Κεφάλαιο 5

5.1 5^{η} Εβδομάδα

Διαχωρισιμότητα (συνέχεια)

Πρόταση 5.1. *Έστω C αλγεβρική κλειστότητα του F και $\alpha \in C$. Τότε ο βαθμός $[F(\alpha) : F]$ είναι πολλαπλάσιο του δείκτη $\{F(\alpha) : F\}$. Επιπλέον, το α είναι διαχωρίσιμο πάνω από το F αν και μόνο αν $[F(\alpha) : F] = \{F(\alpha) : F\}$.*

Απόδειξη. Θεωρώ την ανάλυση του $\operatorname{Irr}(\alpha, F)$ στο $C[X]$. Σύμφωνα με το πόρισμα 4.24, $\operatorname{Irr}(\alpha, F) = c(X-\alpha_1)^r \dots (X-\alpha_k)^r$ με $c \in F$, $\alpha_1, \dots, \alpha_k \in C$ διαφορετικά και $r \geq 1$. Ο βαθμός της επέκτασης είναι

$$[F(\alpha) : F] = \deg \operatorname{Irr}(\alpha, F) = rk.$$

Το πλήθος των F-μονομορφισμών $F(\alpha) \hookrightarrow C$ είναι ακριβώς k, διότι κάθε τέτοιος στέλνει το α (που είναι ρίζα του $\operatorname{Irr}(\alpha, F)$) σε κάποια ρίζα του $\operatorname{Irr}(\alpha, F)$, δηλαδή, σε κάποιο από το $\alpha_1, \dots, \alpha_k$. Άρα, $\{F(\alpha) : F\} = k$ και επομένως, $[F(\alpha) : F] = r\{F(\alpha) : F\}$.

Το α είναι διαχωρίσιμο $\iff r = 1 \iff [F(\alpha) : F] = \{F(\alpha) : F\}$. □

Πρόταση 5.2. *Έστω $F \leq E \leq K$ διαδοχικές επεκτάσεις σωμάτων και η K/F είναι πεπερασμένη (άρα και οι E/F, K/E είναι πεπερασμένες). Τότε $\{K : F\} = \{K : E\}\{E : F\}$.*

Απόδειξη. Έστω C αλγεβρική κλειστότητα του K (οπότε C είναι αλγεβρική κλειστότητα του F και του E, από την άσκηση 4.30). Είναι $\{K : F\} =$ το πλήθος των F μονομορφισμών $K \hookrightarrow C$. Έστω $\{K : E\} = n$ και $\sigma_1, \dots, \sigma_n$ είναι όλοι οι F-μονομορφισμοί $E \hookrightarrow C$. Τέλος έστω $\{K : E\} = m$. Πώς μπορώ να κατασκευάσω ένα F-μονομορφισμό $\tau : K \hookrightarrow C$; Θα δείξω ότι αυτό μπορεί να γίνει με mn τρόπους, οπότε θα έχω τελειώσει.

Έστω $\sigma = \tau|_E : E \hookrightarrow C$ και αφού ο τ είναι F-μονομορφισμός ο σ είναι επίσης F-μονομορφισμός. Επομένως, $\sigma \in \{\sigma_1, \dots, \sigma_n\}$. Τώρα, βλέπω τον τ σαν επέκταση του σ (για τον οποίο σ έχω n επιλογές).

$$\begin{array}{ccc} K & \xhookrightarrow{\tau} & C \\ | & & \\ E & \xhookrightarrow{\sigma} & C \end{array}$$

Με πόσους τρόπους ένας σ όπως στο διάγραμμα μπορεί να επεκταθεί σε $\tau : K \hookrightarrow C$; Απάντηση: με $\{K : E\}$ τρόπους, δηλαδή με m. Άρα για το τ υπάρχουν mn επιλογές. □

Πόρισμα 5.3. *Έστω C αλγεβρική κλειστότητα του F, $\alpha \in C$. Αν το α είναι διαχωρίσιμο πάνω από το F, τότε η $F(\alpha)/F$ είναι διαχωρίσιμη.*

Απόδειξη. Έστω $\beta \in F(\alpha)$. Θα δείξω ότι το β είναι διαχωρίσιμο πάνω από το F. Είναι $F \leq F(\beta) \leq F(\alpha)$, άρα

$$[F(\alpha) : F(\beta)]\,[F(\beta) : F] = [F(\alpha) : F] \overset{5.1}{=} \{F(\alpha) : F\} \overset{5.2}{=} \{F(\alpha) : F(\beta)\}\,\{F(\beta) : F\}$$
$$\overset{5.1}{=} [F(\alpha) : F(\beta)]\,\{F(\beta) : F\}$$

και συγκρίνοντας το αριστερότερο με το δεξιότερο μέλος βλέπομε ότι $[F(\beta) : F] = \{F(\beta) : F\}$, άρα (Πρόταση 5.1) η επέκταση $F(\beta)/F$ είναι διαχωρίσιμη, οπότε το β είναι διαχωρίσιμο πάνω από το F. □

Θεώρημα 5.4. *Έστω πεπερασμένη επέκταση E/F. Η E/F είναι διαχωρίσιμη αν και μόνο αν $[E : F] = \{E : F\}$.*

Απόδειξη. Έστω C αλγεβρική κλειστότητα της E (άρα και τον F) και $\alpha_1, \dots, \alpha_2 \in C$ τέτοιο ώστε $E = F(\alpha_1, \dots, \alpha_n)$.

“ $\Longrightarrow$ ” Αν η E/F είναι διαχωρίσιμη, τότε κάθε α_i είναι διαχωρίσιμο πάνω από το F. Έτσι, το α_1 είναι διαχωρίσιμο πάνω από το F και για $i = 2, \dots, n$ το α_i είναι διαχωρίσιμο πάνω από το $F(\alpha_1, \dots, \alpha_{i-1})$. Άρα από την Πρόταση 5.1,

$$\{F(\alpha_1) : F\} = [F(\alpha_1) : F]$$

και για κάθε $i = 2, \dots, n$,

$$\{F(\alpha_1, \dots, \alpha_i) : F(\alpha_1, \dots, \alpha_{i-1})\} = [F(\alpha_1, \dots, \alpha_i) : F(\alpha_1, \dots, \alpha_{i-1})]\,.$$

Πολλαπλασιάζω κατα μέλη τις ισότητες και χρησιμοποιώ την πολλαπλασιασικότητα των βαθμών και των δεικτών, οπότε

$$\{F(\alpha_1, \dots, \alpha_n) : F\} = [F(\alpha_1, \dots, \alpha_n) : F]\,,$$

δηλαδή $\{E : F\} = [E : F]$.

“ $\Longleftarrow$ ” Έστω ότι $\{E : F\} = [E : F]$. Θα πάρω τυχαίο $\alpha \in E$ και θα δείξω ότι το α είναι διαχωρίσιμο πάνω από το F. Αυτό ισοδυναμεί με το $\{F(\alpha) : F\} = [F(\alpha) : F]$ σύμφωνα με την Πρόταση 5.1.

Έχω ότι

$$[E : F(\alpha)]\,[F(\alpha) : F] = [E : F] \overset{5.1}{=} \{E : F\} \overset{5.2}{=} \{E : F(\alpha)\}\,\{F(\alpha) : F\}\,.$$

Αλλά καθένας από τους δύο παράγοντες του αριστερότερου γινομένου είναι $\geq$ από τον αντίστοιχο παράγοντα του δεξιότερου γινομένου, οπότε, για να ισχύει η ισότητα πρέπει ένας προς έναν να είναι ίσοι, άρα $\{F(\alpha) : F\} = [F(\alpha) : F]$.

□

Θεώρημα 5.5. *Έστω $F \leq K \leq E$ με την E/F πεπερασμένη. Τότε*

$$E/F \text{ διαχωρίσιμη} \iff E/K \text{ διαχωρίσιμη και } K/F \text{ διαχωρίσιμη}$$

Απόδειξη. **“ $\Longrightarrow$ ”** Πολύ εύκολο.

“ $\Longleftarrow$ ” Έστω ότι οι E/K και K/F είναι διαχωρίσιμες. Από την Πρόταση 5.1, $\{E : K\} = [E : K]$ και $\{K : F\} = [K : F]$. Πολλαπλασιάζοντας κατα μέλη έχω $\{E : F\} = [E : F]$, οπότε η E/F είναι διαχωρίσιμη από το Θεώρημα 5.4.

□

Υπενθύμιση 5.6. 1. Έστω τυχαία επέκταση E/F και $\alpha, \beta \in E$ αλγεβρικά πάνω από το F. Λέω ότι τα α, β είναι F-συζυγή αν και μόνο αν $\text{Irr}(\alpha, F) = \text{Irr}(\beta, F)$.

2. Έστω C αλγεβρική κλειστότητα του E άρα και του F και F-μονομορφισμός $\sigma : E \hookrightarrow C$. Αν το $f \in F[X]$ είναι ανάγωγο και $\alpha \in E$ είναι ρίζα του F (οπότε $f = c \cdot \text{Irr}(\alpha, F)$, όπου c είναι ο συντελεστής του μεγιστοβάθμιου όρου του f) τότε το $\sigma(\alpha)$ είναι F-συζυγής του α.
Διότι, αν $f = c_n X^n + \cdots + c_1 X^1 + c_0$, τότε $c_n \alpha^n + \cdots + c_1 \alpha^1 + c_0$. Εφαρμόζω τον σ ($\sigma(c_i) = c_i \forall i$) οπότε $c_n \sigma(\alpha)^n + \cdots + c_1 \sigma(\alpha)^1 + c_0$, δηλαδή $\sigma(\alpha)$ είναι ρίζα του f άρα και του $\text{Irr}(\alpha, F)$, οπότε τα $\alpha, \sigma(\alpha)$ είναι F συζυγή.

   Επειδή ο σ είναι 1-1, διαφορετικές ρίζες του f έχουν διαφορετικές εικόνες μέσω του σ. Άρα ο

$$\sigma : \text{Σύνολο Ριζών} \to \text{Σύνολο Ριζών}$$

   είναι 1-1 απεικόνιση, άρα και επί. Δηλαδή ο σ προκαλεί μετάθεση στις ρίζες του f.

   Οπότε, αν $\alpha_1, \ldots, \alpha_k$ είναι όλες οι διαφορετικές ρίζες του f, τότε $\sigma(\alpha_1), \ldots, \sigma(\alpha_k)$ είναι μετάθεση αυτών.

Κανονικότητα

Ορισμός 5.7. Έστω E/F αλγεβρική. Λέμε ότι η επέκταση είναι κανονική εάν έχει την εξής ιδιότητα: Αν ένα ανάγωγο $f \in F[X]$ έχει μία ρίζα στο E, τότε αναλύεται σε πρωτοβάθμιους παράγοντες του $E[X]$, δηλαδή διασπάται στο Ε.

Πιο παραστατικά διατυπωμένο, η E/F έχει την ιδιότητα «όλα ή τίποτα»: Το f ή δεν έχει καμία ρίζα του στο E ή έχει όλες τις ρίζες στο E.

Παράδειγμα 5.8. Κάθε δευτεροβάθμια επέκταση ενός σώματος F χαρακτηριστικής $\neq 2$, είναι κανονική. Πράγματι, αν η E/F είναι δευτέρου βαθμού, τότε έστω $1, \alpha$ μία βάση της. Αν $\text{Irr}(\alpha, F) = X^2 + bX + c$ με $b, c \in F$, τότε $-b - \alpha$ είναι, επίσης ρίζα, του $\text{Irr}(\alpha, F)$. Αν $b \neq 0$, η ρίζα αυτή είναι διαφορετική από την α. Αν $b = 0$, τότε $c \neq 0$ και δύο ρίζες του $\text{Irr}(\alpha, F)$ είναι οι $\pm\alpha$ και αυτές είναι διαφορετικές γιατί $\text{char}(F) \neq 2$. Άρα, και οι δύο ρίζες του $\text{Irr}(\alpha, F)$ ανήκουν στο E.

Παράδειγμα 5.9. Η $E = \mathbb{Q}(\sqrt[3]{2})$ δεν είναι κανονική, διότι το $X^3 - 2$ είναι ανάγωγο σπό $\mathbb{Q}$ και έχει μία ρίζα στο E, αλλά οι άλλες ρίζες του $\omega\sqrt[3]{2}$ και $\omega^2\sqrt[3]{2}$ (όπου ω κυβική ρίζα της μονάδας $\neq 1$) δεν ανήκουν στο E.

Παράδειγμα 5.10. Η επέκταση $\mathbb{Q}(\alpha)/\mathbb{Q}$ όπου $\alpha \in \mathbb{C}$ είναι ρίζα του αναγώγου $X^2 - 3X - 1 \in \mathbb{Q}[X]$ είναι κανονική, σύμφωνα με την άσκηση 3.16.

Πρόταση 5.11. *Έστω E/F πεπερασμένη επάκταση, C αλγεβρική κλειστότητα του F και F-μονομορφισμός $\sigma : E \hookrightarrow C$. Αν $\sigma(E) \subseteq E$, τότε $\sigma(E) = E$, δηλαδή, ο σ είναι F-αυτομορφισμός του E.*

Απόδειξη. Αν $\sigma(E) \subseteq E$, τότε έχομε τις διαδοχικές επεκτάσεις $F \leq \sigma(E) \leq E$. Λόγω ισομορφίας των E και $\sigma(E)$, οι βαθμοί $[E : F]$ και $[\sigma(E) : F]$ είναι ίσοι (διότι, αν $e_1, \ldots, e_n$ είναι βάση της E/F, τότε είναι απλή άσκηση να δείξομε ότι $\sigma(e_1), \ldots, \sigma(e_n)$ είναι βάση της $\sigma(E)/F$), άρα $[E : \sigma(E)] = 1$, οπότε $\sigma(E) = E$, σύμφωνα με την άσκηση 3.13 (i). □

Θεώρημα 5.12. *Έστω E/F πεπερασμένη και C αλγεβρική κλειστότητα του E (άρα και του F). Η E/F είναι κανονική $\iff$ $\sigma(E) \subseteq E$ για κάθε F-μονομορφισμό $\sigma : E \hookrightarrow \sigma(E) \subseteq C$ $\iff$ κάθε F-μονομορφισμός $\sigma : E \hookrightarrow \sigma(E) \subseteq C$ είναι αυτομορφισμός του E.*

Απόδειξη. Απόδειξη της πρώτης ισοδυναμίας. Έστω $E = F(\alpha_1, \ldots, \alpha_n)$. (αφού E/F πεπερασμένη).

" $\Longrightarrow$ " Έστω E/F κανονική και σ είναι F-μονομορφισμός $E \hookrightarrow C$. Έστω $i \in \{1, \dots, n\}$. Τότε το σ στέλνει το α_i σε ρίζα του $\operatorname{Irr}(\alpha_i, F)$. Αφού $\alpha_i \in E$ και η E/F είναι κανονική, έπεται ότι όλες οι ρίζες του $\operatorname{Irr}(\alpha_i, F)$ (που εξ αρχής ξέρω ότι ανήκουν στο C) ανήκουν στο E. Οπότε $\sigma(\alpha_i) \in E, \forall i = 1, \dots, n$. Επίσης, $\sigma(c) = c, \forall c \in F$, άρα $\sigma(E) = \sigma(F(\alpha_1, \dots, \alpha_n)) \subseteq E$.

" $\Longleftarrow$ " Υποθέτω ότι $\forall F$-μονομορφισμό $\sigma : E \hookrightarrow C$ ισχύει ότι $\sigma(E) \subseteq E$. Έστω ανάγωγο $p \in F[X]$, που έχει μία ρίζα του α στο E. Πρέπει και αρκεί να δείξω ότι κάθε άλλη ρίζα του p (βλέπω τις ρίζες του p σαν στοιχεία του C) ανήκει στο E. Είναι $p = c \operatorname{Irr}(\alpha, C)$ όπου $c \in F$.

Έστω $\beta \in C$ μία άλλη ρίζα του p (δηλαδή του $\operatorname{Irr}(\alpha, F)$.) Ξέρω ότι υπάρχει F-ισομορφισμός $\sigma : F(\alpha) \to F(\beta)$ τέτοιος ώστε $\sigma(\alpha) = \beta$. Αυτός είναι, προφανώς, μονομορφισμός $F(\alpha) \hookrightarrow C$, άρα επεκτείνεται σε μονομορφισμό $\tau : E \hookrightarrow C$, από το Θεώρημα 4.6. Εξ υποθέσεως $\tau(E) \subseteq E$. Όμως, $\beta = \sigma(\alpha) \overset{\alpha \in E}{=} \tau(\alpha) \in E$

Απόδειξη της δεύτερης ισοδυναμίας. Προκύπτει αμέσως λόγω της ήδη αποδειχθείσας πρώτης ισοδυναμίας και της Πρότασης 5.11. □

Παράδειγμα 5.13 (Αντιπαράδειγμα)**.** $E = \mathbb{Q}(\sqrt[3]{2})$ και $\omega \in \mathbb{C}$ κυβική ρίζα της μονάδος, $\omega \neq 1$. Ο $\mathbb{Q}$-μονομορφισμός $\sigma : E \hookrightarrow \mathbb{C}$ με $\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$ δεν έχει την παραπάνω ιδιότητα διότι $\sigma(E) \neq E$

Θεώρημα 5.14. *Έστω E/F πεπερασμένη. Τότε, η E/F είναι κανονική $\iff$ E είναι σώμα διάσπασης κάποιου μη μηδενικού $f \in F[X]$.*

Απόδειξη. " $\Longrightarrow$ " Αφού η επέκταση είναι πεπερασμένη, έστω $E = F(\alpha_1, \dots, \alpha_n)$. Για κάθε $i = 1, \dots, n$ θεωρώ το $\operatorname{Irr}(\alpha_i, F)$ και συμβολίζω με A_i το σύνολο των διαφορετικών ριζών του. Η επέκταση E/F είναι κανονική και $\alpha_i \in E$, άρα $A_i \subseteq E$ για κάθε $i = 1, \dots, n$, οπότε $E = F(A_1 \cup \cdots \cup A_n)$. Αλλά αυτό λέει ότι το E είναι σώμα διάσπασης του πολυωνύμου $\prod_{i=1}^{n} \operatorname{Irr}(\alpha_i, F)$.

" $\Longleftarrow$ " Έστω ότι το E είναι σώμα διάσπασης του $f = \prod_{i=1}^{n} \operatorname{Irr}(\alpha_i, F)$. Για $i = 1, \dots, n$, έστω A_i το σύνολο των διαφορετικών ριζών του $\operatorname{Irr}(\alpha_i, F)$. Εξ υποθέσεως $E = F(A_1 \cup \cdots \cup A_n)$.

Για να δείξω την κανονικότητα της E/F θεωρώ τυχαίο ανάγωγο πολυώνυμο $p \in F[X]$ που έχει κάποια ρίζα του β στο E και θέλω να δείξω ότι, αν $\gamma \in C$ είναι οποιαδήποτε ρίζα του p, τότε $\gamma \in E$. Όπως και στην απόδειξη του θεωρήματος 5.12, μπορώ να βρω F-μονομορφισμό $\tau : E \to C$ με $\tau(\beta) = \gamma$. Από την υπόθεση $\beta \in E$ συμπεραίνω ότι $\beta = g(\alpha_1, \dots, \alpha_n)$ όπου $g \in F[X_1, \dots, X_n]$, άρα $\gamma = \tau(\beta) = \tau g(\tau(\alpha_1), \dots, \tau(\alpha_n))$. Αλλά $\tau g = g$ διότι ο τ αφήνει αναλλοίωτα τα στοιχεία του F και $\tau(\alpha_i) \in A_i \subseteq E$ για κάθε $i = 1, \dots, n$. Άρα $\gamma \in E$.

□

Πόρισμα 5.15. *Αν $F \leq K \leq E$ και η E/F είναι πεπερασμένη και κανονική τότε η E/K είναι κανονική.*

Απόδειξη. Αν η E/F είναι κανονική, τότε, από το Θεώρημα 5.14 το E είναι σώμα διάσπασης ενός μη μηδενικού $f \in F[X]$. Από την άσκηση 3.13 (iii), το E είναι και σώμα διάσπασης του f πάνω από το K. Πάλι από το θεώρημα 5.14, συμπεράινομε ότι η επέκταση E/K είναι κανονική. □

Galois

Ορισμός 5.16. Μια αλγεβρική επέκταση E/F λέγεται επέκταση Galois αν και μόνο αν είναι κανονική και διαχωρίσιμη.

Ορισμός 5.17. Έστω αλγεβρική επέκταση E/F και C μια αλγεβρική κλειστότητα του F (άρα και αλγεβρική κλειστότητα του E, από την άσκηση 4.29 (3)). Η ομάδα των F-αυτομορφισμών του E (με πράξη τη σύνθεση των αυτομορφισμών) λέγεται ομάδα Galois της E/F και συμβολίζεται με $\mathcal{G}(E/F)$, ή $\operatorname{Gal}(E/F)$, ή $\operatorname{Aut}(E/F)$, ή $\operatorname{Aut}_F(E)$ (σχεδόν πάντα θα χρησιμοποιούμε τον πρώτο συμβολισμό).

Θεώρημα 5.18. *Αν η E/F είναι πεπερασμένη και Galois, τότε $|\mathcal{G}(E/F)| = [E : F]$.*

Απόδειξη. Έστω C αλγεβρική κλειστότητα του E. Η E/F είναι κανονική, άρα, από το Θεώρημα 5.12, το σύνολο των F-μονομορφισμών $E \hookrightarrow C$ ταυτίζεται με το σύνολο των F-αυτομορφισμών του E, δηλαδή, με το $\mathcal{G}(E/F)$. Όμως, το πλήθος των F-μονομορφισμών $E \hookrightarrow C$ ισούται με $\{E : F\}$ και επειδή η επέκταση είναι διαχωρίσιμη, $\{E : F\} = [E : F]$ (Θεώρημα 5.4), άρα $|\mathcal{G}(E/F)| = \{E : F\} = [E : F]$. □

Θεώρημα 5.19. *Αν η επέκταση E/F είναι πεπερασμένη, τότε υπάρχει επέκταση N/E με τις εξής ιδιότητες. Η N/F είναι κανονική και ελάχιστη υπό την εξής έννοια: Αν $N \geq K \geq E$ και η K/F είναι κανονική, τότε $K = N$, δηλαδή, δεν υπάρχει γνήσιο υπόσωμα K του N που να περιέχει το E και η επέκταση K/F να είναι κανονική.*

Το N λέγεται κανονική κλειστότητα της E/F (ή κανονική κλειστότητα του E πάνω από το F)

Απόδειξη. Έστω $E = F(\alpha_1, \dots, \alpha_n)$ και $f = \text{Irr}(\alpha_1, F) \dots \text{Irr}(\alpha_n, F)$. Θεωρώ το σώμα διάσπασης του f πάνω από το E, το συμβολίζω N και θα αποδείξω ότι έχει τις απαιτούμενες ιδιότητες της εκφώνησης. Το N είναι σώμα διάσπασης του f και πάνω από το F (απόδειξη στο τέλος). Άρα από το θεώρημα 5.14 η επέκταση N/F είναι κανονική. Έστω τώρα $E \leq K \leq N$ και η K/F είναι κανονική. Θα δείξω ότι $K = N$. Συμβολίζω με $A_i = \{\alpha_i, \alpha_i', \dots\}$ το σύνολο των ριζών του $\text{Irr}(\alpha_i, F)$ $(i = 1, \dots, n)$. Έστω $\nu \in N$ και $\nu = g(\alpha_1, \alpha_1', \dots, \alpha_i, \alpha_i', \dots, \alpha_n, \alpha_n', \dots)$, όπου g είναι πολυώνυμο πολλών μεταβλητών (το πλήθος τους είναι $|A_1 \cup \dots \cup A_n|$) με τους συντελεστές του στο F. Για κάθε $i = 1, \dots, n$, το α_i ανήκει στο F και η K/F είναι κανονική, άρα όλο το σύνολο A_i περιέχεται στο K και, συνεπώς, $g(\alpha_1, \alpha_1', \dots, \alpha_i, \alpha_i', \dots, \alpha_n, \alpha_n', \dots) \in K$, δηλαδή, $\nu \in K$.

Αποδειξη του ισχυρισμού ότι το N είναι σώμα διάσπασης του f και πάνω από το F. Ξέρω ότι $N = E(A_1 \cup \dots \cup A_n)$ και μένει να δείξω ότι $N = F(A_1 \cup \dots \cup A_n)$. Αυτό είναι φανερό, διότι $E = F(\alpha_1, \dots, \alpha_i, \dots, \alpha_n)$ και κάθε α_i ανήκει στο A_i. □

Θεώρημα 5.20. *Κάθε πεπερασμένη και διαχωρίσιμη επέκταση E/F είναι απλή, δηλαδή υπάρχει $a \in E$ τ.ω. $E = F(a)$ (άρα αν $\deg(\text{Irr}(a, F))$, τότε το $1, a, \dots, a^n$ είναι βάση της επέκτασης)*

Απόδειξη. Διακρίνω δυο περιπτώσεις ανάλογα με τον αν το F είναι άπειρο ή πεπερασμένο. Εξετάζω πρώτα την περίπτωση άπειρου F, αποδεικνύοντας το θεώρημα με επαγωγή επί του βαθμού της επέκτασης.

Καταρχάς, κάθε επέκταση βαθμού 1 είναι απλή, καθώς τότε $E = F = F[1]$. Έστω $n > 1$. Υποθέτω ότι κάθε διαχωρίσιμη επέκταση βαθμού $< n$ είναι απλή. Θεωρώ διαχωρίσιμη επέκταση E/F βαθμού n και παίρνω τυχαίο $a \in E \quad F$. Τότε $[F[a] : F] > 1$. Αν $[F[a] : F] = n$, τότε τελείωσα διότι σε τετοια περίπτωση, $[E : F[a]] = 1$ άρα $E = F[a]$. Έστω $[F[a] : F] < n$. Η E/F είναι διαχωρίσιμη, άρα και η $E/F[a]$ είναι διαχωρίσιμη. Άρα, από την επαγωγική υπόθεση, εφαρμοσμένη στην $E/F[a]$. Ξέρω ότι η $E/F[a]$ είναι απλή, δηλαδή $\exists b \in E : E = (F[a])[b] = F[a, b]$. Θα δείξω ότι καθώς c διατρέχει το F, πετυχαίνω ώστε το $a + cb$ να έιναι γεννήτορας της E/F, δηλαδή για κατάλληλο $c \in F$ έχω $F(a + cb) = E$. Σίγουρα, για κάθε $c \in F$ είναι $F(a + cb) \leq E$. Διαιρευνώ ποια είναι η αναγκάια συνθήκη ώστε $F(a + cb) \lneq E$.

Η E/F είναι διαχωρίσιμη, άρα $\{E : F\} = [E : F] = n$, δηλαδή υπάρχουν ακριβώς n το πλήθος F-μονομορφισμοί $\sigma_1, \dots, \sigma_n : E \hookrightarrow C$ (όπου C αλγεβρική κλειστότητα του E που υποτίθεται ότι έχω επιλέξει). Κάθε σ_i περιορισμένος στο υπόσωμα $F(a + cb)$ είναι F-μονομορφισμός: $F(a + cb) \hookrightarrow C$. Έχω λοιπόν n τέτοιους μονομορφισμούς $\sigma_i|F(a+cb)$. Ξέρω όμως ότι το πλήθος των F-μονομορφισμών $F(a + cb) \hookrightarrow C$ είναι $\{F(a + cb) : F\} = [F(a + cb) : F] < n$ αν υποθέσω ότι $F(a + cb) \lneq E$. Άρα οι $\sigma_i|_{F(a+cb)}$ δεν είναι όλοι διαφορετικοί. Αυτό σημαίνει ότι $\exists i, j \in \{1, \dots, n\}, i \neq j$ τ.ω.

$$\sigma_i(a + cb) = \sigma_j(a + cb)$$

άρα $\sigma_i(a)+c\sigma_i(b)=\sigma_j(a)+c\sigma_j(b)$. Έχω $\sigma_i(b)\neq\sigma_j(b)$ γιατί αλλιώς θα ήταν $\sigma_i(a)=\sigma_j(a)$ και, κατά συνέπεια, $\sigma_i=\sigma_j$ σε όλο το E. Οπότε

$$c=\frac{\sigma_i(b)-\sigma_j(b)}{\sigma_i(a)-\sigma_j(a)}.$$

Δηλαδή, αναγκαία συνθήκη για να ισχύει ότι $F(a+cb)\lneq E$ είναι να ίσχυει η παραπάνω σχέση για κάποια $i,j\in\{1,\dots,n\}$ με $i\neq j$. Για δοσμένο i, οι πιθανές τιμές του $\sigma_i(a)$ είναι μέσα στις ρίζες του $\operatorname{Irr}(a,F)$ άρα είναι πεπερασμένες το πλήθος. Ανάλογα για το $\sigma_i(b)$. Επίσης, τα i,j με $i\neq j$ είναι πεπερασμένα το πλήθος. Άρα, τα πιθανά c που ικανοποιούν την παραπάνω σχέση είναι πεπερασμένα το πλήθος. Έχω υποθέσει ότι το F είναι άπειρο, άρα μπορώ να διαλέξω c που να μην ικανοποιεί την παραπάνω σχέση για κανένα ζεύγος (i,j), οπότε γι' αυτό το c, αποκλείεται η $F(a+cb)\lneq E$, δηλαδή αναγκαστικά $F(a+cb)=E$.

Αν το F είναι πεπεπρασμένο είναι γνωστό ότι η πολλαπλασιαστική ομάδα του είναι κυκλική. Άρα, σ' αυτή τη περίπτωση, αν το F είναι πεπερασμένο, τότε και το E είναι πεπερασμένο αφού η E/F είναι πεπερασμένη. (Αν $\beta_1,\dots,\beta_n$ είναι βάση της επέκτασης, τότε κάθε $e\in E$ είναι της μορφής $e=c_1\beta_1+\cdots+c_n\beta_n$ με $c_1,\dots,c_n\in F$, οπότε το πλήθος των $e\in E$ είναι $|F|^n$). Άρα, η πολλαπλασιαστική ομάδα E^* παράγεται από κάποιο $a\in E^*$ και αυτό συνεπάγεται ότι $E=\{0,1,a,\dots,a^{m-1}\}$, $|E|=m$, οπότε και $E=F(a)$. □

Παράδειγμα 5.21. $F=\mathbb{Q}, E=\mathbb{Q}[\sqrt[7]{3},\sqrt[3]{7}]$.

Μια βάση της E/F είναι $\{(\sqrt[7]{3})^i(\sqrt[3]{7})^j : 0\leq i\leq 6, 0\leq j\leq 2\}$.

$$\begin{array}{c}\mathbb{Q}[\sqrt[3]{7},\sqrt[7]{3}]\\ \Big|3\\ \mathbb{Q}[\sqrt[7]{3}]\\ \Big|7\\ \mathbb{Q}\end{array}$$

Το X^3-7 είναι ανάγωγο πάνω από το $\mathbb{Q}[\sqrt[7]{3}]$ διότι αντίθετα, αν $r\in\mathbb{Q}[\sqrt[7]{3}]$ ήταν ρίζα του, τότε $\mathbb{Q}\leq\mathbb{Q}[r]\leq\mathbb{Q}[\sqrt[7]{3}]$, άρα $7=3\cdot\left[\mathbb{Q}(\sqrt[7]{3}):\mathbb{Q}[r]\right]$, άτοπο.

Το θεώρημα μου λέει ότ $\exists a\in\mathbb{Q}[\sqrt[7]{3},\sqrt[3]{7}]$ τ.ω. $E=\mathbb{Q}[a]=\mathbb{Q}[\sqrt[7]{3},\sqrt[3]{7}]$, άρα μια βάση της επέκτασης E/F είναι η $1,a,\dots,a^{20}$. θεωρητικά η $1,a,\dots,a^{20}$ είναι πιο εύκολα διαχειρίσιμη, αλλά αν υπολογίσω το $\operatorname{Irr}(a,\mathbb{Q})$ θα έχει «άσχημους» συντελεστές.

Παρατήρηση 5.22. Έστω E/F πεπερασμένη επέκταση Galois. Μέχρι τώρα έχομε πει τα εξής:

- $\mathcal{G}(E/F)$ είναι η ομαδα των F-αυτομορφισμών του E
- Κάθε F-μονομορφισμός $E\hookrightarrow C$ είναι F-αυτομορφισμός του E, δηλαδή η εικόνα του E ταυτίζεται με το E και συνεπώς ανήκει στην $\mathcal{G}(E/F)$.
- $|\mathcal{G}(E/F)|=[E:F]$.

Ορισμός 5.23. Έστω E/F επέκταση Galois. Συμβολίζω με $\mathcal{E}$ το σύνολο των σωμάτων K με $F\leq K\leq E$ (συμπεριλαμβανομένων και των F,E). Αυτά τα K λέγονται *ενδιάμεσες (μεταξύ F και E) επεκτάσεις*.

Συμβολίζω επίσης με $\mathcal{O}$ το σύνολο των υποομάδων της $G:=\mathcal{G}(E/F)$.

Μεταξύ των $\mathcal{E}$ και $\mathcal{O}$ ορίζω τις απεικονίσεις

$$K \in \mathcal{E} \overset{\mathcal{G}(E/\bullet)}{\longmapsto} \mathcal{G}(E/K) \in \mathcal{O}$$
$$H \in \mathcal{O} \overset{\mathcal{F}(\bullet)}{\longmapsto} \in \mathcal{F}(H) \coloneqq \{a \in E : \sigma(a) = a \forall \sigma \in \mathcal{F}(H)\} \in \mathcal{E}$$

Για να ισχυριστώ ότι αυτές οι αντιστοιχίες είναι καλά ορισμένες, πρέπει να δείξω ότι το σύνολο $\mathcal{G}(E/K)$ είναι υποομάδα της $\mathcal{G}(E/F)$ και το σύνολο $\mathcal{F}(H)$ είναι ενδιάμεση (μεταξύ F και E) επέκταση (άσκηση 5.26).

Πρόταση 5.24. *Έστω E/F επέκταση Galois και $G = \mathcal{G}(E/F)$. Τότε ισχύουν τα εξής:*

α΄) Αν $F \leq K \leq E$, τότε $\mathcal{F}(\mathcal{G}(E/K)) \geq K$

β΄) Αν $H \leq \mathcal{G}(E/F)$, τότε $\mathcal{G}(E/\mathcal{F}(H)) \geq H$

γ΄) Αν $F \leq K_1 \leq K_2 \leq E$ τότε $\mathcal{G}(E/K_1) \geq \mathcal{G}(E/K_2)$

δ΄) Αν $H_1 \leq H_2 \leq G = \mathcal{G}(E/F)$ τότε $\mathcal{F}(H_1) \geq \mathcal{F}(H_2)$

Απόδειξη. Άσκηση 5.27. □

Πρόταση 5.25. *Αν E/F είναι πεπερασμένη επέκταση Galois, τότε*

1) $\mathcal{F}(\mathcal{G}(E/F)) = F$

2) Αν $H \lneqq G$ τότε $\mathcal{F}(H) \gneqq F$

Απόδειξη. 1) Έστω $F_0 \coloneqq \mathcal{F}(\mathcal{G}(E/F))$. Τότε, $F_0 \geq F$ (λόγω του (α΄)) άρα $\mathcal{G}(E/F_0) \leq \mathcal{G}(E/F)$ (λόγω του (γ΄)). Αντίστροφα, $\mathcal{G}(E/F_0) = \mathcal{G}(E/\mathcal{F}(\mathcal{G}(E/F))) \geq \mathcal{G}(E/F)$ (λόγω του (β΄)). Άρα, τελικά, $\mathcal{G}(E/F_0) = \mathcal{G}(E/F)$.

Επίσης, η E/F είναι κανονική και διαχωρίσιμη άρα το ίδιο ισχύει και για την E/F_0, συνεπώς, η E/F_0 είναι Galois. Άρα $|\mathcal{G}(E/F_0)| = [E : F_0]$. Έπεται ότι $[E : F] = |\mathcal{G}(E/F)| = |\mathcal{G}(E/F_0)| = [E : F_0]$ και, συνεπώς, $[F_0 : F] = 1$, οπότε $F = F_0$.

2) Έστω $H \lneqq G$ και $\mathcal{F}(H) = F$.Θα οδηγηθώ σε άτοπο. Αφού η E/F είναι απλή, υπάρχει $a \in E$ τέτοιο ώστε $E = F(a)$. Θεωρώ το εξής πολυώνυμο:

$$f = \prod_{\sigma \in H} (X - \sigma(a)) \in E[X].$$

Έστω $\tau \in H$. Τότε θεωρώντας την επέκταση του τ στον $E[X]$, έχω

$$\tau f = \prod_{\sigma \in H} (X - \tau\sigma(a)) = f,$$

καθώς $\{\tau\sigma : \sigma \in H\} = \{\sigma : \sigma \in H\}$. Δηλαδή κάθε συντελεστής του f μένει αναλλοίωτος από κάθε $\tau \in H$, που σημαίνει ότι κάθε συντελεστής του f ανήκει στο $\mathcal{F}(H)$. Εξ υποθέσεως, αυτό είναι το F, άρα $f \in F[X]$. Αλλά $f(a) = 0$ (διότι για $\sigma = id_E$, $\sigma(a) = a$) άρα $\operatorname{Irr}(a, F) \mid f$ στο $F[X]$, οπότε $\deg \operatorname{Irr}(a, F) \leq \deg f$. Από τον τρόπο που ορίσθηκε το g, είναι $\deg f = |H| < |G|$ (η γνήσια ανισότητα ισχύει γιατί η H είναι γνήσια υποομάδα της πεπερασμένης ομάδας G). Άρα,

$$|G| > |H| \geq \deg \operatorname{Irr}(a, F) = [F(a) : F] = [E : F] = |\mathcal{G}(E/F)| = |G|,$$

άτοπο.

□

Ασκήσεις

Άσκηση 5.26. Με τους συμβολισμούς του Ορισμού 5.23 αποδείξτε ότι το σύνολο $\mathcal{G}(E/K)$ είναι υποομάδα της $\mathcal{G}(E/F)$ και το σύνολο $\mathcal{F}(H)$ είναι ενδιάμεση (μεταξύ F και E) επέκταση.

Άσκηση 5.27. Αποδείξτε την Πρόταση 5.24.

Άσκηση 5.28. Έστω $a = \sqrt{2} + \sqrt{3}$.

(i) Υπολογίστε ένα τεταρτοβάθμιο πολυώνυμο $f \in \mathbb{Q}[X]$, το οποίο έχει ρίζα το a.

(ii) Αποδείξτε ότι ρίζες του f είναι, επίσης, οι $\sqrt{2} - \sqrt{3}$, $-\sqrt{2} + \sqrt{3}$ και $-\sqrt{2} - \sqrt{3}$ και δείξτε ότι το $\mathbb{Q}(a)$ είναι επέκταση του $\mathbb{Q}(\sqrt{2})$ και του $\mathbb{Q}(\sqrt{3})$.

(iii) Αποδείξτε ότι $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(a)$.

(iv) Γιατί η επέκταση $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ είναι Galois;

Άσκηση 5.29. Έστω $b = \sqrt[3]{2} + \sqrt{3}$.

(i) Υπολογίστε ένα εκτοβάθμιο πολυώνυμο $g \in \mathbb{Q}[X]$, το οποίο έχει ρίζα το b.

(ii) Αποδείξτε ότι το g έχει, επίσης, ρίζα το $c = \sqrt[3]{2} - \sqrt{3}$ (υπάρχει «έξυπνος» τρόπος να το αποδείξετε, δίχως πράξεις) και δείξτε ότι το $\mathbb{Q}(b)$ είναι επέκταση του $\mathbb{Q}(\sqrt[3]{2})$ και του $\mathbb{Q}(\sqrt{3})$.

(iii) Αποδείξτε ότι $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) = \mathbb{Q}(b)$.

(iv) Γιατί το πολυώνυμο g είναι ανάγωγο πάνω από το $\mathbb{Q}$;

(v) Γιατί η επέκταση $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})/\mathbb{Q}$ δεν είναι Galois;