

Κεφάλαιο 7

7.1 7^η Εβδομάδα

Πεπερασμένα σώματα

Αν ο p είναι πρώτος, το σώμα των ακεραίων $\text{mod } p$ (δηλαδή το σώμα $\mathbb{Z}/p\mathbb{Z}$) συμβολίζεται με $\mathbb{F}_p$.

Θεώρημα 7.1. Αν το E είναι πεπερασμένο σώμα χαρακτηριστικής p , τότε ισχύουν τα εξής.

- 1) $|E| = p^n$ όπου $n = [E : \mathbb{F}_p] \in \mathbb{N}$
- 2) E είναι το σώμα διάσπασης του $f = X^{p^n} - X \in \mathbb{F}_p[X]$ πάνω από το $\mathbb{F}_p$ και μάλιστα το E είναι το σύνολο των ριζών του f .

Παρατήρηση 7.2. Αν το E είναι σώμα χαρακτηριστικής p , τότε η απεικόνιση, $a \pmod{p} \mapsto a \cdot 1_E$ είναι καλά ορισμένος μονομορφισμός, οπότε μπορώ να θεωρώ ότι το $\mathbb{F}_p$ είναι υπόσωμα του E . Η παραπάνω απεικόνιση είναι καλά ορισμένη. Αυτό προκύπτει από το ότι, αν $a \equiv b \pmod{p}$, τότε

$$a \cdot 1_E - b \cdot 1_E = (a - b) \cdot 1_E = (kp) \cdot 1_E = k(p \cdot 1_E) = k \cdot 0_E = 0_E.$$

Είναι μονομορφισμός, γιατί $a \cdot 1_E = 0_E$ αν και μόνο αν $p \mid a$ δηλαδή αν και μόνο αν $a \equiv 0 \pmod{p}$, άρα $\ker \phi = \{0\}$.

Στην εκφώνηση του θεωρήματος, η σχολαστική γραφή του f είναι $f = 1_E X^{p^n} - 1_E X$.

Απόδειξη. 1) Σύμφωνα με την παραπάνω παρατήρηση, το E είναι επέκταση του $\mathbb{F}_p$. Έστω ότι $[E : \mathbb{F}_p] = n$ και $a_1, \dots, a_n$ είναι μία βάση της $E/\mathbb{F}_p$. Άρα $E = \{c_1 a_1 + \dots + c_n a_n : c_i \in \mathbb{F}_p\}$. Έχω p^n επιλογές για τη n -άδα $(c_1, \dots, c_n)$ άρα $|E| = p^n$.

- 2) $E^* = E \setminus \{0\}$ είναι η πολλαπλασιαστική ομάδα του E . Καθώς $|E^*| = p^n - 1$. Άρα για κάθε $\alpha \in E^*$ ισχύει ότι $\alpha^{p^n-1} = 1$, οπότε και $\alpha^{p^n} = \alpha$, σχέση που ισχύει και για το 0. Συνεπώς, κάθε στοιχείο του E είναι ρίζα του $X^{p^n} - X = f$. Προφανώς, τότε το E είναι σώμα διάσπασης του f πάνω από το $\mathbb{F}_p$. $\square$

Πόρισμα 7.3. Δύο πεπερασμένα σώματα με το ίδιο πλήθος στοιχείων είναι ισόμορφα.

Απόδειξη. Έστω ότι $|E_1| = |E_2| = p^n$, τότε καθένα από τα E_1, E_2 είναι σώμα διάσπασης του πολυωνύμου $X^{p^n} - X$ πάνω από το $\mathbb{F}_p[X]$, άρα είναι ισόμορφα (Πόρισμα 3.9). $\square$

Ορισμός 7.4. Για δοσμένο πρώτο p και $n \geq 1$, «σώμα Galois με p^n στοιχεία» είναι κάθε σώμα με p^n στοιχεία και συμβολίζεται με $\text{GF}(p^n)$. Σύμφωνα με το παραπάνω πόρισμα όλα τα σώματα Galois με p^n στοιχεία είναι ισόμορφα, άρα μπορούμε να λέμε «το σώμα Galois με p^n στοιχεία».

Πόρισμα 7.5. Έστω E σώμα με p^n στοιχεία. Τότε η $E/\mathbb{F}_p$ είναι Galois και $\mathcal{G}(E/\mathbb{F}_p) = \langle \sigma \rangle$, όπου σ είναι ο αυτομορφισμός του Frobenius του E , που ορίζεται: $\sigma(a) = a^p$ (βλ. Ορισμό 4.19).

Απόδειξη. Να δείξω ότι $E/\mathbb{F}_p$ είναι κανονική και διαχωρίσιμη. Κανονική είναι διότι το E είναι το σώμα διάσπασης του πολυνόμου $f = X^{p^n} - X$ πάνω από το $\mathbb{F}_p$, άρα εφαρμόζεται το Θεώρημα 5.14. Επίσης είναι διαχωρίσιμη από την Πρόταση 4.20. Άρα είναι επέκταση Galois.

Για την ομάδα Galois, παρατηρούμε αρχικά ότι $\sigma \in \mathcal{G}(E/\mathbb{F}_p)$ άρα $\langle \sigma \rangle \leq \mathcal{G}(E/\mathbb{F}_p)$. Για να δείξω την ισότητα των ομάδων αρκεί να δείξω την ισότητα των αντιστοίχων σταθεροποιητικών σωμάτων, δηλαδή, να δείξω ότι $\mathcal{F}(\langle \sigma \rangle) = \mathcal{F}(\mathcal{G}(E/\mathbb{F}_p))$. Επειδή η επέκταση $E/\mathbb{F}_p$ είναι Galois, το δεξιό μέλος της τελευταίας ισότητας είναι το $\mathbb{F}_p$. Επομένως, έχω να δείξω ότι $\mathcal{F}(\langle \sigma \rangle) = \mathbb{F}_p$. Απόδειξη της ισότητας: Είναι $\langle \sigma \rangle \leq \mathcal{G}(E/\mathbb{F}_p)$, άρα $\mathcal{F}(\langle \sigma \rangle) \geq \mathcal{F}(\mathcal{G}(E/\mathbb{F}_p)) = \mathbb{F}_p$, οπότε και $|\mathcal{F}(\langle \sigma \rangle)| \geq p$. Αντίστροφα, αν $\sigma(a) = a$, τότε $a^p = a$ οπότε το a είναι ρίζα του $X^p - X$. Καθώς αυτό το πολυνόμο έχει το πολύ p ρίζες, συμπεραίνω ότι $|\mathcal{F}(\langle \sigma \rangle)| \leq p$. Έτσι, $|\mathcal{F}(\langle \sigma \rangle)| = p$, αλλά τότε, το σώμα $\mathcal{F}(\langle \sigma \rangle)$ περιέχει το $\mathbb{F}_p$ και έχει το ίδιο πλήθος στοιχείων με αυτό, οπότε τα δύο σώματα ταυτίζονται. $\square$

Πόρισμα 7.6. Έστω ότι E/K είναι επέκταση πεπερασμένων σωμάτων χαρακτηριστικής p και $|K| = p^m$. Τότε $|E| = p^n$ για κάποιο n πολλαπλάσιο του m και $\mathcal{G}(E/K) = \langle \sigma^m \rangle$, όπου σ ο αυτομορφισμός του Frobenius (όπως στο Πόρισμα 7.5).

Απόδειξη. Κατ' αρχάς, για κάθε $k = 0, 1, 2, \dots$ ισχύει $\sigma^k(a) = a^{p^k}$ για κάθε $a \in E$ (απλή επαγωγική απόδειξη), σχέση την οποία θα χρησιμοποιήσω παρακάτω. Έχω το διάγραμμα αντιστοιχίας Galois:

$$\begin{array}{ccc} E & \longleftrightarrow & \langle id \rangle \\ \downarrow & & \downarrow \\ K & \longleftrightarrow & \mathcal{G}(E/K) \stackrel{?}{=} \langle \sigma^m \rangle \\ \downarrow & & \downarrow \\ \mathbb{F}_p & \longleftrightarrow & \mathcal{G}(E/\mathbb{F}_p) = \langle \sigma \rangle \end{array}$$

όπου σ ο αυτομορφισμός του Frobenius.

Καθώς το E είναι πεπερασμένη επέκταση του $\mathbb{F}_p$, ισχύει $|E| = p^n$ για κάποιο n . Από το Θεώρημα 7.1 (1), $[E : \mathbb{F}_p] = n$ και $[K : \mathbb{F}_p] = m$, άρα $n = [E : K][K : \mathbb{F}_p] = [E : K]m$, που δείχνει ότι $m|n$.

Για την απόδειξη της ισότητας $\mathcal{G}(E/K) = \langle \sigma^m \rangle$ αρκεί να δείξω ότι τα αντίστοιχα σταθεροποιούμενα σώματα είναι ίσα, δηλαδή, να δείξω ότι $\mathcal{F}(\langle \sigma^m \rangle) = \mathcal{F}(\mathcal{G}(E/K))$. Το δεξιό μέλος ισούται με K διότι E/K είναι Galois, άρα πρέπει να αποδείξω ότι $\mathcal{F}(\langle \sigma^m \rangle) = K$. Από το Θεώρημα 7.1 (2) ξέρω ότι το K ταυτίζεται με το σύνολο των ριζών του $X^{p^m} - X$, άρα $a \in K \Leftrightarrow a^{p^m} = a$. Από την άλλη, $a \in \mathcal{F}(\langle \sigma^m \rangle) \Leftrightarrow \sigma^m(a) = a \Leftrightarrow a^{p^m} = a$, οπότε $a \in K \Leftrightarrow a \in \mathcal{F}(\langle \sigma^m \rangle)$. $\square$

Θεώρημα 7.7. Έστω p πρώτος και $m, n \in \mathbb{N}$. Το $\text{GF}(p^m)$ είναι υπόσωμα -με την ευρεία έννοια- του $\text{GF}(p^n)$ αν και μόνο αν $m | n$.

Απόδειξη. Θεωρώ σε κάποια αλγεβρική κλειστότητα C του $\mathbb{F}_p$ το σύνολο ριζών E του $X^{p^n} - X$ και το σύνολο ριζών K του $X^{p^m} - X$. Σύμφωνα με το Θεώρημα 7.1, τα E, K είναι σώματα διάσπασης των αντιστοίχων πολυνόμων, $|E| = p^n$ και $|K| = p^m$. Άρα $E \cong \text{GF}(p^n)$ και $K \cong \text{GF}(p^m)$. Θα δείξω ότι $K \leq E \Leftrightarrow m|n$.

Αν $K \leq E$, τότε εφαρμόζεται το Πόρισμα 7.6 και συμπεραίνω ότι $m|n$.

Αντιστρόφως, έστω $m|n$. Πρέπει και αρκεί να δείξω ότι, αν $a \in K$, τότε και $a \in E$. Δηλαδή, αν $a^{p^m} = a$, τότε και $a^{p^n} = a$. Άρα γενικότερα να δείξω ότι αν $a^{p^m} = a$, τότε $a^{p^{km}} = a$, για κάθε $k \in \mathbb{N}$. Απλή επαγωγή. Για $k = 1$ ισχύει. Έστω ότι ισχύει για $k = \nu$, τότε $a^{p^{m(\nu+1)}} = (a^{p^{m\nu}})^{p^m} = a^{p^m} = a$. $\square$

Πρακτική κατασκευή πεπερασμένων σωμάτων. Θέλω να κατασκευάσω $\text{GF}(p^n)$ για συγκεκριμένο πρώτο p και $n \in \mathbb{N}$. Προσπαθώ να βρω $f \in \mathbb{F}_p$ ανάγωγο βαθμού n . Φαντάζομαι ότι α είναι ρίζα του f σε κάποια αλγεβρική κλειστότητα C του $\mathbb{F}_p$, οπότε $1, \alpha, \dots, \alpha^{n-1}$ είναι βάση για την επέκταση $\mathbb{F}_p(\alpha)/\mathbb{F}_p$. Άρα

$$\mathbb{F}_p(\alpha) = \{c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1} : (c_0, \dots, c_{n-1}) \in \mathbb{F}_p^n\}.$$

Άρα $|\mathbb{F}_p(\alpha)| = p^n$. Από το γεγονός ότι όλα τα πεπερασμένα σώματα που έχουν το ίδιο πλήθος στοιχείων είναι ισόμορφα (Πόρισμα 7.3) έπεται ότι διαφορετικές επιλογές f δίνουν διαφορετικά ενδεχομένως σώματα, τα οποία όμως είναι ισόμορφα.

Παράδειγμα 7.8. Κατασκευή του $\text{GF}(9)$. Θεωρώ το $X^2 + 1 \in \mathbb{F}_3(X)$. Είναι ανάγωγο καθώς δεν έχει ρίζες στο $\mathbb{F}_3$. Θεωρώ α τέτοιο ώστε $\alpha^2 + 1 = 0$. Τότε,

$$\text{GF}(9) = \mathbb{F}_9 = \{0, 1, 2, \alpha, 1 + \alpha, 2 + \alpha, 2\alpha, 1 + 2\alpha, 2 + 2\alpha\}.$$

Για να κάνω πράξεις, χρησιμοποιώ τη σχέση $\alpha^2 + 1 = 0$. π.χ.

$$(2 + \alpha)(1 + 2\alpha) = 2 + 4\alpha + \alpha + 2\alpha^2 = 2 + \alpha + \alpha + 2(-1) = 2\alpha.$$

Ασκήσεις

Άσκηση 7.9. (1) Για το σώμα $\mathbb{F}_9$ που κατασκευάστηκε στο Παράδειγμα 7.8 βρείτε στοιχείο $\gamma \in \mathbb{F}_9$ το οποίο να παράγει την πολλαπλασιαστική ομάδα $\mathbb{F}_9^*$.

(2) Κατασκευάστε σώμα 9 στοιχείων χρησιμοποιώντας διαφορετικό πολυώνυμο από αυτό του Παραδείγματος 7.8.

Άσκηση 7.10. Έστω πρώτος p , $n \in \mathbb{N}$, $f = X^{p^n} - X \in \mathbb{F}_p$, C αλγεβρική κλειστότητα του $\mathbb{F}_p$ και $E \subset C$ το σύνολο των ριζών του f . Αποδείξτε ότι το E εφοδιασμένο με τις πράξεις του C είναι σώμα και $|E| = p^n$.

Άσκηση 7.11. Έστω πεπερασμένο σώμα K με q στοιχεία (άρα $q = p^m$ με p πρώτο και $m \in \mathbb{N}$) και $f \in K[X]$ ανάγωγο. Αποδείξτε ότι $f \mid X^{q^n} - X$ αν και μόνο αν $\deg f \mid n$.

Άσκηση 7.12. Έστω πρώτος p και $n \in \mathbb{N}$. Έστω $f = X^{p^n} - X - 1 \in \mathbb{F}_p[X]$. Αποδείξτε ότι αν το f είναι ανάγωγο πάνω από το $\mathbb{F}_p$, τότε ή $n = 1$, ή $n = p = 2$. Έστω C μια αλγεβρική κλειστότητα του $\mathbb{F}_p$ και $\alpha \in C$ μια ρίζα του f . Ακολουθήστε τα παρακάτω βήματα (δεκτός οποιοσδήποτε διαφορετικός, σωστός τρόπος απόδειξης).

- (1) Αποδείξτε ότι το $\mathbb{F}_p(\alpha)$ περιέχει όλες τις ρίζες του f .
- (2) Αποδείξτε ότι, για κάθε $b \in \mathbb{F}_p$, το $\alpha + b$ είναι ρίζα του f .
- (3) Βασισμένοι στο (2), αποδείξτε ότι $\mathbb{F}_{p^n} \leq \mathbb{F}_p(\alpha)$ και $n = p^i$ για κάποιο $i \in \{0, 1, \dots, n\}$.
- (4) Αποδείξτε ότι η $\mathcal{G}(\mathbb{F}_p(\alpha)/\mathbb{F}_{p^n})$ είναι κυκλική και έστω τ ένας γεννήτοράς της. Υπολογίστε την τάξη του τ συναρτήσει του i του ερωτήματος (3).
- (5) Ανεξάρτητα από το ερώτημα (4), υπολογίστε μια απλή έκφραση του $\tau^k(\alpha)$ και, βάσει αυτής, αποδείξτε ότι η τάξη του τ είναι p .
- (6) Συνδυάζοντας τα (4) και (5) αποδείξτε ότι $[\mathbb{F}_p(\alpha) : \mathbb{F}_{p^n}] = p$.
- (7) Κάνοντας χρήση των βαθμών των διαδοχικών επεκτάσεων $\mathbb{F}_p \leq \mathbb{F}_{p^n} \leq \mathbb{F}_p(\alpha)$ αποδείξτε ότι $np = p^n$ και συμπεράνετε από αυτό ότι ή $n = 1$, ή $n = 2 = p$.

Κυκλοτομικά σώματα

Ορισμός 7.13. Έστω σώμα F και $n \in \mathbb{N}$. Ένα σώμα διάσπασης E του $\Phi_n(X) := X^n - 1 \in F[X]$ λέγεται n -οστό κυκλοτομικό σώμα πάνω από το F .

Παράδειγμα 7.14. Στην περίπτωση που $F = \mathbb{Q} \leq \mathbb{C}$, το E (ως υπόσωμα του $\mathbb{C}$) είναι το $\mathbb{Q}(\zeta_n)$, όπου $\zeta_n = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$. Όλες οι ρίζες είναι του Φ_n είναι οι $\zeta_n^k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$ για $k = 0, \dots, n-1$. Αυτές είναι κορυφές κανονικού n -γώνου στο μιγαδικό επίπεδο, απ' όπου και η ονομασία κυκλο-τομικό σώμα (τέμνει τον κύκλο σε n ίσα τόξα).

Κάθε πεπερασμένη υποομάδα της πολλαπλασιαστικής ομάδας ενός σώματος είναι κυκλική.¹ Το σύνολο U_n των ριζών του $\Phi_n \in F[X]$, εφοδιασμένο με τον πολλαπλασιασμό του E , είναι πεπερασμένη υποομάδα της πολλαπλασιαστικής ομάδας E^* , άρα είναι κυκλική. Συνεπώς, υπάρχει $\omega \in E$ τέτοιο ώστε $\langle \omega \rangle = \{1, \omega, \dots\}$ είναι το σύνολο των ριζών του Φ_n . Δηλαδή υπάρχει $\omega \in E$ τέτοιο ώστε κάθε ρίζα του $X^n - 1$ να είναι της μορφής $\omega^k, k \in \mathbb{Z}$. Αφού $\omega^n = 1$ έπεται ότι η τάξη $\text{ord}(\omega) \mid n$ άρα είναι $\leq n$.

Δεν μπορώ να είμαι σίγουρος ότι $\text{ord}(\omega) = n$. π.χ. αν $\text{char}(F) = p$ και $n = pm$ τότε $0 = 1 - \omega^n = 1 - \omega^{pm} = (1 - \omega^m)^p$ που σημαίνει ότι $\text{ord}(\omega) \leq m < n$. Αν όμως το $\Phi_n \in F[X]$ δεν έχει πολλαπλές ρίζες, τότε όλες οι ρίζες $1, \omega, \dots, \omega^{n-1}$ είναι διαφορετικές, οπότε $|U_n| = n$ ή, ισοδύναμα, $\text{ord} \omega = n$.

Ορισμός 7.15. Το $\omega \in E$ λέγεται πρωταρχική n -οστή ρίζα της μονάδας (δηλαδή, του 1_E) αν, ως στοιχείο της ομάδας E^* έχει τάξη n ($\text{ord}(\omega) = n$), οπότε, όλα τα στοιχεία $\omega^k, k = 0, 1, \dots, n-1$ είναι διαφορετικά και αποτελούν όλες τις ρίζες του Φ_n .

Το Φ_n δεν έχει πολλαπλές ρίζες στις εξής σημαντικές περιπτώσεις:

- $\text{char } F = 0$. (*)
- Όταν $\text{char } F = p$ και $p \nmid n$. (**)

Πράγματι, στις παραπάνω δύο περιπτώσεις είναι η παράγωγος $\Phi'_n = nX^{n-1} \neq 0 \in F[X]$, άρα τα πολυώνυμα Φ_n και Φ'_n δεν έχουν κοινό μη σταθερό παράγοντα και, συνεπώς, εφαρμόζεται η Πρόταση 4.15.

Στα επόμενα υποθέτω ότι ισχύει μία από τις παραπάνω δύο συνθήκες.

Θα μελετήσω την ομάδα $\mathcal{G}(E/F)$. Βάσει των προηγούμενων $E = F(1, \omega, \dots, \omega^{n-1}) = F(\omega)$. Το ω χαρακτηρίζεται (πρωτ)αρχική n -οστή ρίζα της μονάδας. Πότε η ω^k είναι αρχική ρίζα της μονάδας;

Αυτό συμβαίνει αν και μόνο αν $n = \text{ord}(\omega^k) = \frac{\text{ord}(\omega)}{\gcd(\text{ord}(\omega), k)} = \frac{n}{\gcd(n, k)}$, δηλαδή, ισοδύναμα, αν και μόνο αν $\gcd(n, k) = 1$. Άρα υπάρχουν $\phi(n)$ αρχικές n -οστές ρίζες του 1.

Έστω $\sigma \in \mathcal{G}(E/F)$. Ο σ καθορίζεται από το $\sigma(\omega)$. Το ω είναι ρίζα του $X^n - 1$, άρα και το $\sigma(\omega)$ είναι ρίζα του $X^n - 1$, οπότε $\sigma(\omega) = \omega^k$ για κάποιο $k \in \{1, 2, \dots, n-1\}$. Λόγω του ότι ο σ είναι ισομορφισμός, ισχύει $\text{ord}(\sigma(\omega)) = \text{ord}(\omega) = n$ άρα $\gcd(k, n) = 1$. Βασισμένος σ' αυτή την παρατήρηση, ορίζω την αντιστοιχία

$$\begin{aligned} \psi : \mathcal{G}(E/F) &\rightarrow \mathbb{Z}_n^* \\ \sigma &\mapsto k \pmod{n} \end{aligned}$$

όπου το k είναι εκείνο για το οποίο ισχύει $\sigma(\omega) = \omega^k$. Η παραπάνω απεικόνιση είναι μονομορφισμός ομάδων (απλό).

Πρόταση 7.16. Έστω ότι το F ικανοποιεί μια από τις συνθήκες (*) ή (**) και E είναι το n -οστό κυκλο-τομικό σώμα πάνω από το F . Τότε η επέκταση E/F είναι Galois και η $\mathcal{G}(E/F)$ είναι ισόμορφη με μία υποομάδα της $\mathbb{Z}_n^*$. Συνεπώς, η $\mathcal{G}(E/F)$ είναι αβελιανή και η τάξη της είναι διαιρέτης του $\phi(n)$.

¹Έστω υποομάδα G , πεπερασμένης τάξης n . Θεωρώ r το ελάχιστο κοινό πολλαπλάσιο των τάξεων των στοιχείων της G . Καθώς η τάξη ενός στοιχείου διαιρεί το n , και $r \mid n$ (1). Αντίστροφα, αν g στοιχείο της ομάδας, καθώς η τάξη του διαιρεί το r , θα είναι ρίζα του $X^r - 1 \in F[X]$. Καθώς το πολυώνυμο έχει το πολυ r ρίζες, η τάξη της ομάδας θα είναι $n \leq r$ (2). Από τα (1) και (2), καταλήγουμε ότι $r = n$. Τέλος, χρησιμοποιούμε την πρόταση ότι σε κάθε αβελιανή ομάδα, αν υπάρχει στοιχείο τάξης m και στοιχείο τάξης n , τότε υπάρχει και στοιχείο τάξης $\text{lcm}(m, n)$, για να καταλήξουμε ότι υπάρχει στοιχείο τάξης r και συνεπώς ότι η G είναι κυκλική.

Απόδειξη. Έστω ω πρωταρχική n -οστή ρίζα του 1. Όπως είδαμε λίγο πιο πάνω, $E = F(\omega)$. Αφού το ω είναι ρίζα του Φ_n , έπεται ότι το $\text{Irr}(\omega, F)$ διαιρεί το Φ_n (στο $E[X]$). Αλλά, όπως είδαμε λίγο πριν, όταν ικανοποιούνται οι συνθήκες (*) και (**), το Φ_n δεν έχει πολλαπλές ρίζες, άρα ούτε το $\text{Irr}(\omega, F)$ έχει πολλαπλές ρίζες, που σημαίνει ότι το ω είναι διαχωρίσιμο, άρα και η επέκταση $F(\omega)/F$ (δηλαδή, η E/F είναι διαχωρίσιμη (Πόρισμα 5.3). Η ίδια επέκταση είναι και κανονική, αφού το E είναι σώμα διάσπασης του Φ_n πάνω από το F (Θεώρημα 5.14), άρα, τελικά, η E/F είναι Galois.

Ο μονομορφισμός ομάδων ψ , που ορίστηκε πριν από την εκφώνηση της πρότασης έχει ως άμεση συνέπεια ότι $E/F \cong \psi(E/F)$. Η ομάδα στα δεξιά αυτής της σχέσης είναι υποομάδα της $\mathbb{Z}_n^*$, η οποία είναι αβελιανή, τάξεως $\phi(n)$, άρα η υποομάδα είναι αβελιανή και η τάξη της διαιρεί το $\phi(n)$. $\square$

Ορισμός 7.17. Έστω ω πρωταρχική n -οστή ρίζα του 1 (πάνω από το F). Ορίζουμε το πολυώνυμο

$$\Psi_n(X) = \prod_{\substack{1 \leq k \leq n-1 \\ \gcd(k, n) = 1}} (X - \omega^k) = \prod_{i=1}^{\phi(n)} (X - \omega_i),$$

όπου ω_i οι διαφορετικές πρωταρχικές n -οστές ρίζες της 1.

Από τον ορισμό του, $\Psi_n \in E[X]$. Στόχος μου να δείξω ότι $\Psi_n \in \mathbb{P}[X]$, όπου $\mathbb{P}$ είναι το πρώτο σώμα του F .² Κατ' αρχάς, ισχύει η εξής πρόταση.

Πρόταση 7.18. $\Phi_n = \prod_{d|n} \Psi_d$

Απόδειξη. Έστω U_n η πολλαπλασιαστική ομάδα των ριζών του Φ_n . Παρατηρώ τα εξής: Για κάθε διαιρέτη d του n , οι ρίζες του Ψ_d ανήκουν στο U_n (αν $\zeta^d = 1$ τότε και $\zeta^n = 1$). Επιπλέον, οι ρίζες του Ψ_d είναι, ακριβώς, τα στοιχεία της U_n των οποίων η τάξη είναι d . Συνεπώς, αν d_1, d_2 είναι διαφορετικοί διαιρέτες του n , τα Ψ_{d_1} και Ψ_{d_2} δεν έχουν κοινές ρίζες, οπότε το σύνολο των ριζών του δεξιού μέλους της εκφώνησης (που είναι η ξένη ένωση των ριζών όλων των Ψ_d) περιέχεται, δίχως επαναλήψεις, στο U_n . Αντιστρόφως, έστω ζ ρίζα του Φ_n . Αυτή έχει πολλαπλότητα 1 και έστω $\text{ord } \zeta = d$. Από τη στοιχειώδη Θ. Ομάδων, $d|n$ και, φυσικά, $\zeta^d = 1$, άρα η ζ είναι ρίζα του Ψ_d .

Συμπέρασμα: Τα πολυώνυμα Φ_n και $\prod_{d|n} \Psi_d$ έχουν απλές ρίζες, κάθε ρίζα του δεύτερου είναι ρίζα του πρώτου και κάθε ρίζα του πρώτου είναι και ρίζα του δεύτερου. Επιπλέον, τα δύο πολυώνυμα είναι μονικά, άρα, τελικά, αυτά τα πολυώνυμα είναι ίσα. $\square$

Παράδειγμα 7.19. Τα παρακάτω πολυώνυμα Ψ_n θεωρούνται πάνω από ένα σώμα F χαρακτηριστικής 0 ή πάνω από σώμα χαρακτηριστικής p με $p \nmid n$.

Προφανώς, μοναδική πρωταρχική 1^η ρίζα του 1 είναι το 1, άρα $\Psi_1 = X - 1$ και μοναδική πρωταρχική 2^η ρίζα του 1 (όταν $\text{char } F \neq 2$) είναι το -1 , άρα $\Psi_2 = X + 1$. Όταν $\text{char } F \neq 3$, τότε, από την Πρόταση 7.18, $\Phi_3 = \Psi_1 \Psi_3$, άρα

$$\Psi_3 = \frac{\Phi_3}{X - 1} = \frac{X^3 - 1}{X + 1} = X^2 + X + 1.$$

Όταν $\text{char } F \neq 2$, τότε, από την Πρόταση 7.18, $\Phi_4 = \Psi_1 \Psi_2 \Psi_4$, άρα

$$\Psi_4 = \frac{\Phi_4}{\Psi_1 \Psi_2} = \frac{X^4 - 1}{X^2 - 1} = X^2 + 1.$$

Όταν $\text{char } F \neq 2, 3$, τότε, από την Πρόταση 7.18, $\Phi_6 = \Psi_1 \Psi_2 \Psi_3 \Psi_6$, άρα

$$\Psi_6 = \frac{\Phi_6}{\Psi_1 \Psi_2 \Psi_3} = \frac{X^6 - 1}{(X^2 - 1)(X^2 + X + 1)} = \frac{(X^2)^3 - 1}{(X^2 - 1)(X^2 + X + 1)} = \frac{X^4 + X^2 + 1}{X^2 + X + 1} = X^2 - X + 1.$$

²Το πρώτο σώμα $\mathbb{P}$ ενός σώματος F είναι το ελάχιστο υπόσωμα του F . Αν $\text{char } F = 0$, τότε $\mathbb{P} \cong \mathbb{Q}$, ενώ, αν $\text{char } F = p$, τότε $\mathbb{P} \cong \mathbb{F}_p$. Επομένως, μπορούμε να βλέπουμε το F ως επέκταση του $\mathbb{Q}$, στην πρώτη περίπτωση και του $\mathbb{F}_p$ στη δεύτερη περίπτωση.

Σε σχέση με τα παραδείγματα αυτά, δείτε την άσκηση 7.22

Λήμμα 7.20. Έστω ότι $\mathbb{P}$ είναι το πρώτο σώμα του F και $f = gh$, με $f, g \in \mathbb{P}[X]$. Τότε $h \in \mathbb{P}[X]$. Στην ειδική περίπτωση που $F = \mathbb{Q}$ (οπότε $\mathbb{P} = \mathbb{Q}$), τα $f, g \in \mathbb{Z}[X]$ και το g είναι μονικό, ισχύει κάτι ισχυρότερο: $h \in \mathbb{Z}[X]$.

Απόδειξη. Στον δακτύλιο $\mathbb{P}[X]$ εκτελώ την ευκλείδεια διαίρεση του f δια g , οπότε $f = gq + r$, όπου $q, r \in \mathbb{P}[X]$ και $\deg r < \deg g$. Την ισότητα $f = gq + r$ μπορώ να τη 'δω και ως ισότητα ευκλείδειας διαίρεσης στο $F[X]$, με πηλίκο q και υπόλοιπο r . Στο $F[X]$, η σχέση $f = gh + 0$ είναι, επίσης, ισότητα ευκλείδειας διαίρεσης με πηλίκο h και υπόλοιπο 0. Αλλά σε κάθε δακτύλιο πολυωνύμων πάνω από σώμα, το πηλίκο και το υπόλοιπο μιας ευκλείδειας διαίρεσης είναι μονοσημάντως ορισμένα, συνεπώς, $q = h$ και $r = 0$. Άρα, $h = q \in \mathbb{P}[X]$.

Αν $F = \mathbb{Q}$ και το g είναι μονικό, τότε στην ευκλείδεια διαίρεση $f = gq + r$ τα g, r έχουν όλους τους συντελεστές τους στο $\mathbb{Z}$. Ένα εντελώς όμοιο με το παραπάνω επιχείρημα μας οδηγεί στις σχέσεις $q = h$ και $r = 0$, άρα $h \in \mathbb{Z}[X]$. $\square$

Πρόταση 7.21. $\Psi_n \in \mathbb{P}[X]$. Στην ειδική περίπτωση $F = \mathbb{Q}$ ισχύει $\Psi_n \in \mathbb{Z}[X]$.

Απόδειξη. Επαγωγικά επί του n . Για $n = 1$ ισχύει, αφού $\Psi_1 = X - 1$. Θεωρώ $n > 1$ και υποθέτω ότι για κάθε $m < n$ είναι $\Psi_m(X) \in \mathbb{P}[X]$. Τότε από την Πρόταση 7.18,

$$\Phi_n = \Psi_n \times \prod_{d|n, d < n} \Psi_d.$$

Από την επαγωγική υπόθεση, $g := \prod_{d|n, d < n} \Psi_d \in \mathbb{P}[X]$. Άρα $\Phi_n = g\Psi_n$ με τα $g, \Phi_n \in \mathbb{P}[X]$. Από το Λήμμα 7.20 έπεται ότι και το Ψ_n ανήκει στο $\mathbb{P}[X]$.

Στην ειδική περίπτωση που $F = \mathbb{Q}$, επειδή $g, \Phi_n \in \mathbb{Z}[X]$ και το g είναι μονικό, το λήμμα συνεπάγεται ότι $\Psi_n \in \mathbb{Z}[X]$. $\square$

Ασκήσεις

Άσκηση 7.22. Στο Παράδειγμα 7.19 υπολογίζονται τα $\Psi_2, \Psi_3, \Psi_4, \Psi_6 \in F[X]$ υπό την προϋπόθεση ότι η χαρακτηριστική του F είναι διάφορη του 2, 3, 2, και 2, 3, αντιστοίχως. Για $i \in \{2, 3, 4, 6\}$ δείξτε ότι, αν δεν ικανοποιείται ο αντίστοιχος περιορισμός, τότε το Ψ_i δεν είναι ανάγωγο και η i -οστή πρωταρχική ρίζα του $1 \in F$ ανήκει στο F .

Άσκηση 7.23. (1) Σε σώμα F χαρακτηριστικής $\neq 3, 5$ υπολογίστε τα Ψ_5 και Ψ_{15} .
(2) Σε σώμα F χαρακτηριστικής $\neq 2$ υπολογίστε το Ψ_{16} .