ΘΕΩΡΙΑ GALOIS

Εαρινό Εξάμηνο 2011
Ασκήσεις #1

Για τις Ασκήσεις 3 και 4 μπορείτε να χρησιμοποιήσετε την επόμενη πρόταση (Πόρισμα 2.2.13 στο βιβλίο του Ανδρεαδάκη).

Πρόταση 1 *Έστω $f(x) \in \mathbb{Z}[x]$. Το πολυώνυμο $f(x)$ είναι ανάγωγο στο δακτύλιο $\mathbb{Z}[x]$ εάν και μόνο αν το $f(x)$ είναι ανάγωγο στο δακτύλιο $\mathbb{Q}[x]$.*

1. Έστω σώμα F. Βρείτε όλα τα τοιχεία $a \in F$ για τα οποία ισχύει $a = a^{-1}$.

2. Έστω α η πραγματική τρίτη ρίζα του 2. Δείξτε ότι ο $\sqrt{\alpha^2 + 1}$ είναι αλγεβρικός αριθμός επί του $\mathbb{Q}$.

3. Δίνεται το πολυώνυμο $f(x) = x^4 + 1 \in \mathbb{Q}[x]$.

(α) Δείξτε ότι το $f(x)$ είναι ανάγωγο στο δακτύλιο $\mathbb{Q}[x]$.

(β) Συνάγετε ότι το ανάγωγο πολυώνυμο του $\alpha = \frac{1}{\sqrt{2}}(1 + i) \in \mathbb{C}$ επί του $\mathbb{Q}$ είναι το $f(x)$.

4. Έστω $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{C}$. Υπολογίστε (με απόδειξη) το ανάγωγο πολυώνυμο του α επί των σωμάτων:

(α) $\mathbb{Q}$ (β) $\mathbb{Q}(\sqrt{3})$.

5. Έστω α μια μιγαδική ρίζα του ανάγωγου πολυωνύμου $f(x) = x^3 + x + 1$ επί του $\mathbb{Q}$. Υπολογίστε το αντίστροφο του $\beta = 1 + \alpha$ στο σώμα $\mathbb{Q}(\alpha)$ στη μορφή $\beta^{-1} = r + s\alpha + t\alpha^2$ με $r, s, t \in \mathbb{Q}$.

6. Έστω α η πραγματική τρίτη ρίζα του 2, $\zeta = e^{2\pi i/3}$ και $\beta = \zeta\alpha$. Δείξτε ότι το -1 δεν μπορεί να γραφεί ως άθροισμα πεπερασμένου πλήθους τετραγώνων στο σώμα $\mathbb{Q}(\beta)$.

Έως Δευτέρα, 14 Μαρτίου

ΘΕΩΡΙΑ GALOIS

Εαρινό Εξάμηνο 2011
Ασκήσεις #2

Για τις Ασκήσεις 7 και 9 μπορείτε να χρησιμοποιήσετε την επόμενη πρόταση (Θεώρημα 2.2.15 στο βιβλίο του Ανδρεαδάκη), γνωστή ως κριτήριο του Eisenstein.

Πρόταση 2 *Δίνεται πολυώνυμο* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ *και πρώτος αριθμός* p. *Αν ο* p *δε διαιρεί τον* a_n *αλλά διαιρεί τους συντελεστές* $a_{n-1}, \ldots, a_0$ *του* $f(x)$ *και ο* p^2 *δεν διαιρεί τον* a_0, *τότε το* $f(x)$ *είναι ανάγωγο στους δακτυλίους* $\mathbb{Z}[x]$ *και* $\mathbb{Q}[x]$.

7. Έστω $f(x) = x^6 + x^3 + 1$.

(α) Δείξτε ότι το πολυώνυμο $g(x) \in \mathbb{Q}[x]$ με $g(x) = f(x+1)$ είναι ανάγωγο στο δακτύλιο $\mathbb{Q}[x]$.

(β) Συνάγετε ότι το $f(x)$ είναι ανάγωγο στο δακτύλιο $\mathbb{Q}[x]$.

8. Έστω $\alpha \in \mathbb{C}$ αλγεβρικός αριθμός επί του $\mathbb{Q}$. Να εξετάσετε αν $i \in \mathbb{Q}(\alpha)$ στις εξής περιπτώσεις:

(α) $\alpha^2 - 2\alpha + 2 = 0$, (β) $\alpha^3 + \alpha + 1 = 0$.

9. Βρείτε το βαθμό της επέκτασης $F \subseteq K$ στις παρακάτω περιπτώσεις και περιγράψτε μια βάση του F-διανυσματικού χώρου K:

(α) $\mathbb{Q} \subseteq \mathbb{Q}(2+\sqrt{5})$, (β) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{1+\sqrt{3}})$.

10. Έστω $F \subseteq K$ επέκταση σωμάτων και στοιχείο $\alpha \in K$ με $[F(\alpha) : F] = 5$. Δείξτε ότι $F(\alpha^2) = F(\alpha)$.

11. Έστω $F \subseteq K$ επέκταση σωμάτων και $\alpha, \beta \in K$. Αν τα $\alpha+\beta$ και $\alpha\beta$ είναι αλγεβρικά στοιχεία επί του F, δείξτε ότι τα α και β είναι επίσης αλγεβρικά στοιχεία επί του F.

12. Έστω $\zeta = \cos(\frac{2\pi}{9}) + i\sin(\frac{2\pi}{9})$, οπότε $\zeta^9 = 1$, και $f(x) = x^6 + x^3 + 1$.

(α) Δείξτε ότι το ζ είναι ρίζα του $f(x)$.

(β) Συμπεράνετε από το (α) και την Άσκηση 7 ότι το κανονικό εννιάγωνο δεν μπορεί να κατασκευαστεί με κανόνα και διαβήτη.

Έως Δευτέρα, 28 Μαρτίου

ΘΕΩΡΙΑ GALOIS

Εαρινό Εξάμηνο 2011
Ασκήσεις #3

13. Δίνονται τα σώματα $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ και $F = \mathbb{Q}(\sqrt{6}) \subseteq K$. Υπολογίστε το βαθμό της επέκτασης $F \subseteq K$ και περιγράψτε μια βάση του F-διανυσματικού χώρου K.

14. Δίνεται ισόπλευρο τρίγωνο T με πλευρά μήκους 1. Να εξετάσετε αν μπορεί να κατασκευαστεί με κανόνα και διαβήτη τετράγωνο με εμβαδό ίσο με το εμβαδό του T.

15. Δίνονται οι μιγαδικοί αριθμοί $\zeta = \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3})$, $\eta = \cos(\frac{2\pi}{5}) + i\sin(\frac{2\pi}{5})$ και $\theta = \cos(\frac{2\pi}{7}) + i\sin(\frac{2\pi}{7})$. Να εξετάσετε αν:

(α) $\eta \in \mathbb{Q}(\theta)$, (β) $\theta \in \mathbb{Q}(\zeta, \eta)$.

16. Βρείτε ικανή και αναγκαία συνθήκη για το σώμα F και τον πρώτο αριθμό p, έτσι ώστε το πολυώνυμο $x^p - x \in F[x]$ να έχει (μία τουλάχιστον) πολλαπλή ρίζα στο F.

17. Έστω K πεπερασμένο σώμα με q στοιχεία. Δείξτε ότι το γινόμενο των μη μηδενικών στοιχείων του K είναι ίσο με -1.

18. Αναλύστε σε γινόμενο ανάγωγων πολυωνύμων το πολυώνυμο $x^9 - x$ στο $\mathbb{F}_3[x]$. Δείξτε ότι οι παράγοντες που βρήκατε είναι πράγματι ανάγωγα πολυώνυμα στο $\mathbb{F}_3[x]$.

Έως Δευτέρα, 11 Απριλίου

ΘΕΩΡΙΑ GALOIS

Εαρινό Εξάμηνο 2011
Ασκήσεις #4

19. Έστω σώμα F χαρακτηριστικής μηδέν και μη σταθερά πολυώνυμα $f(x), g(x) \in F[x]$. Αν το $g(x)$ είναι ανάγωγο στο $F[x]$ και διαιρεί το $f(x)$ και την παράγωγο $f'(x)$, δείξτε ότι το $(g(x))^2$ διαιρεί το $f(x)$.

20. Έστω $\alpha_1, \alpha_2, \ldots, \alpha_n$ οι ρίζες ενός πολυωνύμου $f(x) \in F[x]$ βαθμού n σε μια επέκταση K του σώματος F. Βρείτε το ελάχιστο άνω φραγμα που μπορείτε για το βαθμό

$$[F(\alpha_1, \alpha_2, \ldots, \alpha_n) : F]$$

ως συνάρτηση του θετικού ακεραίου n.

21. Βρείτε όλες τις 17ες ρίζες του 5 στο σώμα $\mathbb{F}_{17}$, δηλαδή όλα τα στοιχεία $a \in \mathbb{F}_{17}$ με $a^{17} = 5$.

22. Έστω p πρώτος αριθμός. Χρησιμοποιώντας τα βασικά θεωρήματα για πεπερασμένα σώματα ή άλλο τρόπο, δείξτε ότι υπάρχουν ακριβώς

$$\binom{p}{2} = \frac{p(p-1)}{2}$$

μονικά ανάγωγα πολυώνυμα δευτέρου βαθμού στο $\mathbb{F}_p[x]$.

23. Ένα στοιχείο α σώματος F λεγέται *τέλειο τετράγωνο* αν $\alpha = \beta^2$ για κάποιο $\beta \in F$.

(α) Αν ο q είναι άρτιος θετικός ακέραιος, δείξτε ότι κάθε στοιχείο του σώματος $\mathbb{F}_q$ είναι τέλειο τετράγωνο.

(β) Αν ο q είναι περιττός, δείξτε ότι τα μισά ακριβώς μη μηδενικά στοιχεία του $\mathbb{F}_q$ είναι τέλεια τετράγωνα και ότι αν τα $\alpha, \beta \in \mathbb{F}_q$ δεν είναι τέλεια τετράγωνα, τότε το γινόμενό τους $\alpha\beta$ είναι τέλειο τετράγωνο.

24. Έστω V διανυσματικός χώρος διάστασης n πάνω στο πεπερασμένο σώμα $\mathbb{F}_q$ με q στοιχεία. Δείξτε ότι το πλήθος των διανυσματικών υπόχωρων του V διάστασης ένα είναι ίσο με $1 + q + q^2 + \cdots + q^{n-1}$.

Έως Δευτέρα, 9 Μαΐου

ΘΕΩΡΙΑ GALOIS

Εαρινό Εξάμηνο 2011
Ασκήσεις #5

25. Έστω $\zeta = e^{2\pi i/5}$ και $K = \mathbb{Q}(\zeta)$.

(α) Δείξτε ότι το K είναι σώμα διάσπασης για το πολυώνυμο $x^5 - 1$ επί του $\mathbb{Q}$ και υπολογίστε το βαθμό $[K : \mathbb{Q}]$.

(β) Δείξτε, χωρίς χρήση του αντίστοιχου θεωρήματος, ότι το K είναι επέκταση Galois του $\mathbb{Q}$ και υπολογίστε την ομάδα Galois $G(K/\mathbb{Q})$.

26. Υπολογίστε το βαθμό της επέκτασης $[K : \mathbb{Q}]$ και την ομάδα Galois $G(K/\mathbb{Q})$ για το σώμα διάσπασης K του πολυωνύμου $f(x)$ επί του $\mathbb{Q}$ όταν:

(α) $f(x) = x^4 + 1$, (β) $f(x) = x^4 + x^3 + 2x^2 + 3x + 1$.

27. Έστω α μια μη πραγματική ρίζα του πολυωνύμου $f(x) = x^3 + x + 1$ και K ένα σώμα διάσπασης του $f(x)$ επί του $\mathbb{Q}$.

(α) Βρείτε όλους τους αυτομορφισμούς του σώματος $\mathbb{Q}(\alpha)$.

(β) Ανήκει το $i\sqrt{3}$ στο σώμα $\mathbb{Q}(\alpha)$;

(γ) Ανήκει το $i\sqrt{3}$ στο σώμα K;

(δ) Έχει το πολυώνυμο $g(x) = x^3 + 2x + 1$ ρίζα στο K;

28. Έστω $K = \mathbb{Q}(\beta, \zeta)$, όπου $\beta = \sqrt[3]{2}$ και $\zeta = e^{2\pi i/3}$, και έστω $\gamma = \beta + c\,\zeta$.

(α) Είναι το σώμα K επέκταση Galois του $\mathbb{Q}$;

(β) Για ποιες τιμές του $c \in \mathbb{Q}$ ισχύει $K = \mathbb{Q}(\gamma)$;

(γ) Βρείτε την τροχιά του $\beta - \zeta$ ως προς τη δράση της ομάδας Galois $G(K/\mathbb{Q})$.

(δ) Υπολογίστε το ανάγωγο πολυώνυμο του $\beta - \zeta$ επί του $\mathbb{Q}$.

Έως Δευτέρα, 23 Μαΐου

ΘΕΩΡΙΑ GALOIS

Εαρινό Εξάμηνο 2011
Ασκήσεις #6

29. Έστω $\alpha = \sqrt[3]{2}$, $\zeta = e^{2\pi i/3}$ και $\beta = \alpha\zeta$.

(α) Δείξτε ότι για κάθε $c \in \mathbb{Q}$, το $\gamma = \alpha + c\beta$ είναι ρίζα ενός πολυωνύμου της μορφής $x^6 + ax^3 + b$, με $a, b \in \mathbb{Q}$.

(β) Δείξτε ότι ο βαθμός του $\alpha + \beta$ επί του $\mathbb{Q}$ είναι ίσος με 3 και υπολογίστε το ανάγωγο πολυώνυμο αυτού επί του $\mathbb{Q}$.

(γ) Δείξτε ότι ο βαθμός του $\alpha - \beta$ επί του $\mathbb{Q}$ είναι ίσος με 6 και υπολογίστε το ανάγωγο πολυώνυμο αυτού επί του $\mathbb{Q}$.

30. Εκφράστε την παράσταση $u_1^3 + u_2^3 + \cdots + u_n^3$ ως πολυώνυμο στις στοιχειώδεις συμμετρικές συναρτήσεις των $u_1, u_2, \ldots, u_n$.

31. Αποφανθείτε αν η ακόλουθη πρόταση είναι σωστή ή λάθος: Αν F είναι σώμα χαρακτηριστικής μηδέν και L/F και K/L είναι επεκτάσεις Galois, τότε η K/F είναι επίσης επέκταση Galois.

32. Έστω K επέκταση Galois σώματος F χαρακτηριστικής μηδέν της οποίας η ομάδα Galois $G(K/F)$ είναι η συμμετρική ομάδα S_4. Ποιοι ακέραιοι εμφανίζονται ως βαθμοί στοιχείων του K επί του F;

Έως Δευτέρα, 6 Ιουνίου

Υποδείξεις – Λύσεις

1. Έχουμε $a^{-1} = a \Leftrightarrow a^2 = 1 \Leftrightarrow a^2 - 1 = 0 \Leftrightarrow (a-1)(a+1) = 0$. Αφού το F είναι σώμα, οι λύσεις είναι οι $a = 1$ και $a = -1$. Παρατηρήστε ότι η λύση είναι μοναδική αν και μόνο αν η χαρακτηριστική του σώματος F είναι ίση με 2.

2. Θέτοντας $\beta = \sqrt{\alpha^2 + 1}$, έχουμε $\beta^2 = \alpha^2 + 1$ και συνεπώς $\beta^2 - 1 = \alpha^2$. Αφού $\alpha^3 = 2$, βρίσκουμε ότι $(\beta^2 - 1)^3 = 4$ και συνεπώς $\beta^6 - 3\beta^4 + 3\beta^2 - 5 = 0$, από όπου έπεται το ζητούμενο.

3. Για το (α), μπορούμε να δείξουμε ότι το πολυώνυμο $f(x) = x^4 + 1$ είναι ανάγωγο στο δακτύλιο $\mathbb{Z}[x]$ ως εξής. Ας υποθέσουμε αντιθέτως ότι $x^4 + 1 = p(x)q(x)$, όπου $p(x), q(x) \in \mathbb{Z}[x]$ είναι πολυώνυμα θετικού βαθμού. Παρατηρούμε ότι το $x^4 + 1$ δεν έχει ρητές (ούτε πραγματικές) ρίζες και συνεπώς κανένα από τα $p(x), q(x)$ δεν έχει βαθμό ίσο με 1. Άρα τα πολυώνυμα αυτά έχουν βαθμό 2, οπότε γράφοντας $p(x) = ax^2 + bx + c$ και $q(x) = dx^2 + ex + f$, έχουμε

$$x^4 + 1 \;=\; (ax^2 + bx + c)\,(dx^2 + ex + f)$$

με $a, b, c, d, e, f \in \mathbb{Z}$. Εξισώνοντας τους συντελεστές του x^4 και τους σταθερούς όρους στα δύο μέλη της προηγούμενης ισότητας βρίσκουμε ότι $ad = cf = 1$ και συνεπώς $a = d \in \{-1, 1\}$ και $c = f \in \{-1, 1\}$. Προφανώς, μπορούμε να υποθέσουμε ότι $a = d = 1$. Στην περίπτωση $c = f = 1$ έχουμε

$$x^4 + 1 \;=\; (x^2 + bx + 1)\,(x^2 + ex + 1).$$

Εξισώνοντας τους συντελεστές των x και x^2 στα δύο μέλη της προηγούμενης ισότητας βρίσκουμε ότι $b + e = be + 2 = 0$ από όπου προκύπτει ότι $b^2 = 2$, σε αντίθεση με την υπόθεση $b \in \mathbb{Z}$. Παρόμοια καταλήγουμε σε άτοπο στην περίπτωση και $c = f = -1$. Οδηγούμαστε λοιπόν στο συμπέρασμα ότι το $f(x)$ είναι ανάγωγο στο δακτύλιο $\mathbb{Z}[x]$, άρα και στον $\mathbb{Q}[x]$. Όπως έχουμε ήδη διαπιστώσει (Παράδειγμα 2.11), το (β) είναι άμεση συνέπεια του (α).

4. Όπως έχουμε ήδη διαπιστώσει (Παράδειγμα 2.11), το $\alpha = \sqrt{2} + \sqrt{3}$ είναι ρίζα του πολυωνύμου $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. Το ότι το $f(x)$ είναι ανάγωγο στο δακτύλιο $\mathbb{Z}[x]$, άρα και στον $\mathbb{Q}[x]$, προκύπτει με διαδικασία παρόμοια με αυτή στη λύση του Προβλήματος 3 (α). Συνεπώς το $f(x)$ είναι το ανάγωγο πολυώνυμο του α επί του $\mathbb{Q}$. Για το (β), υψώνοντας στο τετράγωνο την ισότητα $\alpha - \sqrt{3} = \sqrt{2}$ προκύπτει ότι $\alpha^2 - 2\sqrt{3}\,\alpha + 1 = 0$, δηλαδή ότι το α είναι ρίζα του πολυωνύμου $g(x) = x^2 - 2\sqrt{3}\,x + 1 \in \mathbb{Q}(\sqrt{3})[x]$. Αφού το α δεν ανήκει στο $\mathbb{Q}(\sqrt{3})$ (εξηγήστε γιατί) και το $g(x)$ έχει βαθμό 2, συμπεραίνουμε ότι το $g(x)$ είναι το ανάγωγο πολυώνυμο του α επί του $\mathbb{Q}(\sqrt{3})$.

5. Έχουμε $\alpha = \beta - 1$. Συνεπώς η σχέση $\alpha^3 + \alpha + 1 = 0$ γράφεται $(\beta - 1)^3 + (\beta - 1) + 1 = 0$, δηλαδή $\beta^3 - 3\beta^2 + 4\beta - 1 = 0$. Γράφοντας την τελευταία ισότητα στη μορφή $\beta(\beta^2 - 3\beta + 4) = 1$, συμπεραίνουμε ότι $\beta^{-1} = \beta^2 - 3\beta + 4 = (\alpha + 1)^2 - 3(\alpha + 1) + 4 = \alpha^2 - \alpha + 2$.

6. Έχουμε $\alpha^3 = \beta^3 = 2$ και επομένως τα α και β είναι ρίζες του $f(x) = x^3 - 2$. Παρατηρούμε ότι το πολυώνυμο $f(x)$ είναι ανάγωγο στο δακτύλιο $\mathbb{Q}[x]$ (εξηγήστε γιατί). Από την Πρόταση 2.27 και τα παραπάνω προκύπτει ότι υπάρχει $\mathbb{Q}$-ισομορφισμός $\sigma : \mathbb{Q}(\beta) \to \mathbb{Q}(\alpha)$. Υποθέτουμε ότι υπάρχουν στοιχεία $x_1, x_2, \ldots, x_n \in \mathbb{Q}(\beta)$ τέτοια ώστε $x_1^2 + x_2^2 + \cdots x_n^2 = -1$. Εφαρμόζοντας τη σ σε αυτή την ισότητα, βρίσκουμε ότι

$$-1 \;=\; \sigma(-1) \;=\; \sigma(x_1^2 + x_2^2 + \cdots x_n^2) \;=\; \sigma(x_1)^2 + \sigma(x_2)^2 + \cdots + \sigma(x_n)^2.$$

Το τελευταίο είναι αδύνατο αφού τα $\sigma(x_i) \in \mathbb{Q}(\alpha)$ είναι πραγματικοί αριθμοί. Αυτή η αντίφαση αποδεικνύει το ζητούμενο.

7. Για το (α) υπολογίζουμε ότι $g(x) = x^6+6x^5+15x^4+21x^3+18x^2+9x+3$, οπότε το κριτήριο του Eisenstein εφαρμόζεται για $p = 3$. Για το (β), ας υποθέσουμε ότι το $f(x)$ δεν είναι ανάγωγο στο $\mathbb{Q}[x]$. Τότε έχουμε $f(x) = p(x)q(x)$ για κάποια πολυώνυμα θετικού βαθμού $p(x), q(x) \in \mathbb{Q}[x]$ και συνεπώς ισχύει $g(x) = f(x+1) = p(x+1)q(x+1)$ στο $\mathbb{Q}[x]$. Αφού τα πολυώνυμα $p(x+1)$ και $q(x+1) \in \mathbb{Q}[x]$ είναι επίσης θετικού βαθμού (εξηγήστε), συμπεραίνουμε ότι το $g(x)$ δεν είναι ανάγωγο στο $\mathbb{Q}[x]$, σε αντίθεση με το αποτέλεσμα του (α). Από την αντίφαση αυτή έπεται το ζητούμενο.

8. Στην πρώτη περίπτωση έχουμε $(\alpha-1)^2 = -1$, οπότε $\alpha - 1 = \pm i$ και $i = \pm(\alpha-1) \in \mathbb{Q}(\alpha)$. Στη δεύτερη περίπτωση έχουμε $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, αφού το πολυώνυμο x^3+x+1 είναι ανάγωγο επί του $\mathbb{Q}$ (εξηγήστε), ενώ ο βαθμός του i επί του $\mathbb{Q}$ είναι ίσος με 2. Από το Πόρισμα 3.10 προκύπτει ότι το i δεν ανήκει στο $\mathbb{Q}(\alpha)$.

9. Για το (α) παρατηρούμε ότι

$$\mathbb{Q}(2+\sqrt{5}) \;=\; \{r+s(2+\sqrt{5}) : r,s \in \mathbb{Q}\} \;=\; \{a+b\sqrt{5} : a,b \in \mathbb{Q}\} \;=\; \mathbb{Q}(\sqrt{5}).$$

Επομένως $[K : F] = [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$ και το ζεύγος $(1, \sqrt{5})$ είναι βάση του F-διανυσματικού χώρου K. Για το (β) θέτουμε $\alpha = (1+\sqrt{3})^{1/2}$ και βρίσκουμε ότι $(\alpha^2-1)^2 = 3$, δηλαδή ότι $\alpha^4 - 2\alpha^2 - 2 = 0$. Εφαρμόζοντας το κριτήριο του Eisenstein για $p = 2$ δείχνουμε ότι το πολυώνυμο $x^4 - 2x^2 - 2$ είναι ανάγωγο επί του $\mathbb{Q}$ και συμπεραίνουμε ότι ο α είναι αλγεβρικός αριθμός επί του $\mathbb{Q}$ βαθμού 4. Επομένως $[K : F] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ και η τετράδα $(1, \alpha, \alpha^2, \alpha^3)$ είναι βάση του F-διανυσματικού χώρου K.

10. Παρατηρούμε ότι $F(\alpha^2) \subseteq F(\alpha)$ και συνεπώς αρκεί να δείξουμε ότι τα σώματα $F(\alpha^2)$ και $F(\alpha)$ έχουν ίσες διαστάσεις ως F-διανυσματικοί χώροι, δηλαδή ότι $[F(\alpha^2) : F] = [F(\alpha) : F]$. Αφού $F \subseteq F(\alpha)$ είναι επέκταση βαθμού 5 και $\alpha^2 \in F(\alpha)$, το α^2 είναι αλγεβρικό στοιχείο επί του F βαθμού 1 ή 5. Ο βαθμός αυτός δεν μπορεί να είναι ίσος με 1, αφού τότε θα είχαμε $\alpha^2 \in F$ και συνεπώς ο βαθμός του α επί του F θα ήταν ίσος με 1 ή 2. Από τα παραπάνω προκύπτει ότι $[F(\alpha^2) : F] = [F(\alpha) : F] = 5$ και ότι $F(\alpha^2) = F(\alpha)$.

11. Θέτουμε $\gamma = \alpha+\beta$ και $\delta = \alpha\beta$ και παρατηρούμε ότι τα α, β είναι ρίζες του πολυωνύμου

$$(x-\alpha)(x-\beta) \;=\; x^2 - \gamma x + \delta \in L[x],$$

όπου $L := F(\gamma, \delta) \subseteq F(\alpha, \beta) \subseteq K$. Επομένως τα $\alpha, \beta \in K$ είναι αλγεβρικά στοιχεία (βαθμού το πολύ 2) επί του L. Θεωρούμε την αλυσίδα επεκτάσεων $F \subseteq L \subseteq F(\alpha, \beta)$. Αφού τα $\gamma, \delta \in L$ είναι αλγεβρικά στοιχεία επί του F, έχουμε

$$[L : F] \;=\; [F(\gamma,\delta) : F] \;=\; [F(\gamma,\delta) : F(\gamma)] \cdot [F(\gamma) : F] < \infty,$$

οπότε η επέκταση $F \subseteq L$ είναι πεπερασμένη. Ομοίως, αφού τα α, β είναι αλγεβρικά στοιχεία επί του L, η επέκταση $L \subseteq F(\alpha, \beta)$ είναι επίσης πεπερασμένη. Από τη μεταβατικότητα του βαθμού επέκτασης προκύπτει ότι και η επέκταση $F \subseteq F(\alpha, \beta)$ είναι πεπερασμένη και συνεπώς τα στοιχεία α, β του $F(\alpha, \beta)$ είναι αλγεβρικά επί του F. **Ερώτημα**: Ποιο είναι το μικρότερο άνω φράγμα για τους βαθμούς των α και β επί του F που μπορείτε να βρείτε, ως συνάρτηση εκείνων των γ και δ;

12. Παρατηρούμε ότι $x^9 - 1 = (x^3-1)f(x)$ και ότι το ζ είναι ρίζα του πολυωνύμου $x^9 - 1$ αλλά όχι του $x^3 - 1$. Άρα, το ζ είναι ρίζα του $f(x)$, δηλαδή ισχύει το (α). Από αυτό και την Άσκηση 7 προκύπτει ότι το ζ είναι αλγεβρικός αριθμός βαθμού 6 επί του $\mathbb{Q}$. Το ζητούμε στο (β) προκύπτει από την πρόταση αυτή όπως στο Παράδειγμα 4.15.

13. Γνωρίζουμε (Άσκηση 4) ότι $[K : \mathbb{Q}] = 4$ και ότι $[F : \mathbb{Q}] = [\mathbb{Q}(\sqrt{6}) : \mathbb{Q}] = 2$. Συνεπώς, από τη μεταβατικότητα $[K : \mathbb{Q}] = [K : F]\,[F : \mathbb{Q}]$ προκύπτει ότι $[K : F] = 2$. Το ζεύγος $(1, \alpha)$ είναι βάση του F-διανυσματικού χώρου K για κάθε $\alpha \in K \setminus F$, για παράδειγμα για $\alpha = \sqrt{2}$.

14. Προφανώς το T έχει εμβαδό $\sqrt{3}/4$ και συνεπώς ρωτάμε αν ο αριθμός $(\sqrt{3}/4)^{1/2} = \sqrt[4]{3}/2$ είναι κατασκευάσιμος. Πράγματι, ο $3 \in \mathbb{Q}$ είναι κατασκευάσιμος, άρα το ίδιο ισχύει για τους $\sqrt{3}$ και $\sqrt{\sqrt{3}} = \sqrt[4]{3}$, άρα και για τον $\sqrt[4]{3}/2$.

15. Γνωρίζουμε ότι τα ζ, η και θ είναι ρίζες των πολυωνύμων $1+x+x^2$, $1+x+x^2+x^3+x^4$ και $1+x+x^2+\cdots+x^6$, αντίστοιχα, και (από το Λήμμα 4.14) ότι τα πολυώνυμα αυτά είναι ανάγωγα επί του $\mathbb{Q}$. Συνεπώς τα ζ, η και θ έχουν βαθμό 2, 4 και 6, αντίστοιχα, επί του $\mathbb{Q}$. Αφού το η έχει βαθμό 4 επί του $\mathbb{Q}$ και το 4 δε διαιρεί το βαθμό $[\mathbb{Q}(\theta):\mathbb{Q}] = 6$, έχουμε $\eta \notin \mathbb{Q}(\theta)$. Επίσης έχουμε

$$[\mathbb{Q}(\zeta,\eta):\mathbb{Q}] \;=\; [\mathbb{Q}(\eta,\zeta):\mathbb{Q}(\eta)]\cdot[\mathbb{Q}(\eta):\mathbb{Q}] \;=\; 4\,[\mathbb{Q}(\eta,\zeta):\mathbb{Q}(\eta)] \;\in\; \{4,8\}.$$

Αφού το θ έχει βαθμό 6 επί του $\mathbb{Q}$ προκύπτει ότι $\theta \notin \mathbb{Q}(\zeta,\eta)$.

16. Θα δείξουμε ότι το $f(x) = x^p - x$ έχει πολλαπλή ρίζα στο F αν και μόνο αν η χαρακτηριστική του F διαιρεί το $p-1$. Πράγματι, έστω ότι το $\alpha \in F$ είναι πολλαπλή ρίζα του $f(x)$. Από το Λήμμα 5.10 προκύπτει ότι $f(\alpha) = \alpha^p - \alpha = 0$ και ότι $f'(\alpha) = p\alpha^{p-1} - 1 = 0$. Από τη δεύτερη ισότητα προκύπτει ότι $\alpha \neq 0$ και συνεπώς από την πρώτη ότι $\alpha^{p-1} = 1$. Άρα η δεύτερη ισότητα δίνει $p-1 = 0$, δηλαδή η χαρακτηριστική του F διαιρεί το $p-1$. Αντιστρόφως, αν ισχύει $p-1=0$ στο F, τότε $f(1) = 1^p - 1 = 0$ και $f'(1) = p-1 = 0$ και συνεπώς το $\alpha = 1$ είναι πολλαπλή ρίζα του $f(x)$.

17. Έστω ότι $\alpha_0 = 0$, $\alpha_1, \ldots, \alpha_{q-1}$ είναι τα στοιχεία του K. Γνωρίζουμε ότι ισχύει

$$x^q - x \;=\; (x-\alpha_0)(x-\alpha_1)\cdots(x-\alpha_{q-1}) \;=\; x(x-\alpha_1)\cdots(x-\alpha_{q-1})$$

στο $K[x]$. Απλοποιώντας το x από τα δύο ακραία μέλη της προηγούμενης ισότητας παίρνουμε $x^{q-1}-1 = (x-\alpha_1)\cdots(x-\alpha_{q-1})$. Θέτοντας $x=0$ (ή εξισώνοντας τους σταθερούς όρους) στην τελευταία ισότητα προκύπτει ότι $-1 = (-1)^{q-1}\alpha_1\cdots\alpha_{q-1} = \alpha_1\cdots\alpha_{q-1}$. Μια διαφορετική λύση είναι η εξής. Από την Άσκηση 1 γνωρίζουμε ότι τα μη μηδενικά στοιχεία α του K για τα οποία ισχύει $\alpha = \alpha^{-1}$ είναι τα $\alpha = 1$ και $\alpha = -1$ (που πιθανώς συμπίπτουν). Τα υπόλοιπα μη μηδενικά στοιχεία του K χωρίζονται σε ζεύγη στοιχείων της μορφής $\{\alpha, \alpha^{-1}\}$ με γινόμενο 1. Κατά συνέπεια, το γινόμενο όλων των μη μηδενικών στοιχείων του K είναι ίσο με -1.

18. Στο $\mathbb{Z}[x]$ έχουμε

$$\begin{aligned} x^9 - x \;&=\; x(x^8-1) \;=\; x(x^4-1)(x^4+1) \;=\; x(x^2-1)(x^2+1)(x^4+1) \\ &=\; x(x-1)(x+1)(x^2+1)(x^4+1). \end{aligned}$$

Στο $\mathbb{F}_3[x]$ ισχύει επιπλέον

$$x^4+1 \;=\; x^4 - 3x^2 + 1 \;=\; (x^2-1)^2 - x^2 \;=\; (x^2-x-1)(x^2+x-1)$$

και συνεπώς $x^9 - x = x(x-1)(x+1)(x^2+1)(x^2-x-1)(x^2+x-1)$. Οι τρεις παράγοντες βαθμού 2 είναι (όπως προβλέπει το μέρος (ε) του Θεωρήματος 6.2) ανάγωγα πολυώνυμα επί του $\mathbb{F}_3$ αφού (όπως προκύπτει με λίγες δοκιμές) δεν έχουν ρίζες στο σώμα αυτό.

19. Αφού το $g(x)$ διαιρεί το $f(x)$ στο $F[x]$, μπορούμε να γράψουμε $f(x) = g(x)h(x)$ για κάποιο πολυώνυμο $h(x) \in F[x]$. Έχουμε $f'(x) = g'(x)h(x) + g(x)h'(x)$ και συνεπώς, αφού το $g(x)$ διαιρεί το $f'(x)$, θα πρέπει να διαιρεί και το γινόμενο $g'(x)h(x)$. Από την υπόθεσή μας ότι το $g(x)$ είναι ανάγωγο και ότι το F έχει χαρακτηριστική μηδέν προκύπτει (όπως είδαμε στην απόδειξη της Πρότασης 5.13) ότι τα $g(x)$ και $g'(x)$ είναι πρώτα μεταξύ τους. Επομένως το $g(x)$ διαιρεί το $h(x)$, δηλαδή υπάρχει πολυώνυμο $q(x) \in F[x]$ με $h(x) = g(x)q(x)$. Έπεται ότι $f(x) = (g(x))^2 q(x)$ και συνεπώς το $(g(x))^2$ διαιρεί το $f(x)$ στο $F[x]$.

20. Θα δείξουμε ότι $[F(\alpha_1, \alpha_2, \ldots, \alpha_n) : F] \leq n!$ με επαγωγή στο n. Το ζητούμενο είναι φανερό για $n = 1$ (εξηγήστε). Έστω ότι $n \geq 2$. Θέτοντας $\alpha_n = \alpha$ και $F(\alpha_1, \ldots, \alpha_{n-1}) = F_1$ έχουμε $F(\alpha_1, \alpha_2, \ldots, \alpha_n) = F_1(\alpha)$ και συνεπώς ζητάμε να δείξουμε ότι $[F_1(\alpha) : F] \leq n!$. Προφανώς ο βαθμός του α επί του F είναι μικρότερος ή ίσος του βαθμού n του $f(x)$, δηλαδή $[F(\alpha) : F] \leq n$. Γράφοντας $f(x) = (x - \alpha)g(x)$, με

$$g(x) \;=\; (x - \alpha_1) \cdots (x - \alpha_{n-1}),$$

έχουμε $g(x) \in F(\alpha)[x]$, ως πηλίκο της διαίρεσης δύο πολυωνύμων του $F(\alpha)[x]$. Επομένως, από την υπόθεση της επαγωγής προκύπτει ότι

$$[F_1(\alpha) : F(\alpha)] \;=\; [F(\alpha)(\alpha_1, \ldots, \alpha_{n-1}) : F(\alpha)] \leq (n-1)!.$$

Συμπεραίνουμε ότι $[F_1(\alpha) : F] = [F_1(\alpha) : F(\alpha)] \cdot [F(\alpha) : F] \leq (n-1)! \cdot n = n!$.

21. Γνωρίζουμε ότι ισχύει $x^{17} = x$ για κάθε $x \in \mathbb{F}_{17}$. Επομένως το μοναδικό στοιχείο $a \in \mathbb{F}_{17}$ με $a^{17} = 5$ είναι το $a = 5$.

22. Έστω m το πλήθος των μονικών, ανάγωγων πολυωνύμων του $\mathbb{F}_p[x]$ δευτέρου βαθμού και έστω $q = p^2$. Γνωρίζουμε ότι το πολυώνυμο $x^q - x$ είναι ίσο με το γινόμενο των μονικών, ανάγωγων πολυωνύμων του $\mathbb{F}_p[x]$ πρώτου ή δευτέρου βαθμού. Προφανώς υπάρχουν ακριβώς p σε πλήθος μονικά, πρωτοβάθμια (αναγκαστικά ανάγωγα) πολυωνύμα στο $\mathbb{F}_p[x]$ (αυτά της μορφής $x - \alpha$ με $\alpha \in \mathbb{F}_p$). Αφού ο βαθμός του γινομένου τους είναι ίσος με p και εκείνος του γινομένου των μονικών, ανάγωγων πολυωνύμων του $\mathbb{F}_p[x]$ δευτέρου βαθμού είναι ίσος με $2m$, θα πρέπει ο βαθμός του $x^q - x$ να είναι ίσος με $p + 2m$. Συνεπώς $p^2 = q = p + 2m$, δηλαδή $m = p(p-1)/2$. Μια πιο στοιχειώδης λύση είναι η εξής: Υπάρχουν συνολικά p^2 μονικά πολυώνυμα δευτέρου βαθμού στο $\mathbb{F}_p[x]$ (αυτά είναι της μορφής $x^2 + ax + b$ με $a, b \in \mathbb{F}_p$). Τα μη ανάγωγα από αυτά είναι εκείνα της μορφής $(x - \alpha)(x - \beta)$ με $\alpha, \beta \in \mathbb{F}_p$. Υπάρχουν ακριβώς p τέτοια πολυώνυμα με $\alpha = \beta$ και ακριβώς $p(p-1)/2$ με $\alpha \neq \beta$. Συνεπώς το ζητούμενο πλήθος είναι ίσο με $p^2 - p - p(p-1)/2 = p(p-1)/2$.

23. Για το (α) παρατηρούμε ότι ισχύει $\alpha = \alpha^q$ για κάθε $\alpha \in \mathbb{F}_q$, οπότε $\alpha = (\alpha^{q/2})^2$ και συνεπώς το α είναι τέλειο τετράγωνο. Για το (β) υποθέτουμε ότι ο q είναι περιττός και υπενθυμίζουμε ότι υπάρχει $\gamma \in \mathbb{F}_q \setminus \{0\}$ τέτοιο ώστε $\mathbb{F}_q \setminus \{0\} = \{1, \gamma, \gamma^2, \ldots, \gamma^{q-2}\}$. Τα $(q-1)/2$ σε πλήθος στοιχεία $1, \gamma^2, \gamma^4, \ldots, \gamma^{q-3}$ είναι προφανώς τέλεια τετράγωνα. Θα δείξουμε ότι τα υπόλοιπα στοιχεία του $\mathbb{F}_q \setminus \{0\}$ δεν είναι. Πράγματι, έστω ότι $\gamma^k = \beta^2$ για κάποιο περιττό αριθμό k και κάποιο $\beta \in \mathbb{F}_q$. Προφανώς έχουμε $\beta \neq 0$ και συνεπώς μπορούμε να γράψουμε $\beta = \gamma^r$ για κάποιο $r \in \mathbb{Z}$, οπότε $\gamma^k = \gamma^{2r}$. Προκύπτει ότι $\gamma^{k-2r} = 1$ και επομένως ότι το $k - 2r$ διαιρείται από την τάξη του γ στην πολλαπλασιαστική ομάδα $\mathbb{F}_q \setminus \{0\}$, δηλαδή από το $q - 1$. Αυτό είναι αδύνατο αφού το $k - 2r$ είναι περιττός αριθμός και το $q - 1$ είναι άρτιος. Από την αντίφαση αυτή συμπεραίνουμε ότι τα $1, \gamma^2, \gamma^4, \ldots, \gamma^{q-3}$ είναι τα μόνα μη μηδενικά στοιχεία του $\mathbb{F}_q$ που είναι τέλεια τετράγωνα. Τέλος, αν τα $\alpha, \beta \in \mathbb{F}_q$ δεν είναι τέλεια τετράγωνα, τότε έχουμε $\alpha = \gamma^{2n+1}$ και $\beta = \gamma^{2m-1}$ για κάποια $n, m \in \mathbb{Z}$ και συνεπώς το γινόμενό τους $\alpha\beta = \gamma^{2n+2m} = (\gamma^{n+m})^2$ είναι τέλειο τετράγωνο στο $\mathbb{F}_q$.

24. Γνωρίζουμε ότι το πλήθος των στοιχείων του V είναι ίσο με q^n. Προφανώς ακριβώς $q^n - 1$ από αυτά τα στοιχεία είναι μη μηδενικά. Παρατηρούμε ότι κάθε τέτοιο στοιχείο $v \in V \setminus \{0\}$ ορίζει το μονοδιάστατο υπόχωρο $L_v = \{\lambda v : \lambda \in \mathbb{F}_q\}$ του V και ότι κάθε υπόχωρος διάστασης ένα του V είναι αυτής της μορφής. Επιπλέον, τα στοιχεία $u \in V \setminus \{0\}$ που ορίζουν τον ίδιο υπόχωρο με το v (δηλαδή με $L_u = L_v$) είναι ακριβώς τα $q - 1$ στοιχεία λv της L_v με $\lambda \in \mathbb{F}_q \setminus \{0\}$. Συμπεραίνουμε ότι το πλήθος των υπόχωρων διάστασης ένα του V είναι ίσο με $(q^n - 1)/(q - 1) = 1 + q + q^2 + \cdots + q^{n-1}$.

25. Η άσκηση αυτή είναι ειδική περίπτωση της Πρότασης 15.1 που στην παρούσα χρονική στιγμή έχουμε αποδείξει. Για παράδειγμα, έχουμε $x^5-1=(x-1)(x-\zeta)(x-\zeta^2)(x-\zeta^3)(x-\zeta^4)$ και συνεπώς το σώμα διάσπασης του x^5-1 επί του $\mathbb{Q}$ είναι το $\mathbb{Q}(\zeta,\zeta^2,\zeta^3,\zeta^4)=\mathbb{Q}(\zeta)=K$. Το ανάγωγο πολυώνυμο του ζ επί του $\mathbb{Q}$ είναι το

$$x^4+x^3+x^2+x+1 \;=\; (x-1)(x-\zeta)(x-\zeta^2)(x-\zeta^3)(x-\zeta^4)$$

(Λήμμα 4.14) και συνεπώς $[K:\mathbb{Q}]=4$. Η ομάδα Galois $G(K/\mathbb{Q})=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$ είναι κυκλική τάξης 4, όπου $\sigma_i\in G(K/\mathbb{Q})$ είναι ο μοναδικός αυτομορφισμός με $\sigma_i(\zeta)=\zeta^i$ για $i\in\{1,2,3,4\}$ (για τον υπολογισμό αυτό μας χρειάζεται μόνο η Πρόταση 2.27).

26. Για το (α), έχουμε

$$x^4+1 \;=\; (x^2-\mathrm{i})(x^2+\mathrm{i}) \;=\; (x-\frac{1+\mathrm{i}}{\sqrt{2}})\,(x+\frac{1+\mathrm{i}}{\sqrt{2}})\,(x-\frac{1-\mathrm{i}}{\sqrt{2}})\,(x+\frac{1-\mathrm{i}}{\sqrt{2}})$$

και συνεπώς το $K=\mathbb{Q}(\,(1+\mathrm{i})/\sqrt{2},\,(1-\mathrm{i})/\sqrt{2}\,)=\mathbb{Q}(\mathrm{i},\sqrt{2})$ είναι διτετραγωνική επέκταση του $\mathbb{Q}$, την ομάδα Galois της οποίας έχουμε υπολογίσει.

Για το (β), έχουμε $f(x)=(x+1)(x^3+2x+1)$ και συνεπώς το K είναι το σώμα διάσπασης του κυβικού πολυωνύμου $g(x)=x^3+2x+1$ επί του $\mathbb{Q}$. Παρατηρούμε ότι η $g(x)$ είναι γνησίως αύξουσα συνάρτηση της πραγματικής μεταβλητής x και ότι έχει μοναδική πραγματική ρίζα. Συνεπώς, σύμφωνα με τη θεωρία, $[K:\mathbb{Q}]=6$ και η ομάδα Galois $G(K/\mathbb{Q})$ είναι ισόμορφη με τη συμμετρική ομάδα S_3.

27. Παρατηρούμε ότι το πολυώνυμο $f(x)$ είναι ανάγωγο επί του $\mathbb{Q}$ και ότι έχει μοναδική πραγματική ρίζα. Συνεπώς, σύμφωνα με τη σχετική θεωρία, $[K:\mathbb{Q}]=6$ και το $\mathbb{Q}(\alpha)$ δεν περιέχει ρίζα του $f(x)$ διαφορετική από το α. Κατά συνέπεια, ο μόνος αυτομορφισμός του $\mathbb{Q}(\alpha)$ είναι ο ταυτοτικός (πράγματι, κάθε αυτομορφισμός σ του $\mathbb{Q}(\alpha)$ είναι $\mathbb{Q}$-αυτομορφισμός και απεικονίζει το α σε ρίζα του $f(x)$, οπότε θα πρέπει $\sigma(\alpha)=\alpha$). Τα ερωτήματα (β), (γ) και (δ) έχουν αρνητική απάντηση: Για το (β) αρκεί να παρατηρήσουμε ότι ο βαθμός του $i\sqrt{3}$ επί του $\mathbb{Q}$ είναι ίσος με 2, ο οποίος δε διαιρεί το $[\mathbb{Q}(\alpha):\mathbb{Q}]=3$. Για το (γ) υπολογίζουμε ότι το $f(x)$ έχει διακρίνουσα ίση με -31. Άρα, όπως γνωρίζουμε από τη σχετική θεωρία, το μόνο υπόσωμα L του K με $[L:\mathbb{Q}]=2$ είναι το $\mathbb{Q}(i\sqrt{31})$ και συνεπώς το K δεν μπορεί να περιέχει το $i\sqrt{3}$. Για το (δ) παρατηρούμε ότι το πολυώνυμο $g(x)$ είναι επίσης ανάγωγο επί του $\mathbb{Q}$ με μοναδική πραγματική ρίζα. Έστω ότι το $g(x)$ έχει ρίζα στο K. Τότε, σύμφωνα με την Πρόταση 11.12, το $g(x)$ έχει όλες τις ρίζες του στο K και συνεπώς το K είναι σώμα διάσπασης και για το $g(x)$. Όμως το $g(x)$ έχει διακρίνουσα ίση με -59 και συνεπώς έχουμε οδηγηθεί στο λανθασμένο συμπέρασμα ότι τα $\mathbb{Q}(i\sqrt{31})$ και $\mathbb{Q}(i\sqrt{59})$ είναι δύο διαφορετικά υποσώματα του K βαθμού 2 επί του $\mathbb{Q}$.

28. Το ερώτημα (α) έχει θετική απάντηση αφού K είναι το σώμα διάσπασης του πολυωνύμου $f(x)=x^3-2=(x-\beta)(x-\beta\zeta)(x-\beta\zeta^{-1})$ επί του $\mathbb{Q}$. Ένας υπολογισμός παρόμοιος με εκείνον του Παραδείγματος 11.2 δείχνει ότι το (β) ισχύει για όλες τις μη μηδενικές τιμές του $c\in\mathbb{Q}$. Αφού το $f(x)$ έχει μοναδική πραγματική ρίζα, έχουμε $[K:\mathbb{Q}]=6$ και η $G(K/\mathbb{Q})$ είναι ισόμορφη με τη συμμετρική ομάδα S_3. Επιπλέον, για κάθε $\sigma\in G(K/\mathbb{Q})$ έχουμε $\sigma(\beta)\in\{\beta,\beta\zeta,\beta\zeta^{-1}\}$ και $\sigma(\zeta)\in\{\zeta,\zeta^{-1}\}$ και συνεπώς η τροχιά του $\beta-\zeta$ υπολογίζεται ως το σύνολο

$$\{\beta-\zeta,\beta\zeta-\zeta,\beta\zeta^{-1}-\zeta,\beta-\zeta^{-1},\beta\zeta-\zeta^{-1},\beta\zeta^{-1}-\zeta^{-1}\}.$$

Σύμφωνα με την Πρόταση 11.5, το ανάγωγο πολυώνυμο του $\beta-\zeta$ επί του $\mathbb{Q}$ είναι ίσο με $(x-\beta+\zeta)(x-\beta\zeta+\zeta)(x-\beta\zeta^{-1}+\zeta)(x-\beta+\zeta^{-1})(x-\beta\zeta+\zeta^{-1})(x-\beta\zeta^{-1}+\zeta^{-1})=f(x+\zeta)f(x+\zeta^{-1})=x^6-3x^5+6x^4-11x^3+12x^2+3x+1$.

29. Για το (α) παρατηρούμε ότι $\gamma=\alpha+c\beta=\alpha(1+c\,\zeta)=\sqrt[3]{2}\,(1+c\,\zeta)$ και συνεπώς ότι $\gamma^3=2(1+c\,\zeta)^3\in\mathbb{Q}(\zeta)$. Αφού $[\mathbb{Q}(\zeta):\mathbb{Q}]=2$, συμπεραίνουμε ότι το γ^3 έχει βαθμό 1 ή 2 επί του $\mathbb{Q}$.

Άρα το γ^3 είναι ρίζα πολυωνύμου $x^2+ax+b \in \mathbb{Q}[x]$, οπότε το γ είναι ρίζα του x^6+ax^3+b, με $a,b \in \mathbb{Q}$. Για το (β) παρατηρούμε ότι $1+\zeta = -\zeta^2$ και συνεπώς ότι για $c=1$ έχουμε $\gamma^3 = 2(1+\zeta)^3 = -2\zeta^6 = -2$. Άρα το ανάγωγο πολυώνυμο του γ επί του $\mathbb{Q}$ είναι το x^3+2. Για $c=-1$ έχουμε $\gamma^3 = 2(1-\zeta)^3 = -6(1+2\zeta) = -6\,i\sqrt{3}$ και συνεπώς $\gamma^6 = -108$. Αφού $2\zeta = -\gamma^3/6 - 1 \in \mathbb{Q}(\zeta)$ και $\sqrt[3]{2} = \gamma/(1-\zeta) \in \mathbb{Q}(\zeta)$, ο βαθμός του γ επί του $\mathbb{Q}$ διαιρείται από το 2 και το 3 και συνεπώς είναι ίσος με 6. Άρα το ανάγωγο πολυώνυμο του γ επί του $\mathbb{Q}$ είναι το x^6+108.

30. Για $n=2$ έχουμε $u_1^3+u_2^3 = (u_1+u_2)^3 - 3u_1u_2(u_1+u_2) = (e_1^0)^3 - 3e_1^0e_2^0$, όπου $e_1^0 = u_1+u_2$ και $e_2^0 = u_1u_2$. Θέτοντας $e_1 = u_1+u_2+u_3$, $e_2 = u_1u_2+u_1u_3+u_2u_3$ και $e_3 = u_1u_2u_3$ υπολογίζουμε για $n=3$ ότι

$$\begin{aligned} u_1^3+u_2^3+u_3^3-e_1^3+3e_1e_2 &= u_1^3+u_2^3+u_3^3-(u_1+u_2+u_3)^3 + \\ &\quad 3(u_1+u_2+u_3)(u_1u_2+u_1u_3+u_2u_3) \\ &= 3u_1u_2u_3 \;=\; 3e_3, \end{aligned}$$

δηλαδή $u_1^3+u_2^3+u_3^3 = e_1^3-3e_1e_2+3e_3$. Εύκολα επαληθεύει κανείς ότι για κάθε θετικό ακέραιο n ισχύει

$$u_1^3+u_2^3+\cdots+u_n^3 \;=\; e_1^3-3e_1e_2+3e_3,$$

όπου $e_1,e_2,\ldots,e_n$ είναι τα στοιχειώδη συμμετρικά πολυώνυμα στις μεταβλητές $u_1,u_2,\ldots,u_n$.

31. Από το παράδειγμα $F=\mathbb{Q}$, $L=\mathbb{Q}(\sqrt{2})$ και $K=\mathbb{Q}(\sqrt[4]{2})$ προκύπτει ότι η πρόταση είναι λανθασμένη. Πράγματι, στην περίπτωση αυτή οι L/F και K/L είναι τετραγωνικές επεκτάσεις σωμάτων χαρακτηριστικής μηδέν, άρα επεκτάσεις Galois. Αντιθέτως, η $G(K/F)$ είναι η ομάδα με δύο στοιχεία (γιατί;) και ισχύει $[K:F]=4$, άρα η K/F δεν είναι επέκταση Galois.

32. Θα δείξουμε ότι οι ακέραιοι αυτοί είναι ακριβώς οι θετικοί διαιρέτες του 24. Πράγματι, έχουμε $[K:F] = |G(K/F)| = 24$. Επομένως για κάθε $\gamma \in K$, ο βαθμός του γ επί του F διαιρεί το βαθμό $[K:F]=24$. Αντιστρόφως, έστω r ένας θετικός διαιρέτης του 24, δηλαδή $r \in \{1,2,3,6,8,12,24\}$. Τότε υπάρχει υποομάδα H της $G(K/F)$ τάξης $|H| = 24/r$ (εξηγήστε). Για το αντίστοιχο ενδιάμεσο σώμα $L=K^H$ της επέκτασης K/F ισχύει $[L:F]=r$. Γνωρίζουμε από το Θεώρημα 11.1 ότι υπάρχει πρωταρχικό στοιχείο γ της L, δηλαδή $L=F(\gamma)$. Τότε $[F(\gamma):F]=r$ και συνεπώς ο βαθμός του γ επί του F είναι ίσος με r.