ΑΠΑΝΤΗΣΕΙΣ ΔΟΘΕΝΤΩΝ ΘΕΜΑΤΩΝ

ΘΕΜΑ 1ο Θεωρούμε το σύνολο

$$S := \left\{ \sum_{j=1}^{n} \lambda_j a_j \;\middle|\; \lambda_1, \dots, \lambda_n \in \mathbb{Z} \right\}.$$

Θέτοντας

$$\varepsilon_{j,l} := \begin{cases} 1, & \text{όταν } j = l, \\ 0, & \text{όταν } j \neq l, \end{cases}$$

για κάθε $j, l \in \{1, \dots, n\}$, έχουμε προφανώς

$$a_l = \sum_{j=1}^{n} \varepsilon_{j,l} a_j \in S, \;\; \forall l \in \{1, \dots, n\}.$$

Εάν κάποιος εκ των $a_1, \dots, a_n$ είναι > 0, τότε $S \cap \mathbb{N} \neq \varnothing$. Ωστόσο, το ότι $S \cap \mathbb{N} \neq \varnothing$ είναι *πάντοτε* αληθές, διότι ακόμη και εάν $a_l < 0$ για *κάθε* $l \in \{1, \dots, n\}$, έχουμε $-a_l = \sum_{j=1}^{n} (-\varepsilon_{j,l})\, a_j \in S \cap \mathbb{N}$. Ως εκ τούτου, το $S \cap \mathbb{N}$ διαθέτει *ελάχιστο* στοιχείο, ας πούμε το $d' = \sum_{j=1}^{n} k_j a_j$. Θα αποδείξουμε ότι $d' = d$. Πράγματι· για οιοδήποτε στοιχείο $m = \sum_{j=1}^{n} \lambda_j a_j$ τού S υπάρχει ένα μονοσημάντως ορισμένο ζεύγος $(q, r) \in \mathbb{Z} \times \mathbb{Z}$, ούτως ώστε να ισχύει

$$m = qd' + r, \text{ όπου } 0 \leq r < d'.$$

Υποθέτοντας ότι $r > 0$ καταλήγουμε σε κάτι το άτοπο, καθόσον $d' > r = \sum_{j=1}^{n} (\lambda_j - k_j q)\, a_j \in S$. Άρα $r = 0 \Longrightarrow d' \mid m$ και, ειδικότερα, $d' \mid a_j$ για κάθε $j \in \{1, \dots, n\}$. Επιπροσθέτως, για οιονδήποτε $\delta \in \mathbb{N}$, για τον οποίο ισχύει $\delta \mid a_1, \dots, \delta \mid a_n$, έχουμε

$$[\delta \mid k_1 a_1, \dots, \delta \mid k_n a_n] \Longrightarrow \delta \mid d' \Longrightarrow \delta \leq d',$$

οπότε τελικώς $d' = d$. □

ΘΕΜΑ 2ο "⇒": Έστω τυχόν $x \in HK$. Τότε $x = hk$ για κάποια $h \in H$ και $k \in K$. Επειδή το HK είναι εξ υποθέσεως υποομάδα τής G, έχουμε $x^{-1} \in HK$ (βλ. 3.2.15 (ii) (c)). Άρα $x^{-1} = h'k'$ για κάποια $h' \in H$ και $k' \in K$, και

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

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

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

Επειδή το HK υπετέθη ότι είναι υποομάδα τής G, έχουμε $\left(y^{-1}\right)^{-1} = y \in HK$. Άρα ισχύει και αντίστροφος εγκλεισμός $HK \supseteq KH$.

"$\Leftarrow$": Επειδή τα H και K είναι υποομάδες τής G, έχουμε $e_G \in H$ και $e_G \in K$, οπότε $e_G e_G = e_G \in HK$. Εν συνεχεία θεωρούμε τυχόντα στοιχεία $x_1, x_2 \in HK$. Εξ ορισμού υπάρχουν $h_1, h_2 \in H$ και $k_1, k_2 \in K$, τέτοια ώστε να ισχύουν οι ισότητες $x_1 = h_1 k_1$ και $x_2 = h_2 k_2$. Επιπροσθέτως,

$$k_1 h_2 \in KH = HK \Rightarrow \exists h_3 \in H \ \text{ και } \ \exists k_3 \in K : k_1 h_2 = h_3 k_3.$$

Κατά συνέπειαν,

$$\begin{aligned} x_1 x_2 &= (h_1 k_1)(h_2 k_2) = h_1 (k_1 h_2) k_2 \\ &= h_1 (h_3 k_3) k_2 = (\underbrace{h_1 h_3}_{\in H})(\underbrace{k_3 k_2}_{\in K}) \in HK. \end{aligned}$$

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

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

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

ΘΕΜΑ 3ο **Θεώρημα τού Cayley**. *Κάθε ομάδα* $(G, \cdot)$ *είναι ισόμορφη με μια υποομάδα τής ομάδας* $(\mathfrak{S}_G, \circ)$.

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

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

(Η απεικόνιση L_g είναι ενριπτική, διότι

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

αλλά *και* επιριπτική, διότι εάν $z \in G$, τότε $L_g\left(g^{-1}z\right) = gg^{-1}z = e_G z = z$). Η L_g ονομάζεται *εξ αριστερών μεταφορά μέσω τού* g. Έστω τώρα G' το υποσύνολο $\{ L_g \mid g \in G \}$ τής $\mathfrak{S}_G$. Η πράξη με την οποία είναι εφοδιασμένη η $\mathfrak{S}_G$ είναι η σύνθεση απεικονίσεων. Ως εκ τούτου, έχουμε

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

Κατά συνέπειαν, το γινόμενο δυο τυχόντων στοιχείων τού G' ανήκει στο G'. Το ταυτοτικό στοιχείο id_G τής $\mathfrak{S}_G$ ανήκει στο G' διότι ισούται με την L_{e_G}, ενώ το αντίστροφο τής L_g εντός τής $\mathfrak{S}_G$ ισούται με την $L_{g^{-1}}$ και ανήκει και αυτό στο G'. Τούτο σημαίνει ότι το σύνολο G' αποτελεί μια *υποομάδα* τής $\mathfrak{S}_G$ δυνάμει γνωστής προτάσεως (βλ. 3.2.15 (ii)). Η απεικόνιση

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

είναι προφανώς επιριπτική και μεταφέρει τον πολλαπλασιασμό τής G στη σύνθεση απεικονίσεων τής G' ($gh \longmapsto L_{gh} = L_g \circ L_h$). Εξάλλου, η εν λόγω απεικόνιση είναι και ενριπτική, αφού από την $L_g = L_h$ έπεται ότι $g = L_g(e_G) = L_h(e_G) = h$. Κατ' αυτόν τον τρόπο κατασκευάσαμε έναν ισομορφισμό μεταξύ τής G και τής υποομάδας G' τής ομάδας $\mathfrak{S}_G$. □

ΘΕΜΑ 4ο **1ο Θεώρημα Ισομορφισμών Δακτυλίων**. *Έστω* $f : R \longrightarrow S$ *ένας ομομορφισμός δακτυλίων. Τότε*

$$R/\mathrm{Ker}(f) \cong \mathrm{Im}(f) = f(R).$$

3ο Θεώρημα Ισομορφισμών Δακτυλίων. *Εάν ο* R *είναι ένας δακτύλιος και τα* I, J *ιδεώδη τού* R *με* $I \subseteq J$, *τότε έχουμε*

$$R/J \cong (R/I) \,/\, (J/I).$$

ΑΠΟΔΕΙΞΗ. Έστω f η απεικόνιση

$$f : R \longrightarrow (R/I) \,/\, (J/I), \ \ a \longmapsto (a + I) + (J/I), \ \forall a \in R.$$

Επειδή $f = \pi_2 \circ \pi_1$, όπου $\pi_1 : R \longrightarrow (R/I)$ και $\pi_2 : R/I \longrightarrow (R/I)\ /\ (J/I)$ οι φυσικοί επιμορφισμοί, η f είναι ένας (καλώς ορισμένος) επιμορφισμός δακτυλίων. Σύμφωνα με το 1ο θεώρημα ισομορφισμών,

$$R/\mathrm{Ker}\,(f) \cong (R/I)\ /\ (J/I)\ .$$

Όμως

$$\begin{aligned}
\mathrm{Ker}(f) &= \left\{ a \in R \mid\ f(a) = 0_{(R/I)\ /\ (J/I)} \right\} \\
&= \left\{ a \in R \mid\ \pi_2(\pi_1(a)) = 0_{(R/I)\ /\ (J/I)} \right\} \\
&= \left\{ a \in R \mid\ \pi_2(a+I) = 0_{(R/I)\ /\ (J/I)} \right\} \\
&= \{ a \in R \mid\ a + I \in \mathrm{Ker}\,(\pi_2) \} \\
&= \{ a \in R \mid\ a + I \in (J/I) \} = J,
\end{aligned}$$

απ' όπου έπεται το ζητούμενο. □

ΘΕΜΑ 5ο (i) Εάν $f(\mathsf{X}) = \sum_{j=0}^{n} a_j \mathsf{X}^j \in \mathbb{Z}[\mathsf{X}] \setminus \{0_{\mathbb{Z}[\mathsf{X}]}\}$ με $a_n \neq 0$, τότε ο αριθμός

$$\mathrm{cont}(f(\mathsf{X})) := \ \mu\kappa\delta(a_0, a_1, \ldots, a_n)$$

καλείται **περιεχόμενο** τού πολυωνύμου $f(\mathsf{X})$. Κάθε τέτοιου είδους πολυώνυμο με $\mathrm{cont}(f(\mathsf{X})) = 1$ καλείται **πρωταρχικό πολυώνυμο**.

Λήμμα τού Gauss. *Το γινόμενο δυο πρωταρχικών πολυωνύμων* ($\alpha\nu\eta\kappa\acute{o}\nu\tau\omega\nu\ \sigma\tau o$ $\mathbb{Z}[\mathsf{X}] \setminus \{0_{\mathbb{Z}[\mathsf{X}]}\}$) *είναι πάντοτε ένα πρωταρχικό πολυώνυμο*.

ΑΠΟΔΕΙΞΗ. Έστω ότι τα $f(\mathsf{X}), g(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}] \setminus \{0_{\mathbb{Z}[\mathsf{X}]}\}$ είναι δυο πρωταρχικά πολυώνυμα. Ας υποθέσουμε ότι το γινόμενό τους $f(\mathsf{X})g(\mathsf{X})$ *δεν* είναι πρωταρχικό πολυώνυμο. Έστω p ένας πρώτος αριθμός που διαιρεί το $\mathrm{cont}(f(\mathsf{X})g(\mathsf{X}))$ και έστω

$$\Psi_p : \mathbb{Z}[\mathsf{X}] \longrightarrow \mathbb{Z}_p[\mathsf{X}]$$

ο ομομορφισμός δακτυλίων ο οριζόμενος μέσω τού τύπου

$$\Psi_p(\sum_{j=0}^{n} a_j \mathsf{X}^j) := \sum_{j=0}^{n} [a_j]_p \mathsf{X}^j, \ \ \forall \sum_{j=0}^{n} a_j \mathsf{X}^j \in \mathbb{Z}[\mathsf{X}].$$

Τότε έχουμε προφανώς $\Psi_p(f(\mathsf{X})), \Psi_p(g(\mathsf{X})) \in \mathbb{Z}_p[\mathsf{X}]$ και

$$\Psi_p(f(\mathsf{X}))\Psi_p(g(\mathsf{X})) = \Psi_p(f(\mathsf{X})g(\mathsf{X})) = 0_{\mathbb{Z}_p[\mathsf{X}]},$$

οπότε *είτε* ο p διαιρεί κάθε συντελεστή τού πολυωνύμου $f(\mathsf{X})$ *είτε* ο p διαιρεί κάθε συντελεστή τού πολυωνύμου $g(\mathsf{X})$. Αυτό σημαίνει ότι *είτε* το $f(\mathsf{X})$ *είτε* το $g(\mathsf{X})$ *δεν* είναι πρωταρχικό. Άτοπο! □

(ii) **Πρόταση**. *Εάν ένα πολυώνυμο* $f(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]$ *είναι ανάγωγο εντός τού πολυωνυμικού δακτυλίου* $\mathbb{Z}[\mathsf{X}]$, *τότε είναι ανάγωγο και εντός τού* $\mathbb{Q}[\mathsf{X}]$.

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι το $f(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]$ δεν ανάγωγο εντός τού $\mathbb{Q}[\mathsf{X}]$. Τότε υπάρχουν πολυώνυμα $g(\mathsf{X}), h(\mathsf{X}) \in \mathbb{Q}[\mathsf{X}]$ βαθμού ≥ 1, τέτοια ώστε να ισχύει η ισότητα $f(\mathsf{X}) = g(\mathsf{X})h(\mathsf{X})$. Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι το $f(\mathsf{X})$ είναι πρωταρχικό (ειδάλλως θεωρούμε αντ' αυτού το $\frac{1}{\mathrm{cont}(f(\mathsf{X}))} f(\mathsf{X})$). Έστω a (και αντιστοίχως, b) το εκπ των παρονομαστών των συντελεστών τού $g(\mathsf{X})$ (και αντιστοίχως, τού $h(\mathsf{X})$). Τότε

$$a\ g(\mathsf{X}), b\ h(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}] \Rightarrow ab\ f(\mathsf{X}) = (a\ g(\mathsf{X}))(b\ h(\mathsf{X})) \in \mathbb{Z}[\mathsf{X}].$$

Θέτοντας $c_1 := \mathrm{cont}(a\ g(\mathsf{X}))$ και $c_2 := \mathrm{cont}(b\ h(\mathsf{X}))$ έχουμε

$$a\ g(\mathsf{X}) = c_1\ \widetilde{g}(\mathsf{X}), \ \ b\ h(\mathsf{X}) = c_2\ \widetilde{h}(\mathsf{X}),$$

για κάποια $\widetilde{g}(\mathsf{X}), \widetilde{h}(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]$ βαθμού ≥ 1 με $\mathrm{cont}(\widetilde{g}(\mathsf{X})) = \mathrm{cont}(\widetilde{h}(\mathsf{X})) = 1$. Προφανώς,

$$\left.\begin{array}{rl} ab\, f(\mathsf{X}) = c_1c_2\, \widetilde{g}(\mathsf{X})\widetilde{h}(\mathsf{X}), & \\ \mathrm{cont}(f(\mathsf{X})) = 1 \Longrightarrow \mathrm{cont}(ab\, f(\mathsf{X})) = ab, & \\ \mathrm{cont}(\widetilde{g}(\mathsf{X})\widetilde{h}(\mathsf{X})) \overset{\text{(Gauss)}}{=} 1 \Longrightarrow \mathrm{cont}(c_1c_2\, \widetilde{g}(\mathsf{X})\widetilde{h}(\mathsf{X})) = c_1c_2, & \end{array}\right\} \Longrightarrow ab = c_1c_2,$$

οπότε $f(t) = \widetilde{g}(t)\widetilde{h}(t) \in \mathbb{Z}[t]$, πράγμα που σημαίνει ότι το $f(t)$ δεν ανάγωγο ούτε εντός τού $\mathbb{Z}[t]$. □

ΘΕΜΑ 6ο (i) Επειδή μκδ$(m, n) = 1$, το θεώρημα 2.4.21 τού Euler περί ισοτιμιών δίδει

$$\left.\begin{array}{l} m^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n) \\ n^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m) \end{array}\right\} \Rightarrow mn \mid \left(m^{\varphi(n)} - 1\right)(n^{\varphi(m)} - 1),$$

οπότε $mn \mid m^{\varphi(n)}n^{\varphi(m)} - (m^{\varphi(n)} + n^{\varphi(m)} - 1) \Rightarrow mn \mid m^{\varphi(n)} + n^{\varphi(m)} - 1 \Rightarrow m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \,(\mathrm{mod}\, mn)$.

(ii) Επειδή μκδ$(5, 24) = 1$, η γραμμική ισοτιμία $5x \equiv 3 (\mathrm{mod}\ 24)$ διαθέτει ακριβώς μία λύση x_0 κατά μόδιο m (βλ. 2.4.35). Γράφοντας $24 = 2^3 \cdot 3$, μέσω γνωστού τύπου (βλ. 2.4.19) προσδιορίζουμε την τιμή $\varphi(24) = (2^3 - 2^2)(3 - 1) = 8$. Επειδή (κατά το θεώρημα 2.4.21 τού Euler περί ισοτιμιών) έχουμε $5^{\varphi(24)} \equiv 1 (\mathrm{mod}\, 24)$, μπορούμε να θέσουμε ως $x_0 := 5^{\varphi(24)-1} \cdot 3 = 5^7 \cdot 3 = 234\,375$. Ωστόσο, είθισται να παρέχουμε τη ζητούμενη λύση στην *ανηγμένη της μορφή*. Επειδή λοιπόν $234\,375 = 9765 \cdot 24 + 15$, έχουμε $[x_0]_{24} = [15]_{24}$, οπότε $5 \cdot 15 \equiv 3 (\mathrm{mod}\ 24)$. (Εναλλακτικώς, για να μην καταφύγουμε σε διαίρεση με έναν τόσο μεγάλο αριθμό, έχουμε τη δυνατότητα να επιχειρηματολογήσουμε ως εξής: $5^2 \equiv 1 (\mathrm{mod}\, 24)$, οπότε $5^6 \equiv 1 (\mathrm{mod}\, 24) \Rightarrow 5^7 \equiv 5 (\mathrm{mod}\, 24) \Rightarrow 5^7 \cdot 3 \equiv 15 (\mathrm{mod}\, 24)$.)

ΘΕΜΑ 7ο (i) Έστω H μια πεπερασμένως παραγόμενη υποομάδα τής $(\mathbb{Q}, +)$. Έστω ότι

$$H = \left\langle \frac{a_1}{d_1}, \frac{a_2}{d_2}, \ldots, \frac{a_r}{d_r} \right\rangle,$$

όπου $r \in \mathbb{N}$, $a_j \in \mathbb{Z},\ d_j \in \mathbb{Z} \setminus \{0\}, \forall j \in \{1, ..., r\}$. Εάν $d := \prod_{j=1}^{r} d_j$, τότε

$$\left.\begin{array}{c} \frac{a_1}{d_1} = \frac{a_1 d_2 \cdots d_r}{d} \in \left\langle \frac{1}{d} \right\rangle \\ \vdots \\ \frac{a_r}{d_r} = \frac{a_r d_1 \cdots d_{r-1}}{d} \in \left\langle \frac{1}{d} \right\rangle \end{array}\right\} \Longrightarrow H \subseteq \left\langle \frac{1}{d} \right\rangle,$$

και η H -ως υποομάδα μιας κυκλικής ομάδας- οφείλει να είναι κυκλική (βλ. 3.2.29 (i)).

(ii) Ας υποθέσουμε ότι η $(\mathbb{Q}, +)$ είναι πεπερασμένως παραγόμενη. Τότε, βάσει τού (i) και τού ότι δεν είναι τετριμμένη, θα ισχύει $\mathbb{Q} = \left\langle \frac{a}{b} \right\rangle$ για κάποια $a, b \in \mathbb{Z} \setminus \{0\}$. Επειδή $\frac{a}{2b} \in \mathbb{Q}$ θα πρέπει να υπάρχει $n \in \mathbb{Z}$, τέτοιο ώστε να ισχύει

$$\frac{a}{2b} = n\frac{a}{b} \Longrightarrow n = \frac{1}{2} \notin \mathbb{Z},$$

πράγμα άτοπο. Κατά συνέπειαν, η $(\mathbb{Q}, +)$ δεν είναι πεπερασμένως παραγόμενη.

(iii) Επειδή για κάθε φυσικό αριθμό $i \geq 1$, $\frac{1}{i!} = (i+1)\frac{1}{(i+1)!} \in H_{i+1}$ και $\frac{1}{(i+1)!} \notin H_i$, έχουμε προφανώς $H_i \subsetneqq H_{i+1}$. Για να δείξουμε ότι $\mathbb{Q} = \bigcup_{n \geq 1} H_n$, αρκεί να δείξουμε ότι για κάθε ρητό αριθμό $\frac{a}{b} \in \mathbb{Q}$ υπάρχει $i_0 \geq 1$ με $\frac{a}{b} \in H_{i_0}$. Τούτο όμως έπεται από το ότι (θέτοντας ως i_0 το $|b|$) λαμβάνουμε

$$\frac{a}{b} = \frac{a}{\mathrm{sign}(b)\,|b|} = \frac{\mathrm{sign}(b)a}{|b|} = (|b| - 1)!\ \mathrm{sign}(b)a\ \frac{1}{|b|!} \in H_{|b|}.$$

(iv) Το U περιέχει το 0 και είναι κλειστό ως προς την πρόσθεση (όπως κανείς μπορεί άμεσα να διαπιστώσει). Επιπροσθέτως, εάν $\frac{a}{b} \in U$, τότε και $\frac{-a}{b} \in U$, καθότι ο $-a$ είναι άρτιος και ο b περιττός αριθμός. Συνεπώς το U συγκροτεί μια (προφανώς *μη τετριμμένη*) υποομάδα τής $(\mathbb{Q}, +)$. Μάλιστα, $U \subsetneqq \mathbb{Q}$, αφού π.χ. $\frac{1}{3} \in \mathbb{Q} \setminus U$. (Εάν $\frac{1}{3} = \frac{a}{b}$, με a άρτιο και b περιττό, θα καταλήγαμε σε άτοπο συμπέρασμα τού τύπου:

άρτιος = περιττός.) Απομένει να δείξουμε ότι η U δεν είναι κυκλική. Εάν υπήρχε $x = \frac{a}{b} \in U$, $a \neq 0$, με $U = \langle x \rangle$, τότε π.χ. $\frac{a}{3b} \in U$ (καθότι το $3b$ παραμένει περιττός), οπότε θα υπήρχε κάποιος $n \in \mathbb{Z}$, τέτοιος ώστε να ισχύει

$$\frac{a}{3b} = nx = n\frac{a}{b} \Longrightarrow n = \frac{1}{3} \notin \mathbb{Z},$$

πράγμα άτοπο. Κατά συνέπειαν, η U δεν είναι κυκλική. □

<u>ΘΕΜΑ 8ο</u> (i) Κατ' αρχάς αποδεικνύουμε ότι το κέντρο $Z(G) := \{\, g \in G \mid xg = gx,\ \forall x \in G\}$ μιας ομάδας G αποτελεί μια *υποομάδα* τής G. Προφανώς, $e_G \in Z(G)$. Επιπροσθέτως, για τυχόντα $g, h \in Z(G)$ και $x \in G$ έχουμε (λόγω τής προσεταιριστικής ιδιότητας και τού ορισμού τού $Z(G)$)

$$xh = hx \Rightarrow h^{-1}(xh) = \left(h^{-1}h\right)x = e_G x = x \Rightarrow h^{-1}x = h^{-1}(xh)\,h^{-1} = xh^{-1}$$

και

$$x(gh^{-1}) = (xg)h^{-1} = (gx)h^{-1} = g(xh^{-1}) = g(h^{-1}x) = (gh^{-1})x \Rightarrow gh^{-1} \in Z(G).$$

Άρα το κέντρο $Z(G)$ είναι όντως μια υποομάδα τής G (βλ. 3.2.15 (iii)). Εν συνεχεία, αποδεικνύουμε ότι αυτό πρόκειται για μια *ορθόθετη* υποομάδα τής G. Προς τούτο αρκεί να θεωρηθούν τυχόντα στοιχεία $g \in Z(G)$ και $x \in G$ και να ληφθεί υπ' όψιν ότι

$$xg = gx \Rightarrow xgx^{-1} = gxx^{-1} = g \Rightarrow xZ(G)x^{-1} \subseteq Z(G).$$

(ii) Εάν η πηλικοομάδα $G/Z(G)$ είναι κυκλική, τότε υπάρχει κάποιο $g \in G$, τέτοιο ώστε να ισχύει $G/Z(G) = \langle gZ(G)\rangle$. Θεωρούμε τυχόντα στοιχεία $a, b \in G$. Τότε υπάρχουν $m, n \in \mathbb{Z}$:

$$\left.\begin{array}{c} aZ(G) = (gZ(G))^m = g^m Z(G) \\ bZ(G) = (gZ(G))^n = g^n Z(G) \end{array}\right\} \Rightarrow \exists h_1, h_2 \in Z(G) : a = g^m h_1,\ b = g^n h_2.$$

Άρα

$$\left.\begin{array}{r} ab = (g^m h_1)(g^n h_2) = g^m (h_1 g^n) h_2 = g^m (g^n h_1) h_2 = g^{m+n} h_1 h_2 \\ ba = (g^n h_2)(g^m h_1) = g^n (h_2 g^m) h_1 = g^n (g^m h_2) h_1 = g^{m+n} h_2 h_1 \\ h_1, h_2 \in Z(G) \Rightarrow h_1 h_2 = h_2 h_1 \end{array}\right\} \Rightarrow ab = ba$$

και η G είναι αβελιανή (και, ως εκ τούτου, η $G/Z(G)$ είναι τετριμμένη).

(iii) Η *ομάδα των τετρανίων*, ήτοι η υποομάδα $\mathbf{Q}$ τής $\mathrm{SU}_2(\mathbb{C})$ η παραγόμενη από τους πίνακες $\mathbf{j}$ και $\mathbf{k}$, έχει τάξη 8, καθότι

$$\mathbf{Q} = \{\pm\mathbf{I}_2, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\},\ (\mathbf{i} := \mathbf{jk}).$$

Σημειωτέον ότι η $\mathbf{Q}$ δεν είναι αβελιανή (αφού π.χ. $\mathbf{kj} \neq \mathbf{jk}$), οπότε $Z(\mathbf{Q}) \subsetneqq \mathbf{Q}$. Επιπροσθέτως, εκτός τού $\mathbf{I}_2$ *και* το $-\mathbf{I}_2$ ανήκει στο κέντρο τής $\mathbf{Q}$,διότι για κάθε πίνακα $\mathbf{A}$ ανήκοντα στην $\mathbf{Q}$ έχουμε

$$\mathbf{A}\cdot(-\mathbf{I}_2) = (-\mathbf{A})\cdot\mathbf{I}_2 = \mathbf{I}_2\cdot(-\mathbf{A}) = (-\mathbf{I}_2)\cdot\mathbf{A}.$$

Συνεπώς, $\{\pm\mathbf{I}_2\} \subseteq Z(\mathbf{Q})$. (Το ότι το κέντρο $Z(\mathbf{Q})$ τής $\mathbf{Q}$ είναι *μη τετριμμένη* υποομάδα τής $\mathbf{Q}$ μπορεί να αποδειχθεί *και εναλλακτικώς* κάνοντας χρήση τού θεωρήματος 3.7.8, αφού $|\mathbf{Q}| = 2^3$.) Επειδή λοιπόν το κέντρο $Z(\mathbf{Q})$ τής $\mathbf{Q}$ είναι μια *μη τετριμμένη*, *γνήσια* και *ορθόθετη* υποομάδα τής $\mathbf{Q}$, το θεώρημα 3.5.18 τού Lagrange μάς πληροφορεί ότι $|Z(\mathbf{Q})| \in \{2, 4\}$, οπότε $|\mathbf{Q}/Z(\mathbf{Q})| = \frac{|\mathbf{Q}|}{|Z(\mathbf{Q})|} \in \{2, 4\}$. Ως γνωστόν, κάθε ομάδα τάξεως 2 είναι *κυκλική* και ισόμορφη τής $(\mathbb{Z}_2, +)$ (βλ. πόρισμα 3.5.21 και θεώρημα 3.3.15 (ii)). Κατά συνέπειαν, εάν υποθέταμε ότι $|\mathbf{Q}/Z(\mathbf{Q})| = 2$, θα είχαμε $\mathbf{Q}/Z(\mathbf{Q}) \cong \mathbb{Z}_2$ και βάσει τού (ii) θα συμπεραίναμε ότι η ίδια η $\mathbf{Q}$ είναι αβελιανή, ήτοι κάτι το εσφαλμένο. Ως εκ τούτου,

$$|\mathbf{Q}/Z(\mathbf{Q})| = 4 \Rightarrow |Z(\mathbf{Q})| = 2 \Rightarrow Z(\mathbf{Q}) \cong \mathbb{Z}_2.$$

(Μάλιστα, βάσει των προαναφερθέντων, $Z(\mathbf{Q}) = \{\pm\mathbf{I}_2\}$.)

(iv) Εργαζόμαστε με «εις άτοπον απαγωγή». Υποθέτουμε ότι υπάρχει κάποιο στοιχείο $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{id}\}$, τέτοιο ώστε να ισχύει $\sigma \circ \tau = \tau \circ \sigma$ ή -ισοδυνάμως- $\sigma \circ \tau \circ \sigma^{-1} = \tau$, *για κάθε* $\tau \in \mathfrak{S}_n$. Το σ (σύμφωνα με γνωστό θεώρημα, βλ. 3.4.13) γράφεται υπο τη μορφή επαλλήλων συνθέσεων (πεπερασμένου πλήθους) ανά δύο ξένων μεταξύ τους κύκλων μήκους ≥ 2, ας πούμε $\sigma = c_1 \circ c_2 \circ \cdots \circ c_\nu$. Έστω ότι $c_1 = [a_1\ a_2\ \cdots\ a_k]$, για κάποιον $k \in \mathbb{N}$, $2 \leq k \leq n$. Εξετάζουμε δύο περιπτώσεις χωριστά:

Περίπτωση πρώτη. Εάν $k \geq 3$, τότε θεωρώντας ως τ τον 2-κύκλο $[a_1\ a_2]$ καταλήγουμε σε άτοπο, καθόσον

$$\sigma \circ \tau \circ \sigma^{-1} = \sigma \circ [a_1\ a_2] \circ \sigma^{-1} = [\sigma(a_1)\ \sigma(a_2)] = [a_2\ a_3] \neq [a_1\ a_2] = \tau.$$

Περίπτωση δεύτερη. Εάν $k = 2$, τότε θεωρώντας ως τ τον 3-κύκλο $[a_1\ a_2\ a_3]$ καταλήγουμε εκ νέου σε άτοπο, καθόσον

$$\sigma \circ \tau \circ \sigma^{-1} = \sigma \circ [a_1\ a_2\ a_3] \circ \sigma^{-1} = [\sigma(a_1)\ \sigma(a_2)\ \sigma(a_3)] = [a_2\ a_1\ \sigma(a_3)],$$

όπου $\sigma(a_3) \notin \{a_1, a_2\}$ και $\left(\sigma \circ \tau \circ \sigma^{-1}\right)(a_2) = a_1 \neq a_3 = \tau(a_2)$. Άρα τελικώς $Z(\mathfrak{S}_n) \cong \{\mathrm{id}\}$ για κάθε φυσικό αριθμό $n \geq 3$. □

<u>ΘΕΜΑ 9ο</u> Έστω ότι τα K και L είναι δυο σώματα, η χαρακτηριστική των οποίων δεν ισούται ούτε με 2 ούτε με 3. Εάν η $f : K \longrightarrow L$ είναι μια απεικόνιση που πληροί τις συνθήκες

$$f(x+y) = f(x) + f(y),\ \forall x, y \in K, \quad f(1_K) = 1_L, \quad f(x^3) = f(x)^3,\ \forall x \in K,$$

ζητείται να αποδειχθεί ότι η f είναι ένας ομομορφισμός σωμάτων, δηλαδή ότι

$$f(xy) = f(x)f(y),\ \forall x, y \in K.$$

ΑΠΟΔΕΙΞΗ. **Βήμα 1ο**. Κατ' αρχάς ισχύει η ισότητα

$$f(x^2) = f(x)^2,\ \forall x \in K. \tag{$\star$}$$

Πράγματι· λόγω τής τρίτης εκ των ανωτέρω συνθηκών έχουμε για κάθε $x \in K$:

$$f((x + 1_K)^3) = f(x + 1_K)^3.$$

Μέσω των ανωτέρω συνθηκών το αριστερό μέλος τής τελευταίας ισότητας γράφεται ως

$$f(x^3 + 3x^2 + 3x + 1_K) = f(x^3) + 3f(x^2) + 3f(x) + f(1_K) = f(x)^3 + 3f(x^2) + 3f(x) + 1_L.$$

και το δεξιό της μέλος ως

$$f(x + 1_K)^3 = (f(x) + f(1_K))^3 = (f(x) + 1_L)^3 = f(x)^3 + 3f(x)^2 + 3f(x) + 1_L.$$

Κατά συνέπειαν,

$$\left.\begin{array}{c} 3\left(f(x^2) - f(x)^2\right) = (1_L + 1_L + 1_L)\left(f(x^2) - f(x)^2\right) = 0_L \\ \text{χαρ}(L) \neq 3 \Rightarrow 1_L + 1_L + 1_L \neq 0_L \end{array}\right\} \Rightarrow f(x^2) = f(x)^2.$$

Βήμα 2ο. Θεωρούμε τυχόντα στοιχεία $x, y \in K$. Επειδή $2xy = (x+y)^2 - x^2 - y^2$, ύστερα από εφαρμογή τής f σε αμφότερα τα μέλη αυτής τής ισότητας η ($\star$) δίδει

$$\begin{aligned} 2f(xy) &= f((x+y)^2) - f(x^2) - f(y^2) = f(x+y)^2 - f(x)^2 - f(y)^2 \\ &= (f(x) + f(y))^2 - f(x)^2 - f(y)^2 = 2f(x)f(y) \end{aligned}$$

οπότε

$$\left.\begin{array}{c} 2\left(f(xy) - f(x)f(y)\right) = (1_L + 1_L)\left(f(xy) - f(x)f(y)\right) = 0_L \\ \text{χαρ}(L) \neq 2 \Rightarrow 1_L + 1_L \neq 0_L \end{array}\right\} \Rightarrow f(xy) = f(x)f(y)$$

και η f είναι όντως ένας ομομορφισμός σωμάτων. □

ΘΕΜΑ 10ο (i) Δίδεται το πολυώνυμο $g(\mathsf{X}) = \mathsf{X}^4 + 5\mathsf{X}^3 - 9\mathsf{X}^2 - 14\mathsf{X} + 24 \in \mathbb{Z}[\mathsf{X}]$. Έστω $r \in \mathbb{Q}$,τέτοιος ώστε να ισχύει η ισότητα $g(r) = 0$. **Ισχυρισμός:** $\boxed{r = -6}$.

ΠΡΩΤΗ ΑΠΟΔΕΙΞΗ ΙΣΧΥΡΙΣΜΟΥ. Εκφράζοντας τον r υπό τη μορφή $r = \frac{\lambda}{\mu}$, όπου $\lambda \in \mathbb{Z}$, $\mu \in \mathbb{Z}\setminus\{0\}$ και μκδ$(\lambda, \mu) = 1$, το κριτήριο ρητών θέσεων μηδενισμού 5.5.1 μας πληροφορεί ότι

$$\lambda \mid 24 \ \text{ και } \ \mu \mid 1,$$

οπότε $\lambda \in \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm8, \pm12, \pm24\}, \mu \in \{\pm1\} \Rightarrow r \in \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm8, \pm12, \pm24\}$. Εκτελώντας απευθείας πράξεις διαπιστώνουμε ότι

$g(1) = 7 \neq 0,$	$g(-1) = 25 \neq 0,$	$g(2) = 16 \neq 0,$	$g(-2) = -8 \neq 0,$
$g(3) = 117 \neq 0,$	$g(-3) = -69 \neq 0,$	$g(4) = 400 \neq 0,$	$g(-4) = -128 \neq 0,$
$g(6) = 1992 \neq 0,$	$g(-6) = 0,$	$g(8) = 5992 \neq 0,$	$g(-8) = 1096 \neq 0,$
$g(12) = 27\,936 \neq 0,$	$g(-12) = 10\,992 \neq 0,$	$g(24) = 395\,400 \neq 0,$	$g(-24) = 257\,832 \neq 0.$

ΔΕΥΤΕΡΗ ΑΠΟΔΕΙΞΗ ΙΣΧΥΡΙΣΜΟΥ. Για να αποφύγουμε τις πολλές πράξεις επιχειρηματολογούμε ως εξής: Προφανώς, $r \in \mathbb{Z}$, διότι το $g(\mathsf{X})$ είναι μονικό. Κατά το (ii) τής προτάσεως 5.3.2,

$$g(r) = 0 \Rightarrow \mathsf{X} - r \mid g(\mathsf{X}) \Rightarrow \exists h(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}] : g(\mathsf{X}) = (\mathsf{X} - r)\, h(\mathsf{X}),$$

οπότε $g(1) = 7 = (1 - r)h(1) \Rightarrow 1 - r \mid 7 \Rightarrow 1 - r \in \{\pm1, \pm7\}$. Άρα $r \in \{0, 2, -6, 8\}$. Αρκεί να παρατηρήσουμε ότι

$$g(0) = 24 \neq 0, \quad g(2) = 16 \neq 0, \quad g(-6) = 0, \quad g(8) = 5992 \neq 0$$

(ii) Δοθέντων δυο ακεραίων αριθμών a, b, θεωρούμε το πολυώνυμο

$$f(\mathsf{X}) = \mathsf{X}^4 + a\mathsf{X}^2 + b^2 \in \mathbb{Z}[\mathsf{X}].$$

Ζητείται να αποδειχθεί ότι το $f(\mathsf{X})$ δεν είναι ανάγωγο εντός τού $\mathbb{Q}[\mathsf{X}]$ *εάν και μόνον εάν* τουλάχιστον ένας εκ των $a^2 - 4b^2, 2b - a, -2b - a$ ισούται με το τετράγωνο κάποιου ακεραίου αριθμού.

ΑΠΟΔΕΙΞΗ. "$\Leftarrow$" Εάν $\exists c \in \mathbb{Z} : a^2 - 4b^2 = c^2$, τότε

$$f(\mathsf{X}) = \left(\mathsf{X}^2 - \frac{a}{2}\right)^2 - \left(\frac{c}{2}\right)^2 = \left(\mathsf{X}^2 - \left(\frac{a-c}{2}\right)\right)\left(\mathsf{X}^2 - \left(\frac{a+c}{2}\right)\right).$$

Εάν $\exists c \in \mathbb{Z} : 2b - a = c^2$, τότε

$$f(\mathsf{X}) = \left(\mathsf{X}^2 + c\mathsf{X} + b\right)\left(\mathsf{X}^2 - c\mathsf{X} + b\right).$$

Τέλος, εάν $\exists c \in \mathbb{Z} : -2b - a = c^2$, τότε

$$f(\mathsf{X}) = \left(\mathsf{X}^2 + c\mathsf{X} - b\right)\left(\mathsf{X}^2 - c\mathsf{X} - b\right).$$

"$\Rightarrow$" Υποθέτουμε ότι το $f(\mathsf{X})$ δεν είναι ανάγωγο εντός τού $\mathbb{Q}[\mathsf{X}]$. Το $f(\mathsf{X})$ θα διαθέτει κάποιο πολυώνυμο (ανήκον στον $\mathbb{Q}[\mathsf{X}]$) βαθμού 1 ή 2 ως παράγοντά του. Εάν το πολυώνυμο αυτό είναι βαθμού 1, τότε το $f(\mathsf{X})$ έχει προφανώς μια θέση μηδενισμού $r \in \mathbb{Q}$. Εάν $r = 0$, τότε $b = 0$, οπότε το $a^2 - 4b^2 = a^2$ είναι το τετράγωνο τού ακεραίου αριθμού a. Εάν $r \neq 0$, τότε $r \neq -r$ και $f(r) = f(-r) = 0$, οπότε (σύμφωνα με τα 5.3.2 (ii) και 5.3.3)

$$\left.\begin{array}{l} \mathsf{X} - r \mid f(\mathsf{X}) \\ \mathsf{X} + r \mid f(\mathsf{X}) \end{array}\right\} \Rightarrow (\mathsf{X} - r)\,(\mathsf{X} + r) = \mathsf{X}^2 - r^2 \mid f(\mathsf{X}).$$

Αυτό σημαίνει ότι όταν το $f(\mathsf{X})$ έχει έναν πρωτοβάθμιο παράγοντα (εντός τού $\mathbb{Q}[\mathsf{X}]$) και $\mathsf{X} \nmid f(\mathsf{X})$, τότε το $f(\mathsf{X})$ έχει κατ' ανάγκην και κάποιο δευτεροβάθμιο πολυώνυμο ως παράγοντά του (εντός τού $\mathbb{Q}[\mathsf{X}]$). Ως εκ τούτου, μπορούμε από τούδε και στο εξής (δίχως βλάβη τής γενικότητας) να υποθέσουμε (κατά την

υπολειπόμενη αποδεικτική πορεία) ότι το $f(\mathsf{X})$ έχει κάποιο *δευτεροβάθμιο* πολυώνυμο ως παράγοντά του (εντός τού $\mathbb{Q}[\mathsf{X}]$), ήτοι ότι

$$\exists g(\mathsf{X}), h(\mathsf{X}) \in \mathbb{Q}[\mathsf{X}] : f(\mathsf{X}) = g(\mathsf{X})h(\mathsf{X}),$$

με $\deg(g(\mathsf{X})) = \deg(h(\mathsf{X})) = 2$. Έστω κ (και αντιστοίχως, λ) το εκπ των παρονομαστών των συντελεστών τού $g(\mathsf{X})$ (και αντιστοίχως, τού $h(\mathsf{X})$). Τότε

$$f(t) = \widetilde{g}(t)\widetilde{h}(t), \quad \widetilde{g}(\mathsf{X}), \widetilde{h}(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}],$$

όπου $\widetilde{g}(\mathsf{X}) := \frac{1}{\mathrm{cont}(\kappa\ g(\mathsf{X}))}\kappa g(\mathsf{X})$, $\widetilde{h}(\mathsf{X}) := \frac{1}{\mathrm{cont}(\lambda\ h(\mathsf{X}))}\lambda h(\mathsf{X})$ (όπως στην απόδειξη τού (ii) τού θέματος 5), με $\deg(\widetilde{g}(\mathsf{X})) = \deg(\widetilde{h}(\mathsf{X})) = 2$. Επειδή το $f(\mathsf{X})$ είναι μονικό, τα $\widetilde{g}(\mathsf{X}), \widetilde{h}(\mathsf{X})$ θα γράφονται υπό την μορφή

$$\widetilde{g}(\mathsf{X}) = \mathsf{X}^2 + s\mathsf{X} + t, \quad \widetilde{h}(\mathsf{X}) = \mathsf{X}^2 + u\mathsf{X} + v,$$

όπου s, t, u, v είναι κατάλληλοι *ακέραιοι*, οπότε το $f(\mathsf{X})$ θα παραγοντοποιείται εν τέλει εντός τού $\mathbb{Z}[\mathsf{X}]$ ως εξής:

$$f(\mathsf{X}) = \left(\mathsf{X}^2 + s\mathsf{X} + t\right)\left(\mathsf{X}^2 + u\mathsf{X} + v\right).$$

Εξισώνοντας τους συντελεστές τού X^3 στα δύο μέλη λαμβάνουμε $u = -s$. Επομένως, κατόπιν εξισώσεως των συντελεστών των $1, \mathsf{X}, \mathsf{X}^2$ στα δύο μέλη συμπεραίνουμε ότι

$$vt = b^2, \ \ s(v-t) = 0, \ \ t + v = s^2 + a.$$

Εάν $s = 0$, τότε $a^2 - 4b^2 = (t+v)^2 - 4vt = (t-v)^2$, ήτοι το $a^2 - 4b^2$ ισούται με το τετράγωνο τού ακεραίου αριθμού $t - v$. Εάν $s \neq 0$, τότε $v = t \Rightarrow t^2 = b^2 \Rightarrow t = \pm b$. Στην περίπτωση κατά την οποία $v = t = b$ έχουμε $2b - a = s^2$ (= το τετράγωνο τού ακεραίου s), ενώ στην περίπτωση κατά την οποία $v = t = -b$ έχουμε $-2b - a = s^2$ (= το τετράγωνο τού ακεραίου s). □

- **Τα θεωρητικά θέματα 1, 2, 3, 4 και 5 είχαν διδαχθεί κατά τη διάρκεια των παραδόσεων.**
- **Τα (i) και (ii) τού θέματος 6 είχαν δοθεί ως ασκήσεις και λυθεί από τον βοηθό στις ώρες των φροντιστηρίων (βλ. ασκήσεις 11 και 13 (ii) τού 4ου καταλόγου προτεινομένων ασκήσεων).**
- **Το θέμα 7 απαιτούσε μόνον τη γνώση τού τι είναι μια πεπερασμένως παραγόμενη ομάδα, τού ότι κάθε υποομάδα μιας κυκλικής ομάδας είναι κυκλική, καθώς και κάποια στοιχειώδη αριθμοθεωρητικά επιχειρήματα.**
- **Στο θέμα 10 υπεισήρχοντο αρκετές πράξεις και παραγοντοποιήσεις. Ωστόσο, τα απαιτούμενα κριτήρια αναγωγιμότητας πολυωνύμων (με συντελεστές ειλημμένους από τους ακεραίους και τους ρητούς) ήταν τα πλέον χρηστικά (και εν πολλοίς κοινότοπα).**
- **Τα θέματα 8 και 9 ήταν κάπως πιο απαιτητικά. Το 8 προϋπέθετε καλή γνώση τού κεφαλαίου περί ομάδων και συνδυασμό αρκετών θεωρητικών αποτελεσμάτων, ενώ το 9 προϋπέθετε έναν κάποιο βαθμό ευρηματικότητας (για την εφαρμογή τού «λυτρωτικού» τεχνάσματος τού πρώτου βήματος).**