Πανεπιστήμιο Κρήτης, Τμήμα Μαθηματικών και Εφ. Μαθ. **Άλγεβρα Ι (MEM 221)**

Χειμερινό Εξάμηνο 2020-2021, Εξέταση Ιανουαρίου **Εξεταστής: Δημήτριος Νταής**

ΛΥΣΕΙΣ ΘΕΜΑΤΩΝ

ΘΕΜΑ 1ο (i) Έστω $p > 5$ ένας πρώτος αριθμός. Προφανώς, $240 = 2^4 \cdot 3 \cdot 5$ και το μικρό θεώρημα τού Fermat (βλ. πόρισμα 2.4.13 ή πόρισμα 5.1.31) δίδει

$$3 \nmid p \Longrightarrow p^2 \equiv 1(\text{mod } 3) \underset{2.4.4\,(\text{iii})}{\Longrightarrow} p^8 = (p^2)^4 \equiv 1^4 = 1(\text{mod } 3) \tag{1}$$

και

$$5 \nmid p \Longrightarrow p^4 \equiv 1(\text{mod } 5) \underset{2.4.4\,(\text{iii})}{\Longrightarrow} p^8 = (p^4)^2 \equiv 1^2 = 1(\text{mod } 5). \tag{2}$$

Επειδή $\phi(16) = \phi(2^4) \underset{2.4.18}{=} 2^3 = 8$, από το θεώρημα τού Euler περί ισοτιμιών (βλ. θεώρημα 2.4.22 ή πόρισμα 5.1.30) λαμβάνουμε

$$\text{μκδ}(p, 16) = \text{μκδ}(p, 2^4) \underset{2.3.17}{=} \text{μκδ}(p, 2) = 1 \Longrightarrow p^8 \equiv 1(\text{mod } 16). \tag{3}$$

Από τις (1), (2), (3) και το πόρισμα 2.4.9 έπεται ότι $p^8 \equiv 1(\text{mod } 240)$. □

(ii) Για την ακολουθία

$$u_n := 2^n + 3^n + 6^n - 1, \quad n \in \mathbb{N},$$

θεωρούμε το σύνολο $\mathcal{A} := \{k \in \mathbb{N} \mid \text{μκδ}(u_n, k) = 1, \forall n \in \mathbb{N}\}$. Θα δειχθεί ότι $\mathcal{A} = \{1\}$ μέσω «εις άτοπον απαγωγής». Εάν υπήρχε κάποιος $k \in \mathcal{A}$, $k \geq 2$, και p ήταν κάποιος πρώτος αριθμός με $p \mid k$, τότε θα έπρεπε (λόγω τού πορίσματος 2.2.12) να ισχύει $\text{μκδ}(u_n, p) = 1$ ή, ισοδυνάμως, $p \nmid u_n$ *για κάθε* $n \in \mathbb{N}$. Αρκεί λοπόν (για να καταλήξουμε στο επιθυμητό άτοπο) να αποδείξουμε ότι *κάθε* πρώτος αριθμός p είναι διαιρέτης τού u_n *για τουλάχιστον έναν* $n \in \mathbb{N}$. Οι πρώτοι αριθμοί $p = 2$ και $p = 3$ είναι διαιρέτες τού $u_2 = 48$. Εάν p είναι ένας πρώτος αριθμός ≥ 5, τότε από το μικρό θεώρημα τού Fermat (βλ. πόρισμα 2.4.13 ή πόρισμα 5.1.31) λαμβάνουμε

$$2^{p-1} \equiv 3^{p-1} \equiv 6^{p-1} \equiv 1(\text{mod } p)$$

και, κατ' επέκταση, $3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} \equiv (3 + 2 + 1)(\text{mod } p) = 6(\text{mod } p)$ ή, ισοδυνάμως,

$$6(2^{p-2} + 3^{p-2} + 6^{p-2} - 1) \equiv 0(\text{mod } p).$$

Τουτέστιν, $p \mid 6u_{p-2} \underset{2.2.9}{\Longrightarrow} p \mid u_{p-2}$. □

ΘΕΜΑ 2ο (i) Έστω ότι n, m είναι δυο φυσικοί αριθμοί ≥ 2 με $m \mid n$. Εάν

$$H(n, m) := \left\{[k]_n \in \mathbb{Z}_n^\times \mid [k]_m = [1]_m\right\},$$

τότε το $H(n, m)$ είναι μη κενό σύνολο (διότι $[1]_n \in H(n, m)$). Επιπροσθέτως, $H(n, m) \sqsubseteq \mathbb{Z}_n^\times$, διότι για $[k]_n, [l]_n, \in H(n, m)$ έχουμε

$$[kl]_m = [k]_m[l]_m = [1]_m[1]_m = [1]_m \Longrightarrow [k]_n[l]_n = [kl]_n \in H(n, m).$$

(Βλ. πόρισμα 3.2.19.) Εν συνεχεία ορίζουμε τη διμελή σχέση

$$f = \{([k]_n, [k]_m) \in \mathbb{Z}_n \times \mathbb{Z}_m \mid k \in \mathbb{Z}\}.$$

Ισχυρισμός πρώτος. Η f είναι μια (καλώς ορισμένη) απεικόνιση:

$$\mathbb{Z}_n \ni [k]_n \overset{f}{\longmapsto} [k]_m \in \mathbb{Z}_m.$$

Πράγματι· εάν υποτεθεί ότι $([a]_n, [b]_m) \in f,\ \ ([a]_n, [c]_m) \in f$, τότε (εξ ορισμού)

$$([a]_n, [b]_m) = ([k]_n, [k]_m),\ \ ([a]_n, [c]_m) = ([k']_n, [k']_m),$$

για κάποιους $k, k' \in \mathbb{Z}$. Επομένως,

$$[k]_n = [a]_n = [k']_n,\ \ [b]_m = [k]_m,\ \ [c]_m = [k']_m,$$

οπότε $n \mid k - k'$, $m \mid b - k$, και $m \mid k' - c$ και, κατ' επέκταση

$$\left.\begin{array}{l} m \mid n \text{ (εξ υπ.)} \\ n \mid k - k' \end{array}\right\} \underset{2.1.5\,(v)}{\Longrightarrow} m \mid k - k'$$

και

$$m \mid b - c = (b - k) + (k - k') + (k' - c) \Longrightarrow [b]_m = [c]_m.$$

Ισχυρισμός δεύτερος. $f(\mathbb{Z}_n^\times) \subseteq \mathbb{Z}_m^\times$. Πράγματι· για οιοδήποτε $[k]_n \in \mathbb{Z}_n^\times$ έχουμε

$$\left.\begin{array}{l} \text{μκδ}(k, n) = 1 \\ m \mid n \text{ (εξ υπ.)} \end{array}\right\} \underset{2.2.12}{\Longrightarrow} \text{μκδ}(k, m) = 1 \Longrightarrow f([k]_n) = [k]_m \in \mathbb{Z}_m^\times.$$

Ισχυρισμός τρίτος. Ο περιορισμός $\widetilde{f} := f|_{\mathbb{Z}_n^\times} : \mathbb{Z}_n^\times \longrightarrow \mathbb{Z}_m^\times$ αποτελεί έναν ομομορφισμό (πολλαπλασιαστικών) ομάδων:

$$\widetilde{f}([k]_n[l]_n) = \widetilde{f}([kl]_n) = [kl]_m = [k]_m[l]_m = \widetilde{f}([k]_n)\widetilde{f}([l]_n),\ \forall (k, l) \in \mathbb{Z} \times \mathbb{Z}.$$

Ισχυρισμός τέταρτος. Ο πυρήνας τού $\widetilde{f}$ ισούται με την $H(n, m)$:

$$\text{Ker}(\widetilde{f}) = \left\{ [k]_n \in \mathbb{Z}_n^\times \;\middle|\; \widetilde{f}([k]_n) = [1]_m \right\} = \left\{ [k]_n \in \mathbb{Z}_n^\times \mid [k]_m = [1]_m \right\} =: H(n, m).$$

Ισχυρισμός πέμπτος. Ο $\widetilde{f}$ είναι επιμορφισμός. Προς τούτο αρκεί να δειχθεί ότι *για κάθε* $k' \in \mathbb{Z}$ με $\text{μκδ}(k', m) = 1$,

$$\exists k \in \mathbb{Z} : [\text{μκδ}(k, n) = 1 \ \text{ κα } \ \widetilde{f}([k]_n) = [k]_m = [k']_m].$$

Εξ υποθέσεως, $\exists q \in \mathbb{N} : n = mq$. Εάν θέσουμε $d := \text{μκδ}(k', n)$, τότε

$$\text{μκδ}(m, d) = \text{μκδ}(m, \text{μκδ}(k', n)) \underset{2.2.16}{=} \text{μκδ}(m, k', n) = \text{μκδ}(k', m) = 1$$

(διότι $m \mid n$), απ' όπου έπεται ότι

$$\left.\begin{array}{l} n = mq,\ d \mid n \\ \text{μκδ}(m, d) = 1 \end{array}\right\} \underset{2.2.9}{\Longrightarrow} d \mid q \Rightarrow \exists q' \in \mathbb{N} : q = q'd.$$

Έστω t το γινόμενο όλων των πρώτων διαιρετών τού q' που δεν διαιρούν το d όταν $q' \geq 2$ και $t := 1$ όταν $q' = 1$. Θέτουμε $k := k' + tm$, παρατηρούμε ότι $[k']_m = [k]_m$, θεωρούμε τυχόντα πρώτο διαιρέτη p τού n και εξετάζουμε 4 περιπτώσεις χωριστά.

Περίπτωση πρώτη. Εάν $p \mid m$, τότε $\text{μκδ}(k', m) = 1 \Rightarrow p \nmid k' \Rightarrow p \nmid k$.

Περίπτωση δεύτερη. Εάν $p \nmid m$, $p \mid q'$ και $p \mid d$, τότε $p \nmid t$ (εξ ορισμού τού t), οπότε

$$[p \mid d \ \text{ και } \ d \mid k'] \Rightarrow p \mid k' \ \text{ και } \ [p \mid k' \ \text{ και } \ p \nmid tm] \Rightarrow p \nmid k.$$

Περίπτωση τρίτη. Εάν $p \nmid m$, $p \mid q'$ και $p \nmid d$, τότε $[p \mid t \ \text{ και } \ p \nmid k'] \Rightarrow p \nmid k$.

Περίπτωση τέταρτη. Εάν $p \nmid m$ και $p \nmid q'$, τότε $p \mid d$ (διότι $n = mq'd$), οπότε έχουμε $[p \mid k' \text{ και } p \nmid t] \Rightarrow p \nmid k$. Επειδή κανένας εκ των πρώτων διαιρετών τού n δεν διαιρεί το k, έχουμε μκδ$(k, n) = 1$ και, κατ' επέκταση, $[k]_n \in \mathbb{Z}_n^\times$.

Ισχυρισμός έκτος. $\mathbb{Z}_n^\times / H(n, m) \cong \mathbb{Z}_m^\times$. Είναι αληθής λόγω τού 1ου *θεωρήματος ισομορφισμών ομάδων* 5.5.3 και τής προηγηθείσας επαληθεύσεως των ανωτέρω ισχυρισμών. □

(ii) Η τάξη τής $G := \mathbb{Z}_5 \times \mathbb{Z}_5^\times$ ισούται με $5 \cdot \phi(5) = 5 \cdot 4 = 20$. Σημειωτέον ότι $[2]_5 \in \mathbb{Z}_5 \cap \mathbb{Z}_5^\times$. Επιπροσθέτως, εντός τής G λαμβάνουμε αφ' ενός μεν

$$([2]_5, [2]_5)^{10} = ([10 \cdot 2]_5, [2^{10}]_5) = ([20]_5, [2^4]_5[2^4]_5[2^2]_5) = ([0]_5, [4]_5) \neq ([0]_5, [1]_5) = e_G,$$

διότι $2^4 \equiv 1 (\text{mod } 5) \Rightarrow [2^4]_5 = [1]_5$, αφ' ετέρου δε

$$([2]_5, [2]_5)^{20} = ([0]_5, [4]_5)^2 = ([0]_5, [16]_5) = ([0]_5, [1]_5) = e_G.$$

Από την πρόταση 3.4.8 έπεται ότι ord$(([2]_5, [2]_5)) \mid 20$ και ord$(([2]_5, [2]_5)) \nmid 10$. Κατά συνέπειαν,

$$\left.\begin{array}{r} \text{ord}(([2]_5, [2]_5)) \in \{4, 20\} \\ ([2]_5, [2]_5)^4 = ([3]_5, [1]_5) \neq e_G \end{array}\right\} \Longrightarrow \text{ord}(([2]_5, [2]_5)) = 20 \underset{3.4.7}{\Longrightarrow} G = \langle([2]_5, [2]_5)\rangle,$$

οπότε $G \underset{3.5.26\,(\text{ii})}{\cong} \mathbb{Z}_{20}$. □

ΘΕΜΑ 3ο (i) Έστω $\mathbf{D}_6 = \langle \alpha, \beta \rangle \sqsubset \mathfrak{S}_{\mathcal{E}_6}$ η διεδρική ομάδα τάξεως 12 (όπου $\mathcal{E}_6 := \left\langle \exp(\frac{\pi i}{3}) \right\rangle \sqsubset \mathbb{S}^1$, $\mathcal{E}_6 \ni z \overset{\alpha}{\longmapsto} \overline{z} \in \mathcal{E}_6$ ο κατοπτρισμός ως προς τον άξονα των πραγματικών αριθμών και $\mathcal{E}_6 \ni z \overset{\beta}{\longmapsto} \exp(\frac{\pi i}{3}) z \in \mathcal{E}_6$ η στροφή κατά $\frac{\pi}{3}$ περί το $0 \in \mathbb{C}$). Προφανώς,

$$\mathbf{D}_6 = \left\{ \alpha^k \circ \beta^j \,|k \in \{0, 1\} \ , \ j \in \{0, 1, ..., 5\} \right\}$$

με καταλόγους τάξεων των στοιχείων της τον

$\text{id}_{\mathcal{E}_6}$	β	β^2	β^3	β^4	β^5
1	6	3	2	3	6

(τον προκύπτοντα από το πόρισμα 3.4.11) και τον

α	$\alpha \circ \beta$	$\alpha \circ \beta^2$	$\alpha \circ \beta^3$	$\alpha \circ \beta^4$	$\alpha \circ \beta^5$
2	2	2	2	2	2

καθόσον

$$\left(\alpha \circ \beta^j\right)^2 = \left(\alpha \circ \beta^{j-1}\right) \circ (\beta \circ \alpha) \circ \beta^j$$

$$= \left(\alpha \circ \beta^{j-1}\right) \circ (\alpha \circ \beta^{-1}) \circ \beta^j = \left(\alpha \circ \beta^{j-1}\right)^2 = \cdots = \alpha^2 = \text{id}_{\mathcal{E}_6}.$$

Έστω H *τυχούσα* υποομάδα τής $\mathbf{D}_6$. *Περίπτωση πρώτη.* Εάν $H \sqsubseteq \langle \beta \rangle$, τότε υπάρχει $d \in \mathfrak{D}_6$, όπου $\mathfrak{D}_6 = \{1, 2, 3, 6\}$ το σύνολο των θετικών ακεραίων διαιρετών τού 6, ούτως ώστε $H = H_d$, όπου[1] $H_d := \left\langle \beta^d \right\rangle \cong \mathbb{Z}_{\frac{6}{d}}$.

Περίπτωση δεύτερη. Εάν $H \not\sqsubseteq \langle \beta \rangle$, τότε υπάρχει κάποιο $h \in H \smallsetminus \langle \beta \rangle$. Προφανώς, $\langle \beta \rangle \coprod h \langle \beta \rangle \subseteq H \langle \beta \rangle$ και

$$\text{card}(\langle \beta \rangle \coprod h \langle \beta \rangle) \underset{5.1.12}{=} |\langle \beta \rangle| + |\langle \beta \rangle| = 6 + 6 = 12$$

$$\Longrightarrow \mathbf{D}_6 = \langle \beta \rangle \coprod h \langle \beta \rangle = H \langle \beta \rangle .$$

[1] Να ληφθεί υπ' όψιν το πόρισμα 3.4.23, το (ii) τού πορίσματος 3.5.29, καθώς και η αμφίρριψη $\mathfrak{D}_6 \ni d \longmapsto \frac{6}{d} \in \mathfrak{D}_6$.

Από τον τύπο τού γινομένου (5.36) (βλ. θεώρημα 5.5.10) λαμβάνουμε

$$12 = |\mathbf{D}_6| = |H\langle\beta\rangle| = \frac{|H|\,|\langle\beta\rangle|}{|H\cap\langle\beta\rangle|} = \frac{6\,|H|}{|H\cap\langle\beta\rangle|} \Rightarrow |H\cap\langle\beta\rangle| = \tfrac{1}{2}\,|H|\,.$$

Επίσης, για κάθε $h \in H\smallsetminus\langle\beta\rangle$ έχουμε

$$(H\cap\langle\beta\rangle)\coprod h\,(H\cap\langle\beta\rangle) \subseteq H\,(H\cap\langle\beta\rangle) \subseteq H,$$

οπότε

$$\mathrm{card}((H\cap\langle\beta\rangle)\coprod h\,(H\cap\langle\beta\rangle)) \underset{5.1.12}{=} 2\,|H\cap\langle\beta\rangle| = |H|\,,$$

πράγμα που σημαίνει ότι

$$H = (H\cap\langle\beta\rangle)\coprod h\,(H\cap\langle\beta\rangle)\,,$$

με $H\cap\langle\beta\rangle \sqsubseteq \langle\beta\rangle \Rightarrow H\cap\langle\beta\rangle = \langle\beta^d\rangle$ για κάποιον[2] $d\in\mathfrak{D}_6$. Επειδή $h\in H\smallsetminus\langle\beta\rangle$, το h δεν μπορεί να είναι μια ακεραία δύναμη τού β, οπότε

$$\exists\iota\in\mathbb{Z} : h = \beta^\iota\circ\alpha.$$

Προφανώς, $\{\beta^{d\nu}\,|0\le\nu\le\frac{6}{d}-1\}\coprod\{\beta^{d\nu+\iota}\circ\alpha\,|0\le\nu\le\frac{6}{d}-1\}\subseteq H$. Και επειδή το πλήθος αυτών των στοιχείων ισούται με $\frac{12}{d}$, έχουμε κατ' ανάγκην

$$H = \left\langle \beta^d, \beta^\iota\circ\alpha\right\rangle.$$

Κατά το θεώρημα 2.1.6, $\exists!\ (q,j)\in\mathbb{Z}\times\mathbb{Z} : \iota = qd+j$, όπου $j\in\{0,...,d-1\}$. Επομένως,

$$H = \langle\beta^d,\beta^\iota\circ\alpha\rangle = \langle\beta^d,\beta^{qd+j}\circ\alpha\rangle = \langle\beta^d,\beta^j\circ\alpha\rangle$$
$$= \left\langle \beta^d, \underbrace{\beta^j\circ\alpha\circ\beta^d}_{=\alpha\circ\beta^{d-j}}\right\rangle = \langle\alpha\circ\beta^{d-j},\beta^d\rangle =: H_{d,j}.$$

Συμπέρασμα: Η $\mathbf{D}_6$ *διαθέτει* ***15*** *υποομάδες*. Συγκεκριμένα[3],

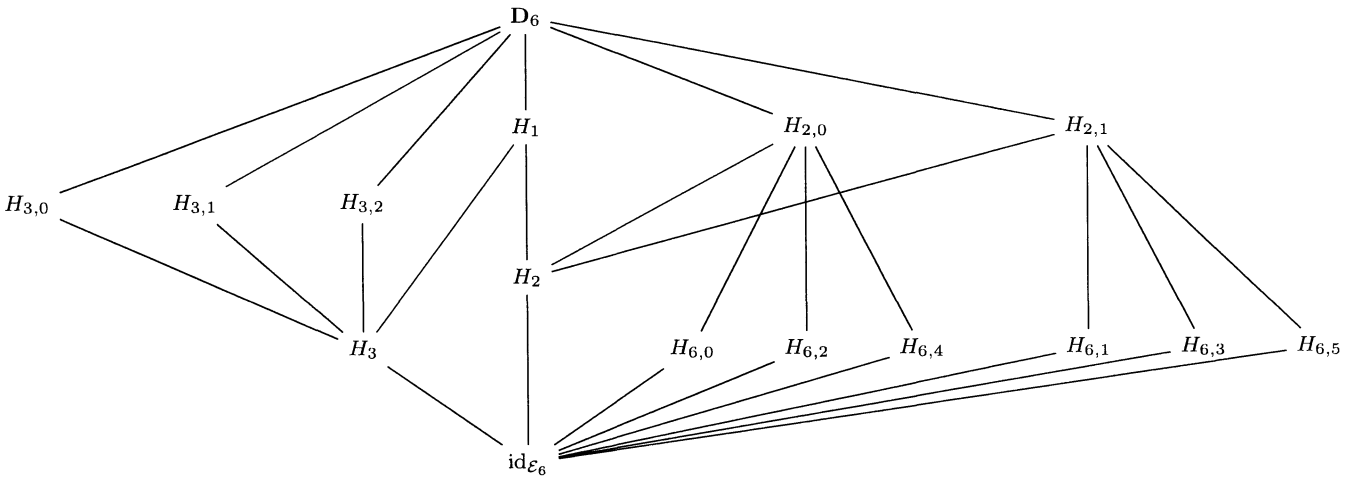
$$\boxed{\mathbf{Subg}(\mathbf{D}_6) = \{H_d|\,d\in\mathfrak{D}_6\}\coprod\{H_{d,j}|\,d\in\mathfrak{D}_6, j\in\{0,...,d-1\}\}\,.}$$

Είναι, μάλιστα, άμεσος ο έλεγχος τού ότι

(α) $H_d \sqsubset H_{d'} \Leftrightarrow [d' \mid d \text{ και } d\neq d']$, για οιουσδήποτε $d,d'\in\mathfrak{D}_6$,

(β) $H_d\sqsubset H_{d,j}$ για κάθε $j\in\{0,...,d-1\}$.

Μέσω αυτών (και παρατηρώντας το ποιοι είναι οι γεννήτορες μιας εκάστης των υποομάδων τής $\mathbf{D}_6$) είμαστε σε θέση να σχεδιάσουμε το διάγραμμα τού Hasse για τον σύνδεσμο $(\mathbf{Subg}(\mathbf{D}_6),\sqsubseteq)$.



[2] Σημειωτέον ότι $|\langle\beta^d\rangle| = \frac{6}{d}, |H| = \frac{12}{d}$, όπου $\langle\beta^d\rangle = \{\beta^{d\nu}\,|0\le\nu\le\frac{6}{d}-1\}$.

[3] Ειδικές υποομάδες: $H_6 = \{\mathrm{id}_{\mathrm{id}_{\mathcal{E}_6}}\}$, $H_{1,0} = \mathbf{D}_6$.

ΘΕΜΑ 4ο (i) Επειδή $\mathfrak{m}_1 \neq \mathfrak{m}_2$, έχουμε $\mathfrak{m}_1 \subsetneqq \mathfrak{m}_1 + \mathfrak{m}_2 \subseteq R \Rightarrow \mathfrak{m}_1 + \mathfrak{m}_2 = R$.

(ii) Τούτο έπεται άμεσα από την πρόταση 7.4.7.

(iii) Θέτοντας $I' := (\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{n-1}) + \mathfrak{m}_n$ λαμβάνουμε

$$\mathfrak{m}_n \subseteq I' \subseteq R \Rightarrow [\text{είτε } I' = \mathfrak{m}_n \text{ είτ } I' = R].$$

Το πρώτο ενδεχόμενο αποκλείεται, διότι εν τοιαύτη περιπτώσει θα είχαμε

$$\mathfrak{m}_n \subseteq \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{n-1} \subseteq \mathfrak{m}_1 \Rightarrow \mathfrak{m}_1 = \mathfrak{m}_n.$$

(iv) Θα χρησιμοποιήσουμε μαθηματική επαγωγή ως προς τον n. Για $n = 2$ τούτο είναι αληθές λόγω τού (ii). Εάν υποθέσουμε ότι

$$\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{n-1} = \mathfrak{m}_1 \cdots \mathfrak{m}_{n-1}$$

για κάποιον $n \geq 3$ και θέσουμε $I := \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{n-1}$, τότε $I + \mathfrak{m}_n = R$ (λόγω τού (iii)). Εφαρμόζοντας την πρόταση 7.4.7 λαμβάνουμε

$$\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{n-1} \cap \mathfrak{m}_n = I \cap \mathfrak{m}_n = I\mathfrak{m}_n = \mathfrak{m}_1 \cdots \mathfrak{m}_{n-1}\mathfrak{m}_n.$$

Από εδώ και στο εξής θα υποθέσουμε ότι ο R είναι μια *απειροπληθής ακεραία περιοχή* έχουσα *πεπερασμένου πλήθους* αντιστρέψιμα στοιχεία.

(v) Έστω ότι υπάρχει κάποιο στοιχείο $a \in J \setminus \{0_R\}$. Τότε $a^k = 0_R$ για κάποιον $k \in \mathbb{N}$. Εάν $k_0 := \min\{k \in \mathbb{N} : a^k = 0_R\}$, τότε $a^{k_0-1} \neq 0_R$ και $a \neq 0_R$ αλλά $a^{k_0-1}a = a^{k_0} = 0_R$. Άτοπο! Άρα $J = \{0_R\}$.

(vi) Θα εργασθούμε με «εις άτοπον απαγωγή». Υποθέτουμε ότι η ακεραία περιοχή R διαθέτει μόνον *πεπερασμένου πλήθους* μεγιστικά ιδεώδη, ας πούμε τα $\mathfrak{m}_1, ..., \mathfrak{m}_n$. Κατ' αρχάς, $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \neq \{0_R\}$, διότι (εξ υποθέσεως[4]) $\mathfrak{m}_j \neq \{0_R\}$ για κάθε $j \in \{1, ..., n\}$, οπότε επιλέγοντας $a_j \in \mathfrak{m}_j \setminus \{0_R\}$ για κάθε $j \in \{1, ..., n\}$, το γινόμενο $a := \prod_{j=1}^{n} a_j$ είναι ένα μη μηδενικό στοιχείο ανήκον στην τομή $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$.

Ισχυρισμός: $1_R - a \in R^\times, \forall a \in \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$.

Επαλήθευση ισχυρισμού : Εάν υπήρχε κάποιο $a \in \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$ με $1_R - a \notin R^\times$, τότε

$$1_R \notin \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \Rightarrow \{0_R\} \subsetneqq \langle 1_R - a\rangle \subsetneqq R.$$

Σύμφωνα με το θεώρημα 7.5.13,

$$\left.\begin{array}{r} \exists j_0 \in \{1, ..., n\} : \langle 1_R - a\rangle \subseteq \mathfrak{m}_{j_0} \\ [a \in \mathfrak{m}_{j_0} \text{ και } 1_R - a \in \mathfrak{m}_{j_0}] \Rightarrow 1_R \in \mathfrak{m}_{j_0} \end{array}\right\} \Rightarrow \mathfrak{m}_{j_0} = R.$$

Άτοπο! Άρα ο ανωτέρω ισχυρισμός είναι όντως αληθής.

Εν συνεχεία, θεωρούμε τυχόν $a \in \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \setminus \{0_R\}$. Παρατηρούμε ότι για οιονδήποτε $\nu \in \mathbb{N}$, $a^\nu \in \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$ και (επειδή, λόγω τού (v), $J = \{0_R\}$) $a^\nu \neq 0_R$. Τούτο σημαίνει ότι όχι μόνον το $1_R - a$ αλλά και, γενικότερα, το $1_R - a^\nu$ είναι αντιστρέψιμο. Επιπροσθέτως, για οιουσδήποτε $\nu_1, \nu_2 \in \mathbb{N}$ με $\nu_1 \neq \nu_2$ έχουμε $a^{\nu_1} \neq a^{\nu_2}$, διότι

$$\left.\begin{array}{r} a^{\max\{\nu_1,\nu_2\}} - a^{\min\{\nu_1,\nu_2\}} \\ = a^{\min\{\nu_1,\nu_2\}}(1_R - a^{\max\{\nu_1,\nu_2\}-\min\{\nu_1,\nu_2\}}), \\ a^{\min\{\nu_1,\nu_2\}} \neq 0_R \\ 1_R - a^{\max\{\nu_1,\nu_2\}-\min\{\nu_1,\nu_2\}} \in R^\times \\ R^\times \subseteq R \setminus \{0_R\} \end{array}\right\} \Rightarrow a^{\max\{\nu_1,\nu_2\}} \neq a^{\min\{\nu_1,\nu_2\}}.$$

[4]Εάν υπήρχε κάποιο $i_0 \in \{1, ..., n\}$ με $\mathfrak{m}_{i_0} = \{0_R\}$, τότε, επειδή $\mathfrak{m}_{i_0} \neq \mathfrak{m}_j$ για κάθε $j \in \{1, ..., n\} \setminus \{i_0\}$, το $\mathfrak{m}_{i_0}$ δεν θα ήταν μεγιστικό ιδεώδες.

Επειδή λοιπόν η ομάδα $R^\times$ των αντιστεψίμων στοιχείων εμπεριέχει το απειροσύνολο $\{\,1_R - a^\nu \,|\, \nu \in \mathbb{N}\}$, θα είναι αφ' εαυτής άπειρη. Άτοπο! Επομένως, η ακεραία περιοχή R διαθέτει *άπειρα* σαφώς διακεκριμένα μεγιστικά ιδεώδη.

(vii) Στην ειδική περίπτωση όπου $R = \mathbb{Z}$, από το (vi) έπεται ότι η ακεραία περιοχή $\mathbb{Z}$ (με $\mathbb{Z}^\times = \{\pm 1\}$) διαθέτει μια *άπειρα* σαφώς διακεκριμένα μεγιστικά ιδεώδη. Επειδή (σύμφωνα με την πρόταση 7.5.18) κάθε μεγιστικό ιδεώδες αυτής είναι ένα κύριο ιδεώδες παραγόμενο από έναν πρώτο αριθμό (και τανάπαλιν), οδηγούμεθα σε μια (επιπρόσθετη) απόδειξη για το ότι το σύνολο των πρώτων αριθμών είναι άπειρο. □

<u>ΘΕΜΑ 5ο</u> (i) Οι τύποι (10.30) τού Viete δίδουν

$$\begin{cases} a+b+c = -a, \\ ab+bc+ca = b, \\ abc = -c. \end{cases}$$

Από τον τρίτο τύπο λαμβάνουμε $c(ab+1) = 0$. Άρα είτε $c = 0$ είτε $ab = -1$.

Περίπτωση πρώτη. Εάν $c = 0$, τότε

$$\left.\begin{array}{c} a+b = -a \Rightarrow 2a+b = 0 \\ ab = b \end{array}\right\} \Rightarrow (a,b,c) \in \{(0,0,0),(1,-2,0)\}.$$

Περίπτωση δεύτερη. Εάν $ab = -1$, τότε $c = -2a - b$ και

$$-1 + b(-2a-b) + (-2a-b)a = b \Rightarrow -1 - 2ab - b^2 - 2a^2 - ab = b$$

$$-1 + 2 - b^2 - 2a^2 + 1 = b \Rightarrow 2a^2 - 2 + b^2 + b = 0$$

$$\Rightarrow 2a^4 - 2a^2 + (ab)^2 + (ab)a = 0 \Rightarrow 2a^4 - 2a^2 - a + 1 = 0.$$

Επειδή $a \in \mathbb{Q}$, $a = \frac{\lambda}{\mu}$, όπου $(\lambda,\mu) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ με μκδ$(\lambda,\mu) = 1$. Από την τελευταία ισότητα έχουμε κατ' ανάγκην $\lambda \mid 1$ και $\mu \mid 2$. (Πρβλ. άσκηση 8 τού φυλλαδίου 13.) Άρα $a \in \{\pm 1, \pm\frac{1}{2}\}$. Σημειωτέον ότι

$$2\cdot 1^4 - 2\cdot 1^2 - 1 + 1 = 0, \qquad 2\cdot(-1)^4 - 2\cdot(-1)^2 + 1 + 1 = 2,$$

$$2\cdot(\tfrac{1}{2})^4 - 2\cdot(\tfrac{1}{2})^2 - \tfrac{1}{2} + 1 = \tfrac{1}{8}, \quad 2\cdot(-\tfrac{1}{2})^4 - 2\cdot(-\tfrac{1}{2})^2 + \tfrac{1}{2} + 1 = \tfrac{9}{8}.$$

Αυτό σημαίνει ότι $a = 1 \Longrightarrow (a,b,c) = (1,-1,-1)$ και ότι τα

$$\mathsf{X}^3,\ \mathsf{X}^3 + \mathsf{X}^2 - 2\mathsf{X},\ \mathsf{X}^3 + \mathsf{X}^2 - \mathsf{X} - 1 \in \mathbb{Z}[\mathsf{X}]$$

είναι τα *ζητούμενα τριτοβάθμια μονικά πολυώνυμα*.

(ii) Έστω ρ ένας φυσικός αριθμός ≥ 2 και έστω

$$\xi := \lambda_1^{2021} + \lambda_2^{2021},\ \ \lambda_1 := \rho + \sqrt{\rho^2 - 1},\ \ \lambda_2 := \rho - \sqrt{\rho^2 - 1}.$$

Προφανώς, $\lambda_1 + \lambda_2 = 2\rho$ και $\lambda_1\lambda_2 = 1$, οπότε τα λ_1, λ_2 είναι οι θέσεις μηδενισμού τού τριωνύμου

$$\mathsf{X}^2 - 2\rho\mathsf{X} + 1.$$

Κατά συνέπειαν,

$$\lambda_1^2 = 2\rho\lambda_1 - 1,\ \ \lambda_2^2 = 2\rho\lambda_2 - 1.$$

Θέτοντας $t_\nu := \lambda_1^\nu + \lambda_2^\nu$, $\nu \in \mathbb{N}_0$, παρατηρούμε ότι $t_0 = 2,\ t_1 = 2\rho$,

$$t_2 = \lambda_1^2 + \lambda_2^2 = (2\rho\lambda_1 - 1) + (2\rho\lambda_2 - 1) = 2\rho t_1 - t_0 = 4\rho^2 - 2,$$

$$t_3 = \lambda_1^3 + \lambda_2^3 = \lambda_1(\lambda_1^2) + \lambda_2(\lambda_2^2) = \lambda_1(2\rho\lambda_1 - 1) + \lambda_2(2\rho\lambda_2 - 1)$$

$$= 2\rho(\lambda_1^2 + \lambda_2^2) - (\lambda_1 + \lambda_2) = 2\rho t_2 - t_1 = 2\rho(t_2 - 1) = 2\rho(4\rho^2 - 2).$$

Άρα τα t_0, t_1, t_2, t_3 είναι ακέραιοι αριθμοί και το 2ρ είναι διαιρέτης των t_1 και t_3. Ακόμη και για *τυχόντα* $\nu \geq 4$,

$$t_\nu = \lambda_1^\nu + \lambda_2^\nu = \lambda_1^{\nu-2}(\lambda_1^2) + \lambda_2^{\nu-2}(\lambda_2^2) = \lambda_1^{\nu-2}(2\rho\lambda_1 - 1) + \lambda_2^{\nu-2}(2\rho\lambda_2 - 1)$$
$$= 2\rho(\lambda_1^{\nu-1} + \lambda_2^{\nu-1}) - (\lambda_1^{\nu-2} + \lambda_2^{\nu-2}) = 2\rho t_{\nu-1} - t_{\nu-2}.$$

Εάν υποθέσουμε ότι $t_\kappa \in \mathbb{Z}$ για κάθε μη αρνητικό ακέραιο αριθμό κ που είναι $< \nu$, τότε (χρησιμοποιώντας τη δεύτερη μορφή μαθηματικής επαγωγής ως προς τον ν) διαπιστώνουμε ότι $t_\nu \in \mathbb{Z}$. Ιδιαιτέρως, $\xi = t_{2021} \in \mathbb{Z}$. Εν συνεχεία, ισχυριζόμαστε ότι το 2ρ είναι διαιρέτης τού t_ν *για κάθε περιττόν* $\nu \geq 5$. Πράγματι· εάν υποθέσουμε ότι για έναν τέτοιον ν το 2ρ είναι διαιρέτης τού t_κ για κάθε θετικό *περιττό* ακέραιο αριθμό κ που είναι $< \nu$, τότε (χρησιμοποιώντας εκ νέου τη δεύτερη μορφή μαθηματικής επαγωγής ως προς τον ν και τον ανωτέρω αναγωγικό τύπο) λαμβάνουμε

$$\left.\begin{array}{r} \nu - 2 \equiv 1 (\mathrm{mod}\, 2) \Rightarrow 2\rho \mid t_{\nu-2} \ \ (\text{επ. υπ.}) \\ 2\rho \mid 2\rho t_{\nu-1} \end{array}\right\} \Rightarrow 2\rho \mid 2\rho t_{\nu-1} - t_{\nu-2} = t_\nu.$$

Ιδιαιτέρως, $2\rho \mid \xi = t_{2021}$. □

<u>ΘΕΜΑ 6ο</u> (i) Ας υποθέσουμε ότι υπάρχει πολυώνυμο $\varphi(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]$, τέτοιο ώστε να ισχύει

$$\varphi(\mathsf{X})^3 - \varphi(\mathsf{X}) + 2 = \psi(\mathsf{X})\left(\mathsf{X}^4 - 7\right)$$

για κάποιο $\psi(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]$. Εάν

$$\varphi(\mathsf{X}) = \sum_{j=0}^{n} a_j \mathsf{X}^j,\ \psi(\mathsf{X}) = \sum_{k=0}^{m} b_k \mathsf{X}^k,$$

τότε

$$\left(\sum_{j=0}^{n} a_j \mathsf{X}^j\right)^3 - \left(\sum_{j=0}^{n} a_j \mathsf{X}^j\right) + 2 = \left(\sum_{k=0}^{m} b_k \mathsf{X}^k\right)\left(\mathsf{X}^4 - 7\right).$$

Εξισώνοντας τους συντελεστές των σταθερών όρων σε αμφότερα μέλη λαμβάνουμε

$$a_0^3 - a_0 + 2 = -7b_0 \Longrightarrow \left[a_0^3\right]_7 - [a_0]_7 + [2]_7 = [-7b_0]_7 = [0]_7.$$

Ωστόσο, εντός τού σώματος $\mathbb{Z}_7$ έχουμε

$[a_0]_7$	$[0]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$
$\left[a_0^3\right]_7 - [a_0]_7 + [2]_7$	$[2]_7$	$[2]_7$	$[1]_7$	$[5]_7$	$[6]_7$	$[3]_7$	$[2]_7$

Αυτό σημαίνει ότι εντός τού $\mathbb{Z}_7$ η εξίσωση

$$\left[a_0^3\right]_7 - [a_0]_7 + [2]_7 = [0]_7$$

δεν διαθέτει καμία λύση. Άτοπο! □

(ii) Για κάθε $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ $(a, b \in \mathbb{Z})$ ορίζουμε την επιρριπτική απεικόνιση

$$f : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}_7,\ \ f(a + b\sqrt{-5}) := [a + 4b]_7.$$

Για οιουσδήποτε $a, b, c, d \in \mathbb{Z}$ έχουμε

$$\begin{aligned} f((a + b\sqrt{-5}) + (c + d\sqrt{-5})) &= f((a + c) + (b + d)\sqrt{-5}) = [(a + c) + 4(b + d)]_7 \\ &= [a + 4b]_7 + [c + 4d]_7 \\ &= f(a + b\sqrt{-5}) + f(c + d\sqrt{-5}) \end{aligned}$$

και

$$\begin{aligned} f((a+b\sqrt{-5})(c+d\sqrt{-5})) &= f((ac-5bd)+(ad+bc)\sqrt{-5}) \\ &= [(ac-5bd)+4(ad+bc)]_7 \\ &= [ac-5bd]_7+[4(ad+bc)]_7 \\ &= [ac]_7+([-5]_7\cdot[bd]_7)+[4(ad+bc)]_7 \\ &= [ac]_7+([16]_7\cdot[bd]_7)+[4(ad+bc)]_7 \\ &= [ac+16bd]_7+[4(ad+bc)]_7 \\ &= [(ac+16bd)+4(ad+bc)]_7 \\ &= [(a+4b)(c+4d)]_7 \\ &= [a+4b]_7\,[c+4d]_7 \\ &= f(a+b\sqrt{-5})f(c+d\sqrt{-5}), \end{aligned}$$

οπότε η f είναι ένας επιμορφισμός δακτυλίων. Σύμφωνα με το 1ο θεώρημα ισομορφισμών δακτυλίων 8.3.3,

$$\mathbb{Z}[\sqrt{-5}]/\mathrm{Ker}(f)\cong\mathbb{Z}_7.$$

Επειδή $f(7)=[7+4\cdot 0]_7=[7]_7=[0]_7$ και $f(4-\sqrt{-5})=[4+4\cdot(-1)]_7=[0]_7$, έχουμε

$$7\in\mathrm{Ker}(f),\ 4-\sqrt{-5}\in\mathrm{Ker}(f)\Rightarrow\left\langle 7,4-\sqrt{-5}\right\rangle\subseteq\mathrm{Ker}(f).$$

Και αντιστρόφως· για τυχόν $a+b\sqrt{-5}\in\mathrm{Ker}(f)$ $(a,b\in\mathbb{Z})$ έχουμε $7\mid a+4b$, οπότε

$$a+b\sqrt{-5}=7\left(\frac{a+4b}{7}\right)-\left(4-\sqrt{-5}\right)b,$$

απ' όπου έπεται και ο αντίστροφος εγκλεισμός $\mathrm{Ker}(f)\subseteq\left\langle 7,4-\sqrt{-5}\right\rangle$. □