Πανεπιστήμιο Κρήτης, Τμήμα Μαθηματικών **Άλγεβρα (Μ 110)**

Εαρινό Εξάμηνο 2009, Εξέταση Σεπτεμβρίου **Εξεταστής: Δημήτριος Νταής**

ΑΠΑΝΤΗΣΕΙΣ ΔΟΘΕΝΤΩΝ ΘΕΜΑΤΩΝ

ΘΕΜΑ 1ο (i) Έστω $k := \min\{ m \in \mathbb{N} \mid m \geq 2 \text{ και } m \mid n\}$. Εάν ο k ήταν σύνθετος αριθμός, τότε θα υπήρχαν $k_1, k_2 \in \mathbb{N}$, τέτοιοι ώστε να ισχύει $2 \leq k_1 \leq k_2 < k$ και $k = k_1 k_2$, πράγμα άτοπο (αφού $k_1 \mid k$ και $k_2 \mid k$), διότι ο k είναι εξ υποθέσεως ο *ελάχιστος* φυσικός ≥ 2 με αυτήν την ιδιότητα. Άρα ο k οφείλει να είναι πρώτος αριθμός.

(ii) Ας υποθέσουμε ότι το σύνολο των πρώτων αριθμών είναι πεπερασμένο, ας πούμε το $\{p_1, p_2, \ldots, p_k\}$, κι ας θεωρήσουμε τον φυσικό αριθμό

$$m := p_1 p_2 \cdots p_k + 1.$$

Τότε είναι πρόδηλο ότι $p_1 \nmid m,\ p_2 \nmid m, \ldots,\ p_n \nmid m$ (διότι εάν υπήρχε κάποιος $j \in \{1, ..., n\}$ με $p_j \mid m$, θα είχαμε $p_j \mid p_1 p_2 \cdots p_k$, οπότε $p_j \mid m - p_1 p_2 \cdots p_k$, ήτοι $p_j \mid 1$, κάτι που θα αντέφασκε προς την ανισότητα $p_j \geq 2$). Τούτο όμως είναι άτοπο επί τη βάσει τού (i). □

ΘΕΜΑ 2ο **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* επιρριπτική, 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 επιρριπτική 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 κατασκευάζεται ένας ισομορφισμός μεταξύ τής G και τής υποομάδας G' τής ομάδας $\mathfrak{S}_G$. □

ΘΕΜΑ 3ο (i) Τούτο έπεται από τις εξής αμφίπλευρες συνεπαγωγές:

$$\begin{aligned}
&g \in A(B \cup C) = \{ xy \mid x \in A \text{ και } y \in B \cup C\} \\
&\Leftrightarrow g \in \{ xy \mid x \in A \text{ και } y \in B \text{ ή } y \in C\} \\
&\Leftrightarrow g \in \{ xy \mid x \in A \text{ και } y \in B\} \text{ ή } g \in \{ xy \mid x \in A \text{ και } y \in C\} \\
&\Leftrightarrow g \in \{ xy \mid x \in A \text{ και } y \in B\} \cup \{ xy \mid x \in A \text{ και } y \in C\} \\
&\Leftrightarrow g \in AB \cup AC.
\end{aligned}$$

(ii) Έστω A ένα σύστημα αριστερών εκπροσώπων *τής* H *εντός τής* G και έστω A' ένα σύστημα αριστερών εκπροσώπων *τής* K *εντός τής* H. Τότε

$$\mathrm{card}(\mathrm{A}) = |G : H| \quad \text{και} \quad \mathrm{card}(\mathrm{A}') = |H : K| \,. \tag{1}$$

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

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

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

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

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

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

όπου η πρώτη είναι προφανής, η δεύτερη απόρροια των όσων έχουμε ήδη προαναφέρει και η τρίτη έπεται από τον νόμο τής διαγραφής (βλ. 3.2.9 (i)). Από το γεγονός τού ότι τελικώς ισχύει

$$g_1h_1 = g_2h_2 \Rightarrow [g_1 = g_2 \quad \text{και} \quad h_1 = h_2]$$

συμπεραίνουμε ότι

$$|G : K| = \mathrm{card}(\mathrm{AA}') = \mathrm{card}(\mathrm{A} \times \mathrm{A}') = \mathrm{card}(\mathrm{A}) \cdot \mathrm{card}(\mathrm{A}'). \tag{2}$$

Ο συνδυασμός των (1) και (2) δίδει την $|G : K| = |G : H|\ |H : K|$. □

ΘΕΜΑ 4ο Έστω ότι ο R είναι ένας δακτύλιος και τα I, J δύο ιδεώδη του. Ορίζουμε την απεικόνιση

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

Η f αποτελεί ομομορφισμό δακτυλίων, καθότι για οιαδήποτε $a, b \in I + J$ έχουμε

$$\begin{aligned} f(a + b) &= ((a + b) + I, (a + b) + J) = ((a + I) + (b + I)\,, (a + J) + (b + J))\,, \\ f(ab) &= (ab + I, ab + J) = ((a + I)\,(b + I)\,, (a + J)\,(b + J))\,. \end{aligned}$$

Ο πυρήνας της ισούται προφανώς με

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

Εν συνεχεία θα δείξουμε ότι η f είναι επιριπτική. Έστω τυχόν στοιχείο

$$(a + I, b + J) \in ((I + J)/I) \times ((I + J)/J)\,.$$

Τότε τα a, b γράφονται ως αθροίσματα

$$a = u + v,\ \ b = w + z,$$

για κατάλληλα $u, w \in I$ και $v, z \in J$. Κατά συνέπειαν,

$$\begin{aligned} f(v) &= (v+I, v+J) = (v+I, 0_{I+J}+J), \\ f(w) &= (w+I, w+J) = (0_{I+J}+I, w+J), \end{aligned}$$

απ' όπου συμπεραίνουμε ότι

$$f(v+w) = f(v)+f(w) = (v+I, w+J) = (u+v+I, w+z+J) = (a+I, b+J),$$

δηλαδή ότι η f είναι επιμορφισμός δακτυλίων με $\mathrm{Ker}(f) = I \cap J$. Αρκεί η εφαρμογή τού 1ου θεωρήματος ισομορφισμών δακτυλίων (βλ. 4.6.6). □

ΘΕΜΑ 5ο (i) **Αλγόριθμος διαιρέσεως**. Δοθέντων δυο πολυωνύμων

$$f(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}]\,, \;\; g(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j \in R[\mathsf{X}]$$

με τους συντελεστές τους ειλημμένους από μια ακεραία περιοχή R, όπου $\mathrm{LC}(g) = b_m \in R^\times$, υπάρχει ένα ζεύγος *μονοσημάντως ορισμένων* πολυωνύμων $q(\mathsf{X})$ και $r(\mathsf{X}) \in R[\mathsf{X}]$, τέτοιων ώστε να ισχύει

$$f(\mathsf{X}) = q(\mathsf{X}) \cdot g\,(\mathsf{X}) + r(\mathsf{X}), \quad \deg\left(r(\mathsf{X})\right) < \deg\left(g\,(\mathsf{X})\right).$$

(ii) Σύμφωνα με τον αλγόριθμο τής διαιρέσεως (i) υπάρχουν πολυώνυμα $q(\mathsf{X})$ και $r(\mathsf{X}) \in R[\mathsf{X}]$, τέτοια ώστε να ισχύει

$$f(\mathsf{X}) = (\mathsf{X}-a)q(\mathsf{X}) + r(\mathsf{X}), \;\; \deg(r(\mathsf{X})) < \deg(\mathsf{X}-a) = 1.$$

Επομένως, $r(\mathsf{X}) = c \in R$, οπότε

$$c = f(\mathsf{X}) - (\mathsf{X}-a)q(\mathsf{X}) \Longrightarrow c = f(a).$$

(iii) Το a είναι μια θέση μηδενισμού τού $f\,(\mathsf{X})$ (εντός τού R) εάν και μόνον εάν το υπόλοιπο τής διαιρέσεως τού $f(\mathsf{X})$ διά τού $\mathsf{X}-a$ είναι 0, πράγμα που σημαίνει ότι $\mathsf{X}-a \mid f(\mathsf{X})$.

(iv) Όταν $k = 1$, αυτό είναι αληθές λόγω τού (iii). Θα εργασθούμε με τη βοήθεια τής μαθηματικής επαγωγής. Υποθέτουμε ότι ο ισχυρισμός είναι αληθής για $k-1$ θέσεις μηδενισμού, οπότε

$$f(\mathsf{X}) = (\mathsf{X}-a_1)\,(\mathsf{X}-a_2)\cdots(\mathsf{X}-a_{k-1})\,g(\mathsf{X})$$

για κάποιο $g(\mathsf{X}) \in R[\mathsf{X}]$. Κατόπιν αποτιμήσεως των δύο μελών τής ανωτέρω ισότητας για $\mathsf{X} = a_k$ λαμβάνουμε

$$0 = f(a_k) = (a_k-a_1)\,(a_k-a_2)\cdots(a_k-a_{k-1})\,g(a_k),$$

απ' όπου προκύπτει ότι $g(a_k) = 0$ (λόγω τής αρχικής υποθέσεώς μας). Άρα το πολυώνυμο $g(\mathsf{X})$ διαιρείται διά τού $\mathsf{X}-a_k$, οπότε ο ισχυρισμός είναι εμφανώς αληθής και για k θέσεις μηδενισμού. □

ΘΕΜΑ 6ο (i) Δίχως βλάβη τής γενικότητας υποθέτουμε ότι $m < n$. Έστω p ένας πρώτος αριθμός που διαιρεί τον $a^{2^m} + 2^{2^m}$. Προφανώς,

$$a^{2^m} \equiv -2^{2^m} (\mathrm{mod}\, p) \underset{\text{2.4.5 (iii)}}{\Longrightarrow} \left(a^{2^m}\right)^{2^{n-m}} \equiv \left(-2^{2^m}\right)^{2^{n-m}} (\mathrm{mod}\, p) \Rightarrow a^{2^n} \equiv 2^{2^n} (\mathrm{mod}\, p).$$

Επειδή ο a είναι εξ υποθέσεως περιττός, έχουμε κατ' ανάγκην $p \neq 2$. Κατά συνέπειαν,

$$2^{2^n} + 2^{2^n} = 2^{2^n+1} \not\equiv 0 (\mathrm{mod}\, p) \Rightarrow a^{2^n} \equiv 2^{2^n} \not\equiv -2^{2^n} (\mathrm{mod}\, p) \Rightarrow p \nmid a^{2^n} + 2^{2^n}.$$

Άρα κανείς πρώτος αριθμός που διαιρεί τον $a^{2^m} + 2^{2^m}$ δεν διαιρεί τον $a^{2^n} + 2^{2^n}$. Τούτο σημαίνει (κατά το λήμμα 2.3.10) ότι

$$\mathrm{μκδ}(a^{2^m} + 2^{2^m}, a^{2^n} + 2^{2^n}) = 1.$$

(ii) Εάν ο p είναι ένας πρώτος αριθμός τής μορφής $3k+2$ (όπου k κάποιος μη αρνητικός ακέραιος) και $p \mid a^2+ab+b^2$, για κάποιους $a, b \in \mathbb{Z}\setminus\{0\}$, θα αποδείξουμε ότι ο p οφείλει να διαιρεί αμφότερους τους a και b. Ας υποθέσουμε ότι $p \nmid a$. Τότε

$$p \mid a^2+ab+b^2 \Rightarrow p \mid a^3-b^3 \quad (\text{διότι } a^3-b^3=(a-b)(a^2+ab+b^2)),$$

οπότε

$$a^3 \equiv b^3 (\mathrm{mod}\, p) \underset{\text{2.4.5 (iii)}}{\Longrightarrow} a^{3k} \equiv b^{3k} (\mathrm{mod}\, p) \Rightarrow p \nmid b \quad (\text{διότι αλλιώς } p \mid a^{3k} \underset{\text{2.2.10}}{\Longrightarrow} p \mid a).$$

Επιπροσθέτως,

$$a^{3k} \equiv b^{3k} (\mathrm{mod}\, p) \underset{\text{2.4.5 (ii)}}{\Longrightarrow} ba^{3k} \equiv b^{3k+1} (\mathrm{mod}\, p).$$

Από την άλλη μεριά, εφαρμόζοντας το μικρό θεώρημα 2.4.14 τού Fermat για τους a και b λαμβάνουμε

$$a^{p-1} \equiv b^{p-1} \equiv 1 (\mathrm{mod}\, p) \Rightarrow a^{3k+1} \equiv b^{3k+1} (\mathrm{mod}\, p),$$

οπότε

$$\left.\begin{array}{r} ba^{3k} \equiv b^{3k+1} \equiv a^{3k+1} (\mathrm{mod}\, p) \Rightarrow b \cdot a^{3k} \equiv a \cdot a^{3k} (\mathrm{mod}\, p) \\ p \nmid a \Rightarrow p \nmid a^{3k} \end{array}\right\} \underset{\text{2.4.7}}{\Longrightarrow} b \equiv a (\mathrm{mod}\, p) \Rightarrow a \equiv b (\mathrm{mod}\, p).$$

Αυτό σημαίνει ότι

$$\left.\begin{array}{r} a^2+ab+b^2 \equiv 0 (\mathrm{mod}\, p) \Rightarrow 3a^2 \equiv 0 (\mathrm{mod}\, p) \Rightarrow p \mid 3a^2 \\ p \neq 3 \end{array}\right\} \underset{\text{2.2.10}}{\Longrightarrow} p \mid a^2 \underset{\text{2.2.10}}{\Longrightarrow} p \mid a.$$

Άτοπο! Παρομοίως θα καταλήγαμε σε άτοπο εάν (αρχικώς) υποθέταμε ότι $p \nmid b$ (λόγω συμμετρίας). Άρα ο ο p οφείλει να διαιρεί αμφότερους τους a και b. □

<u>ΘΕΜΑ 7ο</u> Επί τού καρτεσιανού γινομένου $G := \mathbb{Z} \times \mathbb{Z}$ ορίζεται η εσωτερική πράξη

$$\boxed{(a,b) \star (c,d) := (a+(-1)^b c, b+d),}$$

όπου "+" η συνήθης πράξη τής προσθέσεως επί τού $\mathbb{Z}$.

(i) Το ζεύγος $(G, \star)$ αποτελεί μια μη αβελιανή ομάδα. Πράγματι· για οιαδήποτε $(a,b),(c,d),(e,f) \in G$ έχουμε

$$\begin{aligned} ((a,b) \star (c,d)) \star (e,f) &= \Big(a+(-1)^b c, b+d\Big) \star (e,f) \\ &= (\Big(a+(-1)^b c\Big) + (-1)^{b+d} e, (b+d)+f) \end{aligned}$$

και

$$\begin{aligned} (a,b) \star ((c,d) \star (e,f)) &= (a,b) \star \Big(c+(-1)^d e, d+f\Big) \\ &= (a+(-1)^b \Big(c+(-1)^d e\Big), b+(d+f)) \\ &= (\Big(a+(-1)^b c\Big) + (-1)^{b+d} e, b+(d+f)), \end{aligned}$$

οπότε (λόγω τής ισότητας $(b+d)+f = b+(d+f)$)

$$((a,b) \star (c,d)) \star (e,f) = (a,b) \star ((c,d) \star (e,f)),$$

πράγμα που σημαίνει ότι η πράξη "$\star$" είναι προσεταιριστική. Επιπροσθέτως, για οιοδήποτε $(a,b) \in G$ ισχύει

$$\begin{aligned}(a,b)\star(0,0) &= \Big(a+(-1)^b\cdot 0, b+0\Big) = (a,b)\\ &= \big(0+(-1)^0\, a, 0+b\big) = (0,0)\star(a,b),\end{aligned}$$

οπότε το $(0,0)$ είναι το (κατ' ανάγκην μονοσημάντως ορισμένο) ουδέτερο στοιχείο ως προς την πράξη "$\star$". Από την άλλη μεριά, για οιοδήποτε $(a,b) \in G$ ισχύει

$$\begin{aligned}(a,b)\star\left((-1)^{b+1}\, a, -b\right) &= \Big(a+(-1)^b\left((-1)^{b+1}\, a\right), b+(-b)\Big) = (a+(-a), b+(-b))\\ &= (0,0) = \left((-1)^{b+1}\, a+(-1)^{-b}\, a, (-b)+b\right) = \left((-1)^{b+1}\, a, -b\right)\star(a,b),\end{aligned}$$

οπότε το $\left((-1)^{b+1}\, a, -b\right)$ είναι το (κατ' ανάγκην μονοσημάντως ορισμένο) «αντίστροφο» (= συμμετρικό) στοιχείο $(a,b)^{-1}$ τού (a,b) ως προς την πράξη "$\star$". Ως εκ τούτου, το ζεύγος $(G,\star)$ αποτελεί μια ομάδα, η οποία είναι μη αβελιανή, διότι π.χ.

$$(0,1)\star(1,0) = (-1,1) \neq (1,1) = (1,0)\star(0,1)\,.$$

(ii) Τα $H := \{\,(a,b) \in G \mid\ b=0\}$ και $K := \{\,(a,b) \in G \mid\ a=0\}$ αποτελούν υποομάδες τής $(G,\star)$, διότι $(0,0) \in H \cap K$ και για οιαδήποτε στοιχεία $(a,0),(a',0) \in H$ (και, αντιστοίχως, για οιαδήποτε στοιχεία $(0,b),(0,b') \in K$) έχουμε $(a,0)\star(a',0)^{-1} = (a,0)\star(-a',0) = (a+(-a'),0) \in H$ (και, αντιστοίχως, $(0,b)\star(0,b')^{-1} = (0,b)\star(0,-b') = (0,b+(-b')) \in K$). [Εν προκειμένω, χρησιμοποιήθηκε το κριτήριο (iii) τής προτάσεως 3.2.15.]

(iii) Θεωρούμε την απεικόνιση

$$\vartheta : G \longrightarrow G,\ \ (a,b) \longmapsto \vartheta(a,b) := (0,b).$$

Αυτή είναι *ενδομορφισμός τής ομάδας* $(G,\star)$, καθόσον για οιαδήποτε $(a,b),(a',b') \in G$ έχουμε

$$\begin{aligned}\vartheta\left((a,b)\star(a',b')\right) &= \vartheta\left(a+(-1)^b\, a', b+b'\right) = (0,b+b')\\ &= (0,b)\star(0,b') = \vartheta(a,b)\star\vartheta(a',b').\end{aligned}$$

Ως πυρήνα της έχει την υποομάδα

$$\begin{aligned}\mathrm{Ker}(\vartheta) &= \{\,(a,b)\in G \mid \vartheta(a,b)=(0,0)\} = \{\,(a,b)\in G \mid (0,b)=(0,0)\}\\ &= \{\,(a,b)\in G \mid\ b=0\} = H.\end{aligned}$$

Άρα $H \lhd G$ (κατά το πόρισμα 3.6.12). Από την άλλη μεριά, $K \not\lhd G$, διότι π.χ. $(0,1) \in K$, αλλά

$$\begin{aligned}(1,0)\star(0,1)\star(1,0)^{-1} &= (1,0)\star(0,1)\star(-1,0)\\ &= (1,1)\star(-1,0) = (1+(-1)^1(-1),1) = (2,1) \notin K.\end{aligned}$$

(iv) Για τον ενδομορφισμό ϑ τής $(G,\star)$ τον ορισθέντα στο (iii) έχουμε

$$\mathrm{Ker}(\vartheta) = H,\ \ \mathrm{Im}(\vartheta) = \{\,\vartheta(a,b) \mid (a,b)\in G\} = \{\,(a,b)\in G \mid\ a=0\} = K.$$

Κατά συνέπειαν, από το *1ο θεώρημα ισομορφισμών ομάδων* (βλ. 3.6.27) έπεται η ύπαρξη ενός ισομορφισμού $G/H \cong K$. □

ΘΕΜΑ 8ο Θεωρούμε την απεικόνιση

$$(\mathbb{Z}[\mathsf{X}],+) \xrightarrow{\ \vartheta\ } (\mathbb{Q}_{>0},\cdot),\ \ \sum_{i=0}^{n} a_i\mathsf{X}^i = f(\mathsf{X}) \longmapsto \vartheta\left(f(\mathsf{X})\right) := \prod_{i=0}^{n} p_i^{a_i},$$

όπου $p_0 = 2 < p_1 = 3 < \cdots < p_n$ οι αρχικοί (διαδοχικοί) $n+1$ όροι τής ακολουθίας $(p_\nu)_{\nu\in\mathbb{N}_0}$ (όλων) των πρώτων αριθμών. (Σημειωτέον ότι -εξ ορισμού- η εικόνα τού μηδενικού πολυωνύμου $0_{\mathbb{Z}[\mathsf{X}]}$ μέσω τής ϑ ισούται με το 1.) Η ϑ είναι *ομομορφισμός ομάδων*, καθότι για οιαδήποτε πολυώνυμα

$$f(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in \mathbb{Z}[\mathsf{X}], \quad g(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j \in \mathbb{Z}[\mathsf{X}],$$

έχουμε (υποθέτοντας, δίχως βλάβη τής γενικότητας, ότι $n \leq m$)

$$\begin{aligned} \vartheta\left(f(\mathsf{X}) + g(\mathsf{X})\right) &= p_0^{a_0+b_0} p_1^{a_1+b_1} \cdots p_n^{a_n+b_n} p_{n+1}^{b_{n+1}} \cdots p_m^{b_m} \\ &= \left(\prod_{i=0}^{n} p_i^{a_i}\right)\left(\prod_{j=0}^{m} p_j^{b_j}\right) = \vartheta\left(f(\mathsf{X})\right)\vartheta\left(g(\mathsf{X})\right). \end{aligned}$$

Έστω τυχών $r \in \mathbb{Q}_{>0}$. Ο r γράφεται *μονοσημάντως* ως κλάσμα $r = \frac{\alpha}{\beta}$ δυο *σχετικώς πρώτων* θετικών ακεραίων αριθμών α, β. Εάν $a \geq 2$ (και αντιστοίχως, εάν $\beta \geq 2$), τότε, σύμφωνα με το *Θεμελιώδες Θεώρημα τής Αριθμητικής* 2.3.7., ο α (και αντιστοίχως, ο β) γράφεται *μονοσημάντως* ως γινόμενο πρώτων αριθμών. Εάν λοιπόν $\alpha, \beta \geq 2$, τότε συμπεραίνουμε ότι ο r γράφεται *μονοσημάντως* ως

$$r = s_1^{\gamma_1} s_2^{\gamma_2} \cdots s_l^{\gamma_l},$$

όπου $l \in \mathbb{N}$, οι $s_1, s_2, \ldots, s_l$ πρώτοι αριθμοί με $s_1 < s_2 < \cdots < s_l$ και οι $\gamma_1, \gamma_2, \ldots, \gamma_l$ *μη μηδενικοί ακέραιοι αριθμοί*. Για να συμπεριλάβουμε την περίπτωση όπου κάποιος εκ των α, β είναι $= 1$ και για να εντάξουμε τους πρώτους αριθμούς (εντός τής αποσυνθέσεως *οιουδήποτε* $r \in \mathbb{Q}_{>0}$), οι οποίοι τυγχάνει να υψούνται σε με μη μηδενική ακέραια δύναμη, στην ακολουθία $(p_\nu)_{\nu\in\mathbb{N}_0}$ (όλων) των πρώτων αριθμών, έχουμε (προφανώς) τη δυνατότητα να *επεκτείνουμε* το ανωτέρω συμπέρασμα ως εξής: *Κάθε* $r \in \mathbb{Q}_{>0}$ γράφεται ως

$$r = p_0^{\delta_0} p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}$$

όπου $k \in \mathbb{N}$ και $\delta_0, \ldots, \delta_k$ (όχι κατ' ανάγκην μη μηδενικοί) *ακέραιοι αριθμοί*. Για τους $r \in \mathbb{Q}_{>0} \setminus \{1\}$ η ανωτέρω αποσύνθεση καθίσταται *μονοσήμαντη* θέτοντας ως $k := \max\{\nu \in \mathbb{N}_0 : p_\nu \mid r\}$. Επειδή

$$\vartheta\left(\sum_{i=0}^{k} \delta_i \mathsf{X}^i\right) = r$$

η ϑ είναι *επιριπτική*. Εν συνεχεία προσδιορίζουμε τον πυρήνα $\mathrm{Ker}(\vartheta)$ τής ϑ. Έστω τυχόν στοιχείο

$$f(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in \mathrm{Ker}(\vartheta).$$

Τότε

$$\vartheta\left(f(\mathsf{X})\right) = \prod_{i=0}^{n} p_i^{a_i} = 1 \Rightarrow a_0 = a_1 = \cdots = a_n = 0 \Rightarrow f(\mathsf{X}) = 0_{\mathbb{Z}[\mathsf{X}]},$$

οπότε $\mathrm{Ker}(\vartheta) = \{0_{\mathbb{Z}[\mathsf{X}]}\}$. Προφανώς, $\mathbb{Z}[\mathsf{X}] \cong \mathbb{Z}[\mathsf{X}]/\mathrm{Ker}(\vartheta)$, και, σύμφωνα με το *1ο θεώρημα ισομορφισμών ομάδων* (3.6.27), υφίσταται ένας ισομορφισμός μεταξύ τής $(\mathbb{Z}[\mathsf{X}], +)$ και τής $(\mathbb{Q}_{>0}, \cdot)$. □

<u>ΘΕΜΑ 9ο</u> Έστω $(R, +, \cdot)$ ένας δακτύλιος με μοναδιαίο (πολλαπλασιαστικό) στοιχείο, για τον οποίο ισχύει η ισότητα

$$\boxed{x^3 = x, \ \ \forall x \in R.} \tag{1}$$

(i) Για οιαδήποτε στοιχεία $x, y \in R$ έχουμε (λόγω τής (1))

$$x + y = (x+y)^3 = x + x^2y + xyx + xy^2 + yx^2 + yxy + y^2x + y,$$

οπότε

$$x^2y + xyx + xy^2 + yx^2 + yxy + y^2x = 0_R. \tag{2}$$

Θέτοντας στην (2) $-x$ αντί τού x λαμβάνουμε

$$x^2y + xyx - xy^2 + yx^2 - yxy - y^2x = 0_R. \tag{3}$$

Από τις (2) και (3) συνάγουμε ότι

$$2x^2y + 2xyx + 2yx^2 = 0_R. \tag{4}$$

Εφαρμόζοντας την (4) για $y = x$ και λαμβάνοντας υπ' όψιν ότι $x^3 = x$ (λόγω τής (1)) συμπεραίνουμε τελικώς ότι $6x = 0_R$.

(ii) Πολλαπλασιάζοντας αμφότερα τα μέλη τής (4) εξ αριστερών και εκ δεξιών με το x (και χρησιμοποιώντας τήν (1)) λαμβάνουμε

$$\left.\begin{array}{l} 2xy + 2x^2yx + 2xyx^2 = 0_R \\ 2x^2yx + 2xyx^2 + 2yx = 0_R \end{array}\right\} \Longrightarrow 2xy = 2yx. \tag{5}$$

Εάν στην (3) θέσουμε $y = 1_R$, τότε

$$3x^2 = 3x. \tag{6}$$

Επομένως, θέτοντας $x + y$ αντί τού x στην (6) λαμβάνουμε

$$\begin{array}{l} 3x + 3y = 3(x+y) = 3(x+y)^2 = 3x^2 + 3y^2 + 3xy + 3yx \\ \underset{(6)}{\Longrightarrow} 3xy + 3yx = 0_R \underset{(5)}{\Longrightarrow} 2yx + xy + 3yx = 0_R \\ \Longrightarrow 5yx + xy = 0_R \underset{(i)}{\Longrightarrow} -yx + xy = 0_R \Longrightarrow xy = yx, \end{array}$$

πράγμα που σημαίνει ότι ο R είναι όντως *μεταθετικός δακτύλιος*. □

<u>ΘΕΜΑ 10ο</u> Έστω p ένας περιττός πρώτος. Θεωρούμε το πολυώνυμο

$$\boxed{f_p(\mathsf{X}) := \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} \mathsf{X}^{p-2j}(\mathsf{X}^2-1)^j \in \mathbb{Z}[\mathsf{X}].}$$

Σημειωτέον ότι

$$(\mathsf{X}^2-1)^j = \sum_{k=0}^{j} \binom{j}{k} (-1)^{j-k} \mathsf{X}^{2k},$$

οπότε

$$f_p(\mathsf{X}) = \sum_{j=0}^{\frac{p-1}{2}} \tbinom{p}{2j} \mathsf{X}^{p-2j} \left(\sum_{k=0}^{j} \tbinom{j}{k} (-1)^{j-k} \mathsf{X}^{2k} \right) = \sum_{j=0}^{\frac{p-1}{2}} \tbinom{p}{2j} \left(\sum_{k=0}^{j} \tbinom{j}{k} (-1)^{j-k} \right) \mathsf{X}^{p-2(j-k)}$$

$$= \left(\sum_{j=0}^{\frac{p-1}{2}} \tbinom{p}{2j} \right) \mathsf{X}^p - \left(\sum_{j=1}^{\frac{p-1}{2}} \tbinom{p}{2j} j \right) \mathsf{X}^{p-2} + \left(\sum_{j=2}^{\frac{p-1}{2}} \tbinom{p}{2j} \tbinom{j}{j-2} \right) \mathsf{X}^{p-4} - \cdots$$

$$= \sum_{i=0}^{p} a_i \mathsf{X}^i,$$

όπου

$$a_i := \begin{cases} (-1)^{\frac{p-i}{2}} \left[\sum\limits_{j=\frac{p-i}{2}}^{\frac{p-1}{2}} \binom{p}{2j} \binom{j}{j-\frac{1}{2}(p-i)} \right], & \text{όταν } i \in \{1,3,5,\dots,p-4,p-2,p\}, \\ 0, & \text{όταν } i \in \{0,2,4,\dots,p-5,p-3,p-1\}. \end{cases}$$

(i) Εντός τού $f_p(\mathsf{X})$ ο συντελεστής τού X είναι ο

$$a_1 = (-1)^{\frac{p-1}{2}} \binom{p}{p-1} = (-1)^{\frac{p-1}{2}} p. \tag{1}$$

(ii) Επειδή $a_0 = 0$, το $f_p(\mathsf{X})$ γράφεται υπό τη μορφή $f_p(\mathsf{X}) = \mathsf{X} g_p(\mathsf{X})$, όπου

$$g_p(\mathsf{X}) = \sum_{i=0}^{p-1} b_i \mathsf{X}^i \in \mathbb{Z}[\mathsf{X}], \quad b_i := a_{i+1}, \ \ \forall i \in \{0,1,\dots,p-1\}.$$

(iii) Κατ' αρχάς παρατηρούμε ότι για κάθε $\nu \in \{1,\dots,p-1\}$,

$$\underbrace{\binom{p}{\nu} = \frac{p(p-1)\cdots(p-\nu+1)}{\nu!}}_{\Downarrow}$$
$$p(p-1)\cdots(p-\nu+1) = 1\cdot 2\cdot 3\cdots\nu \cdot \tbinom{p}{\nu},$$

έχουμε

$$\left.\begin{array}{r} p \mid 1\cdot 2\cdot 3\cdots\nu\cdot\binom{p}{\nu} \\ \text{μκδ}(p, 1\cdot 2\cdot 3\cdots\nu) = 1 \end{array}\right\} \underset{(\text{πρβλ. } 2.2.10)}{\Longrightarrow} p \mid \tbinom{p}{\nu}. \tag{2}$$

Ως εκ τούτου,

$$p \mid b_i \ \left(= a_{i+1} = (-1)^{\frac{p-(i+1)}{2}} \left[\sum_{j=\frac{p-(i+1)}{2}}^{\frac{p-1}{2}} \binom{p}{2j} \binom{j}{j-\frac{1}{2}(p-(i+1))} \right] \right)$$

για κάθε $i \in \{0,2,4,\dots,p-5,p-3\}$ (βλ. 2.1.5 (vi)). Επειδή, επιπροσθέτως,

$$p \mid 0 \ (= b_i = a_{i+1}), \ \ \forall i \in \{1,3,5,\dots,p-4,p-2\}$$

(βλ. 2.1.3 (i)), συμπεραίνουμε ότι

$$p \mid b_i, \ \ \forall i \in \mathbb{N} : \ 1 \le i \le p-2. \tag{3}$$

Εκ παραλλήλου, από τις ισότητες (1) έπεται άμεσα ότι

$$p \mid a_1 = b_0, \ \ p^2 \nmid b_0. \tag{4}$$

Τέλος,

$$p \nmid b_{p-1} \ (= a_p = \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j}). \tag{5}$$

[Πράγματι· εάν υποθέταμε ότι $p \mid \sum_{j=1}^{\frac{p-1}{2}} \binom{p}{2j} + 1$, τότε θα υπήρχε κάποιος θετικός ακέραιος αριθμός ℓ, τέτοιος ώστε

$$\sum_{j=1}^{\frac{p-1}{2}} \binom{p}{2j} + 1 = \ell p.$$

Επειδή $p \mid \binom{p}{2j}$, $\forall j \in \{1, 2, \ldots, \frac{p-1}{2}\}$ (πρβλ. (2)), θα είχαμε

$$\left.\begin{array}{r} \text{2.1.5 (vi)} \Rightarrow p \mid \sum_{j=1}^{\frac{p-1}{2}} \binom{p}{2j} \\ p \mid \ell p \end{array}\right\} \underset{\text{2.1.5 (vi)}}{\Longrightarrow} p \mid \ell p - \sum_{j=1}^{\frac{p-1}{2}} \binom{p}{2j} \Rightarrow p \mid 1,$$

κάτι που θα αντέφασκε π.χ. προς το ότι $p \geq 3$ (πρβλ. 2.1.5 (ii)).]

Λόγω των υφιστάμενων σχέσεων διαιρετότητας (3), (4) και (5) είναι δυνατή η εφαρμογή τού κριτηρίου 5.5.9 τού Eisenstein, το οποίο μας εξασφαλίζει την αναγωγιμότητα τού πολυωνύμου $g_p(\mathsf{X})$ εντός τού $\mathbb{Q}[\mathsf{X}]$. □

- **Τα θεωρητικά θέματα 1, 2, 3, 4 και 5 είχαν διδαχθεί κατά τη διάρκεια των παραδόσεων. Μάλιστα, τα θέματα 1, 2 και 4 είχαν ξαναδοθεί σε προηγούμενες εξετάσεις: το 1 τον Ιούλιο 2006, το 2 τον Ιούνιο 2009 και το 4 τον Σεπτέμβριο 2006.**

- **Το θέμα 9 είχε δοθεί ως άσκηση και λυθεί από τον βοηθό στις ώρες των φροντιστηρίων (βλ. άσκηση 3 τού 8ου καταλόγου προτεινομένων ασκήσεων).**

- **Το (i) τού θέματος 6 αντιμετωπιζόταν με στοιχειώδη μέσα (κατ' ουσίαν με τις πρώτιστες ιδιότητες διαιρετότητας ακεραίων και ισοτιμιών, πρβλ. 2.3.10 και 2.4.5). Η υπόδειξη για τον τρόπο αποδείξεως τού (ii) αποτελούσε μια διευκολυντική αφετηρία για την παράθεση των απαραίτητων συλλογισμών.**

- **Το θέμα 7 απαιτούσε μόνον τη γνώση των ορισμών τής ομάδας, τής αβελιανής ομάδας, τής υποομάδας και τής ορθόθετης υποομάδας, και απλή εφαρμογή τού 1ου θεωρήματος ισομορφισμών ομάδων (3.6.27) για την απεικόνιση ϑ. Ο τρόπος ορισμού αυτής υπαγορευόταν άμεσα από το τι επιζητείτο μέσω τού (iv).**

- **Η μοναδική δυσκολία στο θέμα 10 ενέκειτο στον ακριβή προσδιορισμό των συντελεστών τού δοθέντος πολυωνύμου (μέσω τού διωνυμικού τύπου). Ωστόσο, ύστερα από την εύρεση αυτών, τα (i) και (ii) ήσαν τετριμμένα, ενώ το (iii) ανήγετο στην απόδειξη τού ότι πληρούνται οι συνθήκες τού κριτηρίου αναγωγιμότητας 5.5.9 τού Eisenstein, κάτι που εξασφαλιζόταν κάνοντας χρήση απλών, γνωστών ιδιοτήτων διαιρετότητας.**

- **Η άσκηση 8 ήταν κατά τι πιο απαιτητική, καθότι προϋπέθετε έναν κάποιο βαθμό ευρηματικότητας για τον προσδιορισμό τού ισομορφισμού ϑ και κατάλληλο χειρισμό τού Θεμελιώδους Θεωρήματος τής Αριθμητικής.**