Κεφάλαιο 10

10.1 10^{η} Εβδομάδα

Ριζικές επεκτάσεις

Ορισμός 10.1. Η πεπερασμένη επέκταση E/F λέγεται ριζική αν υπάρχει αλυσίδα διαδοχικών επεκτάσεων $F = F_0 \leq F_1 \leq \dots \leq F_r = E$ και $n_1, \dots, n_r \in \mathbb{N}$ τέτοιοι ώστε για $i = 1, \dots, r$, $F_i = F_{i-1}(\alpha_i)$ για κάποιο α_i, τέτοιο ώστε $\alpha_i^{n_i} \in F_{i-1}$. Με άλλα λόγια, για κάθε $i = 1, \dots, , r$, το α_i είναι ρίζα του πολυωνύμου $X^{n_i} - \beta_{i-1}$ για κάποιο $\beta_{i-1} \in F_{i-1}$.

Παρατήρηση 10.2. Αν αυτό συμβαίνει, τότε $\alpha_i^n \in F_{i-1}$ για $n = \mathrm{lcm}(n_1, \dots, n_r)$. Άρα στο εξής, για μια ριζική επέκταση E/F μπορώ ισοδύναμα να υποθέσω την ύπαρξη αλυσίδας $F = F_0 \leq F_1 \leq \dots \leq F_r = E$ και $n \in \mathbb{N}$, ώστε $F_i = F_{i-1}(\alpha_i)$ όπου $\alpha_i^n \in F_{i-1}$ για $i = 1, \dots, r$. Τότε λέω ότι η E/F είναι *επέκταση με n-τάξεως ριζικά*.

Παρατήρηση 10.3. Αν $F \leq K \leq E$ και K/F και E/K ριζικές, τότε έπεται αμέσως από τον ορισμό της ριζικής επέκτασης ότι και η E/F είναι ριζική. Εντελώς ανάλογα, αν κάθε μία από τις K/F και E/K είναι επέκταση με n-τάξεως ριζικά, τότε και η E/F είναι επέκταση με n-τάξεως ριζικά.

Παρατήρηση 10.4. Προφανώς, $E = F(\alpha_1, \dots, \alpha_r)$ όπου $\alpha_1^n = \beta_0 \in F, \dots, \alpha_i^n = \beta_{i-1} \in F(\alpha_1, \dots, \alpha_{i-1}), \dots$. Άρα το E παράγεται από r το πλήθος n-οστές ρίζες. Όμως, ενώ το E περιέχει κάποια ρίζα του $X^n - \beta_{i-1}$ για κάθε $i = 1, \dots, r$ δεν έχω εξασφαλίσει ότι περιέχει όλες τις ρίζες του. Θα ήθελα, λοιπόν, κάποια επέκταση που να περιέχει όλες τις ρίζες των πολυωνύμων $X^n - \beta_{i-1}$. Μια τέτοια ιδιότητα έχει προφανώς η κανονική κλειστότητα του E πάνω από το F, έστω N. Το ερώτημα που τίθεται είναι: «κληρονομεί» η N την ιδιότητα του να είναι ριζική επέκταση του F;

Πρόταση 10.5. *Αν η E/F είναι ριζική και N είναι κανονική κλειστότητα της E/F τότε και N/F ριζική.*

Απόδειξη. Εξ υποθέσεως υπάρχει αλυσίδα $F = F_0 \leq F_1 \leq \cdots \leq F_r = E$ και $n \in \mathbb{N}$ τέτοια ώστε, για κάθε $i = 1, \dots, r$ είναι $F_i = F_{i-1}(\alpha_i)$ και $\alpha_i^n \in F_{i-1}$. Για $i = 1, \dots, r$, εστω $S_i = \{\alpha_i, \alpha_i', \alpha_i'', \dots\}$ το σύνολο των F-συζυγών του α_i. Κατασκευάζω νέα αλυσίδα με $K_0 = F = F_0$ και ορίζω $K_i = K_{i-1}(S_i)$ για κάθε $i = 1, \dots, r$. Απλή συνέπεια αυτής της κατασκευής είναι ότι, για $i = 1, \dots, r$ ισχύει $K_i = F(S_1 \cup \cdots \cup S_i)$ και, ειδικότερα, $K_r = F(S_1 \cup \cdots \cup S_r)$. Για $i = 0, \dots, r$ ισχύουν , επίσης,τα εξής:

- $F_i \leq K_i$. Πράγματι, για $i = 0$ ισχύει η σχέση. Έστω $i > 1$ και $F_{i-1} \leq K_{i-1}$. Τότε $K_i = K_{i-1}(S_i) \geq F_{i-1}(S_i) \geq F_{i-1}(\alpha_i) = F_i$. Ειδικότερα, $K_r \geq F_r = E$.
- Η επέκταση K_i/F είναι κανονική. Αυτό ισχύει διότι $K_i = F(S_1 \cup \cdots \cup S_i)$, άρα K_i είναι σώμα διάσπασης πάνω από το F του $\prod_{k=1}^{i} \mathrm{Irr}\,(\alpha_k, F)$.
- Για $i \geq 1$ η K_i/K_{i-1} $(i \geq 1)$ είναι επέκταση με n-τάξεως ριζικά. Πράγματι, από την αμέσως προηγούμενη παρατήρηση, η K_{i-1}/F είναι κανονική. Επίσης, $\alpha_i^n \in K_{i-1}$. Εφαρμόζοντας την άσκηση 10.13

στην αλυσίδα $F \leq K_{i-1} \leq K_i$, συμπεραίνομε ότι η σχέση $\alpha_i^n \in K_{i-1}$ συνεπάγεται και τις $\beta^n \in K_{i-1}$ για $\beta = \alpha_i', \alpha_i'', ...$, και αυτό αποδεικνύει τον ισχυρισμό.

• $K_r \leq N$. Πράγματι, $\alpha_i \in N$ ($\alpha_i \in F_i \leq N$) και η N/F είναι κανονική, άρα όλες οι ρίζες του $\mathrm{Irr}\,(\alpha_i, F)$ ανήκουν στο N, δηλαδή, $S_i \subseteq N$, οπότε $K_r = F(S_1 \cup \cdots \cup S_r) \leq N$.

Από τις παραπάνω τέσσερις παρατηρήσεις και την Παρατήρηση 10.3 έπεται ότι η K_r/K_0, δηλαδή η K_r/F, είναι επέκταση με n-τάξεως ριζικά. Επίσης, η K_r/F είναι κανονική και $E \leq K_r \leq N$. Λόγω του ότι η N είναι κανονική κλειστότητα της E/F, έπεται ότι $K_r = N$, οπότε η N/F είναι επέκταση με n-τάξεως ριζικά. ☐

Ορισμός 10.6. Λέμε ότι μία ομάδα G είναι επιλύσιμη αν και μόνο αν υπάρχει αλυσίδα υποομάδων της,

$$G = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_r = \langle e \rangle,$$

όπου e είναι το ουδέτερο στοιχείο της G και H_{i-1}/H_i είναι αβελιανή για κάθε $i = 1, \ldots, r$.

Ορισμός 10.7. Έστω σώμα F και $f \in F[X]$ μη σταθερό. Λέμε ότι *το f είναι επιλύσιμο με ριζικά* αν το σώμα διάσπασης του f πάνω από το F περιέχεται σε μια ριζική επέκταση του F. Ανάλογα λέμε ότι το *το f είναι επιλύσιμο με n-τάξεως ριζικά* αν το σώμα διάσπασης του f πάνω από το F περιέχεται σε μια επέκταση του F με n-τάξεως ριζικά.

Θεώρημα 10.8. *Αν* $\mathrm{char}(F) = 0$ *και το μη σταθερό $f \in F[X]$ είναι επιλύσιμο με ριζικά, τότε η ομάδα $\mathcal{G}\,(\mathrm{K}/F)$ είναι επιλύσιμη.*

Απόδειξη. Έστω K σώμα ανάλυσης του f πάνω από το K, E/F επέκταση με ριζικά και $K \leq E$. Αν N είναι η κανονική κλειστότητα της E/F, τότε η N/F είναι ριζική, κανονική και $K \leq N$. Συνεπώς (βλ. Παρατήρηση 10.2), υπάρχει $n \in \mathbb{N}$ και αλυσίδα

$$F = K_0 \leq K_1 \leq \cdots \leq K_r = N, \quad K_i = K_{i-1}(\alpha_i),\ \alpha_i^n \in K_{i-1} \quad (i = 1, \ldots, r).$$

Σε κάποια αλγεβρική κλειστότητα του N, έστω ω μια πρωταρχική n-οστή ρίζα της μονάδος (του F). Θεωρώ την εξής αλυσίδα

$$F \leq K_0(\omega) \leq K_1(\omega) \leq \cdots \leq K_r(\omega) = N(\omega).$$

Αυτη είναι μία αλυσίδα επεκτάσεων με n-οστές ρίζες και $N(\omega)/F$ είναι κανονική (άρα και Galois, αφού $\mathrm{char}(F) = 0$) και ριζική. Για απλούστευση του συμβολισμού θέτω $F_i := K_i(\omega)$ για $i = 0, 1, \ldots, r$.

Αν $\alpha_i^n = \beta_{i-1} \in K_{i-1}$, τότε το α_i είναι ρίζα του $X^n - \beta_{i-1} \in F_{i-1}[X]$ και, επειδή $\omega \in F_{i-1}$, το F_i είναι σώμα διάσπασης του $X^n - \beta_{i-1} \in F_{i-1}[X]$. Άρα, από το Θεώρημα 9.3, η επέκταση F_i/F_{i-1} είναι κυκλική. Η N/F είναι Galois, άρα και η N/F_{i-1} είναι Galois για $1 \leq i \leq r$ και έχω το εξής διάγραμμα αντιστοιχίας Galois:

$$\begin{array}{ccc}
N & \longleftrightarrow & \langle id \rangle \\
\Big| & & \Big| \\
F_i & \longleftrightarrow & \mathcal{G}\,(N/F_i) = H_i \\
\Big| & & \Big| \\
F_{i-1} & \longleftrightarrow & \mathcal{G}\,(N/F_{i-1}) = H_{i-1}
\end{array}$$

Επειδή η F_i/F_{i-1} είναι Galois, το Θεμελιώδες Θεώρμα της Θεωρίας Galois συνεπάγεται ότι $H_i \trianglelefteq H_{i-1}$ και $\mathcal{G}\,(F_i/F_{i-1}) \cong H_{i-1}/H_i$. Έτσι σχηματίζουμε μία αλυσίδα υποομάδων

$$\mathcal{G}\,(N/F) = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_{i-1} \trianglerighteq H_i \trianglerighteq \cdots \trianglerighteq H_r = \langle id \rangle$$

με τις πηλικοομάδες $H_{i-1}/H_i \cong \mathcal{G}(F_i/F_{i-1})$ κυκλικές άρα αβελιανές, οπότε η $\mathcal{G}(N/F)$ είναι επιλύσιμη.

Τώρα θεωρώ το διάγραμμα

$$\begin{array}{ccc} N & \longleftrightarrow & \langle id \rangle \\ | & & | \\ K & \longleftrightarrow & \mathcal{G}(N/K) \\ | & & | \\ F & \longleftrightarrow & \mathcal{G}(N/F) \end{array}$$

Η K/F είναι Galois ως σώμα διάσπασης του f, άρα $\mathcal{G}(N/K) \trianglelefteq \mathcal{G}(N/F)$ και $\mathcal{G}(K/F) \cong \mathcal{G}(N/F)/\mathcal{G}(N/K)$. Άρα, η $\mathcal{G}(\mathrm{K}/F)$ είναι πηλικοομάδα μιας επιλύσιμης ομάδας, οπότε, από την άσκηση 10.14 (2) είναι και αυτή επιλύσιμη. Αλλά επιλυσιμότητα της $\mathcal{G}(K/F)$ σημαίνει (Ορισμός 10.7) επιλυσιμότητα του f με ριζικά. □

Πρόταση 10.9. *Έστω πρώτος $p \geq 5$ και $f \in \mathbb{Q}[X]$ ανάγωγο πολυώνυμο βαθμού p. Αν το f έχει ακριβώς $p-2$ πραγματικές ρίζες, τότε το f δεν είναι επιλύσιμο με ριζικά.*

Απόδειξη. Από την Πρόταση 8.17, ένα πολυώνυμο f όπως στην εκφώνηση έχει ομάδα Galois ισόμορφη με την S_p. Από την αμέσως παρακάτω Πρόταση 10.11, η S_p δεν είναι επιλύσιμη για $p \geq 5$, άρα, βάσει του Θεωρήματος 10.8, το f δεν είναι επιλύσιμο με ριζικά. □

Παράδειγμα 10.10. Το πολυώνυμο $f = X^5 - 20X + 5 \in \mathbb{Q}[X]$ έχει ακριβώς τρεις πραγματικές ρίζες, άρα δεν είναι επιλύσιμο με ριζικά. Συνεπώς, δεν υπάρχει αλγεβρικός τύπος με ριζικά που να δίνει τις ρίζες ενός πεμπτοβάθμιου πολυωνύμου συναρτήσει των συντελεστών του.

Η πρόταση που χρησιμοποιήσαμε στην απόδειξη της Πρότασης 10.9 είναι η εξής:

Πρόταση 10.11. *Για $n \geq 5$, η S_n δεν είναι επιλύσιμη ομάδα.*

Απόδειξη. Έστω $S_n = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_r = \langle id \rangle$ και H_{i-1}/H_i αβελιανή για κάθε i. Θα δείξω επαγωγικά ότι, για $i = 0, 1, \ldots, r$, η H_i περιέχει όλους τους κύκλους μήκους 3, κάτι προφανώς άτοπο, αφού $H_r = \langle id \rangle$.

Για $i = 0$ ο ισχυρισμός αληθεύει, αφού H_0 είναι ολόκληρη η S_n. Έστω $i > 1$ και υποθέτω ότι η H_{i-1} περιέχει όλους τους κύκους μήκους 3. Θα δείξω ότι και η H_i έχει την ίδια ιδιότητα. Παίρνω τυχαία (i, j, k) με $i \neq j \neq k \neq i$ και $1 \leq i, j, k \leq n$. Επειδή $n \geq 5$, μπορώ να επιλέξω $l, m \in \{1, \ldots, n\} \setminus \{i, j, k\}$ με $l \neq m$. Εξ υποθέσεως, $(j, k, m), (i, l, j), (m, k, j), (j, l, i) \in H_{i-1}$. Το γινόμενο των συμπλόκων αυτών των κύκλων (ως προς την υποομάδα H_i), όταν τα πολλαπλασιάσω με αυτή τη σειρά, είναι

$$(j,k,m)H_i \cdot (i,l,j)H_i \cdot (m,k,j)H_i \cdot (j,l,i)H_i = (j,k,m)(i,l,j)(m,k,j)(j,l,i)H_i = (i,j,k)H_i.$$

Η H_{i-1}/H_i έχει υποτεθεί αβελιανή, άρα μπορώ να πολλαπλασιάσω τα παραπάνω σύμπλοκα με άλλη διάταξη και να πάρω το ίδιο αποτέλεσμα. Τώρα, λοιπόν, τα πολλαπλασιάζω ως εξής:

$$(j,k,m)H_i \cdot (m,k,j)H_i \cdot (i,l,j)H_i \cdot (j,l,i)H_i = (j,k,m)(m,k,j)(i,l,j)(j,l,i)H_i = idH_i = H_i,$$

άρα $(i, j, k)H_i = H_i$, που σημαίνει ότι $(i, j, k) \in H_i$. □

Θεώρημα 10.12 (Αντίστροφο του Θεωρήματος 10.8)**.** *Έστω* $\mathrm{char}(F) = 0$ *και μη σταθερό πολυώνυμο $f \in F[X]$, του οποίου η ομάδα Galois είναι επιλύσιμη. Τότε το f είναι επιλύσιμο με n-τάξεως ριζικά, όπου n είναι η τάξη της ομάδας Galois του πολυωνύμου.*

Απόδειξη. Έστω K σώμα διάσπασης του f πάνω από το F. Η επέκταση K/F είναι κανονική, ως σώμα διάσπασης του f, και διαχωρίσιμη, αφού $\operatorname{char}(F) = 0$, άρα είναι επέκταση Galois. Εξ υποθέσεως, η ομάδα $\mathcal{G}(K/F)$ έχει τάξη n και είναι επιλύσιμη. Από την επιλυσιμότητά της έπεται ότι υπάρχει μια αλυσίδα υποομάδων της, ως εξής:

$$\mathcal{G}(K/F) = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_r = \langle id \rangle,$$

Για $i = 0, \dots, r$, έστω $K_i = \mathcal{F}(H_i)\cdot$ ισοδύναμα, $H_i = \mathcal{G}(K/K_i)$. Ειδικότερα, $K_r = K$ και $K_0 = \mathcal{F}(H_0) = \mathcal{F}(\mathcal{G}(K/F)) = F$.

Για $1 \leq i < r$ θεωρώ το διάγραμμα

$$\begin{tikzcd}
K \arrow[r, leftrightarrow] \arrow[d, dash] & H_r = \langle id \rangle \arrow[d, dash] \\
K_i \arrow[r, leftrightarrow] \arrow[d, dash] & H_i \arrow[d, dash] \\
K_{i-1} \arrow[r, leftrightarrow] & H_{i-1}
\end{tikzcd}$$

Είναι $H_i \trianglelefteq H_{i-1}$, άρα, από το Θεμελιώδες Θεώρημα Galois, η K_i/K_{i-1} είναι Galois και $\mathcal{G}(K_i/K_{i-1}) \cong H_{i-1}/H_i$, αβελιανή. Έστω ω πρωταρχική n-οστή ρίζα της μονάδας (του F) σε κάποια αλγεβρική κλειστότητα του K. Θεωρώ την αλυσίδα

$$F(\omega) = K_0(\omega) \leq K_1(\omega) \leq \cdots \leq K_r(\omega) = K(\omega)$$

και θέτω $F_i := K_i(\omega)$ για $i = 0, \dots, r$. Η F_i/F_{i-1} είναι Galois. Πράγματι, η $\mathcal{G}(K_i/K_{i-1})$ είναι Galois, άρα το K_i είναι σώμα διάσπασης ενός πολυωνύμου $g_i \in K_{i-1}[X]$. Αλλά τότε και το $F_i = K_i(\omega)$ είναι σώμα διάσπασης του g_i πάνω από το $F_{i-1} = K_{i-1}(\omega)$, άρα η F_i/F_{i-1} είναι κανονική. Είναι και διαχωρίσιμη, αφού είναι πάνω από σώμα χαρακτηριστικής 0, άρα είναι Galois.

Υπάρχει ένας φυσιολογικός μονομορφισμός ομάδων $\psi : \mathcal{G}(F_i/F_{i-1}) \to \mathcal{G}(K_i/K_{i-1})$ (βλ. σημείωση στο τέλος της απόδειξης), άρα η $\mathcal{G}(F_i/F_{i-1})$ είναι ισόμορφη με υποομάδα της αβελιανής $\mathcal{G}(K_i/K_{i-1})$, οπότε είναι αβελιανή. Συνεπώς, F_i/F_{i-1} είναι επέκταση Kummer (Ορισμός 9.5). Επιπλέον, $\omega \in F_{i-1}$ και (στην επόμενη σχέση το $\#$ συμβολίζει τάξη ομάδας για να μη γίνει σύγχυση με το $|$ που σημαίνει «διαιρεί»)

$$\#\mathcal{G}(F_i/F_{i-1}) \mid \#\mathcal{G}(K_i/K_{i-1}) = \frac{\#H_{i-1}}{\#H_i} \mid \#H_{i-1} \mid \#H_0 = n,$$

άρα $\sigma^n = \mathrm{id}$ για κάθε $\sigma \in \mathcal{G}(F_i/F_{i-1})$. Συνεπώς, από το Θεώρημα 9.9, το F_i είναι σώμα διάσπασης ενός πολυωνύμου της μορφής $(X^n - \alpha_1) \cdots (X^n - \alpha_m) \in F_{i-1}[X]$, άρα η F_i/F_{i-1} είναι επέκταση με n-τάξεως ριζικά. Από την Παρατήρηση 10.3 έπεται ότι η F_r/F_0, δηλαδή η $K(\omega)/F(\omega)$, είναι επέκταση με n-τάξεως ριζικά. Την ίδια ιδιότητα έχει και η $F(\omega)/F$, άρα καταλήγομε στην αλυσίδα $F \leq K \leq K(\omega)$, στην οποία η $K(\omega)/F$ είναι επέκταση με n-τάξεως ριζικά, που είναι και το ζητούμενο.

Σημείωση: Σχετικά με τον ομομορφισμό ψ που χρησιμοποιήθηκε παραπάνω. Αυτός ορίζεται από τη σχέση $\psi(\sigma) = \sigma|_{K_i}$. Είναι καλά ορισμένος, διότι ο $\sigma|_{K_i}$ είναι K_{i-1}-μονομορφισμός $K_i \hookrightarrow F_i$ και, επειδή η K_i/K_{i-1} είναι κανονική, αυτός ο μονομορφισμός είναι, στην πραγματικότητα K_{i-1}-αυτομορφισμός του K_i (Θεώρημα 5.12). Επίσης, η απεικόνιση ψ είναι 1-1 γιατί ο πυρήνας της είναι τετριμμένος. Πράγματι, αν σ είναι F_{i-1}-αυτομορφισμός του F_i και $\sigma \in \ker \psi$, τότε $\psi(\sigma) = id_{K_i}$. Άρα ο σ αφήνει αναλλοίωτα όλα τα στοιχεία του $K_i\cdot$ αφήνει, όμως, αναλλοίωτο και το ω (αφού είναι F_{i-1}-αυτομορφισμός), άρα αφήνει αναλλοίωτα όλα τα στοιχεία του $K_i(\omega) = F_i$. Άρα $\sigma = id_{F_i}$. $\square$

Ασκήσεις

Άσκηση 10.13. Έστω $F \leq K \leq E$ διαδοχικές επεκτάσεις με τις K/F και E/F κανονικές, $n \in \mathbb{N}$ και $\alpha \in E$ ώστε να ισχύει $\alpha^n \in K$. Αν το $\beta \in E$ είναι F-συζυγές του α, αποδείξτε ότι $\beta^n \in K$.

Άσκηση 10.14. (1) Έστω $f : G \to H$ επιμορφισμός ομάδων και η G είναι επιλύσιμη. Αποδείξτε ότι και η H είναι επιλύσιμη ομάδα.
Υπόδειξη. Έστω $G_n = \langle e \rangle \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$, όπου e είναι το ουδέτερο της G και G_{i-1}/G_i είναι αβελιανή για κάθε $i = 1, \ldots, n$. Θεωρήστε τις υποομάδες $f(G_i)$ $(i = 0, \ldots, n)$ της H.
(2) Αν η G είναι επιλύσιμη ομάδα και $H \trianglelefteq G$ τότε και η G/H είναι επιλύσιμη.

Άσκηση 10.15. (1) Γιατί κάθε αβελιανή ομάδα είναι επιλύσιμη;
(2) Αποδείξτε ότι η διεδρική ομάδα D_4 είναι επιλύσιμη.
Υπόδειξη. Δείτε το διάγραμμα υποομάδων του Παραδείγματος 6.11.
(3) Αποδείξτε ότι η εναλλάσουσα ομάδα A_4 είναι επιλύσιμη.
Υπόδειξη. Θεωρήστε δεδομένο ότι $A_4 = \langle (1\,2\,3),\ (1\,2\,4) \rangle$ και εξετάστε πώς σχετίζονται μεταξύ τους οι ομάδες A_4, H, K, όπου $H = \langle (1\,2)(3\,4),\ (1\,3)(2\,4) \rangle$ και $K = \langle (1\,2)(3\,4) \rangle$.
(4) Αποδείξτε ότι η S_4 είναι επιλύσιμη ομάδα.

Άσκηση 10.16 (Τύποι του Cardano για τις ρίζες κυβικού πολυωνύμου)**.** Έστω F σώμα χαρακτηριστικής $\neq 2, 3$ και το πολυώνυμο $f = X^3 + pX + q \in F[X]$. Έστω

$$R = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3, \quad \alpha^3 = -\frac{q}{2} + \sqrt{R}, \quad \beta = -\frac{p}{3\alpha},$$

όπου $\sqrt{R}$ είναι μια οποιαδήποτε από τις δύο τετραγωνικές ρίζες του R. (Δηλαδή, το α είναι μια οποιαδήποτε κυβική ρίζα του $\sqrt{R} - q/2$.) Έστω ω πρωταρχική κυβική ρίζα της μονάδας (σε κάποια επέκταση του F). Τότε,

$$f(X) = (X - r_0)(X - r_1)(X - r_2), \quad r_i = \omega^i \alpha + \omega^{2i} \beta, \ \ i = 0, 1, 2.$$

Υπόδειξη. Δείξτε ότι $\beta^3 = -\frac{q}{2} - \sqrt{R}$. Επίσης, ίσως σας χρησιμεύει η παρατήρηση ότι $-108R = D$, η διακρίνουσα του f.

Υπερβατικότητα

Ορισμός 10.17. Θεωρώ επέκταση σωμάτων E/F.

1. Το $t \in E$ χαρακτηρίζεται υπερβατικό πάνω από το F αν δεν είναι αλγεβρικό πάνω από το F. Δηλαδή $f(t) \neq 0$ για κάθε μη μηδενικό $f \in F[X]$.

2. Τα $t_1, \ldots, t_n \in E$ θα λέμε ότι είναι αλγεβρικώς εξαρτημένα πάνω από το F (F-αλγεβρικώς εξαρτημένα) αν και μόνο αν υπάρχει κάποιο μη μηδενικό $f \in F[X_1, \ldots, X_n]$ τέτοιο ώστε $f(t_1, \ldots, t_n) = 0$. Αν δεν είναι F-αλγεβρικώς εξαρτημένα, τότε θα λέγονται F-αλγεβρικώς ανεξάρτητα.

3. Το υποσύνολο S του E (πεπερασμένο ή άπειρο) λέμε ότι είναι F-αλγεβρικώς ανεξάρτητο, αν κάθε πεπεραμένο υποσύνολο του είναι F-αλγεβρικώς ανεξάρτητο. Δηλαδή, για κάθε $n \in \mathbb{N}$, για κάθε n-άδα $(s_1, \ldots, s_n) \in S^n$ *διαφορετικών μεταξύ τους στοιχείων* και για κάθε μη μηδενικό $f \in F[X_1, \ldots, X_n]$ ισχύει $f(s_1, \ldots, s_n) \neq 0$.
   Το $\emptyset$ οίζεται ως γραμμικώς ανεξάρτητο.

4. Έστω $S \subseteq E$ και $e \in E$. Λέω ότι το $t \in E$ είναι γραμμικώς εξαρτημένο από το S πάνω από το F (ή αλλιώς, S-γραμμικώς εξαρτημένο πάνω από το F) αν το t είναι αλγεβρικό πάνω από το $F(S)$.

5. Το $S \subseteq E$ παράγει το αλγεβρικώς το E/F αν η επέκταση $E/F(S)$ είναι αλγεβρική.
6. Το $S \subseteq E$ λέμε ότι είναι βάση υπερβατικότητας της επέκτασης E/F αν το S πληροί τις εξής συνθήκες: (1) είναι F-αλγεβρικώς ανεξάρτητο και (2) παράγει αλγεβρικώς το E/F.

Ασκήσεις

Άσκηση 10.18. Έστω E/F επέκταση σωμάτων, $\emptyset \neq S \subseteq E$ και $t \in E$ το οποίο είναι S-αλγεβρικώς εξαρτημένο πάνω από το F. Αποδείξτε ότι υπάρχουν $n, r \in \mathbb{N}$, $(s_1, \dots, s_r) \in S^r$ και πολυώνυμα $C_0, \dots, C_n \in F[X_1, \dots, X_r]$, έτσι ώστε $C_n(s_1, \dots, s_r) \neq 0$ και

$$C_n(s_1, \dots, s_r)t^n + \cdots + C_1(s_1, \dots, s_r)t + C_0(s_1, \dots, s_r) = 0$$

Άσκηση 10.19. Έστω E/F επέκταση σωμάτων και $\emptyset \neq S \subseteq E$. Αν το $t \in E$ είναι αλγεβρικό πάνω από το $F(S)$, αποδείξτε ότι υπάρχουν $s_1, \dots, s_r \in S$ τέτοια ώστε το $\{s_1, \dots, s_r, t\}$ να είναι F-αλγεβρικώς εξαρτημένο.

Άσκηση 10.20. Έστω E/F επέκταση σωμάτων και $\emptyset \neq S \subseteq E$. Αν το S είναι F-αλγεβρικώς ανεξάρτητο και το $S \cup \{t\}$ είναι F-αλγεβρικώς εξαρτημένο, αποδείξτε ότι το t είναι αλγεβρικό πάνω από το $F(S)$.