Ιανουάριος

ΑΛΓΕΒΡΑ

Πρόσθετη Εξέταση 2013 - 2014

Θέμα 1 (1 μονάδα).
(α) Βρείτε στοιχείο τάξης 7 στην A_7.
(β) Υπάρχει στοιχείο τάξης 8 στην A_7;

Λύση.
(α) Ο 7-κύκλος $(1\ 2\ 3\ 4\ 5\ 6\ 7)$, όπως και κάθε 7-κύκλος είναι άρτια μετάθεση (άρα ανήκει στην A_7) και έχει τάξη 7.
(β) Όχι. Η τάξη κάθε στοιχείου της A_7 βρίσκεται από την μοναδική του ανάλυση σε γινόμενο ξένων κύκλων και είναι το ελάχιστο κοινό πολλάπλάσιο των μηκών των ξένων κύκλων που εμφανίζονται στην ανάλυση αυτή. Για να είναι το ελάχιστο κοινό πολλαπλάσιο των μηκών ίσο με 8, θα πρέπει ένας από τους εν λόγω κύκλους να έχει μήκος 8, κάτι που είναι αδύνατο στην A_7.

Θέμα 2 (0.5 μονάδα). Έστω G ομάδα με $|G| \leq 500$. Έστω ότι υπάρχουν υποομάδες H, K της G με $|H| = 20$, $|K| = 21$. Δείξτε ότι $|G| = 420$.

Λύση. Από το θεώρημα Lagrange, έχουμε $20 \mid |G|$ και $21 \mid |G|$, άρα $420 \mid |G|$. Αφού $|G| \leq 500$, έπεται ότι $|G| = 420$.

Θέμα 3 (1 μονάδα).
(α) Δείξτε ότι το $2 + i$ διαιρεί το $9 + 2i$ στο $\mathbb{Z}[i]$.
(β) Αναλύστε το $9 + 2i$ σε γινόμενο ανάγωγων στοιχείων του $\mathbb{Z}[i]$.

Λύση.
(α) Θέτοντας $9+2i = (2+i)(a+bi)$, και εξισώνοντας πραγματικά και φανταστικά μέρη, έχουμε $2a-b = 9$ και $a + 2b = 2$. Λύνοντας το σύστημα, βρίσκουμε $a = 4$ και $b = -1$, δηλαδή $9 + 2i = (2 + i)(4 - i)$, άρα $2 + i \mid 9 + 2i$ στο $\mathbb{Z}[i]$.
(β) Χρησιμοποιώντας τη συνήθη νόρμα της Ευκλείδειας περιοχής $\mathbb{Z}[i]$, έχουμε $N(2+i) = 5$, $N(4-i) = 17$, άρα, αφού οι 5 και 17 είναι πρώτοι αριθμοί, έπεται ότι το γινόμενο $(2 + i)(4 - i)$ είναι μία ανάλυση του $9 + 2i$ σε γινόμενο ανάγωγων παραγόντων στο $\mathbb{Z}[i]$.

Θέμα 4 (1 μονάδα). Έστω H υποομάδα μιας ομάδας G τέτοια ώστε $xyx^{-1}y^9 \in H$, για κάθε $x, y \in G$.
(α) Δείξτε ότι η H είναι κανονική υποομάδα της G.
(β) Υπάρχει γνήσια υποομάδα H της S_3 τέτοια ώστε $xyx^{-1}y^9 \in H$, για κάθε $x, y \in S_3$;

Λύση.
(α) Έστω $x \in G$ και $y \in H$. Τότε, από την υπόθεση, $xyx^{-1} = (xyx^{-1}y^9)y^{-9} \in H$. Επομένως, η H είναι κανονική υποομάδα της G.
(β) Ναί, η A_3. Από το (α), μία τέτοια H θα ήταν κανονική υποομάδα της S_3. Οι μόνες γνήσιες κανονικές υποομάδες τηω S_3 είναι οι A_3 και η $\{1\}$. Δεν μπορεί να έχουμε $H = \{1\}$, διότι η $\{1\}$ δεν πληροί τη δοσμένη συνθήκη: αν θέσουμε $x = 1$ και $y = (1\ 2\ 3)$, τότε $xyx^{-1}y^9 = (1\ 2\ 3) \notin \{1\}$. Επομένως, η μόνη πιθανότητα είναι να έχουμε $H = A_3$, η οποία πληροί τη δοσμένη συνθήκη: για κάθε $x, y \in S_3$, έχουμε $\mathrm{sgn}(xyx^{-1}y^9) = \mathrm{sgn}(x)\,\mathrm{sgn}(y)\,\mathrm{sgn}(x)^{-1}\,\mathrm{sgn}(y)^9 = \mathrm{sgn}(y)^{10} = 1$, δηλαδή $xyx^{-1}y^9 \in A_3$.

Θέμα 5 (0.5 μονάδα). Να βρεθούν όλοι οι ακέραιοι m για τους οποίους το ιδεώδες

$$\langle\, x^{1974} + 1940\, m\, x^{1922} + 1896\, m^2\, x^{1821} + 330\, m^3\, x^{1453} + 2014 \,\rangle$$

είναι maximal στο $\mathbb{Q}[x]$.

Λύση. Όποια και αν είναι η τιμή του $m \in \mathbb{Z}$, το δοσμένο πολυώνυμο είναι Eisenstein για $p = 2$, επομένως ανάγωγο στο $\mathbb{Q}[x]$. Αφού το $\mathbb{Q}$ είναι σώμα, έπεται ότι το ιδεώδες που παράγεται από αυτό το πολυώνυμο είναι maximal στο $\mathbb{Q}[x]$.

Θέμα 6 (0.5 μονάδα). Έστω $f(x) \in \mathbb{R}[x]$ τέτοιο ώστε

$$f(1) = f(2) = f(3) = \cdots = f(100) = 101.$$

Δείξτε ότι ο δακτύλιος $\mathbb{R}[x]/\langle f(x) - 101\rangle$ έχει τουλάχιστον 100 πρώτα ιδεώδη.

Λύση. Το πολυώνυμο $f(x) - 101$ διαιρείται από τα $x-1, x-2, \ldots, x-100$ στο $\mathbb{R}[x]$. Επομένως το ιδεώδες $I = \langle f(x) - 100\rangle$ περιέχεται στα πρώτα ιδεώδη $I_k = \langle x - k\rangle$ του $\mathbb{R}[x]$, για $k \in \{1, 2, \ldots, 100\}$. Από το τέταρτο θεώρημα ισομορφισμού δακτυλίων, τα ιδεώδη I_k/I, για $k \in \{1, 2, \ldots, 100\}$, είναι ανά δύο διαφορετικά ιδεώδη του $\mathbb{R}[x]/I$. Από το τρίτο θεώρημα ισομορφισμού δακτυλίων, για κάθε $k \in \{1, 2, \ldots, 100\}$, ο δακτύλιος πηλίκο $(\mathbb{R}[x]/I)\,/\,(I_k/I)$ είναι ισόμορφος με τον δακτύλιο πηλίκο $\mathbb{R}[x]/I_k$, που είναι ακέραια περιοχή. Επομένως τα ιδεώδη I_k/I, για $k \in \{1, 2, \ldots, 100\}$, είναι ανά δύο διαφορετικά πρώτα ιδεώδη του δακτυλίου $\mathbb{R}[x]/I$.

Θέμα 7 (1 μονάδα). Έστω $F^\times = F \setminus \{0\}$ η πολλαπλασιαστική ομάδα ενός σώματος F, όπου $|F| = 37$.
(α) Πόσες διαφορετικές λύσεις έχει η εξίσωση $x^{60} = 1$ στο F;
(β) Βρείτε όλους τους ομομορφισμούς ομάδων $F^\times \to F$.

Λύση.
(α) Κάθε τέτοια λύση θα είναι στοιχείο της $F^\times$ που είναι κυκλική ομάδα με 36 στοιχεία. Έστω g ένας γεννήτορας αυτής της ομάδας. Ψάχνουμε επομένως το πλήθος των $m \in \{0, 1, \ldots, 35\}$ για τα οποία έχουμε $g^{60m} = 1$ δηλαδή για τα οποία $36 \mid 60m$ ή, ισοδύναμα, $3 \mid m$. Άρα υπάρχουν 12 τέτοιες λύσεις.
(β) Από το πρώτο θεώρημα ισομορφισμού ομάδων και το θεώρημα Lagrange, το πλήθος των στοιχείων στην εικόνα ενός ομομορφισμού $F^\times \to F$ θα διαιρούσε το 37 και το 36, άρα θα ήταν ίσο με 1. Επομένως, ο μόνος τέτοιος ομομορφισμός είναι ο τετριμμένος.

Θέμα 8 (1.5 μονάδα).
(α) Είναι το $\mathbb{Z}[x]$ ιδεώδες του $\mathbb{Q}[x]$;
(β) Έστω I πρώτο ιδεώδες του $\mathbb{Q}[x]$. Δείξτε ότι το $I \cap \mathbb{Z}[x]$ είναι πρώτο ιδεώδες του $\mathbb{Z}[x]$.
(γ) Έστω J πρώτο ιδεώδες του $\mathbb{Z}[x]$. Είναι το J απαραίτητα πρώτο ιδεώδες του $\mathbb{Q}[x]$;

Λύση.
(α) Όχι. Έχουμε $\frac{1}{2} \in \mathbb{Q}[x]$ και $x \in \mathbb{Z}[x]$, αλλά $\frac{1}{2}x \notin \mathbb{Z}[x]$.
(β) Τα I και $\mathbb{Z}[x]$ είναι υποδακτύλιοι του $\mathbb{Q}[x]$, άρα το ίδιο ισχύει και για το $I \cap \mathbb{Z}[x]$. Αφού έχουμε $I \cap \mathbb{Z}[x] \subseteq \mathbb{Z}[x]$, έπεται ότι το $I \cap \mathbb{Z}[x]$ είναι υποδακτύλιος του $\mathbb{Z}[x]$. Έστω τώρα $f(x) \in \mathbb{Z}[x]$ και $g(x) \in I \cap \mathbb{Z}[x]$. Τότε $f(x)g(x) \in I$ (αφού το I είναι ιδεώδες του $\mathbb{Q}[x]$) και προφανώς $f(x)g(x) \in \mathbb{Z}[x]$. Άρα $f(x)g(x) \in I \cap \mathbb{Z}[x]$. Επομένως το $I \cap \mathbb{Z}[x]$ είναι ιδεώδες του $\mathbb{Z}[x]$. Επίσης, αφού $1 \notin I$ (διότι το I είναι γνήσιο ιδεώδες του $\mathbb{Q}[x]$), έπεται ότι $1 \notin I \cap \mathbb{Z}[x]$, άρα το $I \cap \mathbb{Z}[x]$ είναι γνήσιο ιδεώδες του $\mathbb{Z}[x]$. Τέλος, έστω $f(x), g(x) \in \mathbb{Z}[x]$ τέτοια ώστε $f(x)g(x) \in I \cap \mathbb{Z}[x]$. Τότε $f(x)g(x) \in I$, άρα, αφού το I είναι πρώτο ιδεώδες του $\mathbb{Q}[x]$, έπεται ότι $f(x) \in I$ ή $g(x) \in I$. Επομένως, $f(x) \in I \cap \mathbb{Z}[x]$ ή $g(x) \in I \cap \mathbb{Z}[x]$.
(γ) Όχι. Το J δεν είναι καν απαραίτητα ιδεώδες του $\mathbb{Q}[x]$. Για παράδειγμα, έστω J το σύνολο των πολυωνύμων με ακέραιους και άρτιους συντελεστές. Το J είναι πρώτο ιδεώδες του $\mathbb{Z}[x]$, διότι, από το πρώτο

θεώρημα ισομορφισμού, ο δακτύλιος $\mathbb{Z}[x]/J$ είναι ισόμορφος με τον $(\mathbb{Z}/2\mathbb{Z})[x]$, που είναι ακέραια περιοχή. Όμως, το J δεν είναι ιδεώδες του $\mathbb{Q}[x]$ διότι $\frac{1}{2} \in \mathbb{Q}[x]$, $2 \in J$, αλλά $1 = \frac{1}{2}2 \notin J$.

Θέμα 9 (1.5 μονάδα). Έστω q πρώτος αριθμός. Για θετικό ακέραιο n, έστω $s(n)$ το άθροισμα των ψηφίων του n στην μοναδική q-αδική του αναπαράσταση, δηλαδή, γράφοντας $n = a_k q^k + a_{k-1} q^{k-1} + \ldots + a_0$, με $k \in \mathbb{N}$ και $a_k, a_{k-1}, \ldots, a_0 \in \{0, 1, \ldots, q-1\}$, θέτουμε $s(n) = a_k + a_{k-1} + \ldots a_0$.
(α) Δείξτε ότι $x^n \equiv x^{s(n)} \pmod{q}$, για κάθε $x \in \mathbb{Z}$.
(β) Δείξτε ότι $5^{7^7+7^6+7^5} \equiv 6 \pmod{7}$.
(γ) Βρείτε $x \in \mathbb{Z}$ τέτοιο ώστε $x \equiv 5^{7^7+7^6+7^5} \pmod{7}$ και $x \equiv 11 \pmod{40}$.

Λύση.
(α) Από το θεώρημα του Fermat έχουμε $x^q \equiv x \pmod{q}$, για κάθε $x \in \mathbb{Z}$. Άρα επαγωγικά έπεται ότι $x^{q^m} \equiv x \pmod{q}$, για κάθε $x \in \mathbb{Z}$ και για κάθε $m \in \mathbb{N}$. Επομένως,

$$x^n \equiv x^{a_k q^k + \cdots + a_0} \equiv x^{a_k + \cdots + a_0} \equiv x^{s(n)} \pmod{q}.$$

(β) Από το (α), για $x = 5$, $q = 7$ και $n = 7^7 + 7^6 + 7^5$, έχουμε $s(n) = 3$, άρα

$$x^{7^7+7^6+7^5} \equiv 5^3 \equiv 6 \pmod{7}.$$

(γ) Από το (β), αρκεί να λύσουμε το σύστημα

$$x \equiv 6 \pmod{7}, \qquad x \equiv 11 \pmod{40}.$$

Εφαρμόζοντας τον αλγόριθμο που περιγράφει το Κινέζικο Θεώρημα, βρίσκουμε ότι $x \equiv 251 \pmod{280}$. Άρα ένα τέτοιο x είναι το 251.

Θέμα 10 (1.5 μονάδα). Έστω $O(3)$ η πολλαπλασιαστική ομάδα των 3×3 ορθογώνιων πινάκων με στοιχεία στο $\mathbb{R}$, δηλαδή $O(3) = \{A \in M_3(\mathbb{R}) : AA^t = I\}$. Έστω $SO(3) = \{A \in O(3) : \det(\mathrm{A}) = 1\}$.
(α) Δείξτε ότι η $\{I, -I\}$ είναι κανονική υποομάδα της $O(3)$.
(β) Δείξτε ότι η ομάδα πηλίκο $O(3)/\{I, -I\}$ είναι ισόμορφη με την $SO(3)$.
(γ) Είναι η $O(3)$ ισόμορφη με την $SO(3) \times \{I, -I\}$;

Λύση.
(α) Αν $A \in O(3)$ και $B = \pm I$, τότε $ABA^{-1} = \pm AA^{-1} = \pm I \in \{I, -I\}$.
(β) Έστω $f : O(3) \to SO(3)$ η απεικόνιση που δίνεται από τον τύπο $f(A) = \det(A)\ A$, για κάθε $A \in O(3)$. Προφανώς, $f(AB) = f(A)f(B)$, για κάθε A, $B \in O(3)$, και $f(\pm I) = I$. Αντίστροφα, αν $f(A) = I$, για κάποιο $A \in O(3)$, τότε $A = \det(A)^{-1} I$. Αφού η ορίζουσα ενός ορθογώνιου πίνακα ισούται με ± 1, έπεται ότι $A = \pm I$. Επομένως, $\mathrm{Ker}(f) = \{I, -I\}$. Επίσης, αν $A \in SO(3)$, τότε $A = \det(A)\ A = f(A)$, άρα η f είναι επί. Επομένως, από το πρώτο θεώρημα ισομορφισμού, η ομάδα πηλίκο $O(3)/\{I, -I\}$ είναι ισόμορφη με την $SO(3)$.
(γ) Ναί. Έστω $g : O(3) \to SO(3) \times \{I, -I\}$ η απεικόνιση με $g(A) = (\det(A)\ A,\ \det(A)\ I)$, για κάθε $A \in O(3)$. Προφανώς η g είναι ομομορφισμός ομάδων. Αν $A \in \mathrm{Ker}(g)$, τότε $\det(A)\ A = I$ και $\det(A)\ I = I$, επομένως $\det(A) = 1$, άρα $A = I$. Επομένως, η g ειναι 1-1. Τέλος, έστω ότι $(B,\ aI) \in SO(3) \times \{I, -I\}$, όπου $a \in \{1, -1\}$. Τότε $g(aB) = (\det(aB)\ aB,\ \det(\mathrm{aB})\ \mathrm{I})$. Αφού $\det(B) = 1$ και $\det(aB) = a^3 = a$, έπεται ότι $g(aB) = (B, aI)$, άρα η g είναι επί.

ΑΛΓΕΒΡΑ

Επαναληπτική Εξέταση 2012 - 2013

Θέμα 1 (1.5 μονάδα). Θεωρούμε τα πολυώνυμα $f(x) = x^2 - 1$ και $g(x) = (x-1)^2$ στο $\mathbb{C}[x]$.
(α) Να βρεθεί ο μέγιστος κοινός τους διαιρέτης $h(x)$.
(β) Βρείτε $\alpha(x), \beta(x) \in \mathbb{Q}[x]$ τέτοια ώστε $h(x) = \alpha(x)f(x) + \beta(x)g(x)$.
(γ) Υπάρχουν $\alpha(x), \beta(x) \in \mathbb{C}[x]$ τέτοια ώστε $h(x) + 1 = \alpha(x)f(x) + \beta(x)g(x)$;

Λύση.
(α) Έχουμε $x^2 - 1 = (x-1)(x+1)$, άρα $h(x) = x - 1$.
(β) Εφαρμόζοντας τον Ευκλείδειο αλγόριθμο, μπορούμε να πάρουμε $\alpha(x) = \frac{1}{2}$, $\beta(x) = -\frac{1}{2}$.
(γ) Όχι, διότι αν υπήρχαν τέτοια $\alpha(x), \beta(x)$, τότε $h(x) \mid \alpha(x)f(x) + \beta(x)g(x) = h(x) + 1$, άρα $h(x) \mid 1$, που είναι άτοπο.

Θέμα 2 (1.5 μονάδα). Έστω τ στοιχείο της S_7 τέτοιο ώστε $\tau(1) = 2$, $\tau(2) = 3$, $\tau(3) = 1$, $\tau(4) = 5$, $\tau(5) = 4$.
(α) Να βρεθεί η τάξη της τ.
(β) Έστω ότι $\tau \in A_7$. Να βρεθούν τα $\tau(6)$, $\tau(7)$.
(γ) Έστω ότι $\tau \notin A_7$. Να βρεθούν όλα τα $n \in \mathbb{Z}$ για τα οποία η τ^n είναι αντιμετάθεση.

(α) Ως γινόμενο ξένων κύκλων, η τ γράφεται ως $\tau = (1\ 2\ 3)(4\ 5)\sigma$, όπου σ είναι είτε η ταυτοτική μετάθεση είτε η αντιμετάθεση $(6\ 7)$. Σε κάθε περίπτωση, ο μέγιστος κοινός διαιρέτης των μηκών των ξένων κύκλων που εμφανίζονται στην ανάλυση της τ ισούται με 6, δηλαδή η τάξη της τ είναι 6.
(β) Ο κύκλος $(1\ 2\ 3)$ είναι άρτια μετάθεση και κάθε αντιμετάθεση είναι περιττή μετάθεση, άρα, για να ισχύει $\tau \in A_7$, πρέπει να ισχύει $\sigma = (6\ 7)$, δηλαδή $\tau(6) = 7$ και $\tau(7) = 6$.
(γ) Αφού $\tau \notin A_7$, έπεται $\tau = (1\ 2\ 3)(4\ 5)$, άρα $\tau^n = (1\ 2\ 3)^n(4\ 5)^n$ για κάθε n. Για να είναι η τ^n αντιμετάθεση, πρέπει η $(1\ 2\ 3)^n$ να είναι τετριμμένη και η $(4\ 5)^n$ να μην είναι τετριμμένη. Πρέπει δηλαδή ο n να διαιρείται με το 3 αλλά όχι με το 2, άρα $n \equiv 3 \pmod 6$.

Θέμα 3 (1.5 μονάδα). Έστω G κυκλική ομάδα με γεννήτορα g και τάξη 6000.
(α) Να βρεθεί η τάξη του g^{18}.
(β) Δείξτε ότι $\langle g^{18} \rangle = \langle g^{42} \rangle$.
(γ) Έστω H κυκλική ομάδα τάξης 49. Να βρεθούν όλοι οι ομομορφισμοί $f : G \to H$.

Λύση.
(α) Επειδή $(18, 6000) = 6$, η τάξη του g^{18} ισούται με $\frac{6000}{6} = 1000$.
(β) Όπως και στο (α), η τάξη του g^{42} ισούται επίσης με 1000. Επειδή υπάρχει μοναδική υποομάδα της G τάξης 1000, έπεται ότι η υποομάδα που γεννάει το g^{18} ισούται με την υποομάδα που γεννάει το g^{42}.
(γ) Το $Im(f)$ είναι υποομάδα της H, άρα, από το θεώρημα Lagrange, το πλήθος των στοιχείων του $Im(f)$ διαιρεί το 49. Από το πρώτο θεώρημα ισομορφισμού και το θεώρημα Lagrange, το πλήθος των στοιχείων του $Im(f)$ διαιρεί το 6000. Αφού $(6000, 49) = 1$, έπεται ότι $Im(f) = \{1\}$, άρα ο f είναι ο τετριμμένος ομομορφισμός.

Θέμα 4 (1 μονάδα).
(α) Βρείτε $a \in \{225, 226, \ldots, 449\}$ τέτοιο ώστε $9 \mid a+1$ και $25 \mid a+2$.
(β) Δείξτε ότι για κάθε $a \in \mathbb{Z}$ ισχύει ότι $9 \mid a^{122} - a^2$ και $25 \mid a^{122} - a^2$.

Λύση.
(α) Θέλουμε να λύσουμε το σύστημα

$$x \equiv 8 \pmod 9, \qquad x \equiv 23 \pmod{25}.$$

Εφαρμόζοντας τον αλγόριθμο της απόδειξης του κινέζικου θεωρήματος, βρίσκουμε $x \equiv 98 \pmod{225}$. Επομένως, η μοναδική λύση στο σύνολο $\{225, 226, \ldots, 449\}$ είναι το $a = 323$.
(β) Έχουμε $\varphi(9) = 6$ και $\varphi(25) = 20$. Αν $(a,3) = 1$, τότε το θεώρημα Euler δίνει $a^6 \equiv 1 \pmod 9$, άρα $a^{120} \equiv 1 \pmod 9$, άρα $9 \mid a^2(a^{120}-1) = a^{122} - a^2$. Αν $3 \mid a$, τότε $9 \mid a^2$, άρα $9 \mid a^2(a^{120}-1) = a^{122} - a^2$. Όμοια, αν $(a,5) = 1$, έχουμε $a^{20} \equiv 1 \pmod{25}$, άρα $a^{120} \equiv 1 \pmod{25}$, άρα $25 \mid a^{122} - a^2$. Αν $5 \mid a$, τότε $25 \mid a^2$, άρα $25 \mid a^{122} - a^2$.

Θέμα 5 (1.5 μονάδα).
(α) Είναι το $\langle x^4 - 14 \rangle$ πρώτο ιδεώδες του $\mathbb{R}[x]$;
(β) Είναι ο δακτύλιος $\mathbb{Q}[x]/\langle x^4 - 14 \rangle$ σώμα;
(γ) Έστω F σώμα χαρακτηριστικής 3. Είναι ο δακτύλιος $F[x]/\langle x^4 - 14 \rangle$ ακέραια περιοχή;

Λύση.
(α) Όχι, διότι το πολυώνυμο $x^4 - 14$ έχει ρίζα στο $\mathbb{R}$, άρα δεν είναι ανάγωγο στο $\mathbb{R}[x]$.
(β) Ναι, διότι, από το κριτήριο Eisenstein για $p = 2$ (ή για $p = 7$), το πολυώνυμο $x^4 - 14$ είναι ανάγωγο στο $\mathbb{Q}[x]$, επομένως το ιδεώδες $\langle x^4 - 14 \rangle$ είναι maximal στο $\mathbb{Q}[x]$.
(γ) Όχι, διότι στο F ισχύει $x^4 - 14 = x^4 + 1 = (x^2 - x - 1)(x^2 + x - 1)$, άρα το $x^4 - 14$ δεν είναι ανάγωγο στο $F[x]$.

Θέμα 6 (1.5 μονάδα). Έστω R ο δακτύλιος των πινάκων της μορφής $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$, όπου $a, b, c \in \mathbb{C}$, με τις συνήθεις πράξεις.
(α) Δείξτε ότι το σύνολο I των στοιχείων του R της μορφής $\begin{bmatrix} 0 & b \\ 0 & c \end{bmatrix}$, όπου $b, c \in \mathbb{C}$, είναι ιδεώδες του R.
(β) Βρείτε ισομορφισμό δακτυλίων $R/I \to \mathbb{C}$.
(γ) Είναι το I maximal ιδεώδες του R;

Λύση.
(α) Με τετριμμένες πράξεις πινάκων αποδεικνύεται ότι $I \neq \emptyset$, ότι $B - C \in I$, για κάθε $B, C \in I$ και επίσης ότι $AB, BA \in I$ για κάθε $A \in R$, $B \in I$. Άρα το I είναι ιδεώδες του R.
(β) Με τετριμμένες πράξεις πινάκων αποδεικνύεται ότι η απεικόνιση $f : R \to \mathbb{C}$ που δίνεται από τον τύπο $f\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\right) = a$, είναι επιμορφισμός δακτυλίων με πυρήνα I. Το ζητούμενο επομένως προκύπτει από το πρώτο θεώρημα ισομορφισμού.
(γ) Ναι, διότι το $\mathbb{C}$ είναι σώμα.

Θέμα 7 (1 μονάδες). Έστω H, K κανονικές υποομάδες μιας ομάδας G με $H, K \neq G$.
(α) Δείξτε ότι η $H \cap K$ είναι κανονική υποομάδα της G.
(β) Έστω ότι η ομάδα $G/(H \cap K)$ είναι κυκλική τάξης 17. Δείξτε ότι $H = K$.

Λύση.
(α) Έστω $a \in H \cap K$ και $g \in G$. Τότε $gag^{-1} \in H$ (διότι $a \in H$ και $H \trianglelefteq G$) και $gag^{-1} \in K$ (διότι $a \in K$ και $K \trianglelefteq G$), άρα $gag^{-1} \in H \cap K$.
(β) Από την υπόθεση, η $G/(H \cap K)$ δεν έχει μη τετριμμένη γνήσια υποομάδα. Επομένως, από το τέταρτο θεώρημα ισομορφισμού, έχουμε ότι $H/(H \cap K) = \{1\}$, άρα $H = H \cap K$. Όμοια, $K = H \cap K$, επομένως, $H = K$.

Θέμα 8 (0.5 μονάδα). Δείξτε ότι οι δακτύλιοι $\mathbb{Q}[x]$ και $\mathbb{Z}[x, y]$ δεν είναι ισόμορφοι.

Λύση. Ο $\mathbb{Q}[x]$ είναι περιοχή κύριων ιδεωδών, ενώ ο $\mathbb{Z}[x, y]$ δεν είναι.

ΑΛΓΕΒΡΑ

Εξέταση Εαρινού Εξαμήνου 2012 - 2013

Θέμα 1 (0.5 μονάδα). Δείξτε ότι το πολυώνυμο $f(x) = 7x^4 + 15x^2 + 30x + 45$ είναι ανάγωγο στο $\mathbb{Q}[x]$.

Λύση. Το ζητούμενο προκύπτει από το κριτήριο Eisenstein για $p = 5$.

Θέμα 2 (1.5 μονάδα). Έστω σ το εξής στοιχείο της S_{10}:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 9 & 7 & 8 & 1 & 4 & 5 & 6 & 2 & 10 \end{pmatrix}.$$

(α) Γράψτε τη μετάθεση σ ως γινόμενο ξένων κύκλων.
(β) Βρείτε την τάξη της σ.
(γ) Εξετάστε αν $\sigma \in A_{10}$.

Λύση.
(α) $\sigma = (1\ 3\ 7\ 5)\ (2\ 9)\ (4\ 8\ 6)$.
(β) Η τάξη ενός γινομένου ξένων κύκλων είναι το ελάχιστο κοινό πολλαπλάσιο των τάξεων των κύκλων που εμφανίζονται στο γινόμενο. Αφού για κάθε θετικό ακέραιο k η τάξη ενός k-κύκλου ισούται με k, έπεται ότι η τάξη της σ ισούται με 12.
(γ) Οι 4-κύκλοι και οι 2-κύκλοι είναι περιττές μεταθέσεις ενώ οι 3-κύκλοι είναι άρτιες μεταθέσεις, άρα η σ είναι άρτια μετάθεση, δηλαδή $\sigma \in A_{10}$.

Θέμα 3 (1 μονάδα). Έστω G κυκλική ομάδα με γεννήτορα g και τάξη 14.
(α) Βρείτε όλες τις υποομάδες της G.
(β) Για κάθε υποομάδα H της G βρείτε όλα τα $h \in H$ για τα οποία ισχύει $H = \langle h \rangle$.

Λύση.
(α) Αφού $14 = 2 \cdot 7$, η θεωρία των κυκλικών ομάδων συνεπάγεται ότι υπάρχουν ακριβώς 4 υποομάδες της G (μία για καθε διαιρέτη του 14) και είναι οι εξής:

$$H_1 = \{1\},$$
$$H_2 = \{1, g^7\},$$
$$H_3 = \{1, g^2, g^4, g^6, g^8, g^{10}, g^{12}\},$$
$$H_4 = \{1, g, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10}, g^{11}, g^{12}, g^{13}\} = G.$$

(β) Από τη θεωρία των κυκλικών ομάδων, έχουμε

$$H_1 = \langle 1 \rangle,$$
$$H_2 = \langle g^7 \rangle$$
$$H_3 = \langle g^2 \rangle = \langle g^4 \rangle = \langle g^6 \rangle = \langle g^8 \rangle = \langle g^{10} \rangle = \langle g^{12} \rangle,$$
$$H_4 = \langle g \rangle = \langle g^3 \rangle = \langle g^5 \rangle = \langle g^9 \rangle = \langle g^{11} \rangle = \langle g^{13} \rangle.$$

Θέμα 4 (0.5 μονάδα). Έστω I το ιδεώδες του $\mathbb{Q}[x]$ που γεννιέται από τα πολυώνυμα $f(x) = x^3 + x - 2$ και $g(x) = x^2 - 1$. Βρείτε $h(x) \in \mathbb{Q}[x]$ τέτοιο ώστε $I = \langle h(x) \rangle$.

Λύση. Εφαρμόζουμε τον αλγόριθμο του Ευκλείδη:

$$x^3 + x - 2 = x\,(x^2 - 1) + (2x - 2),$$

$$x^2 - 1 = (\frac{1}{2}x + \frac{1}{2})(2x - 2) + 0.$$

Άρα ο μέγιστος κοινός διαιρέτης των $f(x)$ και $g(x)$ είναι το $h(x) = x - 1$. Από τη θεωρία, $I = \langle h(x) \rangle$.

Θέμα 5 (1 μονάδα).
(α) Δείξτε ότι ο δακτύλιος $\mathbb{R}[x]/\langle x^3 - x^2 + 3x - 3 \rangle$ είναι ισόμορφος με τον δακτύλιο $\mathbb{R} \times \mathbb{C}$.
(β) Βρείτε όλα τα ιδεώδη I του $\mathbb{R}[x]$ για τα οποία ισχύει $x^3 - x^2 + 3x - 3 \in I$.

(α) Έχουμε $x^3 - x^2 + 3x - 3 = (x - 1)(x^2 + 3)$. Έστω $I_1 = \langle x - 1 \rangle$ και $I_2 = \langle x^2 + 3 \rangle$. Επειδή ισχύει ότι $1 = \frac{1}{4}(x^2 + 3) - (\frac{1}{4}x + \frac{1}{4})(x - 1)$, έπεται ότι $I_1 + I_2 = \mathbb{R}[x]$, άρα $I_1 \cap I_2 = I_1 I_2 = \langle x^3 - x^2 + 3x - 3 \rangle$, από τη θεωρία. Χρησιμοποιώντας τη συνάρτηση εκτίμησης $\mathbb{R}[x] \to \mathbb{R}$ που δίνεται από τον τύπο $f(x) \mapsto f(1)$ και το πρώτο θεώρημα ισομορφισμού, εύκολα παίρνουμε ότι $\mathbb{R}[x]/I_1 \simeq \mathbb{R}$. Όμοια, χρησιμοποιώντας τη συνάρτηση εκτίμησης $\mathbb{R}[x] \to \mathbb{C}$ που δίνεται από τον τύπο $f(x) \mapsto f(\sqrt{-3})$ και το πρώτο θεώρημα ισομορφισμού, εύκολα παίρνουμε ότι $\mathbb{R}[x]/I_2 \simeq \mathbb{C}$. Μία εφαρμογή τώρα του κινέζικου θεωρήματος δίνει

$$\mathbb{R}[x]/\langle x^3 - x^2 + 3x - 3 \rangle \simeq (\mathbb{R}[x]/I_1) \times (\mathbb{R}[x]/I_2) \simeq \mathbb{R} \times \mathbb{C}.$$

(β) Έστω I τέτοιο ιδεώδες. Αφού ο $\mathbb{R}[x]$ είναι δακτύλιος κύριων ιδεωδών, υπάρχει $f(x) \in \mathbb{R}[x]$ τέτοιο ώστε $I = \langle f(x) \rangle$. Αφού $(x - 1)(x^2 + 3) \in I$, έπεται ότι το $f(x)$ διαιρεί το $(x - 1)(x^2 + 3)$. Λόγω μοναδικής παραγοντοποίησης στο $\mathbb{R}[x]$, έπεται ότι το I ισούται με ένα από τα εξής ιδεώδη του $\mathbb{R}[x]$:

$$\langle (x - 1)(x^2 + 3) \rangle = I_1 I_2,$$

$$\langle x - 1 \rangle = I_1,$$

$$\langle x^2 + 3 \rangle = I_2,$$

$$\langle 1 \rangle = \mathbb{R}[x].$$

Θέμα 6 (1 μονάδα).
(α) Είναι οι δακτύλιοι $\mathbb{Z}[i]$ και $\mathbb{Z}[\sqrt{-5}]$ ισόμορφοι;
(β) Είναι οι δακτύλιοι $\mathbb{R}[x]$ και $\mathbb{C}[x]$ ισόμορφοι;

Λύση.
(α) Δεν υπάρχει τέτοιος ισομορφισμός, διότι, όπως ξέρουμε, το $\mathbb{Z}[i]$ είναι περιοχή μοναδικής παραγοντοποίησης, ενώ το $\mathbb{Z}[\sqrt{-5}]$ δεν είναι.
(β) Έστω ότι υπήρχε ισομορφισμός $F : \mathbb{C}[x] \to \mathbb{R}[x]$. Αφού οι δακτύλιοι είναι μοναδιαίοι, έχουμε $F(1) = 1$, επομένως $0 = F(0) = F(1 + (-1)) = F(1) + F(-1)$, δηλαδή $F(-1) = -F(1) = -1$. Αν $g(x) \in \mathbb{R}[x]$ είναι η εικόνα του σταθερού πολυωνύμου $f(x) = i \in \mathbb{C}[x]$ μέσω της F, τότε θα ίσχυε $-1 = F(-1) =$

$F(i^2) = F(f(x)^2) = (F(f(x)))^2 = g(x)^2$, δηλαδή, λόγω βαθμού, το $g(x)$ είναι σταθερό πολυώνυμο στο $\mathbb{R}[x]$ του οποίου το τετράγωνο ισούται με -1, άτοπο, διότι $\pm i \notin \mathbb{R}$. Άρα δεν υπάρχει τέτοιος ισομορφισμός.

Θέμα 7 (2.5 μονάδες). Έστω $\mathbb{Z}_{85}$ η προσθετική ομάδα των ακεραίων modulo 85.
(α) Βρείτε όλες τις λύσεις της εξίσωσης $10x = 35$ στην $\mathbb{Z}_{85}$.
(β) Για πόσα $b \in \mathbb{Z}_{85}$ έχει η εξίσωση $10x = b$ λύση στην $\mathbb{Z}_{85}$;
(γ) Έστω G ομάδα και $f : G \to \mathbb{Z}_{85}$ επιμορφισμός. Δείξτε ότι υπάρχει κανονική υποομάδα της G με δείκτη 5 στην G.
(δ) Υπάρχει υποομάδα της S_{22} που να είναι ισόμορφη με την $\mathbb{Z}_{85}$;
(ε) Δείξτε ότι η $Aut(\mathbb{Z}_{85})$ δεν είναι κυκλική.

Λύση.
(α) Έχουμε $(10, 85) = 5$ και $5 \mid 35$. Επομένως, από τη θεωρία, υπάρχουν 5 λύσεις της εξίσωσης στο $\mathbb{Z}_{85}$. Μία λύση δίνεται από τη σχέση $2x \equiv 7 \pmod{17}$, η οποία δίνει $x \equiv 12 \pmod{17}$. Επομένως, όλες οι λύσεις της εξίσωσης $10x \equiv 35 \pmod{85}$ στο $\mathbb{Z}_{85}$ είναι οι $x = 12$, $x = 29$, $x = 46$, $x = 63$ και $x = 80$.
(β) Από τη θεωρία, η εξίσωση $10x \equiv b \pmod{85}$ έχει λύση αν και μόνο αν $5 \mid b$. Επομένως υπάρχουν 17 τιμές του b για τις οποίες η εξίσωση $10x = b$ έχει λύση στο $\mathbb{Z}_{85}$, δηλαδή $b \in \{0, 5, 10, 15, \ldots, 80\}$.
(γ) Έστω $K = Ker(f)$. Αφού η $\mathbb{Z}_{85}$ είναι κυκλική ομάδα, υπάρχει κανονική της υποομάδα με δείκτη 5 (συγκεκριμένα, η $\{0, 5, 10, \ldots, 80\}$). Αφού από το πρώτο θεώρημα ισομορφισμού ισχύει $G/K \simeq \mathbb{Z}_{85}$ έπεται ότι υπάρχει κανονική υποομάδα N της G/K με $[G/K : N] = 5$. Από το τέταρτο θεώρημα ισομορφισμού, έχουμε $N = H/K$ για κάποια κανονική υποομάδα H της G που περιέχει το K. Τέλος, από το τρίτο θεώρημα ισομορφισμού, παίρνουμε $[G : H] = [G/K : H/K] = [G/K : N] = 5$.
(δ) Έστω σ το εξής στοιχείο της S_{22}:

$$\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17)\ (18\ 19\ 20\ 21\ 22).$$

Αφού η σ είναι γινόμενο δύο ξένων κύκλων, δηλαδή ενός 17-κύκλου και ενός 5-κύκλου, η τάξη της ισούται με 85. άρα η κυκλική υποομάδα $H = \langle \sigma \rangle$ της S_{22} είναι ισόμορφη με την $\mathbb{Z}_{85}$.
(ε) Έχουμε $Aut(\mathbb{Z}_{85}) \simeq U(\mathbb{Z}_{85})$. Αρκεί επομένως να δείξουμε ότι η ομάδα $U(\mathbb{Z}_{85})$ δεν είναι κυκλική. Αφού αυτή η ομάδα έχει $\phi(85) = \phi(5)\phi(17) = 64$ στοιχεία, αρκεί να δείξουμε ότι δεν έχει στοιχείο τάξης 64. Αν $x \in \mathbb{Z}$ με $(x, 85) = 1$, τότε $(x, 5) = 1$ και $(x, 17) = 1$, άρα από το θεώρημα του Fermat παίρνουμε ότι $x^4 \equiv 1 \pmod 5$ και $x^{16} \equiv 1 \pmod{17}$, επομένως $x^{16} \equiv 1 \pmod 5$ και $x^{16} \equiv 1 \pmod{17}$, άρα $x^{16} \equiv 1 \pmod{85}$. Με άλλα λόγια, η τάξη κάθε στοιχείου της ομάδας $U(\mathbb{Z}_{85})$ διαιρεί το 16, επομένως δεν υπάρχει στοιχείο τάξης 64.

Θέμα 8 (0.5 μονάδα). Έστω F σώμα χαρακτηριστικής 2. Θεωρούμε το πολυώνυμο $f(x) = x^4 + x^2 + 1 \in F[x]$. Έστω ότι το F περιέχει μία ρίζα α του $f(x)$. Βρείτε μία παραγοντοποίηση του $f(x)$ σε γινόμενο ανάγωγων πολυωνύμων στο $F[x]$.

Λύση. Αφού η χαρακτηριστική του F ισούται με 2, έπεται ότι το πολυώνυμο $f'(x)$ είναι το μηδενικό πολυώνυμο. Επομένως, όλες οι ρίζες του $f(x)$ (σε οποιαδήποτε επέκταση του F τις περιέχει) θα είναι πολλαπλές. Παρατηρούμε τώρα ότι, λόγω χαρακτηριστικής, $f(x) = (x^2 + x + 1)^2$. Άρα το α είναι ρίζα του $x^2 + x + 1$, επομένως $(1 + \alpha)^2 + (1 + \alpha) + 1 = \alpha^2 + \alpha + 1 = 0$, δηλαδή το $1 + \alpha$ (που προφανώς ανήκει στο F και είναι διάφορο του α) είναι επίσης ρίζα του $f(x)$. Συνοψίζοντας τις παραπάνω παρατηρήσεις, έπεται ότι μία παραγοντοποίηση του $f(x)$ ως γινόμενο ανάγωγων πολυωνύμων στο $F[x]$ είναι η $f(x) = (x - \alpha)^2(x - (1 + \alpha))^2$.

Θέμα 9 (1 μονάδα). Έστω m, n θετικοί ακέραιοι με $m \geq 2$.
(α) Δείξτε ότι $(m, m^n - 1) = 1$.
(β) Δείξτε ότι $n \mid \phi(m^n - 1)$.

Λύση.
(α) Αν για τον θετικό ακέραιο d ισχύει ότι $d \mid m$ και $d \mid m^n - 1$, τότε $d \mid m^n$ και $d \mid m^n - 1$, άρα $d \mid m^n - (m^n - 1)$, άρα $d = 1$.
(β) Έστω R ο δακτύλιος των ακεραίων modulo $(m^n - 1)$. Λόγω του (α), η κλάση του m είναι αντιστρέψιμο στοιχείο του R, άρα, από το θεώρημα Lagrange, η τάξη του στοιχείου m της πολλαπλασιαστικής ομάδας $U(R)$ διαιρεί την τάξη αυτής της ομάδας που ισούται με $\phi(m^n - 1)$. Όμως, για θετικό ακέραιο k η σχέση $m^k = 1$ στο $U(R)$ σημαίνει ότι $m^n - 1 \mid m^k - 1$, άρα $k \geq n$. Επειδή προφανώς ισχύει ότι $m^n = 1$ στο $U(R)$, έπεται ότι η τάξη του m στο $U(R)$ ισούται με n, επομένως $n \mid \phi(m^n - 1)$.

Θέμα 10 (0.5 μονάδα). Έστω $f(x)$, $g(x) \in \mathbb{Q}[x]$ τέτοια ώστε $f(x)g(x) \in \mathbb{Z}[x]$. Δείξτε ότι το γινόμενο οποιουδήποτε συντελεστή του πολυωνύμου $f(x)$ με οποιονδήποτε συντελεστή του πολυωνύμου $g(x)$ ανήκει στο $\mathbb{Z}$.

Λύση. Ο ισχυρισμός είναι προφανής αν κάποιο από τα $f(x)$, $g(x)$ είναι το μηδενικό πολυώνυμο. Έστω λοπόν ότι $f(x), g(x) \neq 0$. Μπορούμε να γράψουμε

$$f(x) = \frac{a}{b}\, f_1(x), \qquad g(x) = \frac{c}{d}\, g_1(x),$$

όπου a, b, c, $d \in \mathbb{Z}$, b, $d \neq 0$ και $f_1(x)$, $g_1(x) \in \mathbb{Z}[x]$ πρωταρχικά πολυώνυμα. Επίσης, αφού ισχύει ότι $f(x)g(x) \in \mathbb{Z}[x] \setminus \{0\}$, μπορούμε να γράψουμε

$$f(x)g(x) = e\, h(x),$$

όπου $e \in \mathbb{Z}$ και $h(x) \in \mathbb{Z}[x]$ πρωταρχικό πολυώνυμο. Επομένως,

$$ebd\, h(x) = ac\, f_1(x)g_1(x).$$

Από το λήμμα του Gauss, το $f_1(x)g_1(x)$ είναι επίσης πρωταρχικό, άρα $bd \mid ac$ στο $\mathbb{Z}$, δηλαδή $\frac{ac}{bd} \in \mathbb{Z}$. Το ζητούμενο επομένως προκύπτει από το γεγονός ότι κάθε συντελεστής του $f(x)$ είναι της μορφής $\frac{a}{b}\, r$, με $r \in \mathbb{Z}$ και κάθε συντελεστής του $g(x)$ είναι της μορφής $\frac{c}{d}\, s$, με $s \in \mathbb{Z}$.