ΑΛΓΕΒΡΑ ΙΙ

Εξέταση Χειμερινού Εξαμήνου 2014-2015

Θέμα 1 (2 μονάδες). Δίνεται ανάγωγο πολυώνυμο $f(x) \in \mathbb{Q}[x]$ με $\deg(f) = 3$. Έστω a, b, c οι μιγαδικές ρίζες του $f(x)$. Θέτουμε $K = \mathbb{Q}(a, b, c)$.
(α) Δείξτε ότι για κάθε m, $n \in \mathbb{N}$ ισχύει ότι

$$a^m b^n + b^m a^n + a^m c^n + c^m a^n + b^m c^n + c^m b^n \ \in \ \mathbb{Q}.$$

(β) Έστω ότι η ομάδα $\mathrm{Gal}(K/\mathbb{Q})$ δεν είναι ισόμορφη με την S_3. Δείξτε ότι δεν υπάρχουν κατασκευάσιμα στοιχεία στο $K \setminus \mathbb{Q}$.

Λύση.
(α) Η δοσμένη παράσταση είναι συμμετρική ως προς a, b, c. Άρα, από γνωστό θεώρημα, ισούται με μια πολυωνυμική παράσταση (με συντελεστές στο $\mathbb{Q}$) των στοιχειωδών συμμετρικών πολυωνύμων στα a, b, c. Το ζητούμενο προκύπτει συνδυάζοντας τους τύπους του Viéte με το γεγονός ότι οι συντελεστές του $f(x)$ είναι ρητοί αριθμοί.
(β) Αφού $[\mathbb{Q}(a) : \mathbb{Q}] = 3$ και $\mathbb{Q}(a) \subseteq K$, έπεται ότι το $[K : \mathbb{Q}]$ διαιρείται με το 3. Από την άλλη, $[K : \mathbb{Q}] < 6$, διότι το K είναι σώμα ριζών ενός ανάγωγου τριτοβάθμιου πολυωνύμου επί του $\mathbb{Q}$ και η αντίστοιχη ομάδα Galois δεν είναι ισόμορφη με την S_3. Επομένως $[K : \mathbb{Q}] = 3$. Αν κάποιο $a \in K \setminus \mathbb{Q}$ ήταν κατασκευάσιμο, τότε ο βαθμός του a θα ήταν μη τετριμμένη δύναμη του 2 και ταυτόχρονα διαιρέτης του 3, άτοπο.

Θέμα 2 (3 μονάδες). Έστω p, q διαφορετικοί πρώτοι.
(α) Δείξτε ότι κάθε ομάδα τάξης $p^2 q$ είναι επιλύσιμη.
(β) Έστω $f(x) \in \mathbb{Q}[x]$ πολυώνυμο με ομάδα Galois τάξης $p^2 q$. Δείξτε ότι, για κάθε $m \in \mathbb{N} \setminus \{0\}$, το πολυώνυμο $g(x) = f(x^m)$ είναι επιλύσιμο με ριζικά επί του $\mathbb{Q}$.
(γ) Ταξινομείστε όλες τις αβελιανές ομάδες τάξης $p^2 q$ ως προς ισομορφισμό.

Λύση.
(α) Έστω G ομάδα τάξης $p^2 q$. Έστω H μια Sylow p-υποομάδα και K μια Sylow q-υποομάδα της G. Αν η H είναι κανονική στην G, τότε η G/H είναι επιλύσιμη (ως ομάδα τάξης q) και η H είναι επιλύσιμη (ως ομάδα τάξης p^2). Από γνωστό θεώρημα, η G είναι επίσης επιλύσιμη. Αν η K είναι κανονική στην G, τότε η G/K είναι επιλύσιμη (ως ομάδα τάξης p^2) και η K είναι επιλύσιμη (ως ομάδα τάξης q). Επομένως και πάλι η G είναι επιλύσιμη. Έστω λοιπόν ότι ούτε η H ούτε η K είναι κανονικές στην G. Το πλήθος των Sylow p-υποομάδων της G είναι $1 \pmod p$ και διαιρεί το q. Αφού δεν ισούται με 1, θα ισούται με q, άρα $q > p$. Επίσης, το πλήθος των Sylow q-υποομάδων της G είναι $1 \pmod q$ και διαιρεί το p^2. Αφού δεν ισούται με 1 και δεν ισούται με p (διότι είναι μεγαλύτερο του q που είναι μεγαλύτερο του p), έπεται ότι πρέπει να ισούται με p^2. Αφού η τομή δύο διαφορετικών Sylow q-υποομάδων της G είναι τετριμμένη, έπεται ότι υπάρχουν ακριβώς $p^2(q-1)$ στοιχεία τάξης q στην G. Επομένως, απομένουν $p^2 q - p^2(q-1) = p^2$ στοιχεία της G τάξης $\neq q$. Τα στοιχεία της H αριθμούν ήδη p^2 τέτοια στοιχεία. Αυτό σημαίνει πως δεν μπορεί να υπάρχει άλλη Sylow p-υποομάδα της G, άτοπο.
(β) Οι ρίζες του $g(x)$ είναι m-οστές ρίζες των ριζών του $f(x)$. Αν K είναι μια ριζική επέκταση του $\mathbb{Q}$ που περιέχει ένα σώμα ριζών του $f(x)$, τότε, επισυνάπτοντας στο K πρώτα μια πρωταρχική m-οστή

ρίζα του 1 και κατόπιν διαδοχικά m-οστές ρίζες των ριζών του $f(x)$, βρίσκουμε μια ριζική επέκταση του $\mathbb{Q}$ που περιέχει ένα σώμα ριζών του $g(x)$, άρα το $g(x)$ είναι επιλύσιμο με ριζικά επί του $\mathbb{Q}$.
(γ) Έστω $G = \mathbb{Z}/p\mathbb{Z}$, $H = \mathbb{Z}/p^2\mathbb{Z}$ και $K = \mathbb{Z}/q\mathbb{Z}$. Με απλή εφαρμογή του θεωρήματος ταξινόμησης των πεπερασμένων αβελιανών ομάδων, βλέπουμε ότι υπάρχουν δύο κλάσεις ισομορφίας, η κλάση της $G \times G \times K$ και η κλάση της $H \times K$.

Θέμα 3 (1 μονάδα). Βρείτε βάση του $\mathbb{Q}(e^{\frac{2\pi i}{9}})$ ως διανυσματικού χώρου επί του $\mathbb{Q}$.

Λύση. Έστω $\zeta = e^{\frac{2\pi i}{9}}$. Το ελάχιστο πολυώνυμο του ζ επί του $\mathbb{Q}$ είναι κυκλοτομικό με βαθμό $\phi(9) = 6$. Επομένως, τα στοιχεια 1, ζ, ζ^2, ζ^3, ζ^4, ζ^5 αποτελούν βάση του $\mathbb{Q}$-διανυσματικού χώρου $\mathbb{Q}(e^{\frac{2\pi i}{9}})$.

Θέμα 4 (2 μονάδες). Έστω K σώμα ριζών του πολυωνύμου $x^5 - 2$ επί του $\mathbb{Q}$.
(α) Δείξτε ότι η ομάδα $\mathrm{Gal}(K/\mathbb{Q})$ έχει τάξη 20.
(β) Δείξτε ότι η $\mathrm{Gal}(K/\mathbb{Q})$ είναι ισόμορφη με την ομάδα Frobenius F_{20}, δηλαδή την υποομάδα της S_5 που παράγεται από τον 5-κύκλο $(1\ 2\ 3\ 4\ 5)$ και τον 4-κύκλο $(2\ 3\ 5\ 4)$.

Λύση.
(α) Έστω $\zeta = e^{\frac{2\pi i}{5}}$ και $a = \sqrt[5]{2}$. Προφανώς, $K = \mathbb{Q}(\zeta, a)$. Το $x^5 - 2$ είναι πολυώνυμο Eisenstein, άρα ανάγωγο επί του $\mathbb{Q}$. Επομένως, $[\mathbb{Q}(a) : \mathbb{Q}] = 5$. Επίσης, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(5) = 4$. Αφού ξέρουμε ότι $\mathbb{Q}(a), \mathbb{Q}(\zeta) \subseteq K$, έχουμε ότι το $[K : \mathbb{Q}]$ διαιρείται και με το 5 και με το 4, άρα διαιρείται με το 20. Από την άλλη,

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\zeta)]\ [\mathbb{Q}(\zeta) : \mathbb{Q}] = 4\ [K : \mathbb{Q}(\zeta)] = 4\ [(\mathbb{Q}(\zeta))(a) : \mathbb{Q}(\zeta)].$$

Όμως το a είναι ρίζα του πολυωνύμου $x^5 - 2 \in \mathbb{Q}(\zeta)[x]$, άρα $[(\mathbb{Q}(\zeta))(a) : \mathbb{Q}(\zeta)] \leq 5$, κάτι που συνεπάγεται ότι $[K : \mathbb{Q}] \leq 20$. Αυτό αποδεικνύει το ζητούμενο.
(β) Έστω $a_i = \zeta^{i-1}a$, για $i \in \{1, \ldots, 5\}$. Κάθε στοιχείο σ της ομάδας $\mathrm{Galois}(K/\mathbb{Q})$ καθορίζεται πλήρως από τη δράση του στα a και ζ. Επειδή $\sigma(a) = a_i$, για κάποιο $1 \leq i \leq 5$, και $\sigma(\zeta) = \zeta^j$, για κάποιο $1 \leq j \leq 4$, υπάρχουν το πολύ $5 \cdot 4 = 20$ πιθανές επιλογές για το σ. Από την άλλη, η ομάδα $\mathrm{Gal}(K/\mathbb{Q})$ έχει 20 στοιχεία, διότι η επέκταση $K/\mathbb{Q}$ είναι Galois. Άρα όλες οι πιθανές επιλογές για το σ πραγματοποιούνται. Έστω τώρα σ και τ τα στοιχεία της ομάδας Galois που ορίζονται από $\sigma(a) = a_2$, $\sigma(\zeta) = \zeta$ και $\tau(a) = a$, $\tau(\zeta) = \zeta^2$, αντίστοιχα. Ταυτίζοντας το σύνολο $\{a_1, \ldots, a_5\}$ με το $\{1, \ldots, 5\}$ και τα στοιχεία της ομάδας Galois με τις αντίστοιχες μεταθέσεις στην S_5, βλέπουμε εύκολα ότι $\sigma = (1\ 2\ 3\ 4\ 5)$ και $\tau = (2\ 3\ 5\ 4)$. Επίσης, $\tau\sigma = \sigma^2\tau$, άρα η $\langle\tau\rangle$ είναι υποομάδα του κανονικοποιητή της $\langle\sigma\rangle$ στην S_5, άρα το σύνολο $\langle\sigma, \tau\rangle = \{\sigma^i\tau^j : 1 \leq i \leq 5,\ 1 \leq j \leq 4\} = \langle\sigma\rangle\langle\tau\rangle$ είναι υποομάδα της S_5 και έχει 20 στοιχεία, διότι $\langle\sigma\rangle \cap \langle\tau\rangle = \{1\}$. Μ' άλλα λόγια, η $\mathrm{Gal}(K/\mathbb{Q})$ είναι ισόμορφη με την F_{20}.

Θέμα 5 (1 μονάδα). Έστω p πρώτος. Ένας περιστρεφόμενος τροχός είναι χωρισμένος σε p κυκλικούς τομείς. Καθε κυκλικός τομέας επιτρέπεται να χρωματιστεί με ένα από k διαφορετικά χρώματα. Δείξτε ότι υπάρχουν συνολικά

$$\frac{k^p + (p-1)k}{p}$$

επιτρεπτοί χρωματισμοί (δύο χρωματισμοί θεωρούνται ίδιοι αν ο ένας προκύπτει από τον άλλο με περιστροφή του τροχού).

Λύση. Θεωρούμε το σύνολο $A = \{(a_1, a_2, \ldots, a_p) : a_1, a_2, \ldots, a_p \in \{1, 2, \ldots, k\}\}$. Η κυκλική υποομάδα $G = \langle (1\ 2\ \ldots\ p) \rangle$ της S_p δρα με τον συνήθη τρόπο στο A. Το πρόβλημα που δίνεται είναι προφανώς ισοδύναμο με τον υπολογισμό του πλήθους των τροχιών αυτής της δράσης. Εφαρμόζουμε το Λήμμα Cauchy-Frobenius-Burnside: Έστω $g \in G$. Αν $g = 1$, τότε το πλήθος των στοιχείων του A τα οποία αφήνει αναλλοίωτα το g ισούται με το $|A| = k^p$. Αν $g \neq 1$, τότε, αφού p πρώτος, το g είναι p-κύκλος, άρα τα μόνα στοιχεία του A που αφήνει το g αναλλοίωτα είναι τα στοιχεία της μορφής $(a, a, \ldots, a)$, όπου $a \in \{1, 2, \ldots, k\}$. Επομένως υπάρχουν k τέτοια στοιχεία του A για κάθε $g \neq 1$. Συμπεραίνουμε ότι το πλήθος των τροχιών της δράσης ισούται με

$$\frac{1}{|G|}\left(k^p + \sum_{g \in G \setminus \{1\}} k\right) = \frac{k^p + (p-1)k}{p}.$$

Θέμα 6 (1 μονάδα). Έστω n θετικός ακέραιος και F σώμα χαρακτηριστικής 0 που περιέχει μια πρωταρχική n-οστή ρίζα της μονάδας. Δίνεται ανάγωγο πολυώνυμο $f(x) = x^n - b \in F[x]$. Έστω K σώμα ριζών του $f(x)$ επί του F. Δείξτε ότι κάθε σώμα E με $F \subseteq E \subseteq K$ έχει τη μορφή $E = F(\sqrt[n]{b^d})$, όπου d κάποιος διαιρέτης του n.

Λύση. Έστω $a \in K$ μια ρίζα του $f(x)$. Το a είναι n-οστή ρίζα του b. Αφού το F περιέχει πρωταρχική n-οστή ρίζα του 1, έπεται ότι $K = F(a)$ και $[K : F] = n$, διότι το $f(x)$ είναι ανάγωγο στο $F[x]$. Απο γνωστή πρόταση, η ομάδα $\mathrm{Gal}(K/F)$ είναι κυκλική τάξης n, επομένως, για κάθε διαιρέτη d του n, υπάρχει μοναδική υποομάδα τάξης d. Άρα, από το Θεμελιώδες Θεώρημα της Θεωρίας Galois, τα ενδιάμεσα υποσώματα E (μεταξύ F και K) είναι σε 1-1 και επί αντιστοιχία με τους διαιρέτες του n. Έστω $E_d = F(a^d)$. Το a είναι ρίζα του πολυωνύμου $x^d - a^d \in E_d[x]$. Άρα $[K : E_d] \leq d$. Αφού $a^n \in F$, έχουμε $(a^d)^{\frac{n}{d}} \in F$. Επομένως $[E_d : F] \leq \frac{n}{d}$. Αφού όμως

$$n = [K : F] = [K : E_d]\ [E_d : F] \leq d\ \frac{n}{d} = n$$

πρέπει απαραίτητα να ισχύει $[K : E_d] = d$. Αυτό ισχύει για κάθε διαιρέτη d του n. Λόγω μοναδικότητας, τα $E_d = F(\sqrt[n]{b^d})$ είναι τα μόνα ενδιάμεσα υποσώματα μεταξύ F και K.