

## Κεφάλαιο 9

### 9.1 9<sup>η</sup> Εβδομάδα

#### Επεκτάσεις κυκλικές και Kummer

**Πρόταση 9.1.** Έστω σώμα  $K$  και  $\sigma_1, \dots, \sigma_n$  διαφορετικοί αυτομορφισμοί του  $K$ , τότε αυτοί είναι  $K$ -γραμμικώς ανεξάρτητοι. Δηλαδή, αν  $\lambda_1, \dots, \lambda_n \in K$  και  $\lambda_1\sigma_1 + \dots + \lambda_n\sigma_n = 0$ <sup>1</sup>, τότε  $\lambda_1 = \lambda_2 = \dots = \lambda_n = 0$ .

*Απόδειξη.* Επαγωγικά επί του  $n$ . Αν  $\lambda_1\sigma_1 = 0$ , τότε  $\lambda_1\sigma_1(1) = 0$ . Αλλά  $\sigma(1) = 1$ , άρα  $\lambda_1 = 0$ .

Έστω  $n > 1$ . Υποθέτω ότι η πρόταση ισχύει για οποιουδήποτε διαφορετικούς αυτομορφισμούς του  $K$  που το πλήθος τους είναι  $< n$ . Θεωρώ  $n$  διαφορετικούς αυτομορφισμούς  $\sigma_1, \dots, \sigma_n$  του  $K$  και υποθέτω ότι υπάρχουν  $\lambda_1, \dots, \lambda_n \in K$ , όχι όλα 0, τέτοια ώστε

$$\lambda_1\sigma_1 + \dots + \lambda_n\sigma_n = 0 \quad (9.1)$$

Μπορώ να υποθέσω ότι  $\lambda_i \neq 0$  για κάθε  $i$ , διότι, αν π.χ.  $\lambda_n = 0$ , τότε  $\lambda_1\sigma_1 + \dots + \lambda_{n-1}\sigma_{n-1} = 0$ , άρα, από επαγωγική υπόθεση,  $\lambda_1 = \dots = \lambda_{n-1} = 0$ .

Επειδή  $\sigma_n \neq \sigma_1$ , έπεται ότι  $\exists \alpha \in K : \sigma_n(\alpha) \neq \sigma_1(\alpha)$ . Από την υπόθεση,

$$\lambda_1(u) + \dots + \lambda_{n-1}\sigma_{n-1}(u) + \lambda_n\sigma_n(u) = 0, \quad \forall u \in K$$

Διαιρώ με  $\lambda_n$  και θέτω  $c_i = \lambda_i/\lambda_n$ , οπότε

$$c_1\sigma_1(u) + \dots + c_{n-1}\sigma_{n-1}(u) + \sigma_n(u) = 0.$$

Θέτοντας στην τελευταία ισότητα το  $\alpha u$  στη θέση του  $u$  παίρνω και τη σχέση

$$c_1\sigma_1(\alpha)\sigma_1(u) + \dots + c_{n-1}\sigma_{n-1}(\alpha)\sigma_{n-1}(u) + \sigma_n(\alpha)\sigma_n(u) = 0 \quad \forall u \in K.$$

Είναι  $\sigma_n(\alpha) \neq 0$ <sup>2</sup>. Πολλαπλασιάζω την προ-τελευταία σχέση με  $\sigma_n(\alpha)$  και την αφαιρώ από την τελευταία, οπότε παίρνω

$$c_1(\sigma_1(\alpha) - \sigma_n(\alpha))\sigma_1(u) + \dots + c_{n-1}(\sigma_{n-1}(\alpha) - \sigma_n(\alpha))\sigma_{n-1}(u) = 0 \quad \forall u \in K.$$

Αυτή η σχέση λέει ότι

$$c_1(\sigma_1(\alpha) - \sigma_n(\alpha))\sigma_1 + \dots + c_{n-1}(\sigma_{n-1}(\alpha) - \sigma_n(\alpha))\sigma_{n-1} = 0,$$

---

<sup>1</sup> Η μηδενική απεικόνιση  $K \rightarrow K$ .

<sup>2</sup>  $\sigma_n(\alpha) = 0 \iff \alpha = 0 \iff \sigma_1(\alpha) = 0$ .

δηλαδή έχω γραμμικό συνδιασμό  $n-1$  διαφορετικών αυτομορφισμών να είναι 0, άρα, από την επαγωγική υπόθεση, όλοι οι συντελεστές είναι 0. Επιπλέον, καθώς  $\sigma_1(\alpha) \neq \sigma_n(\alpha)$ , πρέπει  $c_1 = 0$ , άρα  $\lambda_1 = 0$ , οπότε, λόγω της (9.1),  $\lambda_2\sigma_2 + \dots + \lambda_n\sigma_n = 0$ . Λόγω της επαγωγικής υπόθεσης, η σχέση αυτή συνεπάγεται ότι  $\lambda_i = 0$  για κάθε  $i$ .  $\square$

### Κυκλικές επεκτάσεις

**Ορισμός 9.2.** Μια πεπερασμένη επέκταση  $E/F$  λέμε ότι είναι κυκλική αν και μόνο αν είναι Galois και η  $\mathcal{G}(E/F)$  είναι κυκλική.

**Θεώρημα 9.3.** Έστω σώμα  $F$ ,  $n \in \mathbb{N}$  και  $\omega \in F$  πρωταρχική  $n$ -οστή ρίζα της μονάδας. Έστω  $f = X^n - \alpha$ , όπου  $\alpha \in F$ , και  $E$  το σώμα διάσπασης του  $f$  πάνω από το  $F$ . Τότε η επέκταση  $E/F$  είναι κυκλική και  $|\mathcal{G}(E/F)|$  διαιρεί το  $n$ . Ισχύει επίσης ότι  $|\mathcal{G}(E/F)| = n$  αν και μόνο αν το  $f$  ανάγωγο πάνω από το  $F$ .

*Απόδειξη.* Έστω  $\theta \in E$  κάποια ρίζα του  $f$ . Τότε όλες οι ρίζες του  $f$  είναι  $\theta, \omega\theta, \dots, \omega^{n-1}\theta$  όλες διαφορετικές αν  $\alpha \neq 0$ . Άρα το  $f$  είναι διαχωρίσιμο, άρα η  $E/F$  είναι Galois ως σώμα διάσπασης διαχωρίσιμου πολωνύμου. Θεωρώ την εξής απεικόνιση ομάδων

$$\psi : \mathcal{G}(E/F) \rightarrow \mathbb{Z}_n,$$

που ορίζεται ως εξής:  $\psi(\sigma) = k \pmod{n}$  εξ ορισμού αν  $\sigma(\theta) = \omega^k\theta$ . Αφού ο  $\sigma$  είναι  $F$ -αυτομορφισμός του  $E$ , το  $\theta$  πρέπει να το στέλνει σε ρίζα του  $f$ , άρα σε κάποιο  $\omega^k\theta$ . Το  $k$  είναι μονοσήμαντα ορισμένο  $\pmod{n}$ , διότι αν  $\sigma(\theta) = \omega^k\theta = \omega^l\theta$  τότε  $\omega^{k-l} = 1$ , οπότε  $n \mid k-l$ . Άρα η  $\psi$  είναι καλά ορισμένη. Επίσης, η  $\psi$  είναι ομομορφισμός ομάδων. Πράγματι, αν  $\psi(\sigma) \equiv k$  και  $\psi(\tau) \equiv l \pmod{n}$ , τότε  $\sigma\tau(\theta) = \sigma(\omega^l\theta) = \sigma(\omega)^l\sigma(\theta) = \omega^l\omega^k\theta$  αφού  $\omega \in F$  άρα  $\psi(\sigma\tau) = k+l = \psi(\sigma) + \psi(\tau)$ . Τέλος, η  $\psi$  είναι 1-1, διότι, αν  $\psi(\sigma) = 0$ , τότε  $\sigma(\theta) = \theta = \omega^0\theta$ , άρα  $\psi(\sigma) = 0 \pmod{n}$ , οπότε η  $\psi$  έχει τετριμμένο πυρήνα.

Καθώς η  $\psi$  είναι μονομορφισμός, η  $\mathcal{G}(E/F)$  είναι ισόμορφη με την εικόνα της μέσω του  $\psi$ , η οποία είναι υποομάδα της κυκλικής ομάδας  $\mathbb{Z}_n$ , άρα είναι κυκλική (υποομάδα κυκλικής ομάδας) και έχει τάξη που διαιρεί το  $n$  από το θεώρημα του Lagrange.

Τέλος,  $|\mathcal{G}(E/F)| = [E:F] = [F(\theta):F] = \deg(\text{Irr}(\theta, F))$ . Επειδή το  $f$  έχει ρίζα το  $\theta$ , ισχύει ότι  $\text{Irr}(\theta, F) \mid f$ , άρα  $n = |\mathcal{G}(E/F)| \iff \deg(\text{Irr}(\theta, F)) = n = \deg f \iff \text{Irr}(\theta, F) = f \iff f$  ανάγωγο.  $\square$

**Θεώρημα 9.4** (Αντίστροφο του Θεωρήματος 9.3). Έστω ότι η  $E/F$  είναι κυκλική επέκταση βαθμού  $n$  και το  $F$  περιέχει μία πρωταρχική  $n$ -οστή ρίζα της μονάδας, τότε υπάρχει κάποιο  $\alpha \in F$ , τέτοιο ώστε το  $E$  να είναι σώμα διάσπασης του ανάγωγου πολωνύμου  $f = X^n - \alpha$ .

*Απόδειξη.* Έστω  $\omega \in F$  πρωταρχική  $n$ -οστή ρίζα της μονάδας. Εξ υποθέσεως η ομάδα Galois είναι κυκλική, άρα  $\mathcal{G}(E/F) = \langle \sigma \rangle$  για κάποιο  $\sigma \in \mathcal{G}(E/F)$  με  $\text{ord}(\sigma) = |\mathcal{G}(E/F)| = [E:F] = n$ . Άρα οι  $\text{id}, \sigma, \dots, \sigma^{n-1}$  είναι διαφορετικοί. Από την Πρόταση 9.1, αυτοί οι αυτομορφισμοί είναι γραμμικώς ανεξάρτητοι, άρα  $\exists \beta \in E$  τέτοιο ώστε

$$\theta := \beta + \omega\sigma(\beta) + \dots + \omega^{n-1}\sigma^{n-1}(\beta) \neq 0.$$

Υπολογίζω  $\sigma(\theta) = \sigma(\beta) + \omega\sigma^2(\beta) + \dots + \omega^{n-2}\sigma^{n-1}(\beta) + \omega^{n-1}\beta$ , άρα  $\sigma(\theta) = \omega^{-1}\theta$ . Έπεται ότι  $\sigma(\theta^n) = (\sigma(\theta))^n = \theta^n$  οπότε  $\theta^n \in \mathcal{F}(\langle \sigma \rangle) = \mathcal{F}(\mathcal{G}(E/F)) = F$ , συνεπώς,  $\alpha := \theta^n \in F$ . Θεωρώ το πολώνυμο  $f = X^n - \alpha \in F[X]$ , το οποίο έχει ρίζα το  $\theta$ .

Αφού  $\omega \in F$ , όλες οι ρίζες του  $f$ , δηλαδή οι  $\theta, \omega\theta, \dots, \omega^{n-1}\theta$  ανήκουν στο  $E$ . Άρα το σώμα διάσπασης του  $f$  πάνω από το  $F$  είναι το  $F(\theta)$ . Είναι  $\theta \in E$ , άρα  $F(\theta) \leq E$ . Μένει να δείξω ότι ισχύει η ισότητα.

Είδαμε πριν ότι  $\sigma(\theta) = \omega^{-1}\theta \in F(\theta)$ , άρα, αν θέσω  $\tau = \sigma|_{F(\theta)}$ , τότε ο  $\tau$  είναι  $F$ -μονομορφισμός του  $F(\theta)$ . Η επέκταση  $F(\theta)/F$  είναι Galois ως σώμα διάσπασης του διαχωρίσιμου  $f$ , άρα ο  $\tau$  είναι  $F$ -αυτομορφισμός του  $F(\theta)$ , δηλαδή  $\tau \in \mathcal{G}(F(\theta)/F)$ . Επίσης,  $[F(\theta):F] = |\mathcal{G}(F(\theta)/F)|$ . Θα δείξω στο

τέλος ότι οι  $id, \tau, \dots, \tau^{n-1}$  είναι διαφορετικοί, άρα η  $\mathcal{G}(F(\theta)/F)$  έχει τάξη τουλάχιστον  $n$ . Συνεπώς,  $[F(\theta) : F] = |\mathcal{G}(F(\theta)/F)| \geq n$ . Λόγω της  $F(\theta) \leq E$  είναι και  $[F(\theta) : F] \leq n$ , άρα  $[F(\theta) : F] = n$  και, συνεπώς,  $E = F(\theta)$ .

Μένει να δείξω ότι οι  $id, \tau, \dots, \tau^{n-1}$  είναι διαφορετικοί. Αν ήταν  $\tau^k = \tau^l$  για κάποια  $0 \leq l < k \leq n-1$ , τότε  $\tau^k(\theta) = \tau^l(\theta)$ , άρα  $\sigma^k(\theta) = \sigma^l(\theta)$ . Επειδή  $\sigma(\theta) = \omega^{-1}\theta$ ,  $\sigma^k(\theta) = \omega^{-k}\theta = \omega^{-l}\theta = \sigma^l(\theta)$ , άρα  $\omega^{k-l} = 1$  με  $1 \leq k-l < n$  άτοπο, διότι  $\text{ord}(\omega) = n$ .  $\square$

### Επεκτάσεις Kummer

**Ορισμός 9.5.** Μία πεπερασμένη επέκταση Galois, της οποίας η ομάδα Galois είναι αβελιανή ονομάζεται επέκταση Kummer

**Θεώρημα 9.6.** Έστω  $n \in \mathbb{N}$ ,  $F$  σώμα που περιέχει κάποια  $n$ -οστή ρίζα της μονάδας,  $\alpha_1, \dots, \alpha_r \in F$ ,  $f = (X^n - \alpha_1) \cdots (X^n - \alpha_r)$  και  $E$  το σώμα διάσπασης του  $f$  πάνω από το  $F$ . Τότε η  $E/F$  είναι επέκταση Kummer και  $\sigma^n = id_E$  για κάθε  $\sigma \in \mathcal{G}(E/F)$ .

*Απόδειξη.* Για  $i = 1, \dots, r$ , έστω  $\theta_i \in E$  με  $\theta_i^n = \alpha_i$ . Οι ρίζες του  $f$  είναι οι  $\omega^j \theta_i$  για  $i = 1, \dots, r$  και  $j = 0, \dots, n-1$  και  $E = F(\theta_1, \dots, \theta_r)$ . Έστω  $\sigma \in \mathcal{G}(E/F)$ . Τότε  $\sigma(\theta_i) = \omega^{k_i} \theta_i$  όπου τα  $k_i$  είναι μονοσημάντως ορισμένα mod  $n$ . Ας πάρω και άλλο ένα  $\tau \in \mathcal{G}(E/F)$ . Θα δείξω ότι  $\sigma\tau = \tau\sigma$ .

Έστω ότι  $\tau(\theta_i) = \omega^{l_i} \theta_i$ . Τότε,

$$\sigma\tau(\theta_i) = \sigma(\omega^{l_i} \theta_i) = \omega^{l_i} \omega^{k_i} \theta_i = \omega^{l_i + k_i} \theta_i$$

Όμοιως,  $\tau\sigma(\theta_i) = \omega^{k_i + l_i} \theta_i$ , άρα  $\sigma\tau(\theta_i) = \tau\sigma(\theta_i)$  για  $i = 1, \dots, r$  και, τελικά,  $\sigma\tau = \tau\sigma$ , άρα η επέκταση είναι Kummer. Προφανώς,  $\sigma^n = id$  γιατί, αν  $\sigma(\theta_i) = \omega^{k_i} \theta_i$ , τότε  $\sigma^n(\theta_i) = \omega^{nk_i} \theta_i = \theta_i = id_E(\theta_i)$  για κάθε  $i = 1, \dots, r$ .  $\square$

**Υπενθύμιση 9.7.** Έστω ότι  $(G_i, \cdot)_{i=1, \dots, n}$  είναι αβελιανές ομάδες με ουδέτερα στοιχεία  $e_i$ . Το καρτεσιανό γινόμενο  $G = \prod_{i=1}^n G_i = G_1 \times G_2 \times \cdots \times G_n$ , εφοδαδιασμένο με τον πολλαπλασιασμό κατά συντεταγμένη είναι ομάδα. Η ομάδα  $G_i$  είναι ισόμορφη με την (κανονική) υποομάδα  $\{e_1\} \times \cdots \times G_i \times \cdots \times \{e_n\}$  της  $G$ , οπότε, όταν γράφομε, π.χ.  $G_1 \times G_2 / G_1$ , εννοούμε την ομάδα-πηλίκο  $G_1 \times G_2 / G_1 \times \{e_2\}$ .

Αντίστοιχα, η (κανονική) υποομάδα  $H_i := G_1 \times \cdots \times G_{i-1} \times \{e_i\} \times G_{i+1} \times \cdots \times G_n$  της  $G$  ταυτίζεται με την  $H_i \cong \prod_{j=1, j \neq i}^n G_j$  και  $G/H_i \cong G_i$ .

1<sup>η</sup> Παρατήρηση:  $\bigcap_{i=1}^n H_i = \{e_1, \dots, e_n\}$ , δηλαδή,  $\bigcap_{i=1}^n H_i$  είναι η τετριμμένη υποομάδα της  $G$ .

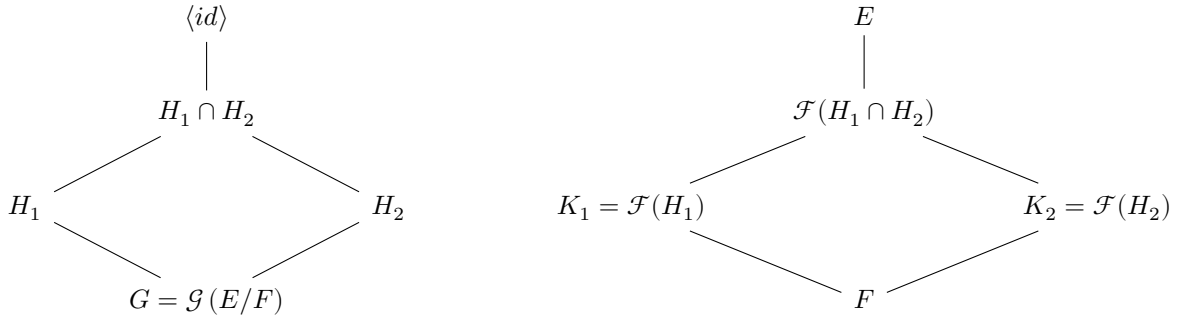
Το Θεμελιώδες Θεώρημα των Πεπερασμένων Παραγόμενων Αβελιανών Ομάδων λέει το εξής: Αν η  $G$  είναι (πεπερασμένα παραγόμενη) αβελιανή ομάδα, τότε  $G \cong C_1 \times \cdots \times C_\mu \times \mathbb{Z}^\nu$ , όπου  $C_i$  πεπερασμένη κυκλική ομάδα, δηλαδή αν  $|C_i| = m_i$ ,  $C_i \cong \mathbb{Z}_{m_i}$ . Προφανώς τα  $\mu$  και  $\nu$  μπορεί να είναι 0. Η υποομάδα  $\text{Tors}(G) = C_1 \times \cdots \times C_\mu \times \langle 0 \rangle^\nu$ , την οποία ταυτίζουμε με την ισόμορφη της  $C_1 \times \cdots \times C_\mu$ , ονομάζεται υποομάδα στρέψεως της  $G$ , ενώ η υποομάδα  $\langle 0_1 \rangle \times \cdots \times \langle 0_\mu \rangle \times \mathbb{Z}^\nu$ , την οποία ταυτίζουμε με την ομάδα  $\mathbb{Z}^\nu$ , ονομάζεται ελεύθερο μέρος της ομάδας  $G$  και ο αριθμός  $\nu$  λέγεται βαθμίδα (rank) της  $G$ .

Το  $\mu$  είτε το  $\nu$  δεν αποκλείεται να είναι 0. Στην περίπτωση πεπερασμένων αβελιανών ομάδων  $G$ , είναι, προφανώς,  $\nu = 0$ .

2<sup>η</sup> Παρατήρηση: Έστω  $G \cong C_1 \times \cdots \times C_\mu \times \mathbb{Z}^\nu$  όπως παραπάνω, με  $\mu > 0$  και  $|C_i| := d_i$  ( $i = 1, \dots, \mu$ ). Τότε  $C_i \cong \mathbb{Z}_{d_i}$ . Αν σταθεροποιήσουμε το  $i$  και θεωρήσουμε το στοιχείο  $(0, \dots, 0, 1, 0, \dots, 0)$  της ομάδας  $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_i} \times \cdots \times \mathbb{Z}_{d_\mu}$ , αυτό, προφανώς, έχει τάξη  $d_i$ . Άρα, η  $G$  περιέχει στοιχείο με τάξη  $d_i$ .

**Λήμμα 9.8.** Έστω  $E/F$  πεπερασμένη επέκταση Galois και  $K_1, K_2$  ενδιάμεσες επεκτάσεις, με αντίστοιχες ομάδες (μέσω της αντιστοιχίας Galois)  $H_1, H_2$ . Τότε το σώμα που αντιστοιχεί στην υποομάδα  $H_1 \cap H_2$  είναι το  $K_1 K_2$ , η λεγόμενη σύνθεση (compositum) των  $K_1 K_2$ , δηλαδή το ελάχιστο υπόσωμα του  $E$  που περιέχει το  $K_1 \cup K_2$ .

Απόδειξη. Έχω το εξής διάγραμμα υποομάδων και σωμάτων



και θέλω να δείξω ότι  $\mathcal{F}(H_1 \cap H_2) = K_1 K_2$ . Είναι  $H_1 \cap H_2 \leq H_1$ , άρα  $\mathcal{F}(H_1 \cap H_2) \geq \mathcal{F}(H_1) = K_1$  για  $i = 1, 2$ . Συνεπώς,  $\mathcal{F}(H_1 \cap H_2) \supseteq K_1 \cup K_2$  άρα και  $\mathcal{F}(H_1 \cap H_2) \geq K_1 K_2$ .

Αντίστροφα,  $K_i \leq K_1 K_2$  για  $i = 1, 2$  άρα  $H_i = \mathcal{G}(E/K_i) \geq \mathcal{G}(E/K_1 K_2)$  οπότε  $H_1 \cap H_2 \geq \mathcal{G}(E/K_1 K_2)$  άρα  $\mathcal{F}(H_1 \cap H_2) \leq \mathcal{F}(\mathcal{G}(E/K_1 K_2)) = K_1 K_2$ .  $\square$

Το Λήμμα γενικεύεται, δίχως δυσκολία, και για περισσότερες από δύο υποομάδες.

Τώρα μπορούμε να αποδείξουμε το (περίπου) αντίστροφο του Θεωρήματος 9.6.

**Θεώρημα 9.9.** Έστω  $n \in \mathbb{N}$  και  $F$  ένα σώμα που περιέχει κάποια πρωταρχική  $n$ -οστή ρίζα της μονάδας. Έστω  $E/F$  επέκταση Kummer,  $G = \mathcal{G}(E/F)$  και ισχύει  $\sigma^n = id$  για κάθε  $\sigma \in G$ . Τότε, υπάρχουν κάποια  $\alpha_1, \dots, \alpha_r \in F$  τ.ω. το  $E$  να είναι το σώμα διάσπασης του  $f = (X^n - \alpha_1) \cdots (X^n - \alpha_r)$ .

Απόδειξη. Η  $G$  είναι πεπερασμένη αβελιανή, ομάδα, άρα  $G \cong C_1 \times \cdots \times C_r$  όπου  $C_i$  πεπερασμένη κυκλική με  $|C_i| := d_i$ . Για  $i = 1, \dots, r$ , έστω  $H_i := \prod_{j \neq i} C_j \trianglelefteq G$ . Σύμφωνα με την υπενθύμιση 9.7, είναι  $G/H_i \cong C_i$ .

Επίσης, έστω  $\mathcal{F}(H_i) := K_i$ . Από το Θεμελιώδες Θεώρημα Galois 6.9 η  $K_i/F$  είναι Galois και  $\mathcal{G}(K_i/F) \cong G/H_i \cong C_i$ . Άρα, για κάθε  $i = 1, \dots, r$ , η επέκταση  $K_i/F$  είναι κυκλική και  $[K_i : F] = |\mathcal{G}(K_i/F)| = |C_i| = d_i$ . Από το Θεώρημα 9.6, το  $K_i$  είναι σώμα διάσπασης του πολυνύμου  $X^{d_i} - \beta_i$  για κάποιο  $\beta_i \in F$  και, μάλιστα,  $K_i = F(\theta_i)$ , όπου  $\theta_i^{d_i} = \beta_i$ .

Τώρα, από τη 2<sup>η</sup> παρατήρηση της υπενθύμισης 9.7, η  $G$  έχει ένα στοιχείο, έστω  $\tau$ , τάξεως  $d_i$  και, λόγω της υπόθεσης,  $\tau^n = id_E$ . Άρα  $d_i | n$ , οπότε  $n/d_i \in \mathbb{N}$  και θέτω  $\alpha_i := \beta_i^{n/d_i}$ . Έτσι,  $\theta_i^n = (\theta_i^{d_i})^{n/d_i} = \beta_i^{n/d_i} = \alpha_i$ , άρα το  $\theta_i$  είναι ρίζα του  $X^n - \alpha_i \in F[X]$ .

Προφανώς,  $F(\theta_1, \dots, \theta_r)$  είναι το σώμα διάσπασης του  $f = (X^n - \alpha_1) \cdots (X^n - \alpha_r)$  και μένει να δείξω ότι  $E = F(\theta_1, \dots, \theta_r)$ .

Το  $F(\theta_1, \dots, \theta_r)$  είναι το ελάχιστο υπόσωμα του  $E$  που περιέχει το σύνολο  $F \cup \{\theta_1, \dots, \theta_r\}$ , άρα  $F(\theta_1, \dots, \theta_r) = K_1 K_2 \cdots K_r$ . Από το Λήμμα 9.8,  $\mathcal{G}(E/K_1 \cdots K_r) = H_1 \cap \cdots \cap H_r = \langle id_E \rangle$ , όπου η τελευταία ισότητα ισχύει σύμφωνα με την 1<sup>η</sup> παρατήρηση της υπενθύμισης 9.7. Άρα,  $K_1 \cdots K_r = \mathcal{F}(\mathcal{G}(E/K_1 \cdots K_r)) = \mathcal{F}(\langle id_E \rangle) = E$ , συνεπώς,  $F(\theta_1, \dots, \theta_r) = K_1 \cdots K_r = E$ .  $\square$

### Ασκήσεις

**Άσκηση 9.10.** Έστω  $n \in \mathbb{N}$ , σώμα  $F$  του οποίου η χαρακτηριστική είναι 0 ή  $p$  με  $p \nmid n$ ,  $c \in F \setminus \{0\}$  και  $E$  σώμα διάσπασης του  $X^n - c$ . Αποδείξτε ότι το  $E$  περιέχει πρωταρχική  $n$ -οστή ρίζα της μονάδας.

**Άσκηση 9.11.** Έστω πρώτος  $p$ , σώμα  $F$  του οποίου η χαρακτηριστική δεν είναι  $p$ ,  $c \in F \setminus \{0\}$ ,  $E$  σώμα διάσπασης του  $f = X^p - c$  και  $\omega \in E$  πρωταρχική  $p$ -οστή ρίζα της μονάδας (η ύπαρξή της εξασφαλίζεται

από την άσκηση 9.10). Υποθέτουμε ότι το  $f$  δεν είναι ανάγωγο πάνω από το  $F$  και  $g \in F[X]$  είναι κάποιος ανάγωγος παράγοντας του  $f$ , με  $\deg g = d$  ( $1 \leq d < p$ ). Τέλος, έστω  $\theta \in E$  ρίζα του  $g$ . Σε καθένα από τα παρακάτω ερωτήματα ισχύουν όλες οι υποθέσεις που προαναφέρθηκαν. Αποδείξτε τα εξής:

- (1) Έστω  $c_0$  το γινόμενο των ριζών του  $g$ . Δείξτε ότι  $c_0 \in F$  και  $c_0^p = c^d$ .
- (2) Παρατηρήστε ότι, καθώς  $(d, p) = 1$ , υπάρχουν ακέραιοι  $a, b : ad + bp = 1$  και χρησιμοποιήστε αυτή τη σχέση, σε συνδυασμό με το (1), για να αποδείξετε ότι το  $f$  έχει ρίζα στο  $F$ .
- (3) Χρησιμοποιήστε το (2) και αποδείξτε ότι  $E = F(\omega)$ .
- (4) Αποδείξτε ότι το  $f$  διασπάται στο  $F$  αν και μόνο αν  $\omega \in F$ . (Το  $f$  έχει υποτεθεί μη ανάγωγο πάνω από το  $F$ , αλλά το ερώτημα αυτό εξετάζει πότε το  $f$  αναλύεται πλήρως σε πρωτοβάθμιους παράγοντες του  $f$ .)

**Άσκηση 9.12.** Έστω σώμα  $F$  χαρακτηριστικής  $p$ ,  $E/F$  κυκλική επέκταση (άρα Galois) βαθμού  $p$  και  $\sigma$  γεννήτορας της  $\mathcal{G}(E/F)$ . Θεωρήστε δεδομένο ότι υπάρχει  $\theta \in E : \sigma(\theta) = \theta + 1$  (η ύπαρξή του εξασφαλίζεται από το λεγόμενο «Θεώρημα 90 του Hilbert»). Αποδείξτε τα εξής:

- (1) Εξηγήστε γιατί η  $F(\theta)/F$  είναι Galois. Έστω  $\tau = \sigma|_{F(\theta)}$ . Αποδείξτε ότι ο μονομορφισμός  $\tau : F(\theta) \rightarrow E$  είναι στοιχείο της  $\mathcal{G}(F(\theta)/F)$  και  $\text{ord}(\tau) = p$ . Βάσει αυτού αποδείξτε ότι  $E = F(\theta)$ .
- (2) Αποδείξτε ότι το  $\theta$  είναι ρίζα κάποιου πολωνύμου  $f = X^p - X - a \in F[X]$  και το  $f$  είναι ανάγωγο πάνω από το  $F$ .

**Άσκηση 9.13.** Έστω σώμα  $F$  χαρακτηριστικής  $p$  και  $E$  σώμα διάσπασης του  $f = X^p - X - a \in F[X]$ , όπου  $a \neq 0$ . Αποδείξτε τα εξής:

- (1) Αν  $\theta \in E$  είναι ρίζα του  $f$ , τότε  $f(\theta + b) = 0$  για κάθε  $b \in \mathbb{F}_p$ . Βάσει αυτού δείξτε ότι  $E = F(\theta)$  και η  $E/F$  είναι διαχωρίσιμη.
- (2) Δείξτε ότι, αν  $g \in F[X]$  είναι ανάγωγος παράγον του  $f$ , τότε  $\deg g = 1$  ή  $p$ . Άρα, αν  $\deg g = 1$ , τότε  $E = F$ , ενώ αν  $\deg g = p$ , τότε το  $f$  είναι ανάγωγο πάνω από το  $F$ .
- (3) Αν το  $f$  είναι ανάγωγο πάνω από το  $F$ , δείξτε ότι η  $E/F$  είναι κυκλική.

**Παρατήρηση.** Ο συνδυασμός των ασκήσεων 9.12 και 9.13 αποδεικνύει το εξής Θεώρημα: Έστω σώμα  $F$  χαρακτηριστικής  $p$ . Η πεπερασμένη επέκταση  $E/F$  είναι κυκλική αν και μόνο αν το  $E$  είναι σώμα διάσπασης ενός ανάγωγου πολωνύμου της μορφής  $f = X^p - X - a \in F[X]$ . Όταν αυτή η συνθήκη ισχύει, τότε  $E = F(\theta)$ , όπου  $\theta$  είναι ρίζα του  $f$ .

**Άσκηση 9.14.** Η άσκηση αυτή δείχνει, μεταξύ άλλων, ότι στο Θεώρημα 9.3 η συνθήκη να περιέχει το  $F$  πρωταρχική  $n$ -οστή ρίζα της μονάδας είναι αναγκαία προκειμένου να εξαχθεί το συμπέρασμα ότι (υπό τις προϋποθέσεις του θεωρήματος) η επέκταση  $\mathcal{G}(E/F)$  είναι κυκλική.

Έστω  $n \in \mathbb{N}$ , σώμα  $F$  του οποίου η χαρακτηριστική είναι 0 ή  $p$  με  $p \nmid n$ ,  $c \in F \setminus \{0\}$  και  $E$  σώμα διάσπασης του  $f = X^n - c$ . Έστω  $\alpha \in E$  ρίζα του  $f$  και  $\omega \in E$  πρωταρχική  $n$ -οστή ρίζα της μονάδας (το  $E$  περιέχει τέτοια ρίζα, σύμφωνα με την άσκηση 9.10).

- (1) Αποδείξτε ότι  $E = F(\alpha, \omega)$ .
- (2) Έστω  $L = F(\omega)$ . Αποδείξτε ότι η  $L/F$  είναι Galois και η  $E/L$  είναι κυκλική.
- (3) Έστω ότι  $\text{Irr}(\omega, F) = (X - \omega)(X - \omega^{-1})$  και  $[E : L] = n$ .<sup>3</sup> Αποδείξτε ότι υπάρχουν  $\sigma, \tau \in \mathcal{G}(E/F)$  με τις εξής ιδιότητες:  $\sigma(\alpha) = \omega\alpha$ ,  $\sigma(\omega) = \omega$  και  $\tau(\alpha) = \alpha$ ,  $\tau(\omega) = \omega^{-1}$ . Επιπλέον, αποδείξτε ότι  $\text{ord}(\sigma) = n$ ,  $\text{ord}(\tau) = 2$  και  $\tau\sigma\tau^{-1} = \sigma^{-1}$  (ισοδύναμα,  $\tau\sigma = \sigma^{-1}\tau = \sigma^{n-1}\tau$ ). Συμπεράνετε ότι η υποομάδα  $\langle \sigma, \tau \rangle$  της  $\mathcal{G}(E/F)$  είναι η διεδρική  $D_n$ . Συγκρίνετε τις τάξεις  $|D_n|$  και  $|\mathcal{G}(E/F)|$  και συμπεράνετε ότι  $\mathcal{G}(E/F) = \langle \sigma, \tau \rangle$ , άρα η  $E/F$  δεν είναι κυκλική, παρά το ότι το  $E$  είναι σώμα διάσπασης του  $X^n - c \in F$ . Αυτό το συμπέρασμα δεν αντιφάσκει, όμως, στο Θεώρημα 9.3, γιατί εκείνο το θεώρημα απαιτεί τη συνθήκη να περιέχει το  $F$  πρωταρχική  $n$ -οστή ρίζα της μονάδας, η οποία εδώ δεν ικανοποιείται.

<sup>3</sup>Στην άσκηση 9.15 θα δούμε παράδειγμα στο οποίο αυτές οι συνθήκες ικανοποιούνται.

**Άσκηση 9.15.** Η άσκηση αυτή δίνει ένα παράδειγμα στο οποίο όλες οι υποθέσεις της άσκησης 9.14 ικανοποιούνται, καθώς και οι υποθέσεις του ερωτήματος (3).

Έστω  $\omega$  πρωταρχική 5<sup>η</sup> ρίζα της μονάδας,  $\beta := \omega + \omega^{-1}$ ,  $F = \mathbb{Q}(\beta)$ ,  $f = X^5 - 2 \in F[X]$  και  $\alpha = \sqrt[5]{2} \in \mathbb{R}$ .

(1) Αποδείξτε ότι  $F = \mathbb{Q}(\sqrt{5})$  και το  $F$  δεν περιέχει καμμία 5<sup>η</sup> ρίζα της μονάδας πλην του 1. Επίσης, δείξτε ότι  $\text{Irr } \omega, F = (X - \omega)(X - \omega^{-1}) = X^2 - \beta X + 1$ .

(2) Δείξτε ότι  $[E : \mathbb{Q}] = 20$  και  $[E : L] = 5$ . Από την άσκηση 9.14 συμπεράνετε ότι  $\mathcal{G}(E/F) \cong D_5$ .