και*

$$G(p_\varrho) := \{ g \in G | \exists j \in \{0, 1, \ldots, \nu_i\} : \mathrm{ord}(g) = p_\varrho^j \} \tag{9.12}$$

*για κάθε $\varrho \in \{1, \ldots, \kappa\}$, τότε*

$$\boxed{G = G(p_1) \oplus_{\text{εσ.}} G(p_2) \oplus_{\text{εσ.}} \cdots \oplus_{\text{εσ.}} G(p_\kappa),} \tag{9.13}$$

*και $|G(p_\varrho)| = p_\varrho^{\nu_\varrho}$, $\forall \varrho \in \{1, \ldots, \kappa\}$.*

ΑΠΟΔΕΙΞΗ. Έπεται ύστερα από διαδοχική εφαρμογή τού λήμματος 9.1.16 ($\kappa - 1$ φορές). □

**9.1.18 Ορισμός.** Η παράσταση (9.13) καλείται **πρωτεύουσα αποσύνθεση τής** $G$ και οι ομάδες $G(p_\varrho)$, $\varrho \in \{1, \ldots, \kappa\}$, καλούνται **πρωτεύουσες συνιστώσες τής** $G$.

**9.1.19 Θεώρημα. (1ο θεμελιώδες θεώρημα περί πεπερασμένων αβελιανών ομάδων.)** *Έστω $(G, +)$ μια μη τετριμμένη πεπερασμένη αβελιανή ομάδα. Εάν*

$$|G| = p_1^{\nu_1} \cdots p_\kappa^{\nu_\kappa}, \ (\kappa \in \mathbb{N}, \ \nu_1, \ldots, \nu_\kappa \in \mathbb{N})$$

*είναι η κανονική παράσταση* (B.19) *τής τάξεώς της ως γινομένου (κατάλληλων δυνάμεων) πρώτων αριθμών $p_1,\ldots,p_\kappa$ με $p_1 < \cdots < p_\kappa$, τότε*

$$\exists s_\varrho \in \{1,\ldots,\nu_\varrho\} \text{ και } \exists (k_1^{(\varrho)}, k_2^{(\varrho)},\ldots, k_{s_\varrho}^{(\varrho)}) \in \Pi_{s_\varrho}(\nu_\varrho)$$

*για κάθε $\varrho \in \{1,\ldots,\kappa\}$, ούτως ώστε να υφίστανται ισομορφισμοί*

$$\boxed{G \cong \bigoplus_{\varrho=1}^{\kappa} G(p_\varrho) \cong \left(\bigoplus_{j_1=1}^{s_1} \mathbb{Z}_{p_1^{k_{j_1}^{(1)}}}\right) \oplus \left(\bigoplus_{j_2=1}^{s_2} \mathbb{Z}_{p_2^{k_{j_2}^{(2)}}}\right) \oplus \cdots \oplus \left(\bigoplus_{j_\kappa=1}^{s_\kappa} \mathbb{Z}_{p_\kappa^{k_{j_\kappa}^{(\kappa)}}}\right).}$$

*Επιπροσθέτως, οι εκφράσεις αυτές είναι μονοσημάντως ορισμένες.*

ΑΠΟΔΕΙΞΗ. Ο πρώτος ισομορφισμός έπεται άμεσα από την πρόταση 9.1.8 και το (ii) τού θεωρήματος 7.1.85, και ο δεύτερος από την πρόταση 9.1.17 και το (v) τής προτάσεως 7.1.55. □

**9.1.20 Ορισμός.** Εάν $(G,+)$ είναι μια μη τετριμμένη πεπερασμένη αβελιανή ομάδα, τότε (γενικεύοντας τον ορισμό 9.1.9) καλούμε τους

$$p_1^{k_1^{(1)}},\ldots,p_1^{k_{s_1}^{(1)}}, p_2^{k_1^{(2)}},\ldots,p_2^{k_{s_2}^{(2)}},\ldots\ldots, p_\kappa^{k_1^{(\kappa)}},\ldots,p_\kappa^{k_{s_\kappa}^{(\kappa)}} \tag{9.14}$$

(τους εμφανιζόμενους στο θεώρημα 9.1.19) **στοιχειώδεις διαιρέτες τής** $G$.

**9.1.21 Πόρισμα.** *Δυο πεπερασμένες μη τετριμμένες αβελιανές ομάδες ίσων τάξεων είναι ισόμορφες εάν και μόνον εάν διαθέτουν τους ίδιους στοιχειώδεις διαιρέτες.*

**9.1.22 Πόρισμα.** *Το πλήθος των ανά ζεύγη μη ισομόρφων πεπερασμένων αβελιανών ομάδων τάξεως $p_1^{\nu_1} \cdots p_\kappa^{\nu_\kappa}$ ($\kappa \in \mathbb{N}$, $\nu_1,\ldots,\nu_\kappa \in \mathbb{N}$), όπου οι $p_1,\ldots,p_\kappa$ είναι σαφώς διακεκριμένοι πρώτοι αριθμοί, ισούται με*

$$\prod_{\varrho=1}^{\kappa} \varpi(\nu_\varrho),$$

*ήτοι με το γινόμενο των πληθικών αριθμών των συνόλων των διαμερίσεων των $\nu_1,\ldots,\nu_\kappa$* (βλ. 5.3.1).

**9.1.23 Παράδειγμα.** Το πλήθος των ανά ζεύγη μη ισομόρφων πεπερασμένων αβελιανών ομάδων τάξεως $3528 = 2^3 \cdot 3^2 \cdot 7^2$ ισούται με $\varpi(3)\varpi(2)^2 = 3 \cdot 2^2 = 12$. Από τον κατάλογο

| $p_\varrho^{\nu_\varrho}$, $\varrho \in \{1,2,3\}$ | Τύποι | Αβελιανές $p_\varrho$-ομάδες |
|---|---|---|
| $2^3$ | $(1,1,1),(1,2),(3)$ | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_4, \mathbb{Z}_8$ |
| $3^2$ | $(1,1),(2)$ | $\mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_9$ |
| $7^2$ | $(1,1),(2)$ | $\mathbb{Z}_7 \oplus \mathbb{Z}_7$, $\mathbb{Z}_{49}$ |

συνάγεται ότι αυτές οι 12 ομάδες είναι οι εξής:

| Αβελιανές ομάδες τάξεως 3528 | |
|---|---|
| $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7,$ | $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49}$ |
| $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7,$ | $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{49}$ |
| $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49},$ | $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$ |
| $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{49},$ | $\mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$ |
| $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7,$ | $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49}$ |
| $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7,$ | $\mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{49}$ |

**9.1.24 Θεώρημα. (Εμφύτευση εντός τής $\mathbb{Z}_m^{\times}$.)** *Για κάθε πεπερασμένη αβελιανή ομάδα $(G,+)$ υπάρχει $m \in \mathbb{N}$, ούτως ώστε αυτή να είναι εμφυτεύσιμη εντός τής ομάδας $\mathbb{Z}_m^{\times}$.*

Αποδειξη. Έστω $(G,+)$ τυχούσα πεπερασμένη αβελιανή ομάδα τάξεως $d$. Εάν $d=1$, ο ισχυρισμός είναι προδήλως αληθής. Ας υποθέσουμε ότι $d \geq 2$.

*Περίπτωση πρώτη.* Εάν η $G$ είναι κυκλική, τότε βάσει τού θεωρήματος B.3.13 τού Dirichlet υπάρχει κάποιος πρώτος αριθμός $q$ τής μορφής $q = 1 + nd$, $n \in \mathbb{N}$, οπότε $d \mid q-1$. Η $\mathbb{Z}_q^{\times}$, ούσα *κυκλική* τάξεως $q-1$, διαθέτει μία (και μόνον) κυκλική υποομάδα $H$ τάξεως $d$. (Βλ. 7.3.7 και 2.3.21 (ii).) Επομένως, $G \cong H \sqsubseteq \mathbb{Z}_q^{\times}$.

*Περίπτωση δεύτερη.* Εάν η $G$ είναι μη κυκλική και $G \cong \bigoplus_{\varrho=1}^{\kappa} G(p_\varrho)$, έχουσα τους (9.14) ως στοιχειώδεις διαιρέτες της (όπως στο θεώρημα 9.1.19), τότε σύμφωνα με το θεώρημα B.3.13 τού Dirichlet έχουμε τη δυνατότητα επιλογής πρώτων αριθμών

$$q_{1,1}, q_{1,2}, \dots, q_{1,s_1}, q_{2,1}, q_{2,2}, \dots, q_{2,s_2}, \dots, q_{\kappa,1}, q_{\kappa,2}, \dots, q_{\kappa,s_\kappa}, \tag{9.15}$$

τέτοιων ώστε $q_{i,j} \equiv 1(\mathrm{mod}\, p_i^{k_j^{(i)}})$, $\forall j \in \{1,\dots,s_i\}$ και $\forall i \in \{1,\dots,\kappa\}$. Μάλιστα, επειδή υπάρχουν *άπειροι* πρώτοι αριθμοί $q_{i,j}$ αυτού τού είδους, μπορούμε δίχως βλάβη τής γενικότητας να υποθέσουμε ότι οι επιλεγόμενοι (9.15) είναι *σαφώς διακεκριμένοι*. Υπό αυτήν την προϋπόθεση, θέτοντας $m := \prod_{i=1}^{\kappa} \left( \prod_{j=1}^{s_i} q_{i,j} \right)$ και λαμβάνοντας υπ' όψιν ότι $\mathbb{Z}_m^{\times} \underset{7.3.2}{\cong} \prod_{i=1}^{\kappa} \left( \prod_{j=1}^{s_i} \mathbb{Z}_{q_{i,j}}^{\times} \right)$ και ότι

$$\exists H_{i,j} \in \mathbf{Subg}(\mathbb{Z}_{q_{i,j}}^{\times}) : H_{i,j} \cong \mathbb{Z}_{p_i^{k_j^{(i)}}}, \ \forall j \in \{1,\dots,s_i\} \text{ και } \forall i \in \{1,\dots,\kappa\},$$

(όπως στην πρώτη περίπτωση), συμπεραίνουμε ότι $G \cong \bigoplus_{i=1}^{\kappa} \left( \bigoplus_{j=1}^{s_i} H_{i,j} \right) \sqsubseteq \mathbb{Z}_m^{\times}$. $\square$

**9.1.25 Θεώρημα. (2ο θεμελιώδες θεώρημα περί πεπερασμένων αβελιανών ομάδων.)** *Εάν $(G,+)$ είναι μια πεπερασμένη μη τετριμμένη αβελιανή ομάδα, τότε ισχύουν τα ακόλουθα:*

(i) *Υπάρχουν ένας $s \in \mathbb{N}$ και (όχι κατ' ανάγκην σαφώς διακεκριμένοι) φυσικοί αριθμοί $m_1, m_2, \dots, m_s$, οι οποίοι είναι $\geq 2$ και τέτοιοι, ώστε*

$$\boxed{G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s}, \text{ με } m_i \mid m_{i+1}, \ \forall i \in \{1,\dots,s-1\}.} \tag{9.16}$$

(ii) *Η έκφραση* (9.16) *είναι μονοσημάντως ορισμένη υπό την εξής έννοια: Εάν υπάρχουν ένας* $t \in \mathbb{N}$ *και (όχι κατ' ανάγκην σαφώς διακεκριμένοι) φυσικοί αριθμοί* $m'_1, m'_2, ..., m'_t$, *οι οποίοι είναι* $\geq 2$ *και τέτοιοι, ώστε*

$$G \cong \mathbb{Z}_{m'_1} \oplus \mathbb{Z}_{m'_2} \oplus \cdots \oplus \mathbb{Z}_{m'_t}, \text{ με } m'_\xi \mid m'_{\xi+1},\ \forall \xi \in \{1, ..., t-1\},$$

*τότε* $t = s$ *και* $m'_i = m_i$ *για κάθε* $i \in \{1,...,s\}$.

Αποδειξη. (i) Εάν $|G| = p_1^{\nu_1} \cdots p_\kappa^{\nu_\kappa}$, ($\kappa \in \mathbb{N}$, $\nu_1, ..., \nu_\kappa \in \mathbb{N}$) είναι η κανονική παράσταση (B.19) τής τάξεως τής $G$ ως γινομένου (κατάλληλων δυνάμεων) πρώτων αριθμών $p_1, ..., p_\kappa$ με $p_1 < \cdots < p_\kappa$, τότε μέσω τού θεωρήματος 9.1.19 αποκτούμε τους στοιχειώδεις διαιρέτες

$$p_1^{k_1^{(1)}}, ..., p_1^{k_{s_1}^{(1)}}, p_2^{k_1^{(2)}}, ..., p_2^{k_{s_2}^{(2)}}, ......, p_\kappa^{k_1^{(\kappa)}}, ..., p_\kappa^{k_{s_\kappa}^{(\kappa)}}$$

τής $G$, όπου $(k_1^{(\varrho)}, k_2^{(\varrho)}, ..., k_{s_\varrho}^{(\varrho)}) \in \Pi_{s_\varrho}(\nu_\varrho)$ για κάθε $\varrho \in \{1, ..., \kappa\}$. Θεωρούμε τον $(s \times \kappa)$-πίνακα

$$\begin{pmatrix} p_1^{n_{1,1}} & p_2^{n_{1,2}} & \cdots & p_\kappa^{n_{1,\kappa}} \\ p_1^{n_{2,1}} & p_2^{n_{2,2}} & & p_\kappa^{n_{2,\kappa}} \\ \vdots & & & \vdots \\ p_1^{n_{s,1}} & p_2^{n_{s,2}} & \cdots & p_\kappa^{n_{s,\kappa}} \end{pmatrix} \in \mathrm{Mat}_{s\times\kappa}(\mathbb{N}), \tag{9.17}$$

όπου $s := \max\{s_1, ..., s_\kappa\}$ και

$$n_{i,j} := \begin{cases} 0, & \text{όταν } s_j < s \text{ και } i \in \{1, ..., s - s_j\}, \\ k_{i-(s-s_j)}^{(j)}, & \text{όταν } i \in \{s - s_j + 1, ..., s\}. \end{cases}$$

Προφανώς, για κάθε $j \in \{1, ..., \kappa\}$ ισχύει $0 \leq n_{1,j} \leq n_{2,j} \leq \cdots \leq n_{s,j}$, όπου $n_{i,j} \geq 1$ για τουλάχιστον έναν $i \in \{1, ..., s\}$. Ορίζοντας ως

$$m_i := p_1^{n_{i,1}} p_2^{n_{i,2}} \cdots p_\kappa^{n_{i,\kappa}}$$

το γινόμενο των εγγραφών τής $i$-οστής γραμμής τού (9.17) για κάθε $i \in \{1, ..., s\}$ λαμβάνουμε

$$[m_i \geq 2,\ \forall i \in \{1, ..., s\}] \text{ και } [m_i \mid m_{i+1},\ \forall i \in \{1, ..., s-1\}],$$

και $G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s}$ (μέσω τού (ii) τής προτάσεως 7.1.55).

(ii) Εάν $G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s} \cong \mathbb{Z}_{m'_1} \oplus \mathbb{Z}_{m'_2} \oplus \cdots \oplus \mathbb{Z}_{m'_t}$, όπου

$$[m_i \geq 2,\ \forall i \in \{1, ..., s\}] \text{ και } [m_i \mid m_{i+1},\ \forall i \in \{1, ..., s-1\}], \tag{9.18}$$

και, ταυτοχρόνως,

$$\left[m'_\xi \geq 2,\ \forall \xi \in \{1, ..., t\}\right] \text{ και } \left[m'_\xi \mid m'_{\xi+1},\ \forall \xi \in \{1, ..., t-1\}\right], \tag{9.19}$$

τότε $m_1 \cdots m_s = m_1' \cdots m_s' = p_1^{\nu_1} \ \cdots \ p_\kappa^{\nu_\kappa}$, οπότε

$$\begin{array}{ll} m_1 = p_1^{\alpha_{1,1}} p_2^{\alpha_{1,2}} \cdots p_\kappa^{\alpha_{1,\kappa}} & m_1' = p_1^{\beta_{1,1}} p_2^{\beta_{1,2}} \cdots p_\kappa^{\beta_{1,\kappa}} \\ m_2 = p_1^{\alpha_{2,1}} p_2^{\alpha_{2,2}} \cdots p_\kappa^{\alpha_{2,\kappa}} & m_2' = p_1^{\beta_{2,1}} p_2^{\beta_{2,2}} \cdots p_\kappa^{\beta_{2,\kappa}} \\ \vdots & \vdots \\ m_s = p_1^{\alpha_{s,1}} p_2^{\alpha_{s,2}} \cdots p_\kappa^{\alpha_{s,\kappa}} & m_t' = p_1^{\beta_{t,1}} p_2^{\beta_{t,2}} \cdots p_\kappa^{\beta_{t,\kappa}} \end{array}$$

με $\alpha_{i,j}, \beta_{i,j}, \in \mathbb{N}_0 : [\alpha_{i,j} \leq \nu_j, \forall i \in \{1,...,s\}]$ και $[\beta_{\xi,j} \leq \nu_j, \forall \xi \in \{1,...,t\}]$, για κάθε $j \in \{1,...,\kappa\}$. (Βλ. λήμμα B.3.14.) Από τις συνθήκες (9.18) και (9.19) συμπεραίνουμε ότι

$$0 \leq \alpha_{1,j} \leq \alpha_{2,j} \leq \cdots \leq \alpha_{s,j} \ \text{ και } \ 0 \leq \beta_{1,j} \leq \beta_{2,j} \leq \cdots \leq \beta_{t,j},$$

με τουλάχιστον έναν εκ των $\alpha_{1,j}, ..., \alpha_{s,j}$ (και αντιστοίχως, με τουλάχιστον έναν εκ των $\beta_{1,j}, ..., \beta_{t,j}$) διάφορο τού μηδενός για κάθε $j \in \{1,...,\kappa\}$. Εξάλλου,

$$\bigoplus_{i=1}^{s} \left( \bigoplus_{j=1}^{\kappa} \mathbb{Z}_{p_j^{\alpha_{i,j}}} \right) \underset{7.1.63}{\cong} \bigoplus_{i=1}^{s} \mathbb{Z}_{m_i} \cong G \cong \bigoplus_{\xi=1}^{t} \mathbb{Z}_{m_\xi'} \underset{7.1.63}{\cong} \bigoplus_{\xi=1}^{t} \left( \bigoplus_{j=1}^{\kappa} \mathbb{Z}_{p_j^{\beta_{\xi,j}}} \right), \tag{9.20}$$

οπότε

$$\bigoplus_{i=1}^{s} \mathbb{Z}_{p_j^{\alpha_{i,j}}} \cong G(p_j) \cong \bigoplus_{\xi=1}^{t} \mathbb{Z}_{p_j^{\beta_{\xi,j}}}, \ \forall j \in \{1,...,\kappa\}.$$

Επειδή

$$2 \leq m_1 \leq \cdots \leq m_s \Rightarrow [\exists j_\bullet \in \{1,...,\kappa\} : 1 \leq \alpha_{1,j_\bullet} \leq \alpha_{2,j_\bullet} \leq \cdots \leq \alpha_{s,j_\bullet}],$$

το $\bigoplus_{i=1}^{s} \mathbb{Z}_{p_{j_\bullet}^{\alpha_{i,j_\bullet}}}$ έχει $s$ *μη τετριμμένους* ευθείς προσθετέους, οπότε

$$\bigoplus_{i=1}^{s} \mathbb{Z}_{p_{j_\bullet}^{\alpha_{i,j_\bullet}}} \cong \bigoplus_{\xi=1}^{t} \mathbb{Z}_{p_{j_\bullet}^{\beta_{\xi,j_\bullet}}} \underset{9.1.8\,(ii)}{\Longrightarrow} \left[ \begin{array}{c} \text{το } \bigoplus_{\xi=1}^{t} \mathbb{Z}_{p_{j_\bullet}^{\beta_{\xi,j_\bullet}}} \text{ έχει } s \text{ μη τετριμ-} \\ \text{μένους ευθείς προσθετέους} \end{array} \right].$$

Επομένως, $s \leq t$. Κατ' αναλογίαν, επειδή $2 \leq m_1' \leq \cdots \leq m_t'$, έχουμε $t \leq s$. Άρα τελικώς $t = s$ και από την (9.20) και το θεώρημα 9.1.19 συνάγεται ότι

$$\alpha_{i,j} = \beta_{i,j}, \ \forall (i,j) \in \{1,...,s\} \times \{1,...,\kappa\},$$

απ' όπου προκύπτει ότι $m_i' = m_i$ για κάθε $i \in \{1,..., s\}$. □

**9.1.26 Ορισμός.** Εάν $(G, +)$ είναι μια μη τετριμμένη πεπερασμένη αβελιανή ομάδα, τότε οι μονοσημάντως ορισμένοι φυσικοί αριθμοί $m_1,..., m_s$ στην έκφρασή της (9.16) ως ευθέος αθροίσματος κυκλικών ομάδων καλούνται **αναλλοίωτοι παράγοντές της**.

**9.1.27 Πόρισμα.** *Δυο πεπερασμένες μη τετριμμένες αβελιανές ομάδες ίσων τάξεων είναι ισόμορφες εάν και μόνον εάν διαθέτουν τους ίδιους αναλλοίωτους παράγοντες.*

**9.1.28 Παραδείγματα.** (i) $\mathbb{Z}_3 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{27} \ncong \mathbb{Z}_{27} \oplus \mathbb{Z}_{27}$.
(ii) $\mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_{32} \ncong \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_{32}$ (παρά το γεγονός ότι αμφότερες οι ομάδες διαθέτουν το ίδιο πλήθος αναλλοίωτων παραγόντων και δύο κοινούς).

**9.1.29 Σημείωση.** Εάν υποθέσουμε ότι για μια δοθείσα πεπερασμένη μη τετριμμένη αβελιανή ομάδα είναι γνωστοί οι αναλλοίωτοι παράγοντες $m_1,\ldots,m_s$, τότε οι στοιχειώδεις διαιρέτες της αποκτώνται απευθείας από την κανονική παράσταση καθενός εκ των $m_1,\ldots,m_s$ ως γινομένου πρώτων αριθμών. Και αντιστρόφως· εάν υποτεθεί ότι είναι γνωστοί οι στοιχειώδεις διαιρέτες της, για την εύρεση των αναλλοίωτων παραγόντων της αρκεί να σχηματίσουμε τα γινόμενα των εγγραφών των γραμμών τού πίνακα (9.17).

**9.1.30 Παράδειγμα.** Έστω $G$ η αβελιανή ομάδα τάξεως 3528 που έχει τους $2, 42, 42$ ως αναλλοίωτους παράγοντές της. Επειδή $42 = 2 \cdot 3 \cdot 7$ και

$$\begin{aligned} G &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{42} \oplus \mathbb{Z}_{42} \\ &\underset{7.1.63}{\cong} \mathbb{Z}_2 \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7) \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7) \\ &\underset{7.1.55\,(ii)}{\cong} (\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2) \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_3) \oplus (\mathbb{Z}_7 \oplus \mathbb{Z}_7), \end{aligned}$$

οι στοιχειώδεις διαιρέτες είναι οι $2, 2, 2, 3, 3, 7, 7$ και η $G$ η πρώτη εκ των αβελιανών ομάδων τού δευτέρου καταλόγου τού εδαφίου 9.1.23.

**9.1.31 Παράδειγμα.** Θεωρούμε την αβελιανή ομάδα $G := \mathbb{Z}_6 \oplus \mathbb{Z}_{10}$ τάξεως 60. Επειδή

$$G \underset{7.1.63}{\cong} (\mathbb{Z}_2 \oplus \mathbb{Z}_3) \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_5) \underset{7.1.55\,(ii)}{\cong} (\mathbb{Z}_2 \oplus \mathbb{Z}_2) \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_5),$$

οι στοιχειώδεις διαιρέτες τής $G$ είναι οι $2, 2, 3, 5$. Χρησιμοποιώντας τόν πίνακα

$$\begin{pmatrix} 2^1 & 3^0 & 5^0 \\ 2^1 & 3^1 & 5^1 \end{pmatrix}$$

διαπιστώνουμε ότι οι $2 \cdot 1 \cdot 1 = 2$ και $2 \cdot 3 \cdot 5 = 30$ είναι οι αναλλοίωτοι παράγοντες τής $G$, οπότε $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{30}$.

**9.1.32 Παράδειγμα.** Θεωρούμε την $G := \mathbb{Z}_5 \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{36} \oplus \mathbb{Z}_{1134}$ τάξεως 76 545 000. Επειδή

$$\begin{aligned} G &= \mathbb{Z}_5 \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_5) \oplus \mathbb{Z}_{5^2} \oplus (\mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^2}) \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_{3^4} \oplus \mathbb{Z}_7) \\ &\underset{7.1.55\,(ii)}{\cong} (\mathbb{Z}_2 \oplus \mathbb{Z}_{2^2}) \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_{3^4}) \oplus (\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{5^2}) \oplus \mathbb{Z}_7, \end{aligned}$$

οι στοιχειώδεις διαιρέτες τής $G$ είναι οι $2, 2^2, 3, 3^2, 3^4, 5, 5, 5^2, 7$. Χρησιμοποιώντας τόν πίνακα

$$\begin{pmatrix} 2^0 & 3^1 & 5^1 & 7^0 \\ 2^1 & 3^2 & 5^1 & 7^0 \\ 2^2 & 3^4 & 5^2 & 7^1 \end{pmatrix}$$

διαπιστώνουμε ότι οι $1 \cdot 3 \cdot 5 \cdot 1 = 15$, $2 \cdot 3^2 \cdot 5 \cdot 1 = 90$ και $2^2 \cdot 3^4 \cdot 5^2 \cdot 7 = 56\,700$ είναι οι αναλλοίωτοι παράγοντες τής $G$, οπότε $G \cong \mathbb{Z}_{15} \oplus \mathbb{Z}_{90} \oplus \mathbb{Z}_{56\,700}$.

► **Αξιοσημείωτα πορίσματα προκύπτοντα από το θεώρημα 9.1.25**. Αυτά συμπεριλαμβάνουν, μεταξύ άλλων, τον υπολογισμό τού εκθέτη μιας πεπερασμένης μη τετριμμένης αβελιανής ομάδας και την απόδειξη τής «κυκλικότητας» κάθε πεπερασμένης υποομάδας τής πολλαπλασιαστικής ομάδας τυχόντος σώματος.

**9.1.33 Πόρισμα.** *Εάν $(G,+)$ είναι μια πεπερασμένη μη τετριμμένη αβελιανή ομάδα έχουσα ως αναλλοίωτους παράγοντές της τους $m_1,...,m_s$* (βλ. (9.16)), *τότε*

$$\boxed{\exp(G) = m_s.}$$

Απόδειξη. Σύμφωνα με το πόρισμα 4.1.29, $\exp(\mathbb{Z}_{m_i}) = m_i$ για κάθε $i \in \{1,...,s\}$. Από το θεώρημα 7.1.61 λαμβάνουμε $\exp(G) = $ εκπ$(m_1,...,m_s)$. Επειδή $m_i \mid m_{i+1}$ για κάθε $i \in \{1,...,s-1\}$, συμπεραίνουμε ότι $\exp(G) = m_s$. □

**9.1.34 Πόρισμα.** *Μια πεπερασμένη αβελιανή ομάδα $(G,+)$ είναι*

$$\boxed{\text{κυκλική} \Longleftrightarrow \exp(G) = |G|\,.}$$

Απόδειξη. "$\Rightarrow$" Έχει ήδη αποδειχθεί στο πόρισμα 4.1.29.

"$\Leftarrow$" Όταν $|G| = 1$, ο ισχυρισμός είναι προδήλως αληθής. Όταν $|G| \geq 2$ και οι αναλλοίωτοι παράγοντες τής $G$ είναι οι $m_1,...,m_s$,τότε από τις ισότητες

$$m_s \underset{9.1.33}{=} \exp(G) = |G| = \prod_{i=1}^{s} m_i \ \ (\text{όπου } \ m_i \geq 2, \ \forall i \in \{1,...,s\})$$

προκύπτει ότι $s = 1$ και $|G| = m_1 \Rightarrow G \cong \mathbb{Z}_{m_1}$. (Εναλλακτικώς, θα μπορούσε κανείς να επιχειρηματολογήσει ως εξής: Εάν $s \geq 2$, τότε

$$[m_i \mid m_{i+1}, \ \forall i \in \{1,...,s-1\}] \Rightarrow [\text{μκδ}(m_i, m_{i+1}) = m_i \geq 2, \ \forall i \in \{1,...,s-1\}],$$

οπότε η $G$ είναι μη κυκλική επί τη βάσει τού θεωρήματος 7.1.64.) □

**9.1.35 Πόρισμα.** *Κάθε πεπερασμένη υποομάδα τής πολλαπλασιαστικής ομάδας* $(F^{\times},\cdot)$, $F^{\times} = F \smallsetminus \{0_F\}$, (*των αντιστρεψίμων στοιχείων*) *ενός σώματος* $(F,+,\cdot)$ *είναι κυκλική.* (*Ιδιαιτέρως, η πολλαπλασιαστική ομάδα ενός πεπερασμένου σώματος είναι κυκλική.*)

Απόδειξη. Έστω $(F,+,\cdot)$ τυχόν σώμα και έστω $L$ μια πεπερασμένη υποομάδα τής $(F^{\times},\cdot)$. Η $(L,\cdot)$ είναι αβελιανή, οπότε είναι *είτε* τετριμμένη *είτε* υπάρχουν ένας $s \in \mathbb{N}$ και (όχι κατ' ανάγκην σαφώς διακεκριμένοι) φυσικοί αριθμοί $m_1,...,m_s$, οι οποίοι είναι $\geq 2$ και τέτοιοι, ώστε

$$L \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s}, \ \text{ με } \ m_i \mid m_{i+1}, \ \forall i \in \{1,...,s-1\}.$$

(Βλ. 9.1.25.) Στην πρώτη περίπτωση η $L$ είναι προφανώς κυκλική. Στη δεύτερη περίπτωση το πόρισμα 9.1.33 μας πληροφορεί ότι $\exp(L) = m_s$. Από τον ορισμό τού εκθέτη για την *πολλαπλασιαστική* ομάδα $L$ έπεται ότι $a^{m_s} = 1_F, \forall a \in L$. Άρα το πλήθος των θέσεων μηδενισμού τού πολυωνύμου $\mathsf{X}^{m_s} - 1_F \in F[\mathsf{X}] \smallsetminus \{0_{F[\mathsf{X}]}\}$

είναι $\geq |L| = \prod_{i=1}^{s} m_i$. Επειδή όμως αυτό το πολυώνυμο, σύμφωνα με το πόρισμα C.2.27, διαθέτει *το πολύ* $m_s$ θέσεις μηδενισμού, έχουμε κατ' ανάγκην $s = 1$ και $L \cong \mathbb{Z}_{m_1}$. $\square$

**9.1.36 Πόρισμα.** *Έστω* $(F, +, \cdot)$ *τυχόν πεπερασμένο σώμα και έστω* $n \in \mathbb{N}$. *Ως γνωστόν, υφίσταται ισομορφισμός σωμάτων μεταξύ αυτού και τού σώματος* $\mathbb{F}_q$ *(με* $\mathrm{card}(F) = q$*), όπου* $q = p^{\nu}$, $p$ *κάποιος πρώτος αριθμός και* $\nu \in \mathbb{N}$. (Βλ. C.2.15 (ii) και C.2.16 (i).) *Το κέντρο*

$$Z(\mathrm{SL}_n(F)) \cong Z(\mathrm{SL}_n(\mathbb{F}_q)) = \{\, \lambda \mathbf{I}_n |\, \lambda \in \mathbb{F}_q^{\times},\ \lambda^n = 1_{\mathbb{F}_q}\}$$

*τής ειδικής γραμμικής ομάδας βαθμού* $n$ *υπεράνω αυτού είναι (προφανώς) ισόμορφο με την υποομάδα* $\left\{ \lambda \in \mathbb{F}_q^{\times} \middle|\, \lambda^n = 1_{\mathbb{F}_q} \right\}$ *τής πολλαπλασιαστικής ομάδας* $(\mathbb{F}_q^{\times}, \cdot)$. (Βλ. πρόταση 5.4.12.) *Ως εκ τούτου, η τάξη του ισούται με*

$$\boxed{|Z(\mathrm{SL}_n(\mathbb{F}_q))| = \text{μκδ}(n, q-1).} \tag{9.21}$$

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το πόρισμα 9.1.35, η $(\mathbb{F}_q^{\times}, \cdot)$ είναι κυκλική και, κατ' επέκταση, η υποομάδα της $L := \left\{ \lambda \in \mathbb{F}_q^{\times} \middle|\, \lambda^n = 1_{\mathbb{F}_q} \right\}$ είναι ωσαύτως κυκλική. Θέτοντας $d := \text{μκδ}(n, q-1)$ παρατηρούμε ότι *για κάθε* $\lambda \in \mathbb{F}_q^{\times}$ ισχύει

$$\lambda^n = 1_{\mathbb{F}_q} \Longleftrightarrow \lambda^d = 1_{\mathbb{F}_q}.$$

Πράγματι· εάν $\lambda^d = 1_{\mathbb{F}_q}$, τότε

$$d \mid n \Rightarrow \lambda^n = (\lambda^d)^{\frac{n}{d}} = (1_{\mathbb{F}_q})^{\frac{n}{d}} = 1_{\mathbb{F}_q}.$$

Και αντιστρόφως· εάν $\lambda^n = 1_{\mathbb{F}_q}$, τότε $\exists k, l \in \mathbb{Z}$: $d = kn + l(q-1)$ (βλ. B.2.5), οπότε

$$\lambda^d = \lambda^{kn+l(q-1)} = (\lambda^n)^k \lambda^{l(q-1)} = \left(1_{\mathbb{F}_q}\right)^k (\lambda^{q-1})^l = (\lambda^{q-1})^l = (1_{\mathbb{F}_q})^l = 1_{\mathbb{F}_q},$$

διότι $\left|\mathbb{F}_q^{\times}\right| = q - 1 \underset{4.1.28}{\Longrightarrow} \lambda^{q-1} = 1_{\mathbb{F}_q}$. Κατά συνέπειαν, $L = \left\{ \lambda \in \mathbb{F}_q^{\times} \middle|\, \lambda^d = 1_{\mathbb{F}_q} \right\}$. Επειδή $d \mid q-1$, το πόρισμα 2.3.22 μας πληροφορεί ότι η $L$ είναι η μοναδική υποομάδα τής $(\mathbb{F}_q^{\times}, \cdot)$ που έχει τάξη $d$. (Εάν $\lambda_* \in \mathbb{F}_q^{\times}$ είναι ένας γεννήτορας τής $(\mathbb{F}_q^{\times}, \cdot)$, τότε $L = <\lambda_*^{\frac{q-1}{d}}>$.) Άρα η (9.21) είναι αληθής. $\square$

► **Ταξινόμηση πεπερασμένων αβελιανών ομάδων τάξεως** $\leq 100$. Η εν λόγω ταξινόμηση (μέχρις ισομορφισμού) επιτυγχάνεται με τη βοήθεια των στοιχειωδών διαιρετών ή, ισοδυνάμως, των αναλλοιώτων παραγόντων, δίχως ιδιαίτερη υπολογιστική δυσκολία (και απευθείας).

**9.1.37 Λήμμα.** *Το πλήθος των ανά ζεύγη μη ισομόρφων πεπερασμένων αβελιανών ομάδων* $G$ *τάξεως* $\leq 100$ *(σημειούμενο ως "Πλ.") είναι αυτό που καταχωρίζεται* *στον κατάλογο*

| $\|G\|$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Πλ. | **1** | **1** | **1** | **2** | **1** | **1** | **1** | **3** | **2** | **1** |
| $\|G\|$ | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| Πλ. | **1** | **2** | **1** | **1** | **1** | **5** | **1** | **2** | **1** | **2** |
| $\|G\|$ | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| Πλ. | **1** | **1** | **1** | **3** | **2** | **1** | **3** | **2** | **1** | **1** |
| $\|G\|$ | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| Πλ. | **1** | **7** | **1** | **1** | **1** | **4** | **1** | **1** | **1** | **3** |
| $\|G\|$ | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |
| Πλ. | **1** | **1** | **1** | **2** | **2** | **1** | **1** | **5** | **2** | **2** |

*όταν* $1 \leq |G| \leq 50$ *και, αντιστοίχως, αυτό που καταχωρίζεται στον κατάλογο*

| $\|G\|$ | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 |
|---|---|---|---|---|---|---|---|---|---|---|
| Πλ. | **1** | **2** | **1** | **3** | **1** | **3** | **1** | **1** | **1** | **2** |
| $\|G\|$ | 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 |
| Πλ. | **1** | **1** | **2** | **11** | **1** | **1** | **1** | **2** | **1** | **1** |
| $\|G\|$ | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 |
| Πλ. | **1** | **6** | **1** | **1** | **2** | **2** | **1** | **1** | **1** | **5** |
| $\|G\|$ | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 |
| Πλ. | **5** | **1** | **1** | **2** | **1** | **1** | **1** | **3** | **1** | **2** |
| $\|G\|$ | 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 |
| Πλ. | **1** | **2** | **1** | **1** | **1** | **7** | **1** | **2** | **2** | **4** |

*όταν* $51 \leq |G| \leq 100$.

Αποδειξη. Έστω $G$ τυχούσα μη τετριμμένη πεπερασμένη αβελιανή ομάδα τάξεως $\leq 100$ και έστω $|G| = p_1^{\nu_1} \cdots p_\kappa^{\nu_\kappa}$, ($\kappa \in \mathbb{N}$, $\nu_1,\ldots,\nu_\kappa \in \mathbb{N}$) η κανονική παράσταση (B.19) τής τάξεώς της ως γινομένου πρώτων αριθμών $p_1,\ldots,p_\kappa$ με $p_1 < \cdots < p_\kappa$. Από τον κατάλογο τού εδαφίου B.3.9 γνωρίζουμε ότι $\kappa \in \{1,2,3\}$ και ότι $\max\{\nu_1,\ldots,\nu_\kappa\} \in \{1,2,3,4,5,6\}$ (όπου η μέγιστη τιμή 6 λαμβάνεται μόνον όταν $\kappa = 1$, $p_1 = 2$ και $|G| = 64 = 2^6$). Επειδή

$$\varpi(1) = 1,\ \varpi(2) = 2,\ \varpi(3) = 3,\ \varpi(4) = 5,\ \varpi(5) = 7,\ \varpi(6) = 11,$$

οι ανωτέρω κατάλογοι προκύπτουν άμεσα από αυτόν τού εδαφίου B.3.9 και το πόρισμα 9.1.22. □

**9.1.38 Θεώρημα. (Ταξινόμηση αβελιανών ομάδων τάξεως** $\leq 100$.)
*Έστω* $G$ *μια αβελιανή ομάδα τάξεως* $\leq 100$. *Εάν*

$$|G| \in \left\{ \begin{array}{c} 1,2,3,5,6,7,10,11,13,14,15,17,19,21,22,23,26, \\ 29,30,31,33,34,35,37,38,39,41,42,43,46,47,51, \\ 53,55,57,58,59,61,62,65,66,67,69,70,71,73,74, \\ 77,78,79,82,83,85,86,87,89,91,93,94,95,97 \end{array} \right\}, \tag{9.22}$$

*τότε αυτή είναι κυκλική (και, ως εκ τούτου, ισόμορφη με την* $\mathbb{Z}_{|G|}$*). Για τους λοιπούς αριθμούς η ταξινόμηση (μέχρις ισομορφισμού) δίδεται στον κατάλογο*

| $\|G\|$ | $G$ |
|---|---|
| 4 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \ (\cong \mathbf{V})\,,\ \mathbb{Z}_4$ |
| 8 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_2 \oplus \mathbb{Z}_4,\ \mathbb{Z}_8$ |
| 9 | $\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$ |
| 12 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \ (\cong \mathbb{Z}_2 \oplus \mathbb{Z}_6)\,,$<br>$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \ (\cong \mathbb{Z}_{12})$ |
| 16 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4,$<br>$\mathbb{Z}_2 \oplus \mathbb{Z}_8,\ \mathbb{Z}_4 \oplus \mathbb{Z}_4,\ \mathbb{Z}_{16}$ |
| 18 | $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \ (\cong \mathbb{Z}_3 \oplus \mathbb{Z}_6)\,,$<br>$\mathbb{Z}_2 \oplus \mathbb{Z}_9 \ (\cong \mathbb{Z}_{18})$ |
| 20 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \ (\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{10})\,,$<br>$\mathbb{Z}_4 \oplus \mathbb{Z}_5 \ (\cong \mathbb{Z}_{20})$ |
| 24 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \ (\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6)\,,$<br>$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \ (\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{12})\,,\ \mathbb{Z}_8 \oplus \mathbb{Z}_3 \ (\cong \mathbb{Z}_{24})$ |

*όταν* $4 \leq |G| \leq 24$*, στον κατάλογο*

| $\|G\|$ | $G$ |
|---|---|
| 25 | $\mathbb{Z}_5 \oplus \mathbb{Z}_5,\ \mathbb{Z}_{25}$ |
| 27 | $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_3 \oplus \mathbb{Z}_9,\ \mathbb{Z}_{27}$ |
| 28 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_7 \ (\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{14})\,,\ \mathbb{Z}_4 \oplus \mathbb{Z}_7 \ (\cong \mathbb{Z}_{28})$ |
| 32 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4,$<br>$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_8,\ \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4,$<br>$\mathbb{Z}_2 \oplus \mathbb{Z}_{16},\ \mathbb{Z}_4 \oplus \mathbb{Z}_8,\ \mathbb{Z}_{32}$ |
| 36 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \ (\cong \mathbb{Z}_6 \oplus \mathbb{Z}_6)\,,$<br>$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \ (\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{18})\,,$<br>$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \ (\cong \mathbb{Z}_3 \oplus \mathbb{Z}_{12})\,,\ \mathbb{Z}_4 \oplus \mathbb{Z}_9 \ (\cong \mathbb{Z}_{36})$ |
| 40 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \ (\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{10})\,,$<br>$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5 \ (\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{20})\,,\ \mathbb{Z}_{40}$ |
| 44 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{11} \ (\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{22})\,,\ \mathbb{Z}_4 \oplus \mathbb{Z}_{11} \ (\cong \mathbb{Z}_{44})$ |
| 45 | $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \ (\cong \mathbb{Z}_3 \oplus \mathbb{Z}_{15})\,,\ \mathbb{Z}_9 \oplus \mathbb{Z}_5 \ (\cong \mathbb{Z}_{45})$ |

*όταν* $25 \leq |G| \leq 45$*, στον κατάλογο*

| $\|G\|$ | $G$ |
|---|---|
| 48 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \ (\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6)\,,$<br>$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \ (\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{12})\,,$<br>$\mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3 \ (\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{24})\,,\ \mathbb{Z}_{16} \oplus \mathbb{Z}_3 \ (\cong \mathbb{Z}_{48})$ |
| 49 | $\mathbb{Z}_7 \oplus \mathbb{Z}_7,\ \mathbb{Z}_{49}$ |
| 50 | $\mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \ (\cong \mathbb{Z}_5 \oplus \mathbb{Z}_{10})\,,\ \mathbb{Z}_2 \oplus \mathbb{Z}_{25} \ (\cong \mathbb{Z}_{50})$ |
| 52 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{13} \ (\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{26})\,,\ \mathbb{Z}_4 \oplus \mathbb{Z}_{13} \ (\cong \mathbb{Z}_{52})$ |
| 54 | $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \ (\cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_6)\,,$<br>$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9 \ (\cong \mathbb{Z}_3 \oplus \mathbb{Z}_{18})\,,\ \mathbb{Z}_2 \oplus \mathbb{Z}_{27} \ (\cong \mathbb{Z}_{54})$ |
| 56 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_7 \ (\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{14})\,,$<br>$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_7 \ (\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{28})\,,\ \mathbb{Z}_8 \oplus \mathbb{Z}_7 \ (\cong \mathbb{Z}_{56})$ |
| 60 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \ (\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{30})\,,\ \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \ (\cong \mathbb{Z}_{60})$ |

*όταν* $48 \leq |G| \leq 60$, *στον κατάλογο*

| $\|G\|$ | $G$ |
|---|---|
| 63 | $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7$ $(\cong \mathbb{Z}_3 \oplus \mathbb{Z}_{21})$, $\mathbb{Z}_9 \oplus \mathbb{Z}_7$ $(\cong \mathbb{Z}_{63})$ |
| 64 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_8$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{16}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8$, $\mathbb{Z}_2 \oplus \mathbb{Z}_{32}$, $\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4$, $\mathbb{Z}_4 \oplus \mathbb{Z}_{16}$, $\mathbb{Z}_8 \oplus \mathbb{Z}_8$, $\mathbb{Z}_{64}$ |
| 68 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{17}$ $(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{34})$, $\mathbb{Z}_4 \oplus \mathbb{Z}_{17}$ $(\cong \mathbb{Z}_{48})$ |
| 72 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ $(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6)$, $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ $(\cong \mathbb{Z}_6 \oplus \mathbb{Z}_{12})$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$ $(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{18})$, $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9$ $(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{36})$, $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ $(\cong \mathbb{Z}_3 \oplus \mathbb{Z}_{24})$, $\mathbb{Z}_8 \oplus \mathbb{Z}_9$ $(\cong \mathbb{Z}_{72})$ |
| 75 | $\mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$ $(\cong \mathbb{Z}_3 \oplus \mathbb{Z}_{15})$, $\mathbb{Z}_3 \oplus \mathbb{Z}_{25}$ $(\cong \mathbb{Z}_{75})$ |
| 76 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{19}$ $(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{38})$, $\mathbb{Z}_4 \oplus \mathbb{Z}_{19}$ $(\cong \mathbb{Z}_{76})$ |
| 80 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5$ $(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{10})$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5$ $(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{20})$, $\mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_5$ $(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{40})$, $\mathbb{Z}_{16} \oplus \mathbb{Z}_5$ $(\cong \mathbb{Z}_{80})$ |

*όταν* $63 \leq |G| \leq 80$, *στον κατάλογο*

| $\|G\|$ | $G$ |
|---|---|
| 81 | $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$, $\mathbb{Z}_3 \oplus \mathbb{Z}_{27}$, $\mathbb{Z}_9 \oplus \mathbb{Z}_9$, $\mathbb{Z}_{81}$ |
| 84 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7$ $(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{42})$, $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7$ $(\cong \mathbb{Z}_{84})$ |
| 88 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{11}$ $(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{22})$, $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{11}$ $(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{44})$, $\mathbb{Z}_8 \oplus \mathbb{Z}_{11}$ $(\cong \mathbb{Z}_{88})$ |
| 90 | $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ $(\cong \mathbb{Z}_3 \oplus \mathbb{Z}_{30})$, $\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$ $(\cong \mathbb{Z}_{90})$ |

*όταν* $81 \leq |G| \leq 90$, *και, αντιστοίχως, στον κατάλογο*

| $\|G\|$ | $G$ |
|---|---|
| 92 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{23}$ $(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{46})$, $\mathbb{Z}_4 \oplus \mathbb{Z}_{23}$ $(\cong \mathbb{Z}_{92})$ |
| 96 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$ $(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6)$ $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3$ $(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{12})$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3$ $(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{24})$, $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3$ $(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{12})$, $\mathbb{Z}_2 \oplus \mathbb{Z}_{16} \oplus \mathbb{Z}_3$ $(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{48})$, $\mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3$ $(\cong \mathbb{Z}_4 \oplus \mathbb{Z}_{24})$, $\mathbb{Z}_{32} \oplus \mathbb{Z}_3$ $(\cong \mathbb{Z}_{96})$ |
| 98 | $\mathbb{Z}_2 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$ $(\cong \mathbb{Z}_7 \oplus \mathbb{Z}_{14})$, $\mathbb{Z}_2 \oplus \mathbb{Z}_{49}$ $(\cong \mathbb{Z}_{98})$ |
| 99 | $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{11}$ $(\cong \mathbb{Z}_3 \oplus \mathbb{Z}_{33})$, $\mathbb{Z}_9 \oplus \mathbb{Z}_{11}$ $(\cong \mathbb{Z}_{99})$ |
| 100 | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$ $(\cong \mathbb{Z}_{10} \oplus \mathbb{Z}_{10})$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{25}$ $(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{50})$, $\mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$ $(\cong \mathbb{Z}_5 \oplus \mathbb{Z}_{20})$, $\mathbb{Z}_4 \oplus \mathbb{Z}_{25}$ $(\cong \mathbb{Z}_{100})$ |

*όταν* $92 \leq |G| \leq 100$.

ΑΠΟΔΕΙΞΗ. Οι αριθμοί τού καταλόγου (9.22) είναι ακριβώς αυτοί για τους οποίους το "Πλ." στο λήμμα 9.1.37 ισούται με 1. (Επειδή για κάθε φυσικό αριθμό $n$ υφίσταται -μέχρις ισομορφισμού- πάντοτε μία και μόνον κυκλική ομάδα τάξεως $n$, οι αβελιανές ομάδες, οι τάξεις των οποίων συγκαταλέγονται σε αυτούς τους 61 αριθμούς, είναι *κατ' ανάγκην κυκλικές*.) Για τις υπολειπόμενες 39 τιμές μέχρι το 100 όλοι δυνατοί στοιχειώδεις διαιρέτες και οι αναλλοίωτοι παράγοντες προκύπτουν άμεσα από το λήμμα 9.1.37, τον κατάλογο τού εδαφίου B.3.9 και τα θεμελιώδη θεωρήματα 9.1.19 και 9.1.25. □

► **Για ποιους** $n \in \mathbb{N}, n \geq 2$, **είναι όλες οι ομάδες τάξεως** $n$ **αβελιανές;** Το ερώτημα αυτό, διατυπωθέν για *κυκλικές* ομάδες, έχει ήδη απαντηθεί στην §7.4. Ιδού η απάντησή του (η οφειλόμενη στον L.E. Dickson[10]) και για *αβελιανές* ομάδες:

**9.1.39 Θεώρημα. (L.E. Dickson, 1905)** *Δοθέντος ενός* $n \in \mathbb{N}, n \geq 2$, *οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Όλες οι ομάδες τάξεως* $n$ *είναι αβελιανές.*

(ii) $n = p_1^{\nu_1} \cdots p_k^{\nu_k}$, $k \in \mathbb{N}$, $\nu_i \in \{1,2\}, \forall i \in \{1,...,k\}$, *όπου* $p_1,...,p_k$ *είναι σαφώς διακεκριμένοι πρώτοι αριθμοί για τους οποίους ισχύει* $p_i^{\xi_i} \not\equiv 1 (\mathrm{mod}\, p_j)$ *για οιονσδήποτε* $i, j \in \{1,...,k\}$, $i \neq j$, *και* $\xi_i \in \mathbb{N}$, $1 \leq \xi_i \leq \nu_i$, *όταν* $k \geq 2$.

Μια απόδειξη τού θεωρήματος 9.1.39 θα δοθεί στην §??. (Βλ. σελίδα ??.)

# 9.2 ΥΠΟΟΜΑΔΕΣ ΠΕΠΕΡΑΣΜΕΝΩΝ ΑΒΕΛΙΑΝΩΝ ΟΜΑΔΩΝ

Εάν $(G, +)$ είναι μια πεπερασμένη αβελιανή υποομάδα, τότε είναι προφανές ότι κάθε υποομάδα της $H$ είναι αβελιανή. Εάν αμφότερες οι $G$ και $H$ είναι μη τετριμμένες, τότε οι στοιχειώδεις διαιρέτες και οι αναλλοίωτοι παράγοντες τής $H$ σχετίζονται κατά τρόπο *φυσικό* με εκείνους τής $G$.

► **Στοιχειώδεις διαιρέτες υποομάδων**. Έστω $|G| = p_1^{\nu_1} p_2^{\nu_2} \cdots p_\kappa^{\nu_\kappa}$ η κανονική παράσταση (B.19) τής τάξεως τής $G$ ως γινομένου (κατάλληλων δυνάμεων) πρώτων αριθμών $p_1,...,p_\kappa$ με $p_1 < \cdots < p_\kappa$ και έστω

$$G = G(p_1) \oplus_{\text{εσ.}} G(p_2) \oplus_{\text{εσ.}} \cdots \oplus_{\text{εσ.}} G(p_\kappa)$$

η πρωτεύουσα αποσύνθεση τής $G$ με $|G(p_\varrho)| = p_\varrho^{\nu_\varrho}$, $\forall \varrho \in \{1,...,\kappa\}$. (Βλ. πρόταση 9.1.17.) Επειδή (σύμφωνα με το 7.1.85 (ii)) $G \cong G(p_1) \oplus \cdots \oplus G(p_\kappa)$ και

$$\mathbf{Subg}(G(p_1) \oplus \cdots \oplus G(p_\kappa)) = \mathbf{Subg}(G(p_1)) \times \cdots \times \mathbf{Subg}(G(p_\kappa))$$

(κατόπιν επαναληπτικής εφαρμογής τού πορίσματος 7.1.11), ο προσδιορισμός των υποομάδων τής $G$ ανάγεται στον προσδιορισμό των υποομάδων καθεμιάς εκ των $G(p_\varrho)$, $\varrho \in \{1,...,\kappa\}$. Ο τελευταίος είναι εφικτός κατόπιν εφαρμογής τού θεωρήματος 9.2.2 (για καθεμιά εξ αυτών των πρωτευουσών συνιστωσών τής $G$). Παρεμπιπτόντως, αξίζει να επισημανθεί ότι

$$\mathrm{card}(\mathbf{Subg}(G)) = \prod_{\varrho=1}^{\kappa} \mathrm{card}(\mathbf{Subg}(G(p_\varrho))) \tag{9.23}$$

[10] L.E. Dickson: *Definitions of a group and a field by independent postulates*, Trans. A.M.S. **6** (1905), 198-204. [Βλ., ιδιαιτέρως, σελ. 200.]

και, κατ' επέκταση[11], λόγω τού θεωρήματος 7.1.64,

$$\operatorname{card}(\mathbf{CSubg}(G)) = \prod_{\varrho=1}^{\kappa} \operatorname{card}(\mathbf{CSubg}(G\,(p_\varrho))). \tag{9.24}$$

**9.2.1 Λήμμα.** *Έστω $(G,+)$ μια πεπερασμένη αβελιανή ομάδα τάξεως $p^\nu$, όπου $p$ πρώτος και $\nu \in \mathbb{N}$. Εάν οι $p^{k_1}, p^{k_2}, \ldots, p^{k_s}$ είναι οι στοιχειώδεις διαιρέτες τής $G$ (ήτοι $(k_1, k_2, \ldots, k_s) \in \Pi_s(\nu)$ και $G \cong \mathbb{Z}_{p^{k_1}} \oplus \mathbb{Z}_{p^{k_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_s}}$ η μονοσημάντως ορισμένη έκφραση* (9.8) *τής προτάσεως* 9.1.8), *τότε $|G[p]| = p^s$.*

ΑΠΟΔΕΙΞΗ. Επειδή $G/G[p] \underset{9.1.4}{\cong} pG$ και

$$pG \underset{9.1.6}{\cong} p\mathbb{Z}_{p^{k_1}} \oplus \cdots \oplus p\mathbb{Z}_{p^{k_s}} \cong \mathbb{Z}_{p^{k_1-1}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_s-1}},$$

λαμβάνουμε $|G[p]| = \frac{|G|}{|pG|} = \frac{p^\nu}{p^{(k_1+\cdots+k_s)-s}} = \frac{p^\nu}{p^{\nu-s}} = p^s$. □

**9.2.2 Θεώρημα.** *Έστω $(G,+)$ μια πεπερασμένη αβελιανή ομάδα τάξεως $p^\nu$, όπου $p$ πρώτος και $\nu \in \mathbb{N}$. Εάν οι $p^{k_1}, p^{k_2}, \ldots, p^{k_s}$ είναι οι στοιχειώδεις διαιρέτες τής $G$, τότε τα ακόλουθα είναι ισοδύναμα:*

(i) *$\exists H \in \mathbf{Subg}(G) \smallsetminus \{\{e_G\}\}$ με τους $p^{l_1}, p^{l_2}, \ldots, p^{l_t}$ ως στοιχειώδεις διαιρέτες της.*

(ii) *$t \leq s$ και $l_1 \leq k_{s-t+1}, l_2 \leq k_{s-t+2}, \ldots, l_t \leq k_s$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Έστω $H \in \mathbf{Subg}(G) \smallsetminus \{\{e_G\}\}$ έχουσα ως στοιχειώδεις διαιρέτες της τους $p^{l_1}, p^{l_2}, \ldots, p^{l_t}$, όπου $t \in \mathbb{N}$ και $(l_1, \ldots, l_t) \in \mathbb{N}^t$ με $l_1 + \cdots + l_t \leq \nu$. Επειδή $H[p] \sqsubseteq G[p]$, το λήμμα 9.2.1 (εφαρμοζόμενο για αμφότερες τις $G$ και $H$) δίδει $|H[p]| = p^t \mid p^s = |G[p]|$, οπότε $t \leq s$. Θα αποδείξουμε ότι οι λοιπές ανισοϊσότητες ικανοποιούνται κάνοντας χρήση μαθηματικής επαγωγής ως προς τον $\nu$. Όταν $\nu = 1$, τούτο είναι προφανές (καθώς $H = G$). Έστω ότι $\nu \geq 2$ και ότι ο ισχυρισμός είναι αληθής για κάθε πεπερασμένη αβελιανή ομάδα τάξεως $p^\xi$ όπου $\xi \in \mathbb{N}, \xi < \nu$.

*Περίπτωση πρώτη.* Εάν $G[p] = G$, τότε $k_1 = \cdots = k_s = 1$, $s = \nu$ και $H[p] \sqsubseteq G[p]$, οπότε[12] $l_1 = \cdots = l_t = 1$.

*Περίπτωση δεύτερη.* Εάν $G[p] \sqsubset G$ και $l_1 = \cdots = l_t = 1$, τότε οι λοιπές ανισοϊσότητες ικανοποιούνται *αυτομάτως*, διότι $k_{s-t+1} \geq 1, \ldots, k_s \geq 1$.

*Περίπτωση τρίτη.* Εάν η $G[p]$ είναι *γνήσια* υποομάδα τής $G$ και τουλάχιστον ένας εκ των $l_1, \ldots, l_t$ είναι $> 1$, τότε θέτουμε

$$s' := \operatorname{card}(\{j \in \mathbb{N} \,|\, j \in \{1, \ldots, s\} : k_j = 1\}), t' := \operatorname{card}(\{j \in \mathbb{N} \,|\, j \in \{1, \ldots, t\} : l_j = 1\}),$$

[11] Υπενθύμιση συμβολισμού: Για *κάθε* ομάδα $G$, $\mathbf{CSubg}(G) := \{\, H \in \mathbf{Subg}(G) \,|\, H \text{ κυκλική}\}$. (Βλ. 2.2.15.)

[12] Η $G[p] = G$ είναι ισόμορφη τής $\underbrace{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{s \text{ φορές}}$ τόσον ως ομάδα όσον και ως $\mathbb{Z}_p$-διανυσματικός χώρος. (Βλ. 9.1.5 (i).) Άρα η $H[p]$ (ως γραμμικός υπόχωρός της) είναι ισόμορφη τής $\underbrace{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{t \text{ φορές}}$.

όπου $s' \in \{0, 1, ..., s-1\}$ και $t' \in \{0, 1, ..., t-1\}$. Προφανώς, $pH \sqsubseteq pG$, με την $pH$ έχουσα ως στοιχειώδεις διαιρέτες της τους[13] $p^{l_{t'+1}-1}$,..., $p^{l_t-1}$ και με την $pG$ έχουσα ως στοιχειώδεις διαιρέτες της τους $p^{k_{s'+1}-1}$,..., $p^{k_s-1}$. Επειδή

$$|pG| = p^{(k_{s'+1}-1)+\cdots+(k_s-1)} < |G| = p^{\nu},$$

έχουμε τη δυνατότητα εφαρμογής τής επαγωγικής υποθέσεως για τις $pH$ και $pG$. Βάσει αυτής, $t - t' \leq s - s'$ και

$$\begin{array}{rcl} l_t - 1 \leq k_s - 1 & \Rightarrow & 1 < l_t \leq k_s, \\ l_{t-1} - 1 \leq k_{s-1} - 1 & \Rightarrow & 1 < l_{t-1} \leq k_{s-1}, \\ \vdots & & \vdots \\ l_{t'+1} - 1 \leq k_{s-(t-t')+1} - 1 & \Rightarrow & 1 < l_{t'+1} \leq k_{s-(t-t')+1}. \end{array}$$

Επειδή $l_1 = \cdots = l_{t'} = 1 = k_1 = \cdots = k_{s'}$, αρκεί να δειχθεί ότι $s' \leq t'$. Ας υποθέσουμε ότι $s' > t'$. Τότε $t - t' > t - s' \Rightarrow s - (t - t') + 1 < s - (t - s') + 1$, οπότε $1 < l_{t'+1} \leq k_{s-(t-t')+1} \leq k_{s-(t-s')+1} \Rightarrow s - (t - s') + 1 < s' + 1 \Rightarrow t > s$. Άτοπο! Ως εκ τούτου, ο ισχυρισμός είναι αληθής *για κάθε* $\nu \geq 1$.

(ii)⇒(i) Εάν $t \in \{1, ..., s\}$ και $l_j \in \{1, ..., k_j\}, \forall j \in \{1, ..., t\}$, τότε $p^{l_1+\cdots+l_t} \mid p^{\nu}$ και η ύπαρξη υποομάδων τής $G$ τάξεως $p^{l_1+\cdots+l_t}$ είναι εξασφαλισμένη από το θεώρημα 4.4.22. Το ότι τουλάχιστον μία εξ αυτών έχει τους $p^{l_1}$,..., $p^{l_t}$ ως στοιχειώδεις διαιρέτες της είναι προφανές (λόγω τής προτάσεως 9.1.8 *για την* $G$, τού (i) τού θεωρήματος 2.3.21 και τού (iii) τής προτάσεως 7.1.57). □

► **Αναλλοίωτοι παράγοντες υποομάδων**. Το αντίστοιχο θεώρημα περί των αναλλοιώτων παραγόντων των υποομάδων *τυχουσών* πεπερασμένων μη τετριμμένων αβελιανών ομάδων είναι το 9.2.4.

**9.2.3 Λήμμα.** *Εάν* $(G, +)$ *είναι μια πεπερασμένη κυκλική ομάδα και* $n \in \mathbb{N}$, *τότε*

$$nG = \{0_G\} \Longleftrightarrow |G| \mid n.$$

ΑΠΟΔΕΙΞΗ. "⇒" Επειδή η $(G, +)$ είναι πεπερασμένη και κυκλική, υπάρχει κάποιο $g \in G$, τέτοιο ώστε $G = \langle g \rangle$ με $\mathrm{ord}(g) = |G|$. (Βλ. πρόταση 2.3.7.) Εάν λοιπόν υποτεθεί ότι $nG = \{0_G\}$, για κάποιον $n \in \mathbb{N}$, τότε $ng = 0_G \underset{2.3.8}{\Longrightarrow} \mathrm{ord}(g) = |G| \mid n$.

"⇐" Εάν $|G| \mid n$, τότε *για κάθε* $x \in G$ έχουμε $nx = \frac{n}{|G|}(|G|\,x) \underset{4.1.28}{=} \frac{n}{|G|}0_G = 0_G$, οπότε $nG = \{0_G\}$. □

**9.2.4 Θεώρημα.** *Έστω* $(G, +)$ *μια πεπερασμένη μη τετριμμένη αβελιανή ομάδα. Εάν οι* $m_1, m_2$,..., $m_s$ *είναι οι αναλλοίωτοι παράγοντες τής* $G$ (βλ. 9.1.26), *τότε τα ακόλουθα είναι ισοδύναμα*:

(i) $\exists H \in \mathbf{Subg}(G) \smallsetminus \{\{e_G\}\}$ *με τους* $n_1, n_2, ..., n_r$ *ως αναλλοίωτους παράγοντές της.*

(ii) $r \leq s$ *και* $n_{r-j+1} \mid m_{s-j+1}$ *για κάθε* $j \in \{1, ..., r\}$.

[13] $pH \cong (p\mathbb{Z}_{p^{l_1}}) \oplus \cdots \oplus (p\mathbb{Z}_{p^{l_s}}) \cong (p\mathbb{Z}_{p^{l_{t'+1}}}) \oplus \cdots \oplus (p\mathbb{Z}_{p^{l_t}}) \cong \mathbb{Z}_{p^{l_{t'+1}-1}} \oplus \cdots \oplus \mathbb{Z}_{p^{l_t-1}}$.

Απόδειξη. (i)⇒(ii) Έστω $H \in \mathbf{Subg}(G)\smallsetminus\{\{e_G\}\}$ έχουσα ως αναλλοίωτους παράγοντές της τους $n_1, n_2, ..., n_r$ ($r \in \mathbb{N}$). Θα εργασθούμε με «εις άτοπον απαγωγή». Υποθέτουμε ότι ο ισχυρισμός είναι εσφαλμένος. Τότε *είτε* υπάρχει κάποιος δείκτης $j_\bullet \in \{1, ..., r\}$ με $n_{r-j_\bullet+1} \nmid m_{s-j_\bullet+1}$ *είτε* $r > s$.

*Περίπτωση πρώτη.* Έστω ότι $\exists j_\bullet \in \{1, ..., r\} : n_{r-j_\bullet+1} \nmid m_{s-j_\bullet+1}$. Θέτουμε $l := \left|m_{s-j_\bullet+1}\mathbb{Z}_{n_{r-j_\bullet+1}}\right|$. Κατά το λήμμα 9.2.3, $l > 1$. Εν συνεχεία, θέτουμε

$$\breve{G} := m_{s-j_\bullet+1}G[l] = \{y \in m_{s-j_\bullet+1}G \,|ly = 0_G\}\,.$$

Επειδή $H \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r}$, με $n_\xi \mid n_{\xi+1}$, $\forall \xi \in \{1, ..., r-1\}$, η $H$ περιέχει μια υποομάδα $K_i \cong \mathbb{Z}_{n_{r-j_\bullet+1}}$ για κάθε $i \in \{r - j_\bullet + 1, ..., r\}$, διότι[14] $n_{r-j_\bullet+1} \mid n_i$. Κατά συνέπειαν,

$$\begin{aligned} &K_i \cong \mathbb{Z}_{n_{r-j_\bullet+1}} \Rightarrow m_{s-j_\bullet+1}K_i \cong m_{s-j_\bullet+1}\mathbb{Z}_{n_{r-j_\bullet+1}} \\ &\underset{9.2.3}{\Longrightarrow} \left[\begin{array}{c} \text{η } l(m_{s-j_\bullet+1}K_i) \cong l(m_{s-j_\bullet+1}\mathbb{Z}_{n_{r-j_\bullet+1}}) \\ \text{είναι τετριμμένη} \end{array}\right], \end{aligned}$$

οπότε $m_{s-j_\bullet+1}K_i \sqsubseteq \breve{G}$, $\forall i \in \{r - j_\bullet + 1, ..., r\}$, και

$$(m_{s-j_\bullet+1}K_{r-j_\bullet+1}) \oplus_{\text{εσ.}} (m_{s-j_\bullet+1}K_{r-j_\bullet+2}) \oplus_{\text{εσ.}} \cdots \oplus_{\text{εσ.}} (m_{s-j_\bullet+1}K_r) \sqsubseteq \breve{G}.$$

Εξ αυτού έπεται ότι η $(m_{s-j_\bullet+1}K_{r-j_\bullet+1}) \oplus_{\text{εσ.}} \cdots \oplus_{\text{εσ.}} (m_{s-j_\bullet+1}K_r)$ έχει τάξη

$$\left|\bigoplus_{i=r-j_\bullet+1}^{r}(m_{s-j_\bullet+1}K_i)\right| = \prod_{i=r-j_\bullet+1}^{r}|m_{s-j_\bullet+1}K_i| = l^{r-(r-j_\bullet+1)+1} = l^{j_\bullet} \leq \left|\breve{G}\right|, \quad (9.25)$$

καθόσον $|m_{s-j_\bullet+1}K_i| = l$, $\forall i \in \{r - j_\bullet + 1, ..., r\}$. Από την άλλη μεριά, επειδή

$$G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s}, \text{ με } m_\nu \mid m_{\nu+1}, \ \forall \nu \in \{1, ..., s-1\},$$

το λήμμα 9.1.6 μας πληροφορεί ότι

$$m_{s-j_\bullet+1}G \cong (m_{s-j_\bullet+1}\mathbb{Z}_{m_1}) \oplus (m_{s-j_\bullet+1}\mathbb{Z}_{m_2}) \oplus \cdots \oplus (m_{s-j_\bullet+1}\mathbb{Z}_{m_s}),$$

όπου $m_{s-j_\bullet+1}\mathbb{Z}_{m_{s-j+1}} = \{[0]_{m_{s-j+1}}\}$ για κάθε $j \in \{j_\bullet, j_\bullet + 1, ..., s\}$, αφού $m_{s-j+1} \mid m_{s-j_\bullet+1}$. (Βλ. 9.2.3.) Επομένως, *είτε* $j_\bullet = 1$ και $m_sG = \{0_G\}$ *είτε* $j_\bullet > 1$ και

$$m_{s-j_\bullet+1}G \cong (m_{s-j_\bullet+1}\mathbb{Z}_{m_{s-j_\bullet+2}}) \oplus (m_{s-j_\bullet+1}\mathbb{Z}_{m_{s-j_\bullet+3}}) \oplus \cdots \oplus (m_{s-j_\bullet+1}\mathbb{Z}_{m_s}).$$

(Πρβλ. 7.1.55 (iv).) Εάν $j_\bullet = 1$ και $m_sG = \{0_G\}$, τότε $\breve{G} = \{0_G\} \Rightarrow \left|\breve{G}\right| = 1$, πράγμα *άτοπο*, διότι $\left|\breve{G}\right| \geq l > 1$. (Βλ. (9.25).) Άρα $j_\bullet > 1$. Έστω

$$f : m_{s-j_\bullet+1}G \xrightarrow{\cong} m_{s-j_\bullet+1}\mathbb{Z}_{m_{s-j_\bullet+2}} \oplus \cdots \oplus m_{s-j_\bullet+1}\mathbb{Z}_{m_s}$$

[14]Για κάθε θετικό ακέραιο διαιρέτη τής τάξεως μιας πεπερασμένης κυκλικής ομάδας υφίσταται μία (κατ' ανάγκην κυκλική) υποομάδα αυτής έχουσα ως τάξη της τον θεωρούμενο διαιρέτη. (Βλ. θεώρημα 2.3.21.)

ένας ισομορφισμός. Θεωρούμε τυχόν στοιχείο $x \in \breve{G}$. Η εικόνα του μέσω τού $f$ γράφεται ως $f(x) = x_1 + x_2 + \cdots + x_{j_\bullet - 1}$ για κάποια (μονοσημάντως ορισμένα)

$$x_1 \in m_{s-j_\bullet+1}\mathbb{Z}_{m_{s-j_\bullet+2}},\ x_2 \in m_{s-j_\bullet+1}\mathbb{Z}_{m_{s-j_\bullet+3}},\ ...,\ x_{j_\bullet-1} \in m_{s-j_\bullet+1}\mathbb{Z}_{m_s}.$$

Εξ αυτού έπεται ότι

$$0_G = lx \Rightarrow f(0_G) = lx_1 + \cdots + lx_{j_\bullet-1} \Rightarrow lx_1 = \cdots = lx_{j_\bullet-1} = f(0_G),$$

ήτοι ότι $f^{-1}(x_1), f^{-1}(x_2), ..., f^{-1}(x_{j_\bullet-1}) \in \breve{G}$. Επομένως,

$$\breve{G} \sqsubseteq (f^{-1}(m_{s-j_\bullet+1}\mathbb{Z}_{m_{s-j_\bullet+2}}) \cap \breve{G}) \oplus \cdots \oplus (f^{-1}(m_{s-j_\bullet+1}\mathbb{Z}_{m_s}) \cap \breve{G}). \quad (9.26)$$

Επειδή η $m_{s-j_\bullet+1}\mathbb{Z}_{m_\varrho}$ (ως υποομάδα τής κυκλικής ομάδας $\mathbb{Z}_{m_\varrho}$) είναι κυκλική, τόσον η $f^{-1}(m_{s-j_\bullet+1}\mathbb{Z}_{m_\varrho})$ όσον και η τομή $f^{-1}(m_{s-j_\bullet+1}\mathbb{Z}_{m_\varrho}) \cap \breve{G}$ είναι κυκλική για κάθε $\varrho \in \{s - j_\bullet + 2, ..., s\}$. (Βλ. 2.4.19 (iii) και 2.2.19 (ii).) Μάλιστα, για οιονδήποτε γεννήτορα $g_\varrho$ τής $f^{-1}(m_{s-j_\bullet+1}\mathbb{Z}_{m_\varrho}) \cap \breve{G}$ έχουμε

$$lg_\varrho = 0_G \Rightarrow \left| f^{-1}(m_{s-j_\bullet+1}\mathbb{Z}_{m_\varrho}) \cap \breve{G} \right| \leq l,\ \forall \varrho \in \{s - j_\bullet + 2, ..., s\}. \quad (9.27)$$

Από τις (9.26) και (9.27) προκύπτει ότι

$$\left|\breve{G}\right| \leq l^{j_\bullet-1} \quad (9.28)$$

και από τις (9.25) και (9.28) ότι $l^{j_\bullet} \leq l^{j_\bullet-1}$, πράγμα *άτοπο*, διότι $l > 1$.

*Περίπτωση δεύτερη*. Εάν $r > s$, τότε η $H$ περιέχει μια υποομάδα $K_i \cong \mathbb{Z}_{n_{r-s}}$, για κάθε $i \in \{r - s, ..., r\}$, διότι $n_{r-s} \mid n_i$. Κατά το λήμμα 9.2.3, η $n_{r-s}K_i$ είναι τετριμμένη, οπότε $K_i \sqsubseteq G[n_{r-s}]$ για κάθε $i \in \{r - s, ..., r\}$ και

$$K_{r-s} \oplus_{\text{εσ.}} K_{r-s+1} \oplus_{\text{εσ.}} \cdots \oplus_{\text{εσ.}} K_r \sqsubseteq G[n_{r-s}] \Rightarrow n_{r-s}^{s+1} \leq |G[n_{r-s}]|\,. \quad (9.29)$$

Έστω $f : G \xrightarrow{\cong} \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s}$ ένας ισομορφισμός. Όπως και στην πρώτη περίπτωση δείχνουμε ότι

$$G[n_{r-s}] \sqsubseteq \bigoplus_{i=1}^{s}(f^{-1}(\mathbb{Z}_{m_i}) \cap G[n_{r-s}]) \Rightarrow |G[n_{r-s}]| \leq n_{r-s}^{s} \quad (9.30)$$

και από τις (9.29) και (9.30) οδηγούμεθα εκ νέου σε *άτοπο*.

(ii)⇒(i) Εάν οι $r$ και $n_1, n_2, ..., n_r$ ικανοποιούν τις αναγραφόμενες συνθήκες, τότε $\sum_{i=1}^{r} n_i \mid |G|$ και η ύπαρξη υποομάδων τής $G$ τάξεως $\sum_{i=1}^{r} n_i$ είναι εξασφαλισμένη από το θεώρημα 4.4.22. Το ότι τουλάχιστον μία εξ αυτών έχει τους $n_1, n_2, ..., n_r$ ως αναλλοίωτους παράγοντές της είναι προφανές (λόγω τού θεωρήματος 9.1.25 *για την* $G$, τού (i) τού θεωρήματος 2.3.21 και τού (iii) τής προτάσεως 7.1.57). □

**9.2.5 Παραδείγματα.** Η ομάδα $\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4$ δεν μπορεί να είναι ισόμορφη με κάποια υποομάδα τής ομάδας $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8$. Παρομοίως, η $\mathbb{Z}_3 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{27}$ δεν μπορεί να είναι ισόμορφη με κάποια υποομάδα τής $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{27} \oplus \mathbb{Z}_{27}$.

►**Υπολογισμός αριθμού κυκλικών υποομάδων**. Ο αριθμός των (κατ' ανάγκην κυκλικών) υποομάδων μιας πεπερασμένης κυκλικής ομάδας $G$ ισούται με[15] τον $\mathrm{card}(\mathfrak{D}_{|G|})$. (Βλ. 2.4.26 (ii).) Η μέθοδος προσδιορισμού τού αριθμού των κυκλικών υποομάδων μιας πεπερασμένης αβελιανής ομάδας είναι κατά τι πιο σύνθετη. Ας υποθέσουμε ότι οι $n_1, ..., n_r$ είναι *τυχόντες* φυσικοί αριθμοί ($r \in \mathbb{N}$). Θέτοντας

$$\mathbf{c}(n_1, ..., n_r) := \mathrm{card}(\mathbf{CSubg}(\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r})),$$

$$\mathbf{c}_\delta(n_1, ..., n_r) := \mathrm{card}(\{H \in \mathbf{CSubg}(\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}) : |H| = \delta\}),$$

$$\mathbf{o}_\delta(n_1, ..., n_r) := \mathrm{card}(\{x \in \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r} : \mathrm{ord}(x) = \delta\}),$$

(όπου $\delta \in \mathbb{N} : 1 \leq \delta \leq n_1 \cdots n_r$) παρατηρούμε ότι

$$\mathbf{c}_\delta(n_1, ..., n_r) = \frac{\mathbf{o}_\delta(n_1, ..., n_r)}{\phi(\delta)}, \tag{9.31}$$

όπου $\phi$ η συνάρτηση φι τού Euler (βλ. B.4.15), διότι κάθε κυκλική ομάδα τάξεως $\delta$ διαθέτει $\phi(\delta)$ γεννήτορες. (Βλ. πόρισμα 2.3.17.) Εξάλλου, επειδή για κάθε ομάδα $H \in \mathbf{CSubg}(\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r})$ τάξεως $|H| = \delta$ ισχύει

$$\delta \underset{9.1.34}{=} \exp(H) \mid \exp(\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}) \underset{7.1.61}{=} \text{εκπ}(n_1, ..., n_r)$$

(βλ. 2.3.25 (iii)), συμπεραίνουμε ότι

$$\mathbf{c}(n_1, ..., n_r) = \sum_{\delta \in \mathfrak{D}_{\text{εκπ}(n_1, ..., n_r)}} \mathbf{c}_\delta(n_1, ..., n_r). \tag{9.32}$$

Μέσω τού κάτωθι θεωρήματος 9.2.7 τού László Tóth[16] (τού βασιζόμενου στο λήμμα 9.2.6) ο $\mathbf{c}(n_1, ..., n_r)$ μπορεί να υπολογισθεί με τη βοήθεια τής συναρτήσεως $\phi$ και των θετικών ακεραίων διαιρετών των $n_1, ..., n_r$.

**9.2.6 Λήμμα.** *Για κάθε $\delta \in \mathfrak{D}_{\text{εκπ}(n_1, ..., n_r)}$ ισχύουν οι ισότητες*

$$\begin{aligned} \mathbf{o}_\delta(n_1, ..., n_r) &= \sum_{\varepsilon \in \mathfrak{D}_\delta} \mu\left(\frac{\delta}{\varepsilon}\right) \text{μκδ}(\varepsilon, n_1) \cdots \text{μκδ}(\varepsilon, n_r) &(9.33)\\ &= \sum_{d_1 \in \mathfrak{D}_{n_1}, ..., d_r \in \mathfrak{D}_{n_r} \text{ με } \text{εκπ}(d_1, ..., d_r) = \delta} \phi(d_1) \cdots \phi(d_r), &(9.34) \end{aligned}$$

*όπου $\mu$ η συνάρτηση μι τού Möbius.* (Βλ. B.4.32.)

ΑΠΟΔΕΙΞΗ. Εάν $x := ([a_1]_{n_1}, ..., [a_r]_{n_r}) \in \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ και $n := \text{εκπ}(n_1, ..., n_r)$, τότε

$$\mathrm{ord}(x) \underset{7.1.60}{=} \text{εκπ}\left(\tfrac{n_1}{\text{μκδ}(n_1, a_1)}, ..., \tfrac{n_r}{\text{μκδ}(n_r, a_r)}\right)$$

$$= \text{εκπ}\left(\frac{n}{\text{μκδ}\left(n_1, \frac{a_1 n}{n_1}\right)}, ..., \frac{n}{\text{μκδ}\left(n_r, \frac{a_r n}{n_r}\right)}\right) = \frac{n}{\text{μκδ}\left(\frac{a_1 n}{n_1}, ..., \frac{a_r n}{n_r}, n\right)}.$$

[15] Υπενθύμιση συμβολισμού: Για κάθε $n \in \mathbb{N}$, $\mathfrak{D}_n := \{d \in \mathbb{N} : d \mid n\}$. (Βλ. B.2.34.)

[16] L. Tóth: *On the number of cyclic subgroups of a finite abelian group*, Bull. Math. Soc. Sci. Math. Roumanie, Tome **55** (103) No. 4, (2012), 423-428.

Όπως προαναφέραμε, $\mathrm{ord}(x) = \delta$ για κάποιον $\delta \in \mathfrak{D}_n$. Για *παγιωμένον* $\delta \in \mathfrak{D}_n$ λαμβάνουμε

$$\text{μκδ}\left(\tfrac{a_1 n}{n_1}, ..., \tfrac{a_r n}{n_r}, n\right) = \tfrac{n}{\delta} \Rightarrow \left[\exists \rho_i \in \mathbb{Z} : \tfrac{a_i n}{n_i} = \tfrac{\rho_i n}{\delta},\ \forall i \in \{1, ..., r\}\right]$$

με $\rho_i = \frac{\delta a_i}{n_i}$, οπότε $\text{μκδ}(\rho_1, ..., \rho_r, \delta) = 1$ (βλ. B.2.14 (ii)) και $\delta a_i \equiv 0 (\operatorname{mod} n_i)$, έχουσα ως λύσεις της κατά μόδιο $n_i$ τις $a_i = \frac{\lambda_i n_i}{\text{μκδ}(\delta, n_i)}$, $\lambda_i \in \{1, ..., \text{μκδ}(\delta, n_i)\}$, για κάθε $i \in \{1, ..., r\}$. (Βλ. B.4.45 και B.4.46.) Κατ' αυτόν τον τρόπο προκύπτει η αμφίρριψη

$$\left\{ \begin{array}{c} x \in \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r} \\ \text{με } \mathrm{ord}(x) = \delta \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} (\lambda_1, ..., \lambda_r) \in \mathbb{N}^r : \\ \text{(i) } \lambda_i \leq \text{μκδ}\,(\delta, n_i)\,, \forall i \in \{1, ..., r\}, \\ \text{(ii) μκδ}\left(\frac{\lambda_1 \delta}{\text{μκδ}(\delta, n_1)}, ..., \frac{\lambda_r \delta}{\text{μκδ}(\delta, n_r)}, \delta\right) = 1. \end{array} \right\}$$

Σημειωτέον ότι για οιαδήποτε $r$-άδα $(\lambda_1, ..., \lambda_r) \in \mathbb{N}^r$ με την ιδιότητα (i) έχουμε

$$\mathfrak{D}_{\text{μκδ}(\lambda_1\delta/\text{μκδ}(\delta,n_1),...,\lambda_r\delta/\text{μκδ}(\delta,n_r),\delta)} = \mathfrak{D}_\delta \cap \mathfrak{D}_{\lambda_1\delta/\text{μκδ}(\delta,n_1)} \cap \cdots \cap \mathfrak{D}_{\lambda_r\delta/\text{μκδ}(\delta,n_r)}$$

(βλ. B.2.37) και, σε ό,τι αφορά στη (ii),

$$\text{μκδ}\left(\tfrac{\lambda_1 \delta}{\text{μκδ}(\delta, n_1)}, ..., \tfrac{\lambda_r \delta}{\text{μκδ}(\delta, n_r)}, \delta\right) = 1 \underset{\text{B.4.33}}{\Longleftrightarrow} \sum_{\varepsilon \in \mathfrak{D}_{\text{μκδ}(\lambda_1\delta/\text{μκδ}(\delta,n_1),...,\lambda_r\delta/\text{μκδ}(\delta,n_r),\delta)}} \mu\,(\varepsilon) = 1.$$

Ως εκ τούτου, ο ζητούμενος αριθμός μπορεί να εκφρασθεί ως ακολούθως:

$$\begin{aligned} \mathbf{o}_\delta(n_1, ..., n_r) &= \sum_{\lambda_1=1}^{\text{μκδ}(\delta,n_1)} \cdots \sum_{\lambda_r=1}^{\text{μκδ}(\delta,n_r)} \sum_{\varepsilon \in \mathfrak{D}_{\text{μκδ}(\lambda_1\delta/\text{μκδ}(\delta,n_1),...,\lambda_r\delta/\text{μκδ}(\delta,n_r),\delta)}} \mu\,(\varepsilon) \\ &= \sum_{\varepsilon \in \mathfrak{D}_\delta} \mu\,(\varepsilon) \sum_{\varepsilon \in \mathfrak{D}_{\lambda_1\delta/\text{μκδ}(\delta,n_1)},\ \lambda_1 \leq \text{μκδ}(\delta,n_1)} \cdots \sum_{\varepsilon \in \mathfrak{D}_{\lambda_r\delta/\text{μκδ}(\delta,n_r)},\ \lambda_r \leq \text{μκδ}(\delta,n_r)} 1. \end{aligned}$$

Προφανώς, $\varepsilon \in \mathfrak{D}_{\lambda_i\delta/\text{μκδ}(\delta,n_i)} \Leftrightarrow \frac{\delta}{\text{μκδ}(\delta,n_i)}\lambda_i \equiv 0 (\operatorname{mod} \varepsilon)$ και αυτή η ισοτιμία διαθέτει $\text{μκδ}\left(\frac{\delta}{\text{μκδ}(\delta,n_i)}, \varepsilon\right)$ λύσεις (ως προς τον $\lambda_i$) κατά μόδιο $\varepsilon$. Συγκεκριμένα, τις

$$\lambda_i = \frac{\lambda_i' \varepsilon}{\text{μκδ}\left(\frac{\delta}{\text{μκδ}(\delta,n_i)}, \varepsilon\right)},\ \ \lambda_i' \in \left\{1, ..., \text{μκδ}\left(\tfrac{\delta}{\text{μκδ}(\delta,n_i)}, \varepsilon\right)\right\}.$$

(Βλ. B.4.45 και B.4.46.) Η αξίωση για τον περιορισμό μας μόνον σε όσες εκ των $\text{μκδ}\left(\frac{\delta}{\text{μκδ}(\delta,n_i)}, \varepsilon\right)$ λύσεων ανήκουν στο σύνολο $\{1, ..., \text{μκδ}(\delta, n_i)\}$ μας οδηγεί στις σχέσεις

$$\frac{\lambda_i' \varepsilon}{\text{μκδ}\left(\frac{\delta}{\text{μκδ}(\delta,n_i)}, \varepsilon\right)} \leq \text{μκδ}\,(\delta, n_i) \Rightarrow 1 \leq \lambda_i' \leq \tfrac{\text{μκδ}(\delta,n_i)}{\varepsilon} \text{μκδ}\left(\tfrac{\delta}{\text{μκδ}(\delta,n_i)}, \varepsilon\right).$$

Άρα για κάθε $i \in \{1, ..., r\}$ το άθροισμα $\sum\limits_{\varepsilon \in \mathfrak{D}_{\lambda_i \delta / \text{μκδ}(\delta, n_i)},\ \lambda_i \leq \text{μκδ}(\delta, n_i)} 1$ ισούται με

$$\frac{\text{μκδ}(\delta, n_i)}{\varepsilon} \text{μκδ}\left(\frac{\delta}{\text{μκδ}(\delta, n_i)}, \varepsilon\right) \underset{\text{B.2.14 (i)}}{=} \text{μκδ}\left(\tfrac{\delta}{\varepsilon}, \text{μκδ}\left(\delta, n_i\right)\right)$$
$$\underset{\text{B.2.16}}{=} \text{μκδ}\left(\tfrac{\delta}{\varepsilon}, \delta, n_i\right) = \text{μκδ}\left(\tfrac{\delta}{\varepsilon}, n_i\right).$$

Γι' αυτόν τον λόγο,

$$\begin{aligned} \mathbf{o}_\delta(n_1, ..., n_r) &= \sum_{\varepsilon \in \mathfrak{D}_\delta} \mu(\varepsilon)\ \text{μκδ}\left(\frac{\delta}{\varepsilon}, n_1\right) \cdots \text{μκδ}\left(\frac{\delta}{\varepsilon}, n_r\right) \\ &= \sum_{\varepsilon \in \mathfrak{D}_\delta} \mu\left(\frac{\delta}{\varepsilon}\right) \text{μκδ}\left(\varepsilon, n_1\right) \cdots \text{μκδ}\left(\varepsilon, n_r\right) \end{aligned}$$

και η (9.33) είναι αληθής[17]. Από την άλλη μεριά, σύμφωνα με την πρόταση B.4.31,

$$\text{μκδ}\left(\varepsilon, n_i\right) = \sum_{d_i \in \mathfrak{D}_{\text{μκδ}(\varepsilon, n_i)}} \phi\left(d_i\right) \underset{\text{B.2.37}}{=} \sum_{d_i \in \mathfrak{D}_\varepsilon \cap \mathfrak{D}_{n_i}} \phi\left(d_i\right),\ \forall i \in \{1, ..., r\},$$

οπότε[18]

$$\begin{aligned} \mathbf{o}_\delta(n_1, ..., n_r) &= \sum_{\varepsilon \in \mathfrak{D}_\delta} \mu\left(\frac{\delta}{\varepsilon}\right) \left(\sum_{d_1 \in \mathfrak{D}_\varepsilon \cap \mathfrak{D}_{n_1}} \phi\left(d_1\right)\right) \cdots \left(\sum_{d_r \in \mathfrak{D}_\varepsilon \cap \mathfrak{D}_{n_r}} \phi\left(d_r\right)\right) \\ &= \sum_{d_1 \in \mathfrak{D}_{n_1}, ..., d_r \in \mathfrak{D}_{n_r}} \phi(d_1) \cdots \phi(d_r) \sum_{a \in \mathfrak{D}_{\frac{\delta}{\text{εκπ}(d_1, ..., d_r)}}} \mu\left(a\right), \end{aligned}$$

όπου το δεύτερο άθροισμα στην τελευταία παράσταση τού $\mathbf{o}_\delta(n_1, ..., n_r)$ είναι $= 1$ όταν εκπ$(d_1, ..., d_r) = \delta$ και $= 0$ όταν εκπ$(d_1, ..., d_r) \neq \delta$. (Βλ. πρόταση B.4.33.) Εξ αυτού εξάγεται η (9.34). □

**9.2.7 Θεώρημα.** **(L. Tóth,** 2012.) *Η ομάδα* $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ *διαθέτει*

$$\boxed{\mathbf{c}(n_1, ..., n_r) = \sum_{d_1 \in \mathfrak{D}_{n_1}, ..., d_r \in \mathfrak{D}_{n_r}} \frac{\phi(d_1) \cdots \phi(d_r)}{\phi(\text{εκπ}(d_1, ..., d_r))}} \qquad (9.35)$$

*κυκλικές υποομάδες.*

ΑΠΟΔΕΙΞΗ. Η (9.35) προκύπτει από τις (9.32), (9.31) και (9.34). □

Όταν $r = 2$ η (9.35) απλουστεύεται ως ακολούθως:

[17] Όταν ο $\varepsilon$ διατρέχει *όλους* τους θετικούς ακέραιους διαιρέτες τού $\delta$, τότε ο $\frac{\delta}{\varepsilon}$ διατρέχει ωσαύτως *όλους* τους θετικούς ακέραιους διαιρέτες τού $\delta$. Με άλλα λόγια, η απεικόνιση $\mathfrak{D}_\delta \ni \varepsilon \longmapsto \frac{\delta}{\varepsilon} \in \mathfrak{D}_\delta$ είναι αμφιρριπτική. Εξ ου και η τελευταία ισότητα.

[18] Αιτιολόγηση τής δεύτερης ισότητας: Έστω $\varepsilon \in \mathfrak{D}_\delta$. Εάν $d_1 \mid \varepsilon, \ldots, d_r \mid \varepsilon$, τότε εκπ$(d_1, \ldots, d_r) \mid \varepsilon$. (Βλ. B.2.25 (ii).) Επομένως, $\exists m \in \mathbb{N}$: $\varepsilon =$ εκπ$(d_1, \ldots, d_r)m$ και $\frac{\delta}{\text{εκπ}(d_1, \ldots, d_r)} = \frac{\delta}{\varepsilon} m \Rightarrow \frac{\delta}{\varepsilon} \in \mathfrak{D}_{\frac{\delta}{\text{εκπ}(d_1, \ldots, d_r)}}$.

**9.2.8 Πόρισμα.** *Ο αριθμός των κυκλικών υποομάδων τής* $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ *είναι ο*

$$\boxed{\mathbf{c}(n_1, n_2) = \sum_{d_1 \in \mathfrak{D}_{n_1},\, d_2 \in \mathfrak{D}_{n_2}} \phi(\text{μκδ}(d_1, d_2)).}$$

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το θεώρημα 9.2.7 και το πόρισμα Β.4.30. □

**9.2.9 Παράδειγμα.** Η αβελιανή ομάδα $\mathbb{Z}_4 \oplus \mathbb{Z}_{12}$ (τάξεως 48) διαθέτει

$$\begin{aligned}
\mathbf{c}(4, 12) &= \sum_{d_1 \in \{1,2,4\},\, d_2 \in \{1,2,3,4,6,12\}} \phi(\text{μκδ}(d_1, d_2)) \\
&= \sum_{i \in \{1,2,3,4,6,12\}} \phi(\text{μκδ}(1, i)) + \sum_{i \in \{1,2,3,4,6,12\}} \phi(\text{μκδ}(2, i)) + \sum_{i \in \{1,2,3,4,6,12\}} \phi(\text{μκδ}(4, i)) \\
&= 6\phi(1) + (2\phi(1) + 4\phi(2)) + (2\phi(1) + 2\phi(2) + 2\phi(4)) \\
&= 10\phi(1) + 6\phi(2) + 2\phi(4) = 20
\end{aligned}$$

κυκλικές υποομάδες.

**9.2.10 Πόρισμα.** *Εάν* $p$ *είναι ένας πρώτος αριθμός και* $n_1 = p^{\alpha_1}, ..., n_r = p^{\alpha_r}$ *για κάποιους* $\alpha_1, ..., \alpha_r \in \mathbb{N}$, *τότε*

$$\mathbf{c}(p^{\alpha_1}, ..., p^{\alpha_r}) = \sum_{j=0}^{\max\{\alpha_1, ..., \alpha_r\}} \mathbf{c}_{p^j}(p^{\alpha_1}, ..., p^{\alpha_r}), \tag{9.36}$$

*όπου για κάθε*[19] $j \in \{1, ..., \max\{\alpha_1, ..., \alpha_r\}\}$,

$$\mathbf{c}_{p^j}(p^{\alpha_1}, ..., p^{\alpha_r}) = \tfrac{1}{p^{j-1}(p-1)} \left( p^{\sum_{\kappa=1}^{r} \min\{j, \alpha_\kappa\}} - p^{\sum_{\kappa=1}^{r} \min\{j-1, \alpha_\kappa\}} \right). \tag{9.37}$$

ΑΠΟΔΕΙΞΗ. Επειδή κάθε $\delta \in \mathbb{N}$ με $\delta \mid \text{εκπ}(p^{\alpha_1}, ..., p^{\alpha_r}) \underset{\text{B.3.20}}{=} p^{\max\{\alpha_1, ..., \alpha_r\}}$ είναι τής μορφής $\delta = p^j$, για κάποιον $j \in \{0, 1, ..., \max\{\alpha_1, ..., \alpha_r\}\}$ (βλ. Β.3.14), η (9.36) προκύπτει άμεσα από την (9.32). Τώρα για κάθε $j \in \{1, ..., \max\{\alpha_1, ..., \alpha_r\}\}$ η (9.33) δίδει

$$\begin{aligned}
\mathbf{c}_{p^j}(p^{\alpha_1}, ..., p^{\alpha_r}) &\underset{(9.31)}{=} \frac{\mathbf{o}_{p^j}(p^{\alpha_1}, ..., p^{\alpha_r})}{\phi(p^j)} \\
&\underset{\text{B.4.19}}{=} \tfrac{1}{p^{j-1}(p-1)} \sum_{i=0}^{j} \mu\left(p^{j-i}\right) \text{μκδ}(p^i, p^{\alpha_1}) \cdots \text{μκδ}(p^i, p^{\alpha_r}).
\end{aligned}$$

Επειδή $\text{μκδ}(p^i, p^{\alpha_\kappa}) \underset{\text{B.3.16}}{=} p^{\min\{i, \alpha_\kappa\}}$ για κάθε $(i, \kappa) \in \{0, 1, ..., j\} \times \{1, ..., r\}$ και

$$\mu\left(p^{j-i}\right) \underset{\text{B.4.32}}{=} \begin{cases} 1, & \text{όταν } i = j, \\ -1, & \text{όταν } i = j - 1, \\ 0, & \text{όταν } i \leq j - 2, \end{cases}$$

[19] Όταν $j = 0$, τότε $\mathbf{c}_1(p^{\alpha_1}, ..., p^{\alpha_r}) = 1$, καθώς η μόνη υποομάδα τής $\mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}$ τάξεως 1 είναι η τετριμμένη.

η (9.37) είναι προφανής. □

Ο αριθμός των κυκλικών υποομάδων *τυχούσας* πεπερασμένης μη τετριμμένης αβελιανής ομάδας ισούται με το γινόμενο των αριθμών των κυκλικών υποομάδων καθεμιάς εκ των πρωτευουσών συνιστωσών της. (Βλ. (9.24).) Επομένως, εάν ληφθεί υπ' όψιν η πρωτεύουσα αποσύνθεσή της, είναι αρκετό (για τον υπολογισμό του) να χρησιμοποιηθεί το επόμενο πόρισμα.

**9.2.11 Πόρισμα.** *Έστω $p$ ένας πρώτος αριθμός και έστω $(G,+)$ μια πεπερασμένη μη τετριμμένη αβελιανή $p$-ομάδα. Τότε ισχύουν τα ακόλουθα:*

(i) *Εάν η $G$ είναι τού τύπου $(\underbrace{k,k,\ldots,k}_{s \text{ φορές}})$, $s \geq 1$, τότε*

$$\boxed{\operatorname{card}(\mathbf{CSubg}(G)) = 1 + \tfrac{p^s-1}{p-1} \sum_{j=1}^{k} p^{(s-1)(j-1)}.}$$

(ii) *Εάν η $G$ είναι τού τύπου $(k_1, k_2, \ldots, k_s)$, $s \geq 2$, και εάν τουλάχιστον δύο εκ των $k_1, \ldots, k_s$ είναι διαφορετικοί, τότε θεωρούμε εκείνο το (μονοσημάντως καθοριζόμενο) υποσύνολο $\{\varrho_1, \ldots, \varrho_\xi\} \subseteq \{1, \ldots, s\}$* (με $\xi \geq 2$ και $\varrho_1 \geq 1$, $\varrho_\xi = s$) *για το οποίο ισχύει*

$$k_1 = \cdots = k_{\varrho_1} < k_{\varrho_1+1} = \cdots = k_{\varrho_2} < \cdots\cdots < k_{\varrho_{\xi-1}+1} = \cdots = k_{\varrho_\xi} = k_s,$$

*και ορίζουμε τους $\varrho_0 := 0$ και $s_i := \varrho_i - \varrho_{i-1}$, $\forall i \in \{1, \ldots, \xi\}$, με $s_1 + s_2 + \cdots + s_\xi = s$. Εν τοιαύτη περιπτώσει*[20],

$$\boxed{\operatorname{card}(\mathbf{CSubg}(G)) = 1 + \sum_{i=0}^{\xi-1} \tfrac{p^{s_{i+1}+\cdots+s_\xi}-1}{p-1} \sum_{k_{\varrho_i} < j \leq k_{\varrho_{i+1}}} p^{s_1 k_{\varrho_1} + \cdots + s_i k_{\varrho_i} + (j-1)(s_{i+1}+\cdots+s_\xi - 1)}.}$$

Αποδειξη. (i) Προφανώς, $\mathbf{c}_1(\underbrace{p^k, \ldots, p^k}_{s \text{ φορές}}) = 1$, ενώ για κάθε $j \in \{1, \ldots, k\}$ η (9.37) (εφαρμοζόμενη για $r = s$ και $\alpha_1 = \cdots = \alpha_s = k$) δίδει

$$\begin{aligned} \mathbf{c}_{p^j}(\underbrace{p^k, \ldots, p^k}_{s \text{ φορές}}) &= \tfrac{1}{p^{j-1}(p-1)} \left(p^{s \min\{j,k\}} - p^{s \min\{j-1,k\}}\right) \\ &= \tfrac{1}{p^{j-1}(p-1)} \left(p^{sj} - p^{s(j-1)}\right) = \tfrac{p^{s(j-1)}(p^s-1)}{p^{j-1}(p-1)} = \tfrac{p^s-1}{p-1} p^{(s-1)(j-1)}. \end{aligned}$$

Κατά συνέπειαν,

$$\operatorname{card}(\mathbf{CSubg}(G)) = \mathbf{c}(\underbrace{p^k, \ldots, p^k}_{s \text{ φορές}}) = \sum_{j=0}^{k} \mathbf{c}_{p^j}(\underbrace{p^k, \ldots, p^k}_{s \text{ φορές}}) = 1 + \tfrac{p^s-1}{p-1} \sum_{j=1}^{k} p^{(s-1)(j-1)}.$$

[20] *Σύμβαση*: Στο άθροισμα για $i = 0$ θέτουμε $k_{\varrho_0} = k_0 := 0$.

(ii) Προφανώς, $\mathbf{c}_1(p^{k_1},...,p^{k_s}) = 1$ και

$$\begin{aligned}\mathrm{card}(\mathbf{CSubg}(G)) &= \mathbf{c}(p^{k_1},...,p^{k_s})\\ &= \sum_{j=0}^{k_s}\mathbf{c}_{p^j}(p^{k_1},...,p^{k_s}) = 1 + \sum_{i=0}^{\xi-1}\sum_{k_{\varrho_i}<j\le k_{\varrho_{i+1}}}\mathbf{c}_{p^j}(p^{k_1},...,p^{k_s}).\end{aligned}$$

Για κάθε $i \in \{0,1,...,\xi-1\}$ και[21] $k_{\varrho_i} < j \le k_{\varrho_{i+1}}$ η (9.37) (εφαρμοζόμενη για $r = s$ και $\alpha_1 = k_1$,..., $\alpha_s = k_s$) δίδει

$$\begin{aligned}&\mathbf{c}_{p^j}(p^{k_1},...,p^{k_s}) = \tfrac{1}{(p-1)p^{j-1}}\left(p^{\min\{j,k_1\}+\cdots+\min\{j,k_s\}} - p^{\min\{j-1,k_1\}+\cdots+\min\{j-1,k_s\}}\right)\\ &= \tfrac{1}{(p-1)p^{j-1}}\left(p^{s_1k_{\varrho_1}+\cdots+s_ik_{\varrho_i}+j(s_{i+1}+\cdots+s_\xi)} - p^{s_1k_{\varrho_1}+\cdots+s_ik_{\varrho_i}+(j-1)(s_{i+1}+\cdots+s_\xi)}\right)\\ &= \tfrac{p^{s_1k_{\varrho_1}+\cdots+s_ik_{\varrho_i}+(j-1)(s_{i+1}+\cdots+s_\xi)}}{(p-1)p^{j-1}}(p^{s_{i+1}+\cdots+s_\xi}-1)\\ &= \tfrac{p^{s_{i+1}+\cdots+s_\xi}-1}{p-1}p^{s_1k_{\varrho_1}+\cdots+s_ik_{\varrho_i}+(j-1)(s_{i+1}+\cdots+s_\xi-1)},\end{aligned}$$

οπότε ο ισχυρισμός είναι αληθής. □

**9.2.12 Παρατήρηση.** Ο $\mathrm{card}(\mathbf{CSubg}(G))$ είναι σε αμφότερες περιπτώσεις[22] η αποτίμηση ενός *πολυωνύμου* (μιας απροσδιορίστου) στο $p$. (Βλ. C.2.22.)

**►Υπολογισμός αριθμού υποομάδων (σε ειδικές περιπτώσεις)**. Ο ακριβής προσδιορισμός τού αριθμού *όλων* των υποομάδων τού ευθέος αθροίσματος *δύο* ή *τριών* κυκλικών ομάδων είναι εφικτός (σύμφωνα με τα θεωρήματα 9.2.14 και 9.2.19 που ακολουθούν, και μάλιστα μέσω απλών «κλειστών» διατυπωμάτων) κάνοντας χρήση αρκούντως *στοιχειωδών* αριθμοθεωρητικών επιχειρημάτων[23].

**9.2.13 Λήμμα.** *Για κάθε ζεύγος* $(n_1,n_2) \in \mathbb{N}\times\mathbb{N}$ *ορίζουμε το σύνολο*

$$I_{n_1,n_2} := \left\{(d_1,d_2,t)\in\mathbb{N}\times\mathbb{N}\times\mathbb{N}_0 \;\middle|\; \begin{array}{c} d_1\in\mathfrak{D}_{n_1},\ d_2\in\mathfrak{D}_{n_2}\\ \text{και } t\le \text{μκδ}(d_1,\frac{n_2}{d_2})-1\end{array}\right\}$$

*και για κάθε* $(d_1,d_2,t)\in I_{n_1,n_2}$ *το*

$$H_{d_1,d_2,t} := \left\{\left(\left[id_1+\tfrac{jtd_1}{\text{μκδ}(d_1,n_2/d_2)}\right]_{n_1},[jd_2]_{n_2}\right) \;\middle|\; \begin{array}{c} i\in\{0,...,\frac{n_1}{d_1}-1\},\\ j\in\{0,...,\frac{n_2}{d_2}-1\}\end{array}\right\}.$$

*Το* $H_{d_1,d_2,t}$ *αποτελεί το υποκείμενο σύνολο μιας υποομάδας τής* $\mathbb{Z}_{n_1}\oplus\mathbb{Z}_{n_2}$ *τάξεως* $|H_{d_1,d_2,t}| = \frac{n_1n_2}{d_1d_2}$ *και η απεικόνιση*

$$I_{n_1,n_2}\ni(d_1,d_2,t)\longmapsto H_{d_1,d_2,t}\in\mathbf{Subg}(\mathbb{Z}_{n_1}\oplus\mathbb{Z}_{n_2})$$

*είναι αμφιρριπτική.*

[21] Σημειωτέον ότι $k_{\varrho_i} < j \le k_{\varrho_{i+1}} \Rightarrow k_{\varrho_i} \le j-1 \le k_{\varrho_{i+1}}-1 < k_{\varrho_{i+1}}$.

[22] Προφανώς, $\frac{p^s-1}{p-1} = 1+p+\cdots+p^{s-1}$ και $\frac{p^{s_{i+1}+\cdots+s_\xi}-1}{p-1} = 1+p+\cdots+p^{s_{i+1}+\cdots+s_\xi-1}$.

[23] Η απόδειξη τού θεωρήματος 9.2.14 εδόθη στην εργασία των M. Hampejs, N. Holighaus, L. Toth & Ch. Wiesmeyr: *On the subgroups of the group* $\mathbb{Z}_m\times\mathbb{Z}_n$, arXiv:1211.1797 (v2, December 2013).

ΑΠΟΔΕΙΞΗ. Ο πρώτος ισχυρισμός είναι εύκολα επαληθεύσιμος. Για να αποδειχθεί η αμφιρριπτικότητα τής ανωτέρω απεικονίσεως αρκεί να θεωρήσουμε τυχούσα $H \in \mathbf{Subg}(\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2})$ και να δείξουμε ότι αυτή είναι τής επιθυμητής μορφής. Η εικόνα $\mathrm{pr}_2(H)$ τής $H$ μέσω τής δεύτερης φυσικής προβολής $\mathrm{pr}_2 : \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \longrightarrow \mathbb{Z}_{n_2}$ αποτελεί μια υποομάδα τής $\mathbb{Z}_{n_2}$, οπότε (σύμφωνα με το (ii) τού θεωρήματος 2.4.26) υπάρχει *ακριβώς ένας* $d_2 \in \mathfrak{D}_{n_2}$ με

$$\mathrm{pr}_2(H) = \langle [d_2]_{n_2} \rangle = \left\{ [jd_2]_{n_2} \,\middle|\, j \in \{0, ..., \tfrac{n_2}{d_2} - 1\} \right\}.$$

Κατ' αναλογίαν, η αντίστροφη εικόνα $\iota_1^{-1}(H)$ τής $H$ μέσω τής πρώτης φυσικής εμφυτεύσεως $\iota_1 : \mathbb{Z}_{n_1} \hookrightarrow \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ αποτελεί μια υποομάδα τής ομάδας $\mathbb{Z}_{n_1}$, οπότε υπάρχει *ακριβώς ένας* $d_1 \in \mathfrak{D}_{n_1}$ με $\iota_1^{-1}(H) = \langle [d_1]_{n_1} \rangle$. Θέτοντας $s := \min\{ u \in \mathbb{N}_0 |\, ([u]_{n_1}, [d_2]_{n_2}) \in H\}$ θα δείξουμε εν πρώτοις ότι

$$H = \left\{ ([i\, d_1 + j\, s]_{n_1}, [jd_2]_{n_2}) \,|(i,j) \in \mathbb{Z} \times \mathbb{Z} \right\}. \tag{9.38}$$

Για κάθε $(i,j) \in \mathbb{Z} \times \mathbb{Z}$ έχουμε

$$([i\, d_1 + j\, s]_{n_1}, [jd_2]_{n_2}) = i \underbrace{([d_1]_{n_1}, [0]_{n_2})}_{=\iota_1([d_1]_{n_1})} + j \underbrace{([s]_{n_1}, [d_2]_{n_2})}_{\in H} \in H.$$

Και αντιστρόφως· για κάθε $([a_1]_{n_1}, [a_2]_{n_2}) \in H$,

$$[a_2]_{n_2} \in \mathrm{pr}_2(H) \Rightarrow \exists j \in \mathbb{Z} : [a_2]_{n_2} = j\,[d_2]_{n_2} = [jd_2]_{n_2}$$

και $([a_1]_{n_1} - j\,[s]_{n_1}, [0]_{n_2}) = \underbrace{([a_1]_{n_1}, [a_2]_{n_2})}_{\in H} - j \underbrace{([s]_{n_1}, [d_2]_{n_2})}_{\in H} \in H$, οπότε

$$[a_1]_{n_1} - j\,[s]_{n_1} \in \iota_1^{-1}(H) \Rightarrow \exists i \in \mathbb{Z} : [a_1]_{n_1} = [i\, d_1 + j\, s]_{n_1}.$$

Άρα η ισότητα (9.38) είναι όντως αληθής. Για να περιγράψουμε την $H$ σε «ανηγμένη» μορφή παρατηρούμε κατ' αρχάς ότι $([\frac{sn_2}{d_2}]_{n_1}, [0]_{n_2}) \in H$. (Αρκεί να θεωρήσουμε τις ειδικές τιμές $i = 0$ και $j = \frac{n_2}{d_2}$). Αυτό σημαίνει ότι

$$\left.\begin{array}{r} [\frac{sn_2}{d_2}]_{n_1} \in \iota_1^{-1}(H) \Rightarrow u \in \mathbb{Z} : [\frac{sn_2}{d_2}]_{n_1} = [u\, d_1]_{n_1} \\ \Rightarrow n_1 \mid \frac{sn_2}{d_2} - u\, d_1 \\ d_1 \mid n_1, \;\; d_1 \mid u\, d_1 \end{array}\right\} \Rightarrow d_1 \mid \frac{sn_2}{d_2},$$

ή, ισοδυνάμως, ότι $\frac{d_1}{\text{μκδ}(d_1, \frac{n_2}{d_2})} \mid s$. Άρα $\exists t, t' \in \mathbb{N}_0 : s = \frac{td_1}{\text{μκδ}(d_1, \frac{n_2}{d_2})}$ και $\frac{sn_2}{d_2} = t'd_1$. Για οιοδήποτε ζεύγος $(i,j) \in \mathbb{Z} \times \mathbb{Z}$ υπάρχουν (σύμφωνα με το θεώρημα B.1.6) μονοσημάντως ορισμένα ζεύγη $(q, i'), (q', j') \in \mathbb{Z} \times \mathbb{Z}$, ούτως ώστε να ισχύει

$$j = q' \tfrac{n_2}{d_2} + j', \text{ όπου } 0 \leq j' \leq \tfrac{n_2}{d_2} - 1 \text{ και}$$
$$i + q't' = q \tfrac{n_1}{d_1} + i', \text{ όπου } 0 \leq i' \leq \tfrac{n_1}{d_1} - 1.$$

Επειδή $jd_2 = (q'\frac{n_2}{d_2} + j')d_2 = q'n_2 + j'd_2$ και

$$\begin{aligned} i\,d_1 + j\,s &= (q\tfrac{n_1}{d_1} + i' - q't')d_1 + (q'\tfrac{n_2}{d_2} + j')s \\ &= qn_1 + i'd_1 - q't'd_1 + q'\tfrac{sn_2}{d_2} + j's = qn_1 + i'd_1 + j's, \end{aligned}$$

το στοιχείο $([i\,d_1 + j\,s]_{n_1}, [jd_2]_{n_2})$ τής $H$ ισούται με το $([i'\,d_1 + j'\,s]_{n_1}, [j'd_2]_{n_2})$, οπότε εντός των αγκίστρων τού δεξιού μέλους τής (9.38) η συνθήκη $(i,j) \in \mathbb{Z} \times \mathbb{Z}$ μπορεί να αντικατασταθεί με την $(i,j) \in \{0,..., \frac{n_1}{d_1} - 1\} \times \{0,..., \frac{n_2}{d_2} - 1\}$. Υπολείπεται ο καθορισμός ανάλογης περιοριστικής συνθήκης *και* για τον $t$. Διαιρώντας τό $s$ διά τού $d_1$ λαμβάνουμε $s = q''d_1 + s'$ για κάποιο $(q'', s') \in \mathbb{Z} \times \mathbb{Z}$ με $0 \leq s' < d_1$. Επειδή $([s']_{n_1}, [d_2]_{n_2}) = \underbrace{([s]_{n_1}, [d_2]_{n_2})}_{\in H} - q'' \underbrace{([d_1]_{n_1}, [0]_{n_2})}_{\in H} \in H$, από τον ορισμό τού $s$ συμπεραίνουμε ότι $\frac{td_1}{\text{μκδ}(d_1, \frac{n_2}{d_2})} = s \leq s' < d_1 \Rightarrow t \in \{0,..., \text{μκδ}(d_1, \frac{n_2}{d_2}) - 1\}$. Τελικώς λοιπόν, $H = H_{d_1,d_2,t}$. □

**9.2.14 Θεώρημα.** *Εάν $n_1, n_2 \in \mathbb{N}$, τότε ο αριθμός των υποομάδων τής $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ είναι ο*

$$\boxed{\text{card}(\mathbf{Subg}(\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2})) = \sum_{d_1 \in \mathfrak{D}_{n_1},\, d_2 \in \mathfrak{D}_{n_2}} \text{μκδ}(d_1, d_2).} \tag{9.39}$$

ΑΠΟΔΕΙΞΗ. Ο εν λόγω αριθμός ισούται (σύμφωνα με το λήμμα 9.2.13) με

$$\text{card}(I_{n_1,n_2}) = \sum_{d_1 \in \mathfrak{D}_{n_1},\, d_2 \in \mathfrak{D}_{n_2}} \; \sum_{0 \leq t \leq \text{μκδ}(d_1, \frac{n_2}{d_2}) - 1} 1 = \sum_{d_1 \in \mathfrak{D}_{n_1},\, d_2 \in \mathfrak{D}_{n_2}} \text{μκδ}(d_1, \frac{n_2}{d_2}),$$

όπου αυτό το τελευταίο άθροισμα ισούται με το δεξιό μέλος τής (9.39) (καθώς η απεικόνιση $\mathfrak{D}_{n_2} \ni d_2 \longmapsto \frac{n_2}{d_2} \in \mathfrak{D}_{n_2}$ είναι αμφιρριπτική). □

**9.2.15 Σημείωση.** Επειδή $\sum_{d \in \mathfrak{D}_{\text{μκδ}(d_1,d_2)}} \phi(d) \underset{\text{(B.47)}}{=} \text{μκδ}(d_1, d_2)$, το άθροισμα (9.39) μπορεί να επανεκφρασθεί ως ακολούθως[24]:

$$\left.\begin{aligned} &\sum_{d_1 \in \mathfrak{D}_{n_1},\, d_2 \in \mathfrak{D}_{n_2}} \; \sum_{d \in \mathfrak{D}_{\text{μκδ}(d_1,d_2)}} \phi(d) = \sum_{n_1 = m_1 d_1,\, n_2 = m_2 d_2} \; \sum_{di = d_1,\, dj = d_2} \phi(d) \\ &= \sum_{d\, i m_1 = n_1,\, d j m_2 = n_2} \phi(d) = \sum_{d\, a = n_1,\, db = n_2} \phi(d) \sum_{i m_1 = a,\, j m_2 = b} 1 \\ &= \sum_{d\, a = n_1,\, db = n_2} \phi(d)\, \text{card}(\mathfrak{D}_a)\, \text{card}(\mathfrak{D}_b) \\ &= \sum_{d \in \mathfrak{D}_{\text{μκδ}(n_1,n_2)}} \phi(d)\, \text{card}(\mathfrak{D}_{\frac{n_1}{d}})\, \text{card}(\mathfrak{D}_{\frac{n_2}{d}}) = \sum_{d \in \mathfrak{D}_{\text{μκδ}(n_1,n_2)}} d\, \text{card}(\mathfrak{D}_{\frac{n_1 n_2}{d^2}}) \end{aligned}\right\} \tag{9.40}$$

[24]Τα $m_1, m_2, i, j, a, b$ χρησιμοποιούνται κατά τρόπο εμφανή (π.χ., $d_1 \in \mathfrak{D}_{n_1} \Leftrightarrow \exists m_1 : n_1 = m_1 d_1$) προκειμένου να γίνει ευκολότερα αντιληπτή η συγχώνευση ή η διάσπαση των εκάστοτε συναντώμενων αθροισμάτων.

όπου η τελευταία ισότητα εξάγεται από τη λεγομένη *ταυτότητα των Busche και Ramanujan*[25].

**9.2.16 Πόρισμα.** *Έστω $p$ ένας πρώτος αριθμός. Ο αριθμός των υποομάδων οιασδήποτε πεπερασμένης αβελιανής $p$-ομάδας $(G,+)$ έχουσας τύπο $(k_1,k_2)$ γράφεται ως εξής:*

$$\boxed{\mathrm{card}(\mathbf{Subg}(G)) = \frac{(k_2-k_1+1)p^{k_1+2}-(k_2-k_1-1)p^{k_1+1}-(k_1+k_2+3)p+(k_1+k_2+1)}{(p-1)^2}.} \tag{9.41}$$

Αποδειξη. Επειδή $G \cong \mathbb{Z}_{p^{k_1}} \oplus \mathbb{Z}_{p^{k_2}}$ και $k_1 \leq k_2$, έχουμε μκδ$(p^{k_1},p^{k_2}) \underset{\text{B.3.16}}{=} p^{k_1}$ και ο αριθμός των υποομάδων τής $G$ (λόγω τής (9.40)) είναι ο[26]

$$\sum_{i=0}^{k_1} p^i\,\mathrm{card}(\mathfrak{D}_{p^{k_1+k_2-2i}}) \underset{\text{B.3.15 (i)}}{=} \sum_{i=0}^{k_1} p^i\ (k_1+k_2-2i+1)$$
$$= (k_1+k_2+1)\sum_{i=0}^{k_1} p^i - 2p\left(\sum_{i=1}^{k_1} ip^{i-1}\right).$$

Χρησιμοποιώντας τις ισότητες

$$\sum_{i=0}^{k_1} p^i = \frac{p^{k_1+1}-1}{p-1} \quad \text{και} \quad \sum_{i=1}^{k_1} ip^{i-1} = \frac{1-(k_1+1)p^{k_1}+k_1p^{k_1+1}}{(p-1)^2}$$

καταλήγουμε (ύστερα από απλές πράξεις) στην (9.41). □

**9.2.17 Παράδειγμα.** Η 3-ομάδα $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ (τάξεως 27 και τύπου $(1,2)$) διαθέτει

$$\frac{(2-1+1)3^3-(2-1-1)3^2-3(1+2+3)+(1+2+1)}{2^2} = 10$$

υποομάδες. Αυτές τις έχουμε ήδη προσδιορίσει *επακριβώς* στο εδάφιο 7.1.13.

**9.2.18 Σημείωση.** (i) Εναλλακτικές αποδείξεις τής (9.41) έχουν δοθεί και από τους G. Călugăreanu[27] και J. Petrillo[28] (μέσω εφαρμογής τού θεωρήματος 7.1.10 των Goursat και Remak), καθώς και από τον M. Tărnăuceanu[29] (μέσω τής χρήσεως οριζουσών κάποιων πινάκων που κατασκευάζονται με τη βοήθεια των αναλλοιώτων παραγόντων).

[25] Αρκεί να εφαρμοσθεί για τη συνάρτηση $\mathbb{N} \ni n \longmapsto \mathrm{card}(\mathfrak{D}_n) \in \mathbb{N}$ (την κλασική συνάρτηση "$\sigma_0$") το (ii) τού πορίσματος τού θεωρήματος 13 (στη σελίδα 225) τού άρθρου των D. Redmond και R. Sivaramakrishnan: *Some properties of specially multiplicative functions*, Journal of Number Theory **13** (1981), 210-227.

[26] Κάθε θετικός ακέραιος διαιρέτης $d$ τού $p^{k_1}$ είναι (σύμφωνα με το λήμμα B.3.14) τής μορφής $d = p^i$, για κάποιον $i \in \{0,1,\ldots,k_1\}$.

[27] G. Călugăreanu: *The total number of subgroups of a finite abelian group*, Sci. Math. Japon. **60** (2004), 157-167.

[28] J. Petrillo: *Counting subgroups in a direct product of finite cyclic groups*, College Math J. **42** (2011), 215-222.

[29] M. Tărnăuceanu: *An arithmetic method of counting the subgroups of a finite abelian group*, Bull. Math. Soc. Sci. Math. Roumanie (N.S.), **53** [101] (2010), 373-386.

(ii) Τα ανάλογα τού θεωρήματος 9.2.14 και τού πορίσματος 9.2.16 (μέσω κατάλληλης προσαρμογής τής ανωτέρω παρατεθείσας αποδεικτικής μεθόδου) για το ευθύ άθροισμα *τριών* κυκλικών ομάδων είναι τα θεωρήματα 9.2.19 και 9.2.20, οφειλόμενα στους M. Hampejs & L. Tóth[30] και στον **J.-M. Oh**[31], αντιστοίχως.

**9.2.19 Θεώρημα.** (**M. Hampejs & L. Tóth**, 2013.) *Εάν* $n_1, n_2, n_3 \in \mathbb{N}$, *τότε*

$$\boxed{\operatorname{card}(\mathbf{Subg}(\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \mathbb{Z}_{n_3})) = \sum_{d_1 \in \mathfrak{D}_{n_1}, d_2 \in \mathfrak{D}_{n_2}, d_3 \in \mathfrak{D}_{n_3}} \frac{ABC}{D^2} \left( \sum_{i=1}^{D} \mu\kappa\delta(i, D) \right),}$$

*όπου* $A := \mu\kappa\delta(d_1, \frac{n_2}{d_2})$, $B := \mu\kappa\delta(d_2, \frac{n_3}{d_3})$, $C := \mu\kappa\delta(d_1, \frac{n_3}{d_3})$, $D := \frac{ABC}{\mu\kappa\delta(d_1 n_3/d_3, ABC)}$.

**9.2.20 Θεώρημα.** (**J.-M. Oh,** 2013.) *Ο αριθμός των υποομάδων οιασδήποτε πεπερασμένης αβελιανής* $p$*-ομάδας* $(G, +)$ *έχουσας τύπο* $(k_1, k_2, k_3)$ *εκφράζεται ως εξής:*

$$\boxed{\begin{aligned} &\operatorname{card}(\mathbf{Subg}(G)) = \tfrac{(k_2+k_3-2k_1+4)k_1 p^{2k_1} + (k_2+k_3-2k_1+2)k_1 p^{2k_1+1}}{p^2-1} \\ &- \tfrac{(k_2+k_3-5k_1+7)p^{2k_1} + (k_2+k_3-5k_1+5)p^{2k_1+1} - (k_1+k_2+k_3-1)p - (k_1+k_2+k_3+1)}{(p^2-1)^2} \\ &- \tfrac{6(p^{2k_1}+p^{2k_1+1}-p^3-p^2)}{(p^2-1)^3} + \tfrac{(k_1+1)((k_3-k_2+1)p^{k_1+k_2+1} - (k_2+k_3-2k_1+3)p^{2k_1})}{p-1} \\ &+ \tfrac{2(k_1+1)(p^{k_1+k_2+1}-p^{2k_1})}{(p-1)^2}. \end{aligned}} \tag{9.42}$$

**9.2.21 Παράδειγμα.** Η 2-ομάδα $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8$ (τάξεως 64 και τύπου $(1, 2, 3)$) διαθέτει 81 υποομάδες.

►**Υπολογισμός αριθμού υποομάδων (στη γενική περίπτωση)**. Για τον υπολογισμό τού αριθμού των υποομάδων *τυχούσας* πεπερασμένης μη τετριμμένης αβελιανής ομάδας αρκεί (λόγω τής (9.23)) να υπολογισθεί ο αριθμός των υποομάδων καθεμιάς εκ των πρωτευουσών συνιστωσών της. Επομένως, το όλο πρόβλημα ανάγεται στον προσδιορισμό τού αριθμού των υποομάδων *τυχούσας* πεπερασμένης μη τετριμμένης αβελιανής $p$-ομάδας. Ο Garrett Birkhoff (1911-1996) ήταν εκείνος που (το έτος 1934) κατασκεύασε μια λεπτομερή αμφίρριψη μεταξύ μιας οικογενείας πολυπαραμετρικών πινάκων και τού συνόλου αυτών των υποομάδων, διευκολύνοντας αισθητά τη μελέτη και την απαρίθμησή τους[32]. Έκτοτε (και μέχρι το 1950) είδαν το φως τής δημοσιότητας αρκετές σχετικές εργασίες, όπως αυτές

[30] M. Hampejs & L. Tóth: *On the subgroups of finite groups of rank* 3, Annales Univ. Sci. Budapest, Sect. Comp. **39** (2013), 111-124.

[31] J.-M. Oh: *An explicit formula for the number of subgroups of a finite abelian p-group up to rank* 3, Commun. Korean Math. Soc. **28**, No. 4 (2013), 649-667.

[32] G. Birkhoff: *Subgroups of abelian groups*, Proceedings of the London Math. Soc. (2), **38** (1934-35), 385-401. (Βλ., ιδιαιτέρως, Thm. 8.1, σελ. 390.)

των G.A. Miller[33], S. Delsarte[34], P.E. Dyubyuk[35], Y. Yeh[36] και Y. Kinosita[37], στις οποίες εδόθησαν διεξοδικές αλλά *περίπλοκες* περιγραφές τού εν λόγω αριθμού (άλλοτε μέσω επαγωγικών επιχειρημάτων και άλλοτε μέσω χρήσεως ειδικών αριθμητικών συναρτήσεων). Αργότερα, κατά τη δεκαετία 1985-1995, οι L.M. Butler[38] και Th. Stehling[39], εκκινώντας από την αρχική εργασία τού Birkhoff, συνέδεσαν τα προηγηθέντα αποτελέσματα με βαθύτερες τεχνικές τής Αλγεβρικής Συνδυαστικής (διαγράμματα τού Ferrer, πολυώνυμα τού Hall, διάφορες συμμετρικές συναρτήσεις κ.ά.). Εδώ θα υιοθετηθεί (με ελάχιστες τροποποιήσεις, αποσκοπούσες σε περαιτέρω απλουστεύσεις) μια μέθοδος *σύντομης* παρουσιάσεως τής επιλύσεως τού προβλήματος, οφειλόμενη στον M. Farrokhi[40], στην οποία δεν υπεισέρχονται «προκεχωρημένα» αλγεβρικά μέσα. (Βλ. θεώρημα 9.2.29.)

**9.2.22 Συμβολισμός.** Δοθέντων ενός πρώτου αριθμού $p$ και ενός $s \in \mathbb{N}$, για κάθε $s$-άδα $\mathbf{k} = (k_1, ..., k_s) \in \mathbb{N}^s$ με $k_1 \leq \cdots \leq k_s$ θέτουμε (για διευκόλυνσή μας)

$$G_{p,\mathbf{k}} := \mathbb{Z}_{p^{k_1}} \oplus \mathbb{Z}_{p^{k_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_s}}.$$

Εξ ορισμού, μια πεπερασμένη μη τετριμμένη αβελιανή $p$-ομάδα $(G, +)$ είναι τού τύπου $\mathbf{k}$ όταν $G \cong G_{p,\mathbf{k}}$. Εν τοιαύτη περιπτώσει, το θεώρημα 9.2.2 μας πληροφορεί ότι το $\mathbf{Subg}(G) \smallsetminus \{\{e_G\}\}$ απαρτίζεται από υποομάδες $H \cong G_{p,\mathbf{l}}$, $\mathbf{l} \in \mathcal{S}(\mathbf{k})$, όπου

$$\mathcal{S}(\mathbf{k}) := \left\{ \mathbf{l} = (l_1, ..., l_t) \in \mathbb{N}^t \,\middle|\, t \leq s, l_1 \leq \cdots \leq l_t, l_1 \leq k_{s-t+1}, l_2 \leq k_{s-t+2}, ..., l_t \leq k_s \right\}.$$

Επειδή $\mathrm{card}(\mathbf{Subg}(G)) = \mathrm{card}(\mathbf{Subg}(G_{p,\mathbf{k}}))$, αρκεί (για την επίλυση τού τιθέμενου προβλήματος) να απαριθμηθούν τα στοιχεία τού $\mathbf{Subg}(G_{p,\mathbf{k}})$. Προς τούτο θα χρησιμοποιηθούν οι πληθικοί αριθμοί των συνόλων

$$\mathfrak{U}_p(\mathbf{k}; \mathbf{l}) := \left\{ (x_1, ..., x_t) \in \underbrace{G_{p,\mathbf{k}} \times ... \times G_{p,\mathbf{k}}}_{t \text{ φορές}} \,\middle|\, \begin{array}{c} |\langle x_j \rangle| = p^{l_j}, \forall j \in \{1, ..., t\}, \\ \text{και } \ \langle x_1, ..., x_t \rangle \cong G_{p,\mathbf{l}} \end{array} \right\}$$

για κάθε $\mathbf{l} = (l_1, ..., l_t) \in \mathcal{S}(\mathbf{k})$, καθώς και η απεικόνιση

$$\{\mathbf{m} = (m_1, ..., m_r) \in \mathbb{N}^r \,|\, m_1 \leq \cdots \leq m_r\} \times \mathbb{N}_0 \ni (\mathbf{m}, i) \longmapsto \mathfrak{E}_i(\mathbf{m}) \in \mathbb{N}_0$$

όπου $r \in \mathbb{N}$,

$$\mathfrak{E}_i(\mathbf{m}) := \begin{cases} ir, & \text{όταν } i < m_1, \\ m_1 + \cdots + m_{\mathfrak{d}(i)} + i(r - \mathfrak{d}(i)), & \text{όταν } m_1 \leq i \leq m_r, \\ m_1 + \cdots + m_r, & \text{όταν } i > m_r, \end{cases}$$

[33] G.A. Miller: *Number of the subgroups of any abelian group*, Proc. Nat. Acad. Sci. U.S.A. **25** (1939), 256-262.

[34] S. Delsarte: *Fonctions de Möbius sur les groupes abeliens finis*, Annals of Mathematics **49** (1948), 600-609.

[35] P.E. Dyubyuk: *On the number of subgroups of a finite abelian group*, Izv. Akad. Nauk SSR Ser. Mat. **12** (1948), 351-378. Translated in: Soviet Math. **2** (1961), 298-300.

[36] Y. Yeh: *On prime power abelian groups*, Bull. Amer. Math. Soc. **54** (1948), 323-327.

[37] Y. Kinosita: *On an enumeration of certain subgroups of a p-group*, J. Osaka Inst. Sci. Tech., Part I, **1** (1949), 13-20.

[38] L.M. Butler: *A unimodality result in the enumeration of subgroups of a finite abelian group*, Proceedings of the Amer. Math. Soc., Vol. **101**, No 4 (1987), 771-775, και

L.M. Butler: *Subgroup Lattices and Symmetric Functions*, Memoirs of the Amer. Math. Soc., Vol. **112**, No 539 (1994).

[39] Th. Stehling: *On computing the number of subgroups of a finite abelian group*, Combinatorica **12** (1992), 475-479.

[40] M. Farrokhi: *Factorization numbers of finite abelian groups*, International Journal of Group Theory **2** (2013), 1-8.

και $\mathfrak{d}(i) := \max\{\, j \in \{1,...,r\} |\, m_j \leq i\}$ (όταν $m_1 \leq i \leq m_r$).

**9.2.23 Λήμμα.** *Για κάθε $i \in \mathbb{N}_0$ και κάθε $\mathbf{m} = (m_1,...,m_r) \in \mathbb{N}^r$ με $m_1 \leq \cdots \leq m_r$ έχουμε*

$$\boxed{\left|G_{p,\mathbf{m}}[p^i]\right| = p^{\mathfrak{E}_i(\mathbf{m})}.}$$

ΑΠΟΔΕΙΞΗ. Επειδή $p^i G_{p,\mathbf{m}} \underset{9.1.6}{\cong} p^i\,\mathbb{Z}_{p^{m_1}} \oplus p^i\,\mathbb{Z}_{p^{m_2}} \oplus \cdots \oplus p^i\,\mathbb{Z}_{p^{m_r}}$ και

$$\mathbb{Z}_{p^{m_j}} = \left\langle [1]_{p^{m_j}} \right\rangle \Rightarrow p^i\,\mathbb{Z}_{p^{m_j}} = \left\langle \left[p^i\right]_{p^{m_j}} \right\rangle,\ \forall j \in \{1,...,r\},$$

η $p^i\,\mathbb{Z}_{p^{m_j}}$ είναι κυκλική τάξεως

$$\frac{p^{m_j}}{\text{μκδ}(p^{m_j}, p^i)} = p^{m_j - \min\{m_j, i\}}$$

(βλ. 2.3.10 (i)), οπότε

$$\left.\begin{array}{l} G_{p,\mathbf{m}}/G_{p,\mathbf{m}}[p^i] \underset{9.1.4}{\cong} p^i G_{p,\mathbf{m}} \\ |G_{p,\mathbf{m}}| = p^{\left(\sum_{j=1}^r m_j\right)} \\ \left|p^i G_{p,\mathbf{m}}\right| = p^{\left(\sum\limits_{j=1}^r m_j\right) - \left(\sum\limits_{j=1}^r \min\{m_j,i\}\right)} \end{array}\right\} \Rightarrow \left|G_{p,\mathbf{m}}[p^i]\right| = p^{\left(\sum\limits_{j=1}^r \min\{m_j,i\}\right)},$$

όπου $\sum_{j=1}^r \min\{m_j, i\} = \mathfrak{E}_i(\mathbf{m})$. □

**9.2.24 Πρόταση.** *Για κάθε $\mathbf{k} = (k_1,...,k_s) \in \mathbb{N}^s$ με $k_1 \leq \cdots \leq k_s$ και κάθε $t$-άδα $\mathbf{l} = (l_1,...,l_t) \in \mathcal{S}(\mathbf{k})$ ο πληθικός αριθμός τού συνόλου $\mathfrak{U}_p(\mathbf{k};\mathbf{l})$ είναι ο*

$$\boxed{\text{card}(\mathfrak{U}_p(\mathbf{k};\mathbf{l})) = \left(\prod_{j=1}^{t-1} (p^{\mathfrak{E}_{l_{t-j}}(\mathbf{k})} - p^{\mathfrak{E}_{l_{t-j-1}}(\mathbf{k}) + \mathfrak{E}_{l_{t-j}}(\mathbf{l}_{(j)}) - \mathfrak{E}_{l_{t-j-1}}(\mathbf{l}_{(j)})})\right)(p^{\mathfrak{E}_{l_t}(\mathbf{k})} - p^{\mathfrak{E}_{l_t - 1}(\mathbf{k})}),}$$

*όπου* $\mathbf{l}_{(j)} := (l_{t-j+1},...,l_t)$. [Στην περίπτωση όπου $t = 1$, το $\prod_{j=1}^{t-1} \cdots$ παραλείπεται.]

ΑΠΟΔΕΙΞΗ. Εάν θεωρήσουμε $x_1,...,x_t \in G_{p,\mathbf{k}}$ με $|\langle x_j\rangle| = p^{l_j}, \forall j \in \{1,...,t\}$, και $\langle x_1,...,x_t\rangle \cong G_{p,\mathbf{l}}$, τότε ως $x_t$ μπορεί να επιλεγεί οιοδήποτε στοιχείο τής διαφοράς $G_{p,\mathbf{k}}[p^{l_t}] \setminus G_{p,\mathbf{k}}[p^{l_t - 1}]$ και, κατ' αναλογίαν, *όταν* $t \geq 2$, ως $x_{t-j}$ οιοδήποτε στοιχείο τής διαφοράς

$$G_{p,\mathbf{k}}[p^{l_{t-j}}] \setminus G_{p,\mathbf{k}}[p^{l_{t-j}-1}]\,\langle x_{t-j+1},...,x_{t-1},x_t\rangle,\ \forall j \in \{1,...,t-1\}.$$

Κατά συνέπειαν, το πλήθος των $t$-άδων $(x_1,...,x_t)$ αυτού τού είδους ισούται με

$$\prod_{j=1}^{t-1}\left(G_{p,\mathbf{k}}[p^{l_{t-j}}] \setminus G_{p,\mathbf{k}}[p^{l_{t-j}-1}]\,\langle x_{t-j+1},...,x_{t-1},x_t\rangle\right)\left(\left|G_{p,\mathbf{k}}[p^{l_t}]\right| - \left|G_{p,\mathbf{k}}[p^{l_t - 1}]\right|\right).$$

Επειδή

$$G_{p,\mathbf{k}}[p^{l_{t-j}}] \setminus G_{p,\mathbf{k}}[p^{l_{t-j}-1}]\,\langle x_{t-j+1},...,x_t\rangle = G_{p,\mathbf{k}}[p^{l_{t-j}-1}] \setminus G_{p,\mathbf{k}}[p^{l_{t-j}-1}]\,\langle x_{t-j+1},...,x_t\rangle\,[p^{l_{t-j}}]$$

και (μέσω τού τύπου (4.35) τού γινομένου[41])

$$\left|G_{p,\mathbf{k}}[p^{l_{t-j}-1}]\left\langle x_{t-j+1},...,x_t\right\rangle[p^{l_{t-j}}]\right| = \frac{\left|G_{p,\mathbf{k}}[p^{l_{t-j}-1}]\right|\left|\left\langle x_{t-j+1},...,x_t\right\rangle[p^{l_{t-j}}]\right|}{\left|\left\langle x_{t-j+1},...,x_t\right\rangle[p^{l_{t-j}-1}]\right|},$$

το πλήθος των εν λόγω $t$-άδων $(x_1,...,x_t)$ ισούται με

$$\prod_{j=1}^{t-1}\left(\left|G_{p,\mathbf{k}}[p^{l_{t-j}}]\right| - \frac{\left|G_{p,\mathbf{k}}[p^{l_{t-j}-1}]\right|\left|G_{p,\mathbf{l}_{(j)}}[p^{l_{t-j}}]\right|}{\left|G_{p,\mathbf{l}_{(j)}}[p^{l_{t-j}-1}]\right|}\right)\left(\left|G_{p,\mathbf{k}}[p^{l_t}]\right| - \left|G_{p,\mathbf{k}}[p^{l_t-1}]\right|\right),$$

διότι $\langle x_{t-j+1},...,x_t\rangle \cong G_{p,\mathbf{l}_{(j)}}$. Αρκεί λοιπόν η εφαρμογή τού 9.2.23 (με τα $\mathbf{k},\mathbf{l}_{(j)}$ στη θέση τού $\mathbf{m}$ και με τους ανωτέρω συναντώμενους εκθέτες τού $p$ ως $i$). □

**9.2.25 Πόρισμα.** *Για κάθε* $\mathbf{k}=(k_1,...,k_s)\in\mathbb{N}^s$ *με* $k_1\leq\cdots\leq k_s$ *ισχύει*

$$\operatorname{card}(\mathfrak{U}_p(\mathbf{k};\mathbf{k})) = |\operatorname{Aut}(G_{p,\mathbf{k}})|. \tag{9.43}$$

ΑΠΟΔΕΙΞΗ. Επειδή $G_{p,\mathbf{k}}=\langle x_1,...,x_s\rangle$ με $|\langle x_j\rangle| = p^{k_j}, \forall j\in\{1,...,s\}$, η απεικόνιση

$$\operatorname{Aut}(G_{p,\mathbf{k}})\ni\vartheta\longmapsto(\vartheta(x_1),...,\vartheta(x_s))\in\mathfrak{U}_p(\mathbf{k};\mathbf{k})$$

είναι αμφιρριπτική. □

**9.2.26 Λήμμα.** *Εάν* $(G,+)$ *είναι μια πεπερασμένη μη τετριμμένη αβελιανή* $p$*-ομάδα με τύπο* $\mathbf{k}=(k_1,...,k_s)$, *τότε ο αριθμός των υποομάδων της οι οποίες έχουν τύπο* $\mathbf{l}=(l_1,...,l_t)\in\mathcal{S}(\mathbf{k})$ *ισούται με*[42] $\frac{\operatorname{card}(\mathfrak{U}_p(\mathbf{k};\mathbf{l}))}{\operatorname{card}(\mathfrak{U}_p(\mathbf{l};\mathbf{l}))}$.

ΑΠΟΔΕΙΞΗ. Το σύνολο $\mathfrak{U}_p(\mathbf{k};\mathbf{l})$ απαρτίζεται από όλες τις δυνατές $t$-άδες $(x_1,...,x_t)$ στοιχείων τής $G_{p,\mathbf{k}}\cong G$ τα οποία παράγουν μια υποομάδα ισόμορφη τής $G_{p,\mathbf{l}}$. Επειδή ισχύει

$$\langle x_1,...,x_t\rangle=\langle x_1',...,x_t'\rangle\cong G_{p,\mathbf{l}}\Longleftrightarrow\exists\vartheta\in\operatorname{Aut}(G_{p,\mathbf{l}}): x_1'=\vartheta(x_1),...,x_t'=\vartheta(x_t),$$

ο αριθμός των υποομάδων τής $G_{p,\mathbf{k}}\cong G$ που έχουν τύπο $\mathbf{l}=(l_1,...,l_t)\in\mathcal{S}(\mathbf{k})$ ισούται με τον πληθικό αριθμό τού $\mathfrak{U}_p(\mathbf{k};\mathbf{l})$ διηρημένο διά τής τάξεως τής $\operatorname{Aut}(G_{p,\mathbf{l}})$ (που υπολογίζεται μέσω τού πορίσματος 9.2.25 θέτοντας το $\mathbf{l}$ στη θέση τού $\mathbf{k}$). □

**9.2.27 Παράδειγμα.** Η 3-ομάδα $\mathbb{Z}_3\oplus\mathbb{Z}_9\oplus\mathbb{Z}_{27}$ (τάξεως 729 και τύπου $(1,2,3)$) διαθέτει

$$\frac{\operatorname{card}(\mathfrak{U}_3((1,2,3);(1,2)))}{\operatorname{card}(\mathfrak{U}_3((1,2);(1,2)))}=\frac{5184}{108}=48$$

υποομάδες τού τύπου $(1,2)$, διότι

$$\begin{aligned}&\mathfrak{E}_1(1,2,3)=3, \mathfrak{E}_0(1,2,3)=0, \mathfrak{E}_1(2)=1, \mathfrak{E}_0(2)=0,\\&\mathfrak{E}_2(1,2,3)=5, \mathfrak{E}_1(1,2,3)=3,\\&\Rightarrow\operatorname{card}(\mathfrak{U}_3((1,2,3);(1,2)))=(3^3-3^{0+1-0})(3^5-3^3)=24\cdot 216=5184\end{aligned}$$

[41]Σημειωτέον ότι $G_{p,\mathbf{k}}[p^{l_{t-j}-1}]\cap\langle x_{t-j+1},\ldots,x_t\rangle[p^{l_{t-j}}]=\langle x_{t-j+1},\ldots,x_t\rangle[p^{l_{t-j}-1}]$.

[42]Προσοχή! *Όλες* οι υποομάδες τής $G$ που έχουν *τον ίδιο τύπο* $\mathbf{l}$ είναι (σύμφωνα με την πρόταση 9.1.8) *ισόμορφες* με την $G_{p,\mathbf{l}}$, χωρίς ωστόσο να είναι κατ' ανάγκην (συνολοθεωρητικώς) ίσες. Εδώ προσμετράται το πλήθος όσων δεν είναι (ανά ζεύγη) ίσες.

και

$$\begin{aligned}&\mathfrak{E}_1(1,2)=2, \mathfrak{E}_0(1,2)=0, \mathfrak{E}_1(2)=1, \mathfrak{E}_0(2)=0,\\ &\mathfrak{E}_2(1,2)=3, \mathfrak{E}_1(1,2)=2,\\ &\Rightarrow \mathrm{card}(\mathfrak{U}_3((1,2);(1,2)))=(3^2-3^{0+1-0})(3^3-3^2)=6\cdot 18=108.\end{aligned}$$

**9.2.28 Θεώρημα.** *Εάν $(G,+)$ είναι μια πεπερασμένη μη τετριμμένη αβελιανή $p$-ομάδα έχουσα τύπο $\mathbf{k}=(k_1,...,k_s)$, δηλαδή εάν $G\cong G_{p,\mathbf{k}}$, τότε ο αριθμός των υποομάδων της που έχουν τάξη $p^\xi$ (για κάποιον φυσικό αριθμό $\xi\leq k_1+...+k_s$) είναι ο*

$$\boxed{\mathrm{card}(\{H\in\mathbf{Subg}(G):|H|=p^\xi\})=\sum_{\mathbf{l}=(l_1,...,l_t)\in\mathcal{S}(\mathbf{k})\cap\Pi_t(\xi)}\left(\frac{\mathrm{card}(\mathfrak{U}_p(\mathbf{k};\mathbf{l}))}{\mathrm{card}(\mathfrak{U}_p(\mathbf{l};\mathbf{l}))}\right)}$$

(*υπολογιζόμενος μέσω τής προτάσεως* 9.2.24).

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το λήμμα 9.2.26. □

**9.2.29 Θεώρημα.** *Εάν $(G,+)$ είναι μια πεπερασμένη μη τετριμμένη αβελιανή $p$-ομάδα έχουσα τύπο $\mathbf{k}=(k_1,...,k_s)$, δηλαδή εάν $G\cong G_{p,\mathbf{k}}$, τότε ο αριθμός όλων των υποομάδων της είναι ο*

$$\boxed{\mathrm{card}(\mathbf{Subg}(G))=1+\sum_{\mathbf{l}\in\mathcal{S}(\mathbf{k})}\left(\frac{\mathrm{card}(\mathfrak{U}_p(\mathbf{k};\mathbf{l}))}{\mathrm{card}(\mathfrak{U}_p(\mathbf{l};\mathbf{l}))}\right)} \tag{9.44}$$

(*υπολογιζόμενος μέσω τής προτάσεως* 9.2.24).

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το λήμμα 9.2.26. □

**9.2.30 Σημείωση.** (i) Το πλήθος των προσθετέων στο άθροισμα (9.44) ισούται με

$$\mathrm{card}(\mathcal{S}(\mathbf{k}))=\sum_{t=1}^{s}\prod_{\varrho=s-t+1}^{s}k_\varrho.$$

Θα ήταν μια καλή εξάσκηση για τον αναγνώστη εάν προσπαθούσε να εξαγάγει για τις τιμές $s=2$ και $s=3$ τις (9.41) και (9.42), αντιστοίχως, *απευθείας* από το (9.44).

(ii) Παρά το γεγονός ότι οι (9.41), (9.42) και (9.44) εκφράζουν τον $\mathrm{card}(\mathbf{Subg}(G))$ ως αποτίμηση μιας *ρητής συναρτήσεως* στο $p$, είναι δυνατόν να αποδειχθεί (όπως συμβαίνει και με τον $\mathrm{card}(\mathbf{CSubg}(G))$, βλ. 9.2.12) ότι ο $\mathrm{card}(\mathbf{Subg}(G))$ ισούται με την αποτίμηση ενός *πολυωνύμου* (μιας απροσδιορίστου, με ακεραίους συντελεστές) στο $p$. (Καθένα εκ των κλασμάτων $\frac{\mathrm{card}(\mathfrak{U}_p(\mathbf{k};\mathbf{l}))}{\mathrm{card}(\mathfrak{U}_p(\mathbf{l};\mathbf{l}))}$ υπολογίζεται συναρτήσει των λεγομένων *γκαουσιανών διωνυμικών συντελεστών*, οι οποίοι, ως γνωστόν, είναι πολυωνυμικοί.)

# 9.3 ΑΥΤΟΜΟΡΦΙΣΜΟΙ ΠΕΠΕΡΑΣΜΕΝΩΝ ΑΒΕΛΙΑΝΩΝ ΟΜΑΔΩΝ

Έστω $|G| = p_1^{\nu_1} \cdots p_\kappa^{\nu_\kappa}$ η κανονική παράσταση (B.19) τής τάξεως τυχούσας πεπερασμένης μη τετριμμένης αβελιανής ομάδας $G$ ως γινομένου (κατάλληλων δυνάμεων) πρώτων αριθμών $p_1,\ldots,p_\kappa$ με $p_1 < \cdots < p_\kappa$ και έστω

$$G = G(p_1) \oplus_{\text{εσ.}} G(p_2) \oplus_{\text{εσ.}} \cdots \oplus_{\text{εσ.}} G(p_\kappa)$$

η πρωτεύουσα αποσύνθεση τής $G$ με $|G(p_\varrho)| = p_\varrho^{\nu_\varrho}$, $\forall \varrho \in \{1,\ldots,\kappa\}$. (Βλ. πρόταση 9.1.17.) Επειδή (σύμφωνα με το 7.1.85 (ii)) $G \cong G(p_1) \oplus \cdots \oplus G(p_\kappa)$ και

$$\mathrm{Aut}(G(p_1) \oplus \cdots \oplus G(p_\kappa)) \cong \mathrm{Aut}(G(p_1)) \times \cdots \times \mathrm{Aut}(G(p_\kappa)) \tag{9.45}$$

(κατόπιν εφαρμογής τής προτάσεως 7.1.76), η μελέτη τής ομάδας των αυτομορφισμών τής $G$ ανάγεται στη μελέτη τής ομάδας των αυτομορφισμών καθεμιάς εκ των $G(p_\varrho)$, $\varrho \in \{1,\ldots,\kappa\}$.

► **Υπολογισμός τού αριθμού των αυτομορφισμών**. Κατ' αρχάς θα υπολογίσουμε την τάξη

$$|\mathrm{Aut}(G)| = \prod_{\varrho=1}^{\kappa} |\mathrm{Aut}(G(p_\varrho))|$$

τής $\mathrm{Aut}(G)$ εφαρμόζοντας το ακόλουθο θεώρημα (για καθεμιά εκ των πρωτευουσών συνιστωσών της).

**9.3.1 Θεώρημα. (Απαρίθμηση αυτομορφισμών)** *Έστω $p$ ένας πρώτος αριθμός. Για κάθε πεπερασμένη μη τετριμμένη αβελιανή $p$-ομάδα $(G,+)$ ισχύουν τα εξής:*
(i) *Εάν η $G$ είναι τού τύπου $\mathbf{k} = (\underbrace{k,k,\ldots,k}_{s \text{ φορές}})$, $s \geq 1$, τότε*[43]

$$\boxed{|\mathrm{Aut}(G)| = \prod_{j=1}^{s} (p^{ks} - p^{(k-1)s+j-1}) = p^{s^2(k-1)} \prod_{j=1}^{s} (p^s - p^{j-1}).}$$

(ii) *Εάν η $G$ είναι τού τύπου $\mathbf{k} = (k_1,k_2,\ldots,k_s)$, $s \geq 2$, και εάν τουλάχιστον δύο εκ των $k_1,\ldots,k_s$ είναι διαφορετικοί, τότε θεωρούμε εκείνο το υποσύνολο δεικτών $\{\varrho_1,\ldots,\varrho_\xi\} \subseteq \{1,\ldots,s\}$* (με $\xi \geq 2$ και $\varrho_1 \geq 1$, $\varrho_\xi = s$) *για το οποίο ισχύει*

$$k_1 = \cdots = k_{\varrho_1} < k_{\varrho_1+1} = \cdots = k_{\varrho_2} < \cdots\cdots < k_{\varrho_{\xi-1}+1} = \cdots = k_{\varrho_\xi} = k_s,$$

*και ορίζουμε τους $\varrho_0 := 0$ και $s_i := \varrho_i - \varrho_{i-1}$, $\forall i \in \{1,\ldots,\xi\}$, με $s_1 + \cdots + s_\xi = s$. Εν τοιαύτη περιπτώσει,*

$$\boxed{|\mathrm{Aut}(G)| = \prod_{i=1}^{\xi} p^{s_i\left(k_{\varrho_i}(2(s-\varrho_i)+s_i)-s_i\right)} \prod_{j=1}^{s_i} (p^{s_i} - p^{j-1}).}$$

[43] Ειδικότερα, όταν η $G$ είναι *στοιχειώδης αβελιανή* (δηλαδή όταν $k=1$), έχουμε $|\mathrm{Aut}(G)| = \prod_{j=1}^{s} (p^s - p^{j-1})$.

ΑΠΟΔΕΙΞΗ. (i) Εάν η $G$ είναι τού τύπου $\mathbf{k} = (\underbrace{k, k, ..., k}_{s \text{ φορές}})$, τότε, επειδή

$$|\mathrm{Aut}(G)| = |\mathrm{Aut}(G_{p,\mathbf{k}})| \underset{(9.43)}{=} \mathrm{card}\left(\mathfrak{U}_p(\mathbf{k};\mathbf{k})\right),$$

είναι αρκετό (για τον υπολογισμό τής τάξεως τής $\mathrm{Aut}(G)$) να χρησιμοποιηθεί η πρόταση 9.2.24 (στην ειδική περίπτωση όπου $t = s$ και $\mathbf{l} = \mathbf{k}$). Σημειωτέον ότι $\mathfrak{E}_k(\mathbf{k}) = ks$, $\mathfrak{E}_{k-1}(\mathbf{k}) = (k-1)s$, και όταν $s \geq 2$,

$$\mathfrak{E}_k(\mathbf{k}_{(j)}) = k(j-1),\ \mathfrak{E}_{k-1}(\mathbf{k}_{(j)}) = (k-1)(j-1),\ \forall j \in \{1, ..., s-1\}.$$

(ii) Εάν η $G$ είναι τού τύπου $\mathbf{k} = (k_1, k_2, ..., k_s)$, $s \geq 2$, και τουλάχιστον δύο εκ των $k_1, k_2, ..., k_s$ είναι διαφορετικοί, τότε $G \cong G_{p,\mathbf{k}} \cong G_{p,\mathbf{k}_1} \oplus G_{p,\mathbf{k}_2} \oplus \cdots \oplus G_{p,\mathbf{k}_\xi}$ και, ως εκ τούτου,

$$\mathrm{Aut}(G) \cong \mathrm{Aut}(G_{p,\mathbf{k}}) \cong \mathrm{Aut}\left(\bigoplus_{i=1}^{\xi} G_{p,\mathbf{k}_i}\right),$$

όπου $\mathbf{k}_i := (\underbrace{k_{\varrho_i}, k_{\varrho_i}, ..., k_{\varrho_i}}_{s_i \text{ φορές}})$, $\forall i \in \{1, ..., \xi\}$. Επειδή οι ομάδες $G_{p,\mathbf{k}_1}, ..., G_{p,\mathbf{k}_\xi}$ δεν διαθέτουν *ανά δύο* κοινούς ευθείς προσθετέους, είναι δυνατόν να εφαρμοσθεί το θεώρημα 7.1.77 τού Bidwell για την ομάδα $\mathrm{Aut}(G)$. Εξ αυτού έπεται ότι

$$|\mathrm{Aut}(G)| = \prod_{i=1}^{\xi} |\mathrm{Aut}(G_{p,\mathbf{k}_i})| \prod_{1 \leq i, i' \leq \xi,\, i \neq i'} |\mathrm{Hom}(G_{p,\mathbf{k}_i}, \underbrace{Z(G_{p,\mathbf{k}_{i'}})}_{= G_{p,\mathbf{k}_{i'}}})|. \tag{9.46}$$

Για κάθε $i \in \{1, ..., \xi\}$ ισχύει (λόγω τού (i))

$$|\mathrm{Aut}(G_{p,\mathbf{k}_i})| = p^{s_i^2 (k_{\varrho_i} - 1)} \prod_{j=1}^{s_i} \left(p^{s_i} - p^{j-1}\right). \tag{9.47}$$

Από την άλλη μεριά, για $i, i' \in \{1, ..., \xi\}$, $i \neq i'$, έχουμε

$$\begin{aligned} \mathrm{Hom}(G_{p,\mathbf{k}_i}, G_{p,\mathbf{k}_{i'}}) &= \mathrm{Hom}(\underbrace{\mathbb{Z}_{p^{k_{\varrho_i}}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_{\varrho_i}}}}_{s_i \text{ φορές}}, \underbrace{\mathbb{Z}_{p^{k_{\varrho_{i'}}}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_{\varrho_{i'}}}}}_{s_{i'} \text{ φορές}}) \\ &\cong \underbrace{\mathrm{Hom}(\mathbb{Z}_{p^{k_{\varrho_i}}}, \mathbb{Z}_{p^{k_{\varrho_{i'}}}}) \oplus \cdots \oplus \mathrm{Hom}(\mathbb{Z}_{p^{k_{\varrho_i}}}, \mathbb{Z}_{p^{k_{\varrho_{i'}}}})}_{s_i s_{i'} \text{ φορές}} \end{aligned}$$

και $\mathrm{Hom}(\mathbb{Z}_{p^{k_{\varrho_i}}}, \mathbb{Z}_{p^{k_{\varrho_{i'}}}}) \cong \mathbb{Z}_{\text{μκδ}(p^{k_{\varrho_i}}, p^{k_{\varrho_{i'}}})}$, όπου $\text{μκδ}(p^{k_{\varrho_i}}, p^{k_{\varrho_{i'}}}) \underset{\text{B.3.16}}{=} p^{\min\{k_{\varrho_i}, k_{\varrho_{i'}}\}}$. (Βλ. ασκήσεις **7-54** και **4-48**.) Επομένως,

$$\left|\mathrm{Hom}(G_{p,\mathbf{k}_i}, G_{p,\mathbf{k}_{i'}})\right| = p^{\min\{k_{\varrho_i}, k_{\varrho_{i'}}\} s_i s_{i'}}$$

και[44]

$$\left\{\begin{array}{l} \displaystyle\prod_{1\leq i,i'\leq \xi, i\neq i'} \left|\mathrm{Hom}(G_{p,\mathbf{k}_i}, G_{p,\mathbf{k}_{i'}})\right| = \prod_{1\leq i,i'\leq \xi, i\neq i'} p^{\min\{k_{\varrho_i},k_{\varrho_{i'}}\}s_i s_{i'}} \\ \displaystyle= \prod_{1\leq i<i'\leq \xi} p^{2\min\{k_{\varrho_i},k_{\varrho_{i'}}\}s_i s_{i'}} = \prod_{1\leq i<i'\leq \xi} p^{2k_{\varrho_i}s_i s_{i'}} = \prod_{i=1}^{\xi} p^{2k_{\varrho_i}s_i(s-\varrho_i)}. \end{array}\right\} \tag{9.48}$$

Η τάξη $|\mathrm{Aut}(G)|$ τής $\mathrm{Aut}(G)$ υπολογίζεται μέσω των (9.46), (9.47) και (9.48). $\square$

**9.3.2 Παράδειγμα.** Η 2-ομάδα $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_8$ (τάξεως 2048 και τύπου $(1,1,1,2,3,3)$) διαθέτει ακριβώς

$$\begin{aligned} &\left(2^{3(1(2(6-3)+3)-3)}(2^3-1)(2^3-2)(2^3-2^2)\right) \\ &\times \left(2^{1(2(2(6-4)+1)-1)}(2-1)\right) \times \left(2^{2(3(2(6-6)+2)-2)}(2^2-1)(2^2-2)\right) \\ &= 44\,040\,192 \cdot 512 \cdot 1536 = 34\,634\,616\,274\,944 \end{aligned}$$

αυτομορφισμούς!

**9.3.3 Πόρισμα.** (**M.J. Curran, R. Heffernan & D. MacHale**, 2011.) *Έστω $(G,+)$ μια πεπερασμένη μη τετριμμένη αβελιανή ομάδα. Εάν ισχύει $|\mathrm{Aut}(G)| = |G|$, τότε*[45] *είτε $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^n}$ για κάποιον $n \geq 2$ είτε $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^n}$ για κάποιον $n \geq 1$.*

**9.3.4 Σημείωση.** Η μελέτη τής ομάδας αυτομορφισμών (αυτής καθεαυτής, όχι απλώς τής τάξεώς της) μιας πεπερασμένης μη τετριμμένης αβελιανής $p$-ομάδας (μέσω καταλλήλων πινάκων) συναντάται για πρώτη φορά (σε πλήρη γενικότητα) σε ένα άρθρο τού A. Ranum[46] το 1907. Αργότερα, κατά τη δεκαετία τού 1920, παρόμοια αποτελέσματα (βασιζόμενα, όμως, σε διαφορετικές αποδεικτικές μεθόδους) εμφανίζονται σε μια μονογραφία τού A. Chatelet[47] και σε ένα άρθρο τού K. Shoda[48]. Επίσης, μια άλλη προσέγγιση (και επέκταση) των αποτελεσμάτων τού Ranum εντοπίζεται σε ένα εκτενές άρθρο τού K. Latt[49] (τού 1970). Σε νεότερες σχετικές εργασίες των C.J. Hillar & D.L. Rhea[50] και M. Golasiński & D.L. Gonçalves[51] έμφαση δίδεται στην απλούστευση τής ορολογίας και των αποδείξεων, και στην πρόταξη τής περιγραφής τού δακτυλίου των ενδομορφισμών των ομάδων αναφοράς.

[44] Η τρίτη εκ των ισοτήτων (9.48) έπεται από το ότι $[i < i' \Rightarrow k_{\varrho_i} < k_{\varrho_{i'}}]$ και η τέταρτη ύστερα από αναπαραμέτρηση των εκθετών (λαμβανομένου υπ' όψιν τού ότι $\varrho_i = s_1 + \cdots + s_i \forall i \in \{1,\ldots,\xi\}$).

[45] Η απόδειξη δεν είναι δύσκολη και μπορεί να διαβασθεί απευθείας από το πρωτότυπο άρθρο των M.J. Curran, R. Heffernan & D. MacHale: *On the order of the automorphism group of a finite group*, Communications in Algebra **39** (2011), 3616-3624.

[46] A. Ranum: *The group of classes of congruent matrices with application to the group of isomorphisms of any abelian group*, Transactions of the Amer. Math. Soc. **8** (1907), 71-91.

[47] A. Chatelet: *Les groupes abéliens finis et les modules de points entiers,* Lille 1925.

[48] K. Shoda: *Über die Automorphismen einer endlichen Abelschen Gruppe,* Mathematische Annalen **100** (1928), 674-686.

[49] K. Latt: *Zur Konstruktion der Automorphismen einer endlichen Abelschen Gruppe*, Mathematische Nachrichten **45** (1970), 101-142.

[50] C.J. Hillar & D.L. Rhea: *Automorphisms of finite abelian groups*, American Math. Monthly **11** (2007), 917-923.

[51] M. Golasiński & D.L. Gonçalves: *On automorphisms of finite abelian p-groups*, Mathematica Solvaca **58** (2008), 405-412.

► **Περιγραφή τού δακτυλίου των ενδομορφισμών**. Έστω $p$ ένας πρώτος αριθμός και έστω $(G,+)$ τυχούσα πεπερασμένη μη τετριμμένη αβελιανή $p$-ομάδα τού τύπου $\mathbf{k}=(k_1,...,k_s)$. Τότε

$$G \cong G_{p,\mathbf{k}} := \mathbb{Z}_{p^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_s}} = \left\langle ([1]_{p^{k_1}},...,[1]_{p^{k_s}}) \right\rangle$$

και κάθε στοιχείο τής $G_{p,\mathbf{k}}$ είναι τής μορφής $([m_1]_{p^{k_1}},...,[m_s]_{p^{k_s}})$, για κάποιους $m_1,...,m_s \in \mathbb{Z}$. Έστω $\pi_j : \mathbb{Z} \longrightarrow \mathbb{Z}_{p^{k_j}}$ ο επιμορφισμός $m \longmapsto \pi_j(m) := [m]_{p^{k_j}}$ (για κάθε $j \in \{1,...,s\}$) και έστω

$$\pi : \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{s \text{ φορές}} \longrightarrow G_{p,\mathbf{k}},\ (m_1,...,m_s) \overset{\pi}{\longmapsto} (\pi_1(m_1),...,\pi_s(m_s)),$$

ο επιμορφισμός ο επαγόμενος επί τής $G_{p,\mathbf{k}}$.

**9.3.5 Λήμμα.** *Εάν* $\vartheta \in \mathrm{End}(G_{p,\mathbf{k}})$ *και εάν*

$$\begin{aligned}
\vartheta([1]_{p^{k_1}},[0]_{p^{k_2}},[0]_{p^{k_3}},...,[0]_{p^{k_s}}) &= ([a_{11}]_{p^{k_1}},[a_{12}]_{p^{k_2}},...,[a_{1s}]_{p^{k_s}}),\\
\vartheta([0]_{p^{k_1}},[1]_{p^{k_2}},[0]_{p^{k_3}},...,[0]_{p^{k_s}}) &= ([a_{21}]_{p^{k_1}},[a_{22}]_{p^{k_2}},...,[a_{2s}]_{p^{k_s}}),\\
&\ \ \vdots\\
\vartheta([0]_{p^{k_1}},[0]_{p^{k_2}},...,[0]_{p^{k_{s-1}}},[1]_{p^{k_s}}) &= ([a_{s1}]_{p^{k_1}},[a_{s2}]_{p^{k_2}},...,[a_{ss}]_{p^{k_s}}),
\end{aligned}$$

*όπου* $0 \le a_{ij} < p^{k_j}, \forall (i,j) \in \{1,...,s\} \times \{1,...,s\}$, *τότε η εικόνα οιουδήποτε στοιχείου* $([m_1]_{p^{k_1}},...,[m_s]_{p^{k_s}}) \in G_{p,\mathbf{k}}$ *μέσω τού* $\vartheta$ *είναι η*

$$\vartheta([m_1]_{p^{k_1}},...,[m_s]_{p^{k_s}}) = \pi((m_1,...,m_s)\mathbf{A}_\vartheta), \tag{9.49}$$

*όπου*

$$\mathbf{A}_\vartheta := \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1s}\\ a_{21} & a_{22} & \cdots & a_{2s}\\ \vdots & \vdots & & \vdots\\ a_{s1} & a_{s2} & \cdots & a_{ss}\end{pmatrix} \in \mathrm{Mat}_{s\times s}(\mathbb{Z}). \tag{9.50}$$

ΑΠΟΔΕΙΞΗ. Προφανώς,

$$\begin{aligned}
&\vartheta([m_1]_{p^{k_1}},...,[m_s]_{p^{k_s}}) = \sum_{i=1}^{s} m_i \vartheta([0]_{p^{k_1}},,...,[1]_{p^{k_i}},...,[0]_{p^{k_s}})\\
&= \sum_{i=1}^{s} m_i([a_{i1}]_{p^{k_1}},[a_{i2}]_{p^{k_2}},...,[a_{is}]_{p^{k_s}}) = \sum_{i=1}^{s} m_i(\pi_1(a_{i1}),...,\pi_s(a_{is}))\\
&= \sum_{i=1}^{s} m_i \pi(a_{i1},...,a_{is}) = \pi\left(\sum_{i=1}^{s} m_i(a_{i1},...,a_{is})\right),
\end{aligned}$$

απ' όπου έπεται η ισότητα (9.49). □

Είναι εύκολο να αποδειχθεί ότι το

$$\mathfrak{R}_{p,\mathbf{k}} := \left\{ \mathbf{A} = (a_{ij})_{1\le i,j\le s} \in \mathrm{Mat}_{s\times s}(\mathbb{Z}) \;\middle|\; \begin{array}{l} a_{ij} \equiv 0 (\mathrm{mod}\, p^{k_j - k_i})\\ \text{για οιουσδήποτε } i,j \in \{1,...,s\}\\ \text{με } 1 \le i \le j \le s \end{array} \right\},$$

εφοδιαζόμενο με τη συνήθη πρόσθεση και με τον συνήθη πολλαπλασιασμό πινάκων, αποτελεί έναν υποδακτύλιο τού δακτυλίου $\mathrm{Mat}_{s\times s}(\mathbb{Z})$ με τον $\mathbf{I}_s$ ως μοναδιαίο του στοιχείο. Όπως θα δούμε στο θεώρημα 9.3.7, μέσω τού $\mathfrak{R}_{p,\mathbf{k}}$ είναι δυνατή μια φυσική περιγραφή (μέχρις ισομορφισμού) τού *δακτυλίου* $\mathrm{End}(G_{p,\mathbf{k}})$ (βλ. 2.4.30 (ii)), ο οποίος είναι ισόμορφος τού $\mathrm{End}(G)$.

**9.3.6 Λήμμα.** *Η απεικόνιση*

$$\mathfrak{h}:\mathfrak{R}_{p,\mathbf{k}}\longrightarrow \mathrm{End}(G_{p,\mathbf{k}}),\ \mathbf{A}\longmapsto \mathfrak{h}(\mathbf{A}),$$
$$\mathfrak{h}(\mathbf{A})([m_1]_{p^{k_1}},...,[m_s]_{p^{k_s}}):=\pi((m_1,...,m_s)\mathbf{A}),$$

*αποτελεί έναν επιμορφισμό δακτυλίων.*

ΑΠΟΔΕΙΞΗ. Εάν $\mathbf{A}=(a_{ij})_{1\leq i,j\leq s}\in\mathfrak{R}_{p,\mathbf{k}}$ και

$$([m_1]_{p^{k_1}},...,[m_s]_{p^{k_s}})=([m_1']_{p^{k_1}},...,[m_s']_{p^{k_s}})$$

για κάποιους $m_1,...,m_s,m_1',...,m_s'\in\mathbb{Z}$, τότε $p^{k_j}\mid m_j-m_j',\forall j\in\{1,...,s\}$, και

$$\pi_j\left(\sum_{i=1}^{s}m_ia_{ij}\right)-\pi_j\left(\sum_{i=1}^{s}m_i'a_{ij}\right)=\pi_j\left(\sum_{i=1}^{s}m_ia_{ij}-\sum_{i=1}^{s}m_i'a_{ij}\right)$$
$$=\sum_{i=1}^{s}\pi_j\left(\tfrac{a_{ij}}{p^{k_j-k_i}}p^{k_j-k_i}\left(m_i-m_i'\right)\right)=([0]_{p^{k_1}},[0]_{p^{k_2}},...,[0]_{p^{k_s}}),$$

διότι $p^{k_j}\mid p^{k_j-k_i}(m_i-m_i')$ όταν $j\in\{i,...,s\}$ και $p^{k_j}\mid m_j-m_j'$ όταν $j\in\{1,...,i-1\}$. Άρα $\pi((m_1,...,m_s)\mathbf{A})=\pi((m_1',...,m_s')\mathbf{A})$ και η ανωτέρω $\mathfrak{h}(\mathbf{A})$ είναι *καλώς ορισμένη* απεικόνιση από την $G_{p,\mathbf{k}}$ στην $G_{p,\mathbf{k}}$. Επειδή δε,

$$\mathfrak{h}(\mathbf{A})\left(([m_1]_{p^{k_1}},..,[m_s]_{p^{k_s}})+([m_1']_{p^{k_1}},..,[m_s']_{p^{k_s}})\right)=\mathfrak{h}(\mathbf{A})([m_1+m_1']_{p^{k_1}},..,[m_s+m_s']_{p^{k_s}})$$
$$=\pi((m_1+m_1',...,m_s+m_s')\mathbf{A})=\pi((m_1,...,m_s)\mathbf{A})+\pi((m_1',...,m_s')\mathbf{A})$$
$$=\mathfrak{h}(\mathbf{A})([m_1]_{p^{k_1}},...,[m_s]_{p^{k_s}})+\mathfrak{h}(\mathbf{A})([m_1']_{p^{k_1}},...,[m_s']_{p^{k_s}}),$$

για οιουσδήποτε $m_1,...,m_s,m_1',...,m_s'\in\mathbb{Z}$, η $\mathfrak{h}(\mathbf{A})$ είναι ένας ενδομορφισμός τής $G_{p,\mathbf{k}}$. Παρομοίως αποδεικνύεται ότι

$$\mathfrak{h}(\mathbf{A}+\mathbf{B})=\mathfrak{h}(\mathbf{A})+\mathfrak{h}(\mathbf{B}),\ \mathfrak{h}(\mathbf{AB})=\mathfrak{h}(\mathbf{A})\circ\mathfrak{h}(\mathbf{B}),\ \mathfrak{h}(\mathbf{I}_s)=\mathrm{id}_{G_{p,\mathbf{k}}},$$

για οιουσδήποτε $\mathbf{A},\mathbf{B}\in\mathfrak{R}_{p,\mathbf{k}}$, οπότε η $\mathfrak{h}$ αποτελεί ομομορφισμό δακτυλίων (με μοναδιαίο στοιχείο). Έστω τώρα τυχών $\vartheta\in\mathrm{End}(G_{p,\mathbf{k}})$. Επειδή για οιουσδήποτε $m_1,...,m_s\in\mathbb{Z}$ έχουμε

$$\vartheta([m_1]_{p^{k_1}},...,[m_s]_{p^{k_s}})=\pi((m_1,...,m_s)\mathbf{A}_\vartheta), \tag{9.51}$$

όπου $\mathbf{A}_\vartheta=(a_{ij})_{1\leq i,j\leq s}$ ο πίνακας (9.50) ο ορισθείς στο λήμμα 9.3.5, και για κάθε $i\in\{1,...,s\}$ ισχύει

$$0_{G_{p,\mathbf{k}}}=([0]_{p^{k_1}},...,[0]_{p^{k_s}})=\vartheta([0]_{p^{k_1}},...,[0]_{p^{k_{i-1}}},[p^{k_i}]_{p^{k_i}},[0]_{p^{k_{i+1}}}...,[0]_{p^{k_s}})$$
$$=p^{k_i}\vartheta([0]_{p^{k_1}},...,[0]_{p^{k_{i-1}}},[1]_{p^{k_i}},[0]_{p^{k_{i+1}}}...,[0]_{p^{k_s}})=p^{k_i}([a_{i1}]_{p^{k_1}},...,[a_{is}]_{p^{k_s}})$$
$$=([p^{k_i}a_{i1}]_{p^{k_1}},...,[p^{k_i}a_{is}]_{p^{k_s}})\Rightarrow p^{k_j}\mid p^{k_i}a_{ij},\forall(i,j)\in\{1,...,s\}\times\{1,...,s\},$$

συμπεραίνουμε ότι $p^{k_j - k_i} \mid a_{ij}$ όταν[52] $1 \leq i \leq j \leq s$. Επομένως, $\mathbf{A}_\vartheta \in \mathfrak{R}_{p,\mathbf{k}}$. Από την (9.51) προκύπτει ότι $\mathfrak{h}(\mathbf{A}_\vartheta) = \vartheta$, ήτοι ότι η $\mathfrak{h}$ είναι επιρριπτική. □

**9.3.7 Θεώρημα. (Χαρακτηρισμός ενδομορφισμών.)** *Η απεικόνιση*

$$\boxed{\begin{gathered}\mathfrak{R}_{p,\mathbf{k}}/\mathrm{Ker}(\mathfrak{h}) \longrightarrow \mathrm{End}(G_{p,\mathbf{k}})\,(\cong \mathrm{End}(G)) \\ \mathbf{A} + \mathrm{Ker}(\mathfrak{h}) \longmapsto \mathfrak{h}(\mathbf{A})\end{gathered}}$$

*αποτελεί έναν ισομορφισμό δακτυλίων, όπου*

$$\mathrm{Ker}(\mathfrak{h}) = \left\{ \mathbf{A} = (a_{ij})_{1 \leq i,j \leq s} \in \mathfrak{R}_{p,\mathbf{k}} \;\middle|\; \begin{array}{l} a_{ij} \equiv 0 (\mathrm{mod}\, p^{k_j}), \\ \forall (i,j) \in \{1,...,s\} \times \{1,...,s\} \end{array} \right\}. \quad (9.52)$$

ΑΠΟΔΕΙΞΗ. Αρκεί να προσδιορισθεί ο $\mathrm{Ker}(\mathfrak{h})$. Έστω $\mathbf{A} = (a_{ij})_{1 \leq i,j \leq s} \in \mathfrak{R}_{p,\mathbf{k}}$, τέτοιος ώστε να ισχύει $p^{k_j} \mid a_{ij}, \forall (i,j) \in \{1,...,s\} \times \{1,...,s\}$. Τότε για κάθε $([m_1]_{p^{k_1}}, ..., [m_s]_{p^{k_s}}) \in G_{p,\mathbf{k}}$ έχουμε

$$\begin{aligned}
&\mathfrak{h}(\mathbf{A})([m_1]_{p^{k_1}}, ..., [m_s]_{p^{k_s}}) = \sum_{i=1}^{s} m_i \mathfrak{h}(\mathbf{A})([0]_{p^{k_1}}, , ..., [1]_{p^{k_i}}, ..., [0]_{p^{k_s}}) \\
&= \sum_{i=1}^{s} m_i (\pi_1(a_{i1}), ..., \pi_s(a_{is})) = \sum_{i=1}^{s} m_i ([a_{i1}]_{p^{k_1}}, ..., [a_{is}]_{p^{k_s}}) \\
&= ([0]_{p^{k_1}}, ..., [0]_{p^{k_s}}) = 0_{G_{p,\mathbf{k}}} \Rightarrow \mathbf{A} \in \mathrm{Ker}(\mathfrak{h}).
\end{aligned}$$

Και αντιστρόφως· εάν $\mathbf{A} = (a_{ij})_{1 \leq i,j \leq s} \in \mathrm{Ker}(\mathfrak{h})$, τότε για κάθε $i \in \{1,...,s\}$ ισχύει

$$\begin{aligned}
&0_{G_{p,\mathbf{k}}} = ([0]_{p^{k_1}}, ..., [0]_{p^{k_s}}) = \mathfrak{h}(\mathbf{A})([0]_{p^{k_1}}, , ..., [1]_{p^{k_i}}, ..., [0]_{p^{k_s}}) \\
&= (\pi_1(a_{i1}), ..., \pi_s(a_{is})) = ([a_{i1}]_{p^{k_1}}, ..., [a_{is}]_{p^{k_s}}) \\
&\Rightarrow p^{k_j} \mid a_{ij}, \ \forall j \in \{1,...,s\},
\end{aligned}$$

οπότε η ισότητα (9.52) είναι αληθής. □

► **Περιγραφή τής ομάδας των αυτομορφισμών**. Διατηρώντας τόν ανωτέρω εισαχθέντα συμβολισμό έχουμε τη δυνατότητα να περιγράψουμε επακριβώς το πότε ένας ενδομορφισμός τής $G \cong G_{p,\mathbf{k}}$ είναι αυτομορφισμός.

**9.3.8 Θεώρημα. (Περί τής Aut$(G)$.)** *Έστω* $\vartheta = \mathfrak{h}(\mathbf{A}_\vartheta) \in \mathrm{End}(G_{p,\mathbf{k}})\,(\cong \mathrm{End}(G))$. *Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*[53]:

(i) $\vartheta \in \mathrm{Aut}(G_{p,\mathbf{k}})$.

(ii) $[\mathbf{A}_\vartheta]_p \in \mathrm{GL}_s(\mathbb{Z}_p)$.

*Ως εκ τούτου,*

$$\boxed{\mathrm{Aut}(G) \cong \mathrm{Aut}(G_{p,\mathbf{k}}) = \{\vartheta \in \mathrm{End}(G_{p,\mathbf{k}}) \,|\, [\mathbf{A}_\vartheta]_p \in \mathrm{GL}_s(\mathbb{Z}_p)\}\,.}$$

[52] Εξ υποθέσεως, $1 \leq i \leq j \leq s \Rightarrow k_i \leq k_j$.

[53] Για κάθε $\mathbf{A} = (a_{ij})_{1 \leq i,j \leq s} \in \mathrm{Mat}_{s \times s}(\mathbb{Z})$ θέτουμε $[\mathbf{A}]_p := ([a_{ij}]_p)_{1 \leq i,j \leq s} \in \mathrm{Mat}_{s \times s}(\mathbb{Z}_p)$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Έστω $\vartheta \in \mathrm{Aut}(G_{p,\mathbf{k}})$. Επειδή $\vartheta = \mathfrak{h}(\mathbf{A}_\vartheta)$ και $\vartheta^{-1} = \mathfrak{h}(\mathbf{A}_{\vartheta^{-1}})$, έχουμε $\mathfrak{h}(\mathbf{A}_\vartheta \mathbf{A}_{\vartheta^{-1}} - \mathbf{I}_s) = \mathfrak{h}(\mathbf{A}_{\vartheta \circ \vartheta^{-1}}) - \mathfrak{h}(\mathbf{I}_s) = \mathfrak{h}(\mathbf{I}_s) - \mathfrak{h}(\mathbf{I}_s) = 0_{\mathrm{End}(G_{p,\mathbf{k}})}$, οπότε $\mathbf{A}_\vartheta \mathbf{A}_{\vartheta^{-1}} - \mathbf{I}_s \in \mathrm{Ker}(\mathfrak{h})$. Επειδή εξ υποθέσεως $k_j \geq 1$, $\forall j \in \{1, ..., s\}$, από την περιγραφή (9.52) τού $\mathrm{Ker}(\mathfrak{h})$ συμπεραίνουμε ότι *όλες* οι εγγραφές τού $\mathbf{A}_\vartheta \mathbf{A}_{\vartheta^{-1}} - \mathbf{I}_s$ είναι διαιρετές δια τού $p$. Επομένως, $[\mathbf{A}_\vartheta \mathbf{A}_{\vartheta^{-1}}]_p = [\mathbf{I}_s]_p$ και

$$[1]_p = [\det(\mathbf{A}_\vartheta \mathbf{A}_{\vartheta^{-1}})]_p \underset{\text{D.2.11}}{=} [\det(\mathbf{A}_\vartheta) \det(\mathbf{A}_{\vartheta^{-1}})]_p = [\det(\mathbf{A}_\vartheta)]_p \, [\det(\mathbf{A}_{\vartheta^{-1}})]_p .$$

Εξ αυτού έπεται ότι $[\det(\mathbf{A}_\vartheta)]_p \neq [0]_p$ ($\Leftrightarrow [\mathbf{A}_\vartheta]_p \in \mathbf{GL}_s(\mathbb{Z}_p)$).

(ii)⇒(i) Ας υποθέσουμε, αντιστρόφως, ότι $p \nmid \det(\mathbf{A}_\vartheta)$. Τότε μκδ$(\det(\mathbf{A}_\vartheta), p) = 1$ και, κατ' επέκταση, μκδ$(\det(\mathbf{A}_\vartheta), p^{k_s}) = 1$. (Βλ. πόρισμα B.2.13.) Επιλέγουμε $\lambda \in \mathbb{Z} : [\lambda]_{p^{k_s}} \, [\det(\mathbf{A}_\vartheta)]_{p^{k_s}} = [1]_{p^{k_s}}$. (Βλ. πρόταση B.4.43.) Προφανώς,

$$\lambda \det(\mathbf{A}_\vartheta) \equiv 1 (\mathrm{mod}\, p^{k_s}) \underset{k_j \leq k_s}{\Longrightarrow} [\lambda \det(\mathbf{A}_\vartheta) \equiv 1 (\mathrm{mod}\, p^{k_j}), \forall j \in \{1, ..., s\}]$$

και ορίζεται ο πίνακας $\mathbf{C}_\vartheta := \lambda \, \mathbf{adj}(\mathbf{A}_\vartheta) \in \mathfrak{R}_{p,\mathbf{k}}$ (όπου $\mathbf{adj}(\mathbf{A}_\vartheta)$ ο πίνακας ο προσαρτημένος στον $\mathbf{A}_\vartheta$, βλ. D.2.12). Δυνάμει τού θεωρήματος D.2.15,

$$\begin{aligned} &\mathfrak{h}(\mathbf{A}_\vartheta) \circ \mathfrak{h}(\mathbf{C}_\vartheta) = \mathfrak{h}(\mathbf{A}_\vartheta \mathbf{C}_\vartheta) = \mathfrak{h}(\mathbf{C}_\vartheta \mathbf{A}_\vartheta) = \mathfrak{h}(\mathbf{C}_\vartheta) \circ \mathfrak{h}(\mathbf{A}_\vartheta) \\ &= \mathfrak{h}(\lambda \det(\mathbf{A}_\vartheta) \mathbf{I}_s) = \mathfrak{h}(\mathbf{I}_s) = \mathrm{id}_{G_{p,\mathbf{k}}}, \end{aligned}$$

καθότι $\lambda \det(\mathbf{A}_\vartheta)\mathbf{I}_s - \mathbf{I}_s = (\lambda \det(\mathbf{A}_\vartheta) - 1)\, \mathbf{I}_s \in \mathrm{Ker}(\mathfrak{h})$. Άρα $\vartheta = \mathfrak{h}(\mathbf{A}_\vartheta) \in \mathrm{Aut}(G_{p,\mathbf{k}})$ (έχων ως αντίστροφό του τον $\vartheta^{-1} = \mathfrak{h}(\mathbf{C}_\vartheta)$). □

**9.3.9 Σημείωση.** Η ομάδα $\mathrm{Aut}(G_{p,\mathbf{k}})$ είναι *μη αβελιανή* όταν $s \geq 2$. Πράγματι· εάν θεωρήσουμε τους πίνακες

$$\mathbf{A}_1 := \begin{pmatrix} 1 & p^{k_2-k_1} & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}, \mathbf{A}_2 := \begin{pmatrix} 1 & 0 & 0 & \cdots & \cdots & 0 \\ 1 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} \in \mathfrak{R}_{p,\mathbf{k}},$$

τότε, σύμφωνα με το λήμμα 9.3.6, υπάρχουν $\vartheta_1, \vartheta_2 \in \mathrm{End}(G_{p,\mathbf{k}})$ με $\vartheta_1 = \mathfrak{h}(\mathbf{A}_1)$ και $\vartheta_2 = \mathfrak{h}(\mathbf{A}_2)$. Παρατηρούμε ότι

$$\mathbf{A}_1 - \mathbf{A}_2 = \begin{pmatrix} 0 & p^{k_2-k_1} & 0 & \cdots & \cdots & 0 \\ -1 & 0 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 0 & & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \cdots & \cdots & 0 & 0 \end{pmatrix}$$

με $p^{k_2} \nmid p^{k_2-k_1}$ (διότι $k_1 \geq 1$), οπότε $\mathbf{A}_1 - \mathbf{A}_2 \notin \mathrm{Ker}(\mathfrak{h}) \Rightarrow \vartheta_1 \neq \vartheta_2$. (Βλ. (9.52).)

Επιπροσθέτως,

$$\mathbf{A}_1\mathbf{A}_2 = \begin{pmatrix} 1+p^{k_2-k_1} & p^{k_2-k_1} & 0 & \cdots & \cdots & 0 \\ 1 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

$$\neq \begin{pmatrix} 1 & p^{k_2-k_1} & 0 & \cdots & \cdots & 0 \\ 1 & 1+p^{k_2-k_1} & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} = \mathbf{A}_2\mathbf{A}_1,$$

με

$$\mathbf{A}_1\mathbf{A}_2 - \mathbf{A}_2\mathbf{A}_1 \notin \mathrm{Ker}(\mathfrak{h}) \Rightarrow \vartheta_1 \circ \vartheta_2 = \mathfrak{h}(\mathbf{A}_1\mathbf{A}_2) \neq \mathfrak{h}(\mathbf{A}_2\mathbf{A}_1) = \vartheta_2 \circ \vartheta_1.$$

Τέλος, $\vartheta_1, \vartheta_2 \in \mathrm{Aut}(G_{p,\mathbf{k}})$, διότι[54] $[\mathbf{A}_1]_p, [\mathbf{A}_2]_p \in \mathrm{GL}_s(\mathbb{Z}_p)$.

**9.3.10 Πόρισμα.** *Η ομάδα αυτομορφισμών οιασδήποτε πεπερασμένης μη κυκλικής αβελιανής ομάδας είναι μη αβελιανή.*

ΑΠΟΔΕΙΞΗ. Έστω $(G, +)$ μια πεπερασμένη μη κυκλική αβελιανή ομάδα. Τουλάχιστον μία εκ των πρωτευουσών συνιστωσών της οφείλει να είναι *μη κυκλική*. (Εάν όλες οι πρωτεύουσες συνιστώσες της ήταν κυκλικές, τότε θα ήταν και η ίδια κυκλική λόγω τού πορίσματος 7.1.63.) Ως εκ τούτου, η $\mathrm{Aut}(G)$ (λόγω τής (9.45), τού (ii) τής προτάσεως 7.1.57 και των όσων προαναφέρθησαν στη σημείωση 9.3.9) είναι κατ' ανάγκην μη αβελιανή. □

**9.3.11 Πόρισμα.** *Η μοναδική (μέχρις ισομορφισμού) πεπερασμένη αβελιανή ομάδα, η οποία είναι ισόμορφη με την ομάδα των αυτομορφισμών της, είναι η τετριμμένη.*

ΑΠΟΔΕΙΞΗ. Έστω $(G, +)$ μια πεπερασμένη αβελιανή ομάδα με $\mathrm{Aut}(G) \cong G$. Ας υποθέσουμε ότι η $G$ δεν είναι τετριμμένη. Η $G$ δεν μπορεί να είναι κυκλική, διότι, εν τοιαύτη περιπτώσει, θα ίσχυε

$$|\mathrm{Aut}(G)| = \phi(|G|)$$

(όπου $\phi$ η συνάρτηση φι τού Euler, βλ. 2.1.7 (iii) και 2.4.32 (ii)), ενώ -ως γνωστόν- $\phi(n) \neq n$ για κάθε $n > 1$. Επομένως η $G$ είναι αβελιανή μη κυκλική έχουσα (κατ' ανάγκην) ως ομάδα αυτομορφισμών της μια *μη αβελιανή* ομάδα. (Βλ. 9.3.10.) Άτοπο (λόγω τού (ii) τής προτάσεως 2.4.19)! Άρα η $G$ είναι τετριμμένη. □

[54]Προφανώς, $\det([\mathbf{A}_1]_p) = \det([\mathbf{A}_2]_p) = [1]_p$. (Βλ. πρόταση D.2.10.)

# 9.4 ΑΒΕΛΙΑΝΕΣ ΟΜΑΔΕΣ ΣΤΡΕΨΕΩΣ

Η κλάση των πεπερασμένων αβελιανών ομάδων περιέχεται στην ευρύτερη κλάση των *αβελιανών ομάδων στρέψεως*.

**9.4.1 Ορισμός.** Έστω $(G,+)$ μια αβελιανή ομάδα και έστω

$$\boxed{\mathrm{tors}(G) := \{g \in G \,|ng = 0_G, \text{ για κάποιον } n \in \mathbb{N}\}}$$

το σύνολο στρέψεώς της το απαρτιζόμενο από όλα τα στοιχεία τής $G$ που έχουν πεπερασμένη τάξη. (Βλ. 2.3.1.) Επειδή η $G$ είναι αβελιανή, αυτό αποτελεί μια υποομάδα της, τη λεγόμενη **υποομάδα στρέψεως** τής $G$. Όταν $\mathrm{tors}(G) = G$, τότε λέμε ότι η $G$ είναι **ομάδα στρέψεως** (ή **περιοδική ομάδα**), ενώ όταν $\mathrm{tors}(G) = \{0_G\}$ λέμε ότι η $G$ **δεν διαθέτει στρέψη** ή ότι η $G$ **στερείται στρέψεως**.

**9.4.2 Παραδείγματα.** (i) Οι ομάδες $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ και $(\mathbb{C},+)$ στερούνται στρέψεως, καθώς, με εξαίρεση το 0, δεν διαθέτουν στοιχεία πεπερασμένης τάξεως.

(ii) Οι πεπερασμένες αβελιανές ομάδες είναι ομάδες στρέψεως. (Βλ. 9.4.3.)

(iii) Η πολλαπλασιαστική ομάδα $(\mathcal{E}_\infty,\cdot)$ όλων των ριζών τής μονάδας αποτελεί παράδειγμα *άπειρης* αβελιανής ομάδας στρέψεως. (Βλ. 2.3.6 (i).)

(iv) Είναι προφανές ότι η $\mathcal{E}_\infty$ είναι η υποομάδα στρέψεως $\mathrm{tors}(\mathbb{C}\smallsetminus\{0\})$ τής πολλαπλασιαστικής αβελιανής ομάδας $(\mathbb{C}\smallsetminus\{0\},\cdot)$.

(v) Η υποομάδα στρέψεως τής πολλαπλασιαστικής αβελιανής ομάδας $(\mathbb{R}\smallsetminus\{0\},\cdot)$ είναι η $\mathrm{tors}(\mathbb{R}\smallsetminus\{0\}) = \{x \in \mathbb{R}\smallsetminus\{0\} | \, x^n = 1, \text{ για κάποιον } n \in \mathbb{N}\} = \{\pm 1\}$, αφού

$$x^n - 1 = \begin{cases} (x-1)(x+1)\prod\limits_{k=1}^{\frac{n}{2}-1}(x^2 - 2\cos(\frac{2k\pi}{n})x + 1), & \text{όταν } n \equiv 0 (\mathrm{mod}\, 2), \\ \\ (x-1)\prod\limits_{k=1}^{\frac{n-1}{2}}(x^2 - 2\cos(\frac{2k\pi}{n})x + 1), & \text{όταν } n \equiv 1 (\mathrm{mod}\, 2). \end{cases}$$

**9.4.3 Πρόταση.** *Για μια αβελιανή ομάδα $(G,+)$ οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Η $G$ είναι πεπερασμένη.*

(ii) *Η $G$ είναι πεπερασμένως παραγόμενη ομάδα στρέψεως.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν $|G| < \infty$, τότε η $G$ είναι προδήλως πεπερασμένως παραγόμενη. Επίσης, για κάθε $g \in G$,

$$[\mathrm{ord}(g) = |\langle g\rangle| \mid |G| \Rightarrow \mathrm{ord}(g) \le |G| < \infty] \Rightarrow \mathrm{tors}(G) = G.$$

(ii)⇒(i) Έστω $\{x_1,...,x_\kappa\}$ κάποιο πεπερασμένο σύστημα γεννητόρων της. *Κάθε* στοιχείο $g \in G$ γράφεται υπό τη μορφή

$$g = n_1x_1 + \cdots + n_\kappa x_\kappa, \text{ για κάποιους } n_1,...,n_\kappa \in \mathbb{Z}.$$

Εξ υποθέσεως, $\mathrm{ord}(x_i) = d_i \in \mathbb{N}$, $\forall i \in \{1, ..., \kappa\}$. Διαιρώντας τόν $n_i$ διά τού $d_i$ λαμβάνουμε ένα μονοσημάντως ορισμένο ζεύγος $(q_i, r_i) \in \mathbb{Z} \times \mathbb{Z}$ με

$$n_i = q_i d_i + r_i,\ 0 \leq r_i \leq d_i - 1,\ \forall i \in \{1, ..., \kappa\}.$$

(Βλ. B.1.6.) Επειδή $d_i x_i = 0_G \Rightarrow n_i x_i = r_i x_i$, $\forall i \in \{1, ..., \kappa\}$, έχουμε

$$G = \left\{ \sum_{i=1}^{\kappa} r_i x_i \,\middle|\, r_i \in \{0, 1, ...., d_i - 1\} \right\}$$

απ' όπου έπεται ότι $|G| \leq \prod_{i=1}^{\kappa} d_i < \infty$. □

**9.4.4 Πόρισμα.** *Κάθε άπειρη αβελιανή ομάδα στρέψεως είναι μη πεπερασμένως παραγόμενη.*

**9.4.5 Πρόταση.** *Για κάθε αβελιανή ομάδα $(G, +)$ η πηλικοομάδα $G/\mathrm{tors}(G)$ στερείται στρέψεως.*

ΑΠΟΔΕΙΞΗ. Έστω $g+ \mathrm{tors}(G) \in G/\mathrm{tors}(G)$ ένα στοιχείο τής πηλικοομάδας $G/\mathrm{tors}(G)$ που έχει τάξη $n \in \mathbb{N}$. Τότε

$$n(g + \mathrm{tors}(G)) = ng + \mathrm{tors}(G) = 0_{G/\mathrm{tors}(G)} = \mathrm{tors}(G) \Rightarrow ng \in \mathrm{tors}(G),$$

οπότε

$$\exists m \in \mathbb{N} : m(ng) = (mn)g = 0_G \Rightarrow g \in \mathrm{tors}(G) \Rightarrow g + \mathrm{tors}(G) = \mathrm{tors}(G) = 0_{G/\mathrm{tors}(G)}.$$

Κατά συνέπειαν, $\mathrm{tors}(G/\mathrm{tors}(G)) = \{0_{G/\mathrm{tors}(G)}\}$. □

**9.4.6 Σημείωση.** Είθισται να λέμε εν συντομία ότι η πηλικοομάδα $G/\mathrm{tors}(G)$ αποτελεί το **άστρεπτο μέρος** τής $G$.

**9.4.7 Λήμμα.** *Εάν $f : G_1 \longrightarrow G_2$ είναι ένας ομομορφισμός (προσθετικών) αβελιανών ομάδων, τότε $f(\mathrm{tors}(G_1)) \sqsubseteq \mathrm{tors}(G_2)$ και, ως εκ τούτου, ορίζεται καλώς ο «κανονιστικός» ομομορφισμός*

$$f^{\text{πηλ.}} : G_1/\mathrm{tors}(G_1) \longrightarrow G_2/\mathrm{tors}(G_2)$$
$$g + \mathrm{tors}(G_1) \longmapsto f^{\text{πηλ.}}(g + \mathrm{tors}(G_1)) := f(g) + \mathrm{tors}(G_2),$$

*ο οποίος καθιστά το διάγραμμα*

$$\begin{tikzcd} G_1 \arrow[r, "f"] \arrow[d, "\pi^{G_1}_{\mathrm{tors}(G_1)}"'] \arrow[dr, phantom, "\circlearrowleft"] & G_2 \arrow[d, "\pi^{G_2}_{\mathrm{tors}(G_2)}"] \\ G_1/\mathrm{tors}(G_1) \arrow[r, dashed, "f^{\text{πηλ.}}"'] & G_2/\mathrm{tors}(G_2) \end{tikzcd}$$

*μεταθετικό. Επιπροσθέτως, ισχύουν τα ακόλουθα:*

(a) *Ο $f^{\text{πηλ.}}$ είναι μονομορφισμός* $\Longleftrightarrow \mathrm{tors}(G_1) = f^{-1}(\mathrm{tors}(G_2))$.

(b) *Ο $f^{\text{πηλ.}}$ είναι επιμορφισμός* $\Longleftrightarrow \mathrm{Im}(f) + \mathrm{tors}(G_2) = G_2$.

ΑΠΟΔΕΙΞΗ. Εάν $g \in G_1$ με $ng = 0_{G_1}$ για κάποιον $n \in \mathbb{N}$, τότε έχουμε

$$nf(g) = f(ng) = f(0_{G_1}) = 0_{G_2} \Rightarrow f(g) \in \mathrm{tors}(G_2).$$

Επομένως, $f(\mathrm{tors}(G_1)) \sqsubseteq \mathrm{tors}(G_2)$. Οι λοιποί ισχυρισμοί είναι αληθείς δυνάμει τού θεωρήματος 4.5.5. □

**9.4.8 Πρόταση.** *Έστω ότι $G_1, G_2$ είναι δυο (προσθετικές) αβελιανές ομάδες. Εάν $G_1 \cong G_2$, τότε ισχύουν τα εξής:*
(i) $\mathrm{tors}(G_1) \cong \mathrm{tors}(G_2)$.
(ii) $G_1/\mathrm{tors}(G_1) \cong G_2/\mathrm{tors}(G_2)$.

ΑΠΟΔΕΙΞΗ. Έστω $f : G_1 \xrightarrow{\cong} G_2$ ένας ισομορφισμός.
(i) Εφαρμόζοντας το λήμμα 9.4.7 τόσον για τον $f$ όσον και για τον $f^{-1}$ λαμβάνουμε

$$\left.\begin{array}{l} f(\mathrm{tors}(G_1)) \sqsubseteq \mathrm{tors}(G_2) \\ f^{-1}(\mathrm{tors}(G_2)) \sqsubseteq \mathrm{tors}(G_1) \end{array}\right\} \Rightarrow f(\mathrm{tors}(G_1)) = \mathrm{tors}(G_2), \tag{9.53}$$

οπότε η $f|_{\mathrm{tors}(G_1)} : \mathrm{tors}(G_1) \longrightarrow \mathrm{tors}(G_2)$ είναι ισομορφισμός με τον $f^{-1}|_{\mathrm{tors}(G_2)}$ ως αντίστροφό του.
(ii) Λόγω τής ισότητας (9.53) πληρούται η συνθήκη (a) τού λήμματος 9.4.7 για τον $f^{\pi\eta\lambda.}$. Επειδή δε $\mathrm{Im}(f) = G_2$,πληρούται *και* η συνθήκη (b) τού λήμματος 9.4.7 για τον $f^{\pi\eta\lambda.}$. Άρα ο $f^{\pi\eta\lambda.}$ είναι ισομορφισμός. □

**9.4.9 Πρόταση.** *Έστω $(G_i)_{i\in I}$ μια οικογένεια (προσθετικών) αβελιανών ομάδων ($I \neq \varnothing$). Εάν $G := \bigoplus_{i\in I}^{\pi\varepsilon\varrho.} G_i$, τότε $\mathrm{tors}(G) = \bigoplus_{i\in I}^{\pi\varepsilon\varrho.} \mathrm{tors}(G_i)$. Ιδιαιτέρως, η $G$ είναι ομάδα στρέψεως εάν και μόνον εάν η $G_i$ είναι ομάδα στρέψεως για κάθε $i \in I$.*

ΑΠΟΔΕΙΞΗ. Αφήνεται ως άσκηση. □

**9.4.10 Σημείωση.** Προσοχή! Εάν $G := \bigoplus_{i\in I} G_i$ (όπου $I$ κάποιο *απειροσύνολο*), τότε $\mathrm{tors}(G) \subsetneq \bigoplus_{i\in I}\mathrm{tors}(G_i)$. Ως εκ τούτου, εάν η $G_i$ στερείται στρέψεως για κάθε $i \in I$, τότε και η ίδια η $G$ στερείται στρέψεως. Ωστόσο, ο εγκλεισμός αυτός ενδέχεται να είναι *αυστηρός*. Επί παραδείγματι, κάθε ευθύς προσθετέος τής $G := \bigoplus_{m=2}^{\infty} \mathbb{Z}_m$ είναι μια μη τετριμμένη ομάδα στρέψεως. Όμως

$$([1]_2, [1]_3, ..., [1]_i, [1]_{i+1}, ....) \in G \smallsetminus \mathrm{tors}(G),$$

διότι $k[1]_{k+1} \neq [0]_{k+1}, \forall k \in \mathbb{N}$.

**9.4.11 Συμβολισμός.** Εάν $(G, +)$ είναι μια αβελιανή ομάδα και $p$ ένας πρώτος αριθμός, τότε ως

$$\boxed{G(p) := \{\, g \in G \,|\, p^n g = 0_G \ \text{ για κάποιον } n \in \mathbb{N}_0 \}}$$

θα συμβολίζουμε την υποομάδα τής $G$ την απαρτιζόμενη από εκείνα τα στοιχεία, οι τάξεις των οποίων είναι ίσες με κάποια (μη αρνητική ακεραία) δύναμη τού $p$.

**9.4.12 Θεώρημα.** *Εάν $(G,+)$ είναι μια μη τετριμμένη αβελιανή ομάδα, τότε*

$$\boxed{\operatorname{tors}(G) = \bigoplus\nolimits^{\text{εσ.}}_{p\ \text{πρώτος}} G(p)\,.}$$

ΑΠΟΔΕΙΞΗ. Έστω τυχόν $g \in G \smallsetminus \{0_G\}$. Προφανώς, $\operatorname{ord}(g) =: d \geq 2$. Ας υποθέσουμε ότι $d = p_1^{\nu_1} \cdots p_\kappa^{\nu_\kappa}$ $(\kappa \in \mathbb{N},\ \nu_1,...,\nu_\kappa \in \mathbb{N})$ είναι η κανονική παράσταση (B.19) τού $d$ ως γινομένου (κατάλληλων δυνάμεων) πρώτων αριθμών $p_1,...,p_\kappa$ με $p_1 < \cdots < p_\kappa$ και $r_i := \frac{d}{p_i^{\nu_i}}$ για κάθε $i \in \{1,...,\kappa\}$. Τότε

$$\text{μκδ}(r_1,...,r_\kappa) = 1 \underset{\text{B.2.8}}{\Longrightarrow} \left[\exists\,(s_1,...,s_\kappa) \in \mathbb{Z}^\kappa : \sum_{i=1}^{\kappa} r_i s_i = 1\right]. \tag{9.54}$$

Επειδή $p_i^{\nu_i}(r_i s_i g) = (p_i^{\nu_i} r_i)\, s_i g = d s_i g = s_i(dg) = s_i 0_G = 0_G$, έχουμε

$$r_i s_i g \in G(p_i),\ \ \forall i \in \{1,...,\kappa\}.$$

Κατά συνέπειαν, $g \underset{(9.54)}{=} s_1 r_1 g + \cdots + s_\kappa r_\kappa g \in \langle \{\, G(p) |\, p \text{ πρώτος}\} \rangle$. Αρκεί λοιπόν να αποδειχθεί ότι $G(p) \cap \langle \{\, G(q) |\, q \text{ πρώτος},\ q \neq p\} \rangle = \{0_G\}$ για κάθε πρώτον αριθμό $p$. (Βλ. 7.1.97.) Έστω $x$ ένα στοιχείο ανήκον σε αυτήν την τομή. Επειδή $x \in G(p)$, υπάρχει $n \in \mathbb{N}_0$, τέτοιος ώστε να ισχύει $p^n x = 0_G$. Από την άλλη μεριά, επειδή

$$x \in \langle \{\, G(q) |\, q \text{ πρώτος},\ q \neq p\} \rangle \underset{2.2.6}{=} \left\{ y_1 + \cdots + y_k \;\middle|\; \begin{array}{c} y_j \in G(q_j),\ q_j \text{ πρώτος}, \\ q_j \neq p,\ \forall j \in \{1,...,k\},\ k \in \mathbb{N} \end{array} \right\},$$

το στοιχείο $x$ είναι τής μορφής $x = y_1 + \cdots + y_k$ με $q_j^{m_j} y_j = 0_G$ για κάποιον $m_j \in \mathbb{N}_0, \forall j \in \{1,...,k\}$.

*Περίπτωση πρώτη.* Εάν $m_1 = \cdots = m_k = 0$, τότε $y_1 = \cdots = y_k = 0_G \Rightarrow x = 0_G$.

*Περίπτωση δεύτερη.* Εάν $\exists \{j_1,...,j_\rho\} \subseteq \{1,...,k\}, \rho \in \{1,...,k\} : m_{j_\xi} \geq 1$ για κάθε $\xi \in \{1,...,\rho\}$, τότε $x = y_{j_1} + \cdots + y_{j_\rho}$. Θέτοντας $u := \prod_{\xi=1}^{\rho} q_{j_\xi}^{m_{j_\xi}}$ παρατηρούμε ότι $ux = 0_G$ και ότι

$$[q_j \neq p,\ \forall j \in \{1,...,k\}] \Rightarrow \text{μκδ}(p^n, u) = 1$$
$$\underset{\text{B.2.8}}{\Longrightarrow} [\exists\,(\lambda_1,\lambda_2) \in \mathbb{Z} \times \mathbb{Z} : \lambda_1 p^n + \lambda_2 u = 1]\,.$$

Επομένως, $x = (\lambda_1 p^n + \lambda_2 u)x = \lambda_1\,(p^n x) + \lambda_2(ux) = \lambda_1 0_G + \lambda_2 0_G = 0_G$. □

**9.4.13 Σημείωση.** Εάν η $(G,+)$ είναι μια μη τετριμμένη *αβελιανή ομάδα στρέψεως*, τότε

$$\boxed{G = \operatorname{tors}(G) = \bigoplus\nolimits^{\text{εσ.}}_{p\ \text{πρώτος}} G(p).} \tag{9.55}$$

Η (9.55) καλείται **πρωτεύουσα αποσύνθεση τής** $G$ και η $G\,(p)$ $p$-**πρωτεύουσα συνιστώσα**[55] **τής** $G$. Στην ειδική περίπτωση όπου η $G$ είναι *πεπερασμένη*, η αποσύνθεση (9.55) ταυτίζεται με την αποσύνθεση (9.13) που είχαμε προσδιορίσει στην πρόταση 9.1.17 (και η παρούσα γενίκευση τής ορολογίας τής εισαχθείσας στο εδάφιο 9.1.18 είναι απολύτως συμβατή).

[55] Φυσικά, καθώς ο $p$ διατρέχει το σύνολο όλων των πρώτων αριθμών, ενδέχεται κάποιες εκ των πρωτευουσών συνιστωσών τής $G$ να είναι τετριμμένες. (Εν τοιαύτη περιπτώσει, εάν αυτές για μια συγκεκριμένη $G$ είναι γνωστές, είθισται να τις παραλείπουμε.)

**9.4.14 Λήμμα.** *Εάν $f : G \longrightarrow H$ είναι ένας ομομορφισμός (προσθετικών) αβελιανών ομάδων, τότε $f(G(p)) \sqsubseteq H(p)$ για κάθε πρώτον αριθμό $p$. Επιπροσθέτως, στην περίπτωση όπου ο $f$ είναι ισομορφισμός, $f(G(p)) = H(p)$.*

ΑΠΟΔΕΙΞΗ. Εάν $g \in G(p)$, τότε $p^n g = 0_G$ για κάποιον $n \in \mathbb{N}_0$, οπότε

$$p^n f(g) = f(p^n g) = f(0_G) = 0_H \Rightarrow f(g) \in H(p).$$

Στην περίπτωση όπου ο $f$ είναι ισομορφισμός, έχουμε

$$\left.\begin{array}{l} f(G(p)) \sqsubseteq H(p) \\ f^{-1}(H(p)) \sqsubseteq G(p) \end{array}\right\} \Rightarrow f(G(p)) = H(p),$$

οπότε η $f|_{G(p)} : G(p) \longrightarrow H(p)$ είναι ισομορφισμός με τον $f^{-1}\big|_{H(p)}$ ως αντίστροφό του. □

**9.4.15 Θεώρημα.** *Εάν $G, H$ είναι δυο (προσθετικές) μη τετριμμένες αβελιανές ομάδες στρέψεως, τότε*

$$\boxed{G \cong H \Longleftrightarrow [G(p) \cong H(p) \text{ για κάθε πρώτον αριθμό } p].}$$

ΑΠΟΔΕΙΞΗ. Η συνεπαγωγή "$\Rightarrow$" έπεται άμεσα από το προηγηθέν λήμμα 9.4.14. Για την "$\Leftarrow$" υποθέτουμε ότι υπάρχουν ισομορφισμοί $f_{(p)} : G(p) \xrightarrow{\cong} H(p)$ για κάθε πρώτον αριθμό $p$. Μέσω αυτών, μέσω των πρωτευουσών αποσυνθέσεων (9.55) και μέσω των ισομορφισμών τού (ii) τού θεωρήματος 7.1.100 επάγεται ισομορφισμός

$$G = \bigoplus\nolimits_{p \text{ πρώτος}}^{\text{εσ.}} G(p) \cong \bigoplus\nolimits_{p \text{ πρώτος}}^{\text{περ.}} G(p) \xrightarrow[f]{\cong} \bigoplus\nolimits_{p \text{ πρώτος}}^{\text{περ.}} H(p) \cong \bigoplus\nolimits_{p \text{ πρώτος}}^{\text{εσ.}} H(p) = H,$$

όπου $f((g_p)_{p \text{ πρώτος}}) := (f_{(p)}(g_p))_{p \text{ πρώτος}}$. □

## 9.5 ΕΛΕΥΘΕΡΕΣ ΑΒΕΛΙΑΝΕΣ ΟΜΑΔΕΣ

Μέχρι στιγμής έχουμε εκμεταλλευθεί ποικιλοτρόπως την ιδιότητα ορισμένων *ειδικών* αβελιανών ομάδων ή πηλικοομάδων να μπορούν να εφοδιάζονται *και* με τη δομή ενός $\mathbb{Z}_p$-διανυσματικού χώρου (για κάποιον πρώτο αριθμό $p$). Ωστόσο, για *τυχούσες* αβελιανές ομάδες $(G, +)$ τούτο δεν είναι εφικτό, καθώς η μόνη διαθέσιμη (εν γένει εξωτερική) πράξη (που θα μπορούσε να αποτελέσει το ανάλογο τού *αριθμητικού* ή *βαθμωτού πολλαπλασιασμού* ενός διανυσματικού χώρου) είναι η

$$\mathbb{Z} \times G \ni (n, g) \longmapsto ng \in G.$$

Παρότι είναι δυνατόν να αντικατασταθούν οι *συνήθεις* γραμμικοί συνδυασμοί (με συντελεστές ειλημμένους από κάποιο σώμα) με $\mathbb{Z}$-*γραμμικούς συνδυασμούς* (με *ακεραίους* συντελεστές) και να ορισθούν (κατά τα ειωθότα) $\mathbb{Z}$-*γραμμικώς ανεξάρτητα υποσύνολα* και $\mathbb{Z}$-*βάσεις* (βλ. 9.5.1 και 9.5.3), παρατηρείται διαφοροποίηση μεταξύ αρκετών αποτελεσμάτων τής Θεωρίας Διανυσματικών Χώρων και των αντιστοίχων τής Θεωρίας Αβελιανών Ομάδων. Εν πρώτοις, υφίστανται αβελιανές ομάδες *χωρίς* $\mathbb{Z}$-βάσεις. Εκείνες που διαθέτουν (τουλάχιστον μία) $\mathbb{Z}$-βάση είναι οι λεγόμενες *ελεύθερες αβελιανές ομάδες*. (Βλ. θεώρημα 9.5.13.) Αλλά *και* εντός τής κλάσεως των ελεύθερων αβελιανών ομάδων, η διαφοροποίηση παραμένει αισθητή. Επί παραδείγματι:

(i) Υπάρχουν συστήματα γεννητόρων ελεύθερων αβελιανών ομάδων τα οποία *δεν περιέχουν καμία* $\mathbb{Z}$-βάση. (Βλ. 9.5.7 (i).)

(ii) Υπάρχουν $\mathbb{Z}$-γραμμικώς ανεξάρτητα υποσύνολα ελεύθερων αβελιανών ομάδων τα οποία *δεν είναι επεκτάσιμα* σε $\mathbb{Z}$-βάσεις. (Βλ. 9.5.7 (ii).)

(iii) Υπάρχουν μη τετριμμένες υποομάδες ελεύθερων αβελιανών ομάδων οι οποίες *δεν διαθέτουν συμπληρώματα*. (Βλ. 9.5.38.)

(iv) Άλλες ιδιότητες τής *διαστάσεως* (διανυσματικών χώρων) διατηρούνται από τη *βαθμίδα* ελεύθερων αβελιανών ομάδων (που αποτελεί το ανάλογό της) και άλλες όχι. (Βλ. 9.5.28, 9.5.31, 9.5.39 και 9.5.40.)

*Μολαταύτα*, η διεξοδική μελέτη των ελεύθερων αβελιανών ομάδων είναι επιβεβλημένη, τουλάχιστον για τους εξής λόγους:

(i) Οι ιδιότητες των διανυσματικών χώρων που «περισώζονται» στις ελεύθερες αβελιανές ομάδες *δεν είναι διόλου αμελητέες* (μονοσήμαντη έκφραση στοιχείων τους ως $\mathbb{Z}$-γραμμικών συνδυασμών στοιχείων οιασδήποτε $\mathbb{Z}$-βάσεως, μεταφορά $\mathbb{Z}$-βάσεων σε $\mathbb{Z}$-βάσεις μέσω ισομορφισμών, ισοπληθικότητα των $\mathbb{Z}$-βάσεων κ.ά.).

(ii) *Κάθε αβελιανή ομάδα* είναι ισόμορφη με πηλικοομάδες που προκύπτουν ύστερα από «διαίρεση» *ελεύθερων* αβελιανών ομάδων διά καταλλήλων υποομάδων τους. (Βλ. θεώρημα 9.5.35.)

(iii) Οι ελεύθερες αβελιανές ομάδες πεπερασμένης βαθμίδας υπεισέχονται κατά τρόπο ουσιαστικό στην ταξινόμηση (μέχρις ισομορφισμού) των μη πεπερασμένων αλλά πεπερασμένως παραγομένων αβελιανών ομάδων. (Βλ. θεώρημα 9.6.7.)

(iv) Οι ελεύθερες αβελιανές ομάδες αποτελούν τους προπομπούς των λεγομένων *ελεύθερων ομάδων* (όχι κατ' ανάγκην αβελιανών), οι οποίες ορίζονται μέσω μιας καθολικής ιδιότητας ανάλογης εκείνης τής προτάσεως 9.5.29 και είναι απαραίτητες για τη εισαγωγή τής εννοίας τής *παραστάσεως* ομάδας.

**9.5.1 Ορισμός.** Έστω $(G,+)$ τυχούσα αβελιανή ομάδα και έστω $X \subseteq G$. Στην περίπτωση όπου $X \neq \varnothing$, λέμε ότι ένα $g \in G$ είναι **$\mathbb{Z}$-γραμμικός συνδυασμός στοιχείων τού** $X$ όταν υπάρχουν (πεπερασμένου πλήθους) στοιχεία $x_1, ..., x_\kappa$ τού $X$ και $n_1, ..., n_\kappa \in \mathbb{Z}$, ούτως ώστε να ισχύει $g = \sum_{i=1}^{\kappa} n_i x_i$. Εν γένει θέτουμε:

$$\mathrm{Lin}_{\mathbb{Z}}(X) := \begin{cases} \{0_G\}, & \text{όταν } X = \varnothing, \\ \left\{ \begin{array}{c} \text{όλοι οι } \mathbb{Z}\text{-γραμμικοί} \\ \text{συνδυασμοί στοιχείων τού } X \end{array} \right\}, & \text{όταν } X \neq \varnothing. \end{cases}$$

**9.5.2 Πρόταση.** *Εάν $(G,+)$ είναι μια αβελιανή ομάδα και $X \subseteq G$, τότε*

$$\mathrm{Lin}_{\mathbb{Z}}(X) = \langle X \rangle \ \left(= \bigcap \{ H \in \mathbf{Subg}(G) \mid X \subseteq H \}\right).$$

ΑΠΟΔΕΙΞΗ. Όταν $X = \varnothing$, είναι προφανές ότι η ελάχιστη (ως προς τη σχέση τού συνολοθεωρητικού εγκλεισμού) υποομάδα τής $G$ που περιέχει το $\varnothing$ είναι η τετριμμένη υποομάδα $\{0_G\}$. Έστω ότι $X \neq \varnothing$. Προφανώς, $0_G \in \mathrm{Lin}_{\mathbb{Z}}(X)$ (διότι $0x = 0_G, \forall x \in X$). Και εάν $g_1, g_2 \in \mathrm{Lin}_{\mathbb{Z}}(X)$, τότε

$$g_1 = \sum_{i=1}^{\kappa_1} n_i x_i \;\text{ και }\; g_2 = \sum_{j=1}^{\kappa_2} m_j y_j,$$

για κάποια $x_1, ..., x_{\kappa_1}, y_1, ..., y_{\kappa_2} \in X$ και κάποιους $n_1, ..., n_{\kappa_1}, m_1, ..., m_{\kappa_2} \in \mathbb{Z}$, οπότε

$$g_1 - g_2 = \sum_{i=1}^{\kappa_1} n_i x_i - \sum_{j=1}^{\kappa_2} m_j y_j \in \mathrm{Lin}_{\mathbb{Z}}(X).$$

Κατά συνέπειαν, $\mathrm{Lin}_{\mathbb{Z}}(X) \in \mathbf{Subg}(G)$ (βλ. 2.1.16 (iii)) και $X \subseteq \mathrm{Lin}_{\mathbb{Z}}(X)$ (διότι $x = 1 \cdot x, \forall x \in X$). Επειδή η ομάδα $\langle X \rangle$ αποτελεί την ελάχιστη υποομάδα τής $G$ που περιέχει το $X$, έχουμε $\langle X \rangle \subseteq \mathrm{Lin}_{\mathbb{Z}}(X)$. Από την άλλη μεριά, είναι προφανές ότι κάθε $\mathbb{Z}$-γραμμικός συνδυασμός στοιχείων τού $X$ ανήκει σε κάθε υποομάδα τής $G$ που περιέχει το $X$, οπότε $\mathrm{Lin}_{\mathbb{Z}}(X) \subseteq \langle X \rangle$. Τελικώς λοιπόν, $\mathrm{Lin}_{\mathbb{Z}}(X) = \langle X \rangle$. □

**9.5.3 Ορισμός.** Έστω $(G, +)$ τυχούσα αβελιανή ομάδα.

(i) Λέμε ότι ένα υποσύνολο $X \subseteq G$ είναι **$\mathbb{Z}$-γραμμικώς ανεξάρτητο** όταν[56] είτε $X = \varnothing$ είτε $X \neq \varnothing$ *και* για οιοδήποτε πεπερασμένο υποσύνολο $\{x_1, ..., x_\kappa\}$ τού $X$ και $n_1, ..., n_\kappa \in \mathbb{Z}$ ισχύει η συνεπαγωγή[57]

$$\sum_{j=1}^{\kappa} n_j x_j = 0_G \Rightarrow [n_j = 0, \ \forall j \in \{1, ..., \kappa\}].$$

(ii) Κάθε $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο $X \subseteq G$ το οποίο αποτελεί σύστημα γεννητόρων τής $G$ (δηλ., $\langle X \rangle = \mathrm{Lin}_{\mathbb{Z}}(X) = G$) καλείται **$\mathbb{Z}$-βάση**[58] τής $G$.

**9.5.4 Πρόταση.** *Κάθε αβελιανή ομάδα διαθέτει (τουλάχιστον ένα) μεγιστικό $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο ως προς τη σχέση "$\subseteq$" τού συνολοθεωρητικού εγκλεισμού*. (Βλ. A.2.10 (i).)

ΑΠΟΔΕΙΞΗ. Εάν $(G, +)$ είναι τυχούσα αβελιανή ομάδα, τότε το $(\mathfrak{X}, \subseteq)$, όπου

$$\mathfrak{X} := \{X \in \mathfrak{P}(G) |\, X \ \ \mathbb{Z}\text{-γραμμικώς ανεξάρτητο}\},$$

είναι μερικώς διατεταγμένο σύνολο. (Σημειωτέον ότι $\mathfrak{X} \neq \varnothing$, διότι $\{\varnothing\} \in \mathfrak{X}$.) Έστω $\mathcal{C} = \{X_i |\, i \in I\}$ τυχούσα αλυσίδα τού $(\mathfrak{X}, \subseteq)$. (Βλ. A.2.18 (i).)

*Ισχυρισμός*. Η ένωση των μελών της $\bigcup_{i \in I} X_i \subseteq G$ είναι $\mathbb{Z}$-γραμμικώς ανεξάρτητο. Πράγματι· εάν $\{x_1, ..., x_\kappa\}$ είναι ένα πεπερασμένο υποσύνολο τού $\bigcup_{i \in I} X_i$, (πληθικού αριθμού $\kappa \in \mathbb{N}$), τότε υπάρχει ένα σύνολο δεικτών $\{i_1, ..., i_\kappa\}$, τέτοιο ώστε

[56] Όταν δεν πληρούται καμία εξ αυτών των συνθηκών, τότε λέμε ότι το $X$ είναι $\mathbb{Z}$-**γραμμικώς εξαρτημένο.**

[57] Με άλλα λόγια, εάν ένας $\mathbb{Z}$-γραμμικός συνδυασμός στοιχείων τού $X$ ισούται με το $0_G$, τότε *όλοι* οι συντελεστές αυτού οφείλουν να είναι ίσοι με το μηδέν.

[58] Προφανώς, το $\varnothing$ αποτελεί $\mathbb{Z}$-βάση τής $G$ εάν και μόνον εάν η $G$ είναι *τετριμμένη*.

να ισχύει $x_j \in X_{i_j}$ για κάθε $j \in \{1, ..., \kappa\}$. Επειδή το $(\mathcal{C}, \subseteq)$ είναι ολικώς διατεταγμένο σύνολο, υπάρχει κάποιος δείκτης $i_\bullet \in I$, ούτως ώστε να ισχύει $X_{i_j} \subseteq X_{i_*}$ για κάθε $j \in \{1, ..., \kappa\}$. Επομένως, $\{x_1, ..., x_\kappa\} \subseteq X_{i_*}$ με το $X_{i_*} \in \mathcal{C}$ ένα (εξ υποθέσεως) $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο τής $G$. Άρα και το ίδιο το $\{x_1, ..., x_\kappa\}$ είναι $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο τής $G$. Επειδή κάθε πεπερασμένο υποσύνολο τού $\bigcup_{i \in I} X_i$ είναι $\mathbb{Z}$-γραμμικώς ανεξάρτητο, και το ίδιο το $\bigcup_{i \in I} X_i$ είναι $\mathbb{Z}$-γραμμικώς ανεξάρτητο και ο ισχυρισμός είναι αληθής.

*Εφαρμογή τού λήμματος τού Zorn.* Επειδή το $\bigcup_{i \in I} X_i$ είναι άνω φράγμα τής $\mathcal{C}$, το $(\mathfrak{X}, \subseteq)$ είναι επαγωγικώς διατεταγμένο. Το λήμμα A.2.20 τού Zorn εγγυάται την ύπαρξη κάποιου *μεγιστικού* $\mathbb{Z}$-γραμμικώς ανεξάρτητου υποσυνόλου $X_\bullet$ τής $G$. □

**9.5.5 Πρόταση.** *Έστω $(G, +)$ μια αβελιανή ομάδα και έστω $\varnothing \neq X \subseteq G$. Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Το $X$ είναι μια $\mathbb{Z}$-βάση τής $G$.*

(ii) *Κάθε στοιχείο τής $G$ γράφεται κατά τρόπο μονοσήμαντο ως $\mathbb{Z}$-γραμμικός συνδυασμός στοιχείων τού $X$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εξ ορισμού, κάθε στοιχείο τής $G$ γράφεται ως $\mathbb{Z}$-γραμμικός συνδυασμός στοιχείων τού $X$. Υποθέτουμε ότι για κάποιο $g \in G$ υφίσταται πεπερασμένο υποσύνολο $\{x_1, ..., x_\kappa\}$ τού $X$ και $n_1, ..., n_\kappa, m_1, ..., m_\kappa \in \mathbb{Z}$, ούτως ώστε να ισχύει

$$g = \sum_{j=1}^{\kappa} n_j x_j = \sum_{j=1}^{\kappa} m_j x_j \Rightarrow \sum_{j=1}^{\kappa} (n_j - m_j) x_j = 0_G.$$

Επειδή το $X$ είναι εξ υποθέσεως $\mathbb{Z}$-γραμμικώς ανεξάρτητο, έχουμε κατ' ανάγκην $n_j = m_j$ για κάθε $j \in \{1, ..., \kappa\}$.

(ii)⇒(i) Αρκεί να αποδειχθεί ότι το $X$ είναι ένα $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο τής $G$. Προς τούτο θεωρούμε τυχόν πεπερασμένο υποσύνολο $\{x_1, ..., x_\kappa\}$ τού $X$. Από κάθε σχέση τής μορφής $\sum_{j=1}^{\kappa} n_j x_j = 0_G$ (με $n_1, ..., n_\kappa \in \mathbb{Z}$) προκύπτει ότι

$$\sum_{j=1}^{\kappa} n_j x_j = 0_G = \sum_{j=1}^{\kappa} 0 x_j \Rightarrow [n_j = 0, \ \forall j \in \{1, ..., \kappa\}]$$

λόγω τής προϋποτεθείσας μοναδικότητας τής παραστάσεως οιουδήποτε στοιχείου τής $G$ ως $\mathbb{Z}$-γραμμικού συνδυασμού στοιχείων τού $X$. □

**9.5.6 Πρόταση.** *Έστω $(G, +)$ μια αβελιανή ομάδα και έστω $X \subseteq G$. Εάν υποτεθεί ότι το $X$ είναι μια $\mathbb{Z}$-βάση τής $G$, τότε ισχύουν τα εξής:*

(i) *Το $X$ είναι ένα ελαχιστικό σύστημα γεννητόρων*[59] *τής $G$.*

(ii) *Το $X$ είναι ένα μεγιστικό $\mathbb{Z}$-γραμμικώς ανεξάρτητο*[60] *υποσύνολο τής $G$.*

[59] Αυτό σημαίνει ότι το υποσύνολο $X \subseteq G$ αποτελεί ένα ελαχιστικό στοιχείο τού μερικώς διατεταγμένου συνόλου $(\{ Z \in \mathfrak{P}(G) | \langle Z \rangle = G \}, \subseteq)$. Βλ. A.2.10 (ii).

[60] Βλ. πρόταση 9.5.4.

ΑΠΟΔΕΙΞΗ. Θα χρησιμοποιήσουμε «εις άτοπον απαγωγή».

(i) Έστω ότι το $X$ δεν είναι ελαχιστικό σύστημα γεννητόρων τής $G$. Τότε $X \neq \varnothing$ και υπάρχει κάποιο $Y \in \mathfrak{P}(G) : \langle Y \rangle = G$ με $Y \subsetneqq X$. Έστω $x \in X \smallsetminus Y$. Επειδή $x \in G = \langle Y \rangle$ , υπάρχουν $y_1, ..., y_\kappa \in Y$ $(\kappa \in \mathbb{N})$ και $m_1, ..., m_\kappa \in \mathbb{Z}$, ούτως ώστε να ισχύει

$$x = \sum_{j=1}^{\kappa} n_j y_j \Rightarrow 1 \cdot x + \sum_{j=1}^{\kappa} (-n_j) y_j = 0_G \ \ ( \{x, y_1, ..., y_\kappa\} \subseteq X).$$

Άρα το $X$ είναι $\mathbb{Z}$-γραμμικώς εξαρτημένο υποσύνολο τής $G$. Άτοπο!

(ii) Εάν $X = \varnothing$, τότε ο ισχυρισμός είναι προδήλως αληθής. Ας υποθέσουμε ότι $X \neq \varnothing$ και ότι το $X$ δεν είναι μεγιστικό $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο τής $G$. Τότε υπάρχει κάποιο $\mathbb{Z}$-γραμμικώς ανεξάρτητο $Y \in \mathfrak{P}(G) : X \subsetneqq Y$. Έστω ότι $y \in Y \smallsetminus X$. Επειδή (εξ υποθέσεως) $G = \langle X \rangle \ni y$, υπάρχουν $x_1, ..., x_\kappa \in X$ $(\kappa \in \mathbb{N})$ και $m_1, ..., m_\kappa \in \mathbb{Z}$, ούτως ώστε να ισχύει

$$y = \sum_{j=1}^{\kappa} m_j x_j \Rightarrow 1 \cdot y + \sum_{j=1}^{\kappa} (-m_j) x_j = 0_G \ \ ( \{y, x_1, ..., x_\kappa\} \subseteq Y).$$

Άρα το $Y$ είναι $\mathbb{Z}$-γραμμικώς εξαρτημένο υποσύνολο τής $G$. Άτοπο! □

**9.5.7 Σημείωση.** (i) Το $\{1\}$ αποτελεί (προφανώς) $\mathbb{Z}$-βάση τής αβελιανής ομάδας $(\mathbb{Z}, +)$. Ωστόσο, υπάρχουν συστήματα γεννητόρων αυτής τα οποία *δεν περιέχουν καμία* $\mathbb{Z}$-βάση. Επί παραδείγματι, $\langle \{2, 3\} \rangle = \mathbb{Z}$ (διότι $3n - 2n = n$ για κάθε $n \in \mathbb{Z}$) αλλά κανένα εκ των μονοσυνόλων $\{2\}, \{3\}$ δεν αποτελεί $\mathbb{Z}$-βάση[61] τής $(\mathbb{Z}, +)$ (διότι $\langle 2 \rangle = 2\mathbb{Z} \subsetneqq \mathbb{Z}$ και $\langle 3 \rangle = 3\mathbb{Z} \subsetneqq \mathbb{Z}$).

(ii) Ας θεωρήσουμε και πάλι την $(\mathbb{Z}, +)$. Το μονοσύνολο $\{2\}$ είναι $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο. (Εάν $n$ είναι ένας ακέραιος, τέτοιος ώστε να ισχύει $n \cdot 2 = 0$, τότε $n = 0$.) Ωστόσο, αυτό δεν μπορεί να συμπληρωθεί (επεκταθεί) καταλλήλως, ούτως ώστε να προκύψει μια $\mathbb{Z}$-βάση. Πράγματι· για να επεκτείνουμε το $\{2\}$ σε ένα σύστημα γεννητόρων τής $(\mathbb{Z}, +)$ θα πρέπει να προσαρτήσουμε τουλάχιστον έναν περιττό ακέραιο αριθμό $2k + 1$ $(k \in \mathbb{Z})$. Όμως το $\{2, 2k + 1\}$ (και οιοδήποτε υπερσύνολο αυτού αποτελούμενο από ακεραίους) *δεν μπορεί να καταστεί* $\mathbb{Z}$-βάση τής $(\mathbb{Z}, +)$, διότι το 1 (εν αντιθέσει προς ό,τι επιτάσσει η συνθήκη (ii) τής προτάσεως 9.5.5) μπορεί να γραφεί κατά δύο διαφορετικούς τρόπους ως $\mathbb{Z}$-γραμμικός συνδυασμός των 2 και $2k + 1$:

$$1 = (k + 1) \cdot 2 + (-1) \cdot (2k + 1) = (-k) \cdot 2 + 1 \cdot (2k + 1).$$

**9.5.8 Πρόταση.** *Εάν $f : G_1 \xrightarrow{\cong} G_2$ είναι ένας ισομορφισμός μεταξύ δυο αβελιανών ομάδων $G_1, G_2$ και $X$ μια $\mathbb{Z}$-βάση τής $G_1$, τότε η εικόνα αυτής $f(X)$ μέσω τού $f$ αποτελεί μια $\mathbb{Z}$-βάση τής $G_2$.*

[61] Το ίδιο το $\{2, 3\}$ είναι $\mathbb{Z}$-γραμμικώς εξαρτημένο, καθώς ισχύει $3 \cdot 2 + (-2) \cdot 3 = 0$.

ΑΠΟΔΕΙΞΗ. Επειδή $G_2 = f(G_1) = f(\langle X\rangle) = \langle f(X)\rangle$, η εικόνα $f(X)$ αποτελεί σύστημα γεννητόρων τής $G_2$. Εάν $X = \varnothing$, τότε αμφότερες οι $G_1, G_2$ είναι τετριμμένες και $f(\varnothing) = \varnothing$. Εάν $X \neq \varnothing$, τότε για οιοδήποτε πεπερασμένο υποσύνολο $\{f(x_1), ..., f(x_\kappa)\}$ τής εικόνας $f(X)$ και $n_1, ..., n_\kappa \in \mathbb{Z}$ με

$$\sum_{j=1}^{\kappa} n_j f(x_j) = 0_{G_2} \quad \left[\Leftrightarrow f(\sum_{j=1}^{\kappa} n_j x_j) = 0_{G_2} \Leftrightarrow \sum_{j=1}^{\kappa} n_j x_j \in \mathrm{Ker}(f)\right]$$

έχουμε $\sum_{j=1}^{\kappa} n_j x_j = 0_{G_1}$ (διότι $\mathrm{Ker}(f) = \{0_{G_1}\}$), οπότε $n_j = 0$, $\forall j \in \{1, ..., \kappa\}$, λόγω τού ότι το $X$ είναι $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο τής $G_1$. Άρα και η εικόνα $f(X)$ είναι $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο τής $G_2$. $\square$

**9.5.9 Ορισμός.** Έστω $X$ τυχόν σύνολο και έστω

$$\boxed{\mathbb{Z}^{(X)} := \left\{ f \in \mathbb{Z}^X \,\middle|\, \text{card}(\text{supp}(f)) < \infty \right\}}$$

η αβελιανή ομάδα η έχουσα ως πράξη της την

$$\mathbb{Z}^{(X)} \times \mathbb{Z}^{(X)} \ni (f_1, f_2) \longmapsto f_1 + f_2 \in \mathbb{Z}^{(X)},$$

όπου[62] $(f_1 + f_2)(x) := f_1(x) + f_2(x)$ για κάθε $x \in X$ και

$$\text{supp}(f) := \{x \in X |\, f(x) \neq 0\},\ \forall f \in \mathbb{Z}^{(X)}.$$

(Πρβλ. εδ.[63] 7.1.94 (ii).) Λέμε ότι η $(\mathbb{Z}^{(X)}, +)$ είναι **η ελεύθερη αβελιανή ομάδα** (η οριζόμενη) **επί τού** $X$.

**9.5.10 Πρόταση.** *Έστω $X$ τυχόν μη κενό σύνολο. Η ενριπτική*[64] *απεικόνιση*

$$\boxed{\begin{array}{c} \delta : X \longrightarrow \mathbb{Z}^{(X)},\ x \longmapsto \delta_x, \\ X \ni y \longmapsto \delta_x(y) := \begin{cases} 1, & \text{όταν } x = y, \\ 0, & \text{όταν } x \neq y, \end{cases} \end{array}} \tag{9.56}$$

*έχει τις εξής ιδιότητες:*

(i) *Η εικόνα* $\mathrm{Im}(\delta) = \{\delta_x |\, x \in X\}$ *τής $\delta$ αποτελεί μια $\mathbb{Z}$-βάση τής* $\mathbb{Z}^{(X)}$.

(ii) *Για κάθε αβελιανή ομάδα $(G, +)$ και για κάθε απεικόνιση $\varphi : X \longrightarrow G$ υπάρχει μονοσημάντως ορισμένος ομομορφισμός ομάδων $\widetilde{\varphi} : \mathbb{Z}^{(X)} \longrightarrow G$, ούτως ώστε το ακόλουθο διάγραμμα να καθίσταται μεταθετικό:*

$$\begin{tikzcd} X \arrow[r, hook, "\delta"] \arrow[dr, "\varphi"'] & \mathbb{Z}^{(X)} \arrow[d, "\widetilde{\varphi}"] \\ & G \end{tikzcd}$$

[62]Το $f_1(x) + f_2(x)$ συμβολίζει το *σύνηθες* άθροισμα των ακεραίων αριθμών $f_1(x)$ και $f_2(x)$.

[63]Όπως αναφέραμε και σε αυτό, όταν $X = \varnothing$ η $\mathbb{Z}^{(\varnothing)}$ θεωρείται ότι είναι μια τετριμμένη ομάδα, ενώ όταν το $X$ είναι ένα *μονοσύνολο*, η $\mathbb{Z}^{(X)}$ ταυτίζεται με την ίδια την $\mathbb{Z}$.

[64]Εάν $\delta_{x_1} = \delta_{x_2}$, τότε $\delta_{x_1}(y) = \delta_{x_2}(y), \forall y \in X$, οπότε για $y = x_1 \Rightarrow 1 = \delta_{x_1}(x_1) = \delta_{x_2}(x_1) \Rightarrow x_2 = x_1$.

ΑΠΟΔΕΙΞΗ. (i) Έστω $f \in \mathbb{Z}^{(X)}$. Για κάθε $x \in X$ θέτουμε $n_x := f(x)$. Επειδή $\mathrm{card}(\mathrm{supp}(f)) < \infty$, το άθροισμα $\sum_{x\in X} n_x\delta_x$ είναι πεπερασμένο (ήτοι διαθέτει το πολύ πεπερασμένου πλήθους προσθετέους διάφορους τού $0_{\mathbb{Z}^{(X)}}$) και για *κάθε* $y \in X$ ισχύει

$$\left(\sum_{x\in X} n_x\delta_x\right)(y) = \sum_{x\in X} n_x\delta_x(y) = f(y) \Rightarrow f = \sum_{x\in X} n_x\delta_x.$$

Άρα η $f$ γράφεται ως $\mathbb{Z}$-γραμμικός συνδυασμός στοιχείων τής $\mathrm{Im}(\delta)$. Ας υποθέσουμε ότι η $f$ είναι εκφράσιμη και ως $f = \sum_{x\in X} m_x\delta_x$ για *κάποιους* $m_x \in \mathbb{Z}$. Τότε $\sum_{x\in X} n_x\delta_x = \sum_{x\in X} m_x\delta_x$, οπότε για *κάθε* $y \in X$ έχουμε

$$0 = \sum_{x\in X} (n_x - m_x)\,\delta_x(y) = \begin{cases} n_y - m_y, & \text{όταν } x = y, \\ 0, & \text{όταν } x \neq y, \end{cases}$$

απ' όπου έπεται ότι $n_y = m_y$, $\forall y \in X$. Σύμφωνα με την πρόταση 9.5.5 η $\mathrm{Im}(\delta)$ αποτελεί μια $\mathbb{Z}$-βάση τής $\mathbb{Z}^{(X)}$.

(ii) Ορίζουμε μια απεικόνιση $\widetilde{\varphi} : \mathbb{Z}^{(X)} \longrightarrow G$ ως εξής[65]:

$$\widetilde{\varphi}(f) := \sum_{x\in X} f(x)\varphi(x),\ \forall f \in \mathbb{Z}^{(X)}. \tag{9.57}$$

Επειδή για τυχούσες $f_1, f_2 \in \mathbb{Z}^{(X)}$ ισχύει

$$\begin{aligned}\widetilde{\varphi}(f_1 + f_2) &= \sum_{x\in X} (f_1 + f_2)(x)\varphi(x) = \sum_{x\in X} (f_1(x) + f_2(x))\varphi(x) \\ &= \sum_{x\in X} f_1(x)\varphi(x) + \sum_{x\in X} f_2(x)\varphi(x) = \widetilde{\varphi}(f_1) + \widetilde{\varphi}(f_2),\end{aligned}$$

έχουμε $\widetilde{\varphi} \in \mathrm{Hom}(\mathbb{Z}^{(X)}, G)$ και $\widetilde{\varphi}(\delta_y) = \sum_{x\in X} \delta_y(x)\varphi(x) = \varphi(y)$ για κάθε $y \in X$, οπότε $\widetilde{\varphi} \circ \delta = \varphi$. Απομένει λοιπόν να δειχθεί η μοναδικότητα τού $\widetilde{\varphi}$ (με αυτήν την ιδιότητα). Ας υποθέσουμε ότι υπάρχει $\widetilde{\varphi}' \in \mathrm{Hom}(\mathbb{Z}^{(X)}, G)$ με $\widetilde{\varphi}' \circ \delta = \varphi$. Τότε

$$f = \sum_{x\in X} f(x)\delta_x \Rightarrow \widetilde{\varphi}'(f) = \sum_{x\in X} f(x)\widetilde{\varphi}'(\delta_x) = \sum_{x\in X} f(x)\varphi(x) = \widetilde{\varphi}(f)$$

για κάθε $f \in \mathbb{Z}^{(X)}$, οπότε $\widetilde{\varphi}' = \widetilde{\varphi}$ και η απόδειξη λήγει εδώ. □

**9.5.11 Σημείωση.** Έστω $r \in \mathbb{N}$ και έστω $X = \{x_1, ..., x_r\}$ οιοδήποτε σύνολο με $\mathrm{card}(X) = r$. Τότε η απεικόνιση

$$\mathbb{Z}^{(X)} \ni \sum_{j=1}^{r} n_j\delta_{x_j} \longmapsto (n_1, ..., n_r) \in \mathbb{Z}^r := \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \text{ φορές}}$$

αποτελεί έναν ισομορφισμό.

**9.5.12 Ορισμός.** Μια αβελιανή ομάδα $(G, +)$ καλείται **ελεύθερη αβελιανή ομάδα** όταν υφίσταται κάποιο σύνολο $X$, τέτοιο ώστε να ισχύει[66] $G \cong \mathbb{Z}^{(X)}$.

[65] *Και εδώ* το άθροισμα αυτό είναι πεπερασμένο, διότι $\mathrm{card}(\mathrm{supp}(f)) < \infty$.

[66] Εάν $G \cong \mathbb{Z}^{(X)}$, τότε έχουμε $|G| = 1$ όταν $X = \varnothing$, $|G| = \aleph_0$ όταν το σύνολο $X$ είναι πεπερασμένο και $|G| = \max\{\aleph_0, \mathrm{card}(X)\}$ όταν το $X$ είναι άπειρο.

**9.5.13 Θεώρημα.** *Για μια αβελιανή ομάδα $(G,+)$ οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Η $G$ είναι ελεύθερη αβελιανή ομάδα.*

(ii) *Η $G$ διαθέτει τουλάχιστον μία $\mathbb{Z}$-βάση.*

ΑΠΟΔΕΙΞΗ. (i)$\Rightarrow$(ii) Ας υποθέσουμε ότι υφίσταται κάποιο σύνολο $X$, τέτοιο ώστε να ισχύει $G \cong \mathbb{Z}^{(X)}$. Εάν $X = \varnothing$, τότε η $G$ είναι τετριμμένη έχουσα (εξ ορισμού) το κενό σύνολο ως (μόνη) $\mathbb{Z}$-βάση της. Εάν $X \neq \varnothing$, τότε η εικόνα $\mathrm{Im}(\delta)$ τής (9.56) είναι μια $\mathbb{Z}$-βάση τής $\mathbb{Z}^{(X)}$. Επομένως, η εικόνα αυτής μέσω οιουδήποτε ισομορφισμού μεταξύ τής $\mathbb{Z}^{(X)}$ και τής $G$ αποτελεί (σύμφωνα με την πρόταση 9.5.8) μια $\mathbb{Z}$-βάση τής $G$.

(ii)$\Rightarrow$(i) Έστω $X$ μια $\mathbb{Z}$-βάση τής $G$. Εάν $X = \varnothing$, τότε είναι προφανές ότι $G \cong \mathbb{Z}^{(\varnothing)}$. Εάν $X \neq \varnothing$, τότε (σύμφωνα με το (ii) τής προτάσεως 9.5.10) υπάρχει μονοσημάντως ορισμένος $\widetilde{\iota} \in \mathrm{Hom}(\mathbb{Z}^{(X)}, G)$, τέτοιος ώστε να ισχύει $\widetilde{\iota} \circ \delta = \iota$, όπου $\iota : X \hookrightarrow G$ η συνήθης ένθεση. Επειδή η εικόνα $\mathrm{Im}(\widetilde{\iota})$ τού $\widetilde{\iota}$ είναι μια υποομάδα τής $G$ που περιέχει το $X$ και $\mathrm{Lin}_{\mathbb{Z}}(X) = G$, η πρόταση 9.5.2 μας πληροφορεί ότι

$$\mathrm{Lin}_{\mathbb{Z}}(X) \subseteq \mathrm{Im}(\widetilde{\iota}) \Rightarrow \mathrm{Im}(\widetilde{\iota}) = G,$$

οπότε ο $\widetilde{\iota}$ είναι επιμορφισμός. Από την άλλη μεριά, επειδή

$$\widetilde{\iota}(f) := \sum_{x \in X} f(x)\iota(x) = \sum_{x \in X} f(x)x, \ \forall f \in \mathbb{Z}^{(X)}$$

(βλ. (9.57)), για κάθε $f \in \mathrm{Ker}(\widetilde{\iota})$ λαμβάνουμε

$$\sum_{x \in X} f(x)x = \widetilde{\iota}(f) = 0_G \Rightarrow [f(x) = 0, \forall x \in X] \Rightarrow \mathrm{supp}(f) = \varnothing \Rightarrow f = 0_{\mathbb{Z}^{(X)}},$$

διότι το $X$ είναι $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο τής $G$. Κατά συνέπειαν, $\mathrm{Ker}(\widetilde{\iota}) = \{0_{\mathbb{Z}^{(X)}}\}$ και ο $\widetilde{\iota}$ είναι μονομορφισμός. (Βλ. πρόταση 2.4.15.) Τελικώς λοιπόν ο $\widetilde{\iota}$ είναι *ισομορφισμός* και, ως εκ τούτου, η $G$ είναι ελεύθερη αβελιανή ομάδα. $\square$

**9.5.14 Πόρισμα.** *Εάν $(G,+)$ είναι αβελιανή ομάδα έχουσα το $X \subseteq G$ ως μια $\mathbb{Z}$-βάση της, τότε $G \cong \mathbb{Z}^{(X)}$.*

**9.5.15 Πόρισμα.** *Για μια μη τετριμμένη αβελιανή ομάδα $(G,+)$ οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Η $G$ είναι ελεύθερη αβελιανή ομάδα.*

(ii) *Υπάρχει $\varnothing \neq X \subseteq G$, τέτοιο ώστε η απεικόνιση $\mathbb{Z} \ni n \longmapsto nx \in \langle x \rangle$ να είναι ισομορφισμός για κάθε $x \in X$ και να ισχύει $G = \bigoplus_{x \in X}^{\text{εσ.}} \langle x \rangle$.*

ΑΠΟΔΕΙΞΗ. (i)$\Rightarrow$(ii) Κατά το θεώρημα 9.5.13 υπάρχει κάποια $\mathbb{Z}$-βάση $X$ τής $G$. Επειδή η $G$ είναι μη τετριμμένη, $X \neq \varnothing$. Κάθε στοιχείο τής $G$ γράφεται ως $\mathbb{Z}$-γραμμικός συνδυασμός στοιχείων τού $X$ (και μάλιστα, σύμφωνα με την πρόταση

9.5.5, κατά τρόπο μονοσήμαντο), οπότε από τη συνεπαγωγή (b)⇒(a) τού θεωρήματος 7.1.98 έπεται ότι $G = \bigoplus_{x\in X}^{\text{εσ.}} \langle x\rangle$. Επίσης, για κάθε $x \in X$ η απεικόνιση $\mathbb{Z} \ni n \longmapsto nx \in \langle x\rangle$ είναι (προφανώς) επιμορφισμός. Η ενριπτικότητά της έπεται άμεσα από το γεγονός ότι το μονοσύνολο $\{x\}$ είναι $\mathbb{Z}$-γραμμικώς ανεξάρτητο.

(ii)⇒(i) Προφανώς, $G = \bigoplus_{x\in X}^{\text{εσ.}} \langle x\rangle \Rightarrow G = \langle X\rangle$. Επειδή η $\mathbb{Z} \ni n \longmapsto nx \in \langle x\rangle$ είναι ισομορφισμός, το μονοσύνολο $\{x\}$ είναι $\mathbb{Z}$-γραμμικώς ανεξάρτητο για κάθε $x \in X$. Έστω $\{x_1, ..., x_\kappa\}$ τυχόν πεπερασμένο υποσύνολο τού $X$. Εάν $n_1, ..., n_\kappa \in \mathbb{Z}$ είναι τέτοιοι, ώστε να ισχύει $\sum_{j=1}^{\kappa} n_j x_j = 0_G$, τότε

$$\left.\begin{array}{l} \sum\limits_{j=1}^{\kappa} \underbrace{n_j x_j}_{\in\langle x_j\rangle} = 0_G = \underbrace{0_G + \cdots + 0_G}_{\kappa \text{ φορές}} \\ G = \bigoplus\limits_{x\in X}^{\text{εσ.}} \langle x\rangle \,,\ \forall j \in \{1, ..., \kappa\} \end{array}\right\} \underset{7.1.98\,(a)\Rightarrow(b)}{\Longrightarrow} n_j x_j = 0_G, \forall j \in \{1, ..., \kappa\},$$

οπότε $n_j = 0$ (αφού το $\{x_j\}$ είναι $\mathbb{Z}$-γραμμικώς ανεξάρτητο) για κάθε $j \in \{1, ..., \kappa\}$. Άρα το $X$ είναι (καθ' ολοκληρίαν) $\mathbb{Z}$-γραμμικώς ανεξάρτητο και, κατ' επέκταση, μια $\mathbb{Z}$-βάση τής $G$. Κατά συνέπειαν, η $G$ είναι ελεύθερη αβελιανή ομάδα (εκ νέου δυνάμει τού θεωρήματος 9.5.13). □

**9.5.16 Πόρισμα.** *Κάθε ελεύθερη αβελιανή ομάδα στερείται στρέψεως.*

ΑΠΟΔΕΙΞΗ. Έστω $(G, +)$ μια ελεύθερη αβελιανή ομάδα. Σύμφωνα με το θεώρημα 9.5.13 υπάρχει κάποια $\mathbb{Z}$-βάση $X$ αυτής. Εάν $X = \varnothing$, τότε η $G$ είναι τετριμμένη και ο ισχυρισμός προδήλως αληθής. Εάν $X \neq \varnothing$ και $g \in G$ είναι ένα στοιχείο *πεπερασμένης* τάξεως, τότε (εξ ορισμού) υπάρχουν $\kappa \in \mathbb{N}$ και $n_1, ..., n_\kappa \in \mathbb{Z}$, $x_1, ..., x_\kappa \in X$ με $g = \sum_{j=1}^{\kappa} n_j x_j$. Προφανώς,

$$\left.\begin{array}{r} 0_G = \operatorname{ord}(g)g = \sum\limits_{j=1}^{\kappa} (\operatorname{ord}(g)n_j)x_j \\ 0_G = 0 \cdot x_1 + \cdots + 0 \cdot x_\kappa \end{array}\right\} \underset{9.5.5}{\Longrightarrow} \operatorname{ord}(g)n_j = 0, \forall j \in \{1, ..., \kappa\},$$

οπότε $[n_j = 0, \forall j \in \{1, ..., \kappa\}] \Rightarrow g = 0_G$. Επομένως, $\operatorname{tors}(G) = \{0_G\}$. □

**9.5.17 Σημείωση.** Το αντίστροφο τού πορίσματος 9.5.16 δεν είναι πάντοτε αληθές. Επί παραδείγματι, η αβελιανή ομάδα $(\mathbb{Q}, +)$ στερείται στρέψεως αλλά δεν είναι ελεύθερη. (Βλ. 9.5.23 (iii).) Ωστόσο, όπως θα δούμε στο θεώρημα 9.6.1, είναι δυνατόν να αποδειχθεί ένα *μερικό αντίστροφο* αυτού. Από την άλλη μεριά, το θεώρημα 9.5.53 περιγράφει επακριβώς το πότε μια *αριθμήσιμη* αβελιανή ομάδα χωρίς στρέψη είναι ελεύθερη.

**9.5.18 Πόρισμα.** *Δεν υφίσταται καμία πεπερασμένη μη τετριμμένη ελεύθερη αβελιανή ομάδα (και, γενικότερα, καμία μη τετριμμένη ελεύθερη αβελιανή ομάδα έχουσα κάποιο στοιχείο, διάφορο τού ουδετέρου, με πεπερασμένη τάξη).*

**9.5.19 Παράδειγμα.** Η άπειρη αβελιανή πηλικοομάδα $(\mathbb{Q}/\mathbb{Z}, +)$ δεν είναι ελεύθερη, διότι (όπως έχουμε αποδείξει στο εδάφιο 4.4.11) είναι περιοδική (= ομάδα στρέψεως).

**9.5.20 Πρόταση.** *Έστω $(G,+)$ μια ελεύθερη αβελιανή ομάδα. Εάν $X$ είναι μια $\mathbb{Z}$-βάση τής $G$, $Y \subseteq X$ και $H := \langle Y \rangle$ η ελεύθερη υποομάδα η παραγόμενη από το*[67] *$Y$, τότε η πηλικοομάδα $G/H$ είναι μια ελεύθερη αβελιανή ομάδα έχουσα το σύνολο $\{x + H | \, x \in X \smallsetminus Y\}$ ως μια $\mathbb{Z}$-βάση της.*

ΑΠΟΔΕΙΞΗ. Αφήνεται ως άσκηση. □

**9.5.21 Πρόταση.** *Έστω $(G,+)$ μια ελεύθερη μη τετριμμένη αβελιανή ομάδα και έστω $X$ μια $\mathbb{Z}$-βάση αυτής. Εάν $x \in X$ και $\ell \in \mathbb{Z} \smallsetminus \{0, \pm 1\}$, τότε $\nexists y \in G : \ell y = x$.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι $\exists y \in G : \ell y = x$. Επειδή $G = \langle X \rangle$, θα υπάρχει κάποιο πεπερασμένο υποσύνολο $\{x_1, ..., x_\kappa\}$ τού $X$ και $n_1, ..., n_\kappa, m_1, ..., m_\kappa \in \mathbb{Z}$, ούτως ώστε να ισχύει

$$x = \sum_{j=1}^{\kappa} n_j x_j \;\text{ και }\; y = \sum_{j=1}^{\kappa} m_j x_j .$$

Επειδή $x \in X$ και $x = 1 \cdot x$ *είναι* μια παράσταση τού $x$ ως $\mathbb{Z}$-γραμμικού συνδυασμού (τού ίδιου τού $x$), από την πρόταση 9.5.5 συνάγεται ότι $\exists j_\bullet \in \{1, ..., \kappa\} : n_j = 0$ για κάθε $j \in \{1, ..., \kappa\} \smallsetminus \{j_\bullet\}$ και $n_{j_\bullet} = 1$, $x = x_{j_\bullet}$. Επομένως,

$$\ell y = x \Rightarrow \sum_{j=1}^{\kappa} (\ell m_j) x_j = x_{j_\bullet} \Rightarrow m_j = 0, \forall j \in \{1, ..., \kappa\} \smallsetminus \{j_\bullet\}, \;\text{ και }\; \ell m_{j_\bullet} = 1.$$

Όμως $\nexists m_{j_\bullet} \in \mathbb{Z} : \ell m_{j_\bullet} = 1$. Άτοπο! □

**9.5.22 Πρόταση.** *Έστω $(G,+)$ μια ελεύθερη μη τετριμμένη αβελιανή ομάδα και έστω $g \in G \smallsetminus \{0_G\}$. Τότε το σύνολο $\{n \in \mathbb{Z} | \, \exists g' \in G : g = ng'\}$ είναι πεπερασμένο.*

ΑΠΟΔΕΙΞΗ. Επειδή η $G$ δεν είναι τετριμμένη, υφίσταται (εξ ορισμού) ισομορφισμός $f : G \xrightarrow{\cong} \mathbb{Z}^{(X)}$, για κάποιο *μη κενό* σύνολο $X$. Εάν $f(g) = a = (a_x)_{x \in X}$, τότε $a \neq 0_{\mathbb{Z}^{(X)}}$ και, ως εκ τούτου, υπάρχει κάποιος $x_0 \in X$, τέτοιος ώστε να ισχύει $a_{x_0} \neq 0$. Για οιονδήποτε $n \in \mathbb{Z}$ για τον οποίο υπάρχει κάποιο $g' \in G \smallsetminus \{0_G\}$ με $g = ng'$ και $f(g') = a' = (a'_x)_{x \in X}$, λαμβάνουμε

$$a = f(g) = f(ng') = nf(g') = na' \Rightarrow a_{x_0} = na'_{x_0} \Rightarrow n \mid a_{x_0}.$$

Επειδή το πλήθος το ακεραίων διαιρετών τού *μη μηδενικού* ακεραίου $a_{x_0}$ είναι πεπερασμένο, ο ισχυρισμός είναι προδήλως αληθής. □

**9.5.23 Παραδείγματα.** (i) Προφανώς, η αβελιανή ομάδα $(\mathbb{Z},+)$ είναι ελεύθερη.

(ii) Γενικότερα, η $(\mathbb{Z}^r,+)$ είναι ελεύθερη για κάθε $r \in \mathbb{N}$. (Βλ. 9.5.11.)

(iii) Η αβελιανή ομάδα $(\mathbb{Q},+)$ δεν είναι ελεύθερη. (Εάν αυτή διέθετε κάποια $\mathbb{Z}$-βάση $X$ και $x \in X$, $\ell \in \mathbb{Z} \smallsetminus \{0, \pm 1\}$, τότε η εξίσωση $\ell y = x$ θα είχε *πάντοτε* μία ρητή λύση $y$, συγκεκριμένα την $y = \frac{x}{\ell}$,κάτι που θα αντέκειτο σε ό,τι απεδείχθη στην πρόταση 9.5.21.)

[67] Είναι προφανές ότι το $Y$ αποτελεί μια $\mathbb{Z}$-βάση τής $H$.

(iv) Από την άλλη μεριά, η *πολλαπλασιαστική* αβελιανή ομάδα $(\mathbb{Q}_{>0}, \cdot)$ *είναι* ελεύθερη, έχουσα το σύνολο των πρώτων αριθμών ως μια $\mathbb{Z}$-βάση της. (Βλ. B.3.10 και 9.5.5, κάνοντας χρήση τού πολλαπλασιαστικού συμβολισμού.)

(v) Η *πολλαπλασιαστική* αβελιανή ομάδα $(\mathbb{R}_{>0}, \cdot)$ δεν είναι ελεύθερη. (Εάν αυτή διέθετε κάποια $\mathbb{Z}$-βάση $X$ και $x \in X$, τότε η μέσω τού πολλαπλασιαστικού συμβολισμού εκφραζόμενη εξίσωση $y^2 = x$ θα είχε *πάντοτε* μία θετική πραγματική λύση $y$, συγκεκριμένα την $y = \sqrt{x}$,κάτι που θα αντέκειτο στο πόρισμα 9.5.21.)

(vi) Η αβελιανή ομάδα $(\mathbb{Z}[\mathsf{X}], +)$ των πολυωνύμων μιας απροσδιορίστου X με ακεραίους συντελεστές (ταυτιζόμενη με την $(\mathbb{Z}^{(\mathbb{N}_0)}, +)$, βλ. εδ. C.1.17) είναι ελεύθερη. (Μάλιστα, ως «συνηθέστερη» $\mathbb{Z}$-βάση της μπορεί να θεωρηθεί η $\{\mathsf{X}^n \,|n \in \mathbb{N}_0\}$ .)

(vii) Μέσω τής προτάσεως 9.5.22 αποδεικνύεται ότι η $(\mathbb{Z}^{\mathbb{N}}, +)$ *δεν είναι ελεύθερη*. (Βλ. θεώρημα 9.5.58.)

**9.5.24 Σημείωση.** Για οιοδήποτε σύνολο $X$ και για οιονδήποτε πρώτον αριθμό $p$ η αβελιανή πηλικοομάδα $\mathbb{Z}^{(X)}/p\mathbb{Z}^{(X)} \cong (\mathbb{Z}/p\mathbb{Z})^{(X)} \cong \mathbb{Z}_p^{(X)}$ μπορεί να ιδωθεί (κατά τα πραναφερθέντα στο εδ. 9.1.5) ως ένας $\mathbb{Z}_p$-διανυσματικός χώρος. Επειδή αυτός έχει είτε το $\varnothing$ (όταν $X = \varnothing$) είτε το σύνολο $\{\, \delta_x + p\, \langle \delta_x \rangle |\, x \in X\}$ (όταν $X \neq \varnothing$) ως βάση του (υπό τη συνήθη έννοια), έχουμε

$$\dim_{\mathbb{Z}_p}(\mathbb{Z}^{(X)}/p\mathbb{Z}^{(X)}) = \text{ card}\,(X)\,. \tag{9.58}$$

**9.5.25 Πρόταση. (Ισοπληθικότητα $\mathbb{Z}$-βάσεων.)** *Όλες οι $\mathbb{Z}$-βάσεις μιας ελεύθερης αβελιανής ομάδας $(G, +)$ είναι ισοπληθείς.*

ΑΠΟΔΕΙΞΗ. Έστω ότι οι $X, Y$ είναι τυχούσες $\mathbb{Z}$-βάσεις τής $G$. Τότε

$$\mathbb{Z}^{(X)} \cong G \cong \mathbb{Z}^{(Y)} \underset{9.1.7}{\Longrightarrow} p\mathbb{Z}^{(X)} \cong p\mathbb{Z}^{(Y)} \underset{4.5.8\,(\text{ii})}{\Longrightarrow} \mathbb{Z}^{(Y)}/p\mathbb{Z}^{(Y)} \cong \mathbb{Z}^{(Y)}/p\mathbb{Z}^{(Y)}.$$

Ο τελευταίος ισομορφισμός ομάδων είναι και ισομορφισμός $\mathbb{Z}_p$-διανυσματικών χώρων, οπότε

$$\text{card}(X) \underset{(9.58)}{=} \dim_{\mathbb{Z}_p}(\mathbb{Z}^{(X)}/p\mathbb{Z}^{(X)}) = \dim_{\mathbb{Z}_p}(\mathbb{Z}^{(Y)}/p\mathbb{Z}^{(Y)}) \underset{(9.58)}{=} \text{card}(Y)\,.$$

Άρα οι $X$ και $Y$ είναι ισοπληθείς. □

**9.5.26 Ορισμός. («Βαθμίδα» ελεύθερης αβελιανής ομάδας.)** Ο πληθικός αριθμός οιασδήποτε $\mathbb{Z}$-βάσεως μιας ελεύθερης αβελιανής ομάδας $G$ καλείται **βαθμίδα** τής $G$ και συμβολίζεται ως $\text{rank}_{\mathbb{Z}}(G)$.

**9.5.27 Παραδείγματα.** (i) Για κάθε $r \in \mathbb{N}_0$ έχουμε $\text{rank}_{\mathbb{Z}}(\mathbb{Z}^r) = r$.

(ii) Προφανώς, η *πολλαπλασιαστική* ελεύθερη αβελιανή ομάδα $(\mathbb{Q}_{>0}, \cdot)$ έχει βαθμίδα $\text{rank}_{\mathbb{Z}}(\mathbb{Q}_{>0}) = \aleph_0$. (Βλ. 9.5.23 (iv).)

(iii) Παρομοίως, $\text{rank}_{\mathbb{Z}}(\mathbb{Z}[\mathsf{X}]) = \aleph_0$. (Βλ. 9.5.23 (vi).)

(iv) $\text{rank}_{\mathbb{Z}}(\mathbb{Z}^{(\mathbb{R})}) = \mathfrak{c}$.

**9.5.28 Παρατήρηση.** Έστω $G$ μια ελεύθερη αβελιανή ομάδα.

(i) Εάν $\mathrm{rank}_{\mathbb{Z}}(G) = r \in \mathbb{N}$, τότε ένα $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο $X$ τής $G$ με $\mathrm{card}(X) = r$ δεν είναι κατ' ανάγκην $\mathbb{Z}$-βάση αυτής! (Π.χ., το μονοσύνολο $X = \{2\}$ είναι $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο τής $(\mathbb{Z}, +)$ αλλά δεν είναι $\mathbb{Z}$-βάση της.)

(ii) Όπως έχει ήδη προαναφερθεί (στο εδ. 9.5.7 (i)), ενδέχεται να υπάρχουν συστήματα γεννητόρων τής $G$ τα οποία δεν περιέχουν $\mathbb{Z}$-βάσεις αυτής. Ωστόσο, εάν η $G$ είναι *πεπερασμένως παραγόμενη*, ας πούμε από ένα υποσύνολο $X$ με $\mathrm{card}(X) = \kappa \in \mathbb{N}$, τότε $\mathrm{rank}_{\mathbb{Z}}(G) \leq \kappa$.

**9.5.29 Πρόταση. («Καθολική ιδιότητα» ελεύθερων αβελιανών ομάδων.)** *Έστω $G_1$ μια ελεύθερη μη τετριμμένη αβελιανή ομάδα και έστω $X$ μια $\mathbb{Z}$-βάση αυτής. Εάν $\varphi : X \longrightarrow G_2$ είναι μια απεικόνιση από το $X$ σε μια τυχούσα αβελιανή ομάδα $G_2$, τότε υπάρχει μονοσημάντως ορισμένος $f \in \mathrm{Hom}(G_1, G_2)$, τέτοιος ώστε να ισχύει $f(x) = \varphi(x), \forall x \in X$, ήτοι $f|_X = \varphi$.*

ΑΠΟΔΕΙΞΗ. Έστω τυχόν $g \in G_1$. Σύμφωνα με την πρόταση 9.5.5 το $g$ γράφεται κατά τρόπο μονοσήμαντο ως $\mathbb{Z}$-γραμμικός συνδυασμός $g = \sum_{j=1}^{\kappa} n_j x_j$ στοιχείων $x_1, ..., x_\kappa$ τού $X$. Ορίζουμε την απεικόνιση

$$f : G_1 \longrightarrow G_2, \;\; g \longmapsto f(g) := \sum_{j=1}^{\kappa} n_j \varphi(x_j).$$

Είναι εύκολο να ελεγχθεί ότι η $f$ είναι ομομορφισμός και ότι $f|_X = \varphi$. Απομένει λοιπόν να δειχθεί η μοναδικότητα τού $f$ (με αυτήν την ιδιότητα). Ας υποθέσουμε ότι υπάρχει $f' \in \mathrm{Hom}(G_1, G_2)$ με $f'|_X = \varphi$. Τότε

$$\begin{aligned} f'(g) &= f'\left(\sum_{j=1}^{\kappa} n_j x_j\right) = \sum_{j=1}^{\kappa} n_j f'(x_j) = \sum_{j=1}^{\kappa} n_j \varphi(x_j) \\ &= \sum_{j=1}^{\kappa} n_j f(x_j) = f\left(\sum_{j=1}^{\kappa} n_j x_j\right) = f(g) \end{aligned}$$

για κάθε $g = \sum_{j=1}^{\kappa} n_j x_j \in G_1$, οπότε $f' = f$ και η απόδειξη λήγει εδώ. □

**9.5.30 Πόρισμα.** *Εάν $X_1, X_2$ είναι δυο μη κενά σύνολα και $\varphi : X_1 \longrightarrow X_2$ τυχούσα απεικόνιση, τότε ισχύουν τα εξής:*

(i) *Υπάρχει μονοσημάντως ορισμένος $f \in \mathrm{Hom}(\mathbb{Z}^{(X_1)}, \mathbb{Z}^{(X_2)})$, ούτως ώστε το ακόλουθο διάγραμμα να καθίσταται μεταθετικό:*

$$\begin{tikzcd} \mathrm{Im}(\delta^{(X_1)}) \arrow[r, hook, "\iota_1"] \arrow[d, "\overline{\varphi}"'] \arrow[dr, phantom, "\circlearrowright"] & \mathbb{Z}^{(X_1)} \arrow[d, "f"] \\ \mathrm{Im}(\delta^{(X_2)}) \arrow[r, hook, "\iota_2"'] & \mathbb{Z}^{(X_2)} \end{tikzcd}$$

(Εν προκειμένω, για $j = 1, 2$ η $\delta^{(X_j)} : X_j \longrightarrow \mathbb{Z}^{(X_j)}$ είναι η ένριψη (9.56) για το $X_j$, $\iota_j : \mathrm{Im}(\delta^{(X_j)}) \hookrightarrow \mathbb{Z}^{(X_j)}$ η συνήθης ένθεση και $\overline{\varphi} : \mathrm{Im}(\delta^{(X_1)}) \longrightarrow \mathrm{Im}(\delta^{(X_2)})$ η απεικόνιση $\overline{\varphi}(\delta_x^{(X_1)}) := \delta_{\varphi(x)}^{(X_2)}, \forall x \in X_1$.)

(ii) *Εάν η $\varphi$ είναι ενριπτική, τότε ο $f$ είναι μονομορφισμός.*

(iii) *Εάν η $\varphi$ είναι αμφιρριπτική, τότε ο $f$ είναι ισομορφισμός.*

ΑΠΟΔΕΙΞΗ. (i) Ο ζητούμενος $f \in \mathrm{Hom}(\mathbb{Z}^{(X_1)}, \mathbb{Z}^{(X_2)})$ προκύπτει ύστερα από εφαρμογή τής προτάσεως 9.5.29 (με τις $\mathbb{Z}^{(X_1)}, \mathbb{Z}^{(X_2)}$ στη θέση των $G_1, G_2$, αντιστοίχως, με την εικόνα $\mathrm{Im}(\delta^{(X_1)})$ στη θέση τού εκεί παρατεθέντος $X$ και με την $\iota_2 \circ \overline{\varphi}$ στη θέση τής εκεί κληθείσας $\varphi$).

(ii) Εάν η $\varphi$ είναι ενριπτική και $y$ τυχόν στοιχείο τού πυρήνα τού ανωτέρω κατασκευασθέντος $f \in \mathrm{Hom}(\mathbb{Z}^{(X_1)}, \mathbb{Z}^{(X_2)})$, τότε $y = \sum_{j=1}^{\kappa} n_j \delta_{x_j}^{(X_1)}$ για κάποιο πεπερασμένο υποσύνολο $\{x_1, ..., x_\kappa\}$ τού $X_1$ και κάποιους $n_1, ..., n_\kappa \in \mathbb{Z}$, οπότε

$$0_{\mathbb{Z}^{(X_2)}} = f(y) = \sum_{j=1}^{\kappa} n_j f(\delta_{x_j}^{(X_1)}) = \sum_{j=1}^{\kappa} n_j \overline{\varphi}(\delta_{x_j}^{(X_1)}) = \sum_{j=1}^{\kappa} n_j \delta_{\varphi(x_j)}^{(X_2)}. \tag{9.59}$$

Επειδή $\varphi(x_j) \neq \varphi(x_{j'})$ για $j, j' \in \{1, ..., \kappa\}$ με $j \neq j'$, η (9.59) σε συνδυασμό με τη $\mathbb{Z}$-γραμμική ανεξαρτησία τού $\mathrm{Im}(\delta^{(X_2)})$ δίδει

$$[n_j = 0,\ \forall j \in \{1, ..., \kappa\}] \Rightarrow y = 0_{\mathbb{Z}^{(X_1)}}.$$

(iii) Εάν η $\varphi$ είναι αμφιρριπτική, τότε και η $\overline{\varphi}$ είναι αμφιρριπτική και εκ νέου εφαρμογή τής προτάσεως 9.5.29 (με τις $\mathbb{Z}^{(X_2)}, \mathbb{Z}^{(X_1)}$ στη θέση των $G_1, G_2$, αντιστοίχως, με την εικόνα $\mathrm{Im}(\delta^{(X_2)})$ στη θέση τού εκεί παρατεθέντος $X$ και με την $\iota_1 \circ \overline{\varphi}^{-1}$ στη θέση τής εκεί κληθείσας $\varphi$) μας οδηγεί στην κατασκευή μονοσημάντως ορισμένου $f' \in \mathrm{Hom}(\mathbb{Z}^{(X_2)}, \mathbb{Z}^{(X_1)})$ με την ιδιότητα $f'|_{\mathrm{Im}(\delta^{(X_2)})} = f' \circ \iota_2 = \iota_1 \circ \overline{\varphi}^{-1}$. Επομένως,

$$(f' \circ f)|_{\mathrm{Im}(\delta^{(X_1)})} = f' \circ f \circ \iota_1 = f' \circ \iota_2 \circ \overline{\varphi} = \overline{\varphi}^{-1} \circ \overline{\varphi} = \mathrm{id}_{\mathrm{Im}(\delta^{(X_1)})},$$
$$(f \circ f')|_{\mathrm{Im}(\delta^{(X_2)})} = f \circ f' \circ \iota_2 = f \circ \iota_1 \circ \overline{\varphi}^{-1} = \overline{\varphi} \circ \overline{\varphi}^{-1} = \mathrm{id}_{\mathrm{Im}(\delta^{(X_2)})}.$$

Επειδή $\left\langle \mathrm{Im}(\delta^{(X_1)}) \right\rangle = \mathbb{Z}^{(X_1)}$ και $\left\langle \mathrm{Im}(\delta^{(X_2)}) \right\rangle = \mathbb{Z}^{(X_2)}$, έχουμε $f' \circ f = \mathrm{id}_{\mathbb{Z}^{(X_1)}}$ και $f \circ f' = \mathrm{id}_{\mathbb{Z}^{(X_2)}}$. (Βλ. 2.4.9 (ii).) Άρα ο $f$ είναι ισομορφισμός και $f' = f^{-1}$. □

**9.5.31 Θεώρημα.** *Για ελεύθερες αβελιανές ομάδες $G_1, G_2$ ισχύει η αμφίπλευρη συνεπαγωγή:*

$$\boxed{G_1 \cong G_2 \Longleftrightarrow \mathrm{rank}_{\mathbb{Z}}(G_1) = \mathrm{rank}_{\mathbb{Z}}(G_2).}$$

ΑΠΟΔΕΙΞΗ. "$\Rightarrow$" Έστω $f : G_1 \xrightarrow{\cong} G_2$ ένας ισομορφισμός. Εάν $X_1$ είναι μια $\mathbb{Z}$-βάση τής $G_1$, τότε (σύμφωνα με την πρόταση 9.5.8) η εικόνα $X_2 := f(X_1)$ τής $X_1$ μέσω τού $f$ αποτελεί μια $\mathbb{Z}$-βάση τής $G_2$, οπότε

$$\mathrm{card}(X_1) = \mathrm{card}(X_2) \Rightarrow \mathrm{rank}_{\mathbb{Z}}(G_1) = \mathrm{rank}_{\mathbb{Z}}(G_2).$$

"$\Leftarrow$" Εάν η κοινή βαθμίδα των $G_1, G_2$ είναι ίση με το $0$, τότε αμφότερες οι $G_1, G_2$ είναι προδήλως τετριμμένες (και, ως εκ τούτου, ισόμορφες). Ας υποθέσουμε ότι η κοινή βαθμίδα των $G_1, G_2$ είναι $> 0$. Εάν $X_1$ είναι μια $\mathbb{Z}$-βάση τής $G_1$, τότε (σύμφωνα με το πόρισμα 9.5.14) $G_1 \cong \mathbb{Z}^{(X_1)}$ και $\mathrm{rank}_{\mathbb{Z}}(G_1) = \mathrm{card}(X_1)$. Έστω $X_2$ *τυχούσα* $\mathbb{Z}$-βάση τής $G_2$. Εξ υποθέσεως,

$$\mathrm{card}(X_1) = \mathrm{rank}_{\mathbb{Z}}(G_1) = \mathrm{rank}_{\mathbb{Z}}(G_2) = \mathrm{card}(X_2),$$

οπότε υπάρχει κάποια αμφίρριψη $\varphi : X_1 \longrightarrow X_2$. Κατά το πόρισμα 9.5.30 υπάρχει ισομορφισμός $f : \mathbb{Z}^{(X_1)} \xrightarrow{\cong} \mathbb{Z}^{(X_2)}$. Άρα $G_1 \cong \mathbb{Z}^{(X_1)} \underset{f}{\xrightarrow{\cong}} \mathbb{Z}^{(X_2)} \cong G_2$. □

**9.5.32 Πόρισμα.** *Για κάθε ελεύθερη αβελιανή $G$ ομάδα με $\mathrm{rank}_{\mathbb{Z}}(G) = r \in \mathbb{N}_0$ έχουμε $G \cong \mathbb{Z}^r$.*

**9.5.33 Πόρισμα.** *Εάν $r_1, r_2 \in \mathbb{N}_0$, τότε $\mathbb{Z}^{r_1} \cong \mathbb{Z}^{r_2} \Longleftrightarrow r_1 = r_2$.*

**9.5.34 Πόρισμα.** *Εάν $r_1, r_2 \in \mathbb{N}_0$ και $G_1, G_2$ είναι ελεύθερες αβελιανές ομάδες βαθμίδας $r_1$ και $r_2$, αντιστοίχως, τότε η $G_1 \oplus G_2$ είναι ελεύθερη βαθμίδας $r_1 + r_2$.*

ΑΠΟΔΕΙΞΗ. Προφανώς, $[G_1 \cong \mathbb{Z}^{r_1}$ και $G_2 \cong \mathbb{Z}^{r_2}] \Rightarrow G_1 \oplus G_2 \cong \mathbb{Z}^{r_1+r_2}$. □

**9.5.35 Θεώρημα.** *Κάθε αβελιανή ομάδα $(G, +)$ είναι ισόμορφη με την πηλικοομάδα $\mathbb{Z}^{(X)}/H$, όπου $X \subseteq G$ είναι οιοδήποτε σύστημα γεννητόρων τής $G$ και $H$ κατάλληλη υπομάδα τής $\mathbb{Z}^{(X)}$ εξαρτώμενη από αυτό.*

ΑΠΟΔΕΙΞΗ. Εάν η $G$ είναι τετριμμένη, τότε $G \cong \mathbb{Z}^{(\varnothing)}$. Εάν η $G$ είναι μη τετριμμένη, θεωρούμε τυχόν σύστημα γεννητόρων[68] $X$ τής $G$. Έστω $\delta : X \longrightarrow \mathbb{Z}^{(X)}$ η ένριψη (9.56). Ορίζουμε την απεικόνιση

$$\varphi : \mathrm{Im}(\delta) \longrightarrow G, \ \ \delta_x \longmapsto \varphi(\delta_x) := x, \ \forall x \in X.$$

Επειδή η εικόνα $\mathrm{Im}(\delta)$ τής $\delta$ αποτελεί μια $\mathbb{Z}$-βάση τής $\mathbb{Z}^{(X)}$ (βλ. 9.5.10 (i)), η πρόταση 9.5.29 μας εγγυάται την ύπαρξη ενός και μόνον $f \in \mathrm{Hom}(\mathbb{Z}^{(X)}, G)$, ούτως ώστε να ισχύει $f(\delta_x) = \varphi(\delta_x) := x$, $\forall x \in X$. Έστω τυχόν $g \in G$. Εξ ορισμού, υπάρχουν $\kappa \in \mathbb{N}$ και $n_1, ..., n_\kappa \in \mathbb{Z}$, $x_1, ..., x_\kappa \in X$ με $g = \sum_{j=1}^{\kappa} n_j x_j$. Αυτό σημαίνει ότι

$$f\left(\sum_{j=1}^{\kappa} n_j \delta_{x_j}\right) = \sum_{j=1}^{\kappa} n_j f(\delta_{x_j}) = \sum_{j=1}^{\kappa} n_j \varphi(\delta_{x_j}) = \sum_{j=1}^{\kappa} n_j x_j = g,$$

ήτοι ότι ο $f$ είναι επιμορφισμός. Επομένως, $G \cong \mathbb{Z}^{(X)}/H$, όπου $H := \mathrm{Ker}(f)$. (Βλ. θεώρημα 4.5.2.) □

► **Υποομάδες**. Οι υποομάδες ελεύθερων αβελιανών ομάδων είναι ωσαύτως ελεύθερες και περιγράψιμες (μέχρις ισομορφισμού) μέσω τού θεωρήματος 9.5.39.

**9.5.36 Λήμμα.** *Για κάθε επιμορφισμό $f : G \longrightarrow H$ από μια αβελιανή ομάδα $G$ επί μιας ελεύθερης αβελιανής ομάδας $H$*

$$\exists f' \in \mathrm{Hom}(H, G) : [f \circ f' = \mathrm{id}_H \ \text{ και } \ G = \mathrm{Ker}(f) \oplus_{\text{εσ.}} \mathrm{Im}(f')].$$

[68] Το πλέον προφανές (αλλά κατά κανόνα «ανοικονόμητο») σύστημα γεννητόρων τής $G$ είναι το $X = G$.

ΑΠΟΔΕΙΞΗ. Όταν η $H$ είναι τετριμμένη, ο ισχυρισμός είναι προδήλως αληθής. Έστω ότι $\{0_H\} \sqsubset H$ και ότι $X$ είναι μια $\mathbb{Z}$-βάση τής $H$. Εξ υποθέσεως, για κάθε στοιχείο $x \in X$ υπάρχει κάποιο $g_x \in G$, τέτοιο ώστε να ισχύει $f(g_x) = x$. Θεωρούμε την απεικόνιση

$$\varphi : X \longrightarrow G, \ \ x \longmapsto \varphi(x) := g_x.$$

Δυνάμει τής προτάσεως 9.5.29 υπάρχει ένας (και μόνον) $f' \in \mathrm{Hom}(H, G)$ με την ιδιότητα $f'(x) = \varphi(x) := g_x$, $\forall x \in X$. Προφανώς,

$$[(f \circ f')(x) = f(g_x) = x, \forall x \in X] \Rightarrow f \circ f'\big|_X = \mathrm{id}_X \underset{2.4.9\,\text{(ii)}}{\Longrightarrow} f \circ f' = \mathrm{id}_H.$$

Αυτό σημαίνει ότι ο $f'$ είναι *μονομορφισμός* και η απεικόνιση $\widehat{f'} : H \longrightarrow \mathrm{Im}(f')$ (που προκύπτει ύστερα από περιορισμό τού πεδίου τιμών τού $f'$ στην εικόνα του) είναι *ισομορφισμός*, έχων τον περιορισμό $f|_{\mathrm{Im}(f')} : \mathrm{Im}(f') \xrightarrow{\cong} H$ τού $f$ επί τής $\mathrm{Im}(f')$ ως αντίστροφό του. Από την ενριπτικότητα αυτού τού περιορισμού έπεται, ιδιαιτέρως, ότι

$$\mathrm{Ker}(f) \cap \mathrm{Im}(f') = \mathrm{Ker}(f|_{\mathrm{Im}(f')}) = \{0_G\}. \tag{9.60}$$

Από την άλλη μεριά, για κάθε $g \in G$ ισχύει

$$g = \underbrace{(g - f'(f(g)))}_{\in\, \mathrm{Ker}(f)} + \underbrace{f'(f(g))}_{\in \mathrm{Im}(f')}, \tag{9.61}$$

διότι $f(g - f'(f(g))) = f(g) - (f \circ f')(f(g)) = f(g) - \mathrm{id}_H(f(g)) = f(g) - f(g) = 0_H$. Από τις (9.60) και (9.61) συνάγεται ότι $G = \mathrm{Ker}(f) \oplus_{\text{εσ.}} \mathrm{Im}(f')$. □

**9.5.37 Πρόταση.** *Έστω $(G, +)$ μια αβελιανή ομάδα. Εάν $H$ είναι μια υποομάδα αυτής, τέτοια ώστε η αβελιανή πηλικοομάδα $G/H$ να είναι ελεύθερη, τότε η $H$ διαθέτει κάποιο συμπλήρωμα* (βλ. 7.6.42 (ii)), *ήτοι*

$$\exists K \in \mathbf{Subg}(G) : G = H \oplus_{\text{εσ.}} K.$$

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμοσθεί το λήμμα 9.5.36 για τον φυσικό επιμορφισμό $\pi_H^G : G \longrightarrow G/H$ (με $\mathrm{Ker}(\pi_H^G) = H$) και να τεθεί $K := \mathrm{Im}((\pi_H^G)')$. □

**9.5.38 Παρατήρηση.** Εάν η $G/H$ δεν είναι ελεύθερη, τότε η $H$ ενδέχεται να μην διαθέτει κανένα συμπλήρωμα (ακόμη και όταν η ίδια η $G$ είναι ελεύθερη). Επί παραδείγματι, εάν θεωρήσουμε την υποομάδα $2\mathbb{Z}$ των αρτίων ακεραίων τής ελεύθερης αβελιανής ομάδας $(\mathbb{Z}, +)$ και υποθέσουμε ότι $\exists K \in \mathbf{Subg}(\mathbb{Z}) : \mathbb{Z} = 2\mathbb{Z} \oplus_{\text{εσ.}} K$, θα πρέπει να ισχύει $K \underset{7.1.29}{\cong} \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$, πράγμα αδύνατο (καθόσον κάθε μη τετριμμένη υποομάδα τής $(\mathbb{Z}, +)$ είναι, σύμφωνα με τα προαναφερθέντα στο (i) τής προτάσεως 2.2.19, *άπειρη*).

**9.5.39 Θεώρημα.** *Εάν $(G, +)$ είναι μια ελεύθερη αβελιανή ομάδα, τότε ισχύουν τα εξής:*

(i) *Κάθε $H \in \mathbf{Subg}(G)$ είναι ελεύθερη και* $\mathrm{rank}_{\mathbb{Z}}(H) \leq \mathrm{rank}_{\mathbb{Z}}(G)$.

(ii) *Κάθε ελεύθερη αβελιανή ομάδα $\mathbb{Z}^{(Y)}$ επί ενός συνόλου $Y$ με* $\mathrm{card}(Y) \leq \mathrm{rank}_{\mathbb{Z}}(G)$ *είναι ισόμορφη με μια υποομάδα τής $G$.*

ΑΠΟΔΕΙΞΗ ΤΟΥ (i). *Περίπτωση πρώτη.* Εάν $\mathrm{rank}_{\mathbb{Z}}(G) = 0$, τότε η $G$ είναι τετριμμένη και δεν διαθέτει άλλη υποομάδα πέραν τού εαυτού της.

*Περίπτωση δεύτερη.* Εάν $\mathrm{rank}_{\mathbb{Z}}(G) = r \in \mathbb{N}$, τότε χρησιμοποιούμε μαθηματική επαγωγή ως προς τον $r$. Εάν $r = 1$, τότε $G \cong \mathbb{Z}$ και κάθε $H \in \mathbf{Subg}(G)$ είναι $\cong d\mathbb{Z}$ για κάποιον $d \in \mathbb{N}_0$. (Βλ. 2.2.19 (i).) Επειδή έχουμε $d\mathbb{Z} \cong \mathbb{Z}, \forall d \in \mathbb{N}$ (βλ. το (iii) τού εδ. 2.4.11), κάθε $H \in \mathbf{Subg}(G)$ είναι ελεύθερη βαθμίδας $\mathrm{rank}_{\mathbb{Z}}(H) \in \{0, 1\}$. Έστω τώρα ότι $r \geq 2$ και ότι ο ισχυρισμός είναι αληθής για όλες τις ελεύθερες αβελιανές ομάδες βαθμίδας $\leq r - 1$. Θεωρούμε μια $\mathbb{Z}$-βάση $\{x_1, ..., x_r\}$ τής $G$. Σύμφωνα με το πόρισμα 9.5.15, $G = \langle x_1 \rangle \oplus_{\text{εσ.}} \cdots \oplus_{\text{εσ.}} \langle x_r \rangle$ . Θέτοντας

$$\overline{G} := \langle x_1 \rangle \oplus_{\text{εσ.}} \cdots \oplus_{\text{εσ.}} \langle x_{r-1} \rangle \in \mathbf{Subg}(G)$$

παρατηρούμε ότι η απεικόνιση

$$G \ni \textstyle\sum_{j=1}^{r} n_j x_j \longmapsto n_r x_r \in \langle x_r \rangle$$

($n_1, ..., n_r \in \mathbb{Z}$) είναι επιμορφισμός έχων την $\overline{G}$ ως πυρήνα του. Άρα υφίστανται ισομορφισμοί

$$G/\overline{G} \underset{4.5.2}{\xrightarrow{\cong}} \langle x_r \rangle \quad \text{και} \quad \langle x_r \rangle \xrightarrow{\cong} \mathbb{Z},$$

$$\textstyle\sum_{j=1}^{r} n_j x_j + \overline{G} \longmapsto n_r x_r \quad \text{και} \quad n x_r \longmapsto n.$$

Έστω $H \in \mathbf{Subg}(G)$. Επειδή $\mathrm{rank}_{\mathbb{Z}}(\overline{G}) = r - 1$ και $\overline{H} := \overline{G} \cap H \in \mathbf{Subg}(\overline{G})$, η $\overline{H}$ (σύμφωνα με την επαγωγική υπόθεση) είναι ελεύθερη βαθμίδας $\leq r - 1$. Επιπροσθέτως, ο πυρήνας τού περιορισμού $\pi_{\frac{G}{\overline{G}}}\big|_H : H \longrightarrow G/\overline{G}$ τού φυσικού επιμορφισμού $\pi_{\frac{G}{\overline{G}}} : G \longrightarrow G/\overline{G}$ επί τής $H$ είναι η ομάδα

$$\mathrm{Ker}\left(\pi_{\frac{G}{\overline{G}}}\big|_H\right) = \mathrm{Ker}(\pi_{\frac{G}{\overline{G}}}) \cap H = \overline{G} \cap H = \overline{H},$$

οπότε $H/\overline{H} \underset{4.5.2}{\cong} \mathrm{Im}\left(\pi_{\frac{G}{\overline{G}}}\big|_H\right) \sqsubseteq G/\overline{G} \cong \mathbb{Z}$, όπου η $G/\overline{G}$ είναι ελεύθερη βαθμίδας 1. Κατά συνέπειαν, η πηλικοομάδα $H/\overline{H}$ (ούσα ισόμορφη με κάποια υποομάδα μιας ελεύθερης αβελιανής ομάδας βαθμίδας 1) είναι ελεύθερη έχουσα βαθμίδα είτε 0 είτε 1 και (μέσω τής προτάσεως 9.5.37)

$$\exists K \in \mathbf{Subg}(H) : H = \overline{H} \oplus_{\text{εσ.}} K \underset{7.1.43\,\text{(ii)}}{\cong} \overline{H} \oplus K.$$

Επειδή $K \underset{7.1.29}{\cong} H/\overline{H}$, η $H$ (λόγω τού πορίσματος 9.5.34) είναι ωσαύτως ελεύθερη, έχουσα βαθμίδα $\mathrm{rank}_{\mathbb{Z}}(H) = \mathrm{rank}_{\mathbb{Z}}(\overline{H})+ \mathrm{rank}_{\mathbb{Z}}(K) \leq (r - 1) + 1 = r$. Άρα ο αρχικός ισχυρισμός είναι αληθής *για κάθε* $r \geq 1$.

*Περίπτωση τρίτη.* Υποθέτουμε ότι $\mathrm{rank}_{\mathbb{Z}}(G) \geq \aleph_0$. Εάν $H = \{0_G\}$, τότε η $H$ έχει το $\varnothing$ ως $\mathbb{Z}$-βάση της και είναι ελεύθερη έχουσα βαθμίδα 0. Εάν $\{0_G\} \neq H \sqsubseteq G$, τότε θεωρούμε μια $\mathbb{Z}$-βάση $\{\, x_i |\, i \in I\}$ τής $G$ (με $\mathrm{card}(I) = \mathrm{rank}_{\mathbb{Z}}(G)$) και για κάθε υποσύνολο $J \subseteq I$ θέτουμε $G_J := \langle \{\, x_j |\, j \in J\} \rangle$ και $H_J := G_J \cap H$.

*Ισχυρισμός πρώτος.* Η ακόλουθη οικογένεια τριάδων είναι μη κενή:

$$\mathfrak{N} := \left\{ (J, J', \varphi) \,\middle|\, \begin{array}{l} J' \subseteq J \subseteq I \text{ και } \varphi : J' \longrightarrow H_J \text{ απεικόνιση τέτοια,} \\ \text{ώστε η } \{\varphi(j) | \, j \in J'\} \text{ να είναι μια } \mathbb{Z}\text{-βάση τής } H_J \end{array} \right\}.$$

*Απόδειξη πρώτου ισχυρισμού.* Επειδή $H \neq \{0_G\}$, υπάρχει κάποιο $x \in G \smallsetminus \{0_G\}$. Αυτό γράφεται ως $\mathbb{Z}$-γραμμικός συνδυασμός $x = n_1 x_{j_1} + \cdots + n_\rho x_{j_\rho}$ στοιχείων τής $\{x_i | \, i \in I\}$ (με τουλάχιστον έναν εκ των συντελεστών $\neq 0$). Επομένως, $x \in H_J$, όπου $J := \{j_1, ..., j_\rho\} \subsetneqq I$. Αυτό σημαίνει ότι $H_J \neq \{0_G\}$ και ότι η $G_J$ είναι μια ελεύθερη αβελιανή ομάδα έχουσα βαθμίδα $\text{rank}_{\mathbb{Z}}(G_J) \leq \rho < \infty$. Σύμφωνα με τα προαναφερθέντα στη δεύτερη περίπτωση, η $H_J$ είναι ωσαύτως ελεύθερη αβελιανή ομάδα έχουσα βαθμίδα

$$1 \leq \text{rank}_{\mathbb{Z}}(H_J) =: l \leq \text{rank}_{\mathbb{Z}}(G_J) \leq \rho < \infty.$$

Έστω $\{y_1, ..., y_l\}$ μια $\mathbb{Z}$-βάση τής $H_J$. Θέτοντας $J' := \{j_1, ..., j_l\} \subseteq J$ και

$$\varphi : J' \longrightarrow H_J, \;\; j_\xi \longmapsto \varphi(j_\xi) := y_\xi, \; \forall \xi \in \{1, ..., l\},$$

παρατηρούμε ότι η (συγκεκριμένη) τριάδα $(J, J', \varphi)$ ανήκει στην $\mathfrak{N}$.

*Εφαρμογή τού λήμματος τού Zorn.* Η οικογένεια $\mathfrak{N} \neq \varnothing$ καθίσταται μερικώς διατεταγμένο σύνολο ως προς την ακόλουθη "$\preceq$":

$$(J, J', \varphi) \preceq (L, L', \theta) \underset{\text{ορσ}}{\Longleftrightarrow} [J \subseteq L, \; J' \subseteq L' \text{ και } \; \theta|_{J'} = \varphi].$$

Για κάθε αλυσίδα $(J_\lambda, J'_\lambda, \varphi_\lambda)_{\lambda \in \Lambda}$ τού $(\mathfrak{N}, \preceq)$ η τριάδα $\left(\bigcup_{\lambda \in \Lambda} J_\lambda, \bigcup_{\lambda \in \Lambda} J'_\lambda, \Phi\right)$ με $\Phi|_{J'_\lambda} = \varphi_\lambda$ είναι ένα άνω φράγμα αυτής, οπότε το $(\mathfrak{N}, \preceq)$ είναι επαγωγικώς διατεταγμένο. Δυνάμει τού λήμματος A.2.20 τού Zorn το $(\mathfrak{N}, \preceq)$ διαθέτει κάποιο μεγιστικό στοιχείο $(J_\bullet, J'_\bullet, \varphi_\bullet)$.

*Ισχυρισμός δεύτερος.* $J_\bullet = I$.

*Απόδειξη δεύτερου ισχυρισμού.* Ας υποθέσουμε ότι $J_\bullet \subsetneqq I$, ας επιλέξουμε ένα $i_\bullet \in I \smallsetminus J_\bullet$ και ας θέσουμε $L_\bullet := J_\bullet \cup \{i_\bullet\}$. Εάν $H_{J_\bullet} = H_{L_\bullet}$, τότε ισχύει $(J_\bullet, J'_\bullet, \varphi_\bullet) \underset{\neq}{\preceq} (L_\bullet, J'_\bullet, \varphi_\bullet)$, κάτι που αντίκειται στη μεγιστικότητα τής τριάδας $(J_\bullet, J'_\bullet, \varphi_\bullet)$ εντός τής $\mathfrak{N}$. Άρα $H_{J_\bullet} \sqsubset H_{L_\bullet}$ και

$$H_{L_\bullet} / (H_{L_\bullet} \cap G_{J_\bullet}) \cong (H_{L_\bullet} + G_{J_\bullet}) / G_{J_\bullet} \sqsubseteq G_{L_\bullet} / G_{J_\bullet} = \langle x_{i_\bullet} + G_{J_\bullet} \rangle .$$

Η πηλικοομάδα $(H_{L_\bullet} + G_{J_\bullet})/G_{J_\bullet}$ (ως μη τετριμμένη υποομάδα μιας ελεύθερης αβελιανής ομάδας βαθμίδας 1) είναι ελεύθερη κυκλική έχουσα το μονοσύνολο $\{dx_{i_\bullet} + G_{J_\bullet}\}$ (για κάποιον $d \in \mathbb{N}$) ως μια $\mathbb{Z}$-βάση της. Επιλέγοντας ένα $z \in H_{L_\bullet}$, τέτοιο ώστε $z = dx_{i_\bullet} + w$ για κάποιο $w \in G_{J_\bullet}$, λαμβάνουμε

$$(H_{L_\bullet} + G_{J_\bullet})/G_{J_\bullet} = \langle z + G_{J_\bullet} \rangle .$$

Εν συνεχεία, θέτοντας $L'_\bullet := J'_\bullet \cup \{i_\bullet\}$ και ορίζοντας την απεικόνιση

$$\theta_\bullet : L'_\bullet \longrightarrow H_{L_\bullet}, \;\; j \longmapsto \theta_\bullet(j) := \begin{cases} \varphi_\bullet(j), & \text{όταν } j \in J'_\bullet, \\ z, & \text{όταν } j = i_\bullet, \end{cases}$$

παρατηρούμε ότι για κάθε $x \in H_{L_\bullet}$ ισχύει $x + G_{J_\bullet} = cz + G_{J_\bullet}$ για κάποιον $c \in \mathbb{Z}$, οπότε

$$\left.\begin{array}{l} x - cz \in G_{J_\bullet} \cap H =: H_{J_\bullet} \\ \langle \{ \varphi_\bullet(j) |\, j \in J'_\bullet \} \rangle = H_{J_\bullet} \end{array}\right\} \Rightarrow x - cz = m_1\varphi_\bullet(j_1) + \cdots + m_\kappa\varphi_\bullet(j_\kappa),$$

για κάποιους $m_1, ..., m_\kappa \in \mathbb{Z}$ και $\{j_1, ..., j_\kappa\} \subseteq J'_\bullet$. Επομένως,

$$x = c\theta_\bullet(i_\bullet) + m_1\theta_\bullet(j_1) + \cdots + m_\kappa\theta_\bullet(j_\kappa) \Rightarrow \langle \{ \theta_\bullet(j) |\, j \in L'_\bullet \} \rangle = H_{L_\bullet}.$$

Από την άλλη μεριά, από κάθε σχέση τής μορφής

$$m_0 \underbrace{\theta_\bullet(i_\bullet)}_{=z} + m_1\theta_\bullet(j_1) + \cdots + m_\nu\theta_\bullet(j_\nu) = 0_G \tag{9.62}$$

(για κάποιους $m_0, m_1, ..., m_\nu \in \mathbb{Z}$ και $\{i_\bullet, j_1, ..., j_\nu\} \subseteq L'_\bullet$) προκύπτει ότι

$$dm_0x_{i_\bullet} = -(m_0w + m_1\theta_\bullet(j_1) + \cdots + m_\nu\theta_\bullet(j_\nu)) \Rightarrow dm_0x_{i_\bullet} \in G_{J_\bullet} \cap \langle x_{i_\bullet} \rangle = \{0_G\}.$$

Επειδή το $\{ x_i |\, i \in I \}$ είναι $\mathbb{Z}$-βάση τής $G$, έχουμε

$$dm_0x_{i_\bullet} = 0_G \Rightarrow dm_0 = 0 \underset{d\neq 0}{\Longrightarrow} m_0 = 0,$$

οπότε

$$\left.\begin{array}{r} m_1\varphi_\bullet(j_1) + \cdots + m_\nu\varphi_\bullet(j_\nu) = 0_G \\ \text{και το } \{ \varphi_\bullet(j) |\, j \in J'_\bullet \} \text{ είναι } \mathbb{Z}\text{-βάση τής } H_{J_\bullet} \end{array}\right\} \Rightarrow m_1 = \cdots = m_\nu = 0. \tag{9.63}$$

Από τις (9.62) και (9.63) συνάγεται ότι το $\{ \theta_\bullet(j) |\, j \in L'_\bullet \}$ αποτελεί μια $\mathbb{Z}$-βάση τής $H_{L_\bullet}$. Αυτό σημαίνει ότι $(J_\bullet, J'_\bullet, \varphi_\bullet) \underset{\neq}{\preceq} (L_\bullet, L'_\bullet, \theta_\bullet)$, κάτι που αντίκειται εκ νέου στη μεγιστικότητα τής τριάδας $(J_\bullet, J'_\bullet, \varphi_\bullet)$ εντός τής $\mathfrak{N}$. Άτοπο!

*Αποπεράτωση αποδείξεως.* Επειδή $J_\bullet = I$, έχουμε $G_{J_\bullet} = G$, $H_{J_\bullet} = H$ και το $\{ \varphi_\bullet(j) |\, j \in J' \}$ αποτελεί μια $\mathbb{Z}$-βάση τής $H$. Άρα η $H$ είναι ελεύθερη αβελιανή ομάδα και $\text{rank}_\mathbb{Z}(H) = \text{card}(J') \leq \text{card}(I) = \text{rank}_\mathbb{Z}(G)$.

ΑΠΟΔΕΙΞΗ ΤΟΥ (ii). Έστω $Y$ ένα σύνολο με $\text{card}(Y) \leq \text{rank}_\mathbb{Z}(G)$ και έστω $X$ τυχούσα $\mathbb{Z}$-βάση τής $G$. Επειδή $G \cong \mathbb{Z}^{(X)}$, έχουμε

$$\text{card}(Y) \leq \text{rank}_\mathbb{Z}(G) = \text{card}(X),$$

οπότε υφίσταται κάποια ένριψη $\varphi : Y \longrightarrow X$. Σύμφωνα με το (ii) τού πορίσματος 9.5.30 ο επαγόμενος ομομορφισμός $f : \mathbb{Z}^{(Y)} \longrightarrow \mathbb{Z}^{(X)}$ είναι μονομορφισμός, οπότε $\mathbb{Z}^{(Y)} \cong f(\mathbb{Z}^{(Y)}) \sqsubseteq \mathbb{Z}^{(X)} \cong G$. □

**9.5.40 Παρατήρηση.** Εάν $\text{rank}_\mathbb{Z}(G) \in \mathbb{N}$ και $\text{rank}_\mathbb{Z}(H) = \text{rank}_\mathbb{Z}(G)$ για κάποια $H \in \mathbf{Subg}(G)$, τότε δεν είναι απαραίτητο[69] να έχουμε $H = G$ (παρά το γεγονός ότι $H \underset{9.5.31}{\cong} G$). Επί παραδείγματι, $2\mathbb{Z} \sqsubset \mathbb{Z}$ με $2\mathbb{Z} \cong \mathbb{Z}$ και $\text{rank}_\mathbb{Z}(2\mathbb{Z}) = \text{rank}_\mathbb{Z}(\mathbb{Z}) = 1$.

[69] Αντιθέτως, εάν $V$ είναι ένας διανυσματικός χώρος *πεπερασμένης διαστάσεως* (ορισμένος υπεράνω ενός σώματος $F$) και $U$ ένας γραμμικός υπόχωρος αυτού, τέτοιος ώστε να ισχύει $\dim_F(U) = \dim_F(V)$, τότε $U = V$.

► «**Ελεύθερη = προβολική**». Μια ενδιαφέρουσα ικανή και αναγκαία συνθήκη για να είναι μια αβελιανή ομάδα ελεύθερη δίδεται στο θεώρημα 9.5.42.

**9.5.41 Ορισμός.** Λέμε ότι μια αβελιανή ομάδα $G$ είναι **προβολική** όταν για κάθε επιμορφισμό αβελιανών ομάδων $\beta : H \longrightarrow K$ και κάθε $\theta \in \mathrm{Hom}(G,K)$ υπάρχει $f \in \mathrm{Hom}(G,H)$ που καθιστά το ακόλουθο διάγραμμα μεταθετικό.

$$\begin{tikzcd} & G \arrow[dl, dashed, "f"'] \arrow[dr, "\theta"] \arrow[d, phantom, "\circlearrowleft"] & \\ H \arrow[rr, "\beta"'] & & K \end{tikzcd}$$

**9.5.42 Θεώρημα. (S. Mac Lane,** 1950.**)** *Μια αβελιανή ομάδα είναι ελεύθερη εάν και μόνον είναι προβολική.*

Απόδειξη[70]. Ας υποθέσουμε ότι $(G,+)$ είναι μια ελεύθερη αβελιανή ομάδα, $\beta : H \longrightarrow K$ ένας επιμορφισμός αβελιανών ομάδων και $\theta \in \mathrm{Hom}(G,K)$. Εάν η $G$ είναι τετριμμένη και $f : G \to H$ η $f(0_G) := 0_H$, τότε προφανώς $\beta \circ f = \theta$. Στην περίπτωση όπου η $G$ είναι μη τετριμμένη, θεωρούμε μια $\mathbb{Z}$-βάση της $X$, τη συνήθη ένθεση $\iota : X \hookrightarrow G$ και την απεικόνιση $\varphi : X \longrightarrow H$ την οριζόμενη ως ακολούθως: Εάν $x \in X$, τότε $\theta(x) \in K$ και, επειδή ο $\beta$ είναι επιμορφισμός, $\exists y \in H : \beta(y) = \theta(x)$. Θέτουμε $\varphi(x) := y$. Κατά την πρόταση 9.5.29 υπάρχει ένας (και μόνον) ομομορφισμός $f \in \mathrm{Hom}(G,H)$ με $f \circ \iota = \varphi$. Έστω $z$ τυχόν στοιχείο τής $G$. Επειδή το $X$ είναι $\mathbb{Z}$-βάση τής $G$, το $z$ παριστάται (μονοσημάντως) ως $\mathbb{Z}$-γραμμικός συνδυασμός

$$z = \sum_{j=1}^{\kappa} n_j x_j = \sum_{j=1}^{\kappa} n_j \iota(x_j) \ \ (\kappa \in \mathbb{N},\ n_1,...,n_\kappa \in \mathbb{Z},\ \{x_1,...,x_\kappa\} \subseteq X),$$

οπότε

$$\begin{aligned}(\beta \circ f)(z) &= \beta(f(z)) = \sum_{j=1}^{\kappa} n_j \beta(f(\iota(x_j))) = \sum_{j=1}^{\kappa} n_j \beta(\varphi(x_j)) \\ &= \sum_{j=1}^{\kappa} n_j \theta(x_j) = \theta\left(\sum_{j=1}^{\kappa} n_j x_j\right) = \theta(z).\end{aligned}$$

Κατά συνέπειαν, $\beta \circ f = \theta$ και η $G$ είναι προβολική.

Και αντιστρόφως· εάν υποθέσουμε ότι $(G,+)$ είναι μια προβολική αβελιανή ομάδα, τότε, σύμφωνα με τα προαναφερθέντα στην απόδειξη τού θεωρήματος 9.5.35, για κάθε σύστημα γεννητόρων $X$ κατασκευάζεται επιμορφισμός $\beta : \mathbb{Z}^{(X)} \longrightarrow G$, οπότε υπάρχει $f \in \mathrm{Hom}(G, \mathbb{Z}^{(X)})$ που καθιστά το ακόλουθο διάγραμμα μεταθετικό.

$$\begin{tikzcd} & G \arrow[dl, dashed, "f"'] \arrow[dr, "\mathrm{id}_G"] \arrow[d, phantom, "\circlearrowleft"] & \\ \mathbb{Z}^{(X)} \arrow[rr, "\beta"'] & & G \end{tikzcd}$$

[70]Βλ. S. Mac Lane: *Duality for groups*, Bulletin of American Math. Soc. **56** (1950), 485-516.

Από την ισότητα $\beta\circ f = \mathrm{id}_G$ έπεται ότι ο $f$ είναι μονομορφισμός και, κατ' επέκταση, ότι $\mathrm{Ker}(f) = \{0_G\} \underset{4.5.2}{\Longrightarrow} G \cong \mathrm{Im}(f) \sqsubseteq \mathbb{Z}^{(X)}$. Επειδή η $\mathbb{Z}^{(X)}$ είναι ελεύθερη, *και* η $\mathrm{Im}(f) \cong G$ οφείλει να είναι ελεύθερη λόγω τού (i) τού θεωρήματος 9.5.39. □

► **«Άστρεπτη βαθμίδα» και το θεώρημα τού Pontryagin**. Γενικεύοντας καταλλήλως την έννοια τής βαθμίδας για τις (όχι κατ' ανάγκην ελεύθερες) αβελιανές ομάδες χωρίς στρέψη έχουμε τη δυνατότητα να διατυπώσουμε και να αποδείξουμε το θεώρημα 9.5.53 τού Pontryagin, μέσω τού οποίου δίδεται ένα εύληπτο «κριτήριο ελευθερίας» *αριθμήσιμων* αβελιανών ομάδων χωρίς στρέψη.

**9.5.43 Λήμμα.** *Έστω $(G,+)$ μια αβελιανή ομάδα στερούμενη στρέψεως και έστω $X = (x_i)_{i\in I} \subseteq G$ (με $I \neq \varnothing$). Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*[71]:

(i) *Το $X$ είναι $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο.*

(ii) $\langle X\rangle = \bigoplus_{i\in I}^{\text{εσ.}} \langle x_i\rangle$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν $i \in I$ και $g \in \langle x_i\rangle \cap \langle\{\langle x_j\rangle | j \in I\smallsetminus\{i\}\}\rangle$, τότε υπάρχει $n_i \in \mathbb{Z} : g = n_i x_i$ και υπάρχει κάποιο πεπερασμένο υποσύνολο $\{j_1,...,j_\kappa\}$ τού $I\smallsetminus\{i\}$ και $n_{j_1},...,n_{j_\kappa} \in \mathbb{Z}$, ούτως ώστε να ισχύει $g = \sum_{l=1}^{\kappa} n_{j_l} x_{j_l}$. Επομένως, λόγω τής προϋποτιθέμενης $\mathbb{Z}$-γραμμικής ανεξαρτησίας τού $X$ έχουμε

$$n_i x_i + \sum_{l=1}^{\kappa}(-n_{j_l})x_{j_l} = 0_G \Rightarrow n_i = n_{j_1} = \cdots = n_{j_\kappa} = 0 \Rightarrow g = 0_G,$$

οπότε $\langle X\rangle = \bigoplus_{i\in I}^{\text{εσ.}} \langle x_i\rangle$. (Βλ. 7.1.97.)

(ii)⇒(i) Εάν, αντιστρόφως, $\langle X\rangle = \bigoplus_{i\in I}^{\text{εσ.}} \langle x_i\rangle$, τότε το $0_G \in \langle X\rangle$ γράφεται μονοσημάντως (μέχρις αναδιατάξεως των δεικτών) υπό τη μορφή

$$0_G = n_{j_1}x_{j_1} + \cdots + n_{j_k}x_{j_k} \quad (n_{j_1},...,n_{j_k} \in \mathbb{Z})$$

για κάποιον $k \in \mathbb{N}$, όπου οι δείκτες $j_1,...,j_k \in I$ είναι σαφώς διακεκριμένοι. (Βλ. 7.1.98 (iii).) Επειδή $0_G = \underbrace{0_G + \cdots + 0_G}_{k \text{ φορές}}$, λαμβάνουμε

$$\left.\begin{array}{l} n_{j_1}x_{j_1} = \cdots = n_{j_k}x_{j_k} = 0_G \\ x_{j_1} \neq 0_G,...,x_{j_k} \neq 0_G \\ \mathrm{tors}(G) = \{0_G\} \end{array}\right\} \Rightarrow n_{j_1} = \cdots = n_{j_k} = 0,$$

οπότε το $X$ είναι όντως $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο τής $G$. □

**9.5.44 Λήμμα.** *Έστω $(G,+)$ μια αβελιανή ομάδα στερούμενη στρέψεως. Εάν αυτή διαθέτει ένα πεπερασμένο μεγιστικό $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο $X$, τότε* $\mathrm{card}(Y) \leq \mathrm{card}(X)$ *για οιοδήποτε $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολό της $Y$.*

[71] Η προϋπόθεση "$\mathrm{tors}(G) = \{0_G\}$" απαιτείται μόνον για την απόδειξη τής συνεπαγωγής "(ii)⇒(i)".

ΑΠΟΔΕΙΞΗ. Έστω ότι $X = \{x_1, ..., x_\kappa\}$ και ότι $Y = (y_i)_{i \in I}$ είναι ένα $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο τής $G$ (με $\mathrm{card}(Y) = \mathrm{card}(I)$). Θεωρούμε τυχόν $i \in I$. Λόγω τής $\mathbb{Z}$-γραμμικής ανεξαρτησίας τού $Y$ έχουμε $y_i \neq 0_G$. Εάν το $y_i$ δεν ανήκει στο $X$, τότε το $X \cup \{y_i\}$ είναι $\mathbb{Z}$-γραμμικώς εξαρτημένο, οπότε

$$l_i y_i + \sum_{j=1}^{\kappa} n_j x_j = 0_G \Rightarrow l_i y_i = \sum_{j=1}^{\kappa} (-n_j)\, x_j \in \langle X \rangle\,,$$

για κάποιους $l_i, n_1, ...., n_k \in \mathbb{Z}$, με τουλάχιστον έναν εξ αυτών $\neq 0$. Μεταξύ εκείνων των συντελεστών που είναι $\neq 0$ συγκαταλέγεται[72] ο $l_i$. Θέτοντας λοιπόν

$$\ell_i := \begin{cases} 1, & \text{όταν } y_i \in X, \\ \\ l_i, & \text{όταν } y_i \notin X, \end{cases}$$

λαμβάνουμε $\ell_i y_i \in \langle X \rangle$ με $\ell_i y_i \neq 0_G$ (αφού $\mathrm{tors}(G) = \{0_G\}$) για κάθε $i \in I$. Το $\{\, \ell_i y_i |\, i \in I\}$ είναι $\mathbb{Z}$-γραμμικώς ανεξάρτητο[73], οπότε

$$\bigoplus_{i \in I}^{\text{εσ.}} \langle \ell y_i \rangle = \langle \{\, \ell_i y_i |\, i \in I\} \rangle \sqsubseteq \langle X \rangle = \bigoplus_{1 \leq j \leq \kappa}^{\text{εσ.}} \langle x_j \rangle\,.$$

(Βλ. λήμμα 9.5.43.) Καθένα εκ των $\ell_i y_i, i \in I, x_1, ..., x_\kappa$ (ως μη μηδενικό στοιχείο μιας αβελιανής ομάδας χωρίς στρέψη) έχει άπειρη τάξη, οπότε παράγει μια άπειρη κυκλική ομάδα ($\cong \mathbb{Z}$). Κατά συνέπειαν, η ελεύθερη ομάδα[74] $\langle X \rangle \cong \mathbb{Z}^\kappa$ έχει την $\langle \{\, \ell_i y_i |\, i \in I\} \rangle \cong \mathbb{Z}^{\mathrm{card}(I)}$ ως υποομάδα της, απ' όπου έπεται ότι $\mathrm{card}(I) \leq \kappa$. (Βλ. το (i) τού θεωρήματος 9.5.39.) □

Για την εξέταση τού τι συμβαίνει στην περίπτωση κατά την οποία το μεγιστικό $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο αναφοράς μας είναι *άπειρο*, προτάσσουμε δύο στοιχειώδη λήμματα από τη Θεωρία Συνόλων.

**9.5.45 Λήμμα.** *Εάν το $A$ είναι ένα απειροσύνολο, τότε* $\mathrm{card}(A \times A) = \mathrm{card}(A)$ *και, γενικότερα,* $\mathrm{card}(A^n) = \mathrm{card}(A)$ *για κάθε* $n \in \mathbb{N}$.

**9.5.46 Λήμμα.** *Εάν τα $A, B$ είναι δυο απειροσύνολα, τότε*

$$(\mathrm{card}(A)\,\mathrm{card}(B) :=)\,\mathrm{card}(A \times B) = \max\{\mathrm{card}(A), \mathrm{card}(B)\}.$$

ΑΠΟΔΕΙΞΗ. Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι ισχύει[75] $\mathrm{card}(A) \leq \mathrm{card}(B)$. Προφανώς,

$$\mathrm{card}(B) \leq \mathrm{card}(A \times B) \leq \mathrm{card}(B \times B) \underset{9.5.45}{=} \mathrm{card}(B).$$

[72]Εάν $l_i = 0$, τότε θα έπρεπε να ισχύει $n_1 = \cdots = n_\kappa = 0$ λόγω τής $\mathbb{Z}$-γραμμικής ανεξαρτησίας τού $X$.

[73]Πράγματι· για οιοδήποτε πεπερασμένο σύνολο δεικτών $\{i_1, ..., i_m\} \subseteq I$ και $r_1, ..., r_m \in \mathbb{Z}$ για τους οποίους ισχύει $\sum_{\nu=1}^{m} r_\nu \ell_{i_\nu} y_{i_\nu} = 0_G$ λαμβάνουμε $r_1 \ell_{i_1} = \cdots = r_m \ell_{i_m} = 0$ (λόγω τής $\mathbb{Z}$-γραμμικής ανεξαρτησίας τού $Y$) και, κατ' επέκταση, $r_1 = \cdots = r_m = 0$, διότι $\ell_{i_\nu} \neq 0, \forall \nu \in \{1, ..., m\}$.

[74]Η ομάδα $\langle X \rangle$ είναι ελεύθερη, διότι διαθέτει το $X$ ως μια $\mathbb{Z}$-βάση της. (Βλ. θεώρημα 9.5.13.)

[75]Για *τυχόντα* σύνολα $A, B$ ισχύει είτε $\mathrm{card}(A) \leq \mathrm{card}(B)$ είτε $\mathrm{card}(B) \leq \mathrm{card}(A)$. (Τούτο αποδεικνύεται στη Θεωρία Συνόλων με τη βοήθεια τού λήμματος Α.2.20 τού Zorn.)

Μέσω αυτών καταλήγουμε στην ισότητα $\text{card}(A \times B) = \text{card}(B)$ (δυνάμει τού θεωρήματος των Schröder και Bernstein[76]). □

**9.5.47 Λήμμα.** *Έστω* $(G, +)$ *μια αβελιανή ομάδα στερούμενη στρέψεως. Εάν αυτή διαθέτει ένα άπειρο μεγιστικό* $\mathbb{Z}$*-γραμμικώς ανεξάρτητο υποσύνολο* $X$*, τότε ισχύει η ισότητα* $\text{card}(X) = |G|$.

ΑΠΟΔΕΙΞΗ. Εάν $X = (x_i)_{i \in I} \subseteq G$ είναι ένα άπειρο μεγιστικό $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο (με $\text{card}(X) = \text{card}(I)$), τότε για κάθε $g \in G \smallsetminus \{0_G\}$ υπάρχουν $n(g), n_1(g), ..., n_\kappa(g) \in \mathbb{Z} \smallsetminus \{0\}$ και δείκτες $i_1(g), ..., i_\kappa(g) \in I$ (για κάποιον $\kappa \in \mathbb{N}$), ούτως ώστε να ισχύει

$$0_G \neq n(g)g = n_1(g)x_{i_1(g)} + \cdots + n_\kappa(g)x_{i_\kappa(g)}. \tag{9.64}$$

Πράγματι· εάν $g = x_j \in X$ (για κάποιο $j \in I$), τότε αρκεί να θέσουμε $n(g) := 1$, $\kappa := 1$, $n_1(g) := 1$ και $i_1 := j$. Εάν $g \notin X$, τότε το $X \cup \{g\}$ είναι $\mathbb{Z}$-γραμμικώς εξαρτημένο, οπότε υπάρχει κάποιος $\mathbb{Z}$-γραμμικός συνδυασμός τού $g$ και των στοιχείων κάποιου πεπερασμένου υποσυνόλου $X'$ τού $X$ που ισούται με το $0_G$, με τουλάχιστον έναν εκ των συντελεστών $\neq 0$. Μεταξύ εκείνων των συντελεστών που είναι $\neq 0$ συγκαταλέγεται (λόγω τής $\mathbb{Z}$-γραμμικής ανεξαρτησίας τού $X$) ο συντελεστής τού $g$ (τον οποίο καλούμε $n(g)$). Επειδή $\text{tors}(G) = \{0_G\} \Rightarrow n(g)g \neq 0_G$, τουλάχιστον ένας εκ των συντελεστών των στοιχείων τού $X'$ οφείλει να είναι $\neq 0$. Εάν κρατήσουμε μόνον εκείνα τα στοιχεία τού $X'$ που εμφανίζονται με συντελεστές $\neq 0$ (καλώντας τα $x_{i_1(g)}, ..., x_{i_\kappa(g)}$) καταλήγουμε στην (9.64). Εν συνεχεία, παρατηρούμε ότι για κάθε $\kappa \in \mathbb{N}$ το σύνολο $\mathcal{A}_\kappa := \{\kappa\} \times (\mathbb{Z} \smallsetminus \{0\})^{\kappa+1} \times I^\kappa$ έχει πληθικό αριθμό

$$\begin{aligned} \text{card}(\mathcal{A}_\kappa) &= \text{card}((\mathbb{Z} \smallsetminus \{0\})^{\kappa+1})\, \text{card}(I^\kappa) \\ &\underset{9.5.45}{=} \text{card}(\mathbb{Z} \smallsetminus \{0\})\, \text{card}(I) = \aleph_0\, \text{card}(I) \underset{9.5.46}{=} \text{card}(I), \end{aligned}$$

διότι (εξ υποθέσεως) $\text{card}(I) \geq \aleph_0$. Μέσω των συντελεστών και των δεικτών των εμφανιζομένων στην (9.64) κατασκευάζεται η απεικόνιση

$$f : G \smallsetminus \{0_G\} \longrightarrow \bigcup_{\kappa \in \mathbb{N}} \mathcal{A}_\kappa \left( = \coprod_{\kappa \in \mathbb{N}} \mathcal{A}_\kappa \right),$$

$$g \longmapsto f(g) := (\kappa, (n(g), n_1(g), ..., n_\kappa(g)), (i_1(g), ..., i_\kappa(g))) \in \mathcal{A}_\kappa.$$

Αυτή είναι *ενριπτική*, διότι εάν ισχύει $f(g) = f(g')$, τότε $n(g) = n(g')$ και

$$\left. \begin{array}{l} n(g)(g - g') = 0_G \\ \text{tors}(G) = \{0_G\} \end{array} \right\} \Rightarrow g = g'.$$

[76]**Θεώρημα των Schröder και Bernstein**: Για *τυχόντα* σύνολα $A$, $B$ ισχύει η ακόλουθη συνεπαγωγή:

$$[\text{card}(A) \leq \text{card}(B) \;\text{ και }\; \text{card}(B) \leq \text{card}(A)] \Longrightarrow \text{card}(A) = \text{card}(B).$$

Κατά συνέπειαν,

$$|G| = \mathrm{card}(G\diagdown\{0_G\}) \leq \aleph_0 \ (\aleph_0\, \mathrm{card}(I)) = \aleph_0\, \mathrm{card}(I) = \mathrm{card}(I).$$

Από την άλλη μεριά, είναι προφανές ότι $\mathrm{card}(I) \leq |G|$ . Άρα $\mathrm{card}(I) = |G|$ (δυνάμει τού θεωρήματος των Schröder και Bernstein). □

**9.5.48 Πρόταση.** *Εάν $(G,+)$ είναι μια αβελιανή ομάδα στερούμενη στρέψεως, τότε όλα τα μεγιστικά $\mathbb{Z}$-γραμμικώς ανεξάρτητα υποσύνολά της είναι ισοπληθή.*

Απόδειξη. Την *ύπαρξη* μεγιστικών $\mathbb{Z}$-γραμμικώς ανεξαρτήτων υποσυνόλων τής $G$ την εγγυάται η πρόταση 9.5.4. Ας υποθέσουμε ότι η $G$ είναι μη τετριμμένη[77] και ότι $X, Y$ είναι δυο μεγιστικά $\mathbb{Z}$-γραμμικώς ανεξάρτητα υποσύνολά της.

*Περίπτωση πρώτη.* Εάν το $X$ είναι *πεπερασμένο*, τότε το λήμμα 9.5.44 μας πληροφορεί ότι το $Y$ οφείλει να είναι ωσαύτως πεπερασμένο με $\mathrm{card}(Y) \leq \mathrm{card}(X)$. Λόγω τής μεγιστικότητας τού $Y$ έχουμε το δικαίωμα εναλλαγής των ρόλων των $X$ και $Y$. Επομένως, $\mathrm{card}(X) \leq \mathrm{card}(Y)$. Από το θεώρημα των Schröder και Bernstein έπεται ότι $\mathrm{card}(X) = \mathrm{card}(Y)$.

*Περίπτωση δεύτερη.* Εάν το $X$ είναι *άπειρο*, τότε το $Y$ οφείλει να είναι ωσαύτως άπειρο[78], οπότε $\mathrm{card}(X) = |G| = \mathrm{card}(Y)$ δυνάμει τού λήμματος 9.5.47. □

**9.5.49 Ορισμός.** (i) Ο πληθικός αριθμός οιουδήποτε μεγιστικού $\mathbb{Z}$-γραμμικώς ανεξαρτήτου υποσυνόλου μιας αβελιανής ομάδας $(G,+)$ στερούμενης στρέψεως καλείται **άστρεπτη βαθμίδα** τής $G$ και συμβολίζεται ως $\text{tf-rank}_{\mathbb{Z}}(G)$.

(ii) Γενικότερα, για *τυχούσα* αβελιανή ομάδα $(G,+)$ η **άστρεπτη βαθμίδα** ορίζεται ως εξής: $\text{tf-rank}_{\mathbb{Z}}(G) := \text{tf-rank}_{\mathbb{Z}}(G/\mathrm{tors}(G))$.

**9.5.50 Παρατήρηση.** Τα κάτωθι είναι άμεσα επακόλουθα τού ορισμού 9.5.49.

(i) $\text{tf-rank}_{\mathbb{Z}}(H) \leq \text{tf-rank}_{\mathbb{Z}}(G),\ \forall H \in \mathbf{Subg}(G)$.

(ii) Εάν η $G$ είναι ελεύθερη, τότε $\text{tf-rank}_{\mathbb{Z}}(G) = \mathrm{rank}_{\mathbb{Z}}(G)$.

(iii) $\text{tf-rank}_{\mathbb{Z}}(G) = 0 \Leftrightarrow$ η $G$ είναι[79] ομάδα στρέψεως.

**9.5.51 Παράδειγμα.** Εάν $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in \mathbb{Q}$ $(a_1, a_2 \in \mathbb{Z},\ b_1, b_2 \in \mathbb{Z}\diagdown\{0\})$, τότε

$$a_2 b_1 \left(\frac{a_1}{b_1}\right) + (-a_1 b_2)\left(\frac{a_2}{b_2}\right) = 0,$$

οπότε η (μη ελεύθερη) $(\mathbb{Q},+)$ έχει άστρεπτη βαθμίδα $\text{tf-rank}_{\mathbb{Z}}(\mathbb{Q}) = 1$.

**9.5.52 Λήμμα.** *Έστω $(G,+)$ μια αβελιανή ομάδα. Εάν $H \sqsubseteq G$, τότε*

$$\text{tf-rank}_{\mathbb{Z}}(G) = \text{tf-rank}_{\mathbb{Z}}(G/H) + \text{tf-rank}_{\mathbb{Z}}(H).$$

[77] Εάν η $G$ είναι τετριμμένη, τότε το μόνο $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολό της είναι το κενό.

[78] Εάν το $Y$ ήταν πεπερασμένο, τότε και το $X$ θα ήταν πεπερασμένο (καθώς θα εμπίπταμε στην πρώτη περίπτωση).

[79] Ιδιαιτέρως, εάν η $G$ στερείται στρέψεως, τότε $\text{tf-rank}_{\mathbb{Z}}(G) = 0 \Leftrightarrow$ η $G$ είναι τετριμμένη.

ΑΠΟΔΕΙΞΗ. Αφήνεται ως άσκηση. □

**9.5.53 Θεώρημα. (L.S. Pontryagin,** 1934.) *Έστω* $(G,+)$ *μια αβελιανή ομάδα στερούμενη στρέψεως. Εάν* $|G| = \aleph_0$, *τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*[80]:

(i) *Η* $G$ *είναι ελεύθερη.*

(ii) *Κάθε υποομάδα τής* $G$ *έχουσα πεπερασμένη άστρεπτη βαθμίδα είναι ελεύθερη.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Τούτο είναι προφανές λόγω τού 9.5.39 (i).

(ii)⇒(i) Προφανώς, $\text{tf-rank}_{\mathbb{Z}}(G) \leq |G| = \aleph_0$. Εάν η άστρεπτη βαθμίδα τής $G$ είναι πεπερασμένη, τότε η $G$ είναι (εκ τής υποθέσεώς μας) ελεύθερη. Γι' αυτόν τον λόγο *θα υποθέσουμε* (*από εδώ και στο εξής*) ότι $\text{tf-rank}_{\mathbb{Z}}(G) = \aleph_0$. Έστω $\{g_1, g_2, ..., g_k, g_{k+1}, ...\}$ ένα (κατ' ανάγκην *αριθμήσιμο*) μεγιστικό $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο τής $G$. Θέτουμε $G_0 := \{0_G\}$ και

$$G_k := \{x \in G |\, \exists m \in \mathbb{N} : mx \in \langle g_1, ..., g_k\rangle\},\ \forall k \in \mathbb{N}.$$

Είναι άμεσος ο έλεγχος τού ότι $G_k \sqsubset G_{k+1}$ για κάθε $k \in \mathbb{N}_0$, καθώς και τού ότι $G = \bigcup_{k\in\mathbb{N}_0} G_k$ (λόγω τής μεγιστικότητας τού $\{g_1, g_2, ..., g_k, g_{k+1}, ...\}$). Η ομάδα $G_1 := \{x \in G |\, \exists m \in \mathbb{N} : mx \in \langle g_1\rangle\}$ έχει άστρεπτη βαθμίδα[81] $\text{tf-rank}_{\mathbb{Z}}(G_1) = 1$, οπότε (λόγω τής προϋποτιθέμενης συνθήκης (ii)) είναι ελεύθερη αβελιανή ομάδα με $\text{rank}_{\mathbb{Z}}(G_1) = 1 \Rightarrow G_1 \cong \mathbb{Z}$. Εξάλλου, είναι εύκολο να ελεγχθεί επαγωγικώς[82] ότι $\text{tf-rank}_{\mathbb{Z}}(G_k) = k$, απ' όπου έπεται (εκ τής υποθέσεώς μας) ότι η $G_k$ είναι ελεύθερη βαθμίδας $k$ (και, ιδιαιτέρως, πεπερασμένως παραγόμενη) *για κάθε* $k \in \mathbb{N}$. Το λήμμα 9.5.52 δίδει

$$\begin{aligned} k+1 &= \text{tf-rank}_{\mathbb{Z}}(G_{k+1}) = \text{tf-rank}_{\mathbb{Z}}(G_{k+1}/G_k) + \text{tf-rank}_{\mathbb{Z}}(G_k) \\ &= \text{tf-rank}_{\mathbb{Z}}(G_{k+1}/G_k) + k \Rightarrow \text{tf-rank}_{\mathbb{Z}}(G_{k+1}/G_k) = 1,\ \forall k \in \mathbb{N}. \end{aligned}$$

Από την άλλη μεριά, η πηλικοομάδα $G/G_k$ στερείται στρέψεως[83] και έχει τάξη[84] $|G/G_k| = \aleph_0$. Η υποομάδα $G_{k+1}/G_k \sqsubseteq G/G_k$ (ως πεπερασμένως παραγόμενη και στερούμενη στρέψεως) είναι ελεύθερη[85]. Άρα

$$\text{rank}_{\mathbb{Z}}(G_{k+1}/G_k) = \text{tf-rank}_{\mathbb{Z}}(G_{k+1}/G_k) = 1 \Rightarrow G_{k+1}/G_k \cong \mathbb{Z},\ \forall k \in \mathbb{N}.$$

[80] Βλ. L.S. Pontryagin: *The theory of topological commutative groups*, Annals of Mathematics **35** (1934), 361-388.

[81] Η $G_1$ δεν είναι τετριμμένη, διότι $0_G \neq g_1 \in G_1$. Εάν $x, x' \in G_1$, τότε υπάρχουν $m, m', n, n' \in \mathbb{N}$, τέτοιοι ώστε να ισχύει $mx = ng_1$ και $m'x' = n'g_1$, οπότε $(n'm)x - (nm')x' = (n'n)g_1 - (nn')g_1 = 0_G$.

[82] Έστω $k \in \mathbb{N}$. Οιαδήποτε $k+2$ στοιχεία τής $G_{k+1}$ είναι $\mathbb{Z}$-γραμμικώς εξαρτημένα. Άρα $\text{tf-rank}_{\mathbb{Z}}(G_{k+1}) \leq k+1$. Επειδή $G_k \sqsubset G_{k+1}$ και (από την επαγωγική υπόθεση) $\text{tf-rank}_{\mathbb{Z}}(G_k) = k$, έχουμε $\text{tf-rank}_{\mathbb{Z}}(G_{k+1}) \in \{k, k+1\}$. Η απόδειξη τού ότι $\text{tf-rank}_{\mathbb{Z}}(G_{k+1}) \neq k$ αφήνεται ως άσκηση.

[83] Έστω $g + G_k \in G/G_k$ ($g \in G$) τυχόν στοιχείο πεπερασμένης τάξεως. Τότε $\exists l \in \mathbb{N} : l\,(g + G_k) = G_k$, οπότε $l\,g \in G_k$. Επομένως, $\exists m \in \mathbb{N}, n_1, ..., n_k \in \mathbb{N} : ml\,g = n_1g_1 + \cdots + n_kg_k \Rightarrow g \in G_k$, απ' όπου έπεται ότι $g + G_k = G_k = 0_{G/G_k}$. Κατά συνέπειαν, $\text{tors}(G/G_k) = \{0_{G/G_k}\}$.

[84] Η επιρριπτικότητα τής $\pi^G_{G_k} : G \longrightarrow G/G_k$ δίδει $\aleph_0 = |G| \geq |G/G_k|$. Εάν η $G/G_k$ ήταν πεπερασμένη, τότε θα ήταν τετριμμένη (αφού στερείται στρέψεως), οπότε θα είχαμε $G = G_k \cong \mathbb{Z}^k \Rightarrow \text{tf-rank}_{\mathbb{Z}}(G) = \text{rank}_{\mathbb{Z}}(G) = k$, πράγμα αδύνατο, διότι έχουμε προϋποθέσει ότι $\text{tf-rank}_{\mathbb{Z}}(G) = \aleph_0$.

[85] Για τις αποδείξεις (σε πλήρη γενικότητα) τού ότι *κάθε πηλικοομάδα πεπερασμένως παραγόμενης ομάδας είναι πεπερασμένως παραγόμενη* και τού ότι *κάθε πεπερασμένως παραγόμενη αβελιανή ομάδα που δεν διαθέτει στρέψη είναι ελεύθερη*, βλ. λήμμα 9.6.3 και θεώρημα 9.6.1.

Σύμφωνα με την πρόταση 9.5.37, $\exists K_{k+1} \in \mathbf{Subg}(G_{k+1}) : G_{k+1} = G_k \oplus K_{k+1}$ με $K_{k+1} \cong \mathbb{Z}$. Έστω $y_1$ ένας γεννήτορας τής $G_1$ και $y_{k+1}$ ένας γεννήτορας τής $K_{k+1}$ για κάθε $k \in \mathbb{N}$. Τότε το σύνολο $\{y_1, y_2, ..., y_k, y_{k+1}, ...\}$ αποτελεί μια $\mathbb{Z}$-βάση τής $G$. Πράγματι· εάν υπήρχαν $n_1, ..., n_k \in \mathbb{Z}$ με

$$\sum_{j=1}^{k} n_j y_j = 0_G \;\text{ και }\; n_k \neq 0 \;\text{ για κάποιον }\; k \in \mathbb{N},$$

τότε θα έπρεπε να ισχύει $n_k y_k + G_{k-1} = n_k (y_k + G_{k-1}) = G_{k-1}$, κάτι που είναι αδύνατον (αφού η $G_k/G_{k-1}$ είναι άπειρη κυκλική έχουσα το $y_k + G_{k-1}$ ως γεννήτορά της). Άρα το $\{y_1, y_2, ..., y_k, y_{k+1}, ...\}$ είναι $\mathbb{Z}$-γραμμικώς ανεξάρτητο. Επιπροσθέτως, $G_k = \langle y_1, y_2, ..., y_k \rangle$ (επαγωγικώς, για κάθε $k \in \mathbb{N}$) και, ως εκ τούτου, $G = \bigoplus_{k \in \mathbb{N}}^{\text{εσ.}} \langle y_k \rangle$. Τελικώς λοιπόν η $G$ είναι ελεύθερη αβελιανή ομάδα (δυνάμει τού θεωρήματος 9.5.13). □

Όπως δείχνει το θεώρημα 9.5.60 των Baer και Specker που ακολουθεί, το θεώρημα 9.5.53 τού Pontryagin *παύει να ισχύει* για ομάδες με (ακόμη) μεγαλύτερες τάξεις. Τα αποτελέσματα των Baer και Specker βασίζονται στη μελέτη των ιδιοτήτων τής αβελιανής ομάδας[86] $(\mathbb{Z}^{\mathbb{N}}, +)$ (ήτοι τού *απεριορίστου* εξωτερικού ευθέος αθροίσματος *αριθμησίμων* αντιτύπων τής $(\mathbb{Z}, +)$).

**9.5.54 Σημείωση.** Επειδή κάθε στοιχείο $a = (a_n)_{n \in \mathbb{N}}$ τής $\mathbb{Z}^{\mathbb{N}}$ δεν είναι παρά μια ακολουθία ακεραίων αριθμών, είθισται να γράφουμε

$$a = (a_1, a_2, ..., a_n, a_{n+1}, .......)$$

με το $a$ έχον τον $a_i$ ως «$i$-οστή συντεταγμένη του» για κάθε $i \in \mathbb{N}$.

**9.5.55 Ορισμός.** Λέμε ότι ένα στοιχείο $a = (a_1, ..., a_n, a_{n+1}, ...)$ τής $\mathbb{Z}^{\mathbb{N}}$ είναι μια **πολλαπλασιαστική ακολουθία** όταν[87] $\frac{a_{n+1}}{a_n} \in \mathbb{Z} \smallsetminus \{\pm 1\}$ για κάθε $n \in \mathbb{N}$ και συμβολίζουμε το σύνολο όλων των πολλαπλασιαστικών ακολουθιών που ανήκουν στην $\mathbb{Z}^{\mathbb{N}}$ ως $\mathrm{MS}(\mathbb{Z}^{\mathbb{N}})$.

**9.5.56 Παραδείγματα.** Οι $(1!, 2!, ..., n!, (n+1)!, ...)$ και $(2, 4, 8, ..., 2^n, 2^{n+1}, ...)$ είναι πολλαπλασιαστικές ακολουθίες.

**9.5.57 Λήμμα.** *Το σύνολο* $\mathrm{MS}(\mathbb{Z}^{\mathbb{N}})$ *είναι υπεραριθμήσιμο.*

ΑΠΟΔΕΙΞΗ. Το σύνολο $\mathfrak{B} := \{(b_1, ..., b_n, b_{n+1}, ...) \in \mathbb{Z}^{\mathbb{N}} : |b_n| > 1, \ \forall n \in \mathbb{N}\}$ είναι υπεραριθμήσιμο[88]. Επειδή η απεικόνιση

$$\mathfrak{B} \ni (b_1, b_2, ..., b_n, ...) \longmapsto (b_1, b_1 b_2, ..., \prod_{j=1}^{n} b_j, ...) \in \mathrm{MS}(\mathbb{Z}^{\mathbb{N}})$$

είναι ενριπτική, έχουμε $\aleph_0 < \mathrm{card}(\mathfrak{B}) \leq \mathrm{card}(\mathrm{MS}(\mathbb{Z}^{\mathbb{N}}))$. □

[86] Πρβλ. S. Schröer: *Baer' result: The infinite product of the integers has no bases*, The American Mathematical Monthly **115** (2008), 660-663.

[87] Εξ αυτής τής συνθήκης έπεται, ιδιαιτέρως, ότι $a_n \neq 0, \forall n \in \mathbb{N}$.

[88] Π.χ., $\{2, 3\}^{\mathbb{N}} \subseteq \mathfrak{B}$ και $\mathrm{card}(\{2, 3\}^{\mathbb{N}}) = 2^{\aleph_0} > \aleph_0$.

**9.5.58 Θεώρημα.** *Η αβελιανή ομάδα* $(\mathbb{Z}^{\mathbb{N}}, +)$ *(τάξεως* $\left|\mathbb{Z}^{\mathbb{N}}\right| = \aleph_0^{\aleph_0} > \aleph_0$*) δεν είναι ελεύθερη.*

ΑΠΟΔΕΙΞΗ. Θα εργασθούμε με «εις άτοπον απαγωγή». Ας υποθέσουμε ότι η $\mathbb{Z}^{\mathbb{N}}$ *είναι* ελεύθερη. Τότε αυτή (σύμφωνα με το θεώρημα 9.5.13) διαθέτει κάποια $\mathbb{Z}$-βάση $X$ (και $\mathbb{Z}^{\mathbb{N}} \cong \mathbb{Z}^{(X)}$). Μάλιστα, επειδή η ίδια η $\mathbb{Z}^{\mathbb{N}}$ είναι υπεραριθμήσιμη και στερείται στρέψεως (βλ. 9.4.10), έχουμε $\mathrm{card}(X) = \left|\mathbb{Z}^{\mathbb{N}}\right|$, οπότε και το $X$ είναι υπεραριθμήσιμο. (Βλ. λήμμα 9.5.47.) Έστω $f : \mathbb{Z}^{\mathbb{N}} \xrightarrow{\cong} \mathbb{Z}^{(X)}$ ένας ισομορφισμός και έστω $e_n := (0, 0, ..., 0, \underbrace{1}_{n\text{-οστή θέση}}, 0, 0, ...)$ για κάθε $n \in \mathbb{N}$. Η εικόνα $f(e_n)$ τού $e_n$ μέσω τού $f$ γράφεται ως $\mathbb{Z}$-γραμμικός συνδυασμός $f(e_n) = \sum_{x\in X} l_{x,n}x$, $l_{x,n} \in \mathbb{Z}$, όπου το $Y_n := \{x \in X |\, l_{x,n} \neq 0\}$ είναι πεπερασμένο για κάθε $n \in \mathbb{N}$. Θέτοντας $Y := \bigcup_{n\in\mathbb{N}} Y_n$ και $H := \langle Y \rangle$ παρατηρούμε ότι η πηλικοομάδα $\mathbb{Z}^{(X)}/H$ είναι ελεύθερη έχουσα (κατά την πρόταση 9.5.20) το $\{\, x + H |\, x \in X \smallsetminus Y\}$ ως μια $\mathbb{Z}$-βάση της, με[89]

$$\left.\begin{array}{l} \mathrm{card}(X) > \aleph_0 \\ \mathrm{card}(Y) = \aleph_0 \end{array}\right\} \Rightarrow \mathrm{card}(X \smallsetminus Y) > \aleph_0 \Rightarrow \left|\mathbb{Z}^{(X)}/H\right| > \aleph_0$$

και $f(\mathbb{Z}^{(\mathbb{N})}) \sqsubseteq H$ (διότι ισχύει $\mathbb{Z}^{(\mathbb{N})} = \langle\{\, e_n |\, n \in \mathbb{N}\}\rangle$ και $f(e_n) \in H, \forall n \in \mathbb{N}$). Εν συνεχεία, παρατηρούμε ότι υπάρχει πάντοτε κάποια πολλαπλασιαστική ακολουθία $a^* = (a_1^*, ..., a_n^*, a_{n+1}^*, ...) \in \mathrm{MS}(\mathbb{Z}^{\mathbb{N}})$ με $f(a^*) \notin H$ ($\Leftrightarrow f(a^*) + H \neq H$), διότι

$$|H| = \aleph_0 \;\text{ και }\; \mathrm{card}(f(\mathrm{MS}(\mathbb{Z}^{\mathbb{N}}))) = \mathrm{card}(\mathrm{MS}(\mathbb{Z}^{\mathbb{N}})) \underset{9.5.57}{>} \aleph_0.$$

Επειδή $f(\mathbb{Z}^{(\mathbb{N})}) \sqsubseteq H$ το $h^{(n)} := f(\sum_{k=1}^{n} a_k^* e_k) = f(a_1^*, ..., a_n^*, 0, 0, ..., 0, ...)$ είναι ένα στοιχείο τής $H$ για κάθε $n \in \mathbb{N}$. Επειδή για το

$$z^{(n)} := f(\underbrace{0, 0, ..., 0, 0}_{n \text{ φορές}}, \tfrac{a_{n+1}^*}{a_n^*}, \tfrac{a_{n+2}^*}{a_n^*}, \tfrac{a_{n+3}^*}{a_n^*}, .....) \in \mathbb{Z}^{(X)}$$

$$\Rightarrow a_n^* z^{(n)} = f(\underbrace{0, 0, ..., 0, 0}_{n \text{ φορές}}, a_{n+1}^*, a_{n+2}^*, a_{n+3}^*, .....)$$

έχουμε $a_n^* z^{(n)} = f(a^*) - h^{(n)} \in f(a^*) + H \Rightarrow f(a^*) + H = a_n^*(z^{(n)} + H)$ *για κάθε* $n \in \mathbb{N}$, το σύνολο

$$\left\{ m \in \mathbb{Z} |\, \exists g + H \in \mathbb{Z}^{(X)}/H, g \in \mathbb{Z}^{(X)} : f(a^*) + H = m(g + H) \right\}$$

*δεν είναι πεπερασμένο.* Τούτο *αντίκειται* σε ό,τι απεδείχθη στην πρόταση 9.5.22 (με την $\mathbb{Z}^{(X)}/H$ στη θέση τής *εκεί* παρατεθείσας $G$). Άρα η $\mathbb{Z}^{(X)}/H$ και, κατ' επέκταση, η $\mathbb{Z}^{\mathbb{N}}$ *δεν είναι ελεύθερη.* □

[89] Σημειωτέον ότι το $Y$ είναι αριθμήσιμο ως *ένωση αριθμησίμου πλήθους πεπερασμένων συνόλων*. (Ως εκ τούτου, και η ελεύθερη ομάδα $H \cong \mathbb{Z}^{(Y)}$ είναι αριθμήσιμη.)

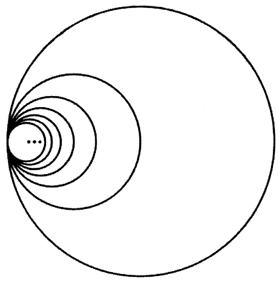
**9.5.59 Σημείωση.** Η μη ελεύθερη αβελιανή ομάδα $(\mathbb{Z}^{\mathbb{N}},+)$ κάνει αισθητή την παρουσία της και στην Αλγεβρική Τοπολογία. Επί παραδείγματι, για την (υπεραριθμήσιμη, μη αβελιανή) *θεμελιώδη ομάδα* $\pi_1(\mathcal{H})$ τού (μονοδιάστατου, τοπικώς δρομοσυνεκτικού, μετρικού) τοπολογικού υπόχωρου

$$\mathcal{H} := \bigcup_{n\in\mathbb{N}} C_n,\ C_n := \left\{ (x,y)\in\mathbb{R}^2 \,\middle|\, (x-\tfrac{1}{n})^2 + y^2 = \tfrac{1}{n^2} \right\},\ \forall n\in\mathbb{N},$$

τού ευκλειδείου επιπέδου, γνωστού υπό την ονομασία *χαβανέζικο σκουλαρίκι*, ορίζεται η απεικόνιση

$$\mathrm{Hom}(\pi_1(\mathcal{H}),\mathbb{Z}) \ni f \longmapsto (f(\mathfrak{l}_1), f(\mathfrak{l}_2), ..., f(\mathfrak{l}_n), ......) \in \mathbb{Z}^{\mathbb{N}},$$

όπου $\mathfrak{l}_n$ είναι ένας γεννήτορας τής θεμελιώδους ομάδας $\pi_1(C_n) \cong \mathbb{Z}$ τού κύκλου $C_n$ για κάθε $n\in\mathbb{N}$.



Αυτή αποδεικνύεται[90] ότι είναι ένας *μονομορφισμός ομάδων* έχων ως εικόνα του την (αριθμήσιμη) ελεύθερη αβελιανή ομάδα $\mathbb{Z}^{(\mathbb{N})}$.

**9.5.60 Θεώρημα. (R. Baer,** 1937/**E. Specker,** 1950.) *Εάν $X$ είναι τυχόν απειροσύνολο, τότε η ομάδα $\left(\mathbb{Z}^X,+\right)$ (τάξεως $\left|\mathbb{Z}^X\right| = \aleph_0^{\mathrm{card}(X)}$) έχει τις εξής ιδιότητες*[91]:

(i) *Η $\mathbb{Z}^X$ είναι μη ελεύθερη αβελιανή ομάδα χωρίς στρέψη.*

(ii) *Κάθε πεπερασμένο υποσύνολο τής $\mathbb{Z}^X$ περιέχεται σε μια πεπερασμένως παραγόμενη υποομάδα της, η οποία διαθέτει συμπλήρωμα (εντός αυτής) που είναι ισόμορφο με το απεριόριστο εξωτερικό ευθύ άθροισμα μιας οικογενείας άπειρων κυκλικών ομάδων.*

(iii) *Κάθε υποομάδα τής $\mathbb{Z}^X$ έχουσα τάξη $\leq \aleph_0$ είναι ελεύθερη.*

ΑΠΟΔΕΙΞΗ. (i) Το ότι η $\mathbb{Z}^X$ δεν διαθέτει στρέψη είναι προφανές. (Βλ. 9.4.10.) Επειδή $\aleph_0 \leq \mathrm{card}(X)$, υπάρχει μια ενριπτική απεικόνιση $\mathbb{N} \hookrightarrow X$. Μέσω αυτής

[90] Βλ. B. de Smith: *The fundamental group of the Hawaiian earring is not free*, International Journal of Algebra and Computation **2** (1992), 33-37 και

J.W. Cannon & G.R. Conner: *The combinatorial structure of the Hawaiian earring group*, Topology and its Applications **106** (2000), 225-271.

[91] Βλ. R. Baer: *Abelian groups without elements of finite order*, Duke Mathematical Journal **3** (1937), 68-122,

και E. Specker: *Additive Gruppen von Folgen ganzer Zahlen*, Portugaliae Mathematica **9** (1950), 131-140.

Επίσης, για μια λεπτομερέστερη μελέτη των ελευθέρων υποομάδων τής $(\mathbb{Z}^X,+)$, βλ.

A. Blass & J. Irwin: *Free subgroups of the Baer-Specker group*, Communications in Algebra **29** (2001), 5769-5794.

επάγεται μονομορφισμός $\mathbb{Z}^{\mathbb{N}} \hookrightarrow \mathbb{Z}^X$. Επομένως, η $\mathbb{Z}^{\mathbb{N}}$ είναι ισόμορφη με μια υποομάδα τής $\mathbb{Z}^X$. Εάν η ομάδα $\mathbb{Z}^X$ ήταν ελεύθερη, τότε (σύμφωνα με το (i) τού θεωρήματος 9.5.39) θα ήταν ελεύθερη και η $\mathbb{Z}^{\mathbb{N}}$, κάτι που θα αντέκειτο σε ό,τι απεδείχθη στο θεώρημα 9.5.58.

(ii) Έστω $K_x := \mathrm{Ker}(\mathrm{pr}_x)$ ο πυρήνας τής φυσικής προβολής

$$\mathrm{pr}_x : \mathbb{Z}^X \longrightarrow \mathbb{Z},\ \ (g_y)_{y\in X} \longmapsto g_x,$$

για κάθε $x \in X$ και έστω $\{g^{(1)}, g^{(2)}, ..., g^{(n)}\}$ ένα πεπερασμένο υποσύνολο τής $\mathbb{Z}^X$. Η απόδειξη θα γίνει με τη βοήθεια τής μαθηματικής επαγωγής ως προς τον $n$. Όταν $n = 1$, μπορούμε να υποθέσουμε ότι[92] $g^{(1)} = (g_x^{(1)})_{x\in X} \neq 0_{\mathbb{Z}^{\mathbb{N}}}$, να θεωρήσουμε τον

$$k := \min\left\{\left|g_x^{(1)}\right| : x \in \left\{y \in X \,\middle|\, g_y^{(1)} \neq 0\right\}\right\} \in \mathbb{N}$$

και να χρησιμοποιήσουμε μαθηματική επαγωγή ως προς αυτόν. Εάν $k = 1$, τότε είναι προφανές ότι $\exists x_0 \in X : g_{x_0}^{(1)} \in \{\pm 1\}$ και $\mathbb{Z}^X = \left\langle g^{(1)} \right\rangle \oplus_{\text{εσ.}} K_{x_0}$, όπου $K_{x_0} \cong \mathbb{Z}^{X\smallsetminus\{x_0\}}$. Εάν $k \geq 2$ και εάν υποθέσουμε ότι ο ισχυρισμός είναι αληθής για όλα στοιχεία τής $\mathbb{Z}^X$ τα έχοντα ελάχιστη απόλυτη τιμή των μη μηδενικών συντεταγμένων τους $< k$, τότε για κάθε $x \in X$ μπορούμε να γράψουμε το $g_x^{(1)}$ υπό τη μορφή $g_x^{(1)} = kq_x + r_x$ για κάποιο (μονοσημάντως ορισμένο) ζεύγος $(q_x, r_x) \in \mathbb{Z}\times\mathbb{Z}$ με $0 \leq r_x < k$ (βλ. B.1.6) και να ορίσουμε τα στοιχεία $q = (q_x)_{x\in X}$ και $r = (r_x)_{x\in X} \in \mathbb{Z}^X$. Προφανώς, $g^{(1)} = kq + r$. Επειδή $\exists x_0 \in X : g_{x_0}^{(1)} \in \{\pm k\}$ με $q_{x_0} \in \{\pm 1\}$ και $r_{x_0} = 0$, έχουμε $|q_{x_0}| = 1$ και μπορούμε να εφαρμόσουμε ό,τι προηγήθηκε (στην περίπτωση όπου $k = 1$, αλλά με το $q_{x_0}$ στη θέση τού *εκεί* εμφανισθέντος $g_{x_0}^{(1)}$), καταλήγοντας στο συμπέρασμα ότι $\mathbb{Z}^X = \langle q\rangle \oplus_{\text{εσ.}} K_{x_0}$. Επειδή $r_{x_0} = 0 \Rightarrow r \in K_{x_0}$ και $\min\{|r_x| : x \in \{y \in X\,|r_y \neq 0\}\} < k$, υπάρχουν (κατά την επαγωγική μας υπόθεση) $L, M \in \mathbf{Subg}(\mathbb{Z}^X)$ με $K_{x_0} = L \oplus_{\text{εσ.}} M$, όπου η $L$ είναι πεπερασμένως παραγόμενη και περιέχει το $q$, και η $M$ είναι ισόμορφη με την $\mathbb{Z}^Y$, για κάποιο $Y \subsetneqq X$. Επομένως, $g^{(1)} = kq + r \in \langle q\rangle \oplus_{\text{εσ.}} K_{x_0}$ και

$$\mathbb{Z}^X = \langle q\rangle \oplus_{\text{εσ.}} K_{x_0} = \langle q\rangle \oplus_{\text{εσ.}} L \oplus_{\text{εσ.}} M.$$

Εν συνεχεία, ολοκληρώνουμε το επαγωγικό μας επιχείρημα ως προς τον $n$. Υποθέτουμε ότι $n \geq 2$, ότι τα $g^{(1)}, ..., g^{(n-1)}$ περιέχονται σε μια πεπερασμένως παραγόμενη $H_1 \sqsubseteq \mathbb{Z}^X$ και ότι $\mathbb{Z}^X = H_1 \oplus_{\text{εσ.}} H_2$ για κάποια $H_2 \in \mathbf{Subg}(\mathbb{Z}^X)$ με $H_2 \cong \mathbb{Z}^W$ ($W \subsetneqq X$). Το $g^{(n)}$ γράφεται μονοσημάντως υπό τη μορφή $g^{(n)} = g'^{(n)} + g''^{(n)}$, όπου $g'^{(n)} \in H_1$ και $g''^{(n)} \in H_2$. Εφαρμόζοντας ό,τι προηγήθηκε (στην περίπτωση όπου $n = 1$, αλλά με το $g''^{(n)}$ στη θέση τού *εκεί* θεωρηθέντος $g^{(1)}$), συμπεραίνουμε ότι το $g''^{(n)}$ ανήκει σε μια πεπερασμένως παραγόμενη $H_3 \sqsubseteq \mathbb{Z}^X$ και ότι $H_2 = H_3 \oplus_{\text{εσ.}} H_4$ για κάποια $H_4 \in \mathbf{Subg}(\mathbb{Z}^X)$ με $H_4 \cong \mathbb{Z}^Z$ ($Z \subsetneqq X$). Κατά συνέπειαν, $\mathbb{Z}^X = H_1 \oplus_{\text{εσ.}} H_3 \oplus_{\text{εσ.}} H_4$, όπου τα $g^{(1)}, ..., g^{(n-1)}, g^{(n)}$ περιέχονται στην $H_1 \oplus_{\text{εσ.}} H_3$.

(iii) Ας υποθέσουμε ότι υπάρχει κάποια *μη ελεύθερη* υποομάδα $H$ τής $\mathbb{Z}^X$ τάξεως $\leq \aleph_0$. Τότε (σύμφωνα με το θεώρημα 9.5.53 τού Pontryagin) υπάρχει κάποια *μη*

[92] Το $0_{\mathbb{Z}^{\mathbb{N}}}$ ανήκει σε κάθε υποομάδα τής $\mathbb{Z}^X$.

*ελεύθερη* υποομάδα $K$ τής $H$ έχουσα *πεπερασμένη* άστρεπτη βαθμίδα. Έστω $S$ ένα μεγιστικό $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο τής $K$. Επειδή το $S$ είναι πεπερασμένο, υπάρχουν (σύμφωνα με τα αποδειχθέντα στο (ii)) υποομάδες $J_1, J_2$ τής $\mathbb{Z}^X$ με $\mathbb{Z}^X = J_1 \oplus_{\varepsilon\sigma.} J_2$, όπου η $J_1$ είναι πεπερασμένως παραγόμενη και περιέχει το $S$, και $J_2 \cong \mathbb{Z}^{X'}$ ($X' \subsetneqq X$). Για οιοδήποτε στοιχείο $g \in K$ υπάρχει κάποιος $m \in \mathbb{N}$, τέτοιος ώστε να ισχύει $mg \in \langle S \rangle \sqsubseteq J_1$. Επειδή η πηλικοομάδα $\mathbb{Z}^X/J_1$ ($\cong J_2 \cong \mathbb{Z}^{X'}$) στερείται στρέψεως και $m(g+J_1) = mg + J_1 = J_1 = 0_{\mathbb{Z}^X/J_1}$, λαμβάνουμε $g + J_1 = J_1 \Rightarrow g \in J_1$, οπότε $K \sqsubseteq J_1$. Η $J_1$ (ως υποομάδα τής $\mathbb{Z}^X$) στερείται στρέψεως και είναι (εκ τού ορισμού της) πεπερασμένως παραγόμενη. Άρα η $J_1$ είναι ελεύθερη[93]. Δυνάμει τού (i) τού θεωρήματος 9.5.39 η $K$ είναι ωσαύτως ελεύθερη. Άτοπο! Άρα *κάθε* υποομάδα τής $\mathbb{Z}^X$ τάξεως $\leq \aleph_0$ είναι κατ' ανάγκην ελεύθερη. $\square$

► **Ενδομορφισμοί ελεύθερων αβελιανών ομάδων πεπερασμένης βαθμίδας**. Εάν $(G,+)$ είναι μια ελεύθερη αβελιανή ομάδα έχουσα βαθμίδα $\mathrm{rank}_{\mathbb{Z}}(G) = r \in \mathbb{N}$, τότε ο δακτύλιος $(\mathrm{End}(G), +, \circ)$ των ενδομορφισμών τής $G$ είναι ισόμορφος με τον δακτύλιο $(\mathrm{Mat}_{r\times r}(\mathbb{Z}), +, \cdot)$ των $(r \times r)$-πινάκων με ακέραιες εγγραφές. Πράγματι· εάν $X = \{x_1, ..., x_r\}$ είναι μια $\mathbb{Z}$-βάση τής $G$ και $\vartheta \in \mathrm{End}(G)$, τότε η εικόνα $\vartheta(x_j)$ τού $x_j$ γράφεται κατά τρόπο μονοσήμαντο ως $\mathbb{Z}$-γραμμικός συνδυασμός

$$\vartheta(x_j) = \sum_{i=1}^{r} n_{ij} x_i,\ n_{ij} \in \mathbb{Z},$$

των $x_1, ..., x_\kappa$ για κάθε $j \in \{1, ..., r\}$. Θέτουμε

$$\mathbf{A}_{\vartheta,X} := \begin{pmatrix} n_{11} & n_{12} & \cdots & n_{1r} \\ n_{21} & n_{22} & \cdots & n_{2r} \\ \vdots & \vdots & & \vdots \\ n_{r1} & n_{r2} & \cdots & n_{rr} \end{pmatrix} \in \mathrm{Mat}_{r\times r}(\mathbb{Z}).$$

**9.5.61 Θεώρημα.** *Η απεικόνιση*

$$\boxed{f_X : \mathrm{End}(G) \longrightarrow \mathrm{Mat}_{r\times r}(\mathbb{Z}),\ \vartheta \longmapsto f_X(\vartheta) := \mathbf{A}_{\vartheta,X},}$$

*αποτελεί ισομορφισμό δακτυλίων για κάθε $\mathbb{Z}$-βάση $X = \{x_1, ..., x_r\}$ τής $G$.*

ΑΠΟΔΕΙΞΗ. Εάν $\vartheta, \vartheta' \in \mathrm{End}(G)$ και

$$\vartheta(x_j) = \sum_{i=1}^{r} n_{ij} x_i,\ \ \vartheta'(x_j) = \sum_{i=1}^{r} n'_{ij} x_i,$$

τότε $\mathbf{A}_{\vartheta,X} = (n_{ij})_{1\leq i,j\leq r}$, $\mathbf{A}_{\vartheta',X} = (n'_{ij})_{1\leq i,j\leq r}$ και

$$f_X(\vartheta + \vartheta') = \mathbf{A}_{\vartheta+\vartheta',X} = \mathbf{A}_{\vartheta,X} + \mathbf{A}_{\vartheta',X} = f_X(\vartheta) + f_X(\vartheta'). \tag{9.65}$$

[93] *Κάθε πεπερασμένως παραγόμενη αβελιανή ομάδα που δεν διαθέτει στρέψη είναι ελεύθερη.* (Βλ. θεώρημα 9.6.1.)

Επειδή (εισάγοντας -για ευνόητους λόγους- έναν τρίτο *βοηθητικό* δείκτη $k$) έχουμε $\mathbf{A}_{\vartheta',X} = (n'_{jk})_{1\leq j,k\leq r}$, υποθέτοντας ότι $(\vartheta\circ\vartheta')(x_k) = \sum_{i=1}^{r} m_{ik}x_i$ (ήτοι ότι $\mathbf{A}_{\vartheta\circ\vartheta',X} = (m_{ik})_{1\leq i,k\leq r}$), λαμβάνουμε

$$(\vartheta\circ\vartheta')(x_k) = \vartheta\left(\sum_{j=1}^{r} n'_{jk}x_j\right) = \sum_{j=1}^{r} n'_{jk}\vartheta(x_j)$$

$$= \sum_{j=1}^{r} n'_{jk}\left(\sum_{i=1}^{r} n_{ij}x_i\right) = \sum_{i=1}^{r}\left(\sum_{j=1}^{r} n_{ij}n'_{jk}\right)x_i.$$

Εξ αυτού (για $1\leq i,k\leq r$) έπεται ότι

$$m_{ik} = \sum_{j=1}^{r} n_{ij}n'_{jk} \Rightarrow f_X(\vartheta\circ\vartheta') = \mathbf{A}_{\vartheta\circ\vartheta',X} = \mathbf{A}_{\vartheta,X}\mathbf{A}_{\vartheta',X} = f_X(\vartheta)f_X(\vartheta'), \quad (9.66)$$

οπότε (λόγω των (9.65) και (9.66)) η $f_X$ είναι ομομορφισμός δακτυλίων. Επιπροσθέτως, $f_X(\mathrm{id}_G) = \mathbf{I}_r$ και επειδή

$$\mathrm{Ker}(f_X) = \{\vartheta\in\mathrm{End}(G) \mid \mathbf{A}_{\vartheta,X} = \mathbf{I}_r\} = \{\vartheta\in\mathrm{End}(G) \mid \vartheta(x_j) = x_j, \forall j\in\{1,...,r\}\}$$

$$= \left\{\vartheta\in\mathrm{End}(G) : \vartheta|_X = \mathrm{id}_G|_X\right\} = \{\mathrm{id}_G\},$$

η απεικόνιση $f_X$ είναι μονομορφισμός δακτυλίων. Τέλος, ορίζοντας για κάθε πίνακα $\mathbf{A} = (n_{ij})_{1\leq i,j\leq r}\in\mathrm{Mat}_{r\times r}(\mathbb{Z})$ την απεικόνιση

$$\varphi_{\mathbf{A}} : X \longrightarrow G,\ x_j \longmapsto \varphi_{\mathbf{A}}(x_j) := \sum_{i=1}^{r} n_{ij}x_i,\ \forall j\in\{1,...,r\},$$

γνωρίζουμε (από την πρόταση 9.5.29) ότι υπάρχει $\vartheta_{\mathbf{A}}\in\mathrm{Hom}(G,G)\,(=\mathrm{End}(G))$ με $\vartheta_{\mathbf{A}}|_X = \varphi_{\mathbf{A}}$, οπότε

$$f_X(\vartheta_{\mathbf{A}}) = \mathbf{A}_{\vartheta_{\mathbf{A}},X} = \mathbf{A} \quad (9.67)$$

(καθώς ισχύει $\vartheta_{\mathbf{A}}(x_j) = \varphi_{\mathbf{A}}(x_j) = \sum_{i=1}^{r} n_{ij}x_i$ για κάθε $j\in\{1,...,r\}$). Από την (9.67) συνάγεται ότι η $f_X$ είναι, συν τοις άλλοις, και επιρριπτική και, ως εκ τούτου, ισομορφισμός δακτυλίων. □

► **Αυτομορφισμοί ελεύθερων αβελιανών ομάδων πεπερασμένης βαθμίδας**. Επειδή $\mathrm{Aut}(G) = \mathrm{End}(G)^{\times}$ (βλ. 2.4.30 (i)), καταλήγουμε στο ακόλουθο:

**9.5.62 Θεώρημα.** *Εάν $(G,+)$ είναι μια ελεύθερη αβελιανή ομάδα έχουσα βαθμίδα $\mathrm{rank}_{\mathbb{Z}}(G) = r\in\mathbb{N}$, τότε για κάθε $\mathbb{Z}$-βάση $X$ τής $G$ ο περιορισμός*

$$f_X|_{\mathrm{Aut}(G)} : \mathrm{Aut}(G) \longrightarrow \mathrm{GL}_r(\mathbb{Z}),\ \vartheta \longmapsto f_X(\vartheta) := \mathbf{A}_{\vartheta,X},$$

*αποτελεί ισομορφισμό ομάδων, οπότε*

$$\boxed{\mathrm{Aut}(G) = \{\vartheta\in\mathrm{End}(G) \mid \det(\mathbf{A}_{\vartheta,X})\in\{\pm1\}\} \cong \mathrm{GL}_r(\mathbb{Z}).}$$

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το ότι

$$f_X(\mathrm{Aut}(G)) = f_X(\mathrm{End}(G)^{\times}) = (f_X(\mathrm{End}(G)))^{\times} \underset{9.5.61}{=} (\mathrm{Mat}_{r\times r}(\mathbb{Z}))^{\times}$$

$$= \mathrm{GL}_r(\mathbb{Z}) = \{\mathbf{A}\in\mathrm{Mat}_{r\times r}(\mathbb{Z}) \mid \det(\mathbf{A})\in\{\pm1\}\}.$$

(Βλ. θεώρημα D.2.18.) □

# 9.6 ΠΕΠΕΡΑΣΜΕΝΩΣ ΠΑΡΑΓΟΜΕΝΕΣ ΑΒΕΛΙΑΝΕΣ ΟΜΑΔΕΣ

Η κλάση των πεπερασμένων αβελιανών ομάδων περιέχεται και σε μια δεύτερη, ευρύτερη κλάση, ήτοι εκείνη των *πεπερασμένως παραγομένων αβελιανών ομάδων*. Όσες εκ των ομάδων αυτής τής ευρύτερης κλάσεως στερούνται στρέψεως είναι ελεύθερες και έχουν πεπερασμένη βαθμίδα. Οι πεπερασμένως παραγόμενες αβελιανές ομάδες είναι ισόμορφες με το ευθύ άθροισμα των υποομάδων στρέψεώς τους και των άστρεπτων μερών τους, κάτι που διευκολύνει την (μέχρις ισομορφισμού) ταξινόμησή τους και τη μελέτη των υποομάδων και των αυτομορφισμών τους.

**9.6.1 Θεώρημα.** *Κάθε πεπερασμένως παραγόμενη αβελιανή ομάδα που δεν διαθέτει στρέψη είναι ελεύθερη και έχει πεπερασμένη βαθμίδα.*

Απόδειξη. Έστω $(G,+)$ μια πεπερασμένως παραγόμενη αβελιανή ομάδα με $\mathrm{tors}(G)=\{0_G\}$ και έστω $X$ ένα πεπερασμένο σύστημα γεννητόρων αυτής. Εάν $X=\{0_G\}$, τότε η $G$ είναι τετριμμένη και, ως εκ τούτου, ελεύθερη με βαθμίδα $0$. Εάν $\mathrm{card}(X)\geq 1$ και $X\neq\{0_G\}$, τότε η $G$ είναι μη τετριμμένη και η οικογένεια

$$\mathfrak{V}:=\{Y\in\mathfrak{P}(X)\smallsetminus\{\varnothing\}\,|\,Y\ \ \mathbb{Z}\text{-γραμμικώς ανεξάρτητο}\}$$

όλων των μη κενών $\mathbb{Z}$-γραμμικώς ανεξαρτήτων υποσυνόλων $Y\subseteq G$ που περιέχονται στο $X$ είναι *μη κενή* [94]. Θέτουμε $r:=\max\{\mathrm{card}(Y)\,|\,Y\in\mathfrak{V}\}$ και θεωρούμε ένα σύνολο $\{x_1,...,x_r\}$ ανήκον στην $\mathfrak{V}$ και έχον πληθικό αριθμό $r$. Επειδή $\mathrm{tors}(G)=\{0_G\}$, οι επιμορφισμοί $\mathbb{Z}\ni n\longmapsto nx_j\in\langle x_r\rangle,\ \ j\in\{1,...,r\}$, είναι ισομορφισμοί, οπότε η $H:=\langle x_1\rangle\oplus_{\text{εσ.}}\cdots\oplus_{\text{εσ.}}\langle x_r\rangle\sqsubseteq G$ είναι ελεύθερη αβελιανή ομάδα έχουσα βαθμίδα $r$. (Βλ. πόρισμα 9.5.15.) Θα αποδείξουμε ότι η $G$ είναι ωσαύτως ελεύθερη έχουσα βαθμίδα $\mathrm{rank}_{\mathbb{Z}}(G)=r$. Στην περίπτωση όπου $H=G$, τούτο είναι προφανές. Ας υποθέσουμε ότι $H\sqsubset G$. Τότε[95] $X\nsubseteq H$. Θεωρούμε τυχόν $x\in X\smallsetminus\{x_1,...,x_r\}$. Λόγω τού τρόπου ορισμού τού $\{x_1,...,x_r\}$, το $\{x,x_1,...,x_r\}\subseteq G$ είναι κατ' ανάγκην $\mathbb{Z}$-γραμμικώς εξαρτημένο υποσύνολο, κάτι που σημαίνει ότι υπάρχουν $n_x,n_1,...,n_r\in\mathbb{Z}$, με κάποιον ή κάποιους εξ αυτών $\neq 0$, ούτως ώστε να ισχύει

$$n_xx+n_1x_1+\cdots+n_rx_r=0_G\Rightarrow n_xx=-(n_1x_1+\cdots+n_rx_r)\in H.$$

Σημειωτέον ότι ο $n_x$ συγκαταλέγεται πάντοτε σε εκείνους τους συντελεστές που είναι $\neq 0$. (Εάν ίσχυε $n_x=0$, τότε θα είχαμε $n_1x_1+\cdots+n_rx_r=0_G$, απ' όπου θα έπετο ότι $n_1=\cdots=n_r=0$ λόγω τής $\mathbb{Z}$-γραμμικής ανεξαρτησίας τού $\{x_1,...,x_r\}$.) Επειδή το $X$ είναι πεπερασμένο, ορίζεται καλώς ο ακέραιος

$$m:=\prod_{x\in X\smallsetminus\{x_1,..,x_r\}}n_x\in\mathbb{Z}\smallsetminus\{0\}.$$

[94] Επειδή $\mathrm{tors}(G)=\{0_G\}$, $\{g\}\in\mathfrak{V}$ για κάθε $g\in G\smallsetminus\{0_G\}$.

[95] Εάν $X\subseteq H$, τότε θα είχαμε $G=\mathrm{Lin}_{\mathbb{Z}}(X)\subseteq\mathrm{Lin}_{\mathbb{Z}}(H)=H\Rightarrow H=G$.

Προφανώς, $mx \in \langle n_x x \rangle \sqsubseteq H \Rightarrow m\langle x \rangle \sqsubseteq H$ *για κάθε* $x \in X \smallsetminus \{x_1,...,x_r\}$. Κατά συνέπειαν,

$$G = \bigoplus_{x\in X}^{\text{εσ.}} \langle x \rangle \Rightarrow mG = \left( \bigoplus\nolimits^{\text{εσ.}}_{x\in X\smallsetminus\{x_1,\ldots,x_r\}} m\langle x \rangle \right) \oplus_{\text{εσ.}} mH \sqsubseteq H$$

και η απεικόνιση $f : G \longrightarrow H, g \longmapsto f(g) := mg$, είναι μονομορφισμός ομάδων. (Η ενριπτικότητά της οφείλεται στην απουσία στρέψεως.) Άρα $\mathrm{Ker}(f) = \{0_G\}$ και $G \cong \mathrm{Im}(f) = mG \sqsubseteq H$. Επειδή η $H$ είναι ελεύθερη βαθμίδας $r$, η $mG$ και, κατ' επέκταση, και η $G \cong mG$ είναι ωσαύτως ελεύθερη με

$$\mathrm{rank}_{\mathbb{Z}}(G) = \mathrm{rank}_{\mathbb{Z}}(mG) =: s \leq r. \tag{9.68}$$

(Βλ. 9.5.39 και 9.5.31.) Από την άλλη μεριά, $H \sqsubset G \underset{9.5.39}{\Longrightarrow} r \leq s$, οπότε η (9.68) δίδει $s = r$. □

**9.6.2 Σημείωση.** Στην προηγηθείσα απόδειξη η ομάδα $mG$ (ούσα ελεύθερη βαθμίδας $s \geq 1$) διαθέτει τουλάχιστον μία $\mathbb{Z}$-βάση $\{my_1, ..., my_s\}$ για κάποια $y_1, ..., y_s \in G$. Αξίζει να επισημανθεί ότι το σύνολο $\{y_1, ..., y_s\}$ αποτελεί μια $\mathbb{Z}$-βάση τής $G$. Πράγματι· εάν $l_1, ..., l_s \in \mathbb{Z}$ είναι τέτοιοι, ώστε $\sum_{j=1}^{s} l_j y_j = 0_G$, τότε

$$\left.\begin{array}{c} \sum_{j=1}^{s} l_j(my_j) = m0_G = 0_G \\ \{my_1, ..., my_s\}\ \mathbb{Z}\text{-βάση τής } mG \end{array}\right\} \Longrightarrow l_j = 0,\ \forall j \in \{1, ..., s\}.$$

Επιπροσθέτως, για κάθε $g \in G$,

$$mg \in mG = \langle my_1, ..., my_s \rangle \Rightarrow [\exists \lambda_1, ..., \lambda_s \in \mathbb{Z} : mg = \sum_{j=1}^{s} \lambda_j(my_j)]$$

$$\Rightarrow \left\{\begin{array}{c} m(g - \sum_{j=1}^{s} \lambda_j y_j) = 0_G \\ m \neq 0 \end{array}\right\} \underset{\mathrm{tors}(G)=\{0_G\}}{\Longrightarrow} g = \sum_{j=1}^{s} \lambda_j y_j,$$

οπότε $G = \langle y_1, ..., y_s \rangle$. (Φυσικά, όπως προαναφέραμε, $s = r :=$ μέγιστο πλήθος $\mathbb{Z}$-γραμμικώς ανεξαρτήτων στοιχείων τής $G$.)

► **Ταξινόμηση μέχρις ισομορφισμού**. Για τις πεπερασμένως παραγόμενες αβελιανές ομάδες αυτή ανάγεται (μέσω τού θεωρήματος 9.6.7) στις γνωστές ταξινομήσεις των συστατικών μερών τους.

**9.6.3 Λήμμα.** *Εάν $H$ είναι μια υποομάδα μιας πεπερασμένως παραγόμενης αβελιανής ομάδας $(G, +)$, τότε η πηλικοομάδα $G/H$ είναι πεπερασμένως παραγόμενη.*

ΑΠΟΔΕΙΞΗ. Εάν $\{x_1, ..., x_\kappa\}$ είναι κάποιο πεπερασμένο σύστημα γεννητόρων τής $G$, τότε το $\{x_1 + H, ..., x_\kappa + H\}$ αποτελεί ένα σύστημα γεννητόρων[96] τής πηλικοομάδας $G/H$. (Βλ. πρόταση 4.4.18.) □

**9.6.4 Λήμμα.** *Εάν $(G, +)$ είναι μια πεπερασμένως παραγόμενη αβελιανή ομάδα, τότε η πηλικοομάδα $G/\mathrm{tors}(G)$ είναι ελεύθερη και έχει βαθμίδα $r \in \mathbb{N}_0$.*

[96] Ο πληθικός αριθμός αυτού τού συστήματος γεννητόρων τής $G/H$ είναι $\leq \kappa$.

ΑΠΟΔΕΙΞΗ. Η $G/\mathrm{tors}(G)$ (σύμφωνα με την πρόταση 9.4.5 και το λήμμα 9.6.3) δεν διαθέτει στρέψη και είναι πεπερασμένως παραγόμενη. Ο ισχυρισμός είναι αληθής δυνάμει τού θεωρήματος 9.6.1. □

**9.6.5 Λήμμα.** *Εάν $(G,+)$ είναι μια πεπερασμένως παραγόμενη αβελιανή ομάδα, τότε*

$$\boxed{G \cong \mathrm{tors}(G) \oplus (G/\mathrm{tors}(G)) \cong \mathrm{tors}(G) \oplus \mathbb{Z}^r,}$$

*όπου* $r := \mathrm{rank}_{\mathbb{Z}}\,(G/\mathrm{tors}(G)) \in \mathbb{N}_0$.

ΑΠΟΔΕΙΞΗ. Επειδή (κατά το λήμμα 9.6.4) η πηλικοοομάδα $G/\mathrm{tors}(G)$ είναι ελεύθερη έχουσα βαθμίδα $r \in \mathbb{N}_0$,

$$\exists K \in \mathbf{Subg}(G) : G = \mathrm{tors}(G) \oplus_{\text{εσ.}} K \underset{7.1.43\,\text{(ii)}}{\cong} \mathrm{tors}(G) \oplus K,$$

όπου $K \cong G/\mathrm{tors}(G) \cong \mathbb{Z}^r$. (Βλ. προτάσεις 9.5.37 και 7.1.29.) □

**9.6.6 Πρόταση.** *Εάν $G_1, G_2$ είναι δυο πεπερασμένως παραγόμενες αβελιανές ομάδες, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) $G_1 \cong G_2$.

(ii) $\mathrm{tors}(G_1) \cong \mathrm{tors}(G_2)$ *και* $\mathrm{rank}_{\mathbb{Z}}\,(G_1/\mathrm{tors}(G_1)) = \mathrm{rank}_{\mathbb{Z}}(G_2/\mathrm{tors}(G_2))$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Σύμφωνα με την πρόταση 9.4.8, ισχύει $\mathrm{tors}(G_1) \cong \mathrm{tors}(G_2)$ και $G_1/\mathrm{tors}(G_1) \cong G_2/\mathrm{tors}(G_2)$. Οι τελευταίες είναι ελεύθερες. (Βλ. 9.6.4.) Το ότι οι βαθμίδες τους είναι ίσες έπεται από το θεώρημα 9.5.31.
(ii)⇒(i) Εάν $\mathrm{tors}(G_1) \cong \mathrm{tors}(G_2)$ και

$$\mathrm{rank}_{\mathbb{Z}}\,(G_1/\mathrm{tors}(G_1)) = \mathrm{rank}_{\mathbb{Z}}(G_2/\mathrm{tors}(G_2)) \underset{9.5.31}{\Longrightarrow} G_1/\mathrm{tors}(G_1) \cong G_2/\mathrm{tors}(G_2),$$

τότε $G_1 \cong \mathrm{tors}(G_1) \oplus (G_1/\mathrm{tors}(G_1)) \cong \mathrm{tors}(G_2) \oplus (G_2/\mathrm{tors}(G_2)) \cong G_2$ λόγω τού λήμματος 9.6.5 και τού (v) τής προτάσεως 7.1.55. □

**9.6.7 Θεώρημα. (Θεμελιώδες θεώρημα περί πεπ. παραγομένων αβελιανών ομάδων.)**
(a) *Εάν $(G,+)$ είναι μια πεπερασμένως παραγόμενη αβελιανή ομάδα, τότε*

$$\boxed{G \cong \mathrm{tors}(G) \oplus \mathbb{Z}^r, \text{ όπου } |\mathrm{tors}(G)| < \infty \text{ και } r := \mathrm{rank}_{\mathbb{Z}}\,(G/\mathrm{tors}(G)) \in \mathbb{N}_0.}$$

(b) *Εάν $G_1, G_2$ είναι δυο πεπερασμένως παραγόμενες αβελιανές ομάδες και*

$$G_1 \cong \mathrm{tors}(G_1) \oplus \mathbb{Z}^{r_1}, \;\; G_2 \cong \mathrm{tors}(G_2) \oplus \mathbb{Z}^{r_2},$$

*τότε $G_1 \cong G_2$ εάν και μόνον εάν ικανοποιούνται οι ακόλουθες συνθήκες*:

(i) $r_1 = r_2$.

(ii) $|\mathrm{tors}(G_1)| = |\mathrm{tors}(G_2)|$ *και οι ομάδες* $\mathrm{tors}(G_1), \mathrm{tors}(G_2)$ *έχουν (στην περίπτωση όπου αυτές είναι μη τετριμμένες) τους ίδιους στοιχειώδεις διαιρέτες (ή, εναλλακτικώς, τους ίδιους αναλλοίωτους παράγοντες).*

ΑΠΟΔΕΙΞΗ. (a) Τούτο έπεται από το λήμμα 9.6.5 και την πρόταση 9.4.3.

(b) Αρκεί να εφαρμοσθεί η πρόταση 9.6.6 σε συνδυασμό με το πόρισμα 9.1.21 (ή, εναλλακτικώς, με το πόρισμα 9.1.27). □

► **Υποομάδες**. Η ιδιότητα τού *πεπερασμένως παραγομένου* μιας αβελιανής ομάδας διατηρείται στις υποομάδες αυτής. Γι' αυτόν τον λόγο ο (μέχρις ισομορφισμού) προσδιορισμός των υποομάδων μιας πεπερασμένως παραγόμενης αβελιανής ομάδας ανάγεται (δυνάμει τού θεωρήματος 9.6.10) στον προσδιορισμό των υποομάδων τής υποομάδας στρέψεώς της και των υποομάδων τού άστρεπτου μέρους της (που είναι εφικτός μέσω των θεωρημάτων 9.2.2, 9.2.4 και 9.5.39).

**9.6.8 Λήμμα.** *Εάν $(G,+)$ είναι μια πεπερασμένως παραγόμενη αβελιανή ομάδα, τότε υφίσταται επιμορφισμός $f:\mathbb{Z}^\kappa \longrightarrow G$ για κάποιον $\kappa \in \mathbb{N}$.*

ΑΠΟΔΕΙΞΗ. Εάν $\{x_1,...,x_\kappa\}$ είναι κάποιο πεπερασμένο σύστημα γεννητόρων τής $G$, τότε η απεικόνιση $f:\mathbb{Z}^\kappa \longrightarrow G, (n_1,...,n_\kappa) \longmapsto f(n_1,...,n_\kappa) := \sum_{j=1}^{\kappa} n_j x_j$ είναι ένας επιμορφισμός από την ελεύθερη αβελιανή ομάδα $\mathbb{Z}^\kappa$ επί τής $G$. □

**9.6.9 Πρόταση.** *Κάθε υποομάδα μιας πεπερασμένως παραγόμενης αβελιανής ομάδας $(G,+)$ είναι αφ' εαυτής πεπερασμένως παραγόμενη.*

ΑΠΟΔΕΙΞΗ. Έστω $H \in \mathbf{Subg}(G)$. Το λήμμα 9.6.8 εγγυάται την ύπαρξη ενός επιμορφισμού $f:\mathbb{Z}^\kappa \longrightarrow G$ για κάποιον $\kappa \in \mathbb{N}$. Η αντίστροφη εικόνα $f^{-1}(H)$ τής $H$ μέσω αυτού αποτελεί μια υποομάδα τής ελεύθερης αβελιανής ομάδας $\mathbb{Z}^\kappa$. Σύμφωνα με το θεώρημα 9.5.39 η $f^{-1}(H)$ είναι ελεύθερη με βαθμίδα $r \leq \kappa$.

*Περίπτωση πρώτη*. Εάν $r=0$, τότε οι $f^{-1}(H)$, $H=f(f^{-1}(H))$ είναι τετριμμένες.

*Περίπτωση δεύτερη*. Εάν $r \geq 1$, τότε θεωρούμε μια $\mathbb{Z}$-βάση $Y=\{y_1,...,y_r\}$ τής $f^{-1}(H)$. Επειδή $f^{-1}(H)=\langle Y\rangle$, έχουμε

$$H=f(f^{-1}(H))=f(\langle Y\rangle)=f(\langle y_1,...,y_r\rangle) \underset{2.4.9\,(\mathrm{i})}{=} \langle f(y_1),...,f(y_r)\rangle,$$

οπότε η $H$ διαθέτει ένα πεπερασμένο σύστημα γεννητόρων. □

**9.6.10 Θεώρημα.** *Εάν $(G,+)$ είναι μια πεπερασμένως παραγόμενη αβελιανή ομάδα, τότε ισχύουν τα εξής:*

(i) *Εάν $H \in \mathbf{Subg}(G)$, τότε $H \cong H_1 \oplus H_2$ για κάποιες $H_1 \in \mathbf{Subg}(\mathrm{tors}(G))$ και $H_2 \in \mathbf{Subg}(G/\mathrm{tors}(G))$.*

(ii) *Εάν $H_1 \in \mathbf{Subg}(\mathrm{tors}(G))$ και $H_2 \in \mathbf{Subg}(G/\mathrm{tors}(G))$, τότε η $H_1 \oplus H_2$ είναι ισόμορφη με κάποια υποομάδα τής $G$.*

ΑΠΟΔΕΙΞΗ. (i) Έστω $H \in \mathbf{Subg}(G)$ και έστω $\iota: H \hookrightarrow G$ η συνήθης ένθεση. Επειδή η $\iota$ είναι μονομορφισμός, το λήμμα 9.4.7 μας πληροφορεί αφ' ενός μεν ότι

$$\iota(\mathrm{tors}(H)) \sqsubseteq \mathrm{tors}(G) \Rightarrow \mathrm{tors}(H) \cong \iota|_{\mathrm{tors}(H)}(\mathrm{tors}(H)) =: H_1 \sqsubseteq \mathrm{tors}(G),$$

αφ' ετέρου δε ότι ο επαγόμενος ομομορφισμός $\iota^{\text{πηλ.}} : H/\text{tors}(H) \longrightarrow G/\text{tors}(G)$ είναι μονομορφισμός, απ' όπου έπεται ότι $\iota^{\text{πηλ.}}(H/\text{tors}(H)) =: H_2 \sqsubseteq G/\text{tors}(G)$. Σύμφωνα με την πρόταση 9.6.9 η $H$ είναι πεπερασμένως παραγόμενη, οπότε

$$H \underset{9.6.5}{\cong} \text{tors}(H) \oplus (H/\text{tors}(H)) \cong H_1 \oplus H_2.$$

(ii) Εάν $H_1 \in \mathbf{Subg}(\text{tors}(G))$ και $H_2 \in \mathbf{Subg}(G/\text{tors}(G))$, τότε

$$H_1 \oplus H_2 \underset{7.1.6\,(\text{i})}{\sqsubseteq} \text{tors}(G) \oplus (G/\text{tors}(G)) \cong G,$$

οπότε το ευθύ άθροισμα $H_1 \oplus H_2$ είναι ισόμορφο με κάποια υποομάδα τής $G$. $\square$

► **Αυτομορφισμοί**. *Η ομάδα αυτομορφισμών μιας πεπερασμένως παραγόμενης αβελιανής ομάδας* αποκτάται από την ομάδα αυτομορφισμών τής υποομάδας στρέψεώς της και από την ομάδα αυτομορφισμών τού άστρεπτου μέρους της (τις οποίες γνωρίζουμε από τα θεωρήματα 9.3.8 και 9.5.62), ύστερα από κατασκευή κατάλληλου *ημιευθέος γινομένου* (με *πρώτο τον παράγοντα* την ομάδα των ομομορφισμών από το άστρεπτο μέρος της στην ομάδα στρέψεώς της και *δεύτερό τον παράγοντα* το ευθύ γινόμενο των προαναφερθεισών ομάδων αυτομορφισμών). Συγκεκριμένα, ισχύει το ακόλουθο:

**9.6.11 Θεώρημα. (M. Golasiński & D.L. Gonçalves,** 2008.) *Εάν $(G,+)$ είναι μια πεπερασμένως παραγόμενη αβελιανή ομάδα, τότε μέσω τού ισομορφισμού*

$$G \underset{9.6.5}{\xrightarrow{\cong}} \text{tors}(G) \oplus (G/\text{tors}(G))$$

*επάγεται (σε επίπεδο ομάδων αυτομορφισμών) ένας ισομορφισμός*[97]

$$\boxed{\text{Aut}(G) \cong \text{Hom}(G/\text{tors}(G), \text{tors}(G)) \rtimes_{\varphi} (\text{Aut}(\text{tors}(G)) \times \text{Aut}(G/\text{tors}(G)))\,,}$$

*όπου* $\text{Hom}(G/\text{tors}(G),\text{tors}(G)) \cong (\text{tors}(G))^r$, $r := \text{rank}_{\mathbb{Z}}(G/\text{tors}(G)) \in \mathbb{N}_0$, *και για*[98] $r \geq 1$ *το ανωτέρω εξωτερικό ημιευθύ γινόμενο είναι αυτό που κατασκευάζεται με τη βοήθεια τού ομομορφισμού*

$$\varphi : \text{Aut}(\text{tors}(G)) \times \text{Aut}(G/\text{tors}(G)) \longrightarrow \text{Aut}(\text{Hom}(G/\text{tors}(G), \text{tors}(G))),$$

$$(\vartheta_1, \vartheta_2) \longmapsto \varphi_{(\vartheta_1,\vartheta_2)},$$

$$\text{Hom}(G/\text{tors}(G), \text{tors}(G)) \ni \theta \longmapsto \varphi_{(\vartheta_1,\vartheta_2)}(\theta) := \vartheta_1 \circ \theta \circ \vartheta_2,$$

[97] Ο εν λόγω ισομορφισμός προκύπτει από τη βραχεία ακριβή ακολουθία

$$0 \longrightarrow \text{Hom}(G/\text{tors}(G), \text{tors}(G)) \longrightarrow \text{Aut}(G) \longrightarrow \text{Aut}(\text{tors}(G)) \times \text{Aut}(G/\text{tors}(G)) \longrightarrow 0.$$

Βλ. Corollary 6, σελ. 411, στο άρθρο των M. Golasiński & D.L. Gonçalves: *On automorphisms of finite abelian p-groups*, Mathematica Solvaca **58** (2008), 405-412.

[98] Εάν $r = 0$, τότε $G = \text{tors}(G) \Rightarrow \text{Aut}(G) = \text{Aut}(\text{tors}(G))$.

*τού υλοποιούμενου μέσω τού μεταθετικού διαγράμματος*

$$\begin{tikzcd} \mathrm{tors}(G) \arrow[r, "\vartheta_1"] & \mathrm{tors}(G) \\ G/\mathrm{tors}(G) \arrow[u, "\theta"] \arrow[ur, phantom, "\circlearrowleft"] & G/\mathrm{tors}(G) \arrow[l, "\vartheta_2"] \arrow[u, "\varphi_{(\vartheta_1,\vartheta_2)}(\theta)"'] \end{tikzcd}$$

*και τού θεσπίζοντος, ως εκ τούτου, την εσωτερική πράξη*

$$\big((\theta,(\vartheta_1,\vartheta_2)),(\theta',(\vartheta_1',\vartheta_2'))\big) \longmapsto (\theta\circ\varphi_{(\vartheta_1,\vartheta_2)}(\theta'),(\vartheta_1\circ\vartheta_1',\vartheta_2\circ\vartheta_2')).$$

# $\boxed{9.7}$ ΔΙΑΙΡΕΤΕΣ ΚΑΙ ΑΝΗΓΜΕΝΕΣ ΑΒΕΛΙΑΝΕΣ ΟΜΑΔΕΣ

*Κάθε* αβελιανή ομάδα $(G,+)$ διασπάται σε ένα *διαιρετό μέρος* $\mathrm{div}(G)$ και σε ένα *ανηγμένο μέρος*. (Βλ. θεώρημα 9.7.40.) Το πρώτο εξ αυτών μπορεί να θεωρηθεί ως γνωστό, διότι οι *διαιρετές* αβελιανές ομάδες είναι πλήρως περιγράψιμες μέχρις ισομορφισμού (μέσω τού θεωρήματος 9.7.35). Ως προς το δεύτερο, σε ό,τι αφορά στις μη πεπερασμένως παραγόμενες *ανηγμένες* αβελιανές ομάδες, περιοριζόμαστε στην παράθεση μόνον κάποιων χαρακτηριστικών παραδειγμάτων. Ωστόσο, αξίζει να επισημανθεί ότι *κάθε* αβελιανή ομάδα είναι εμφυτεύσιμη εντός κάποιας διαιρετής. (Βλ. θεώρημα 9.7.19.)

**9.7.1 Ορισμός.** Έστω $(G,+)$ μια αβελιανή ομάδα. Λέμε ότι ένα στοιχείο $g\in G$ είναι **διαιρετό** όταν για κάθε $n\in\mathbb{N}$ υπάρχει $x\in G$, τέτοιο ώστε να ισχύει $g=nx$. Το σύνολο

$$\boxed{\mathrm{Div}(G) := \{\, g\in G \,|\, g \text{ διαιρετό}\} = \bigcap_{n\in\mathbb{N}} nG,} \tag{9.69}$$

ως τομή υποομάδων, αποτελεί μια υποομάδα τής $G$.

**9.7.2 Πρόταση.** *Για μια αβελιανή ομάδα $(G,+)$ οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) $\mathrm{Div}(G)=G$.

(ii) $nG=G$, $\forall n\in\mathbb{N}$.

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από την ισότητα (9.69). □

**9.7.3 Ορισμός.** Μια αβελιανή ομάδα $(G,+)$ καλείται **διαιρετή** όταν γι' αυτήν ικανοποιούνται οι συνθήκες τής προτάσεως 9.7.2.

**9.7.4 Παραδείγματα.** (i) Η αβελιανή ομάδα $(\mathbb{Q},+)$ είναι διαιρετή. (Πράγματι· για κάθε $n\in\mathbb{N}$ και για κάθε $q=\frac{a}{b}\in\mathbb{Q}$, όπου $a\in\mathbb{Z}, b\in\mathbb{Z}\smallsetminus\{0\}$, έχουμε $q=nq'$, όπου $q':=\frac{a}{nb}\in\mathbb{Q}$.) Και γενικότερα, η προσθετική ομάδα $(F,+)$ οιουδήποτε σώματος

$(F, +, \cdot)$ χαρακτηριστικής μηδέν είναι διαιρετή.

(ii) Εν αντιθέσει προς ό,τι συμβαίνει με τις ελεύθερες αβελιανές ομάδες (βλ. θεώρημα 9.5.39), μια μη τετριμμένη υποομάδα μιας διαιρετής αβελιανής ομάδας δεν είναι κατ' ανάγκην διαιρετή. (Π.χ., η $(\mathbb{Q}, +)$ είναι διαιρετή, ενώ η $(\mathbb{Z}, +)$ δεν είναι[99].)

(iii) Κάθε μη τετριμμένη πεπερασμένη αβελιανή ομάδα είναι μη διαιρετή. (Πράγματι· εάν $(G, +)$ είναι μια διαιρετή αβελιανή ομάδα, τότε *για κάθε* $n \in \mathbb{N}$ έχουμε $G = nG \underset{9.1.4}{\cong} G/G[n]$, οπότε η $G[n] := \{x \in G \,|\, nx = 0_G\}$ είναι η τετριμμένη υποομάδα τής $G$. Αυτό σημαίνει είτε ότι η $G$ είναι τετριμμένη είτε ότι η $G$ περιέχει κάποιο στοιχείο άπειρης τάξεως.)

(iv) Κάθε μη τετριμμένη κυκλική ομάδα είναι μη διαιρετή (καθώς είναι είτε πεπερασμένη είτε $\cong \mathbb{Z}$).

(v) Η *πολλαπλασιαστική* αβελιανή ομάδα $(\mathbb{C} \smallsetminus \{0\}, \cdot)$ είναι διαιρετή, διότι κάθε μη μηδενικός μιγαδικός αριθμός διαθέτει $n$-οστές ρίζες[100] για κάθε $n \in \mathbb{N}$.

**9.7.5 Ορισμός.** Έστω $p$ ένας πρώτος αριθμός. Μια αβελιανή ομάδα $(G, +)$ καλείται $p$-**διαιρετή** όταν $p^k G = G$ για κάθε $k \in \mathbb{N}$.

**9.7.6 Πρόταση.** *Κάθε αβελιανή ομάδα $(G, +)$ με $pG = G$ (για κάποιον πρώτο αριθμό $p$) είναι $p$-διαιρετή.*

ΑΠΟΔΕΙΞΗ. Έστω $(G, +)$ μια αβελιανή ομάδα με $pG = G$. Προφανώς έχουμε $p^2 G = p(pG) = pG = G$. Εάν λοιπόν για $k \in \mathbb{N}, k \geq 3$, υποθέσουμε ότι $p^{k-1}G = G$, τότε $p^k G = p(p^{k-1}G) = pG = G$. Άρα η $G$ είναι $p$-διαιρετή. $\square$

**9.7.7 Παράδειγμα.** Η υποομάδα $\mathbb{Z}[\frac{1}{p}] := \left\{ \frac{a}{p^i} \,\middle|\, a \in \mathbb{Z}, i \in \mathbb{N}_0 \right\}$ τής $(\mathbb{Q}, +)$, όπου $p$ τυχών πρώτος αριθμός, είναι $p$-διαιρετή, διότι για κάθε στοιχείο $\frac{a}{p^i} \in \mathbb{Z}[\frac{1}{p}]$ έχουμε $\frac{a}{p^i} = p\left(\frac{a}{p^{i+1}}\right) \Rightarrow p\mathbb{Z}[\frac{1}{p}] = \mathbb{Z}[\frac{1}{p}]$. Ωστόσο, δεν είναι διαιρετή! (Βλ. εδ. 9.7.47.)

**9.7.8 Πρόταση.** *Μια αβελιανή ομάδα $(G, +)$ είναι διαιρετή εάν και μόνον εάν είναι $p$-διαιρετή για κάθε πρώτον αριθμό $p$.*

ΑΠΟΔΕΙΞΗ. Εάν η $G$ είναι διαιρετή, τότε είναι (εξ ορισμού) $p$-διαιρετή για κάθε πρώτον αριθμό $p$. Και αντιστρόφως· εάν η $G$ είναι $p$-διαιρετή για κάθε πρώτον αριθμό $p$, $n \in \mathbb{N}, n \geq 2$, και $n = p_1^{\nu_1} p_2^{\nu_2} \cdots p_\kappa^{\nu_\kappa}$ ($\kappa \in \mathbb{N}$, $\nu_1, \ldots, \nu_\kappa \in \mathbb{N}$) η κανονική παράσταση (B.19) τού $n$ ως γινομένου (κατάλληλων δυνάμεων) πρώτων αριθμών $p_1, \ldots, p_\kappa$, τότε $nG = (p_1^{\nu_1} \cdots p_{\kappa-1}^{\nu_{\kappa-1}})(p_\kappa^{\nu_\kappa} G) = (p_1^{\nu_1} \cdots) \, p_{\kappa-1}^{\nu_{\kappa-1}} G = \cdots = p_1^{\nu_1} G = G$, οπότε η $G$ είναι διαιρετή. $\square$

► **Κύριες ιδιότητες των διαιρετών αβελιανών ομάδων**. Αυτές διατυπώνονται στις προτάσεις 9.7.9, 9.7.14 και 9.7.27 και στα πορίσματά τους, καθώς και στο θεώρημα

[99] Π.χ., $1 \in \mathbb{Z}$, $2 \in \mathbb{N}$ αλλά $\nexists x \in \mathbb{Z} : 1 = 2x$.

[100] Εάν $w \in \mathbb{C} \smallsetminus \{0\}$, τότε η $z^n = w$ διαθέτει ακριβώς $n$ λύσεις. (Συγκεκριμένα, εάν $w = r(\cos(\theta) + i\sin(\theta))$, $r \in \mathbb{R}_{>0}$, $\theta \in \mathbb{R}$, τότε αυτές είναι οι $z_j = r^{\frac{1}{n}}(\cos(\frac{2j\pi+\theta}{n}) + i\sin(\frac{2j\pi+\theta}{n}))$, $j \in \{0, \ldots, n-1\}$.)

9.7.19, μέσω τού οποίου διασφαλίζεται η εμφυτευσιμότητα *οιασδήποτε* αβελιανής ομάδας σε κάποια διαιρετή.

**9.7.9 Πρόταση.** *Εάν $f : G \longrightarrow H$ είναι ένας ομομορφισμός μεταξύ (προσθετικών) αβελιανών ομάδων και η $G$ διαιρετή, τότε και η εικόνα αυτής $f(G) = \mathrm{Im}(f)$ μέσω τού $f$ είναι διαιρετή.*

ΑΠΟΔΕΙΞΗ. Έστω $h \in \mathrm{Im}(f)$ και έστω $n \in \mathbb{N}$. Τότε υπάρχει $g \in G$, τέτοιο ώστε να ισχύει $h = f(g)$. Εξ υποθέσεως, $\exists x \in G : g = nx$. Κατά συνέπειαν, $h = nf(x)$. □

**9.7.10 Πόρισμα.** *Εάν $(G, +)$ είναι μια διαιρετή αβελιανή ομάδα και $H \in \mathbf{Subg}(G)$, τότε η πηλικοομάδα $G/H$ είναι διαιρετή.*

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμοσθεί η πρόταση 9.7.9 για τον φυσικό επιμορφισμό $\pi_H^G : G \longrightarrow G/H$. □

**9.7.11 Παραδείγματα.** Οι αβελιανές ομάδες $(\mathbb{R}/\mathbb{Z}, +)$ και $(\mathbb{Q}/\mathbb{Z}, +)$ είναι διαιρετές.

**9.7.12 Πόρισμα.** *Εάν $(G, +)$ είναι μια διαιρετή αβελιανή ομάδα, τότε και κάθε ομάδα, η οποία είναι ισόμορφη με αυτήν, είναι διαιρετή.*

**9.7.13 Παραδείγματα.** Οι πολλαπλασιαστικές αβελιανές ομάδες $(\mathbb{S}^1, \cdot)$ και $(\mathcal{E}_\infty, \cdot)$ (βλ. 2.1.21 (vi) και 2.3.6) είναι διαιρετές, διότι $\mathbb{R}/\mathbb{Z} \cong \mathbb{S}^1$ και $\mathbb{Q}/\mathbb{Z} \cong \mathcal{E}_\infty$. (Βλ. το (ii) τού εδ. 4.5.3 και την άσκηση **4-42**.)

**9.7.14 Πρόταση.** *Έστω $(G_i)_{i\in I}$ μια οικογένεια (προσθετικών) αβελιανών ομάδων $(I \neq \varnothing)$. Εάν $G := \bigoplus_{i\in I} G_i$ (και αντιστοίχως, εάν $G := \bigoplus_{i\in I}^{\text{περ.}} G_i$) τότε*

$$\mathrm{Div}(G) = \bigoplus\nolimits_{i\in I} \mathrm{Div}(G_i) \ \ (\text{και αντιστοίχως, } \mathrm{Div}(G) = \bigoplus\nolimits_{i\in I}^{\text{περ.}} \mathrm{Div}(G_i)).$$

*Άρα η $G$ είναι διαιρετή εάν και μόνον εάν η $G_i$ είναι διαιρετή για κάθε $i \in I$.*

ΑΠΟΔΕΙΞΗ. Εάν $G := \bigoplus_{i\in I} G_i$, $g = (g_i)_{i\in I} \in \mathrm{Div}(G)$ και $n \in \mathbb{N}$, τότε υπάρχει $x = (x_i)_{i\in I} \in G$, τέτοιο ώστε να ισχύει $g = nx$ ή, ισοδυνάμως, $g_i = nx_i$ για κάθε $i \in I$, οπότε $[g_i \in \mathrm{Div}(G_i), \forall i \in I] \Rightarrow g \in \bigoplus_{i\in I} \mathrm{Div}(G_i)$. Και αντιστρόφως· εάν $g = (g_i)_{i\in I} \in \bigoplus_{i\in I} \mathrm{Div}(G_i)$ και $n \in \mathbb{N}$, τότε υπάρχει στοιχείο $x_i \in G_i$, τέτοιο ώστε να ισχύει $g_i = nx_i$ για κάθε $i \in I$, οπότε το $x := (x_i)_{i\in I} \in G$ ικανοποιεί την $g = nx$ και $g \in \mathrm{Div}(G)$. Άρα $\mathrm{Div}(G) = \bigoplus_{i\in I}\mathrm{Div}(G_i)$. Εάν υποθέσουμε ότι η $G_i$ είναι διαιρετή για κάθε $i \in I$, τότε

$$[\mathrm{Div}(G_i) = G_i, \ \forall i \in I] \Rightarrow \mathrm{Div}(G) = \bigoplus_{i\in I} \mathrm{Div}(G_i) = \bigoplus_{i\in I} G_i = G,$$

οπότε και η $G$ είναι διαιρετή. Και αντιστρόφως· εάν υποθέσουμε ότι η $G$ είναι διαιρετή και ότι υπάρχει $j \in I$ με $\mathrm{Div}(G_j) \sqsubset G_j$, τότε καταλήγουμε σε άτοπο, καθώς

$$G = \mathrm{Div}(G) = \left( \bigoplus_{i\in I\setminus\{j\}} \mathrm{Div}(G_i) \right) \oplus \mathrm{Div}(G_j) \sqsubset \bigoplus_{i\in I} G_i = G.$$

Άρα η $G_i$ είναι διαιρετή για κάθε $i \in I$. (Στην περίπτωση όπου $G := \bigoplus_{i\in I}^{\text{περ.}} G_i$ η απόδειξη είναι παρόμοια.) □

**9.7.15 Παραδείγματα.** Τόσον οι $(\mathbb{Q}^X,+)$, $(\mathbb{R}^X,+)$, $(\mathbb{Z}(p^\infty)^X,+)$, $((\mathbb{R}/\mathbb{Z})^X,+)$ και $((\mathbb{Q}/\mathbb{Z})^X,+)$ όσον και οι

$$(\mathbb{Q}^{(X)},+),\ (\mathbb{R}^{(X)},+),\ (\mathbb{Z}(p^\infty)^{(X)},+), ((\mathbb{R}/\mathbb{Z})^{(X)},+)\ \text{και}\ ((\mathbb{Q}/\mathbb{Z})^{(X)},+)$$

(καθώς *και* το ευθύ άθροισμα οιωνδήποτε εξ αυτών) είναι διαιρετές αβελιανές ομάδες *για κάθε σύνολο* $X$.

**9.7.16 Πόρισμα.** *Ας υποθέσουμε ότι $I$ είναι ένα μη κενό σύνολο και $(H_i)_{i\in I}$ μια οικογένεια υποομάδων μιας αβελιανής ομάδας $(G,+)$, με τους δείκτες της ειλημμένους από το $I$, τέτοια ώστε να ισχύει $G = \bigoplus_{i\in I}^{\text{εσ.}} H_i$. Τότε η $G$ είναι διαιρετή εάν και μόνον εάν η $H_i$ είναι διαιρετή για κάθε $i \in I$.*

ΑΠΟΔΕΙΞΗ. Επειδή $G \underset{7.1.100\,(ii)}{\cong} \bigoplus_{i\in I}^{\text{περ.}} H_i$, τούτο έπεται από την πρόταση 9.7.14 και το πόρισμα 9.7.12. □

**9.7.17 Πόρισμα.** *Εάν $p$ είναι ένας πρώτος αριθμός, τότε η $p$-σχεδόν κυκλική ομάδα*

$$\boxed{\mathbb{Z}(p^\infty) := \mathbb{Z}[\tfrac{1}{p}]/\mathbb{Z} = \left\{ \tfrac{a}{p^i} + \mathbb{Z} \;\middle|\; a \in \mathbb{Z}, i \in \mathbb{N}_0 \right\} \sqsubset \mathbb{Q}/\mathbb{Z}}$$

(πρβλ. άσκηση **4-41**) *είναι διαιρετή.*

ΑΠΟΔΕΙΞΗ[101]. Ως γνωστόν, η $(\mathbb{Q}/\mathbb{Z},+)$ είναι ομάδα στρέψεως. (Βλ. 4.4.11.) Άρα

$$\mathbb{Q}/\mathbb{Z} \underset{(9.55)}{=} \bigoplus\nolimits^{\text{εσ.}}_{p\ \text{πρώτος}} (\mathbb{Q}/\mathbb{Z})(p) = \bigoplus\nolimits^{\text{εσ.}}_{p\ \text{πρώτος}} \mathbb{Z}(p^\infty),$$

διότι η $p$-πρωτεύουσα συνιστώσα τής $\mathbb{Q}/\mathbb{Z}$ είναι η

$$\begin{aligned}(\mathbb{Q}/\mathbb{Z})(p) &:= \{\, q+\mathbb{Z} \in \mathbb{Q}/\mathbb{Z} |\, q \in \mathbb{Q} \text{ και } p^i(q+\mathbb{Z}) = \mathbb{Z} \text{ για κάποιον } i \in \mathbb{N}_0 \} \\ &= \{\, q+\mathbb{Z} \in \mathbb{Q}/\mathbb{Z} |\, q \in \mathbb{Q} \text{ και } p^i q = a \text{ για κάποιους } a \in \mathbb{Z} \text{ και } i \in \mathbb{N}_0 \} \\ &= \left\{ \tfrac{a}{p^i} + \mathbb{Z} \;\middle|\; a \in \mathbb{Z}, i \in \mathbb{N}_0 \right\} = \mathbb{Z}(p^\infty)\end{aligned}$$

για κάθε πρώτον αριθμό $p$. Επειδή η $(\mathbb{Q}/\mathbb{Z},+)$ είναι διαιρετή, η $(\mathbb{Z}(p^\infty),+)$ είναι ωσαύτως διαιρετή για κάθε πρώτον αριθμό $p$ (βάσει τού πορίσματος 9.7.16). □

**9.7.18 Πόρισμα.** *Κάθε μη τετριμμένη διαιρετή αβελιανή ομάδα είναι μη πεπερασμένως παραγόμενη.*

ΑΠΟΔΕΙΞΗ. Έστω $(G,+)$ μια πεπερασμένως παραγόμενη διαιρετή αβελιανή ομάδα. Τότε $G \cong \text{tors}(G) \oplus \mathbb{Z}^r$, όπου $r \in \mathbb{N}_0$ και $|\text{tors}(G)| < \infty$. (Βλ. θεώρημα 9.6.7.) Σύμφωνα με την πρόταση 9.7.14 αμφότερες οι $\text{tors}(G)$ και $\mathbb{Z}^r$ οφείλουν να είναι διαιρετές. Αυτό σημαίνει ότι $\text{tors}(G) = \{0_G\}$ (βλ. 9.7.4 (iii)) και ότι $r = 0$. (Ο $r$, εκ νέου λόγω τής προτάσεως 9.7.14, δεν μπορεί να είναι $\geq 1$, διότι η $(\mathbb{Z},+)$ δεν είναι διαιρετή.) Άρα και η ίδια η $G$ είναι τετριμμένη. □

[101]Επειδή η $\mathbb{Z}[\frac{1}{p}]$ δεν είναι διαιρετή (βλ. 9.7.47), για την απόδειξη τού ότι η πηλικοομάδα $\mathbb{Z}(p^\infty) := \mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ είναι διαιρετή δεν είναι δυνατόν να εφαρμοσθεί το πόρισμα 9.7.10.

**9.7.19 Θεώρημα.** *Κάθε αβελιανή ομάδα $(G, +)$ είναι εμφυτεύσιμη εντός μιας διαιρετής αβελιανής ομάδας.*

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το θεώρημα 9.5.35, $G \cong \mathbb{Z}^{(X)}/\mathrm{Ker}(f)$, όπου $X \subseteq G$ είναι οιοδήποτε σύστημα γεννητόρων τής $G$ και $f : \mathbb{Z}^{(X)} \longrightarrow G$ επιμορφισμός. Έστω $\iota : \mathbb{Z}^{(X)} \hookrightarrow \mathbb{Q}^{(X)}$ η συνήθης ένθεση. Ο επαγόμενος ομομορφισμός $\iota^{\text{πηλ.}} : \mathbb{Z}^{(X)}/\mathrm{Ker}(f) \longrightarrow \mathbb{Q}^{(X)}/\mathrm{Ker}(f)$ (σε επίπεδο πηλικοομάδων, βλ. 4.5.5) είναι μονομορφισμός. Επειδή η $\mathbb{Q}^{(X)}$ είναι διαιρετή, *και* η πηλικοομάδα $\mathbb{Q}^{(X)}/\mathrm{Ker}(f)$ (εντός τής οποίας εμφυτεύεται η $G$) είναι διαιρετή. (Βλ. πόρισμα 9.7.10.) $\square$

► «**Διαιρετή = εμβολική**». Στο εδάφιο 9.5.41 εδόθη ο ορισμός τής *προβολικής* αβελιανής ομάδας και στο θεώρημα 9.5.42 απεδείχθη ότι οι έννοιες *ελεύθερη* και *προβολική* αβελιανή ομάδα είναι ισοδύναμες. Το ίδιο συμβαίνει και με τις έννοιες *διαιρετή* και *εμβολική*, όπου η τελευταία είναι *δυϊκή* (τρόπον τινά[102]) τής *προβολικής*. (Βλ. θεώρημα 9.7.22.)

**9.7.20 Ορισμός.** Λέμε ότι μια αβελιανή ομάδα $(G, +)$ είναι **εμβολική** όταν για κάθε μονομορφισμό αβελιανών ομάδων $\beta : H \hookrightarrow K$ και για κάθε $\theta \in \mathrm{Hom}(H, G)$ υπάρχει $f \in \mathrm{Hom}(K, G)$ που καθιστά το ακόλουθο διάγραμμα μεταθετικό.

$$\begin{tikzcd}
& G & \\
H \arrow[ur, "\theta"] \arrow[rr, hook, "\beta"'] & \arrow[u, phantom, "\circlearrowleft"] & K \arrow[ul, dashed, "f"']
\end{tikzcd}$$

**9.7.21 Θεώρημα.** (**Κριτήριο τού R. Baer,** 1940.) *Για μια αβελιανή ομάδα $(G, +)$ οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Η $G$ είναι εμβολική.*

(ii) *Για κάθε υποομάδα $M$ τής ομάδας $(\mathbb{Z}, +)$ και κάθε $\psi \in \mathrm{Hom}(M, G)$ υπάρχει $\varphi \in \mathrm{Hom}(\mathbb{Z}, G)$, ούτως ώστε να ισχύει $\varphi|_M = \psi$ (ή, ισοδυνάμως, $\varphi \circ \iota = \psi$, όπου $\iota : M \hookrightarrow \mathbb{Z}$ η συνήθης ένθεση).*

ΑΠΟΔΕΙΞΗ[103]. (i)⇒(ii) Τούτο είναι προφανές από τον ορισμό 9.7.20. (Αρκεί σε αυτόν να τεθεί $H := M$, $K := \mathbb{Z}$ και $\beta, \theta$ και $f$ αντί των $\iota, \psi$ και $\varphi$, αντιστοίχως.)

(ii)⇒(i) Έστω $\beta : H \hookrightarrow K$ ένας μονομορφισμός (προσθετικών) αβελιανών ομάδων και έστω $\theta \in \mathrm{Hom}(H, G)$. Θα δείξουμε ότι υπάρχει κάποιος $f \in \mathrm{Hom}(K, G)$ με $f \circ \beta = \theta$. Ας συμβολίσουμε ως $\widehat{\beta} : H \xrightarrow{\cong} \mathrm{Im}(\beta)$ τον ισομορφισμό τον προκύπτοντα ύστερα από περιορισμό τού πεδίου τιμών τού $\beta$ επί τής $\mathrm{Im}(\beta)$.

*Περίπτωση πρώτη.* Εάν $\mathrm{Im}(\beta) = K$, τότε $\widehat{\beta} = \beta$ και αρκεί να τεθεί $f := \theta \circ \beta^{-1}$.

[102] Εάν στο μεταθετικό διάγραμμα τού εδαφίου 9.5.41 αντικαταστήσουμε τον επιμορφισμό $\beta$ με μονομορφισμό, εναλλάξουμε τους $f$ και $\theta$ και *αντιστρέψουμε* τη φορά των βελών, τότε αποκτούμε το μεταθετικό διάγραμμα τού εδαφίου 9.7.20.

[103] Βλ. R. Baer: *Abelian groups that are direct summands of every containing abelian group*, Bulletin of the American Math. Soc. **46** (1940), 800-806.

*Περίπτωση δεύτερη.* Εάν $\mathrm{Im}(\beta) \sqsubset K$, τότε θεωρούμε την οικογένεια ζευγών

$$\mathcal{L} := \left\{ (L, f_L) \,\middle|\, \mathrm{Im}(\beta) \sqsubseteq L \sqsubseteq K, \text{ όπου } f_L \in \mathrm{Hom}\,(L, G) : f_L \circ j_L \circ \widehat{\beta} = \theta \right\},$$

με

$$j_L : \mathrm{Im}(\beta) \hookrightarrow L,\ \beta\,(h) \longmapsto j_L(\beta\,(h)) := \beta\,(h)\,,\ \forall h \in H.$$

Αυτή είναι μη κενή (διότι προφανώς $(\mathrm{Im}(\beta), \theta \circ \widehat{\beta}^{-1}) \in \mathcal{L}$) και καθίσταται μερικώς διατεταγμένο σύνολο ως προς την ακόλουθη "$\preceq$":

$$(L_1, f_{L_1}) \preceq (L_2, f_{L_2}) \underset{\text{ορσ}}{\Longleftrightarrow} [L_1 \subseteq L_2 \text{ και } f_{L_2}|_{L_1} = f_{L_1}].$$

Για κάθε αλυσίδα $(L_\lambda, f_{L_\lambda})_{\lambda \in \Lambda}$ τού $(\mathcal{L}, \preceq)$ το ζεύγος $(\langle \{ L_\lambda |\, \lambda \in \Lambda \} \rangle, \Phi)$ με[104] $\Phi|_{L_\lambda} = f_{L_\lambda}$ είναι ένα άνω φράγμα αυτής, οπότε το $(\mathcal{L}, \preceq)$ είναι επαγωγικώς διατεταγμένο. Δυνάμει τού λήμματος A.2.20 τού Zorn το $(\mathcal{L}, \preceq)$ διαθέτει κάποιο μεγιστικό στοιχείο $(L_\bullet, f_{L_\bullet})$. Αρκεί λοιπόν να αποδείξουμε ότι $L_\bullet = K$. Θα χρησιμοποιήσουμε «εις άτοπον απαγωγή». Υποθέτουμε ότι $L_\bullet \sqsubset K$, επιλέγουμε ένα $x \in K \smallsetminus L_\bullet$ και θεωρούμε την $M := \{ n \in \mathbb{Z} |\, nx \in L_\bullet \} \sqsubset \mathbb{Z}$. Εν συνεχεία, ορίζουμε την απεικόνιση

$$\psi : M \longrightarrow G,\ n \longmapsto \psi(n) := f_{L_\bullet}(nx)$$

και παρατηρούμε ότι $\psi \in \mathrm{Hom}(M, G)$, διότι για οιουσδήποτε $n_1, n_2 \in M$ έχουμε

$$\psi(n_1 + n_2) := f_{L_\bullet}((n_1 + n_2)x) = f_{L_\bullet}(n_1 x + n_2 x) = \psi(n_1) + \psi(n_2).$$

Εξ υποθέσεως υπάρχει $\varphi \in \mathrm{Hom}(\mathbb{Z}, G)$, ούτως ώστε να ισχύει $\varphi \circ \iota = \psi$, όπου $\iota : M \hookrightarrow \mathbb{Z}$ η συνήθης ένθεση. Επιπροσθέτως, εάν θέσουμε $\widetilde{L}_\bullet := L_\bullet + \langle x \rangle$, η

$$f_{\widetilde{L}_\bullet} : \widetilde{L}_\bullet \longrightarrow G,\ \ f_{\widetilde{L}_\bullet}(z + nx) :=\ f_{L_\bullet}(z) + \varphi(n),\ \forall z \in L_\bullet \text{ και } \forall n \in \mathbb{Z},$$

είναι καλώς ορισμένη απεικόνιση[105], διότι εάν $z + nx = z' + n'x$, τότε

$$\begin{aligned}
&(n - n')x = z' - z \in L_\bullet \Rightarrow n - n' \in M \\
&\Rightarrow\ f_{L_\bullet}(z') -\ f_{L_\bullet}(z) =\ f_{L_\bullet}(z' - z) = f_{L_\bullet}((n - n')x) = \psi(n - n') \\
&= \varphi(n - n') = \varphi(n) - \varphi(n') \Rightarrow\ f_{L_\bullet}(z) + \varphi(n) =\ f_{L_\bullet}(z') + \varphi(n').
\end{aligned}$$

Επίσης, για $z_1, z_2 \in L_\bullet$ και $n_1, n_2 \in \mathbb{Z}$ έχουμε

$$\begin{aligned}
&f_{\widetilde{L}_\bullet}((z_1 + z_2) + (n_1 + n_2)x) =\ f_{L_\bullet}(z_1 + z_2) + \varphi(n_1 + n_2) \\
&=\ f_{L_\bullet}(z_1) + f_{L_\bullet}(z_2) + \varphi(n_1)\ + \varphi(n_2) =\ f_{L_\bullet}(z_1) + \varphi(n_1) + f_{L_\bullet}(z_2) + \varphi(n_2) \\
&= f_{\widetilde{L}_\bullet}(z_1 + n_1 x) + f_{\widetilde{L}_\bullet}(z_2 + n_2 x) \Rightarrow f_{\widetilde{L}_\bullet} \in \mathrm{Hom}(\widetilde{L}_\bullet, G).
\end{aligned}$$

---

[104] Επειδή η $(L_\lambda, f_{L_\lambda})_{\lambda \in \Lambda}$ είναι αλυσίδα, ορίζεται πάντοτε «κοινή» επέκταση $\Phi$ των ομομορφισμών $f_{L_\lambda}$. (Εάν $z \in \langle \{ L_\lambda |\, \lambda \in \Lambda \} \rangle$, τότε $z \in L_\lambda$ για κάποιο $\lambda \in \Lambda$ και αρκεί να θέσουμε $\Phi(z) := f_{L_\lambda}(z)$.)

[105] Εν προκειμένω, το «τέχνασμα» στην απόδειξη έγκειται στην κατασκευή τής $f_{\widetilde{L}_\bullet}$ κατά τέτοιον τρόπο, ώστε οι τιμές της να συμπίπτουν με εκείνες που λαμβάνει η $f_{L_\bullet}$ *και* σε όποια πολλαπλάσια τού $x$ τυγχάνει να ορίζεται. Η $M$ δεν είναι τίποτε άλλο παρά η συλλογή αυτών των «κατάλληλων» ακεραίων συντελεστών.

Επειδή $f_{\widetilde{L}_\bullet}(z) = f_{L_\bullet}(z), \forall z \in L_\bullet$, συμπεραίνουμε ότι $f_{\widetilde{L}_\bullet}\big|_{L_\bullet} = f_{L_\bullet} \Rightarrow (\widetilde{L}_\bullet, f_{\widetilde{L}_\bullet}) \in \mathcal{L}$. Κατόπιν προσαρτήσεως τού $f_{\widetilde{L}_\bullet}$ το ακόλουθο διάγραμμα παραμένει μεταθετικό.

$$
\begin{tikzcd}
& & G & & \mathbb{Z} \arrow[ll, dashed, "\varphi"'] \\
& & & & M \arrow[u, "\iota"'] \arrow[llu, "\psi"'] \\
& \operatorname{Im}(\beta) \arrow[r, hook, "j_{L_\bullet}"] \arrow[ruu, "\theta\circ\widehat{\beta}^{-1}"] \arrow[rr, bend right, "j_{\widetilde{L}_\bullet}"'] & L_\bullet \arrow[r, hook] \arrow[uu, dashed, "f_{L_\bullet}"'] & \widetilde{L}_\bullet \arrow[luu, dashed, "f_{\widetilde{L}_\bullet}"'] \arrow[rd, hook] & \\
H \arrow[ru, "\widehat{\beta}"] \arrow[rruuu, "\theta"] \arrow[rrrr, hook, "\beta"'] & & & & K
\end{tikzcd}
$$

Προφανώς, $(L_\bullet, f_{L_\bullet}) \underset{\neq}{\preceq} (\widetilde{L}_\bullet, f_{\widetilde{L}_\bullet})$, κάτι που αντίκειται στη μεγιστικότητα τού $(L_\bullet, f_{L_\bullet})$ εντός τής $\mathcal{L}$. Άτοπο! Άρα $L_\bullet = K$ και αρκεί να τεθεί $f := f_K$. $\square$

**9.7.22 Θεώρημα.** *Μια αβελιανή ομάδα είναι διαιρετή εάν και μόνον εάν είναι εμβολική.*

ΑΠΟΔΕΙΞΗ. Έστω ότι $(G,+)$ είναι μια διαιρετή αβελιανή ομάδα, $M := d\mathbb{Z} = \langle d \rangle$ για κάποιον $d \in \mathbb{N}_0$ και $\psi \in \operatorname{Hom}(M,G)$. Τότε $\psi(d) \in G$ και $\exists x \in G : \psi(d) = dx$. Θεωρώντας τόν ομομορφισμό $\varphi_x : \mathbb{Z} \longrightarrow G,\ n \longmapsto \varphi_x(n) := nx$, παρατηρούμε ότι $\varphi_x(kd) = k\varphi_x(d) = k\psi(d) = \psi(kd)$ για κάθε $k \in \mathbb{Z}$. Κατά συνέπειαν, $\varphi_x|_M = \psi$, οπότε (μέσω τής συνεπαγωγής (ii)⇒(i) στο θεώρημα 9.7.21) η $G$ είναι εμβολική.

Και αντιστρόφως· υποθέτοντας ότι $(G,+)$ είναι μια εμβολική αβελιανή ομάδα, $g \in G$, $n \in \mathbb{N}$ και $M := n\mathbb{Z} = \langle n \rangle$ , ορίζουμε τον ομομορφισμό

$$\psi_g : M \longrightarrow G, kn \longmapsto \psi_g\,(kn) := kg,$$

κατασκευάζουμε (μέσω τής συνεπαγωγής (i)⇒(ii) στο θεώρημα 9.7.21) έναν ομομορφισμό $\varphi_g \in \operatorname{Hom}(\mathbb{Z}, G)$ με $\varphi_g\big|_M = \psi_g$ και, εν συνεχεία, θέτοντας $x := \varphi_g(1)$ διαπιστώνουμε ότι $g = \psi_g\,(n) = \varphi_g(n) = \varphi_g(n \cdot 1) = n\varphi_g(1) = nx$. Αυτό σημαίνει ότι η $G$ είναι διαιρετή. $\square$

**9.7.23 Πόρισμα.** *Εάν $(G,+)$ είναι μια αβελιανή ομάδα, τότε κάθε διαιρετή υποομάδα $H$ αυτής διαθέτει κάποιο συμπλήρωμα* (βλ. 7.6.42 (ii)), *ήτοι*

$$\exists K \in \mathbf{Subg}(G) : G = H \oplus_{\text{εσ.}} K.$$

ΑΠΟΔΕΙΞΗ. Επειδή η $H$ (ως διαιρετή) είναι (σύμφωνα με το θεώρημα 9.7.22) εμβολική, για τη συνήθη ένθεση $\iota : H \hookrightarrow G$ και για την ταυτοτική $\mathrm{id}_H : H \longrightarrow H$

υπάρχει (σύμφωνα με τον ορισμό[106] 9.7.20) κάποιος $f \in \mathrm{Hom}(G, H)$ που καθιστά το ακόλουθο διάγραμμα μεταθετικό.

$$\begin{tikzcd} & H & \\ H \arrow[ur, "\mathrm{id}_H"] \arrow[rr, hook, "\iota"'] \arrow[r, phantom, shift left=4ex, "\circlearrowleft"] & & G \arrow[ul, dashed, "f"'] \end{tikzcd}$$

Επομένως, $f \circ \iota = \mathrm{id}_H$ (ή, ισοδυνάμως, $f|_H = \mathrm{id}_H$) και, ως εκ τούτου, $\mathrm{Im}(f) = H$. Θέτοντας $K := \mathrm{Ker}(f)$ παρατηρούμε εν πρώτοις ότι $G = H + K$. Πράγματι· εάν $g \in G$ και $h := f(g)$, τότε

$$f(g) = h = \mathrm{id}_H(h) = (f \circ \iota)(h) = f(\iota(h)) = f(h) \Rightarrow f(g - h) = 0_G$$
$$\Rightarrow g - h \in K \Rightarrow [\exists k \in K : g = h + k] \Rightarrow G = H + K.$$

Εν συνεχεία διαπιστώνουμε ότι $H \cap K = \{0_G\}$. (Πράγματι· εάν $x \in H \cap K$, τότε έχουμε προφανώς $0_G = f(x) = f(\iota(x)) = \mathrm{id}_H(x) = x$, οπότε η $H \cap K$ είναι τετριμμένη.) Τελικό συμπέρασμα: $G = H \oplus_{\text{εσ.}} K$. $\square$

**9.7.24 Πόρισμα.** *Μια αβελιανή ομάδα είναι διαιρετή εάν και μόνον εάν είναι ευθύς προσθετέος οιασδήποτε αβελιανής ομάδας που την περιέχει.*

ΑΠΟΔΕΙΞΗ. Έστω $G$ μια αβελιανή ομάδα που περιέχεται σε κάποια αβελιανή ομάδα $(L, +)$. Εάν η $G$ είναι διαιρετή, τότε υπάρχει $K \sqsubseteq L$ με $L = G \oplus_{\text{εσ.}} K$. (Βλ. πόρισμα 9.7.23.) Και αντιστρόφως· εάν $G$ είναι μια αβελιανή ομάδα και υπάρχει $K \sqsubseteq L$ με $L = G \oplus_{\text{εσ.}} K$ για *κάθε* αβελιανή ομάδα $(L, +)$ για την οποία ισχύει $G \sqsubseteq L$, τότε μπορούμε (δυνάμει τού θεωρήματος 9.7.19) να υποθέσουμε ότι η $L$ είναι διαιρετή, οπότε και η $G$ είναι διαιρετή (ως ευθύς προσθετέος διαιρετής). $\square$

► **Διαιρετές υποομάδες**. Όπως έχει ήδη προαναφερθεί στο εδάφιο 9.7.4 (ii), μια μη τετριμμένη υποομάδα μιας διαιρετής αβελιανής ομάδας δεν είναι κατ' ανάγκην διαιρετή. Ωστόσο, μεταξύ εκείνων των υποομάδων που παραμένουν διαιρετές συγκαταλέγονται πάντοτε οι *αμιγείς* υποομάδες. (Μία εξ αυτών είναι η υποομάδα στρέψεως.) Επίσης, οι διαιρετές υποομάδες εμπεριέχονται σε μία και μόνον («μέγιστη») διαιρετή υποομάδα.

**9.7.25 Ορισμός.** Μια υποομάδα $H$ μιας αβελιανής υποομάδας $(G, +)$ καλείται **αμιγής υποομάδα** όταν[107] $H \cap nG = nH$, $\forall n \in \mathbb{N}$.

**9.7.26 Πρόταση.** *Κάθε αμιγής υποομάδα μιας διαιρετής αβελιανής ομάδας* $(G, +)$ *είναι διαιρετή.*

ΑΠΟΔΕΙΞΗ. Για αμιγείς $H \sqsubseteq G$ έχουμε $H = H \cap G = H \cap nG = nH$, $\forall n \in \mathbb{N}$. $\square$

[106] Εδώ εφαρμόζεται ο ορισμός 9.7.20 με τις $H, G, H$ στη θέση των σε αυτόν παρατεθεισών ομάδων $H, K$ και $G$, αντιστοίχως, και με $\beta := \iota$ και $\theta := \mathrm{id}_H$.

[107] Ο εγκλεισμός $nH \subseteq H \cap nG$ ισχύει *για κάθε* $H \sqsubseteq G$.

**9.7.27 Πόρισμα.** *Η υποομάδα στρέψεως* $\mathrm{tors}(G)$ *οιασδήποτε διαιρετής αβελιανής ομάδας* $(G,+)$ *είναι αμιγής και, ως εκ τούτου, διαιρετή.*

ΑΠΟΔΕΙΞΗ. Έστω $n \in \mathbb{N}$ και έστω $g \in \mathrm{tors}(G) \cap nG$. Τότε υπάρχει $x \in G : g = nx$. Εάν $\mathrm{ord}(g) = m$, τότε ισχύει $(mn)x = m(nx) = mg = 0_G \Rightarrow \mathrm{ord}(x) \leq mn$, οπότε $x \in \mathrm{tors}(G) \Rightarrow g \in nG$. □

**9.7.28 Συμβολισμός.** Εάν $(G,+)$ είναι μια αβελιανή ομάδα, τότε θέτουμε

$$\boxed{\mathrm{div}(G) := \langle \{ H \in \mathbf{Subg}(G) |\, H \text{ διαιρετή} \} \rangle \,.}$$

**9.7.29 Πρόταση.** *Η* $\mathrm{div}(G)$ *αποτελεί τη μέγιστη*[108] *διαιρετή υποομάδα τής* $G$.

ΑΠΟΔΕΙΞΗ. Για διευκόλυνσή μας ας συμβολίσουμε ως $(H_i)_{i\in I}$ την οικογένεια όλων των διαιρετών υποομάδων τής $G$ (όπου $I$ κατάλληλο σύνολο δεικτών). Επειδή η $G$ είναι αβελιανή, η συνθήκη (ii) τού λήμματος 7.1.99 ικανοποιείται αυτομάτως και η απεικόνιση $f_{(H_i)_{i\in I}} : \bigoplus_{i\in I}^{\text{περ.}} H_i \longrightarrow G$ (βλ. (7.31)) είναι (λόγω *και* τού (i) τού ίδιου λήμματος) ένας ομομορφισμός με εικόνα του την

$$\mathrm{Im}(f_{(H_i)_{i\in I}}) = \langle \{ H_i |\, i \in I \} \rangle =: \mathrm{div}(G).$$

Επειδή η $H_i$ είναι διαιρετή για κάθε $i \in I$, το περιορισμένο άθροισμα $\bigoplus_{i\in I}^{\text{περ.}} H_i$ είναι μια διαιρετή ομάδα (λόγω τής προτάσεως 9.7.14). Άρα η $\mathrm{div}(G)$, ούσα η εικόνα τού $f_{(H_i)_{i\in I}}$, είναι διαιρετή υποομάδα τής $G$. (Βλ. πρόταση 9.7.9.) Εξ ορισμού, η $\mathrm{div}(G)$ περιέχει όλες τις διαιρετές υποομάδες τής $G$. (Βλ. 2.2.2 (ii).) □

**9.7.30 Σημείωση.** (i) Είθισται να λέμε εν συντομία ότι η υποομάδα $\mathrm{div}(G)$ αποτελεί το **διαιρετό μέρος** τής $G$.

(ii) Ο εγκλεισμός $\mathrm{div}(G) \subseteq \mathrm{Div}(G)$ ενδέχεται να είναι αυστηρός[109]. (Φυσικά, η ίδια η $G$ είναι διαιρετή $\Leftrightarrow \mathrm{div}(G) = \mathrm{Div}(G) = G$.)

**9.7.31 Πρόταση.** *Εάν* $f : G_1 \longrightarrow G_2$ *είναι ένας ομομορφισμός (προσθετικών) αβελιανών ομάδων, τότε* $f(\mathrm{div}(G_1)) \sqsubseteq \mathrm{div}(G_2)$ *και, ως εκ τούτου, ορίζεται καλώς ο «κανονιστικός» ομομορφισμός*

$$f^{\text{πηλ.}} : G_1/\mathrm{div}(G_1) \longrightarrow G_2/\mathrm{div}(G_2)$$

$$g + \mathrm{div}(G_1) \longmapsto f^{\text{πηλ.}}(g + \mathrm{div}(G_1)) := f(g) + \mathrm{div}(G_2),$$

*ο οποίος καθιστά το διάγραμμα*

$$\begin{tikzcd} G_1 \arrow[r, "f"] \arrow[d, "\pi^{G_1}_{\mathrm{div}(G_1)}"'] \arrow[dr, phantom, "\circlearrowleft"] & G_2 \arrow[d, "\pi^{G_2}_{\mathrm{div}(G_2)}"] \\ G_1/\mathrm{div}(G_1) \arrow[r, dashed, "f^{\text{πηλ.}}"'] & G_2/\mathrm{div}(G_2) \end{tikzcd}$$

[108]Εδώ, «μέγιστη» = «μοναδική μεγιστική» ως προς την "$\sqsubseteq$" με την εν λόγω ιδιότητα. (Πρβλ. 2.1.36.)

[109]Για την κατασκευή ενός (δύσκολου) παραδείγματος μιας $G$ με $\mathrm{div}(G) \subsetneqq \mathrm{Div}(G)$ βλ. Hofmann K.H. & Morris S.A.: *The Structure of Compact Groups*, second ed., De Gruyter Studies in Mathematics, Vol. 25, Walter de Gruyter, 2006, Thm. A1.32, σελ. 652-654.

*μεταθετικό. Επιπροσθέτως, ισχύουν τα ακόλουθα:*

(a) *Ο* $f^{\text{πηλ.}}$ *είναι μονομορφισμός* $\Longleftrightarrow \text{div}(G_1) = f^{-1}(\text{div}(G_2))$.

(b) *Ο* $f^{\text{πηλ.}}$ *είναι επιμορφισμός* $\Longleftrightarrow \text{Im}(f) + \text{div}(G_2) = G_2$.

ΑΠΟΔΕΙΞΗ. Εάν $H$ είναι μια διαιρετή υποομάδα τής $G_1$, τότε η εικόνα της $f|_H(H) = f(H)$ μέσω τού $f|_H : H \longrightarrow G_2$ είναι διαιρετή υποομάδα τής $G_2$ (βλ. 9.7.9 και 2.4.4 (i)), οπότε

$$\begin{aligned} f(\text{div}(G_1)) &= \langle \{ f(H) \in \mathbf{Subg}(G_2) \,|\, H \in \mathbf{Subg}(G_1) \text{ διαιρετή} \} \rangle \\ &\sqsubseteq \langle \{ L \in \mathbf{Subg}(G_2) \,|\, L \text{ διαιρετή} \} \rangle = \text{div}(G_2). \end{aligned}$$

Οι λοιποί ισχυρισμοί είναι αληθείς δυνάμει τού θεωρήματος 4.5.5. □

► **Διαιρετές αβελιανές ομάδες στρέψεως**. Το θεώρημα 9.7.33 μας πληροφορεί ότι αυτές «οικοδομούνται» με τη βοήθεια τής οικογενείας $\{ (\mathbb{Z}(p^\infty), +) \,|\, p \text{ πρώτος} \}$.

**9.7.32 Λήμμα.** *Κάθε διαιρετή αβελιανή p-ομάδα στρέψεως (p πρώτος) είναι ισόμορφη με την* $(\mathbb{Z}(p^\infty)^{(X)}, +)$ *για κάποιο (κατάλληλο) σύνολο* $X$.

ΑΠΟΔΕΙΞΗ. Έστω $(G, +)$ μια διαιρετή αβελιανή $p$-ομάδα. Εάν η $G$ είναι τετριμμένη, τότε ο ισχυρισμός είναι προδήλως αληθής. Ας υποθέσουμε ότι $\{0_G\} \sqsubset G$.

**Βήμα 1ο**. Επειδή η $G[p] := \{ g \in G \,|\, pg = 0_G \} \sqsubseteq G$ (σύμφωνα με τα προαναφερθέντα στο εδάφιο 9.1.5 (i)) είναι εφοδιασμένη με τη δομή διανυσματικού χώρου υπεράνω τού σώματος $\mathbb{Z}_p$, μπορούμε να θεωρήσουμε μια *βάση* αυτού $X \subseteq G[p]$ (υπό τη συνήθη έννοια). Για *κάθε* $x \in X$ κατασκευάζουμε μια ακολουθία στοιχείων τής $G$ ως ακολούθως: Θέτουμε $x_0 := 0_G$ και $x_1 := x$. (Προφανώς, το $x$, ως στοιχείο τής βάσεως $X$, είναι $\neq 0_G$. Από την άλλη μεριά, $x \in G[p] \Rightarrow px = 0_G$.) Επειδή (εξ υποθέσεως) η $G$ είναι διαιρετή, έχουμε[110] $pG = G$, οπότε $\exists x_2 \in G : px_2 = x_1$. Εν συνεχεία, επαναλαμβάνοντας αυτήν τη διαδικασία (με το $x_2$ στη θέση τού $x_1$ κ.ο.κ.) επιλέγουμε $x_3, x_4, ....$ με $px_i = x_{i-1}$ για κάθε $i \in \mathbb{N}$. Εάν $a, a' \in \mathbb{Z}$ και $i, i' \in \mathbb{N}_0$ είναι τέτοιοι, ώστε να ισχύει $\frac{a}{p^i} = \frac{a'}{p^{i'}}$ (εντός τής $\mathbb{Z}[\frac{1}{p}]$) και υποθέσουμε (δίχως βλάβη τής γενικότητας) ότι $i \leq i'$, τότε

$$\begin{aligned} &[ap^{i'-i} = a'] \Rightarrow a'x_{i'} = ap^{i'-i}x_{i'} = ap^{i'-i-1}x_{i'-1} \\ &= ap^{i'-i-2}x_{i'-2} = \cdots = ap^{i'-i-(i'-i-1)}x_{i'-(i'-i-1)} = apx_{i+1} = ax_i, \end{aligned}$$

οπότε ορίζεται καλώς η απεικόνιση

$$f_x : \mathbb{Z}[\tfrac{1}{p}] \longrightarrow G, \ \tfrac{a}{p^i} \longmapsto f_x(\tfrac{a}{p^i}) := ax_i.$$

Αυτή είναι ομομορφισμός ομάδων, διότι για $\frac{a}{p^i}, \frac{b}{p^j} \in \mathbb{Z}[\frac{1}{p}]$ με $i \leq j$,

$$\begin{aligned} f_x(\tfrac{a}{p^i} + \tfrac{b}{p^j}) &= f_x(\tfrac{ap^{j-i}+b}{p^j}) = (ap^{j-i} + b)x_j \\ &= ap^{j-i}x_j + bx_j = f_x(\tfrac{ap^{j-i}}{p^j}) + f_x(\tfrac{b}{p^j}) = f_x(\tfrac{a}{p^i}) + f_x(\tfrac{b}{p^j}). \end{aligned}$$

[110]Προσοχή! Το ότι ισχύει $G/G[p] \underset{9.1.4}{\cong} pG = G$, *δεν σημαίνει* ότι η $G[p]$ είναι τετριμμένη, καθώς η $G$ (ως μη τετριμμένη και διαιρετή) είναι άπειρη! (Πρβλ. παράδειγμα 4.5.3 (iv).)

Επιπροσθέτως, $\mathrm{Ker}(f_x) = \mathbb{Z}$. (Πράγματι· ο εγκλεισμός $\mathbb{Z} \subseteq \mathrm{Ker}(f_x)$ είναι προφανής, διότι

$$f_x(1) = f_x(\tfrac{p}{p}) = px_1 = px = 0_G.$$

Ας υποθέσουμε ότι $\mathbb{Z} \subsetneqq \mathrm{Ker}(f_x)$. Τότε υπάρχουν $a \in \mathbb{Z} \smallsetminus \{0\}$ και $i \in \mathbb{N}$ με $p \nmid a$, ούτως ώστε να ισχύει $f_x(\frac{a}{p^i}) = ax_i = 0_G$. Επειδή

$$\mu\kappa\delta(a,p) = 1 \underset{\text{B.2.13}}{\Longrightarrow} \mu\kappa\delta(a,p^i) = 1 \underset{\text{B.2.8}}{\Longrightarrow} [\exists c, d \in \mathbb{Z} : ca + dp^i = 1],$$

έχουμε $x_i = c(ax_i) + dp^i x_i = c\, 0_G + dp^i x_i = d\left(p^i x_i\right)$, όπου

$$p^i x_i = p^{i-1}(px_i) = p^{i-1}x_{i-1} = p^{i-2}x_{i-2} = \cdots = p^{i-(i-1)}x_{i-(i-1)} = px_1 = px = 0_G.$$

Άρα $x_i = 0_G$. Όμως $p^{i-1}x_i = x_1 = x \neq 0_G \Rightarrow x_i \neq 0_G$. Άτοπο!) Επομένως υφίσταται μοναδικός *ισομορφισμός*

$$\mathbb{Z}(p^\infty) := \mathbb{Z}[\tfrac{1}{p}]/\mathbb{Z} \ni \tfrac{a}{p^i} + \mathbb{Z} \overset{\hat{f}_x}{\longmapsto} \hat{f}_x(\tfrac{a}{p^i} + \mathbb{Z}) \in \mathrm{Im}(f_x)$$

με $\hat{f}_x(\frac{a}{p^i} + \mathbb{Z}) = f_x(\frac{a}{p^i})$ (βλ. 4.5.2) και η εικόνα του $\mathrm{Im}(f_x) = \langle \{ x_i | \, i \in \mathbb{N}\} \rangle \cong \mathbb{Z}(p^\infty)$ είναι μια υποομάδα τής $G$ περιέχουσα το $x$ (διότι $x = f_x(\frac{1}{p})$). Σημειωτέον ότι

$$\mathrm{Im}(f_x)[p] = \langle \{ x_i | \, i \in \mathbb{N} : px_i = 0_G\} \rangle = \langle \{ x_i | \, i \in \mathbb{N} : x_{i-1} = 0_G\} \rangle = \langle x_1 \rangle = \langle x \rangle .$$

**Βήμα 2ο**. Κατ' αρχάς παρατηρούμε ότι

$$\textstyle\bigoplus_{x\in X}^{\text{περ.}} \mathrm{Im}(f_x)[p] = \bigoplus_{x\in X}^{\text{περ.}} \langle x \rangle \underset{\text{7.1.100 (ii)}}{\cong} \bigoplus_{x\in X}^{\text{εσ.}} \langle x \rangle = G[p]. \tag{9.70}$$

Εν συνεχεία, ορίζουμε τον ομομορφισμό[111]

$$\boldsymbol{\beta} : \bigoplus_{x\in X}^{\text{περ.}} \mathrm{Im}(f_x) \longrightarrow G, \; g = (g_x)_{x\in X} \longmapsto \boldsymbol{\beta}(g) := \begin{cases} 0_G, & \text{όταν } g = 0_G, \\ \sum\limits_{x \in \,\mathrm{supp}(g)} g_x, & \text{όταν } g \neq 0_G, \end{cases}$$

με εικόνα του την $\mathrm{Im}(\boldsymbol{\beta}) = \langle \{ \mathrm{Im}(f_x) | \, x \in X\} \rangle$, ήτοι μια διαιρετή[112] υποομάδα τής $G$. Ο περιορισμός του

$$\boldsymbol{\beta}|_{\bigoplus_{x\in X}^{\text{περ.}} \mathrm{Im}(f_x)[p]} : \textstyle\bigoplus_{x\in X}^{\text{περ.}} \mathrm{Im}(f_x)[p] \xrightarrow{\cong} G[p] \tag{9.71}$$

είναι ο ισομορφισμός (9.70). Κατά το πόρισμα 9.7.23 υπάρχει κάποια $K \sqsubseteq G$ με $G = \mathrm{Im}(\boldsymbol{\beta}) \oplus_{\text{εσ.}} K$. Επομένως,

$$G[p] = \mathrm{Im}(\boldsymbol{\beta})[p] \oplus_{\text{εσ.}} K[p].$$

[111] Πρόκειται για τον ομομορφισμό (7.31) (ύστερα από κατάλληλη αλλαγή τού συμβολισμού).

[112] Η $\mathrm{Im}(f_x) \cong \mathbb{Z}(p^\infty)$ είναι διαιρετή για κάθε πρώτο αριθμό $p$. (Βλ. πορίσματα 9.7.17 και 9.7.12.) Επομένως, λόγω των προτάσεων 9.7.14 και 9.7.9, οι $\bigoplus_{x\in X}^{\text{περ.}} \mathrm{Im}(f_x)$ και $\mathrm{Im}(\boldsymbol{\beta})$ είναι ωσαύτως διαιρετές.

Επειδή όμως

$$\mathrm{Im}(\boldsymbol{\beta})[p] = \langle \{ \mathrm{Im}(f_x)[p] |\, x \in X\} \rangle = \langle \{ \langle x \rangle |\, x \in X\} \rangle = \textstyle\bigoplus_{x\in X}^{\text{εσ.}} \langle x \rangle = G[p],$$

έχουμε $K[p] = \{0_G\}$, απ' όπου έπεται ότι[113] $K = \{0_G\}$ και ότι ο $\boldsymbol{\beta}$ είναι επιμορφισμός. Έστω τώρα $g = (g_x)_{x\in X} \in \mathrm{Ker}(\boldsymbol{\beta})$. Εάν υποθέσουμε ότι $g \neq 0_G$ και θέσουμε

$$m := \max \{ \nu_x \in \mathbb{N} |\ \mathrm{ord}(g_x) = p^{\nu_x},\ x \in\ \mathrm{supp}(g)\}$$

και $\Lambda(g) := \{ x \in\ \mathrm{supp}(g) |\, \mathrm{ord}(g_x) = p^m \}$, τότε

$$\boldsymbol{\beta}(g) = 0_G \Rightarrow 0_G = p^{m-1}\boldsymbol{\beta}(g) = \boldsymbol{\beta}(p^{m-1}g) = \sum_{x\in\ \mathrm{supp}(g)} p^{m-1} g_x = \sum_{x\in\ \Lambda(g)} p^{m-1} g_x .$$

Για κάθε $x \in X$ έχουμε $p(p^{m-1}g_x) = p^m g_x = 0_G \Rightarrow p^{m-1}g_x \in \mathrm{Im}(f_x)[p]$. Ως εκ τούτου,

$$\begin{aligned} 0_G &= \sum_{x\in\ \Lambda(g)} p^{m-1} g_x = \boldsymbol{\beta}(p^{m-1}g) = \boldsymbol{\beta}|_{\bigoplus_{x\in X}^{\text{περ.}} \mathrm{Im}(f_x)[p]} (p^{m-1}g) \\ &\Rightarrow p^{m-1}g \in \mathrm{Ker}(\boldsymbol{\beta}|_{\bigoplus_{x\in X}^{\text{περ.}} \mathrm{Im}(f_x)[p]}) \underset{(9.71)}{=} \{0_G\} \Rightarrow p^{m-1}g = 0_G \\ &\Rightarrow [p^{m-1}g_x = 0_G,\ \forall x \in\ \mathrm{supp}(g)]. \end{aligned}$$

Ιδιαιτέρως, για κάθε $x \in \Lambda(g)$, $p^{m-1}g_x = 0_G \Rightarrow \mathrm{ord}(g_x) \leq p^{m-1}$. Άτοπο! Άρα $g = 0_G$ και $\mathrm{Ker}(\boldsymbol{\beta}) = \{0_G\}$. Κατά συνέπειαν, η σύνθεση

$$\begin{tikzcd} \mathbb{Z}(p^\infty)^{(X)} \arrow[r, "\bigoplus_{x\in X} \hat{f}_x"] \arrow[rr, bend left] & \bigoplus_{x\in X}^{\text{περ.}} \mathrm{Im}(f_x) \arrow[r, "\boldsymbol{\beta}"] & G \end{tikzcd}$$

είναι ισομορφισμός τόσον *ομάδων* όσον και $\mathbb{Z}_p$-*διανυσματικών χώρων*. $\square$

**9.7.33 Θεώρημα.** *Μια αβελιανή ομάδα* $(G, +)$ *είναι διαιρετή ομάδα στρέψεως εάν και μόνον εάν*

$$\boxed{G \cong \bigoplus_{p\ \text{πρώτος}}^{\text{περ.}} \mathbb{Z}(p^\infty)^{(X_p)}} \tag{9.72}$$

*για κάποια σύνολα* $X_p$.

ΑΠΟΔΕΙΞΗ. Εάν $(G, +)$ είναι μια διαιρετή αβελιανή ομάδα στρέψεως, τότε

$$G \underset{(9.55)}{=} \bigoplus_{p\ \text{πρώτος}}^{\text{εσ.}} G(p) \underset{7.1.100\,(ii)}{\cong} \bigoplus_{p\ \text{πρώτος}}^{\text{περ.}} G(p) \cong \bigoplus_{p\ \text{πρώτος}}^{\text{περ.}} \mathbb{Z}(p^\infty)^{(X_p)},$$

διότι η $p$-πρωτεύουσα συνιστώσα $G(p)$ τής $G$ είναι (ως ευθύς προσθετέος διαιρετής) διαιρετή (βλ. 9.7.14) και (λόγω τού λήμματος 9.7.32) ισόμορφη με την $\mathbb{Z}(p^\infty)^{(X_p)}$, όπου $X_p$ είναι οιαδήποτε βάση τού $\mathbb{Z}_p$-διανυσματικού χώρου $G[p]$ για

[113]Εάν $y \in K$, τότε υπάρχει κάποιος $\nu \in \mathbb{N} : p^\nu y = 0_G$, διότι η $G$ είναι $p$-ομάδα. Επειδή $K[p] = \{0_G\}$, έχουμε $p^{\nu-1}y = 0_G \Rightarrow p^{\nu-2}y = 0_G \Rightarrow \cdots \Rightarrow y = 0_G$.

κάθε πρώτον αριθμό $p$. Και αντιστρόφως· εάν για μια αβελιανή ομάδα $(G,+)$ ισχύει η (9.72) για *τυχόντα* σύνολα $X_p$, τότε αυτή είναι διαιρετή ομάδα στρέψεως λόγω των πορισμάτων 9.7.12 και 9.7.17, και των προτάσεων 9.7.14 και 9.4.9. □

► **Διαιρετές αβελιανές ομάδες στερούμενες στρέψεως**. Αυτές δεν είναι τίποτα άλλο παρά οι προσθετικές ομάδες των $\mathbb{Q}$-*διανυσματικών χώρων*.

**9.7.34 Θεώρημα.** *Εάν $(G,+)$ είναι μια διαιρετή αβελιανή ομάδα χωρίς στρέψη, τότε ισχύουν τα εξής:*
(i) *Εάν για κάθε $g \in G$ θεωρήσουμε τον ομομορφισμό*

$$\theta_g : \mathbb{Z} \longrightarrow G, \;\; n \longmapsto \theta_g(n) := ng,$$

*τότε υπάρχει ακριβώς ένας $f_g \in \mathrm{Hom}(\mathbb{Q},G)$ με $f_g|_{\mathbb{Z}} = \theta_g$.*
(ii) *Η τριάδα $(G,+,\cdot)$, όπου το “$\cdot$” συμβολίζει τον «αριθμητικό πολλαπλασιασμό»*

$$\boxed{\mathbb{Q}\times G \longrightarrow G, \; (q,g) \longmapsto q\cdot g := f_g(q),}$$

*αποτελεί έναν διανυσματικό χώρο υπεράνω τού σώματος των ρητών αριθμών.*
(iii) *Εάν $Y \subseteq G$, τότε το $Y$ είναι μεγιστικό $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο τής $G$ εάν και μόνον εάν είναι βάση (υπό τη συνήθη έννοια) τού ανωτέρω διανυσματικού χώρου. Κατά συνέπειαν, υπάρχει πάντοτε κάποιο σύνολο $Y$, τέτοιο ώστε να ισχύει*

$$\boxed{G \cong \mathbb{Q}^{(Y)}.} \tag{9.73}$$

*Και αντιστρόφως· εάν $(G,+)$ είναι μια αβελιανή ομάδα ισόμορφη τής $\mathbb{Q}^{(Y)}$, όπου $Y$ τυχόν σύνολο, τότε αυτή είναι διαιρετή και δεν διαθέτει στρέψη.*

Απόδειξη. Έστω $(G,+)$ μια διαιρετή αβελιανή ομάδα χωρίς στρέψη.
(i) Επειδή η $G$ (ως διαιρετή) είναι εμβολική, υπάρχει κάποιος $f_g \in \mathrm{Hom}(\mathbb{Q},G)$ με $f_g|_{\mathbb{Z}} = \theta_g$ για κάθε $g \in G$. Εάν ένας $f'_g \in \mathrm{Hom}(\mathbb{Q},G)$ έχει την ιδιότητα $f'_g|_{\mathbb{Z}} = \theta_g$ για κάθε $g \in G$, τότε για κάθε $q = \frac{n}{m}$ ($n \in \mathbb{Z}, m \in \mathbb{Z}\smallsetminus\{0\}$) έχουμε

$$\left.\begin{array}{r} m\left(f'_g(q) - f_g(q)\right) = f'_g(mq) - f_g(mq) \\ = f'_g(n) - f_g(n) = \theta_g(n) - \theta_g(n) = 0_G, \\ \mathrm{tors}(G) = \{0_G\} \end{array}\right\} \Rightarrow f'_g(q) = f_g(q).$$

(ii) Κατ' αρχάς, $1\cdot g = f_g(q) = \theta_g(q) = g, \forall g \in G$. Επίσης, για $q_1,q_2 \in \mathbb{Q}$,

$$(q_1+q_2)\cdot g = f_g(q_1+q_2) = f_g(q_1) + f_g(q_2) = q_1\cdot g + q_2\cdot g, \; \forall g \in G.$$

Εν συνεχεία, επειδή (για οιαδήποτε $g_1,g_2 \in G$) αμφότεροι οι ομομορφισμοί

$$\mathbb{Q} \longrightarrow G, \; q \longmapsto q\cdot(g_1+g_2) \;\text{ και }\; q \longmapsto q\cdot g_1 + q\cdot g_2$$

αποτελούν επεκτάσεις τού ομομορφισμού

$$\theta_{g_1+g_2} : \mathbb{Z} \longrightarrow G, n \longmapsto \theta_{g_1+g_2}(n) = n(g_1+g_2) = ng_1 + ng_2,$$

συμπεραίνουμε ότι $q\cdot(g_1+g_2) = q\cdot g_1 + q\cdot g_2$ για κάθε $q \in \mathbb{Q}$ (μέσω τής ιδιότητας τής μοναδικότητας των επεκτάσεων τής αποδειχθείσας στο (i)). Τέλος, εάν $q_1 = \frac{n_1}{m_1}$, $q_2 = \frac{n_2}{m_2}$, όπου $n_1, n_2 \in \mathbb{Z}$, $m_1, m_2 \in \mathbb{Z}\smallsetminus\{0\}$, και $g \in G$, τότε έχουμε αφ' ενός μεν

$$m_1 m_2 f_g(q_1 q_2) = f_g(m_1 q_1 m_2 q_2) = f_g(n_1 n_2) = \theta_g(n_1 n_2) = (n_1 n_2)g = n_1(n_2 g),$$

αφ' ετέρου δε

$$\begin{aligned} m_1 m_2 f_{q_2\cdot g}(q_1) &= m_2 f_{q_2\cdot g}(m_1 q_1) = m_2 f_{q_2\cdot g}(n_1) = m_2 \theta_{q_2\cdot g}(n_1) = m_2 n_1 (q_2\cdot g) \\ &= n_1(m_2 f_g(q_2)) = n_1 f_g(m_2 q_2) = n_1 f_g(n_2) = n_1 \theta_g(n_2) = n_1(n_2 g), \end{aligned}$$

απ' όπου προκύπτει ότι

$$\left.\begin{array}{r} |m_1 m_2|\,(f_g(q_1 q_2) - f_{q_2\cdot g}(q_1)) = 0_G \\ \mathrm{tors}(G) = \{0_G\} \end{array}\right\} \Rightarrow f_g(q_1 q_2) = f_{q_2\cdot g}(q_1),$$

ήτοι ότι $(q_1 q_2)\cdot g = q_1\cdot(q_2\cdot g)$.

(iii) Κάθε μεγιστικό $\mathbb{Z}$-γραμμικώς ανεξάρτητο υποσύνολο $Y$ τής $G$ αποτελεί μεγιστικό γραμμικώς ανεξάρτητο υποσύνολο και, ως εκ τούτου, *βάση* (υπό τη συνήθη έννοια) τού $\mathbb{Q}$-διανυσματικού χώρου τού ορισθέντος στο (ii) και τανάπαλιν. Πράγματι· εάν $y_1, ..., y_\kappa \in Y$ ($\kappa \in \mathbb{N}$), τότε από κάθε σχέση τής μορφής

$$\sum_{j=1}^{\kappa} q_j y_j = 0_G \ \ (\text{όπου } q_1 = \tfrac{n_1}{m_1}, .., q_\kappa = \tfrac{n_\kappa}{m_\kappa},\ n_1, .., n_\kappa \in \mathbb{Z}, m_1, .., m_\kappa \in \mathbb{Z}\smallsetminus\{0\})$$

λαμβάνουμε $\sum_{j=1}^{\kappa} m q_j y_j = 0_G$ (όπου $m := \prod_{j=1}^{\kappa} m_j$) και, προϋποτεθείσας τής $\mathbb{Z}$-γραμμικής ανεξαρτησίας τού $Y$,

$$\sum_{j=1}^{\kappa} \underbrace{n_j}_{\in\mathbb{Z}} \underbrace{\Bigg(\prod_{i\in\{1,\ldots,\kappa\}\smallsetminus\{j\}} m_i\Bigg)}_{\in\mathbb{Z}\smallsetminus\{0\}} y_j = 0_G \Rightarrow n_1 = \cdots = n_\kappa = 0 \Rightarrow q_1 = \cdots = q_\kappa = 0.$$

Άρα το $Y$ είναι όντως γραμμικώς ανεξάρτητο υποσύνολο τού αντίστοιχου $\mathbb{Q}$-διανυσματικού χώρου (και εμφανώς μεγιστικό με αυτήν την ιδιότητα ως προς τη σχέση εγκλεισμού) και, ως εκ τούτου, βάση αυτού. (Το αντίστροφο είναι προφανές.) Έτσι, μέσω *οιασδήποτε* βάσεώς του $Y$, μέσω των[114]

$$Y \ni x \longmapsto \delta_y(x) := \begin{cases} 1, & \text{όταν } x = y, \\ 0, & \text{όταν } x \neq y, \end{cases}$$

και μέσω $\mathbb{Q}$-γραμμικής επεκτάσεως δημιουργείται ένας ισομορφισμός (9.73):

$$G = \bigoplus\nolimits_{y\in Y}^{\text{πεϱ.}} \mathbb{Q}y \xrightarrow{\cong} \mathbb{Q}^{(Y)},\ \ (y)_{y\in Y} \longmapsto (\delta_y)_{y\in Y},$$

τόσον *ομάδων* όσον και $\mathbb{Q}$-*διανυσματικών χώρων*.

Και αντιστρόφως· εάν $(G, +)$ είναι μια αβελιανή ομάδα με $G \cong \mathbb{Q}^{(Y)}$, όπου $Y$ *τυχόν* σύνολο, τότε η $G$ είναι διαιρετή χωρίς στρέψη λόγω τού πορίσματος 9.7.12 και των προτάσεων 9.7.14 και 9.4.9. □

► **Ταξινόμηση διαιρετών αβελιανών ομάδων μέχρις ισομορφισμού**. Λαμβάνοντας υπ' όψιν τα μέχρι στιγμής αποδειχθέντα καταλήγουμε στο ακόλουθο:

[114]Η οικογένεια $(\delta_y)_{y\in Y}$ αποτελεί τη «συνήθη» βάση τού $\mathbb{Q}$-διανυσματικού χώρου $\mathbb{Q}^{(Y)}$.

**9.7.35 Θεώρημα.** **(Θεμελιώδες θεώρημα περί των διαιρετών αβελιανών ομάδων.)**
(a) *Εάν* $(G,+)$ *είναι μια διαιρετή αβελιανή ομάδα, τότε*

$$\boxed{G \cong \left(\bigoplus_{p\ \text{πρώτος}}^{\text{περ.}} \mathbb{Z}(p^{\infty})^{(X_p)}\right) \oplus \mathbb{Q}^{(Y)},\ \text{για κάποια σύνολα } X_p \text{ και } Y.}$$

(b) *Ας υποθέσουμε ότι* $G_1, G_2$ *είναι δυο διαιρετές αβελιανές ομάδες με*

$$G_1 \cong \left(\bigoplus_{p\ \text{πρώτος}}^{\text{περ.}} \mathbb{Z}(p^{\infty})^{(X_p^{[1]})}\right) \oplus \mathbb{Q}^{\left(Y^{[1]}\right)},\ \ G_2 \cong \left(\bigoplus_{p\ \text{πρώτος}}^{\text{περ.}} \mathbb{Z}(p^{\infty})^{(X_p^{[2]})}\right) \oplus \mathbb{Q}^{\left(Y^{[2]}\right)}.$$

*Τότε* $G_1 \cong G_2$ *εάν και μόνον εάν ικανοποιούνται οι ακόλουθες συνθήκες:*
(i) $\text{card}(X_p^{[1]}) = \text{card}(X_p^{[2]})$ *για κάθε πρώτον αριθμό* $p$.
(ii) $\text{card}(Y^{[1]}) = \text{card}(Y^{[2]})$.

ΑΠΟΔΕΙΞΗ. (a) Σύμφωνα με το πόρισμα 9.7.27 η $\text{tors}(G)$ είναι διαιρετή. Άρα υπάρχει $K \sqsubseteq G$ με $G = \text{tors}(G) \oplus_{\text{εσ.}} K$. (Βλ. πόρισμα 9.7.23.) Ως γνωστόν, $K \cong G/\text{tors}(G)$ και η $K$ στερείται στρέψεως. (Βλ. προτάσεις 7.1.29 και 9.4.5.) Κατά συνέπειαν, από τα θεωρήματα 9.7.33 και 9.7.34 έπεται ότι

$$G \cong \text{tors}(G) \oplus K \cong \text{tors}(G) \oplus (G/\text{tors}(G)) \cong \left(\bigoplus_{p\ \text{πρώτος}}^{\text{περ.}} \mathbb{Z}(p^{\infty})^{(X_p)}\right) \oplus \mathbb{Q}^{(Y)}$$

για κάποια σύνολα $X_p$ και $Y$.
(b) Εάν $G_1 \cong G_2$, τότε, σύμφωνα με την πρόταση 9.4.8,

$$\bigoplus_{p\ \text{πρώτος}}^{\text{περ.}} \mathbb{Z}(p^{\infty})^{(X_p^{[1]})} \cong \text{tors}(G_1) \cong \text{tors}(G_2) \cong \bigoplus_{p\ \text{πρώτος}}^{\text{περ.}} \mathbb{Z}(p^{\infty})^{(X_p^{[2]})} \tag{9.74}$$

και

$$\mathbb{Q}^{\left(Y^{[1]}\right)} \cong G_1/\text{tors}(G_1) \cong G_2/\text{tors}(G_2) \cong \mathbb{Q}^{\left(Y^{[2]}\right)}. \tag{9.75}$$

Από τους ισομορφισμούς (9.74) και από το θεώρημα 9.4.15 έπεται ότι

$$\mathbb{Z}(p^{\infty})^{(X_p^{[1]})} \cong \mathbb{Z}(p^{\infty})^{(X_p^{[2]})} \tag{9.76}$$

για κάθε πρώτον αριθμό $p$. Επειδή οι ισομορφισμοί ομάδων (9.76) είναι *και* ισομορφισμοί $\mathbb{Z}_p$-διανυσματικών χώρων, έχουμε

$$\text{card}(X_p^{[1]}) = \dim_{\mathbb{Z}_p}(\mathbb{Z}(p^{\infty})^{(X_p^{[1]})}) = \dim_{\mathbb{Z}_p}(\mathbb{Z}(p^{\infty})^{(X_p^{[2]})}) = \text{card}(X_p^{[2]})$$

για κάθε πρώτον αριθμό $p$. Κατ' αναλογίαν, επειδή οι (9.75) είναι *και* ισομορφισμοί $\mathbb{Q}$-διανυσματικών χώρων, έχουμε

$$\text{card}(Y^{[1]}) = \dim_{\mathbb{Q}}(\mathbb{Q}^{\left(Y^{[1]}\right)}) = \dim_{\mathbb{Q}}(\mathbb{Q}^{\left(Y^{[1]}\right)}) = \text{card}(Y^{[2]}).$$

Το αντίστροφο είναι προφανές. □

**9.7.36 Παρατήρηση.** Εάν $Y \neq \varnothing$, τότε $\left|\mathbb{Q}^{(Y)}\right| = \max\{\aleph_0, \text{card}(Y)\}$ και εάν $X_p \neq \varnothing$ για τουλάχιστον έναν πρώτο $p$, τότε

$$\left|\bigoplus_{p\ \text{πρώτος}}^{\text{περ.}} \mathbb{Z}(p^{\infty})^{(X_p)}\right| = \prod_{p\ \text{πρώτος}:\ X_p \neq \varnothing} \max\{\aleph_0, \text{card}(X_p)\}.$$

**9.7.37 Παραδείγματα.** (i) Επειδή η $(\mathbb{R},+)$ είναι διαιρετή και χωρίς στρέψη, λαμβάνουμε $\mathbb{R} \cong \mathbb{Q}^{(Y)}$, όπου $Y$ οιοδήποτε σύνολο έχον (κατ' ανάγκην) *την ισχύ τού συνεχούς* $\mathfrak{c} = \mathrm{card}(\mathbb{R})$. Ωστόσο, το ίδιο ισχύει και και για την $(\mathbb{C},+)$! Επομένως[115],

$$\mathbb{R} \cong \mathbb{C} \underset{7.1.24}{=} \mathbb{R} \oplus_{\varepsilon\sigma.} \mathbb{R} \underset{7.1.43\,(\mathrm{ii})}{\cong} \mathbb{R} \oplus \mathbb{R}.$$

Και, γενικότερα, $\mathbb{R}^m \cong \mathbb{R}^n$ για *οιουσδήποτε* $m, n \in \mathbb{N}$ (ακόμη και όταν $m \neq n$)! Τούτο έγκειται στις ιδιαιτερότητες τού λογισμού με «μεγάλους» πληθικούς αριθμούς[116]. Το σύμβολο "$\cong$" υποδηλοί εδώ ισομορφισμό ομάδων και ισομορφισμό $\mathbb{Q}$-διανυσματικών χώρων (αλλά *όχι* ισομορφισμό $\mathbb{R}$-διανυσματικών χώρων). Όταν $m \neq n$, τα $\mathbb{R}^m$ και $\mathbb{R}^n$ (με τις συνήθεις πράξεις προσθέσεως και αριθμητικού πολλαπλασιασμού) είναι *μη ισόμορφοι* $\mathbb{R}$-διανυσματικοί χώροι αλλά *ισόμορφοι* $\mathbb{Q}$-διανυσματικοί χώροι!

(ii) Επειδή[117] $\mathrm{tors}(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$ και (προφανώς) $\mathrm{tors}(\mathbb{C}\smallsetminus\{0\}) = \mathcal{E}_\infty$, ιδού κάποιοι επιπρόσθετοι *ενδιαφέροντες* ισομορφισμοί[118]:

$$\begin{aligned}\mathbb{S}^1 &\cong \mathbb{R}/\mathbb{Z} \cong \mathrm{tors}(\mathbb{R}/\mathbb{Z}) \oplus (\mathbb{R}/\mathbb{Z})/\mathrm{tors}(\mathbb{R}/\mathbb{Z}) \cong \mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}/\mathbb{Q}\\ &\cong \mathbb{Q}/\mathbb{Z} \oplus \mathbb{R} \cong \mathcal{E}_\infty \oplus \mathbb{R} \cong \mathrm{tors}(\mathbb{C}\smallsetminus\{0\}) \oplus \mathbb{R} \cong \mathbb{C}\smallsetminus\{0\}.\end{aligned}$$

(Π.χ., η διαιρετή πολλαπλασιαστική ομάδα $(\mathbb{C}\smallsetminus\{0\},\cdot)$ *των μη μηδενικών μιγαδικών αριθμών* είναι ισόμορφη με τη γνήσια υποομάδα της $(\mathbb{S}^1,\cdot)$, το υποκείμενο σύνολο τής οποίας είναι *ο μοναδιαίος κύκλος*.)

► **Ανηγμένες αβελιανές ομάδες**. Στον αντίποδα των διαιρετών αβελιανών ομάδων βρίσκονται οι *ανηγμένες*.

**9.7.38 Ορισμός.** Λέμε ότι μια αβελιανή ομάδα $(G,+)$ είναι **ανηγμένη** όταν[119] $\mathrm{div}(G) = \{0_G\}$, δηλαδή όταν πέραν τής τετριμμένης δεν διαθέτει άλλες διαιρετές υποομάδες.

**9.7.39 Πρόταση.** *Έστω μια $(G,+)$ αβελιανή ομάδα. Εάν $\mathrm{Div}(G) = \{0_G\}$, τότε η $G$ είναι ανηγμένη.*

---

[115] Έστω $Y$ μια βάση τού $\mathbb{R}$ ως $\mathbb{Q}$-διανυσματικού χώρου. (Τετοιες βάσεις ονομάζονται ενίοτε και *βάσεις τού Hamel*.) Τότε $\mathrm{card}(Y) = \mathfrak{c}$ και υπάρχει αμφίρριψη μεταξύ τής $Y$ και τού $Y' := (Y \times \{0\}) \cup (\{0\} \times Y)$, ήτοι ενός συνόλου που μπορεί να θεωρηθεί ως βάση τού $\mathbb{Q}$-διανυσματικού χώρου $\mathbb{R} \oplus \mathbb{R}$. Προφανώς, $\mathbb{Q}^{(Y')} \cong \mathbb{Q}^{(Y)}$. Φυσικά, όλα αυτά ισχύουν μόνον υπό την προϋπόθεση ότι χρησιμοποιούμε το σύστημα αξιωμάτων ZF+AC. Βλ. εδ. A.2.21. (Η *ύπαρξη βάσεως* αποδεικνύεται με τη βοήθεια τού λήμματος A.2.20 τού Zorn το οποίο είναι ισοδύναμο με το Αξίωμα τής Επιλογής.) Πρβλ. C.J. Ash: *A consequence of the axiom of choice*, Journal of Australian Math. Soc **19** (1975), 303-308.

[116] $\mathrm{card}(\mathbb{R}^n) = \mathrm{card}(\mathbb{R}) = \mathfrak{c}$ για κάθε $n \in \mathbb{N}$.

[117] Επειδή $\mathbb{Q}/\mathbb{Z} \sqsubseteq \mathbb{R}/\mathbb{Z} \Rightarrow \mathbb{Q}/\mathbb{Z} \underset{4.4.11}{=} \mathrm{tors}(\mathbb{Q}/\mathbb{Z}) \sqsubseteq \mathrm{tors}(\mathbb{R}/\mathbb{Z})$, αρκεί να αποδειχθεί ο αντίστροφος εγκλεισμός. Έστω $x + \mathbb{Z} \in \mathbb{R}/\mathbb{Z}$ τάξεως $n \in \mathbb{N}$. Τότε $nx \in \mathbb{Z}$ οπότε υπάρχει $k \in \mathbb{Z}$ με $nx = k \Rightarrow x = \frac{k}{n} \in \mathbb{Q}$.

[118] Για τον πρώτο ισομορφισμό: $(\mathbb{S}^1,\cdot) \cong (\mathbb{R}/\mathbb{Z},+)$, βλ. εδ. 4.5.3 (ii). Ο δεύτερος προκύπτει από τα προαναφερθέντα στο 9.7.35 και ο τρίτος από το ότι $\mathrm{tors}(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$ και $(\mathbb{R}/\mathbb{Z})/\mathrm{tors}(\mathbb{R}/\mathbb{Z}) = (\mathbb{R}/\mathbb{Z})/(\mathbb{Q}/\mathbb{Z}) \cong \mathbb{R}/\mathbb{Q}$. Επειδή

$$\dim_{\mathbb{Q}}(\mathbb{R}/\mathbb{Q}) + \dim_{\mathbb{Q}}(\mathbb{Q}) = \dim_{\mathbb{Q}}(\mathbb{R}/\mathbb{Q}) + 1 = \dim_{\mathbb{Q}}(\mathbb{R}) = \mathfrak{c} \Rightarrow \dim_{\mathbb{Q}}(\mathbb{R}/\mathbb{Q}) = \mathfrak{c},$$

έχουμε $\mathbb{R} \cong \mathbb{Q}^{(Y)} \cong \mathbb{R}/\mathbb{Q}$ με $\mathrm{card}(Y) = \mathfrak{c}$, απ' όπου έπεται ο τέταρτος. Ο τελευταίος έπεται από το 9.7.35, καθώς το άστρεπτο μέρος τής $\mathbb{C}\smallsetminus\{0\}$ οφείλει να έχει την ισχύ $\mathfrak{c}$ τού συνεχούς (αφού $|\mathbb{Q}/\mathbb{Z}| = \left|\bigoplus_{p\ \pi\rho\acute{\omega}\tau o\varsigma}^{\pi\varepsilon\rho.} \mathbb{Z}(p^\infty)\right| = \aleph_0$).

[119] Προφανώς, μια αβελιανή ομάδα είναι *ταυτοχρόνως* ανηγμένη και διαιρετή *εάν και μόνον εάν είναι τετριμμένη*.

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το ότι $\mathrm{div}(G) \sqsubseteq \mathrm{Div}(G)$. □

**9.7.40 Θεώρημα.** (a) *Κάθε αβελιανή ομάδα* $(G,+)$ *γράφεται ως εσωτερικό άθροισμα*

$$\boxed{G = \mathrm{div}(G) \oplus_{\text{εσ.}} K \; \Big(\underset{7.1.43\,(\mathrm{ii})}{\cong} \mathrm{div}(G) \oplus K\Big)}$$

*τής* $\mathrm{div}(G)$ *και κάποιας ανηγμένης υποομάδας της*[120] $K$.

(b) *Ας υποθέσουμε ότι* $G_1, G_2$ *είναι δυο αβελιανές ομάδες. Τότε* $G_1 \cong G_2$ *εάν και μόνον εάν ικανοποιούνται οι ακόλουθες συνθήκες:*

(i) $\mathrm{div}(G_1) \cong \mathrm{div}(G_2)$.

(ii) $G_1/\mathrm{div}(G_1) \cong G_2/\mathrm{div}(G_2)$.

ΑΠΟΔΕΙΞΗ. (a) Σύμφωνα με το πόρισμα 9.7.23 η $\mathrm{div}(G)$ (ως διαιρετή υποομάδα τής $G$) διαθέτει κάποιο συμπλήρωμα $K$ εντός τής $G$. Εάν $H$ είναι τυχούσα διαιρετή υποομάδα τής $K$, τότε $H \sqsubseteq \mathrm{div}(G)$. (Βλ. πρόταση 9.7.29.) Εξ αυτού έπεται ότι

$$H \sqsubseteq \mathrm{div}(G) \cap K = \{0_G\} \Rightarrow H = \{0_G\} \Rightarrow \mathrm{div}(K) = \{0_G\} = \{0_K\},$$

οπότε η $K$ είναι ανηγμένη.

(b) Έστω $f : G_1 \xrightarrow{\cong} G_2$ ένας ισομορφισμός.

(i) Εφαρμόζοντας την πρόταση 9.7.31 τόσον για τον $f$ όσον και για τον $f^{-1}$ λαμβάνουμε

$$\left.\begin{array}{l} f(\mathrm{div}(G_1)) \sqsubseteq \mathrm{div}(G_2) \\ f^{-1}(\mathrm{div}(G_2)) \sqsubseteq \mathrm{div}(G_1) \end{array}\right\} \Rightarrow f(\mathrm{div}(G_1)) = \mathrm{div}(G_2), \tag{9.77}$$

οπότε η $f|_{\mathrm{div}(G_1)} : \mathrm{div}(G_1) \longrightarrow \mathrm{div}(G_2)$ είναι ισομορφισμός με τον $f^{-1}|_{\mathrm{div}(G_2)}$ ως αντίστροφό του.

(ii) Λόγω τής ισότητας (9.77) πληρούται η συνθήκη (a) τής προτάσεως 9.7.31 για τον $f^{\text{πηλ.}}$. Επειδή δε $\mathrm{Im}(f) = G_2$,πληρούται *και* η συνθήκη 9.7.31 (b) για τον $f^{\text{πηλ.}}$. Άρα ο $f^{\text{πηλ.}}$ είναι ισομορφισμός.

Αντιστρόφως τώρα· εάν ικανοποιούνται οι συνθήκες (i) και (ii), υπάρχουν (σύμφωνα με το (a)) ανηγμένες $K_1 \sqsubseteq G_1$ και $K_2 \sqsubseteq G_2$ με

$$G_1 = \mathrm{div}(G_1) \oplus_{\text{εσ.}} K_1,\; G_2 = \mathrm{div}(G_2) \oplus_{\text{εσ.}} K_2.$$

Επομένως, $G_1 \cong \mathrm{div}(G_1) \oplus K_1 \cong \mathrm{div}(G_2) \oplus K_2 \cong G_2$ (διότι $K_i \cong G_i/\mathrm{div}(G_i)$, $i = 1, 2$, βλ. 7.1.29). □

[120] Η $\mathrm{div}(G)$ είναι μια μονοσημάντως ορισμένη υποομάδα τής $G$. Αντιθέτως, τα ανηγμένα συμπληρώματά της $K$ είναι μονοσημάντως ορισμένα *μόνον μέχρις ισομορφισμού*. (Βλ. 7.6.42 (i).)

**9.7.41 Σημείωση.** (i) Εάν $(G, +)$ είναι τυχούσα αβελιανή ομάδα, είθισται να λέμε εν συντομία ότι η πηλικοομάδα $G/\mathrm{div}(G)$ αποτελεί το **ανηγμένο μέρος** τής $G$. Κατά το θεώρημα 9.7.40, δυο αβελιανές ομάδες είναι ισόμορφες εάν και μόνον εάν αυτές διαθέτουν ισόμορφα διαιρετά και ισόμορφα ανηγμένα μέρη.

(ii) Το διαιρετό μέρος τόσον των πεπερασμένως παραγομένων όσον και (όλων) των ελευθέρων αβελιανών ομάδων είναι τετριμμένο. (Βλ. πρόταση 9.7.42 και πόρισμα 9.7.44.)

(iii) Παραδείγματα ανηγμένων ομάδων στρέψεως και ανηγμένων ομάδων χωρίς στρέψη δίδονται στο πόρισμα 9.7.45 και στις προτάσεις 9.7.46 και 9.7.50, αντιστοίχως. Τέλος, ένα παράδειγμα μιας ανηγμένης, *μικτής* και *μη διασπώμενης* αβελιανής ομάδας δίδεται στην πρόταση 9.7.55.

**9.7.42 Πρόταση.** *Κάθε πεπερασμένως παραγόμενη αβελιανή ομάδα είναι ανηγμένη.*

ΑΠΟΔΕΙΞΗ. Έστω $(G, +)$ μια πεπερασμένως παραγόμενη αβελιανή ομάδα. Σύμφωνα με την πρόταση 9.6.9 η $\mathrm{div}(G)$ είναι ωσαύτως πεπερασμένως παραγόμενη. Επομένως, $\mathrm{div}(G) = \{0_G\}$. (Βλ. πόρισμα 9.7.18.) □

**9.7.43 Πρόταση.** *Έστω $(G_i)_{i\in I}$ μια οικογένεια (προσθετικών) αβελιανών ομάδων $(I \neq \varnothing)$. Εάν $G := \bigoplus_{i\in I} G_i$ (και αντιστοίχως, εάν $G := \bigoplus_{i\in I}^{\text{περ.}} G_i$) τότε η $G$ είναι ανηγμένη εάν και μόνον εάν η $G_i$ είναι ανηγμένη για κάθε $i \in I$.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι $G := \bigoplus_{i\in I} G_i$. Εάν η $G$ είναι μη ανηγμένη, τότε υπάρχει κάποια διαιρετή μη τετριμμένη υποομάδα $H$ τής $G$. Άρα υπάρχει κάποιος δείκτης $j \in I$, τέτοιος ώστε η εικόνα $\mathrm{pr}_j(G)$ τής $G$ μέσω τής $j$-οστής φυσικής προβολής $\mathrm{pr}_j : G \longrightarrow G_j$ να είναι μια μη τετριμμένη υποομάδα τής $G_j$. Επειδή η $\mathrm{pr}_j$ είναι επιμορφισμός, η $\mathrm{pr}_j(G)$ είναι διαιρετή (λόγω τής προτάσεως 9.7.9) και, ως εκ τούτου, μη ανηγμένη. Και αντιστρόφως· εάν υπάρχει κάποιος δείκτης $j \in I$, τέτοιος ώστε η $G_j$ να είναι μη ανηγμένη, τότε η $G_j$ διαθέτει κάποια διαιρετή μη τετριμμένη υποομάδα $H_j$. Επειδή η εικόνα $\iota_j(G_j)$ τής $G_j$ μέσω τής $j$-οστής φυσικής εμφυτεύσεως $\iota_j : G_j \longrightarrow G$ είναι μια υποομάδα τής $G$ (ισόμορφη τής $G_j$), η $\iota_j(G_j)$ είναι μη τετριμμένη και διαιρετή, οπότε η $G$ είναι μη ανηγμένη. (Στην περίπτωση όπου $G := \bigoplus_{i\in I}^{\text{περ.}} G_i$ η απόδειξη είναι παρόμοια.) □

**9.7.44 Πόρισμα.** *Κάθε ελεύθερη αβελιανή ομάδα είναι ανηγμένη.*

ΑΠΟΔΕΙΞΗ. Κάθε ελεύθερη αβελιανή ομάδα είναι (εξ ορισμού) ισόμορφη με την $\mathbb{Z}^{(X)}$, για κάποιο σύνολο $X$. Επειδή η $(\mathbb{Z}, +)$ (ως κυκλική) είναι ανηγμένη, κάθε ελεύθερη αβελιανή ομάδα είναι ανηγμένη (δυνάμει τής προτάσεως 9.7.43 όταν[121] $X \neq \varnothing$). □

**9.7.45 Πόρισμα.** *Η $(\bigoplus_{p \text{ πρώτος}}^{\text{περ.}} \mathbb{Z}_p, +)$ είναι μια (μη πεπερασμένως παραγόμενη[122]) ανηγμένη αβελιανή ομάδα στρέψεως.*

[121] Εάν $X = \varnothing$, τότε ο ισχυρισμός είναι προδήλως αληθής.

[122] Επειδή αυτή είναι άπειρη ομάδα, άπαξ και έχει αποδειχθεί ότι είναι ομάδα στρέψεως, το ότι δεν είναι πεπερασμένως παραγόμενη έπεται από την πρόταση 9.4.3.

ΑΠΟΔΕΙΞΗ. Η $(\mathbb{Z}_p, +)$ (ως πεπερασμένη κυκλική) είναι ανηγμένη αβελιανή ομάδα στρέψεως για κάθε πρώτον αριθμό $p$. Αυτή η ιδιότητα μεταφέρεται (μέσω των προτάσεων 9.4.9 και 9.7.43) και στο περιορισμένο ευθύ άθροισμα $\bigoplus_{p \text{ πρώτος}}^{\text{περ.}} \mathbb{Z}_p$. □

**9.7.46 Πρόταση.** *Κάθε γνήσια υποομάδα τής (διαιρετής αβελιανής ομάδας) $(\mathbb{Q}, +)$ είναι ανηγμένη (χωρίς στρέψη* [123]*).*

ΑΠΟΔΕΙΞΗ. Έστω $H \sqsubset \mathbb{Q}$. Ας υποθέσουμε ότι $\{0\} \sqsubset \text{div}(H)$. Τότε υπάρχει κάποιο $r = \frac{a}{b} \in \text{div}(H)$, όπου $a, b \in \mathbb{Z}\smallsetminus\{0\}$. Έστω τυχόν $q = \frac{c}{d} \in \mathbb{Q}$ $(c \in \mathbb{Z},\, d \in \mathbb{Z}\smallsetminus\{0\})$. Επειδή η ίδια η $\text{div}(H)$ είναι διαιρετή και $ad \neq 0$, υπάρχει κάποιο $s \in \text{div}(H)$, τέτοιο ώστε να ισχύει $r = |ad|\, s$. Επομένως,

$$s = \frac{r}{|a||d|} = \frac{\text{sign}(a)}{b|d|} \in \text{div}(H) \Rightarrow q = (\underbrace{\text{sign}(a)\text{sign}(d)cb}_{\in \mathbb{Z}})s \in \text{div}(H),$$

απ' όπου έπεται ότι $\mathbb{Q} \sqsubseteq \text{div}(H) \sqsubseteq H \sqsubset \mathbb{Q}$. Άτοπο! Άρα $\text{div}(H) = \{0\}$. □

**9.7.47 Παράδειγμα.** Η $p$-διαιρετή υποομάδα $\mathbb{Z}[\frac{1}{p}]$ τής ομάδας $(\mathbb{Q}, +)$ (όπου $p$ πρώτος, βλ. 9.7.7) είναι μη τετριμμένη και γνήσια[124], οπότε είναι *ανηγμένη* και *μη διαιρετή* (*χωρίς στρέψη*). Επίσης, είναι *μη ελεύθερη* (όπως κανείς διαπιστώνει εύκολα μέσω τού πορίσματος 9.5.21) και, ως εκ τούτου, *μη πεπερασμένως παραγόμενη* [125].

Ένας εύκολος τρόπος κατασκευής πολλών παραδειγμάτων αβελιανών ομάδων *χωρίς στρέψη* υποδεικνύεται από την ακόλουθη:

**9.7.48 Πρόταση.** *Εάν οι $G, H$ είναι δυο (προσθετικές) αβελιανές ομάδες με την $G$ διαιρετή, τότε η $\text{Hom}(G, H)$ στερείται στρέψεως.*

ΑΠΟΔΕΙΞΗ. Έστω $f \in \text{Hom}(G, H)$ με $\text{ord}(f) = n \in \mathbb{N}$ και έστω *τυχόν* $g \in G$. Επειδή η $G$ είναι διαιρετή, $\exists x \in G : g = nx$. Επομένως,

$$\begin{aligned} & nf = 0_{\text{Hom}(G,H)} \Rightarrow nf(x) = 0_{\text{Hom}(G,H)}(x) = 0_H \\ & \Rightarrow 0_H = nf(x) = f(nx) = f(g) \Rightarrow f = 0_{\text{Hom}(G,H)} \end{aligned}$$

και, ως εκ τούτου, $\text{tors}(\text{Hom}(G, H)) = \{0_{\text{Hom}(G,H)}\}$. □

**9.7.49 Συμβολισμός.** Για κάθε πρώτον αριθμό $p$ συμβολίζουμε ως

$$\boxed{\mathbb{J}_p := \text{Hom}(\mathbb{Z}(p^\infty), \mathbb{Z}(p^\infty)) = \text{End}(\mathbb{Z}(p^\infty))}$$

το υποκείμενο σύνολο τής προσθετικής ομάδας τού δακτυλίου των ενδομορφισμών τής $p$-σχεδόν κυκλικής ομάδας $\mathbb{Z}(p^\infty)$.

[123] Εάν $H \sqsubseteq \mathbb{Q}$, τότε $\text{tors}(H) \sqsubseteq \text{tors}(\mathbb{Q}) = \{0\} \Rightarrow \text{tors}(H) = \{0\}$.

[124] Π.χ., $\frac{1}{p+1} \in \mathbb{Q}\smallsetminus\mathbb{Z}[\frac{1}{p}]$.

[125] Επειδή η $\mathbb{Z}[\frac{1}{p}]$ δεν διαθέτει στρέψη, εάν ήταν πεπερασμένως παραγόμενη, τότε (σύμφωνα με το θεώρημα 9.6.1) θα έπρεπε να είναι ελεύθερη.

**9.7.50 Πρόταση.** *Η αβελιανή ομάδα* $(\mathbb{J}_p,+)$ *είναι ανηγμένη (χωρίς στρέψη) για κάθε πρώτον αριθμό* $p$.

ΑΠΟΔΕΙΞΗ. Έστω $f \in \bigcap_{n\in\mathbb{N}_0} p^n\mathbb{J}_p$ και έστω τυχόν στοιχείο $\frac{a}{p^i}+\mathbb{Z} \in \mathbb{Z}(p^\infty)$ (όπου $a\in\mathbb{Z}$, $i\in\mathbb{N}_0$). Επειδή $f\in p^i\mathbb{J}_p$, υπάρχει $f'\in\mathbb{J}_p : f=p^if'$. Κατά συνέπειαν,

$$\begin{aligned} f(\tfrac{a}{p^i}+\mathbb{Z}) &= p^if'(\tfrac{a}{p^i}+\mathbb{Z}) = f'(p^i(\tfrac{a}{p^i}+\mathbb{Z})) \\ &= f'(a+\mathbb{Z}) = f'(\mathbb{Z}) = f'(0_{\mathbb{Z}(p^\infty)}) = 0_{\mathbb{Z}(p^\infty)} \Rightarrow f = 0_{\mathbb{J}_p}. \end{aligned}$$

Άρα $\bigcap_{n\in\mathbb{N}_0} p^n\mathbb{J}_p = \{0_{\mathbb{J}_p}\}$ και $\mathrm{Div}(\mathbb{J}_p) \sqsubseteq \bigcap_{n\in\mathbb{N}_0} p^n\mathbb{J}_p \Rightarrow \mathrm{Div}(\mathbb{J}_p)=\{0_{\mathbb{J}_p}\}$, απ' όπου έπεται ότι η (εκ κατασκευής στερούμενη στρέψεως) αβελιανή ομάδα $(\mathbb{J}_p,+)$ είναι ανηγμένη. (Βλ. προτάσεις 9.7.48 και 9.7.39.) □

**9.7.51 Σημείωση.** Επειδή $\mathbb{Z}(p^\infty) = \left\langle\left\{ \frac{1}{p^i}+\mathbb{Z} \,\middle|\, i\in\mathbb{N}_0\right\}\right\rangle$, κάθε ενδομορφισμός $f\in\mathbb{J}_p$ καθορίζεται από τις τιμές που λαμβάνει σε καθέναν εξ αυτών των γεννητόρων. (Βλ. 2.4.9 (i).) Η κυκλική υποομάδα $\left\langle \frac{1}{p^i}+\mathbb{Z}\right\rangle$ (τάξεως $p^i$) τής $\mathbb{Z}(p^\infty)$ είναι πλήρως αναλλοίωτη για κάθε $i\in\mathbb{N}_0$. (Βλ. πρόταση 6.2.5.) Κατά συνέπειαν, για κάθε $f\in\mathbb{J}_p$ και για κάθε $i\in\mathbb{N}_0$ έχουμε

$$f(\tfrac{1}{p^i}+\mathbb{Z}) = k_i(\tfrac{1}{p^i}+\mathbb{Z}) = \tfrac{k_i}{p^i}+\mathbb{Z}$$

για κάποιον $k_i\in\{0,1,...,p^i-1\}$. (Προφανώς, $k_0=0$.) Επομένως, για $i\geq 1$,

$$\begin{aligned} \tfrac{k_{i+1}}{p^i}+\mathbb{Z} &= p(\tfrac{k_{i+1}}{p^{i+1}}+\mathbb{Z}) = pf(\tfrac{1}{p^{i+1}}+\mathbb{Z}) = f(p(\tfrac{1}{p^{i+1}}+\mathbb{Z})) \\ &= f(\tfrac{1}{p^i}+\mathbb{Z}) = \tfrac{k_i}{p^i}+\mathbb{Z} \Rightarrow \tfrac{k_{i+1}-k_i}{p^i}\in\mathbb{Z} \Rightarrow k_{i+1}\equiv k_i (\operatorname{mod} p^i) \end{aligned}$$

και η απεικόνιση $\mathbb{J}_p \ni f \longmapsto \mathfrak{k} = ([k_i]_{p^i})_{i\in\mathbb{N}} = \left(\sum_{j=0}^{i-1} c_jp^j\right)_{i\in\mathbb{N}} \in \mathbb{Z}_{p\text{-adic}}$ καθορίζει έναν ισομορφισμό τόσον *ομάδων* όσον και *ακεραίων περιοχών*:

$$\boxed{\mathbb{J}_p \xrightarrow{\cong} \mathbb{Z}_{p\text{-adic}},} \tag{9.78}$$

όπου $c_i := \frac{\overline{k_{i+1}}-\overline{k_i}}{p^i}\in\mathbb{Z}$, $\forall i\in\mathbb{N}_0$ (με $\overline{k_0}:=0$) και ο $\overline{k_i}\in\{0,1,...,p^i-1\}$ προκύπτει από τον $k_i$ ύστερα από αναγωγή του $\operatorname{mod} p^i$, $\forall i\in\mathbb{N}$. (Βλ. εδ. C.2.31.) Ο αντίστροφός του είναι ο

$$\mathbb{Z}_{p\text{-adic}} \ni \left(\sum_{j=0}^{i-1} c_jp^j\right)_{i\in\mathbb{N}} \longmapsto f\in\mathbb{J}_p,$$

$$\text{όπου}\quad f(\tfrac{1}{p^i}+\mathbb{Z}) := \tfrac{1}{p^i}\left(\sum_{j=0}^{i-1} c_jp^j\right)+\mathbb{Z},\ \forall i\in\mathbb{N}.$$

Ο (9.78), περιοριζόμενος στις πολλαπλασιαστικές ομάδες των αντιστρεψίμων στοιχείων των ανωτέρω δακτυλίων, δίδει έναν ισομορφισμό ομάδων

$$\boxed{\mathrm{Aut}(\mathbb{Z}(p^\infty)) \xrightarrow{\cong} \mathbb{Z}^\times_{p\text{-adic}}}$$

μεταξύ τής ομάδας των αυτομορφισμών τής $(\mathbb{Z}(p^\infty),+)$ και τής ομάδας $(\mathbb{Z}^\times_{p\text{-adic}},\cdot)$ των $p$-αδικών ακεραίων αριθμών που διαθέτουν μη μηδενικό σταθερό όρο (στο $p$-αδικό τους ανάπτυγμα). Βλ. εδ. C.2.33.

► **Μη διασπώμενες μικτές ανηγμένες αβελιανές ομάδες**. Η κλάση των *μικτών*, μη πεπερασμένως παραγομένων και ανηγμένων αβελιανών ομάδων $(G,+)$ (ήτοι με $\{0_G\} \neq \mathrm{tors}(G) \sqsubset G$) είναι ευρύτατη[126]. Μάλιστα, εντός αυτής υφίσταται πληθώρα ομάδων που είναι *μη διασπώμενες*. Ένα απλό παράδειγμα αυτού τού είδους δίδεται στην πρόταση 9.7.55.

**9.7.52 Ορισμός.** Μια μικτή αβελιανή ομάδα καλείται **διασπώμενη** όταν η υποομάδα στρέψεώς της διαθέτει κάποιο συμπλήρωμα εντός αυτής.

**9.7.53 Παραδείγματα.** Οι μικτές πεπερασμένως παραγόμενες και οι μικτές διαιρετές αβελιανές ομάδες είναι διασπώμενες.

**9.7.54 Λήμμα.** *Ας υποθέσουμε ότι* $(G_p)_{p \text{ πρώτος}}$ *είναι μια οικογένεια (προσθετικών) αβελιανών ομάδων με τους δείκτες της ειλημμένους από το σύνολο των πρώτων αριθμών. Εάν η* $G_p$ *είναι* $p$*-ομάδα για κάθε πρώτον αριθμό* $p$, *τότε η πηλικοομάδα* $(\bigoplus_{p \text{ πρώτος}} G_p)/(\bigoplus_{p \text{ πρώτος}}^{\text{περ.}} G_p)$ *είναι διαιρετή.*

ΑΠΟΔΕΙΞΗ. Έστω $f + \bigoplus_{p \text{ πρώτος}}^{\text{περ.}} G_p \in (\bigoplus_{p \text{ πρώτος}} G_p)/(\bigoplus_{p \text{ πρώτος}}^{\text{περ.}} G_p)$ και έστω $n \in \mathbb{N}$. Αρκεί να αποδείξουμε ότι υπάρχει $f' \in \bigoplus_{p \text{ πρώτος}} G_p$, τέτοιο ώστε να ισχύει

$$f + \bigoplus_{p \text{ πρώτος}}^{\text{περ.}} G_p = nf' + \bigoplus_{p \text{ πρώτος}}^{\text{περ.}} G_p \ \left(\Leftrightarrow nf' - f \in \bigoplus_{p \text{ πρώτος}}^{\text{περ.}} G_p\right). \tag{9.79}$$

Για κάθε πρώτον αριθμό $p$ το $f(p)$ ανήκει στην $G_p$ και έχει ως τάξη του κάποια δύναμη τού $p$, ας πούμε την $p^{m(p)}$ $(m(p) \in \mathbb{N}_0)$. Θα προσδιορίσουμε το ζητούμενο στοιχείο $f'$ ορίζοντας το $f'(p)$ για κάθε πρώτον αριθμό $p$. Στην περίπτωση όπου $p \nmid n$,

$$\text{μκδ}(n,p) = 1 \underset{\text{B.2.13}}{\Longrightarrow} \text{μκδ}(n,p^{m(p)}) = 1 \underset{\text{B.2.8}}{\Longrightarrow} \left[\exists\,(k,l) \in \mathbb{Z}\times\mathbb{Z} : kn + lp^{m(p)} = 1\right].$$

Θέτοντας λοιπόν $k_\bullet := \min\{|k| \mid (k,l) \in \mathbb{Z}\times\mathbb{Z} : kn + lp^{m(p)} = 1\}$ ορίζουμε το $f'$ως ακολούθως:

$$\left\{\begin{array}{c}\text{πρώτοι}\\ \text{αριθμοί}\end{array}\right\} \ni p \overset{f'}{\longmapsto} f'(p) \in G_p,\ f'(p) := \begin{cases} 0_{G_p}, & \text{όταν } p \mid n,\\ k_\bullet f(p), & \text{όταν } p \nmid n.\end{cases}$$

*Ισχυρισμός*: $\mathrm{supp}(nf' - f) \subseteq \{p \text{ πρώτος} : p \mid n\}$. Για κάθε πρώτον αριθμό $p$ που δεν διαιρεί τον $n$ έχουμε

$$(nf' - f)(p) = nf'(p) - f(p) = (nk_\bullet - 1)f(p) = l\left(p^{m(p)} f(p)\right) = l\,0_{G_p} = 0_{G_p},$$

οπότε $p \notin \mathrm{supp}(nf' - f)$ και ο ισχυρισμός είναι αληθής. Άρα $\mathrm{supp}(nf' - f) < \infty$, απ' όπου έπεται η (9.79). □

[126]Προφανώς, οι $(\bigoplus_{p \text{ πρώτος}}^{\text{περ.}} \mathbb{Z}_p) \oplus \mathbb{Z}[\frac{1}{q}]$ και $(\bigoplus_{p \text{ πρώτος}}^{\text{περ.}} \mathbb{Z}_p) \oplus \mathbb{J}_q$ ανήκουν σε αυτήν για κάθε πρώτον αριθμό $q$.

**9.7.55 Πρόταση.** *Η αβελιανή ομάδα* $(\bigoplus_{p\ \text{πρώτος}} \mathbb{Z}_p, +)$ *είναι ανηγμένη, μικτή και μη διασπώμενη, έχουσα ως υποομάδα στρέψεώς της την*

$$\operatorname{tors}(\bigoplus_{p\ \text{πρώτος}} \mathbb{Z}_p) = \bigoplus_{p\ \text{πρώτος}}^{\text{περ.}} \mathbb{Z}_p. \tag{9.80}$$

ΑΠΟΔΕΙΞΗ. Επειδή η $(\mathbb{Z}_p, +)$ (ως πεπερασμένη κυκλική) είναι ανηγμένη για κάθε πρώτον αριθμό $p$, η $\bigoplus_{p\ \text{πρώτος}} \mathbb{Z}_p$ είναι ανηγμένη. (Βλ. πρόταση 9.7.43.) Από την άλλη μεριά, γνωρίζουμε (από το πόρισμα 9.7.45) ότι η $\bigoplus_{p\ \text{πρώτος}}^{\text{περ.}} \mathbb{Z}_p$ είναι ομάδα στρέψεως (και γνήσια υποομάδα τής $\bigoplus_{p\ \text{πρώτος}} \mathbb{Z}_p$), οπότε

$$\bigoplus_{p\ \text{πρώτος}}^{\text{περ.}} \mathbb{Z}_p \subseteq \operatorname{tors}(\bigoplus_{p\ \text{πρώτος}} \mathbb{Z}_p).$$

Θα δείξουμε ότι ισχύει και ο αντίστροφος εγκλεισμός. Προς τούτο θεωρούμε τυχόν στοιχείο $f \in \operatorname{tors}(\bigoplus_{p\ \text{πρώτος}} \mathbb{Z}_p)$. Προφανώς, $\operatorname{ord}(f) = n \in \mathbb{N}$. Αρκεί να δειχθεί ότι ο φορέας $\operatorname{supp}(f) := \{\, p \text{ πρώτος} \mid f(p) \neq [0]_p\}$ τού $f$ είναι *πεπερασμένος*. Για κάθε $p \in \operatorname{supp}(f)$ έχουμε $f(p) \in \mathbb{Z}_p \smallsetminus \{[0]_p\}$, οπότε $\operatorname{ord}(f(p)) = p$ (εντός τής $\mathbb{Z}_p$) και

$$nf = 0_{\bigoplus_{p\ \text{πρώτος}}^{\text{περ.}} \mathbb{Z}_p} \Rightarrow nf(p) = [0]_p \underset{2.3.8}{\Longrightarrow} p \mid n,$$

απ' όπου έπεται ότι $\operatorname{supp}(f) < \infty$ (διότι υπάρχουν μόνον πεπερασμένου πλήθους πρώτοι διαιρέτες τού $n$). Άρα η ισότητα (9.80) είναι αληθής και η $\bigoplus_{p\ \text{πρώτος}} \mathbb{Z}_p$ μικτή. Εάν η υποομάδα στρέψεως αυτής διέθετε κάποιο συμπλήρωμα, δηλαδή εάν

$$\exists K \in \mathbf{Subg}(\bigoplus_{p\ \text{πρώτος}} \mathbb{Z}_p) : \bigoplus_{p\ \text{πρώτος}} \mathbb{Z}_p = \bigoplus_{p\ \text{πρώτος}}^{\text{περ.}} \mathbb{Z}_p \oplus_{\text{εσ.}} K,$$

τότε θα ίσχυε $K \cong (\bigoplus_{p\ \text{πρώτος}} \mathbb{Z}_p)/(\bigoplus_{p\ \text{πρώτος}}^{\text{περ.}} \mathbb{Z}_p)$ και η $K$ θα ήταν μια *μη τετριμμένη* και (σύμφωνα με το λήμμα 9.7.54) *διαιρετή* υποομάδα τής ανηγμένης ομάδας $\bigoplus_{p\ \text{πρώτος}} \mathbb{Z}_p$, κάτι που είναι αδύνατο. Άρα η $\bigoplus_{p\ \text{πρώτος}} \mathbb{Z}_p$ είναι μη διασπώμενη. □