Άλγεβρα ΙΙ

Σημειώσεις Μεταπτυχιακού Μαθήματος

Διδάσκων: Ν.Γ. Τζανάκης

Πανεπιστήμιο Κρήτης
Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών

Εαρινό Εξάμηνο 2023

Περιεχόμενα

Κεφάλαιο 1

1.1 1η Εβδομάδα

Πίνακας 1.1: Αντιστοιχία ιδιοτήτων του $\mathbb{Z}$ και του $K[X]$, με K σώμα

$\mathbb{Z}$	$K[X]$
αντιστρέψιμα στοιχεία: ± 1	αντιστρέψιμα στοιχεία: $c \in K^*$
$p > 1$ πρώτος: $p \neq ab$ με $a, b > 1$	$p(X) \notin K$ ανάγωγο: $p(\mathrm{X}) \neq a(X)b(X)$ με $a(X), b(X) \notin K$
$d = \mathrm{ΜΚΔ}(a, b)$ (1) d κ.δ. των a, b (2) αν d' είναι κ.δ. των a, b τότε $d' \mid d$	$d(X) = \mathrm{ΜΚΔ}(a(X), b(x))$ (1) $d(X)$ κ.δ. των $a(X), b(X)$ (2) αν $d'(X)$ είναι κ.δ. των $a(X), b(X)$ τότε $d'(X) \mid d(X)$ (3) $d(X)$ είναι μονικό
Ανάλυση σε πρώτους: $a > 1$ $a = p_1 \cdots p_n$ $p_1, \dots, p_n$ πρώτοι. Αν $a = q_1 \cdots q_l, \quad q_1, \dots, q_l$ πρώτοι, τότε $l = n$ και $(q_1, \dots, q_n)$ είναι μετάθεση των $(p_1, \dots, p_n)$	Ανάλυση σε ανάγωγα: $a(X) \notin K$ $a(X) = p_1(X) \cdots p_n(X)$ $p_1(X), \dots, p_n(X)$ ανάγωγα. Αν $a(X) = q_1(X) \cdots q_l(X), \quad q_1(X), \dots, q_l(X)$ ανάγωγα, τότε $l = n$ και υπάρχει μετάθεση $(i_1, \dots, i_n)$ της $(1, \dots, n)$ ώστε $q_k(X) =$ σταθερά $\cdot\, p_{i_k}(X)$ για κάθε $k = 1, \dots, n$
Αν $a \in \mathbb{Z}$ και p πρώτος, τότε $p \mid a$ είτε $\mathrm{ΜΚΔ}(a, p) = 1$	Αν $a(X) \in K[X]$ και $p(X) \in K[X]$ ανάγωγο, τότε $p(\mathrm{X}) \mid a(\mathrm{X})$ είτε $\mathrm{ΜΚΔ}(a(\mathrm{X}), p(\mathrm{X})) = 1$
$\mathrm{ΜΚΔ}(a, b) = d \Rightarrow \exists\, a', b' :$ $a' \cdot a + b' \cdot b = d$	$\mathrm{ΜΚΔ}(a(X), b(X)) = d(X) \Rightarrow \exists\, a'(X), b'(X) \in K[X] :$ $a'(X) \cdot a(X) + b'(X) \cdot b(X) = d(X)$
Ευκλείδεια διαίρεση: $a, b \in \mathbb{Z}$, $b \neq 0$ $\exists\, q, r \in \mathbb{Z},\ 0 \leq r < b \ : a = bq + r$	Ευκλείδεια διαίρεση: $a(X), b(X) \in K[X]$, $b(X) \neq 0$ $\exists\, q(X), r(X) \in K[X],\ \deg r(X) < \deg b(X) \ : a(X) = b(X)q(X) + r(X)$ Σύμβαση: $\deg 0 = -\infty$ και $-\infty < m \ \ \forall m \in \mathbb{Z}$

Ορισμός 1.1. Έστω R μεταθετικός δακτύλιος με μοναδιαίο στοιχείο 1_R. Συνήθως, αντί για 1_R θα γράφομε, απλούστερα, 1. Ανάλογα, αντί για 0_R (μηδενικό στοιχείο του R), θα γράφομε 0. Το $\emptyset \neq I \subseteq R$ ονομάζεται ιδεώδες αν και μόνον αν

1. $a, b \in I \implies a - b \in I$
2. $a \in I,\ r \in R \implies ra \in I$

Παράδειγμα 1.2. $\{0\}$ το μηδενικό ιδεώδες και R ολόκληρος ο δακτύλιος

Αν το I είναι ιδεώδες του δακτυλίου R, τότε ορίζω τη σχέση ισοδυναμίας $a \sim b \iff a - b \in I$. Η κλάση ισοδυναμίας του $a \in R$ είναι το σύνολο

$$a + I = \{a+ = r : r \in R\}$$

Στο σύνολο πηλίκο του ως προς την $\sim$, δηλαδή στο σύνολο των κλάσεων ισοδυναμίας, που συμβολίζεται R/I ορίζω πράξεις

$$+ : (a + I) + (b + I) \coloneqq (a + b) + I$$
$$\cdot : (a + I) \cdot (b + I) \coloneqq ab + I$$

Πρόταση. *Οι πράξεις είναι καλά ορισμένες. Δηλαδή, αν $a + I = a' + I$ και $b + I = b' + I$, τότε $(a + I) + (b + I) = (a' + I) + (b' + I)$ και $(a + I) \cdot (b + I) = (a' + I) \cdot (b' + I)$.*

Απόδειξη.

$$a + I = a' + I : \iff a' = a + \imath_1, \qquad \imath_1 \in I$$
$$b + I = b' + I : \iff b' = b + \imath_2, \qquad \imath_2 \in I$$

άρα $a'b' = ab + a\imath_2 + b\imath_1 + \imath_1\imath_2$ και συνεπώς $a'b' - ab \in I$, δηλαδή $a'b' + I = ab + I$. □

Παράδειγμα 1.3 (όχι καλά ορισμένων "πράξεων"). $R = \mathbb{Z}, I = 7\mathbb{Z}$ άρα $R/I = \{0+I, \dots, 6+I\}$. Ορίζω την "πράξη" $(a+7\mathbb{Z}) \star (b+7\mathbb{Z}) = c+7\mathbb{Z}$ όπου c το υπόλοιπο της διαίρεσης του ab διά 5.

Ελέγχω το αποτέλεσμα στην εξής περίπτωση:

$$(4+7\mathbb{Z}) \star (3+7\mathbb{Z}) = 2+7\mathbb{Z}$$
$$(11+7\mathbb{Z}) \star (10+7\mathbb{Z}) = 1+7\mathbb{Z}$$

Δηλαδή, ενώ $4+7\mathbb{Z} = 11+7\mathbb{Z}$ και $3+7\mathbb{Z} = 10+7\mathbb{Z}$, οι αντίστοιχοι πολλαπλασιασμοί δίνουν διαφορετικά αποτελέσματα, άρα η φαινομενική "πράξη" δεν είναι πράξη.

Ιδεώδες που παράγεται από κάποια στοιχεία $\alpha, \beta, \gamma, \dots \in R$. Συμβολίζεται με $\langle \alpha, \beta, \gamma, \dots \rangle$ και ορίζεται ως το σύνολο

$$\{r_1\alpha + r_2\beta + \dots : r_1, r_2, \dots \in R\}$$

Αν τα στοιχεία $\alpha, \beta, \gamma, \dots$ είναι άπειρα στο πλήθος, τότε εννοείται ότι μόνο πεπερασμένο το πλήθος $r_1, r_2, r_3, \dots$ είναι $\neq 0$ Σημαντική ειδική περίπτωση: Ιδεώδες που παράγεται από ένα μόνο στοιχείο. Ένα τέτοιο ιδεώδες λέγεται *κύριο*. Η τυπική του μορφή είναι

$$\langle a \rangle = \{ra : r \in R\}$$

Ορισμός 1.4. Ένας δακτύλιος του οποίου όλα τα ιδεώδη είναι κύρια ονομάζεται *δακτύλιος κυρίων ιδεωδών* (Δ.Κ.Ι. ή στ' αγγλικά P.I.D. principal ideal domain)

Παράδειγμα 1.5. Ο δακτύλιος $\mathbb{Z}$ καθώς και οι πολυωνυμικοί δακτύλιοι $K[X]$, όπου K σώμα, είναι Δ.Κ.Ι. Αυτό ισχύει γιατί και στους δύο υπάρχει ευκλείδια διαίρεση.

Παράδειγμα 1.6 (Δακτύλιος που δεν είναι Δ.Κ.Ι.). Έστω ο υποδακτύλιος R του $\mathbb{C}$, που ορίζεται ως εξής: $R = \{a + bi\sqrt{5} : a, b \in \mathbb{Z}\}$. Θεωρώ το ιδεώδες $I = \{2x + (1+i\sqrt{5})y : x, y \in \mathbb{Z}\}$. Αν ήταν το I κύριο ιδεώδες, τότε θα υπήρχαν $a_0, b_0 \in \mathbb{Z}$ ώστε $I = \langle a_0 + b_0 i\sqrt{5} \rangle$, δηλαδή

$$\{2x + (1+i\sqrt{5})y : x, y \in \mathbb{Z}\} = \{(a_0 + b_0 i\sqrt{5})(r + si\sqrt{5}) : r, s \in \mathbb{Z})\} \tag{1.1}$$

Για $x = 1, y = 0$ παίρνω το 2. Άρα το 2 ανήκει στο αριστερό μέρος της (1.1), οπότε θα πρέπει να υπάρχουν $r_1, s_1 \in \mathbb{Z}$ ώστε

$$2 = (a_0 + b_0 i\sqrt{5})(r + si\sqrt{5})$$

Η συζυγής μιγαδική σχέση είναι

$$2 = (a_0 - b_0 i\sqrt{5})(r - si\sqrt{5})$$

Πολλαπλασιάζοντας τις δύο σχέσεις έχω $4 = (a_0^2 + 5b_0^2)(r_1^2 + 5s_1^2)$. Επείδη οι παράγοντες είναι θετικοί ακέραιοι, $a_0^2 + 5b_0^2 = 1$ ή 2 ή 4.

$$a_0^2 + 5b_0^2 = 1 \therefore a_0 = \pm 1, b_0 = 0$$
$$a_0^2 + 5b_0^2 = 2 \quad \text{προφανώς αδύνατη}$$
$$a_0^2 + 5b_0^2 = 4 \therefore a_0 = \pm 2, b_0 = 0$$

άρα $a_0 + b_0 i\sqrt{5} = \pm 1$ ή ± 2. Στο αριστερό μέλος της (1.1) ανήκει το $1 + i\sqrt{5}$ (πάρε $x = 0, y = 1$) άρα πρέπει να ανήκει και στο δεξιό μέλος της (1.1), δηλαδή

$$1 + i\sqrt{5} = \pm 1(r_2 + s_2 i\sqrt{5}) \quad \text{ή} \quad \pm 2(r_2 + s_2 i\sqrt{5})$$

Το δευτερό προφανώς αποκλείεται, οπότε καταλήγω στο συμπέρασμα ότι $a_0 + b_0 i\sqrt{5} = \pm 1$. Άρα το $I = \langle \pm 1 \rangle = R$ και συμπεραίνω ότι $\{2x + (1+i\sqrt{5})y : x, y \in \mathbb{Z}\} = R$. Αλλά $1 \in R$, άρα πρέπει να υπάρχουν $x, y \in \mathbb{Z}$, ώστε $2x + (1+i\sqrt{5})y = 1$. Αυτό συνεπάγεται ότι $2x + y = 1$ και $y = 0$, οπότε $2x = 1$, άτοπο αφού $x \in \mathbb{Z}$.

Ορισμός 1.7. Έστω δακτύλιος R και ιδεώδες $I \neq \{0\},\ R$ του R. Λέω ότι το I είναι maximal (μεγιστικό) αν δεν υπάρχει γνήσιο μεγαλύτερο απο το I ιδεώδες του R, εκτός από τον ίδιο τον R, δηλ. είναι αδύνατον να βρω ιδεώδες J του R με $I \subsetneq J \subsetneq R$.
- Ισοδύναμη διατύπωση: Αν το J είναι ιδεώδες του R και $I \subseteq J$, τότε $J = I$ ή $J = R$.
- Ισοδύναμη διατύπωση: Αν το J είναι ιδεώδες του R και $I \subsetneq J$, τότε $J = R$.

Παράδειγμα. Στάνταρ παραδείγματα.

1. $R = \mathbb{Z}$. Εδώ όλα τα ιδεώδη είναι κύρια, δηλαδή της μορφής $\langle m \rangle$.
   Ισχύει το εξής: Το $\langle m \rangle$ είναι maximal $\iff$ m πρώτος.

2. $R = K[X]$ με K σώμα. Όλα τα ιδεώδη είναι κύρια, δηλαδή, της μορφής $I = \langle f(X) \rangle$.
   Ισχύει το εξής: Τό $\langle f(X) \rangle$ είναι maximal $\iff$ $f(X)$ ανάγωγο στο $K[X]$.

Πρόταση 1.8. *Ο δακτύλιος πηλίκο R/I είναι σώμα $\iff$ I είναι maximal ιδεώδες του R.*

Έστω K σώμα και $f(X) \in K[X]$ μη μηδενικό, $I = \langle f(X) \rangle$.

Πόρισμα 1.9. *Αν το K είναι σώμα και $p(x) \in K[X]$ ανάγωγο, τότε ο δακτύλιος πηλίκο $K/\langle p(X) \rangle$ είναι σώμα.*

Σχόλιο 1.10 (Αλγεβρο-φιλοσοφικό)**.** Έστω ένα σώμα F και ένα "άλλο" σώμα E. Επεκτείνω την έννοια του υποσώματος ως εξής. Το E είναι υπόσωμα του F αν υπάρχει μονομορφισμός σωμάτων $\imath : E \to F$. Η ειδική περίπτωση που $E \subseteq F$ και το E με τις πράξεις του F είναι σώμα, εμπίπτει στον παρπάνω ορισμό με $i = id_E : E \to F$.

Παράδειγμα 1.11. Το $\mathbb{C} = \{(a, b) : a, b \in \mathbb{R}\}$ με πράξεις

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2 + b_1 b_2, a_1 b_2 + a_2 b_1)$$

Η απεικόνιση $\imath : \mathbb{R} \to \mathbb{C}$ με $\imath(a) = (a, 0)$ είναι μονομορφισμός σωμάτων οπότε επιτρέπεται να λέω ότι το $\mathbb{R}$ είναι υπόσωμα του $\mathbb{C}$.

Ερώτημα 1.12. Μου δίδεται σώμα F και ανάγωγο πολυώνυμο $p(X) \in F[X]$ (εξ ορισμού του «ανάγωγου», το $p(X)$ δεν είναι σταθερό) και ρωτάω αν υπάρχει σώμα που να περιέχει το F, μέσα στο οποίο το $p(X)$ να έχει ρίζα. Το ερώτημά μου, ακριβέστερα διατυπωμένο, είναι, αν υπάρχει σώμα K του οποίου το F είναι υπόσωμα (οπότε μπορώ να δω το $p(X)$ ως πολυώνυμο με συντελεστές από το K), τ.ω. για κάποιο $a \in K$ να έχω $p(a) = 0$.

Η απάντηση είναι καταφατική. Συγκεκριμένα, ένα τέτοιο σώμα είναι το $K = F[X]/\langle p(X) \rangle$.

Απόδειξη. Ήδη ξέρω ότι είναι το K είναι σώμα διότι το $p(X)$ είναι ανάγωγο (Πόρισμα 1.9). Στη συνέχεια ισχυρίζομαι τα εξής:
- Το F είναι υπόσωμα του K.

Πράγματι, ο $\imath : F \to K$ με $a \mapsto a + \langle p(X) \rangle$ είναι μονομορφισμός σωμάτων. Δηλαδή "ταυτίζω" κάθε $a \in F$ με το $a + \langle p(X) \rangle \in K$. Για τα πολυώνυμα πάνω από το K χρησιμοποιώ τη μεταβλητή Y. Άρα το πολυώνυμο p το βλέπω ως πολυώνυμο $p(Y) \in K[Y]$. Δηλαδή, αν

$$p(X) = a_n X^n + \cdots + a_1 X + a_0 \in F[X],$$

τότε

$$p(Y) = (a_n + \langle p(X) \rangle) Y^n + \cdots + (a_1 + \langle p(X) \rangle) Y + (a_0 + \langle p(X) \rangle) \in K[Y].$$

- Το $p(Y)$ έχει ρίζα στο K. Μια τέτοια ρίζα είναι το στοιχείο $u := X + \langle p(X)\rangle$ του K. Πράγματι,

$$\begin{aligned} p(u) &= (a_n + \langle p(X)\rangle)(X + \langle p(X)\rangle)^n + \cdots + (a_1 + \langle p(X)\rangle)(X + \langle p(X)\rangle) + (a_0 + \langle p(X)\rangle) \\ &= a_n X^n + \cdots + a_1 X + a_0 + \langle p(X)\rangle \\ &= p(X) + \langle p(X)\rangle \\ &= 0 + \langle p(X)\rangle \\ &= 0_K \end{aligned}$$

- Επιπλέον, κάθε στοιχείο του K είναι της μορφής $f(u)$, όπου $f(X) \in F[X]$. Πράγματι, το τυπικό στοιχείο του K είναι της μορφής $f(X) + \langle p(X)\rangle$. Έστω

$$f(X) = b_m X^m + \cdots + b_1 X + b_0 \in F[X].$$

Τότε

$$\begin{aligned} f(X) + p(X) &= (b_m + \langle p(X)\rangle)(X + \langle p(X)\rangle)^m + \cdots + (b_1 + \langle p(X)\rangle)(X + \langle p(X)\rangle) + (b_0 + \langle p(X)\rangle) \\ &= (b_m + \langle p(X)\rangle)u^m + \cdots + (b_1 + \langle p(X)\rangle)u + (b_0 + \langle p(X)\rangle) \\ &= \imath(b_m)u^m + \cdots + \imath(b_1)u + \imath(b_0) \\ &\text{“=”}\ b_m u^m + \cdots + b_1 u + b_0 = f(u), \end{aligned}$$

όπου το “=” σημαίνει ότι έχω ταυτίσει κάθε $\imath(b_i)$ με το b_i. Άρα, με τα παραπάνω απέδειξα το εξής:

Θεώρημα 1.13. *Έστω σώμα F και ανάγωγο πολυώνυμο $p(X) \in F[X]$. Τότε υπάρχει σώμα K, του οποίου το F είναι υπόσωμα (ισοδύναμη διατύπωση υπάρχει επέκταση K του F) με τις εξής ιδιότητες:*

1. *Υπάρχει $u \in K$ με $p(u) = 0$, δηλαδή το p έχει ρίζα στο K.*
2. *$K = F[u]$ = σύνολο των πολυωνυμικών παραστάσεων του u με συντελεστές στο F.*

□

Αναφερόμενοι στο (2) του Θεωρήματος, αν $f(X) \in F[X]$ και $f(u) \neq 0$, το $1/f(u) \in K$ (αφού το K είναι σώμα), άρα υπάρχει $g(X) \in F[X]$ τ.ω. $1/f(u) = g(u)$. Δείτε το ερώτημα 1.19.

Ορισμός 1.14. Έστω σώμα F. Το σώμα E χαρακτηρίζεται επέκταση του F (συμβολισμοι: E/F, $E \geq F$, $F \leq K$) αν και μόνο αν το F είναι υπόσωμα του E.

Παρατήρηση 1.15. Η επέκταση E/F είναι F-διανυσματικός χώρος. Τα «διανύσματα» είναι τα στοιχεία του E και τα «βαθμωτά» είναι τα στοιχεία του F. «Πρόσθεση διανυσμάτων» είναι η πράξη της πρόσθεσης του E. Αν $v \in E$ και $a \in F$, τότε πολλαπλασιασμός του «βαθμωτού» a επί το «διάνυσμα» v σημαίνει το γινόμενο $a \cdot v$, θεωρούμενο ως πράξη του E.

Ορισμός 1.16. Τη διάσταση του F-διανυσματικού χώρου E (άπειρη ή πεπερασμένη) ονομάζουμε βαθμό της επέκτασης E/F και τη συμβολίζομε $[E : F]$.

Θεώρημα 1.17. *Έστω $F \subseteq E \subseteq K$ διαδοχικές επεκτάσεις σωμάτων (ισοδύναμος συμβολισμός $K/E/F$). Έστω $\{a_i\}_{i\in I}$ βάση της E/F και $\{b_j\}_{j\in J}$ βάση της K/E. Τα σύνολα δεικτών I και J μπορεί να είναι άπειρα ή πεπερασμένα. Τότε, το σύνολο $S = \{a_i b_j\}_{i\in I, j\in J}$ είναι βάση της επέκτασης K/F. Ειδικότερα, αυτό συνεπάγεται τη σχέση*

$$[K : F] = [K : E] \cdot [E : F]\,.$$

Απόδειξη. (i) Το S παράγει το K/F.
Απόδειξη: Έστω $u \in K$, τότε $u = \sum'_{j\in J} e_j b_j$ για κάποια $e_j \in E$. (Ο τόνος στο άθροισμα σημαίνει ότι το πολύ πεπερασμένο πλήθος εκ των $e_j \neq 0$. Ισοδύναμη διατύπωση, σχεδόν όλα τα $e_j = 0$.) Κάθε e_j γράφεται ως $\sum'_{i\in I} f_{ji} a_i$ για κάποια $f_{ji} \in F$. Άρα $u = \sum'_{j\in J} \left(\sum'_{i\in I} f_{ji} a_i\right) b_j = \sum'_{i\in I, j\in J} f_{ji} a_i b_j$, οπότε το u είναι F-γραμμικός συνδυασμός των $a_i b_j$.

(ii) Το S είναι F-γραμμικά ανεξάρτητο.
Απόδειξη: Έστω ένα πεπερασμένο υποσύνολο του $\{a_i b_j\}_{i\in I, j\in J}$. Δηλαδή, έστω πεπερασμένο $I_0 \subseteq I$ και πεπερασμένο $J_0 \subseteq J$. Θα δείξω ότι το $\{a_i b_j\}_{i\in I_0, j\in J_0}$ είναι F-γραμμικώς ανεξάρτητο. Έστω $\sum_{i\in I_0, j\in J_0} c_{ij} a_i b_j = 0$ με $c_{ij} \in F$. Τότε $\sum_{j\in J_0} \left(\sum_{i\in I_0} c_{ij} a_i\right) b_j$. Επειδή τα b_j είναι E-γραμμικώς ανεξάρτητα, έπεται ότι $\sum_{i\in I_0} c_{ij} a_i = 0$ για κάθε $j \in J_0$. Λόγω της F-γραμμικής ανεξαρτησίας των a_i έπεται ότι $\forall j \in J_0$ είναι όλα τα c_{ij} μηδενικά. □

Παρατήρηση 1.18. Το Θεώρημα 1.17 γενικεύεται με απλή χρήση επαγωγής, ως εξής:

Αν $K = E_n/E_{n-1}/\cdots/E_2/E_1/E_0 = F$ είναι διαδοχικές επεκτάσεις (πεπερασμένες είτε άπειρες), τότε ισχύει η σχέση

$$[K : F] = [E_n : E_0] = [E_n : E_{n-1}] \cdot [E_{n-1} : E_{n-2}] \cdots [E_2 : E_1] \cdot [E_1 : E_0] .$$

Στην περίπτωση που μία τουλάχιστον επέκταση E_{i+1}/E_i είναι άπειρη, ο βαθμός $[E_{i+1} : E_i]$ εἰναι άπειρος πληθάριθμος και τότε το γινόμενο στο δεξιό μέλος της παραπάνω σχέσης είναι γινόμενο πληθαρίθμων, όπως αυτός ορίζεται στη Θεωρία Συνόλων. Όμοιο σχόλιο και για τις διαδοχικές επεκτάσεις του Θεωρήματος 1.17.

Ερώτημα 1.19. Έστω e ένα στοιχείο μιας επέκτασης E του F. Ποια είναι η διαφορά μεταξύ των $F[e]$ και $F(e)$;

Απάντηση: $F[e]$ είναι το σύνολο των πολυωνυμικών παραστάσεων του e με συντελεσστές στο F, ενώ

$$F(e) = \left\{ \frac{f(e)}{g(e)} : f(X), g(X) \in F[X] \text{ και } g(e) \neq 0 \right\}$$

είναι το σύνολο όλων των πηλίκων των πολυωνυμικών πραστάσεων του e με συντελεστές στο F.

Εν γένει $F[e] \subsetneq F(e)$. Όμως, σύμφωνα με την παρατήρηση αμέσως μετά το Θεώρημα 1.13, ισχύει $F[u] = F(u)$.

Ορισμός 1.20. Έστω επέκταση E/F. Το $e \in E$ λέμε ότι είναι αλγεβρικό πάνω από το F αν υπάρχει μη μηδενικό πολυώνυμο $f \in F[X]$ με $f(e) = 0$. Αν δεν υπάρχει τέτοιο πολυώνυμο f, το e χαρακτηρίζεται υπερβατικό πάνω από το F.

Στην ειδική περίπτωση $\mathbb{C}/\mathbb{Q}$, παραλείπομε το «πάνω από το $\mathbb{Q}$» και λέμε απλώς «αλγεβρικός αριθμός» ή «υπερβατικός αριθμός».

Αν όλα τα στοιχεία της E είναι αλγεβρικά πάνω από το F τότε η επέκταση χαρακτηρίζεται αλγεβρική.

Πρόταση 1.21. *Έστω σώμα F και $p \in F[X]$ ανάγωγο.*

1. *Αν $f \in F[X]$ μη μηδενικό με $\deg f < \deg p$, τότε το f δεν έχει κοινή ρίζα με το p σε καμία επέκταση του F.*

2. *Αν το $f \in F[X]$ είναι ανάγωγο και έχει κοινή ρίζα με το F σε κάποια επέκταση του F τότε $f(X) = cp(X)$ για κάποιο $c \in F$. Άρα στην ειδική περίπτωση που τα p, f είναι μονικά (συντελεστές μεγιστοβάθμιου όρου το 1), τότε $f = p$, δηλαδή ανάγωγα μονικά πολυώνυμα του $F[X]$ με κοινή ρίζα σε κάποια επέκταση του F ταυτίζονται.*

Απόδειξη. Θα αποδείξουμε το 2ο μέρος. Έστω $f, p \in F[X]$ ανάγωγα και έστω E/F στην οποία έχουν κοινή ρίζα e. Αφού το p είναι ανάγωγο ή $p \mid f$ ή $\gcd(p, f) = 1$. Το 2ο αποκλείεται, διότι συνεπάγεται ότι υπάρχουν $g, h \in F[X]$ ώστε $p(X)g(X) + f(X)h(X) = 1$, το οποίο δίνει $0 = 1$ κάνοντας την αντικατάσταση $X \leftarrow e$ (βλέποντας την προηγούμενη σχέση ως ισότητα στο $E[X]$). Άρα $p \mid f$. Ομοίως, αν δούμε το f σαν ανάγωγο, οδηγούμαστε στη σχέση $f \mid p$. Άλλα $p \mid f$ και $f \mid p$ συνεπάγεται ότι $\exists c \in F$ ώστε $f(X) = cp(X)$. □

Θεώρημα 1.22. *Έστω σώμα F και επέκταση E/F και $\alpha \in E$ αλγεβρικό πάνω από το F. Τότε*

i) Υπάρχει ένα μοναδικό μονικό ανάγωγο $p \in F[X]$ τ.ω. $p(\alpha) = 0$.

ii) Ο δακτύλιος $F[\alpha]$ είναι σώμα, οπότε $F[\alpha] = F(\alpha)$. Άρα έχω την εξής εικόνα

$$\begin{array}{c} E \\ | \\ F[\alpha] = F(\alpha) \\ | \\ F \end{array}$$

iii) Αν $\deg p = n$, τότε τα $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ είναι βάση της επέκτασης $F[\alpha]/F$. Ειδικότερα, $[F[\alpha] : F] = n$.

Απόδειξη. (i) Εξ υποθέσεως, υπάρχει $f \in F[X]$ με $f(\alpha) = 0$. Φαντάζομαι την ανάλυση του f σε ανάγωγα του $F[X]$. Άρα, αφού $f(\alpha) = 0$, το α μηδενίζει κάποιο ανάγωγο παράγοντα του $f(X)$, έστω $p_1(X)$. Αν $c \in F$ ο συντελεστής του μεγιστοβάθμιου όρου του $p_1(X)$, τότε $p(X) = c^{-1}p_1(X)$ είναι μονικό ανάγωγο και έχει ρίζα το α. Λόγω της πρότασης 1.21, δεν υπάρχει άλλο μονικό ανάγωγο στο $F[X]$ με ρίζα το α.

(ii) Γενικά ισχύει

$$F[\alpha] \subseteq F(\alpha) \tag{1.2}$$

Θα δείξω ότι το F είναι σώμα. Προφανώς είναι ακέραια περιοχή, άρα έχω να δέιξω ότι κάθε μη μηδενικό $\in F[\alpha]$ έχει αντίστροφο. Το τυπικό μη μηδενικό στοιχείο του $F[\alpha]$ είναι της μορφής $f(\alpha)$ όπου $f(X) \in F[X]$ και $f(\alpha) \neq 0$. Τι σχέση έχει το f με το p του πρώτου σκέλους; Ή $p \mid f$ ή $\gcd(p, f) = 1$. Το πρώτο αποκλείεται, διότι $f = pg \implies f(\alpha) = p(\alpha)g(\alpha) = 0$ αντίφαση. Άρα ισχύει το 2ο και $\exists g, h \in F[X]$ τέτοια ώστε $p(X)g(X) + f(X)h(X) = 1$. Η αντικατάσταση $x \leftarrow \alpha$ δίνει $f(\alpha)h(\alpha) = 1$, δηλαδή το $h(\alpha)$ είναι αντίστροφο του $f(\alpha)$.

Τώρα ξέρω ότι $F[\alpha]$ σώμα. Γιατί στην (1.2) έχω τελικα ισότητα; Παίρνω ένα τυχαίο $\frac{f(\alpha)}{g(\alpha)} \in F(\alpha)$ όπου $f, g \in F[X]$ και $g(\alpha) \neq 0$. Επειδή $g(\alpha) \in F[\alpha]$ το οποίο είναι σώμα, έπεται ότι το $\frac{1}{g(\alpha)} \in F[\alpha]$ άρα και το $\frac{1}{g(\alpha)} f(\alpha) \in F[\alpha]$.

Έστω ότι το $p(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$, $c_i \in F$. Από τη σχέση $p(\alpha) = 0$ φαίνεται ότι α^n είναι F-γραμμικός συνδυασμός των $1, \alpha, \dots, \alpha^{n-1}$. Όμοια το $\alpha^{n+1} = -c_0\alpha - c_1\alpha^2 - \cdots - \alpha^n$. Αντικαθιστώ το $\alpha^n = -c_0 - c_1\alpha - \dots \alpha^{n-1}$. Άρα το α^{n+1} είναι F-γραμμικός συνδυασμός των $1, \alpha, \dots, \alpha^{n-1}$. Συνεχίζοντας επαγωγικά μπορώ να δείξω ότι όλες οι δυνάμεις του α γράφονται ως F-γραμμικοί συνδυασμοί των $1, \alpha, \dots, \alpha^{n-1}$. Άρα τα $1, \alpha, \dots, \alpha^{n-1}$ παράγουν τον $F[\alpha]$ πάνω από τον F.

Αν δεν ήταν γραμμικώς ανεξάρτητα, θα υπήρχαν $b_0, \dots, b_{n-1} \in F$ όχι όλα μηδέν ώστε $b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = 0$ δηλαδή θα υπήρχε πολυώυμο στο $F[X]$ βαθμού $\leq n - 1 < degp$ που θα είχε κοινή ρίζα με το p. Άτοπο, πάλι χάρη στην Πρόταση 1.21. □

Ορισμός 1.23. Το ανάγωγο πολυώνυμο $p \in F[X]$ του πρώτου σκέλους του Θεωρήματος 1.22 καλείται ελάχιστο πολυώνυμο του α πάνω από το F.

Παρατήρηση 1.24. Ο όρος «ελάχιστο πολυώνυμο» είναι σχετικός, εξαρτώμενος από το σώμα πάνω από το οποίο θεωρούμε το πολυώνυμο. Έτσι, για παράδειγμα, το ελάχιστο πολυώνυμο του $\sqrt{2}$ πάνω από το $\mathbb{Q}$ είναι $X^2 - 2$, ενώ το ελάχιστο πολυώνυμο του $\sqrt{2}$ πάνω από το $\mathbb{R}$ είναι $X - \sqrt{2}$.

Ασκήσεις

Άσκηση 1.25. Έστω $p(X) = X^2 + X + 1 \in \mathbb{Q}[X]$ και $I = \langle p(X) \rangle$. Δείξτε ότι το $p(X)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$. Σύμφωνα με το Πόρισμα 1.9, ο δακτύλιος $K[X]/I$ είναι σώμα. Υπολογίστε το αντίστροφο στοιχείο του $(X^3 + 3X^2 + 4X + 3) + I$.

Άσκηση 1.26. Έστω πεπερασμένη επέκταση E/F, $e \in E$ και $p(X) \in F[X]$ το ελάχιστο πολυώνυμο του e πάνω από το F. Αποδείξτε ότι ο βαθμός του $p(X)$ διαιρεί τον βαθμό $[E : F]$ της επέκτασης E/F. Υπόδειξη. Θεωρήστε την επέκταση $F[e]/F$. Είναι $E/F[e]/F$.

Άσκηση 1.27. Έστω $K/E/F$ και $u \in K$ αλγεβρικό πάνω από το F. Αποδείξτε τα εξής:

(i) Το u είναι αλγεβρικό πάνω από το E.

(ii) Έστω $p_F(X)$ και $p_E(X)$ τα ελάχιστα πολυώνυμα του u πάνω από το F και πάνω από το E αντιστοίχως. Προφανώς, $p_F(X) \in E[X]$. Αποδείξτε ότι $p_E(X) \mid p_F(X)$.

Άσκηση 1.28. Το πολυώνυμο $f(X) = X^3 + 3X^2 + 6X + 3 \in \mathbb{Q}[X]$ είναι ανάγωγο, όπως προκύπτει από το *κριτήριο Eisenstein*. Θεωρήστε την επέκταση $\mathbb{Q}(u)/\mathbb{Q}$ όπου $f(u) = 0$. Σύμφωνα με το Θεώρημα 1.22, ο βαθμός της επέκτασης είναι 3 και κάθε στοιχείο του $\mathbb{Q}(u)$ είναι της μορφής $c_0 + c_1 u + c_2 u^2$, με τα c_i ρητούς αριθμούς. Γράψτε το στοιχείο $(u^2 + u - 1)^{-1}$ με τη μορφή $c_0 + c_1 u + c_2 u^2$.

Υπόδειξη: Πρέπει να βρείτε $c_0, c_1, c_2 \in \mathbb{Q}$ ώστε να ισχύει η σχέση $(u^2+u-1)(c_0+c_1u+c_2u^2) = 1$. Κάνετε τις πράξεις στο αριστερό μέλος, εκφράζοντας τα u^3, u^4 συναρτήσει των $1, u, u^2$, οπότε θα καταλήξετε σε παράσταση της μορφής $L_0(c_0, c_1, c_2) + L_1(c_0, c_1, c_2)u + L_2(c_0, c_1, c_2)u^2 = 1 = 1 + 0 \cdot u + 0 \cdot u^2$, με τα L_i γραμμικές παραστάσεις των c_0, c_1, c_2. Αφού τα $1, u, u^2$ είναι βάση της επέκτασης $\mathbb{Q}(u)/\mathbb{Q}$, πρέπει $L_0 = 1, L_1 = 0, L_2 = 0$ οπότε θα λύσετε ένα 3×3 γραμμικό σύστημα μα αγνώστους c_0, c_1, c_2.

Κεφάλαιο 2

2.1 2^{η} Εβδομάδα

Πρόταση 2.1. *Κάθε πεπερασμένη επέκταση είναι αλγεβρική.*

Απόδειξη. Έστω E/F επέκταση πεπερασμένη, $[E:F] = n \in \mathbb{N}$. Έχω να δείξω ότι κάθε $e \in E$ είναι αλγεβρικό πάνω από το F. Θεωρώ τα στοιχεία $1, e, \dots, e^n \in E$. Αυτά είναι $(n+1)$ στοιχεία του E, ο οποίος έχει διάσταση n, άρα είναι γραμμικώς εξαρτημμένα. Άρα $\exists\, c_0, \dots, c_n \in F$ όχι όλα 0 τ.ω. $c_0 + c_1 e + \cdots + c_n e^n = 0$. Δηλαδή το e είναι ρίζα του μη μηδενικού πολυωνύμου $c_0 + c_1 X + \cdots + c_n X^n \in F[X]$, άρα το e είναι αλγεβρικό πάνω από το F. □

Πρόταση 2.2. *Έστω επέκταση E/F. Θεωρώ το ενδιάμεσο υποσύνολο*

$$\mathrm{Cl}(E/F) = \{\alpha \in E : \alpha \text{ αλγεβρικό πάνω από το } F\}.$$

Το $\mathrm{Cl}(E/F)$ είναι σώμα, υπόσωμα του E και, φυσικά, η επέκταση $\mathrm{Cl}(E/F)/F$ είναι αλγεβρική.
Το $\mathrm{Cl}(E/F)$ λέγεται αλγεβρική κλειστότητα του F στο E.

Απόδειξη. Αρκεί να δείξω ότι για $a, b \in \mathrm{Cl}(E/F)$ με $b \notin 0$ είναι και $a - b$ και $ab^{-1} \in \mathrm{Cl}(E/F)$. Πράγματι, αυτά ισχύουν για τον εξής λόγο: Έχομε τις διαδοχικές επεκτάσεις $F(a,b) = F(a)(b)/F(a)/F$, κάθε μία από τις οποίες είναι πεπερασμένη λόγω του Θεωρήματος 1.22 (iii). Τότε, από το Θεώρημα 1.17 συμπεραίνομε ότι η επέκταση $F(a,b)/F$ είναι πεπερασμένη, άρα αλγεβρική, βάσει της Πρότασης 2.1. Άλλα προφανώς, $a - b, ab^{-1} \in F(a,b)$ άρα είναι αλγεβρικά πάνω από το F και συνεπώς ανήκουν στο $\mathrm{Cl}(E/F)$. □

Ορισμός 2.3. Έστω E/F επέκταση σωμάτων και $\emptyset \neq S \subseteq E$. Ορίζομε το σύνολο $F(S)$ ως το υποσύνολο του E, με την εξής ιδιότητα: $e \in F(S)$ αν και μόνο αν υπάρχει πεπερασμένο πλήθος στοιχείων του S, έστω $s_1, \dots, s_n$ και πολυώνυμα $f[X_1, \dots, X_n],\ g[X_1, \dots, X_n] \in F[X_1, \dots, X_n]$ ώστε $g(s_1, \dots, s_n) \neq 0$ και $e = f(s_1, \dots, s_n)/g(s_1, \dots, s_n)$.

Στην περίπτωση που το S είναι πεπερασμένο, έστω $S = \{s_1, \dots, s_n\}$, αντί για $F(\{s_1, \dots, s_n\})$ γράφομε, απλούστερα, $F(s_1, \dots, s_n)$.

Πρόταση 2.4. *Έστω επέκταση σωμάτων E/F, S μη κενό υποσύνολο του E και το σύνολο $F(S)$ του Ορισμού 2.3. Ισχύουν τα εξής: Το $F(S)$ σώμα και, μάλιστα, είναι το ελάχιστο υπόσωμα του E που περιέχει το F και το S.*

Απόδειξη. Κατ' αρχάς θα δείξομε ότι το $F(S)$ είναι υπόσωμα. Έστω $\frac{f(s_1,\dots,s_n)}{g(s_1,\dots,s_n)}$ και $\frac{p(s'_1,\dots,s'_m)}{q(s'_1,\dots,s'_m)}$ στοιχεία του $F(S)$. Τότε

$$\frac{f(s_1,\dots,s_n)}{g(s_1,\dots,s_n)} - \frac{p(s'_1,\dots,s'_m)}{q(s'_1,\dots,s'_m)} = \frac{f(s_1,\dots,s_n)q(s'_1,\dots,s'_m) - g(s_1,\dots,s_n)p(s'_1,\dots,s'_m)}{g(s_1,\dots,s_n)q(s'_1,\dots,s'_m)}$$
$$\frac{f(s_1,\dots,s_n)}{g(s_1,\dots,s_n)} \cdot \frac{p(s'_1,\dots,s'_m)}{q(s'_1,\dots,s'_m)} = \frac{f(s_1,\dots,s_n)p(s'_1,\dots,s'_m)}{g(s_1,\dots,s_n)q(s'_1,\dots,s'_m)}$$

Και στις δύο περιπτώσεις τα κλάσματα στο δεξιό μέλος είναι πηλίκα πολυωνυμικών παραστάσεων των $s_1,\dots,s_n,s'_1,\dots,s'_m$ με συντελεστές από το F (και μη μηδενικούς παρονομαστές), άρα το $F(S)$ είναι υποδακτύλιος του E. Το γεγονος ότι είναι υπόσωμα προκύπτει εύκολα, καθώς αν $\frac{f(s_1,\dots,s_n)}{g(s_1,\dots,s_n)}$ είναι μη μηδενικό στοιχείο του $F(S)$, τότε $f(s_1,\dots,s_n)\neq 0$, άρα το $\frac{g(s_1,\dots,s_n)}{f(s_1,\dots,s_n)}$ έχει νόημα ως στοιχείο του $F(S)$ και, προφανώς, είναι το αντίστροφο του $\frac{f(s_1,\dots,s_n)}{g(s_1,\dots,s_n)}$.

Έχοντας αποδείξει ότι το $F(S)$ είναι υπόσωμα του E, μένει να αποδείξομε ότι είναι το ελάχιστο υπόσωμα του E που περιέχει το σύνολο $F\cup S$. Αν το K είναι υπόσωμα του E με $F\cup S\subseteq K$, θα δείξουμε ότι $F(S)\subseteq K$. Έστω $\frac{f(s_1,\dots,s_n)}{g(s_1,\dots,s_n)}$ το τυπικό στοιχείο του $F(S)$. Αφού το K είναι κλειστό ως προς τις πράξεις του σώματος και τα $f(s_1,\dots,s_n)$, $g(s_1,\dots,s_n)$ προκύπτουν απο άθροισμα γινομένων μεταξύ στοιχείων του F και των $s_1,\dots,s_n$, τα οποία βρίσκονται εντός του E, έχουμε ότι $f(s_1,\dots,s_n),g(s_1,\dots,s_n)\in K$. Επίσης, αφού $g(s_1,\dots,s_n)\neq 0$ και το K είναι σώμα, έπεται ότι και το $g(s_1,\dots,s_n)^{-1}$ ανήκει στο K. Συνεπώς, $\frac{f(s_1,\dots,s_n)}{g(s_1,\dots,s_n)} = f(s_1,\dots,s_n)g(s_1,\dots,s_n)^{-1}\in K$, άρα $F(S)\subseteq K$. □

Παρατήρηση 2.5. Έστω $\phi: K\to K'$ ισομορφισμός σωμάτων. Τότε ο ϕ επεκτείνεται σε ισομορφισμό δακτυλίων $K[X]\to K'[X]$ ώστε $X\mapsto X$. Συνήθως θα χρησιμοποιούμε και για αυτόν το γράμμα ϕ και για κάθε $f\in K[X]$ θα συμβολίζομε με ϕf την εικόνα f μέσω αυτού του ομομορφισμού, ο οποίος ορίζεται ως εξής:

$$K[X]\ni f = c_0+c_1X+\cdots+c_nX^n \mapsto \phi f = \phi(c_0)+\phi(c_1)X+\cdots+\phi(c_n)X^n\in K'[X].$$

Είναι απλό να δούμε ότι, αν το $p\in K[X]$ είναι ανάγωγο, τότε και το $p'=\phi p\in K'[X]$ είναι ανάγωγο. Πράγματι, έστω $p'=g'h'$ με $g',h'\in F'[X]$ όχι σταθερά. Καθώς η ϕ είναι επί, υπάρχουν $g,h\in K[X]$, μη σταθερά, με $\phi g=g'$ και $\phi h=h'$, οπότε $\phi p = g'h' = (\phi g)(\phi h)=\phi(gh)$. Επειδή η ϕ είναι 1-1, $p=gh$ άτοπο καθώς g,h αναγκαστικά μη σταθερά.

Πρόταση 2.6. *Έστω $\phi: F\to F'$ ισομορφισμός σωμάτων, $p\in F[X]$ ανάγωγο και $p'=\phi f\in F'[X]$. Έστω ότι σε κάποια επέκτασης K/F έχω κάποιο $u\in K$ που είναι ρίζα του p και σε κάποια επέκταση K'/F' έχω κάποιο $u'\in K$ που είναι ρίζα του p'. Τότε ο ϕ επεκτείνεται σε ισομορφισμό σωμάτων $\tilde\phi: F[u]\to F'[u']$ με την ιδιότητα $\tilde\phi(u)=u'$.*

Απόδειξη. Ορίζομε τον $\tilde\phi$ ως εξής,

$$\tilde\phi(c_0+c_1u+\cdots+c_nu^n) \coloneqq \phi(c_0)+\phi(c_1)u'+\cdots+\phi(c_n)u'^n,$$

και πρέπει να αποδείξομε ότι ο $\tilde\phi$ είναι ομομορφισμός σωμάτων και, επιπλέον, είναι 1-1 και $\tilde\phi$ επί. Το ότι ο $\tilde\phi$ είναι επιμορφισμός, είναι εύκολο, οπότε, έχοντας αποδείξει αυτό, δείχνομε ότι ο $\tilde\phi$ είναι 1-1. Αυτό ισχύει αν και μόνο αν $\ker\tilde\phi=\{0\}$. Έστω, λοιπόν, ότι $f(X)=c_0+c_1X+\cdots+c_nX^n\in F[X]$ και $f(u)\in\ker\tilde\phi$. Αυτό σημαίνει ότι

$$0=\tilde\phi(c_0+c_1u+\cdots+c_nu^n)=\phi(c_0)+\phi(c_1)u'+\cdots+\phi(c_n)u'^n=(\phi f)(u)$$

Αφού ο $\phi : F[X] \to F[X]$ είναι ισομορφισμός δακτυλίων (βλ. Παρατήρηση 2.5) και το p είναι ανάγωγο στο $F[X]$, έπεται ότι το p' είναι ανάγωγο στο $F'[X]$. Έχομε λοιπόν ότι το ϕf έχει κοινή ρίζα με το ανάγωγο $p' \in K'[X]$. Άρα $p' \mid \phi f$ που σημαίνει $\exists g' \in F'[X] : \phi f = p'g'$. Λόγω του ισομορφισμού $\phi : K[X] \to K'[X]$ (εδώ μας χρειάζεται μόνο το «επί») $\exists g \in K[X] : \phi g = g'$. Αραμ η σχέση $\phi f = p'g'$ γίνεται $\phi f = (\phi f)(\phi g) =$ (ϕ είναι ομομορφισμός) $\phi(fg)$ και λόγω του ότι ο ϕ είναι 1-1, έπεται ότι $f = pg$, άρα $f(u) = 0$. Συμπεραίνομε ότι το 0 είναι το μόνο στοιχείο του $F[u]$ που απεικονίζεται μέσω του $\tilde{\phi}$ στο $0 \in F'[u']$. □

Ορισμός 2.7. Έστω σώμα F και $f \in F[X]$, βαθμού $n \geq 1$. Μία επέκταση K/F λέμε ότι είναι σώμα διάσπασης (ή σώμα ριζών) του f πάνω από το F αν πληροί τις εξής απαιτήσεις.

(i) Υπάρχουν $c \in F$ και $u_1, \dots, u_n \in K$ ώστε $f(X) = c(X - u_1) \dots (X - u_n)$.

(ii) $K = F[u_1, \dots, u_n]$.

Ορισμός 2.8. Τη συνθήκη (i) του παραπάνω ορισμού διατυπώνομε ισοδύναμα λέγοντας ότι *το f διασπάται στο K*. Άρα, λέγοντας ότι το f διασπάται στο K, καταλαβαίνομε ότι, αν αναλύσομε το f σε ανάγωγα πολυώνυμα του $K[X]$, όλα αυτά τα πολυώνυμα είναι πρώτου βαθμού.

Πρόταση 2.9. *Έστω K/F σώμα διάσπασης του $f \in K[X]$ και E ενδιάμεση επέκταση, δηλαδή, $F \leq E \leq K$. Αν το f διασπάται και στο E, τότε $E = K$.*

Απόδειξη. Έστω $\deg f = n$. Το f διασπάται στο K, άρα $f(X) = c(X - u_1) \cdots (X - u_n)$ με τα $u_1, \dots, u_n \in K$ και c τον συντελεστή μεγιστοβαθμίου όρου του f. Επιπλέον, εξ ορισμού του σώματος διάσπασης, είναι $K = F(u_1, \dots, u_n)$. Το f, όμως, διασπάται και στο E, άρα $f(X) = c(X - e_1) \cdots (X - e_n)$ με τα $e_1, \dots, e_n \in E$. Άρα στο $K[X]$ έχω τη σχέση $(X - e_1) \cdots (X - e_n) = (X - u_1) \cdots (X - u_n)$. Λόγω της μονοσήμαντης ανάλυσης σε ανάγωγα πολυώνυμα, η οποία ισχύει στον δακτύλιο $K[X]$, συμπεραίνω ότι τα πολυώνυμα $X - e_1, \dots, X - e_n$ είναι μια μετάθεση των πολυωνύμων $X - u_1, \dots, X - u_n$. Άρα τα σύνολα $\{e_1, \dots, e_n\}$ και $\{u_1, \dots, u_n\}$ ταυτίζονται, οπότε $u_1, \dots, u_n \in E$. Αλλά τότε $K = F(u_1, \dots, u_n) \subseteq E$. Είναι και $E \subseteq K$, άρα $E = K$. □

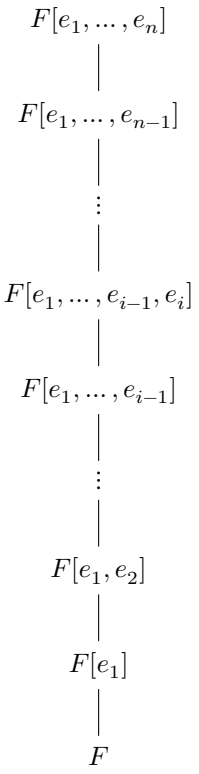
Θεώρημα 2.10. *Έστω σώμα F και $f \in F[X]$, $\deg f \geq 1$, τότε υπάρχει σώμα διάσπασης του F πάνω από το F. Δηλαδή, υπάρχει επέκταση του F, η οποία είναι σώμα διάσπασης του f.*

Απόδειξη. Αναλύω το f σε ανάγωγα του $F[X]$, έστω $f = p_1 \dots p_k$. Αν όλα τα $p_1, \dots, p_k$ είναι πρώτου βαθμού, τότε προφανώς το ζητούμενο K είναι το ίδιο το F. Έστω τώρα ότι (χ.β.τ.γ.) $\deg(p_1) > 1$. Τότε μπορώ να βρω επέκταση F_1 του F με τις εξής ιδιότητες: $\exists u_1 \in F_1$ τ.ω. $p_1(u_1) = 0$ και $F_1 = F[u_1]$ σύμφωνα με το Θεώρημα 1.13. Οπότε $f(X) = (X - u_1)f_1(X)$, όπου $f_1 \in F_1[X]$.

Τώρα έχω την εξής νέα κατάσταση. Ένα νέο σώμα F_1 (επέκταση του F), $f_1 \in F_1[X]$ με $\deg(f_1) = \deg(f) - 1$. Θα επαναλάβω το συλλογισμό με F_1 και f_1 στη θέση των F και f, κ.ο.κ. μέχρι να φτάσω σε μία ανάλυση $f(X) = (X - u_1) \dots (X - u_{n-1})(X - u_n)c$ όπου $c \in F$. □

Πρόταση 2.11. *Έστω επέκταση σωμάτων E/F και για τα $e_1, \dots, e_n \in E$ ισχύουν τα εξής: Το e_1 είναι αλγεβρικό πάνω από το F και για κάθε $i = 1, \dots, n-1$ το e_{i+1} είναι αλγεβρικό πάνω από το $F[e_1, \dots, e_i]$. Τότε η επέκταση $F[e_1, \dots, e_n]/F$ είναι πεπερασμένη, άρα και αλγεβρική.*

Απόδειξη. Έχομε τον παρακάτω «πύργο» επεκτάσεων:



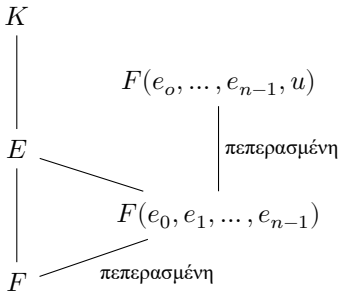
Εφαρμόζομε το Θεώρημα 1.22 διαδοχικά: Η επέκταση $F[e_1]/F$ είναι πεπερασμένη. Αφού το e_2 είναι αλγεβρικό πάνω από το $F[e_1]$, η επέκταση $F[e_1, e_2]/F[e_1]$ είναι πεπερασμένη …το e_i είναι αλγεβρικό πάνω από το $F[e_1, \dots, e_{i-1}]$ άρα η επέκταση $F[e_1, \dots, e_{i-1}, e_i]/F[e_1, \dots, e_{i-1}]$ είναι πεπερασμένη κ.ο.κ. Δηλαδή, στον παραπάνω «πύργο», κάθε σώμα είναι πεπερασμένη επέκταση του σώματος που βρίσκεται αμέσως παρακάτω. Εφαρμόζοντας τώρα την Παρατήρηση 1.18 συμπεραίνομε ότι η επέκταση $F[e_1, \dots, e_n]/F$ είναι πεπερασμένη. □

Θεώρημα 2.12. *Θεωρώ τις διαδοχικές επεκτάσεις $K/E/F$ για τις οποίες ισχύει ότι η E/F και η K/E είναι αλγεβρικές. Τότε και η K/F είναι αλγεβρική.*

Απόδειξη. Έστω τυχαίο $u \in K$. Θα δείξω ότι το u είναι αλγεβρικό πάνω από το F. Το u είναι αλγεβρικό πάνω από το E. Άρα

$$u^n + e_{n-1}u^{n-1} + \cdots + e_1 u + e_0 = 0$$

για κάποια $e_1, \dots, e_{n-1} \in E$.



Η επέκταση $F(e_0,\dots,e_{n-1})/F$ είναι πεπερασμένη αφού όλα τα $e_0,\dots,e_{n-1}$ είναι αλγεβρικά πάνω από το F (Πρόταση 2.11). Όμοια και η επέκταση $F(e_0,\dots,e_{n-1},u)/F(e_0,\dots,e_{n-1})$ και συνεπώς και η $F(e_0,\dots,e_{n-1},u)/F$ είναι πεπερασμένη άρα και αλγεβρική. Άρα το u είναι αλγεβρικό πάνω από το F. □

Θεώρημα 2.13. *Κάθε διάγραμμα όπως το παρακάτω (το $\sim$ πάνω από $\longrightarrow$ δηλώνει ισομορφισμό σωμάτων),*

$$\begin{array}{ccc} K & & K' \\ | & & | \\ F & \xrightarrow[\phi]{\sim} & F' \end{array}$$

όπου το K είναι σώμα διάσπασης ενός πολυωνύμου $f \in F[X]$ πάνω από το F και K' σώμα διάσπασης του πολυωνύμου $\phi f = f' \in F'[X]$ πάνω από το F', μπορεί να συμπληρωθεί με ένα ισομορφισμό $\tilde{\phi} : K \to K'$ ο οποίος επεκτείνει τον ϕ.

Απόδειξη. Επαγωγική απόδειξη επί του βαθμού d της αριστερής επέκτασης (της K/F).

Αν $d = 1$, τότε (άσκηση 2.15 (ii)) $K = F$. Άρα το f είναι της μορφής $f = c(X-a_1)\dots(X-a_n)$ όπου $c, a_1,\dots,a_n \in F$, τότε $f' = \phi(c)(X-\phi(a_1))\dots(X-\phi(a_n))$ με τα $\phi(c), \phi(a_1),\dots,\phi(a_n) \in F'$. Άρα το f' διασπάται στο F' που είναι υπόσωμα του σώματος διάσπασης K' του f'. Από την Πρόταση 2.9 έπεται ότι $K' = F'$. Συνεπώς, $K = F$, $K' = F'$ και ο ζητούμενος ισομορφισμός $\tilde{\phi}$ δεν είναι άλλος από τον ίδιο τον ϕ.

Επαγωγική Υπόθεση: Έστω $m > 1$. Υποθέτω ότι για κάθε διάγραμμα όπως στην εκφώνηση, για το οποίο $d < m$ ισχύει το θεώρημα.

Θεωρώ ένα διάγραμμα, στο οποίο $d = m$ και θα δείξω ότι ο ϕ μπορεί να επεκταθεί σε ισομορφισμό $\tilde{\phi} : K \to K'$. Αφού $[K : F] = m > 1$, έπεται ότι αν αναλύσω το f σε ανάγωγα του $F[X]$, ένα τουλάχιστον από αυτά, έστω $p \in F[X]$ έχει $\deg p > 1$. Επιλέγω μία οποιαδήποτε ρίζα α του p στο K και μία οποιαδήποτε ρίζα α' του $p' = \phi p$ στο K'. Από την Πρόταση 2.6, υπάρχει ισομορφισμός $\phi_1 : F_1 := F[\alpha] \to F_1' := F'[\alpha']$ με $\phi_1(\alpha) = \alpha'$.

Θεωρώ το εξής διάγραμμα.

$$\begin{array}{ccc} K & & K' \\ | & & | \\ F_1 & \xrightarrow[\phi_1]{\sim} & F_1' \end{array}$$

Ο βαθμός της επέκτασης K/F_1 είναι $[K : F_1] = \frac{[K:F]}{[F_1:F]} = \frac{m}{\deg p} < m$. Από την άσκηση 2.15 (iii), το K είναι σώμα διάσπασης του f πάνω από το F_1 και το K' σώμα διάσπασης του f' πάνω από το F'. Εφαρμόζοντας την επαγωγική υπόθεση στο παραπάνω διάγραμμα συμπεραίνομε ότι ο ϕ_1 επεκτείνεται σε ισομορφισμό $\tilde{\phi} : K \to K'$ και, προφανώς, ο $\tilde{\phi}$ είναι επέκταση του ϕ. □

Πόρισμα 2.14. *Αν το $f \in F[X]$ είναι μη μηδενικό, τότε όλα τα σώματα διάσπασης του f πάνω από το F είναι F-ισόμορφα, δηλαδη αν K, K' είναι σώματα διάσπασης του f πάνω από το F τότε υπάρχει ισομορφισμός $\psi : K \to K'$ με $\psi(a) = a \ \ \forall a \in F$.*

Απόδειξη. Εφαρμόζω το θεώρημα για $F' = F$ και $\phi = id_F$. □

Ασκήσεις

Άσκηση 2.15. Οι απαντήσεις στά παρακάτω ερωτήματα πρέπει να είναι πολύ σύντομες. Εκτός από θεωρήματα/προτάσεις, μπορείτε να βασιστείτε σε προηγούμενες ασκήσεις:

(i) Αν $[K : F] = 1$, τότε $K = F$.

(ii) Αν το K είναι σώμα διάσπασης του $f \in F[X]$ πάνω από το F και E είναι ενδιάμεση επέκταση (δηλαδή, $F \leq E \leq K$), τότε το K είναι σώμα διάσπασης του f και πάνω από το E.

Άσκηση 2.16. Θεωρήστε τα πολυώνυμα $X^2-3,\ X^3-2 \in \mathbb{Q}[X]$. Προφανώς, και τα δύο αυτά πολυώνυμα είναι ανάγωγα πάνω από το $\mathbb{Q}$. Έστω επέκταση $K/\mathbb{Q}$ η οποία περιέχει μια ρίζα α του πρώτου πολυωνύμου και μία ρίζα β του δεύτερου. (Δείτε το K ως αφηρημένο σώμα και όχι ως υπόσωμα του $\mathbb{C}$.)

(i) Δείτε το $X^2 - 3$ ως πολυώνυμο πάνω από το σώμα $\mathbb{Q}[\alpha]$ και, ως τέτοιο, δείξτε ότι είναι ανάγωγο.

(ii) Έστω $E = \mathbb{Q}[\alpha, \beta]$. Βρείτε τον βαθμό μια βάση της επέκτασης $E/\mathbb{Q}$ συναρτήσει των α, β

Άσκηση 2.17. Έστω $f(X) = X^3 - 9X + 9 \in \mathbb{Q}[X]$ και $K = \mathbb{Q}[u]$ όπου u είναι ρίζα του f.

(i) Αποδείξτε ότι και τα στοιχεία $-6 + u + u^2$, $6 - 2u - u^2$ είναι ρίζες του f. Γιατί οι ρίζες αυτές είναι διαφορετικές από την u και διαφορετικές μεταξύ τους;

(ii) Έστω σ ο $\mathbb{Q}$-αυτομορφισμός του K που στέλνει τη ρίζα u στη ρίζα $-6 + u + u^2$ (τέτοιος αυτομορφισμός υπάρχει λόγω της Πρότασης 2.6). Υπολογίστε τα $\sigma(-6 + u + u^2)$ και $\sigma^3(u)$.

Σημείωση. Για ακέραιο $n \geq 1$, σ^n σημαίνει $\underbrace{\sigma \circ \sigma \circ \cdots \circ \sigma}_{n \text{ φορές}}$. Ορίζουμε σ^0 να σημαίνει τον ταυτοτικό ισομορφισμό.

(iii) Ποιο είναι το σώμα διάσπασης του f πάνω από το $\mathbb{Q}$;

Άσκηση 2.18. Έστω $K = \mathbb{Q}[\omega, \rho]$ όπου ω είναι ρίζα του $f(X) = X^2 + X + 1 \in \mathbb{Q}[X]$ και ρ ρίζα του $X^3 - 2 \in \mathbb{Q}[X]$. Αποδείξτε ότι το K είναι σώμα διάσπασης του $X^3 - 2$ πάνω από το $\mathbb{Q}$. Υπολογίστε μια βάση της επέκτασης $K/\mathbb{Q}$. Μη θεωρήσετε τους ω, ρ ως πραγματικούς ή μιγαδικούς αριθμούς.

Υπόδειξη. Για τον υπολογισμό βάσης της επέκτασης θα κάνετε χρήση του Θεωρήματος 1.17.

Άσκηση 2.19. Θεωρήστε τις διαδοχικές επεκτάσεις $F \leq E \leq K$ και έστω ότι το $u \in K$ είναι αλγεβρικό πάνω από το F. Αποδείξτε ότι το u είναι αλγεβρικό πάνω από το E και $[E(u) : E] \leq [F(u) : F]$.

Άσκηση 2.20. Έστω $f, g \in F[X]$ ανάγωγα με αντίστοιχους βαθμούς m, n. Έστω επέκταση K/F η οποία περιέχει ρίζα α του f και β του g και $E = F[\alpha, \beta]$.

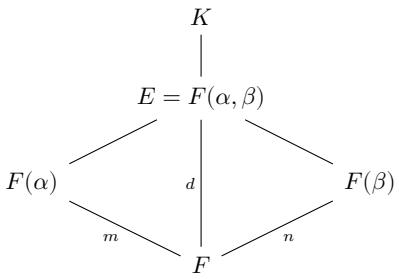
(i) Αποδείξτε ότι $[E : F] \leq mn$.

Υπόδειξη. Χρησιμοποιήστε την άσκηση 2.19.

(ii) Αποδείξτε ότι $\text{ΕΚΠ}(m, n) \mid [E : F]$.

(iii) Αν οι m, n είναι πρώτοι μεταξύ τους, αποδείξτε ότι $[E : F] = mn$.

Υπόδειξη. Το παρακάτω διάγραμμα ίσως σας φανεί πολύ βοηθητικό. Ποια είναι η σχέση των m και n με το d;



Κεφάλαιο 3

3.1 3^{η} Εβδομάδα

Η εξαιρετικά σημαντική ιδιότητα της επέκτασης $\mathbb{C}/\mathbb{R}$ είναι ότι κάθε $f \in \mathbb{R}[X]$ μη σταθερό, αναλύεται σε πρωτοβάθμια του $\mathbb{C}[X]$. Επόμενος στόχος μας είναι να εξετάσομε το εξής: Αν αντί του $\mathbb{R}$ είχαμε ένα οποιοδήποτε σώμα F, υπάρχει επέκταση C/F με ανάλογη ιδιότητα, δηλαδή, κάθε μη σταθερό πολυώνυμο του $F[X]$ να αναλύεται πλήρως σε πρωτοβάθμια του $C[X]$; Μια πρώτη προσέγγιση στο ερώτημα γίνεται μέσω του επόμενου θεωρήματος.

Θεώρημα 3.1. *Έστω σώμα C. Οι εξής συνθήκες είναι ισοδύναμες:*

1. *Κάθε μη σταθερό $f \in C[X]$ έχει μία τουλάχιστον ρίζα στο C.*
2. *Κάθε μη σταθερό $f \in C[X]$ διασπάται στο C.*
3. *Κάθε ανάγωγο του $C[X]$ είναι πρωτοβάθμιο.*
4. *Δεν υπάρχει γνήσια αλγεβρική επέκταση του C.*

Ορισμός 3.2. Κάθε σώμα που ικανοποιεί τις παραπάνω ισοδύναμες συνθήκες χαρακτηρίζεται αλγεβρικώς κλειστό.

Απόδειξη. $(1) \implies (2)$: Απλούστατο.

$(2) \implies (3)$: Απλούστατο.

$(3) \implies (4)$: Έστω D/C αλγεβρική επέκταση του C. Έστω ένα $a \in D\cdot$ θα δείξω ότι το $a \in C$. Το a είναι αλγεβρικό πάνω από το C, άρα μπορώ να θεωρήσω το ελάχιστο πολυώνυμο του a πάνω από το C, έστω $p \in C[X]$. Το p είναι ανάγωγο εξ ορισμού του ελαχίστου πολυωνύμου. Από την υπόθεση, έπεται ότι $\deg p = 1$ άρα το a που είναι ρίζα του p, ανήκει στο C.

$(4) \implies (1)$: Έστω μη σταθερό $f \in C[X]$. Θεωρώ ένα ανάγωγο παράγοντα του f, έστω τον $p \in C[X]$. Από το Θεώρημα 1.13 υπάρχει επέκταση D/C και $u \in D$ ώστε $D = C[u]$ και $p(u) = 0$. Αφού, όμως, ισχύει η συνθήκη (4), η D/C δεν είναι γνήσια επέκταση, άρα $D = C$, οπότε $u \in C$, που σημαίνει ότι η ρίζα u του p, που είναι, βεβαίως, και ρίζα του f, ανήκει στο C. □

Ορισμός 3.3. Έστω F σώμα. Ένα σώμα C καλείται αλγεβρική κλειστότητα του F, αν η επέκταση C/F είναι αλγεβρική και το σώμα C είναι αλγεβρικώς κλειστό.

Θεώρημα 3.4. *Κάθε σώμα διαθέτει αλγεβρική κλειστότητα.*

Παράδειγμα 3.5. Το $\mathbb{R}$ έχει αλγεβρική κλειστότητα το $\mathbb{C}$. Το $\mathbb{Q}$ έχει μια αλγεβρική κλειστότητα που συμβολίζεται $\bar{\mathbb{Q}}$

Πρόταση 3.6. *Αν C είναι αλγεβρική κλειστότητα του σώματος F και $\mathrm{Cl}(C/F)$ είναι η αλγεβρική κλειστότητα του F στο C (βλ. Πρόταση 2.2), τότε $\mathrm{Cl}(C/F) = C$.*

Απόδειξη. Εξ ορισμού, το $\mathrm{Cl}(C/F)$ περιέχει όλα τα στοιχεία του C που είναι αλγεβρικά πάνω από το $F\cdot$ ειδικότερα, $\mathrm{Cl}(C/F) \subseteq C$. Αφετέρου, εξ ορισμού της αλγεβρικής κλειστότητας του F, η επέκταση C/F είναι αλγεβρική, άρα $C \subseteq \mathrm{Cl}(C/F)$ και, συνεπώς, $\mathrm{Cl}(C/F) = C$. □

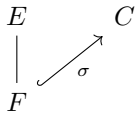
Πρόταση 3.7. *Έστω αλγεβρική επέκταση C/F. Το C είναι αλγεβρική κλειστότητα του F αν και μόνο αν κάθε μη σταθερό πολυώνυμο του $F[X]$ διασπάται στο C.*

Απόδειξη. Καθώς η επέκταση C/F είναι αλγεβρική, αυτό που πρέπει να αποδείξομε είναι ότι το C είναι αλγεβρικά κλειστό αν και μόνο αν κάθε μη σταθερό $f \in F[X]$ διασπάται στο C.

Αν το C είναι αλγεβρικά κλειστό, τότε κάθε $f \in F[X]$ ανήκει και στο $C[X]$ και, συνεπώς, αν είναι μη σταθερό, διασπάται στο C (Ορισμός 3.2 και Θεώρημα 3.1).

Αντιστρόφως, αν κάθε μη σταθερό πολυώνυμο του $F[X]$ διασπάται στο C. Θα δείξομε ότι το C είναι αλγεβρικά κλειστό. Για τον σκοπό αυτό θα δείξομε ότι ικανοποιείται η συνθήκη (1) του Θεωρήματος 3.1. Θεωρούμε ένα μη σταθερό $g \in C[X]$ και θα αποδείξομε ότι το g έχει μια τουλάχιστον ρίζα στο C. Από το Θεώρημα 1.22 υπάρχει επέκταση K/C και στοιχείο $u \in K$, τ.ω. $g(u) = 0$ και $K = C(u)$. Οι επεκτάσεις K/C και C/F είναι αλγεβρικές, άρα η επέκταση K/F είναι αλγεβρική (Θεώρημα 2.12). Συνεπώς, το u είναι αλγεβρικό πάνω από το F και έστω $f \in F[X]$ το ελάχιστο πολυώνυμό του. Από την υπόθεσή μας έπεται ότι το f διασπάται στο C, άρα $f = c(X - u_1)\cdots(X - u_n)$ με τα $u_1, \ldots, u_n \in C$. Επειδή $f(u) = 0$, συμπεραίνομε ότι $u = u_i$ για κάποιο i, οπότε $u \in C$. □

Θεώρημα 3.8. *Σε κάθε διάγραμμα όπως το παρακάτω, στο οποίο η επέκταση E/F είναι αλγεβρική και το C είναι η αλγεβρική κλειστότητα του F, ο μονομορφισμός σ επεκτείνεται σε μονομορφισμό $\tilde{\sigma} : E \to F$.*



Θεώρημα 3.9. *Αν τα C, C' είναι αλγεβρικές κλειστότητες του ίδιου σώματως τότε είναι F-ισόμορφες, δηλαδή υπάρχει ισομορφισμός $\sigma : C' \to C$ με $\sigma(a) = a\ \forall a \in F$.*

Απόδειξη. Στο διάγραμμα του Θεωρήματος 3.8 θέτω C' στη θέση του E και στη θέση του σ την εμφύτευση $\imath : F \hookrightarrow C$ ($\imath(c) = c\ \forall c \in F$). Συμπεραίνω ότι υπάρχει μονομορφισμός $\phi : C' \hookrightarrow C$, ο οποίος επεκτείνει τον $\imath$. Το σώμα $\phi(C')$ είναι ισόμορφο με το C', άρα είναι αλγεβρικά κλειστό (απλή άσκηση). Επίσης, το F είναι υπόσωμα του $\phi(C')$. Πράγματι, $F = \imath(F) = \phi(F) \subseteq \phi(C')$. Τώρα έχομε την εξής κατάσταση: $F \leq \phi(C') \leq C$ και η επέκταση C/F είναι αλγεβρική, άρα και η $C/\phi(C')$ είναι αλγεβρική. Καθώς όμως το $\phi(C')$ είναι αλγεβρικά κλειστό, το Θεώρημα 3.1 (4) με τον Ορισμό 3.2 εφαρμοζόμενα στο σώμα $\phi(C')$, μας οδηγούν στο συμπέρασμα ότι δεν υπάρχει γνήσια αλγεβρική επέκταση του $\phi(C')$, άρα πρέπει $C = \phi(C')$. Συνεπώς, ο ϕ είναι «επί», άρα, τελικά, ο ϕ είναι ισομορφισμός. □

Θεώρημα 3.10. *Έστω $f : F \to F'$ ισομορφισμός και C, C' αλγεβρικές κλειστότητες των F, F' τότε ο f επεκτείνεται σε ισομορφισμό $C \to C'$.*

Απόδειξη. Έστω $\imath : F' \hookrightarrow C'$ η ταυτοτική εμφύτευση του F' στο C' και $\sigma = \imath \circ f : F \hookrightarrow C'$. Εφαρμόζω το Θεώρημα 3.8 με C στη θέση του E, C' στη θέση του C και σ όπως τον όρισα μόλις πριν. Συμπεραίνω ότι υπάρχει μονομορφισμός $\tilde{\sigma} : C \hookrightarrow C'$ που επεκτείνει τον σ. Το F' είναι υπόσωμα του $\tilde{\sigma}(C)$. Πράγματι, $F' = \imath(F') = \imath(f(F)) = (\imath \circ f)(F) = \sigma(F) = \tilde{\sigma}(F) \subseteq \tilde{\sigma}(C)$, άρα έχω τις διαδοχικές επεκτάσεις $F' \leq \tilde{\sigma}(C) \leq C'$. Η C'/F' είναι αλγεβρική, άρα και η $C'/\tilde{\sigma}(C)$ είναι αλγεβρική. Το $\tilde{\sigma}(C)$ είναι ισόμορφο με το C, το οποίο είναι αλγεβρικά κλειστό, άρα και το $\tilde{\sigma}(C)$ είναι αλγεβρικά κλειστό (απλή άσκηση). Εφαρμόζοντας το Θεώρημα 3.1 (4) με τον Ορισμό 3.2 στο σώμα αυτό, συμπεραίνομε ότι δεν υπάρχει γνήσια αλγεβρική επέκτασή του, άρα πρέπει $C' = \tilde{\sigma}(C)) \cong C$. □

Διαχωρισιμότητα

Ορισμός 3.11. Έστω σώμα F. Το ανάγωγο $f \in F[X]$ χαρακτηρίζεται διαχωρίσιμο αν όλες οι ρίζες του είναι διαφορετικές. Δηλαδή αν θεωρήσω ένα σώμα διάσπασης K/F, και αναλύσω το f σε πρωτοβάθμια του $K[X]$, τότε τότε η ανάλυση του f πάνω από το K έχει τη μορφή $f(X) = c(X - u_1)\cdots(X - u_n)$, όπου τα $u_1, \ldots, u_n \in K$ διαφορετικά μεταξύ τους και $c \in F$ είναι ο συντελεστής του μεγιστοβαθμίου όρου του f.

Παρατήρηση 3.12. Έστω $f \in F[X]$ και $f = (X-\alpha)^r g$ με $r \geq 1, g \in K[X], g(\alpha) \neq 0$Έστω K'/F είναι ένα άλλο σώμα διάσπασης, τότε υπάρχει ένας F-ισομορφισμός $\sigma : K \to K'$ (Θεώρημα 2.13). Αυτός επεκτείνεται σε ισομορφισμό δακτυλίων $\sigma : K[X] \to K'[X]$ (Παρατήρηση 2.5). Άρα, εφαρμόζοντας στη σχέση $f = (X-\alpha)^r g$ αυτόν τον ισομορφισμό, παίρνομε $f = \sigma f = (X-\sigma(\alpha))^r \sigma g$ (η αριστερότερη ισότητα έπεται από το ότι $f \in F[X]$ και ο σ είναι F-ισομορφισμός). Είναι $g(\alpha) \neq 0$, άρα $\sigma g(\sigma(\alpha)) \neq 0$. Άρα η ρίζα $\sigma(\alpha)$ είναι ρίζα του f με πολλαπλότητα r. Δηλαδή, αν το f έχει ρίζα στο K πολλαπλότητας r, τότε έχει και στο K' ρίζα πολλαπλότητας r. Άρα, έχω την παρακάτω πρόταση.

Πρόταση 3.13. *Το να πω ότι «ένα $f \in F[X]$ έχει απλές μόνο ρίζες» ή ότι «έχει ρίζα πολλαπλότητας ≥ 1» δεν εξαρτάται από το σώμα διάσπασης του f πάνω από το F Αυτό «νομιμοποιεί» τον ορισμό 3.11.*

Ορισμός 3.14 (Συνέχεια του Ορισμού 3.11)**.** Ένα μη σταθερό $f \in F[X]$ χαρακτηρίζεται διαχωρίσιμο αν όλοι οι ανάγωγοι παράγοντες του είναι διαχωρίσιμοι.

Παράδειγμα 3.15. Το $f(X) = (X^2 - 2)^2(X^2 + 3) \in \mathbb{Q}[X]$ είναι διαχωρίσιμο καθώς οι ανάγωγοι παράγοντες του είναι οι $(X^2 - 2)$ και $(X^2 + 3)$ έχουν διαφορετικές ρίζες. ($\pm\sqrt{2}$ και $\pm i\sqrt{3}$ αντιστοιχα).

Εργαλείο για τη μελέτη των διαχωρίσιμων πολυωνύμων είναι η τυπική (formal) παράγωγος.

Ορισμός 3.16. Έστω $f \in F[X]$, $f = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$, τότε ορίζω την παράγωγο του f να είναι το πολυώνυμο

$$f' = n a_n X^{n-1} + (n-1)a_{n-1}X^{n-2} \cdots + a_1 \in F[X].$$

Ισχύουν οι αναμενόμενες ιδιότητες $(f \pm g)' = f' \pm g'$ και για τον πολλαπλασιαμό $(fg)' = fg' + f'g$. Οι αποδείξεις τους συμβολικές (formal).

Πρόταση 3.17. *Έστω C αλγεβρική κλειστότητα του σώματος F και μη μηδενικό πολυώνυμο $f \in F[X]$. Το f έχει πολλαπλή ρίζα (εννοείται, στο C) αν και μόνο αν τα πολυώνυμα f και f' (η τυπική παράγωγος του f) έχουν μη σταθερό κοινό διαιρέτη $g \in F[X]$.*

Απόδειξη. Έστω $\alpha \in C$ πολλαπλή ρίζα του f. Τότε $f = (X-\alpha)^r h$ με $h(\alpha) \neq 0$ και $r \geq 2$. Η τυπική παράγωγος είναι $f' = r(X-\alpha)^{r-1}h + (X-\alpha)^r h$, άρα, επειδή $r-1 \geq 1$, έπεται ότι $f'(\alpha) = 0$. Έστω $g \in F[X]$ το ελάχιστο πολυώνυμο του α πάνω από το F. Τότε, τα f, g έχουν κοινή ρίζα, άρα $g|f$ και, ομοίως, $g|f'$.

Αντιστρόφως. Αν f και f' έχουν μη σταθερό κοινό διαιρέτη στο $F[X]$, θα δείξομε ότι το f έχει πολλαπλή ρίζα. Ισοδύναμα (αντιστροφο-αντίθετη συνεπαγωγή): Αν το f δεν έχει πολλαπλή ρίζα (δηλαδή έχει μόνο απλές ρίζες) θα δείξομε, με απαγωγή σε άτοπο, ότι τα f, f' δεν έχουν μη σταθερό κοινό διαιρέτη. Διότι, έστω ότι το $g \in F[X]$ είναι μη σταθερό πολυώνυμο που διαιρεί τα f και f'. Καθώς το C είναι αλγεβρικά κλειστό, το g διασπάται στο C και έστω μια οποιαδήποτε ρίζα $a \in C$ του g. Τότε $f(a) = 0$ και $f'(a) = 0$. Το f έχει απλές, μόνο, ρίζες, άρα $f(X) = (X-a)h(X)$ με $h(a) \neq 0$. Παραγωγίζοντας έχω: $f'(X) = h(X) + (X-a)h'(X)$, οπότε η αντικατάσταση $X \leftarrow a$ δίνει $0 = h(a)\cdot$ αντίφαση. □

Πόρισμα 3.18. *1. Αν* $\mathrm{char}(F) = 0$*, τότε καθε ανάγωγο* $f \in F[X]$ *είναι διαχωρίσιμο.*

2. Αν $\mathrm{char}(F) = p$ *(πρώτος), τότε ένα ανάγωγο* $f \in F[X]$ *έχει πολλαπλή ρίζα αν και μόνο αν* $f(X) \in F[X^p]$*. Η συνθήκη αυτή είναι (προφανώς) ισοδύναμη με το ότι το* f *είναι της μορφής*

$$f(X) = c_0 + c_1 X^{m_1 p} + c_2 X^{m_2 p} + \cdots + c_r X^{m_r p}, \quad c_1, c_2, \ldots, c_r \neq 0. \tag{3.1}$$

Απόδειξη. 1. Αν $f = a_n X^n + \cdots + a_0, n \geq 1, a_n \neq 0$, τότε $f' = n a_n X^{n-1} + \cdots + a_1 \neq 0$ καθώς $n a_n \neq 0$. Αν το f δεν είναι διαχωρίσιμο, τότε (από την Πρόταση 3.17) υπάρχει μη σταθερό $g \in F[X]$ που διαιρεί το f και το f'. Αφού $f' \neq 0$, έπεται ότι το $\deg g \leq \deg f' < \deg f$, άτοπο διότι το f είναι ανάγωγο.

2. Αν το f είναι της μορφής (3.1), τότε, παραγωγίζοντας, βλέπομε ότι όλοι οι όροι του f' έχουν συντελεστές που είναι πολλαπλάσια του p άρα είναι ίσοι με το $0 \in F$, άρα $f' = 0$. Αλλά τότε $f|f'$, οπότε τα f, f' έχουν μη σταθερό κοινό διαιρέτη και αυτό, λόγω της Πρότασης 3.17, μας λέει ότι το f έχει πολλαπλή ρίζα.

Αντιστρόφως, έστω ότι το f έχει πολλαπλή ρίζα. Τότε, από την Πρόταση 3.17, τα f, f' έχουν μη σταθερό κοινό διαιρέτη $g \in F[X]$. Αν $f' \neq 0$, τότε $\deg g \leq \deg f' < \deg f$ και καταλήγομε στο άτοπο συμπέρασμα ότι το ανάγωγο f έχει ένα μη σταθερο διαιρέτη g μικρότερου βαθμού. Άρα $f' = 0 \in F[X]$. Το f είναι της μορφής (αν γράψομε μόνο τους μη μηδενικούς όρους του)

$$f(X) = c_0 + c_1 X^{n_1} + c_2 X^{n_2} + \cdots + c_r X^{n_r}, \quad c_1, c_2, \ldots, c_r \neq 0.$$

Παραγωγίζοντας έχομε

$$f'(X) = n_1 c_1 X^{n_1 - 1} + n_2 c_2 X^{n_2 - 1 +} = \cdots + n_r c_r X^{n_r - 1}.$$

Για να είναι $f' = 0$ πρέπει όλοι οι συντελεστές του να είναι 0. Αλλά όλα τα $c_i \in F$ είναι μη μηδενικά, άρα πρέπει όλα τα n_i να είναι πολλαπλάσια του p. Θέτοντας $n_i = p m_i$ για $i = 1, \ldots, r$ βλέπομε ότι το f είναι της μορφής (3.1). □

Την καλή ιδιότητα των σωμάτων χαρακτηριστικής 0, έχουν και τα πεπερασμένα σώματα, όπως θα δούμε, παρακάτω, στην Πρόταση 3.22. Πιο πριν υπενθυμίζομε κάποια πράγματα.

Υπενθύμιση 3.19. Κάθε πεπερασμένο σώμα έχει πληθάριθμο $q = p^n$, όπου ο p είναι πρώτος και $n \geq 1$. Ένα τέτοιο σώμα συμβολίζεται $\mathbb{F}_q$ και η χαρακτηριστική του είναι p. Υπάρχουν όμως σώματα χαρακτηριστικής p που είναι άπειρα.

Υπενθύμιση 3.20. (Freshman's Dream)[1] Αν $\mathrm{char}(F) = p$, τότε $(a+b)^p = a^p + b^p$

[1] Το «όνειρο» του πρωτοετούς. Άλλα «όνειρα», απραγματοποίητα όμως, είναι π.χ. $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$, $\sin(nx)/n = \sin(x)$ και άλλα πολλά....

Απόδειξη.

$$(a+b)^p = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{k} a^k b^{p-k}$$

Το $\binom{p}{k}$ είναι πολλαπλάσιο του p για κάθε $k = 1, \dots, p-1$. □

Ορισμός 3.21. *Έστω σώμα F πεπερασμένο χαρακτηριστικής p. Η απεικόνηση $a \mapsto a^p$ λέγεται αυτομορφισμός του Frobenius.*

Ο χαρακτηρισμός «αυτομορφισμός» δικαιολογείται ως εξής: Από την υπενθύμιση 3.20, η απεικόνηση $a \mapsto a^p$ είναι ομομορφισμός. Είναι 1-1 διότι: $a^p = b^p \implies (a-b)^p = 0 \implies a = b$. Αφού το F είναι πεπερασμένο και η απεικόνηση είναι 1-1, θα είναι και επί.

Πρόταση 3.22. *Αν το F είναι πεπερασμένο σώμα, τότε κάθε ανάγωγο πολυώνυμο του $F[X]$ είναι διαχωρίσιμο.*

Απόδειξη. Έστω $\text{char}(F) = p$, και $f \in F[X]$ ανάγωγο. Αν το f δεν είναι διαχωρήσιμο, τότε από το Πόρισμα 3.18 (2), $f(X) = c_0 + c_1 X^{m_1 p} + c_2 X^{m_2 p} + \cdots + c_r X^{m_r p}$. Από τον αυτομορφισμό του Frobenius, $\forall c_i \; \exists a_i \in F$ τ.ω. $a_i^p = c_i$. Οπότε

$$f = a_1^p X^{m_1 p} + a_2^p X^{m_2 p} + a_r^p X^{m_r p} = (a_1 X^{m_1} + a_2 X^{m_2} + \cdots + a_r X^{m_r})^p,$$

άτοπο διότι το f είναι ανάγωγο. □

Ορισμός 3.23. *Έστω επέκταση E/F. Αν το $\alpha \in E$ είναι αλγεβρικό πάνω από το F και το ελάχιστο πολυώνυμο του α πάνω από το F είναι διαχωρίσιμο, τότε λέμε ότι το α είναι διαχωρίσιμο πάνω από το F. Μία αλγεβρική επέκταση E/F λέγεται διαχωρίσιμη αν κάθε στοιχείο της $\alpha \in E$ είναι διαχωρίσιμο πάνω από το F.*

Λήμμα 3.24. *Έστω διαδοχικές επεκτάσεις $K/E/F$. Αν η K/F είναι διαχωρίσιμη, τότε οι επεκτάσεις E/F και η K/E ειναι διαχωρίσιμες.*

Απόδειξη. Η E/F είναι διαχωρίσιμη για τετριμμένο λόγο, αφού $E \subseteq K$. Θα δείξω ότι η K/E είναι διαχωρίσιμη. Έστω $\alpha \in K$ και $g \in E[X]$ το ελάχιστο πολυώνυμο του α πάνω από το E. Θα δείξω ότι το g είναι διαχωρίσιμο. Έστω $f \in F[X]$ το ελάχιστο πολυώνυμο του α πάνω από το F. Το f είναι διαχωρίσιμο λόγω της διαχωρισιμότητας της επέκτασης K/F. Όμως $g|f$ (άσκηση 1.27), άρα $f = gh$ για κάποιο $h \in E[X]$. Από τη σχέση αυτή γίνεται φανερό ότι, αφού το f δεν έχει πολλαπλή ρίζα, ούτε το g έχει τέτοια ρίζα. □

Πρόταση 3.25. *Έστω $f \in F[X]$ ανάγωγο και C αλγεβρική κλειστότητα του F. Τότε όλες οι ρίζες του f στο C έχουν την ίδια πολλαπλότητα.*

Απόδειξη. Έστω $\alpha, \beta \in C$ ρίζες του f.Έστω ο F-ισομορφισμός $\sigma : F(\alpha) \to F(\beta)$ με $\sigma(\alpha) = \beta$. (Ο σ επεκτείνει τον id_F). Έστω $\tau : C \to C$ που επεκτείνει τον σ η ύπαρξη του οποίου εξασφαλίζεται από το Θεώρημα 3.10. Έστω $r \geq 1$ η πολλαπλότητα του α στο f, οπότε $f = (X-\alpha)^r g(X)$ με $g \in F(\alpha)[X], g(\alpha) \neq 0$. Τότε $f(X) = \sigma f(X) = (X - \sigma(\alpha))^r \cdot \sigma g(X) = (X-\beta)^r \cdot \sigma g(X)$. Όμως $g(\alpha) \neq 0$ άρα $\sigma g(\sigma(\alpha)) \neq 0$, δηλαδή, $\sigma g(\beta) \neq 0$ που σημαίνει ότι η β είναι πολλαπλότητας r στο f. □

Πόρισμα 3.26. *Έστω $f \in F[X]$ ανάγωγο και C αλγεβρική κλειστότητα του F. Τότε η ανάλυση του f στο $C[X]$ έχει τη μορφή $f = c(X-\alpha_1)^r \dots (X-\alpha_\nu)^r$ όπου $\alpha_1, \dots, \alpha_\nu \in C$ είναι διαφορετικά, $\nu > 1$ και $c \in F$ είναι ο συντελεστής του μεγιστοβαθμίου όρου του f.*

Παρατήρηση 3.27. Έστω E/F πεπερασμένη και $a_1, \dots, a_n \in E$ είναι βάση της. Τότε $E = F(a_1, \dots, a_n)$.

Λήμμα 3.28. *Έστω μονομορφισμός σωμάτων $\sigma : F \hookrightarrow L$, με το L αλγεβρικά κλειστό και πεπερασμένη επέκταση E/F. Τότε ο σ μπορεί να επεκταθεί σε μονομορφισμό $\tau : E \hookrightarrow L$ με πεπερασμένο πλήθος τρόπων.*

Απόδειξη. Έστω $\alpha_1, \dots, \alpha_n$ μία βάση της επέκτασης E/F. Έστω ο τυπικός $\tau : E \hookrightarrow L$. Κάθε στοιχείο στο E γράφεται ως $e = b_1\alpha_1 + \cdots + b_n\alpha_n$ με $b_1, \dots, b_n \in F$. Άρα

$$\begin{aligned}\tau(e) &= \tau(b_1)\tau(\alpha_1) + \cdots + \tau(b_n)\tau(\alpha_n)\\ &= \sigma(b_1)\tau(\alpha_1) + \cdots + \sigma(b_n)\tau(\alpha_n)\end{aligned}$$

Ο σ είναι δεδομένος, άρα ο τ χαρακτηρίζεται από τις τιμές του στα $\alpha_1, \dots, \alpha_n$. Άρα, αυτό που αρκεί να δείξω είναι ότι για κάθε $\alpha \in \{\alpha_1, \dots, \alpha_n\}$, οι δυνατές τιμές του $\tau(\alpha)$ είναι πεπερασμένες το πλήθος. Πράγματι, έστω $p = X^k + c_{k-1}X^{k-1} \cdots + c_1X + c_0 \in F[X]$ το ελάχιστο πολυώνυμο του α. Τότε, $\alpha^k + c_{k-1}\alpha^{k-1} \cdots + c_1\alpha + c_0 = 0$ και εφαρμόζοντας τον τ,

$$\tau(\alpha)^k + \sigma(c_{k-1})\tau(\alpha)^{k-1} + \cdots + \sigma(c_1)\tau(\alpha) + \sigma(c_0) = 0.$$

Άρα το $\tau(\alpha)$ είναι ρίζα του σp, οπότε το πλήθος των δυνατών τιμών του $\tau(\alpha)$ είναι πεπερασμένο. □

Παρατήρηση 3.29. Έστω μονομορφισμός σωμάτων $\sigma : F \hookrightarrow L$, με το L αλγεβρικά κλειστό. Το $\sigma(F)$ είναι υπόσωμα του αλγεβρικά κλειστού L, άρα, από την άσκηση 3.34, υπάρχει αλγεβρική κλειστότητα C του $\sigma(F)$, η οποία περιέχεται στο L. Άρα μπορούμε να θεωρούμε τον σ ως μονομορφισμό $\sigma : F \hookrightarrow C$. Μ' άλλα λόγια, κάθε εμφύτευση σ ενός σώματος F σε ένα αλγεβρικά κλειστό σώμα είναι εμφύτευση του F σε μια αλγεβρική κλειστότητα του $\sigma(F)$.

Στη συνέχεια μελετούμε το εξής ζήτημα: Έστω μονομορφισμός σωμάτων $\sigma : F \hookrightarrow L$, με το L αλγεβρικά κλειστό και πεπερασμένη επέκταση E/F. Σύμφωνα με το Λήμμα 3.28, το σύνολο

$$S_\sigma = \{\tilde{\sigma} : E \hookrightarrow L,\ \tilde{\sigma} \text{ επέκταση του } \sigma\}$$

είναι πεπερασμένο. Αν τώρα θεωρήσομε έναν άλλο, ανάλογο, μονομορφισμό $\tau : F \hookrightarrow L'$, με το L' αλγεβρικά κλειστό και θεωρήσομε το αντίστοιχο πεπερασμένο σύνολο

$$S_\tau = \{\tilde{\tau} : E \hookrightarrow L',\ \tilde{\tau} \text{ επέκταση του } \tau\},$$

πώς σχετίζονται οι πληθάριθμοι των δύο συνόλων; *Απάντηση:* Είναι ίσοι· συνεπώς:

Ορισμός 3.30. Το πλήθος των επεκτάσεων του $\sigma : F \hookrightarrow L$ σε $\tilde{\sigma} : E \hookrightarrow L$ είναι ανεξάρτητο του σ (στην έννοια του σ υπονοείται και το L), εξαρτάται δε μόνο από την επέκταση E/F. Ο αριθμός αυτός συμβολίζεται με $\{E : F\}$ και λέγεται *δείκτης* της επέκτασης E/F. Εναλλακτικά, συμβολίζεται με $[E : F]_s$ και λέγεται *βαθμός διαχωρισιμότητας* της επέκτασης E/F. Αν E/F είναι πεπερασμένη επέκταση, και ο δείκτης $\{E : F\}$ (εναλλακτικά: ο βαθμός διαχωρισιμότητας $[E : F]_s$ είναι ίσος με n, τότε συμπεραίνομε ότι ένας οποιοσδήποτε μονομορφισμός $\sigma : F \hookrightarrow L$ (L αλγεβρικά κλειστό) επιδέχεται ακριβώς n το πλήθος επεκτάσεις $\tilde{\sigma} : E \hookrightarrow L$.

Για να έχει, βεβαίως, νόημα ο Ορισμός 3.30, πρέπει να αποδειχθεί ο ισχυρισμός (βλ. παραπάνω) ότι $S_\sigma = S_\tau$. Διατυπώνομε και αποδεικνύομε το σχετικό θεώρημα.

Θεώρημα 3.31. *Έστω πεπερασμένη επέκταση E/F και μονομορφισμοί σωμάτων $\sigma : F \hookrightarrow L$, $\tau : F \hookrightarrow L'$ με τα L, L' αλγεβρικώς κλειστά. Τότε τα (πεπερασμένα βάσει του Λήμματος 3.28) σύνολα*

$$S_\sigma = \{\tilde{\sigma} : E \hookrightarrow L,\ \tilde{\sigma} \text{ επέκταση του } \sigma\} \quad \text{και} \quad S_\tau = \{\tilde{\tau} : E \hookrightarrow L',\ \tilde{\tau} \text{ επέκταση του } \tau\},$$

είναι ισοπληθή.

Απόδειξη. Σύμφωνα με την Παρατήρηση 3.29, μπορούμε να αντικαταστήσομε τα L και L' από αλγεβρικές κλειστότητες C και C' των $\sigma(F)$ και $\tau(F)$, αντιστοίχως ($C \leq L$ και $C' \leq L'$). Θα ορίσομε μια 1-1 αντιστοιχία $S_\sigma \to S_\tau$ ως εξής: Έστω $\tilde{\sigma} \in S_\sigma$. Έχομε την κατάσταση που φαίνεται στο παρακάτω διάγραμμα.

$$\begin{array}{ccccc} C' & \xleftarrow{\quad\sim_{\lambda}\quad} & & & C \\ | & & & & | \\ \tilde{\tau}(E) & \xleftarrow[\sim]{\tilde{\tau}} & E & \xrightarrow[\tilde{\sigma}]{\sim} & \tilde{\sigma}(E) \\ | & & | & & | \\ \tau(F') & \xleftarrow[\sim]{\tau} & F & \xrightarrow[\sigma]{\sim} & \sigma(F) \end{array}$$

Επεξηγήσεις: Το $\sim$ πάνω ή κάτω από το «βέλος» μιας απεικόνισης δηλώνει ισομορφισμό. Το λ συμβολίζει ισομορφισμό ο οποίος επεκτείνει τον (προφανή) ισομορφισμό $\tau \circ \sigma^{-1} : \sigma(F) \to \tau(F')$ (βλ. Θεώρημα 3.10). Ορίζομε $\tilde{\tau} = \lambda \circ \tilde{\sigma}$ και καθώς είναι σύνθεση μονομορφισμών με πεδίο ορισμού το E και πεδίο τιμών το C', έπεται ότι $\tilde{\tau} : E \hookrightarrow C'$. Είναι όμως $\tilde{\tau} \in S_\tau$; Για να ισχύει αυτό πρέπει να δείξομε ότι αυτός ο $\tilde{\tau}$ επεκτείνει τον τ. Πράγματι, αυτό συμβαίνει, διότι, αν $a \in F$, τότε $\tilde{\tau}(a) = \lambda \circ \tilde{\sigma}(a) = \lambda(\sigma(a))$ (είναι $\tilde{\sigma}(a) = \sigma(a)$ γιατί $a \in F$). Καθώς ο λ επεκτείνει τον $\tau \circ \sigma^{-1}$ και $\sigma(a) \in \sigma(F)$, έπεται ότι $\lambda(\sigma(a)) = (\tau \circ \sigma^{-1})(\sigma(a)) = \tau(a)$, άρα, τελικά, $\tilde{\tau}(a) = \tau(a)$ για $a \in F$.

Συνεπώς η απεικόνιση $S_\sigma \ni \tilde{\sigma} \mapsto \lambda \circ \tilde{\sigma} \in S_\tau$ είναι 1-1. Αφετέρου, ο ρόλος των σ και τ στο θεώρημα είναι απολύτως συμμετρικός, άρα υπάρχει και 1-1 απεικόνιση $S_\tau \to S_\sigma$ (στην πραγματικότητα τέτοια είναι η απεικόνιση $S_\tau \ni \tilde{\tau} \mapsto \lambda^{-1} \circ \tilde{\tau} \in S_\sigma$), άρα τα σύνολα S_σ και S_τ έχουν τον ίδιο πληθάριθμο. □

Πρόταση 3.32. *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 $\mathrm{Irr}(\alpha, F)$ στο $C[X]$. Σύμφωνα με το Πόρισμα 3.26, $\mathrm{Irr}(\alpha, F) = (X - \alpha_1)^r \dots (X - \alpha_k)^r$ με $\alpha_1, \dots, \alpha_k \in C$ διαφορετικά και $r \geq 1$. Ο βαθμός της επέκτασης είναι

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

Το πλήθος των F-μονομορφισμών $F(\alpha) \hookrightarrow C$ είναι ακριβώς k, διότι κάθε τέτοιος στέλνει το α (που είναι ρίζα του $\mathrm{Irr}(\alpha, F)$) σε κάποια ρίζα του $\mathrm{Irr}(\alpha, F)$, 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 3.33. *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 3.35). 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. □

Ασκήσεις

Άσκηση 3.34. Έστω $F \leq L$ με το L αλγεβρικά κλειστό. Τότε το $C := \mathrm{Cl}(L/F)$ είναι αλγεβρική κλειστότητα του F, η οποία περιέχεται στο L.

Άσκηση 3.35. Έστω $F \leq E \leq K \leq C$ διαδοχικές επεκτάσεις σωμάτων και η K/F είναι αλγεβρική. Αποδείξτε ότι, αν το C είναι αλγεβρική κλειστότητα ενός οποιουδήποτε από τα τρία σώματα F, E, K, τότε είναι αλγεβρική κλειστότητα και για τα υπόλοιπα δύο σώματα.

Άσκηση 3.36. Έστω πρώτος p, σώμα F χαρακτηριστικής p και $u \in F$. Υποθέτομε ότι το πολυώνυμο $f(X) = X^p - u \in F[X]$ είναι ανάγωγο πάνω από το F. Έστω C αλγεβρική κλειστότητα του F. Αποδείξτε ότι το f έχει μόνο μία ρίζα στο C και η πολλαπλότητά της είναι p.

Άσκηση 3.37. Σ' αυτή την άσκηση θεωρήστε ότι η αλγεβρική κλειστότητα $\bar{\mathbb{Q}}$ του $\mathbb{Q}$ είναι υπόσωμα του $\mathbb{C}$. Το $i \in \mathbb{C}$ έχει τη συνήθη σημασία: είναι ρίζα του $X^2 + 1 \in \mathbb{Q}[X]$.
Έστω $f(X) = X^4 - 2X^2 - 1 \in \mathbb{Q}[X]$ και ρ ρίζα του f. Αποδείξτε ότι το f είναι ανάγωγο πάνω από το $\mathbb{Q}$ και το $K = \mathbb{Q}(\rho, i)$ είναι σώμα διάσπασης του f. Υπολογίστε τον βαθμό $[K : \mathbb{Q}]$ και μια βάση της επέκτασης $K/\mathbb{Q}$.
Υπόδειξη. Μπορεί να σας βοηθήσει (δίχως να είναι απαραίτητο) να δείτε τη ρίζα ρ του f σαν μία από τις πραγματικές ρίζες του f.

Άσκηση 3.38. Έστω F σώμα χαρακτηριστικής $p > 0$ και E πεπερασμένη επέκταση του F.
(i) Έστω $a \in E$ και $f = \mathrm{Irr}\,(a, F(a^p))$. Δείξτε ότι $f(X) = (X - a)^r$ με $1 \leq r \leq p$.
(ii) Αν το $a \in E$ είναι διαχωρίσιμο πάνω από το $F(a^p)$, αποδείξτε ότι $a \in F(a^p)$.

Άσκηση 3.39. Ένα σώμα χαρακτηρίζεται *τέλειο* αν κάθε ανάγωγο πολυώνυμο πάνω από το F είναι διαχωρίσιμο. Λόγω του Πορίσματος 3.18 και της Πρότασης 3.22, τα σώματα χαρακτηριστικής 0, καθώς και όλα τα πεπερασμένα σώματα είναι τέλεια, αλλά δεν είναι τα μόνα τέλεια σώματα.
Έστω τώρα ένα σώμα F χαρακτηριστικής $p > 0$. Αποδείξτε ότι το F είναι τέλειο αν και μόνο αν κάθε στοιχείο του F είναι p-δύναμη κάποιου στοιχείου του F.
Υπόδειξη. Αποδείξτε πρώτα ότι το $F^p := \{a^p : a \in F\}$ είναι σώμα.

Κεφάλαιο 4

4.1 4^{η} Εβδομάδα

Διαχωρισιμότητα (συνέχεια)

Πόρισμα 4.1. *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 $F \leq F(\beta) \leq F(\alpha)\cdot$ επίσης, το α είναι διαχωρίσιμο πάνω από το $F(\beta)$ γιατί είναι διαχωρίσιμο πάνω από το F. Έχω τώρα,

$$[F(\alpha) : F(\beta)]\,[F(\beta) : F] = [F(\alpha) : F] \overset{3.32}{=} \{F(\alpha) : F\} \overset{3.33}{=} \{F(\alpha) : F(\beta)\}\,\{F(\beta) : F\}$$
$$\overset{3.32}{=} [F(\alpha) : F(\beta)]\,\{F(\beta) : F\}$$

και συγκρίνοντας το αριστερότερο με το δεξιότερο μέλος βλέπομε ότι $[F(\beta) : F] = \{F(\beta) : F\}$, άρα (Πρόταση 3.32) η επέκταση $F(\beta)/F$ είναι διαχωρίσιμη, οπότε το β είναι διαχωρίσιμο πάνω από το F. □

Θεώρημα 4.2. *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 3.32,

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

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 3.32.

Έχω ότι

$$[E:F(\alpha)]\,[F(\alpha):F] = [E:F] \overset{3.32}{=} \{E:F\} \overset{3.33}{=} \{E:F(\alpha)\}\,\{F(\alpha):F\}\,.$$

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 4.3. *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 3.32, $\{E:K\} = [E:K]$ και $\{K:F\} = [K:F]$. Πολλαπλασιάζοντας κατα μέλη έχω $\{E:F\} = [E:F]$, οπότε η E/F είναι διαχωρίσιμη από το Θεώρημα 4.2. □

Πόρισμα 4.4. *Αν $E = F(\alpha_1,\dots,\alpha_n)$ και κάθε α_i είναι διαχωρίσιμο πάνω από το F, τότε η επέκταση E/F είναι διαχωρίσιμη.*

Απόδειξη. Από το Πόρισμα 4.1 η επέκταση $F(\alpha_1)/F$ είναι διαχωρίσιμη. Θα δείξομε επαγωγικά ότι, για $i = 2,\dots,n$, η επέκταση $F(\alpha_1,\dots,\alpha_i)/F$ είναι διαχωρίσιμη. Έστω $i \geq 2$ και ας υποθέσομε ότι έχομε ήδη αποδείξει ότι η $F(\alpha_1,\dots,\alpha_{i-1})/F$ είναι διαχωρίσιμη. Το α_i είναι διαχωρίσιμο πάνω από το F άρα και πάνω από το $F(\alpha_1,\dots,\alpha_{i-1})$, οπότε η $F(\alpha_1,\dots,\alpha_{i-1},\alpha_i)/F(\alpha_1,\dots,\alpha_{i-1})$ είναι διαχωρίσιμη λόγω του Πορίσματος 4.1. Εφαρμόζομε τώρα το Θεώρημα 4.3 με $F(\alpha_1,\dots,\alpha_{i-1},\alpha_i)$ στη θέση του E και $F(\alpha_1,\dots,\alpha_{i-1})$ στη θέση του K. □

Ορισμός 4.5. Έστω τυχαία επέκταση E/F και $\alpha,\beta \in E$ αλγεβρικά πάνω από το F. Τα α,β λέμε ότι είναι F-συζυγή αν και μόνο αν $\operatorname{Irr}(\alpha,F) = \operatorname{Irr}(\beta,F)$.

Υπενθύμιση 4.6. 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 $f = c \cdot \operatorname{Irr}(\alpha,F)$, όπου c είναι ο συντελεστής του μεγιστοβάθμιου όρου του f) τότε το $\sigma(\alpha)$ είναι F-συζυγής του α.
Διότι, αν $f = c_nX^n + \cdots + c_1X + c_0$, τότε $c_n\alpha^n + \cdots + c_1\alpha + c_0$. Εφαρμόζω τον σ ($\sigma(c_i) = c_i \forall i$) οπότε $c_n\sigma(\alpha)^n + \cdots + c_1\sigma(\alpha) + c_0$, δηλαδή $\sigma(\alpha)$ είναι ρίζα του f άρα και του $\operatorname{Irr}(\alpha,F)$, 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 $\alpha_1,\dots,\alpha_k$ είναι όλες οι διαφορετικές ρίζες του f, τότε $\sigma(\alpha_1),\dots,\sigma(\alpha_k)$ είναι μετάθεση αυτών.

Κανονικότητα

Ορισμός 4.7. 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 E.

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 4.8. 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 4.9. Η $E = \mathbb{Q}(\sqrt[3]{2})$ δεν είναι κανονική, διότι το $\mathrm{X}^3 - 2$ 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 4.10. Η επέκταση $\mathbb{Q}(\alpha)/\mathbb{Q}$ όπου $\alpha \in \mathbb{C}$ είναι ρίζα του αναγώγου $X^2 - 9X + 9 \in \mathbb{Q}[X]$ είναι κανονική, σύμφωνα με την άσκηση 2.17 και το παρακάτω Θεώρημα 4.14.

Πρόταση 4.11. *Έστω E/F πεπερασμένη επέκταση, 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 $e_1, \dots, e_n$ είναι βάση της E/F, τότε είναι απλή άσκηση να δείξομε ότι $\sigma(e_1), \dots, \sigma(e_n)$ είναι βάση της $\sigma(E)/F$), άρα $[E : \sigma(E)] = 1$, οπότε $\sigma(E) = E$, σύμφωνα με την άσκηση 2.15 (i). □

Θεώρημα 4.12. *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 $\sigma : E \hookrightarrow C$ είναι F-αυτομορφισμός του E.*

Απόδειξη. Απόδειξη της πρώτης ισοδυναμίας. Έστω $E = F(\alpha_1, \dots, \alpha_n)$. (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 $\text{Irr}\,(\alpha_i, F)$. Αφού $\alpha_i \in E$ και η E/F είναι κανονική, έπεται ότι όλες οι ρίζες του $\text{Irr}\,(\alpha_i, F)$ (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 $p = c\,\text{Irr}\,(\alpha, C)$ όπου $c \in F$.

Έστω $\beta \in C$ μία άλλη ρίζα του p (δηλαδή του $\text{Irr}\,(\alpha, F)$.) 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 3.8. 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 4.11. □

Παράδειγμα 4.13 (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 4.14. *Έστω E/F πεπερασμένη. Τότε, η E/F είναι κανονική $\iff$ E είναι σώμα διάσπασης πάνω από το F 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 $\text{Irr}\,(\alpha_i, F)$ 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 $\prod_{i=1}^{n} \text{Irr}\,(\alpha_i, F)$.

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

Έστω μη σταθερό πολυώνυμο $p \in F[X]$ το οποίο έχει μια ρίζα του β μέσα στο E και K σώμα διάσπασης του p πάνω από το E. Θέλω να δείξω ότι, αν $\gamma \in K$ είναι οποιαδήποτε ρίζα του p, τότε $\gamma \in E$. Θεωρώ τον F-ισομορφισμό $\sigma : F(\beta) \to F(\gamma)$ που μου εξασφαλίζει η Πρόταση 1.21 και, στη συνέχεια, έναν ισομορφισμό $\tau : K \to K$ που επεκτείνει τον σ, τον οποίο μου εξασφαλίζει το Θεώρημα 2.13. 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 $\gamma \in E$. □

Ασκήσεις

Άσκηση 4.15. Στην αλυσσίδα επεκτάσεων $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt[4]{2})$, όπου τα $\sqrt{2}$ και $\sqrt[4]{2}$ συμβολίζουν πραγματικές θετικές ρίζες, αιτιολογήστε γιατί κάθε μία από τις ενδιάμεσες επεκτάσεις $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ και $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ είναι κανονική. Αποδείξτε, όμως, ότι η επέκταση $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ δεν είναι κανονική.

Άσκηση 4.16. Έστω C αλγεβρική κλειστότητα του σώματος F, $\alpha \in C$ και σ_i, $i = 1, \dots, k$ όλες οι διαφορετικές εμφυτεύσεις $F \hookrightarrow C$. Αποδείξτε ότι

$$(\sigma_1(\alpha) \cdots \sigma_k(\alpha))^r \in F \quad \text{και} \quad r\,(\sigma_1(\alpha) + \cdots + \sigma_k(\alpha)) \in F, \quad \text{όπου} \quad r = \frac{[F(\alpha) : F]}{\{F(\alpha) : F\}}.$$

Υπόδειξη. Θεωρήστε το $f = \mathrm{Irr}\,(\alpha, F)$. Επίσης, είναι χρήσιμο να έχετε υπόψη την απλά αποδείξιμη σχέση (ισχύει γενικά για πολυώνυμα πάνω από αντιμεταθετικό δακτύλιο με μοναδιαίο) $(X^k + a_{k-1}X^{k-1} + \cdots + a_1X + a_0)^r = X^{kr} + ra_{k-1}x^{rk-1} + \cdots + a_0^r$.

Άσκηση 4.17. (i) Έστω σώμα F και $f \in F[X]$ με $\deg f = p$ πρώτο, το οποίο έχει την εξής ιδιότητα: Για κάθε επέκταση E του F ισχύει ότι, αν το f έχει μία ρίζα στο E, τότε το f διασπάται στο E. Αποδείξτε ότι τότε, ή το f είναι ανάγωγο πάνω από το F ή το f έχει ρίζα στο F (άρα διασπάται στο F).

(ii) Αποδείξτε ότι περιπτώσεις ζευγαριών (F, f) που ικανοποιούν τις υποθέσεις του (i) είναι τα εξής: (Υπενθύμιση: Αν $\mathrm{char}F = p$ πρώτος, τότε το F είναι επέκταση του $\mathbb{F}_p$.)

1. $f(x) = X^p - a \in F[X]$, όπου $\mathrm{char}F = p$.
2. $f(X) = X^p - X - a \in F[X]$, όπου $\mathrm{char}F = p$.
   Υπόδειξη. Αν β είναι ρίζα του f σε κάποια αλγεβρική κλειστότητα του F, τότε και το $\beta + c$, με $c \in \mathbb{F}_p$ είναι ρίζα του f.
3. $f(X) = X^p - a \in F[X]$, όπου $\mathrm{char}F \neq p$ και το F περιέχει στοιχείο $\omega \neq 1$ με την ιδιότητα $\omega^p = 1$.
   Υπόδειξη. Θα χρειαστεί να δείξετε ότι $\omega^k \neq 1$ για $1 \leq k < p$.

Άσκηση 4.18. Έστω E/F κανονική επέκταση και $p \in F[X]$ ανάγωγο. Έστω ότι $q_1, q_2 \in E[X]$ είναι μονικοί ανάγωγοι παράγοντες του p. Αποδείξτε ότι υπάρχει F-αυτομορφισμός του E, έστω σ, ώστε $\sigma q_1 = q_2$.
Πόρισμα: Αν $p = q_1 \cdots q_n$, όπου τα $q_1, \dots, q_n \in E[X]$ είναι ανάγωγα, τότε $\deg q_1 = \deg q_2 = \cdots = \deg q_n$.

Κεφάλαιο 5

5.1 5^{η} Εβδομάδα

Κανονικότητα (συνέχεια)

Πόρισμα 5.1. *Αν $F \leq K \leq E$ και η E/F είναι πεπερασμένη καi κανονική τότε η E/K είναι κανονική.*

Απόδειξη. Αν η E/F είναι κανονική, τότε, από το Θεώρημα 4.14 το E είναι σώμα διάσπασης ενός μη μηδενικού $f \in F[X]$. Από την άσκηση 2.15 (iii), το E είναι και σώμα διάσπασης του f πάνω από το K. Πάλι από το θεώρημα 4.14, συμπεράινομε ότι η επέκταση E/K είναι κανονική. □

Θεώρημα 5.2. *Αν η επέκταση E/F είναι πεπερασμένη, τότε υπάρχει πεπερασμένη 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 $f = \operatorname{Irr}(\alpha_1, F) \dots \operatorname{Irr}(\alpha_n, F)$. Θεωρώ το σώμα διάσπασης του f πάνω από το E, το οποίο συμβολίζω με N. Προφανώς, η επέκταση N/E είναι πεπερασμένη. Θα αποδείξω ότι το N έχει τις απαιτούμενες από την εκφώνηση ιδιότητες.

Το N είναι σώμα διάσπασης του f και πάνω από το F (απόδειξη στο τέλος). Άρα από το θεώρημα 4.14 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 $\operatorname{Irr}(\alpha_i, F)$ $(i = 1, \dots, n)$. 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 K 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 5.3. *Κάθε πεπερασμένη και διαχωρίσιμη επέκταση E/F είναι απλή, δηλαδή υπάρχει $a \in E$ τ.ω. $E = F(a)$ (άρα αν $\deg(\operatorname{Irr}(a, F)) = n$, 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 έιναι 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 $e = c_1\beta_1 + \dots + c_n\beta_n$ 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 5.4. $F = \mathbb{Q}, E = \mathbb{Q}[\sqrt[7]{3}, \sqrt[3]{7}]$.

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.

Galois

Ορισμός 5.5. Μια αλγεβρική επέκταση E/F λέγεται επέκταση Galois αν και μόνο αν είναι κανονική και διαχωρίσιμη.

Ορισμός 5.6. Έστω αλγεβρική επέκταση E/F. 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 $\mathrm{Gal}(E/F)$, ή $\mathrm{Aut}(E/F)$, ή $\mathrm{Aut}_F(E)$ (σχεδόν πάντα θα χρησιμοποιούμε τον πρώτο συμβολισμό).

Θεώρημα 5.7. *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 4.12, 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 4.2), άρα $|\mathcal{G}(E/F)| = \{E : F\} = [E : F]$. □

Παρατήρηση 5.8. 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 5.9. 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 συνόλων $\mathcal{E}$ και $\mathcal{O}$ ορίζω τις απεικονίσεις

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

Οι αντιστοιχίες αυτές είναι καλά ορισμένες γιατί είναι πολύ απλό να δείξεις κανείς 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.

Πρόταση 5.10. *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 5.15. □

Πρόταση 5.11. *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 $F_0 := \mathcal{F}(\mathcal{G}(E/F))$. 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.

□

Πρόταση 5.12 (Αντίστροφη της Πρότασης 5.11 (1))**.** *Αν η επέκταση* E/F *είναι πεπερασμένη και* $\mathcal{F}(\mathcal{G}(E/F)) = F$*, τότε η* E/F *είναι Galois.*

Απόδειξη. Πρώτα θ' αποδείξω την κανονικότητα της E/F. Θεωρώ ανάγωγο $f \in F[X]$, το οποίο έχει μία ρίζα $\alpha \in E$ και θα δείξω ότι το f διασπάται στο E. Δίχως βλάβη της γενικότητας, υποθέτω ότι το f είναι μονικό, οπότε $f = \operatorname{Irr}(\alpha, F)$.

Έστω $\mathcal{G}(E/F) = \{\sigma_1 = id_E, \sigma_2, \ldots, \sigma_n\}$, $\alpha := \alpha_1 = \sigma_1(\alpha)$ και $\sigma_i(\alpha) := \alpha_i$ για $i = 2, \ldots, n$. Έστω ότι ακριβώς r από τα $\alpha_1, \ldots, \alpha_n$ διαφορετικά ($r \leq n$). Αριθμώ τους $\sigma_2, \ldots, \sigma_n$ έτσι ώστε τα r πρώτα από αυτά να είναι όλα-όλα τα διαφορετικά α_i (που σημαίνει ότι, αν $r < n$, τότε καθένα από τα υπόλοιπα, $\alpha_{r+1}, \ldots, \alpha_n$ ισούται με κάποιο από τα $\alpha_1, \ldots, \alpha_r$). Ορίζω το

$$g(X) = \prod_{j=1}^{r} (X - \alpha_j) \in E[X]$$

και πρώτα-πρώτα παρατηρώ ότι είναι διαχωρίσιμο εκ κατασκευής (αφού τα $\alpha_1, \ldots, \alpha_r$ έχουν υποτεθεί διαφορετικά). Θα δείξω ότι $g(X) \in F[X]$ ως εξής: Θεωρώ τυχαίο $\sigma_i \in \mathcal{G}(E/F)$ ($1 \leq i \leq n$) και το πολυώνυμο

$$\sigma_i g(X) = \prod_{j=1}^{r} (X - \sigma_i(\alpha_j)) = \prod_{j=1}^{r} (X - \sigma_i\sigma_j(\alpha)).$$

Είναι $\sigma_i\sigma_j \in \mathcal{G}(E/F) = \{\sigma_1, \dots, \sigma_n\}$, συνεπώς $\sigma_i\sigma_j(\alpha) \in \{\alpha_1, \dots, \alpha_r\}$. Επίσης, οι τιμές $\sigma_i\sigma_j(\alpha)$ είναι διαφοετικές μεταξύ τους διότι, αν $\sigma_i\sigma_j(\alpha) = \sigma_i\sigma_k(\alpha)$, επειδή σ_i είναι 1-1 έπεται ότι $\sigma_j(\alpha) = \sigma_k(\alpha)$ δηλαδή $\alpha_j = \alpha_k$, που αντιφάσκει στο ότι οι $1 \leq k, j \leq r$ και $k \neq j$. Συνεπώς, τα $\sigma_i\sigma_j(\alpha)$, $j = 1, \dots, r$ αποτελούν μετάθεση των $\alpha_1, \dots, \alpha_r$, άρα $\sigma_i g = g$, οπότε κάθε συντελεστής του g μένει αναλλοίωτος από κάθε $\sigma_i \in \mathcal{G}(E/F)$. Αυτό σημαίνει ότι κάθε συντελεστής του g ανήκει στο $\mathcal{F}(\mathcal{G}(E/F)) = F$, άρα $g \in F[X]$. Ισχυρίζομαι τώρα ότι $g = \mathrm{Irr}(\alpha, F)$. Πράγματι, το $f = \mathrm{Irr}(\alpha, F)$ και το g έχουν κοινή ρίζα το α, άρα $f \mid g$. Ειδικότερα $\deg f \leq \deg g = r$. Αφετέρου, η σχέση $f(\alpha) = 0$ συνεπάγεται την $0 = \sigma_i(f(\alpha)) = f(\sigma_i(\alpha)) = f(\alpha_i)$ για κάθε $i = 1, \dots, r$, άρα το f έχει τουλάχιστον r διαφορετικές ρίζες, οπότε $\deg f \geq r$. Έτσι, $\deg f = \deg g$ και, συνεπώς, $f = g$. Αλλά το g, διασπάται στο E, άρα το f διασπάται στο E. Αυτό ολοκληρώνει την απόδειξη της κανονικότητας της επέκτασης E/F. Επιπλέον, απέδειξα παράλληλα ότι κάθε ανάγωγο $f \in F[X]$ είναι διαχωρίσιμο, άρα αν θεωρήσω ένα οποιοδήποτε $\beta \in E$, τότε το $\mathrm{Irr}(\beta, F)$ είναι διαχωρίσιμο, που σημαίνει ότι το β είναι διαχωρίσιμο. Συνεπώς, η επέκταση E/F είναι και διαχωρίσιμη. □

Πόρισμα 5.13. *Η πεπερασμένη επέκταση E/F είναι Galois αν και μόνο αν ισχύει $\mathcal{F}(\mathcal{G}(E/F)) = F$.*

Απόδειξη. Προφανής συνδυασμός των Προτάσεων 5.12 και 5.11 (1). □

Παρατήρηση 5.14. Οι Ορισμοί 5.5 (επέκτασης Galois) και 5.6 (ομάδας Galois) αναφέρονται σε αλγεβρική επέκταση E/F, όχι κατ' ανάγκη πεπερασμένη. Το ίδιο ισχύει και για τα σύνολα $\mathcal{E}$ ενδιάμεσων επεκτάσεων της E/F και $\mathcal{O}$ υποομάδων της $\mathcal{G}(E/F)$ και τις μεταξύ τους αντιστοιχίες $\mathcal{G}(E/\bullet)$ και $\mathcal{F}(\bullet)$. Μπορεί να αποδειχθεί ότι το Πόρισμα 5.13 ισχύει γενικότερα για αλγεβρικές επεκτάσεις, όχι κατ' ανάγκη πεπερασμένες. Συνεπώς,

$$E/F \text{ αλγεβρική και Galois} \overset{5.5}{\iff} E/F \text{ κανονική και διαχωρίσιμη} \iff \mathcal{F}(\mathcal{G}(E/F)) = F,$$

όπου, βεβαίως, για την τελευταία ισοδυναμία απαιτείται απόδειξη που δεν προϋποθέτει ότι η επέκταση είναι κανονική.

Ο ορισμός της επέκτασης Galois γενικεύεται ακόμη περισσότερο, ώστε να συμπεριλάβει και μη αλγεβρικές επεκτάσεις: *Μία επέκταση E/F λέγεται Galois αν ικανοποιεί τη συνθήκη $\mathcal{F}(\mathcal{G}(E/F)) = F$.* Παρατηρήστε ότι, για οποιαδήποτε επέκταση E/F, οι Ορισμοί 5.6 και 5.9 εξακολουθούν να έχουν νόημα, ανεξαρτήτως του αν η επέκταση E/F είναι αλγεβρική. Όμως, όταν η E/F δεν είναι αλγεβρική, *δεν* ισχύει η ισοδυναμία E/F Galois $\iff$ E/F κανονική και διαχωρίσιμη.

Ασκήσεις

Άσκηση 5.15. Απόδείξτε την Πρόταση 5.10.

Άσκηση 5.16. Έστω E/F επέκταση Galois, ανάγωγα πολυώνυμα $f, g \in F[X]$, $\alpha, \alpha' \in E$ ρίζες του f και $\beta, \beta' \in E$ ρίζες του g. Αν το g είναι ανάγωγο πάνω από το $F(\alpha)$, αποδείξτε ότι υπάρχει $\sigma \in \mathcal{G}(E/F)$ που στέλνει το α στο α' και το β στο β'.

Σημείωση: Οι συλλογισμοί σας να τεκμηριώνονται βάσει των θεωρημάτων/προτάσεων των σημειώσεων.

Άσκηση 5.17. Έστω $E = \mathbb{Q}(\alpha, i)$, όπου $\alpha = \sqrt{1+\sqrt{2}}$ και $i^2 + 1 = 0$. Αποδείξτε τα παρακάτω:

(i) Ο α είναι $\mathbb{Q}$-συζυγής με τον $\alpha' = \sqrt{1-\sqrt{2}}$.

(ii) Η επέκταση $E/\mathbb{Q}$ είναι Galois.

(iii) $\exists\, \sigma \in \mathcal{G}(E/\mathbb{Q}) : \sigma(\alpha) = \alpha'$ και $\sigma(i) = -i$. Ποια είναι η τάξη του σ στην ομάδα $\mathcal{G}(E/\mathbb{Q})$;

(iv) $\exists\, \tau \in \mathcal{G}(E/\mathbb{Q}(i)) : \tau(\alpha) = -\alpha'$. Ποια είναι η τάξη του τ στην ομάδα $\mathcal{G}(E/\mathbb{Q})$;

(v) Δεν υπάρχει στοιχείο της $\mathcal{G}\left(E/\mathbb{Q}(\sqrt{2})\right)$ που να στέλνει το α στο α'. (Προφανώς, $\mathbb{Q}(\sqrt{2}) \leq E$.)

(vi) Βάσει του (i), είναι $\mathrm{Irr}(\alpha, \mathbb{Q}) = \mathrm{Irr}(\alpha', \mathbb{Q}) =$ (έστω) f. Έστω $g = X^2 - 2 \in \mathbb{Q}[X]$ και $\beta = \beta' = \sqrt{2}$. Σύμφωνα με το (v), δεν υπάρχει $\sigma \in \mathcal{G}(E/\mathbb{Q}) : \sigma(\alpha) = \alpha'$ και $\sigma(\beta) = \beta'$. Γιατί αυτό το συμπέρασμα δεν έρχεται σε αντίφαση με την άσκηση 5.16;

Άσκηση 5.18. Έστω ότι K και L είναι κανονικές επεκτάσεις του F. Αποδείξτε ότι και επέκταση KL/F είναι κανονική, όπου KL είναι η ελάχιστη επέκταση του F που περιέχει τα K και L. (Ισοδύναμα: $KL = F(K \cup L)$.)

Υπόδειξη. Θεωρήστε μια αλγεβρική κλειστότητα C του KL. Έστω $f \in F[X]$ ανάγωγο και $\alpha \in KL$ ρίζα του f. Έστω $\beta \in C$ μια οποιαδήποτε άλλη ρίζα του f. Δείξτε (με προσεκτική επιχειρηματολογία) ότι υπάρχει F-μονομορφισμός $\sigma : KL \hookrightarrow C$ με $\sigma(\alpha) = \beta$. Τί μορφή έχει το α, καθώς γνωρίζομε ότι $\alpha \in KL$;

Κεφάλαιο 6

6.1 6η Εβδομάδα

Θεμελιώδες Θεώρημα Galois

Το θεώρημα θα χωριστεί σε μικρότερες προτάσεις. Υποθέτω ότι E/F είναι πεπερασμένη επέκταση Galois.

Πρόταση 6.1. *Οι απεικονίσεις $\mathcal{G}(E/\bullet)$ και $\mathcal{F}(\bullet)$ είναι αντίστροφες η μία της άλλης, άρα τα σύνολα $\mathcal{E}, \mathcal{O}$ βρίσκονται σε αμφιμονοσήμαντη αντιστοιχία.*

Απόδειξη. Θα δείξω ότι $\mathcal{F}(\mathcal{G}(E/\bullet)) = id_{\mathcal{E}}$ και $\mathcal{G}(E/\mathcal{F}(\bullet)) = id_{\mathcal{O}}$.

Για την πρώτη ισότητα, έχω να δείξω ότι αν $F \leq K \leq E$ τότε $\mathcal{F}(\mathcal{G}(E/K)) = K$. Πράγματι, αφού E/F είναι Galois, τότε είναι κανονική και διαχωρίσιμη. Άρα και η E/K ειναι κανονική (Πόρισμα 5.1) και διαχωρίσιμη (Θεώρημα 4.3), δηλαδή Galois. Εφαρμόζοντας την Πρόταση 5.11 για το σώμα K στη θέση του F, προκύπτει η ισότητα.

Για την δεύτερη, αν $H \leq \mathcal{G}(E/F)$ θέλω να δείξω ότι $\mathcal{G}(E/\mathcal{F}(H)) = H$. Από την Πρόταση 5.10 (β′), $\mathcal{G}(E/\mathcal{F}(H)) \geq H$ και θα δείξω ότι ισχύει η ισότητα. Έστω ότι η H ήταν γνήσια υποομάδα της $\mathcal{G}(E/\mathcal{F}(H))$. Προηγουμένως έδειξα ότι η επέκταση E/K είναι Galois για κάθε ενδιάμεση επέκταση K. Άρα και η $E/\mathcal{F}(H)$ είναι Galois. Εφαρμόζω την Πρόταση 5.11 (2) με το $\mathcal{F}(H)$ στη θέση του F και έχω: Αν $H \lneq \mathcal{G}(E/\mathcal{F}(H))$ τότε $\mathcal{F}(H) \gneq \mathcal{F}(H)$ άτοπο. Άρα, αναγκαστικά $\mathcal{G}(E/\mathcal{F}(H)) = H$. □

Παρατήρηση 6.2. Την 1-1 αντιστοιχία της Πρότασης 6.1 συμβολίζομε $\longleftrightarrow$. Η τυπική περίπτωση φαίνεται στο παρακάτω διάγραμμα:

$$\begin{array}{ccc} E & \longleftrightarrow & \mathcal{G}(E/E) = \langle id_E \rangle \\ | & & | \\ K & \longleftrightarrow & H \\ | & & | \\ F & \longleftrightarrow & \mathcal{G}(E/F) =: G \end{array}$$

Την αντιστοιχία $K \leftrightarrow H$ μπορώ να δω με δύο ισοδύναμους τρόπους: Είτε ότι $H = \mathcal{G}(E/K)$ είτε ότι $K = \mathcal{F}(H)$.

Πρόταση 6.3. *Αν στην αντιστοιχια Galois είναι $K \leftrightarrow H$ και $\sigma \in \mathcal{G}(E/F)$ τότε $\sigma(K) \leftrightarrow \sigma H \sigma^{-1}$*

Απόδειξη. Για να δείξω το ζητούμενο έχω δύο επιλογές. Ή θα δείξω ότι $\sigma H\sigma^{-1} = \mathcal{G}\left(E/\sigma(K)\right)$ ή ότι $\sigma(K) = \mathcal{F}\left(\sigma H\sigma^{-1}\right)$. Θα αποδείξω το δεύτερο. Έχω ότι

$$\begin{aligned} u \in \mathcal{F}\left((\sigma H\sigma^{-1})\right) &\iff \\ u \text{ μενει αναλοίωτο από κάθε στοιχείο της } \sigma H\sigma^{-1} &\iff \\ \sigma\tau\sigma^{-1}(u) = u, \forall \tau \in H &\iff \\ \tau\sigma^{-1}(u) = \sigma^{-1}(u), \forall \tau \in H &\iff \\ \sigma^{-1}(u) \in \mathcal{F}(H) &\iff \\ \sigma^{-1}(u) \in K &\iff \\ \sigma(\sigma^{-1}(u)) \in \sigma(K) &\iff \\ u \in \sigma(K) & \end{aligned}$$

□

Πρόταση 6.4. *Αν στην αντιστοιχια Galois είναι $K \leftrightarrow H$, τότε*

$$[E : K] = |H| \quad \textit{και} \quad [K : F] = [G : H] := \frac{|G|}{|H|}.$$

Απόδειξη. Αφού E/F είναι Galois και η E/K θα είναι επίσης όπως είδαμε και στην απόδειξη της Πρότασης 6.1. Άρα $[E : K] = |\mathcal{G}\left(E/K\right)| = |H|$. Επίσης,

$$[K : F] = \frac{[E : F]}{[E : K]} = \frac{|\mathcal{G}\left(E/F\right)|}{|H|} = \frac{|G|}{|H|} = [G : H].$$

(Ο τελευταίος φυσικός αριθμός ονομάζεται δείκτης της H στην G και μετρά το πλήθος των αριστερών ή των δεξιών συμπλόκων της H στη G. Τα αριστερά σύμπλοκα και τα δεξιά σύμπλοκα της H στην G είναι εν γένει διαφορετικά. Ομως, το πλήθος τους συμπίπτει και ταυτίζεται με το δείκτη της H στην G) □

Συνέχεια του Θεμελιώδου Θεωρήματος Galois. Έχουμε ήδη δει ότι αν $F \leq K \leq E$ και η επέκταση E/F είναι Galois, τότε και η επέκταση E/K είναι Galois. Μένει λοιπόν το ερώτημα, πότε η K/F είναι Galois. Επειδή είναι πάντα διαχωρίσιμη, το ερώτημα ισοδυναμεί με το πότε η K/F είναι κανονική. Διατηρούμε το συμβολισμό $G = \mathcal{G}\left(E/F\right)$ και $H = \mathcal{G}\left(E/K\right) \leq G$.

Πρόταση 6.5. *H K/F είναι κανονική (άρα και Galois) αν και μόνο αν $H \trianglelefteq G$ (η H ειναι κανονική υποομάδα της G)*

Απόδειξη. Έστω C μία αλγεβρική κλειστότητα της E.

" $\Longleftarrow$ ": Έστω $H \trianglelefteq K$. Για να δείξω όι η K/F είναι κανονική, αρκεί κάθε F-μονομορφισμός $\sigma : K \hookrightarrow C$ να είναι F-αυτομορφισμός του K σύμφωνα με το Θεώρημα 4.12. Θα πάρω επομένως τυχαίο F-μονομορφισμό $\sigma : K \hookrightarrow C$ και θα δείξω ότι $\sigma(K) = K$. Επειδή η αντιστοιχία Galois είναι αμφιμονοσήμαντη, ισχύει $K = \sigma(K)$ αν και μόνο αν οι αντίστοιχες υποομάδες αυτών είναι ισές. Η υποομάδα που αντιστοιχεί στην K είναι η H και από την Πρόταση 6.3, αυτή που αντιστοιχεί στην $\sigma(K)$ είναι η $\sigma H\sigma^{-1}$. Αφού η H είναι κανονική $H = \sigma H\sigma^{-1}$ άρα $\sigma(K) = K$.

" $\Longleftarrow$ ": Υποθέτω ότι K/F είναι κανονική και θέλω να δείξω ότι $H \trianglelefteq G$, δηλαδή, ότι για κάθε $\sigma \in G$ ισχύει $\sigma H\sigma^{-1} = H$. Θα δείξω ότι τα αντίστοιχα σταθεροποιούμενα σώματα είναι ίσα. Όμως η $\sigma H\sigma^{-1}$ αντιστοιχεί στο $\sigma(K)$ και η H στο K. Άρα αρκεί να δείξω ότι $K = \sigma(K)$. Ο σ είναι F-αυτομορφισμός του E. Άρα ο $\sigma|_K$ είναι F-μονομορφισμός $K \hookrightarrow E$. Επειδή η K/F είναι κανονική, ο $\sigma|_K$ στην πραγματικότητα είναι F-αυτομορφισμός του K, άρα είναι και επί. Επομένως $\sigma|_K(K) = \sigma(K) = K$. □

Πρόταση 6.6. *Στην περίπτωση που η K/F είναι κανονική ισχύει ότι $\mathcal{G}(K/F) = G/H$, δηλαδή*

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

Απόδειξη. Θεωρώ την απεικόνιση $\psi : \mathcal{G}(E/F) \to \mathcal{G}(K/F)$ με $\sigma \mapsto \sigma|_K$. Από την απόδειξη της προηγούμενης πρότασης, η επέκταση K/F είναι κανονική και ο $\sigma|_K$ είναι F-αυτομορφισμός του K άρα η ψ είναι καλά ορισμένη, δηλαδή, $\psi(\sigma) \in \mathcal{G}(K/F)$. Προφανώς, για κάθε $u \in K$ και κάθε $\sigma \in \mathcal{G}(E/F)$, ισχύει $\psi(\sigma)(u) = \sigma(u)$. Από αυτό έπεται ότι, για κάθε $\sigma, \tau \in \mathcal{G}(E/F)$ ισχύει $\psi(\sigma\tau)(u) = (\psi(\sigma)\psi(\tau))(u)$ για κάθε $u \in K$, άρα $\psi(\sigma\tau) = \psi(\sigma)\psi(\tau)$ ο ψ είναι ομομορφισμός ομάδων.

Ο ψ είναι επιμορφισμός. Έστω $\tau \in \mathcal{G}(K/F)$. Θεωρώ την επέκταση του τ, $\tilde{\tau} : C \hookrightarrow C$ και μετά θεωρώ την $\sigma = \tilde{\tau}|_E$. Ο σ είναι F-μονομορφισμός $E \hookrightarrow C$. Αλλά η E/F είναι κανονική άρα $\sigma \in \mathcal{G}(E/F)$. Προφανώς $\sigma_K = \tau$ άρα η ψ είναι επί.

Τέλος, έστω $\mathcal{G}(E/F) = G$. Είναι $\ker\psi = \{\sigma \in G : \psi(\sigma) = id_K\}$ άρα $\sigma \in \ker\psi \iff \sigma|_K = id_K \iff \sigma \in \mathcal{G}(E/K)$. Άρα $\ker\psi = \mathcal{G}(E/K) = H$. Από το πρώτο θεώρημα ομομορφισμών ομάδων έπεται ότι

$$\mathcal{G}(E/F)/\mathcal{G}(E/K) = G/H = G/\ker\psi \cong \operatorname{Im}\psi = \mathcal{G}(K/F).$$

□

Συγκεντρώνοντας τα συμπεράσματα των Προτάσεων 5.11 (1), 5.12, 6.1, 6.3, 6.5, 6.6, διατυπώνομε το εξής

Θεώρημα 6.7 (Θεμελιώδες Θεώρημα της Θεωρίας Galois)**.** *Έστω E/F πεπερασμένη επέκταση Galois, $\mathcal{E}$ το σύνολο των ενδιάμεσων επεκτάσεων και $\mathcal{O}$ το σύνολο των υποομάδων της $G := \mathcal{G}(E/F)$.*

1. *Οι απεικονίσεις*

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

   είναι αντίστροφες η μία της άλλης, άρα κάθε μία είναι 1-1 και επί. Συμβολικά όταν γράφω $K \leftrightarrow H$ εννοώ αυτή την αμφιμονοσήμαντη αντιστοιχία.

2. *Αν $K \in \mathcal{E}$ και $K \leftrightarrow H$ τότε $[E : K] = |H|$ και $[K : F] = [G : H] = \frac{|G|}{|H|}$. Ειδικότερα $[E : F] = |\mathcal{G}(E/F)|$.*

3. *Αν $K \leftrightarrow H$ τότε για κάθε $\sigma \in G$, $\sigma(K) \longleftrightarrow \sigma H \sigma^{-1}$.*

4. *Αν $K \in \mathcal{E}$ τότε η E/K είναι Galois. Επιπλέον η K/F είναι Galois αν και μόνο αν $\mathrm{H} \trianglelefteq G$ όπου $H = \mathcal{G}(E/K)$ (δηλαδή $K \leftrightarrow H$). Στην περίπτωση που αυτη η συνθήκη ισχύει, έχομε τον ισομορφισμό ομάδων $\mathcal{G}(K/F) \cong \mathcal{G}(E/F)/\mathcal{G}(E/K)$.*

Υπενθύμιση 6.8 (Για το παράδειγμα που θα ακολουθήσει)**.** Η ομάδα

$$D_n = \langle a, b | a^n = b^2 = 1, ba = a^{n-1}b \rangle$$

ονομάζεται διεδρική βαθμού n και έχει τάξη $|D_n| = 2n$.

Παράδειγμα 6.9. Έστω $f = X^4 - 2 \in \mathbb{Q}[X]$ και E το σώμα διάσπασης του πάνω από το $\mathbb{Q}$. Εύκολα μπορούμε να δούμε ότι $E = \mathbb{Q}(\rho, i)$ με $\rho^4 = 2$ και $i^2 = -1$ και ότι $[E : \mathbb{Q}] = 8$ με βάση τα $\{\rho^k i^l\}_{0 \le k \le 3, 0 \le l \le 1}$.

Η επέκταση $E/\mathbb{Q}$ είναι Galois αφού είναι κανονική (το E είναι σώμα διάσπασης του f) και διαχωρίσιμη (το $\mathbb{Q}$ έχει χαρακτηριστική 0). Άρα $|\mathcal{G}(E/\mathbb{Q})| = [E:\mathbb{Q}] = 8$. Έστω $G = \mathcal{G}(E/\mathbb{Q})$. Ελέγξτε ότι υπάρχουν $\sigma, \tau \in G$ τέτοιοι ώστε $\sigma(\rho) = i\rho$, $\sigma(i) = i$, $\tau(\rho) = \rho$ και $\tau(i) = -i$

Κάθε στοιχείο της G χαρακτηρίζεται από τις τιμές του στα ρ και i. Οι δράσεις των αυτομορφισμών της G στα ρ και i φαίνονται στον παρακάτω πίνακα

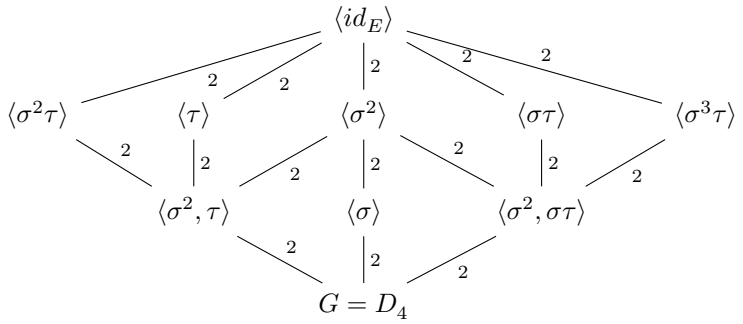
αυτομορφισμός	δράση στο ρ	δράση στο i
id_E	ρ	i
σ	$i\rho$	i
σ^2	$-\rho$	i
σ^3	$-i\rho$	i
τ	ρ	$-i$
$\sigma\tau$	$i\rho$	$-i$
$\sigma^2\tau$	$-\rho$	$-i$
$\sigma^3\tau$	$-i\rho$	$-i$

Ελέγχω ότι $\mathrm{ord}(\sigma) = 4$, $\mathrm{ord}(\tau) = 2$ και ότι $\tau\sigma = \sigma^3\tau$. Άρα μέσα στη G έχω την ομάδα

$$\langle \sigma, \tau | \sigma^4 = id = \tau^2, \tau\sigma = \sigma^3\tau \rangle \cong D_4$$

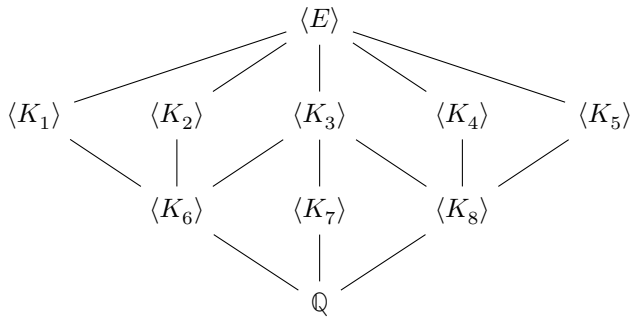
η οποία είναι τάξεως 8, άρα αυτή η ομάδα ταυτίζεται με τη G και $G \cong D_4$.

Το δίκτυο υποομάδων της D_4 είναι



Σε κάθε ακμή σημειώνεται ο δείκτης της υποομάδας που βρίσκεται πάνω, ως προς αυτή απο κάτω της. Επιπλέον, βλέπομε ότι η πρώτη υποομάδα είναι τάξης 1, αυτές της δέυτερης γραμμής είναι τάξης 2, της τρίτης γραμμής είναι τάξης 4 και η G τάξης 8.

Μέσω της αντιστοιχίας Galois, γνωρίζομε ότι οι ενδιάμεσες επεκτάσεις της E/K είναι σε ένα δίκτυο της ίδιας μορφής



Κάθε K_i αντιστοιχεί, μέσω της αντιστοιχίας Galois, με την υποομάδα του διαγράμματος υποομάδων, η οποία βρίσκεται στην ακριβώς αντίστοιχη θέση. Π.χ. $E \longleftrightarrow \langle id_E \rangle$, $\mathbb{Q} \longleftrightarrow G$, $K_2 \longleftrightarrow \langle \tau \rangle$, $K_8 \longleftrightarrow \langle \sigma^2, \sigma\tau \rangle$. Εδώ, όλες οι διαδοχικές επεκτάσεις είναι βαθμού 2 όσο και οι αντίστοιχοι δείκτες υποομάδων. Επιπλέον μπορούμε να δείξομε ότι

$$\begin{aligned} K_1 &= \mathbb{Q}(i\rho) \\ K_2 &= \mathbb{Q}(\rho) \\ K_3 &= \mathbb{Q}(i\rho^2) = \mathbb{Q}(i\sqrt{2}) \\ K_4 &= \mathbb{Q}((1+i)\rho) \\ K_5 &= \mathbb{Q}((1-i)\rho) \\ K_6 &= \mathbb{Q}(\sqrt{2}) \\ K_7 &= \mathbb{Q}(i) \\ K_8 &= \mathbb{Q}(i\sqrt{2}) \end{aligned}$$

Πώς αποδεικνύονται αυτές οι ισότητες; Μια κάπως δύσκολη αντιστοιχία είναι

$$\langle \sigma\tau \rangle \longleftrightarrow \mathbb{Q}((1+i)\rho),$$

δηλαδή, $K_4 = \mathbb{Q}((1+i)\rho)$.
Έχω το διάγραμμα

$$\begin{array}{ccc} \langle id_E \rangle & \longrightarrow & E = \mathbb{Q}(i,\rho) \\ \Big| & & \Big|_2 \\ \langle \sigma\tau \rangle & \longrightarrow & K_4? \\ \Big|_2 & & \Big|_4 \\ G & \longrightarrow & \mathbb{Q} \end{array}$$

Άρα περιμένω το σταθεροποιούμενο απ το $\langle \sigma\tau \rangle$ να είναι επέκταση του $\mathbb{Q}$ βαθμού 4.
Βάση της $E/\mathbb{Q} : 1, \rho, \rho^2, \rho^3, i, i\rho, i\rho^2, i\rho^3$. Έστω

$$u = a_0 + a_1\rho + a_2\rho^2 + a_3\rho^3 + b_0 i + b_1 i\rho + b_2 i\rho^2 + b_3 i\rho^3 \in K_4$$

με τα $a_i, b_i \in \mathbb{Q}$. Τότε,

$$u = \sigma\tau(u) = a_0 + a_1 i\rho + a_2(-\rho^2) + a_3(-i\rho^3) - b_0 i + b_1\rho + b_2 i\rho^2 - b_3\rho^3$$

Άρα,

$$\begin{aligned} a_1 &= b_1 \\ a_2 &= -a_2 \\ b_3 &= -a_3 \\ -b_0 &= b_0 \\ a_1 &= b_1 \\ b_3 &= -a_3, \end{aligned}$$

οπότε $a_2 = b_0 = 0$ και ελεύθερες παράμετροι είναι τα a_0, a_1, a_3 και b_2. Συνεπώς,

$$\begin{aligned} u &= a_0 + a_1\rho + a_3\rho^3 + a_1 i\rho + b_2 i\rho^3 - a_3 i\rho^3 \\ &= a_0 + a_1\rho(1+i) + b_2 i\rho^2 + a_3(1-i)\rho^3 \end{aligned}$$

Αν $\lambda := \rho(1+i)$, τότε $\lambda^2 = 2\rho^2 i$ και $\lambda^3 = \rho^3 2(i-1)$. Επομένως,

$$u = a_0 + a_1\lambda + \frac{b_2}{2}\lambda^2 - \frac{a_3}{2}\lambda^3$$

Άρα το u είναι γραμμικός συνδυασμός των $1, \lambda, \lambda^2, \lambda^3$. Συνεπώς, $u = \sigma\tau(u) \iff u \in \mathbb{Q}(\lambda)$. Αλλά

$$\lambda^4 = (\rho^2(1+i)^2)^2 = (\sqrt{2}(2i))^2 = -8,$$

άρα το λ είναι ρίζα του $X^4 + 8$.

Με ανάλογο τρόπο, μπορώ να δείξω την αντιστοιχία

$$\langle\sigma^3\tau\rangle \longleftrightarrow \mathbb{Q}((1-i)\rho).$$

Αν $\mu = (1-i)\rho$, τότε πάλι

$$\mu^4 = ((1-i)^2\rho^2)^2 = ((-2i)\sqrt{2})^2 = -8$$

Είναι $\langle\sigma\tau\rangle \neq \langle\sigma^3\tau\rangle$, άρα (λόγω του 1-1 της αντιστοιχίας Galois) $\mathbb{Q}(\mu) \neq \mathbb{Q}(\lambda)$, παρά το ότι τα μ, λ είναι ρίζες του ιδίου ανάγωγου πολυωνύμου $X^4 + 8$.

Ερώτηση: Είναι η $\langle\sigma\tau\rangle$ κανονική υποομάδα της G;

Ισοδύναμο ερώτημα: Είναι η $\mathbb{Q}(\lambda)/\mathbb{Q}$ επέκταση Galois;

Επειδή είναι διαχωρίσιμη, ισοδύναμο ερώτημα: Είναι η $\mathbb{Q}(\lambda)/\mathbb{Q}$ κανονική επέκταση;

Απάντηση, όχι! Το $X^4 + 8$ έχει τη ρίζα $\lambda \in \mathbb{Q}(\lambda)$, όμως $\mu \notin \mathbb{Q}(\lambda)$, διότι $\mathbb{Q}(\mu) \neq \mathbb{Q}(\lambda)$.

Το ότι $(1-i)\rho \notin \mathbb{Q}((1+i)\rho)$ δεν είναι προφανές αν δεν κάνω χρήση του θεωρήματος Galois! Αν όμως κάνω χρήση του θεωρήματος, τότε καθώς $\langle\sigma\tau\rangle \neq \langle\sigma^3\tau\rangle$, προκύπτει αμέσως ότι $\mathbb{Q}(\mu) \neq \mathbb{Q}(\lambda)$ και, άρα, $\mu \notin \mathbb{Q}(\lambda)$.

Ένα δεύτερο παράδειγμα αντιστοιχίας που απαιτεί λιγότερες πράξεις:

$$\langle\sigma^2\rangle \longleftrightarrow \mathbb{Q}(i, \sqrt{2}),$$

δηλαδή, $K_3 = \mathbb{Q}(i, \sqrt{2})$. Αυτή η ισότητα προκύπτει αμέσως, ως εξής: Είναι $\sigma(i) = i$, άρα $\sigma^2(i) = i$. Επίσης, $\sigma(\sqrt{2}) = \sigma(\rho^2) = (\sigma(\rho))^2 = (i\rho)^2 = -\sqrt{2}$, οπότε $\sigma^2(\sqrt{2}) = \sqrt{2}$. Συνεπώς, τα i και $\sqrt{2}$ ανήκουν στο σταθεροποιούμενο σώμα του σ^2. Αυτό συνεπάγεται ότι $\mathbb{Q}(i, \sqrt{2}) \leq \mathcal{F}(\langle\sigma^2\rangle)$. Από το Θεώρημα Galois, το $\mathcal{F}(\langle\sigma^2\rangle)$ έχει βαθμό πάνω από το $\mathbb{Q}$ ίσο με τον δείκτη $[G : \langle\sigma^2\rangle] = 4$. Επειδή είναι και $\left[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}\right] = 4$, συμπεραίνω ότι $K_3 = \mathcal{F}(\langle\sigma^2\rangle) = \mathbb{Q}(i, \sqrt{2})$.

Τώρα έχομε το διάγραμμα

$$\begin{array}{ccc} E & \longrightarrow & \langle id\rangle \\ \Big| 2 & & \Big| \\ K_3 = \mathbb{Q}(i, \sqrt{2}) & \longrightarrow & \langle\sigma^2\rangle \\ \Big| 4 & & \Big| \\ \mathbb{Q} & \longrightarrow & G \end{array}$$

Η επέκταση $K_3/\mathbb{Q}$ είναι προφανώς κανονική ως σώμα διάσπασης του $(X^2+1)(X^2-2)$, άρα, από το Θεώρημα Galois συμπεραίνω ότι $\sigma^2 \trianglelefteq G$ και, ακόμη, ότι $\mathcal{G}\left(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}\right) \cong G/\langle\sigma^2\rangle$.

Έχω τώρα, $G/\langle\sigma^2\rangle = \{\bar{1}, \bar{\sigma}, \bar{\tau}, \bar{\tau\sigma}\}$, όπου $\bar{1} = \{id_E, \sigma^2\}$, $\bar{\sigma} = \{\sigma, \sigma^3\}$, $\bar{\tau} = \{\tau, \tau\sigma^2\}$, $\bar{\tau\sigma} = \{\tau\sigma, \tau\sigma^3\}$. Ο πίνακας της ομάδας $G/\langle\sigma^2\rangle$ είναι

	$\bar{1}$	$\bar{\sigma}$	$\bar{\tau}$	$\bar{\tau\sigma}$
$\bar{1}$	$\bar{1}$	$\bar{\sigma}$	$\bar{\tau}$	$\bar{\tau\sigma}$
$\bar{\sigma}$	$\bar{\sigma}$	$\bar{1}$	$\bar{\tau\sigma}$	$\bar{\tau}$
$\bar{\tau}$	$\bar{\tau}$	$\bar{\tau\sigma}$	$\bar{1}$	$\bar{\sigma}$
$\bar{\tau\sigma}$	$\bar{\tau\sigma}$	$\bar{\tau}$	$\bar{\sigma}$	$\bar{1}$

Βλέπομε πως έχομε τον πίνακα ομάδα τάξεως 4, της οποίας κάθε στοιχείο έχει τάξη 2, άρα είναι η «ομάδα των τεσσάρων» $Klein\ \langle a, b | a^2 = b^2 = 1, ba = ab\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

Πώς «μεταφράζω» το ότι $\mathcal{G}\left(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}\right) \cong G/\langle\sigma^2\rangle$; Αφού η ομάδα στα δεξιά είναι ομάδα Klein, έπεται ότι η ομάδα $\mathcal{G}(K_3/\mathbb{Q})$ ($K_3 = \mathbb{Q}(i, \sqrt{2})$) παράγεται από δύο αυτομορφισμούς, έστω $\phi, \psi \in \mathcal{G}(K/\mathbb{Q})$, για τους οποίους ισχύει $\phi^2 = \psi^2 = id_K$.

Εις αναζήτησιν $\mathbb{Q}$-αυτομορφισμού ϕ του $K = \mathbb{Q}(i, \sqrt{2})$ με τις παραπάνω ιδιότητες: Ξέρω ότι $\phi(i) \in \{\pm i\}$ και $\phi(\sqrt{2}) \in \{\pm\sqrt{2}\}$. Επιλέγω τον ϕ να ικανοποιεί τις σχέσεις $\phi(i) = -i$ και $\phi(\sqrt{2}) = \sqrt{2}$. Ανάλογα επιλέγω τον ψ να ικανοποιεί τις $\psi(i) = i$ και $\psi(\sqrt{2}) = -\sqrt{2}$. Ελέγχοντας τη δράση των ϕ^2 και ψ^2 στα στοιχεία $i, \sqrt{2}$ βλέπω ότι τα αφήνουν αναλλοίωτα, άρα $\phi^2 = \psi^2 = id_K$.

Γιατί υπάρχει τέτοιος ϕ; Είναι επέκταση του ταυτοτικού $id_{\mathbb{Q}(\sqrt{2})}$ στο παρακάτω διάγραμμα στέλνοντας το i στο $-i$.

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2}, i) & \xrightarrow{\phi} & \mathbb{Q}(\sqrt{2}, i) \\ \Big| & & \Big| \\ \mathbb{Q}(\sqrt{2}) & \xrightarrow{id} & \mathbb{Q}(\sqrt{2}) \end{array}$$

Ανάλογα αποδεικνύεται και η ύπαρξη του ψ.

Ασκήσεις

Άσκηση 6.10. Η άσκηση έχει να κάνει ἀποκλειστικά με ομάδες, αλλά χρειάζεται σε ένα ερώτημα της επόμενης άσκησης.
Έστω ομάδα $(G, \cdot)$, $H \leq G$ και $J = \bigcap_{g\in G} gHg^{-1}$. Αποδείξτε ότι $J \trianglelefteq G$.

Άσκηση 6.11. Έστω πεπερασμένη διαχωρίσμη επέκταση E/F και N κανονική κλειστότητα του E πάνω από το F.
(α΄) Αποδείξτε ότι η N/F είναι Galois.
Υπόδειξη. Από το Θεώρημα 5.3, η επέκταση E/F είναι απλή. Έστω $E = F(\alpha)$, $f = \mathrm{Irr}(\alpha, F)$ και $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n \in N$ όλες οι ρίζες του f. Δείξτε ότι $N = F(\alpha_1, \ldots, \alpha_n)$.
(β΄) Έστω $G = \mathcal{G}(N/F)$ και $H = \mathcal{G}(N/E)$.
(β΄.1) Έστω $H' \trianglelefteq G$ τέτοια ώστε $H' \leq H$. Αποδείξτε ότι στην επέκταση N/F το σταθεροποιούμενο σώμα της H' είναι το N και συμπεράνετε ότι $H' = \langle id_N\rangle$.
(β΄.2) Εφαρμόζοντας την άσκηση 6.10 αποδείξτε ότι $\bigcap_{\sigma\in G} \sigma H\sigma^{-1} = \langle id_N\rangle$.

Άσκηση 6.12. Έστω $\bar{\mathbb{Q}}$ αλγεβρική κλειστότητα του $\mathbb{Q}$ (δεν είναι απαραίτητο να τη δείτε ως υπόσωμα του $\mathbb{C}$). Θεωρούμε τους $\alpha, \beta, \gamma \in \bar{\mathbb{Q}}$ που ικανοποιούν τις σχέσεις $\alpha^2 = 2$, $\beta^2 = 3$ και $\gamma^2 = 5$.
(1) Αποδείξτε ότι το $X^2 - 3$ είναι ανάγωγο πάνω από το $\mathbb{Q}(\alpha)$.
(2) Έστω $K = \mathbb{Q}(\alpha, \beta)$. Αποδείξτε ότι η επέκταση $K/\mathbb{Q}$ είναι Galois. Αποδείξτε, επίσης, ότι υπάρχουν $\sigma, \tau \in \mathcal{G}(K/\mathbb{Q})$ με τις εξής ιδιότητες: $\sigma(\alpha) = -\alpha$, $\sigma(\beta) = \beta$ και $\tau(\alpha) = \alpha$, $\tau(\beta) = -\beta$. Δείξτε ότι $\mathcal{G}(K/\mathbb{Q}) = \langle\sigma, \tau\rangle$ και αυτή η ομάδα είναι η V_4 («ομάδα των τεσσάρων του Klein»). Κατασκευάστε το δίκτυο των υποομάδων της $\mathcal{G}(K/\mathbb{Q})$ και το αντίστοιχο δίκτυο ενδιαμέσων επεκτάσεων της $K/\mathbb{Q}$.

(3) Αποδείξτε με «έξυπνο» τρόπο, δίχως καθόλου πράξεις (εκμεταλλευόμενοι το (2)), ότι το X^2-5 είναι ανάγωγο πάνω από το K. Συμπεράνετε ότι η επέκταση E/K είναι βαθμού 2, όπου $E=\mathbb{Q}(\alpha,\beta,\gamma)$. Αποδείξτε ότι η $E/\mathbb{Q}$ είναι Galois, βαθμού 8 και βρείτε μια βάση της.
(4) Έστω $G=\mathcal{G}(E/\mathbb{Q})$. Αποδείξτε ότι υπάρχουν $\phi,\chi,\psi\in G$ με τις εξής ιδιότητες:

$$\phi(\alpha)=-\alpha,\ \phi(\beta)=\beta,\ \phi(\gamma)=\gamma$$
$$\chi(\alpha)=\alpha,\ \chi(\beta)=-\beta,\ \chi(\gamma)=\gamma$$
$$\psi(\alpha)=\alpha,\ \psi(\beta)=\beta,\ \psi(\gamma)=-\gamma$$

Κατασκευάστε πίνακα που θα δείχνει πώς δρουν στα α,β,γ οι αυτομορφισμοί $\mathrm{id}_E,\phi,\chi,\psi,\phi\chi,\phi\psi,\chi\psi,\phi\chi\psi$.
(5) Αποδείξτε ότι $G=\langle\phi,\chi,\psi\rangle$, η G είναι αβελιανή, τάξεως 8 και τα στοιχεία της έχουν τάξη 2.
(6) Θεωρήστε δεδομένα τα εξής: Όλες οι υποομάδες της G τάξεως 2 είναι οι

$$\langle\phi\rangle,\ \langle\chi\rangle,\ \langle\psi\rangle,\ \langle\phi\chi\rangle,\ \langle\phi\psi\rangle,\ \langle\chi\psi\rangle,\ \langle\phi\chi\psi\rangle.$$

Όλες οι υποομάδες της G τάξεως 4 είναι οι

$$\langle\phi,\chi\rangle,\ \langle\phi,\psi\rangle,\ \langle\chi,\psi\rangle,\ \langle\phi,\chi\psi\rangle,\ \langle\chi,\phi\psi\rangle,\ \langle\psi,\phi\chi\rangle,\ \langle\phi\chi,\phi\psi\rangle.$$

Με τη βοήθεια του πίνακα του ερωτήματος (4) υπολογίστε την ενδιάμεση επέκταση που αντιστοιχεί σε κάθε μία από τις παραπάνω 14 υποομάδες.

Άσκηση 6.13. Έστω σώμα F με $\mathrm{char}F\neq 2,3$, το πολυώνυμο $f=X^3+aX+b\in F[X]$, του οποίου οι τρεις ρίζες (σε κάποια αλγεβρική κλειστότητα του F) υποθέτομε ότι είναι διαφορετικές και E σώμα διάσπασης του f πάνω από το F. Παρατηρήστε ότι η E/F είναι επέκταση Galois.
Παρατήρηση που δικαιολογεί γιατί όταν μελετούμε κυβικά πολυώνυμα σ' ένα σώμα F όπως το παραπάνω, μπορούμε να θεωρούμε ότι ο συντελεστής του X^2 είναι 0: Αν $g(X)=X^3+pX^2+qX+r\in F[X]$, τότε το $g(X-p/3)$ έχει συντελεστή του X^2 ίσο με 0, άρα είναι της μορφής του παραπάνω f και, επιπλέον, οι ρίζες του διαφέρουν από αυτές του $g(X)$ κατά $p/3$, οπότε αυτά τα δύο πολυώνυμα έχουν το ίδιο σώμα διάσπασης. Γράφοντας $p/3$ εννοούμε, βεβαίως, $p/(3\cdot 1_F)$.
(i) Έστω $\delta=(\rho_1-\rho_2)(\rho_1-\rho_3)(\rho_2-\rho_3)$. Αποδείξτε, με χρήση Θεωρίας Galois, ότι $\delta^2\in F$.
(ii) Αν $\delta\notin F$ αποδείξτε ότι $E=F(\rho,\delta)$ δίχως να χρησιμοποιήσετε το επόμενο ερώτημα (iv). Περιγράψτε την $\mathcal{G}(E/F)$, δηλαδή, τους γεννήτορες αυτομορφισμούς της, τη «δράση» τους στα ρ και δ και τις τάξεις τους στην ομάδα.
(iii) Εκφράστε τις ρίζες ρ_2,ρ_3 ως στοιχεία του $F(\rho,\delta)$, ανεξάρτητα από το αν το δ ανήκει στο F ή όχι, είναι ο εξής (εννοείται ότι μπορείτε να βρείτε διαφορετικό τρόπο από αυτόν που προτείνεται εδώ): Έστω $\beta=\rho-\rho_2$ και $\gamma=\rho-\rho_3$. Τότε $\delta=\beta\gamma(\gamma-\beta)$. Με τη βοήθεια των σχέσεων ριζών-συντελεστών (τύποι του Viéte) δείξτε ότι $\beta+\gamma=3\rho$ και $\beta\gamma=3\rho^2+a$. Βάσει αυτών των σχέσεων μπορείτε να εκφράσετε και το $\gamma-\beta$ ως στοιχείο του $F(\rho,\delta)$. (Εδώ θα χρειαστεί να είναι $\mathrm{char}F\neq 2$.

Πεπερασμένα σώματα

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

Θεώρημα 6.14. *Αν το E είναι πεπερασμένο σώμα χαρακτηριστικής p, τότε ισχύουν τα εξής.*

1) $|E|=p^n$ *όπου* $n=\left[E:\mathbb{F}_p\right]\in\mathbb{N}$

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 6.15. Αν το E είναι σώμα χαρακτηριστικής p, τότε η απεικόνηση, $a\pmod p\overset{\phi}{\mapsto}a\cdot 1_E$ 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 $E = \{c_1 a_1 + \cdots + c_n a_n : c_i \in \mathbb{F}_p\}$. Έχω p^n επιλογές για τη n-άδα $(c_1, \dots, c_n)$, συνεπώς, $|E| = p^n$.

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 πανω από το $\mathbb{F}_p$. □

Πόρισμα 6.16. *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 2.14). □

Ορισμός 6.17. Για δοσμένο πρώτο p και $n \geq 1$, «σώμα Galois με p^n στοιχεία» είναι κάθε σώμα με p^n στοιχεία και συμβολίζεται με $\mathrm{GF}(p^n)$. 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 6.18. *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 Froebenius του E, που ορίζεται: $\sigma(a) = a^p$* (βλ. Ορισμό 3.21).

Απόδειξη. Να δείξω ότι $E/\mathbb{F}_p$ είναι κανονική και διαχωρίσιμη. Κανονική είναι διότι, σύμφωνα με το Θεώρημα 6.14 (2), το E είναι το σώμα διάσπασης του πολυωνύμου $f = X^{p^n} - X$ πάνω από το $\mathbb{F}_p$, άρα εφαρμόζεται το Θεώρημα 4.14.

Τώρα θα δείξομε ότι η επέκταση $E/\mathbb{F}_p$ είναι διαχωρίσιμη, αποδεικνύοντας ότι κάθε $\alpha \in E$ είναι διαχωρίσιμο πάνω από το $\mathbb{F}_p$. Πράγματι, κάθε $\alpha \in E$ είναι ρίζα του $f = X^{p^n} - X$. Η παράγωγος $f' = p^n X^{p^{n-1}} - 1 = -1$, άρα τα f, f' δεν έχουν κοινό μη σταθερό κοινό διαιρέτη. Έπεται (Πρόταση 3.17) ότι το πολυώνυμο f δεν έχει πολλαπλή ρίζα. Το $\mathrm{Irr}(\alpha, \mathbb{F}_p)$ διαιρεί το f, άρα το $\mathrm{Irr}(\alpha, \mathbb{F}_p)$ δεν έχει πολλαπλή ρίζα, συνεπώς το α είναι διαχωρίσιμο πάνω από το $\mathbb{F}_p$.

Για την ομάδα Galois, παρατηρούμε αρχικά ότι ο σ αφήνει αναλλοίωτα όλα τα στοιχεία του $\mathbb{F}_p$ (μικρό Θεώρημα του Fermat), άρα $\langle\sigma\rangle \leq \mathcal{G}(E/\mathbb{F}_p)$. Για την ισότητα των ομάδων αρκεί να δείξομε την ισότητα των αντιστοίχων σταθεροποιητικών σωμάτων, δηλαδή, να δείξομε 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 τελευταίας ισότητας: Το αριστερό μέλος ισούται με το σύνολο $\{\alpha \in E : \alpha^p = \alpha\}$, δηλαδή με το σύνολο των ριζών του $X^p - X \in \mathbb{F}_p[X]$. Κάθε στοιχείο του $\mathbb{F}_p$ είναι ρίζα του πολυωνύμου αυτού, το οποίο είναι βαθμού p. Καθώς το $\mathbb{F}_p$ περιέχει p στοιχεία, συμπεραίνομε ότι το σύνολο των ριζών του $X^p - X$ είναι το $\mathbb{F}_p$. □

Πόρισμα 6.19. *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 6.18).

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:

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

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 6.14 (1), $\left[E : \mathbb{F}_p\right] = n$ και $\left[K : \mathbb{F}_p\right] = m$, άρα $n = [E : K]\left[K : \mathbb{F}_p\right] = [E : K]m$, που δείχνει ότι $m|n$.

Για την απόδειξη της ισότητας $\mathcal{G}(E/K) = \langle \sigma^m \rangle$ παρατηρούμε ότι, λόγω του Θεμελιώδους Θεωρήματος Galois (Θεώρημα 6.7) είναι $|\mathcal{G}(E/K)| = [E : K] = n/m$. Αφετέρου, η $\mathcal{G}(E/K)$ είναι υποομάδα της κυκλικής ομάδας $\langle \sigma \rangle$, άρα ταυτίζεται με τη μοναδική υποομάδα της $\langle \sigma \rangle$ η οποία έχει τάξη n/m[1]. Συνεπώς, αρκεί να δείξω ότι, στην ομάδα $\langle \sigma \rangle$, η τάξη του σ^m είναι n/m. Πράγματι, από το Θεώρημα 6.7 (2) είναι $\text{ord}(\sigma) = |\langle \sigma \rangle| = |\mathcal{G}\left(E/\mathbb{F}_p\right)| = \left[E : \mathbb{F}_p\right] = n$ και από τη Στοιχειώδη Θεωρία Ομάδων,

$$\text{ord}(\sigma^m) = \frac{\text{ord}(\sigma)}{\text{ΜΚΔ}(\text{ord}(\sigma), m)} = \frac{n}{\text{ΜΚΔ}(n, m)} = \frac{n}{m},$$

όπου η τελευταία ισότητα ισχύει γιατί $m|n$. □

Θεώρημα 6.20. *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 $m \mid n$.*

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 6.14, τα E, K είναι σώματα διάσπασης των αντιστοίχων πολυωνύμων, $|E| = p^n$ 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 6.19 και συμπεραίνω ότι $m|n$.

Αντιστρόφως, έστω $m|n$. Πρέπει και αρκεί να δειξω 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 $a^{p^{m(\nu+1)}} = (a^{p^m \nu})^{p^m} = a^{p^m} = a$. □

Πρακτική κατασκευή πεπερασμένων σωμάτων. Θέλω να κατασκευάσω $\text{GF}(p^n)$ για συγκεκριμμένο 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 $1, \alpha, \ldots, \alpha^{n-1}$ είναι βάση για την επέκταση $\mathbb{F}_p(\alpha)/\mathbb{F}_p$. Άρα

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

Άρα $\left|\mathbb{F}_p(\alpha)\right| = p^n$. Από το γεγονός ότι όλα τα πεπερασμενα σώματα που έχουν το ίδιο πλήθος στοιχείων είναι ισόμορφα (Πόρισμα 6.16) έπεται ότι διαφορετικές επιλογές f δίνουν διαφορετικά ενδεχομένως σώματα, τα οποία όμως είναι ισόμορφα.

[1] Είναι γνωστό από τη Στοιχεώδη Θεωρία Ομάδων ότι, αν η πεπερασμένη κυκλική ομάδα G είναι τάξεως n, τότε σε κάθε θετικό διαιρέτη d του n αντιστοιχεί ακριβώς μία υποομάδα της G τάξεως d.

Παράδειγμα 6.21. Κατασκευή του 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,

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

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

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

Ασκήσεις Σε όλες τις παρακάτω ασκήσεις η σχέση $\leq$ δηλώνει υπόσωμα υπό στενή έννοια, δηλαδή, το αριστερό μέλος είναι και υποσύνολο του δεξιού.

Άσκηση 6.22. Έστω πρώτος p, C αλγεβρική κλειστότητα του $\mathbb{F}_p$ και E_1, E_2 πεπερασμένα υποσώματα του C με $|E_1| = p^m$, $|E_2| = p^n$ και $m|n$. Δείξτε ότι $E_1 \leq E_2$.

Άσκηση 6.23. Έστω πρώτος p και $q = p^r$ με $r \geq 1$. Έστω C αλγεβρική κλειστότητα του $\mathbb{F}_p$ και $K \leq C$ με $|K| = q$. Δείξτε ότι το $\mathbb{F}_{q^n}$ (θεωρούμενο ως υπόσωμα του C) είναι σώμα διάσπασης του $X^{q^n} - X$ πάνω από το K.

Άσκηση 6.24. Έστω πρώτος p και $q = p^r$ με $r \geq 1$. Έστω C αλγεβρική κλειστότητα του $\mathbb{F}_p$ και $K \leq C$ με $|K| = q$. Έστω, επίσης, $n \in \mathbb{N}$ και $E \leq C$. Δείξτε ότι το E είναι επέκταση του K βαθμού n αν και μόνο αν το E είναι σώμα διάσπασης του $X^{q^n} - X$ πάνω από το K.

Άσκηση 6.25. Έστω πρώτος p και q δύναμη του p. Έστω C αλγεβρική κλειστότητα του $\mathbb{F}_p$, F υπόσωμα του C με $|F| = q$ και $E, K \leq C$ επεκτάσεις του F με $[E:F] = n$ και $[K:F] = m$. Δείξτε ότι $K \leq E \Leftrightarrow m|n$.

Άσκηση 6.26. 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 6.27. 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 $n = p = 2$. Ακολουθήστε τα παρακάτω βήματα (δεκτός οποιοσδήποτε διαφορετικός, σωστός τρόπος απόδειξης).
Έστω C μια αλγεβρική κλειστότητα του $\mathbb{F}_p$ και $\alpha \in C$ μια ρίζα του f. Στα παρακάτω ερωτήματα όλα τα πεπερασμένα σώματα νοούνται ως υποσύνολα του C.
(1) Αποδείξτε ότι το $\mathbb{F}_p(\alpha)$ περιέχει όλες τις ρίζες του f.
(2) Αποδείξτε ότι, για κάθε $b \in \mathbb{F}_{p^n}$, 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 $i \in \{0, 1, \ldots, n\}$.
(4) Αποδείξτε ότι η $\mathcal{G}\left(\mathbb{F}_p(\alpha)/\mathbb{F}_{p^n}\right)$ 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 $\left[\mathbb{F}_p(\alpha) : \mathbb{F}_{p^n}\right] = p$.
(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 (επιχειρηματολογώντας, όχι με ένα απλό «άρα») ότι ή $n = 1$, ή $n = 2 = p$.

Κεφάλαιο 7

7.1 7η Εβδομάδα

Κυκλοτομικά σώματα

Ορισμός 7.1. 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 7.2. 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 ομάδα 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 τών 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 $\mathrm{ord}(\omega) \mid n$ άρα είναι $\leq n$.

Δεν μπορώ να είμαι σίγουρος ότι $\mathrm{ord}(\omega) = n$. π.χ. αν $\mathrm{char}(F) = p$ και $n = pm$ τότε $0 = 1 - \omega^n = 1 - \omega^{pm} = (1 - \omega^m)^p$ που σημαίνει ότι $\mathrm{ord}(\omega) \leq m < n$. 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, $\mathrm{ord}\,\omega = n$.

Ορισμός 7.3. Το $\omega \in E$ λέγεται πρωταρχική n-οστή ρίζα της μονάδας (δηλαδή, του 1_E) αν, ως στοιχείο της ομάδας E^* έχει τάξη n ($\mathrm{ord}\,(\omega) = n$), 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:

- $\mathrm{char}\, F = 0$. (*)
- Όταν $\mathrm{char}\, F = p$ 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 3.17.

[1] Έστω 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 $\mathrm{lcm}(m, n)$, για να καταλήξουμε ότι υπάρχει στοιχείο τάξης r και συνεπώς ότι η G είναι κυκλική.

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

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

Αυτό συμβαίνει αν και μόνο αν $n = \text{ord}(\omega^k) = \dfrac{\text{ord}(\omega)}{\gcd(\text{ord}(\omega), k)} = \dfrac{n}{\gcd(n,k)}$, 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

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

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

Πρόταση 7.4. *Έστω ότι το F ικανοποιεί μια από τις συνθήκες (*) ή (**) και E είναι το n-οστό κυκλοτομικό 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 $\phi(n)$.*

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 4.1). Η ίδια επέκταση είναι και κανονική, αφού το E είναι σώμα διάσπασης του Φ_n πάνω από το F (Θεώρημα 4.14), άρα, τελικά, η E/F είναι Galois.

Ο μονομορφισμός ομάδων ψ, που ορίσθηκε πριν από την εκφώνηση της πρότασης έχει ως άμεση συνέπεια ότι $\mathcal{G}(E/F) \cong \psi(\mathcal{G}(E/F))$. 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 $\phi(n)$. □

Ορισμός 7.5. Έστω ω πρωταρχική n-οστή ρίζα του 1 (πάνω από το F). Ορίζομε το πολυώνυμο

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

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] Πριν προχωρήσομε στην απόδειξη της επόμενης πρότασης, κάνομε την εξής πολύ απλή, αλλά χρήσιμη παρατήρηση:

Παρατήρηση 7.6. Έστω σώμα F και τα μη σταθερά μονικά πολυώνυμα $f, g \in F[X]$ έχουν μόνο απλές ρίζες (σε κάποια αλγεβρική κλειστότητα του F). Άν τα σύνολα των ριζών τους είναι ίσα, τότε $f = g$.

Πρόταση 7.7. $\Phi_n = \prod_{d|n} \Psi_d$

[2] Το 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 βλέπομε το F ως επέκταση του $\mathbb{Q}$, στην πρώτη περίπτωση και του $\mathbb{F}_p$ στη δεύτερη περίπτωση.

Απόδειξη. Έστω U_n η πολλαπλασιστική ομάδα των ριζών του Φ_n. Παρατηρούμε τα εξής: Για κάθε διαιρέτη d του n, οι ρίζες του Ψ_d ανήκουν στο U_n (αν $\zeta^d = 1$ τότε και $\zeta^n = 1$). Κάθε Ψ_d έχει κοινή ρίζα με το Φ_n και, καθώς είναι ανάγωγο, έπεται ότι διαιρεί το Φ_n· ειδικότερα, το Ψ_d δεν έχει πολλαπλές ρίζες. 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. Συμπέρασμα: το πολυώνυμο του δεξιού μέλους της εκφώνησης δεν έχει πολλαπλές ρίζες και κάθε ρίζα του είναι και ρίζα του Φ_n. Αντιστρόφως, έστω ζ ρίζα του Φ_n και έστω $\operatorname{ord}(\zeta) = d$. Από τη στοιχειώδη Θ. Ομάδων, $d|n$ και, φυσικά, $\zeta^d = 1$, άρα η ζ είναι ρίζα του Ψ_d, άρα ρίζα του πολυωνύμου του δεξιού μέλους.

Τα παραπάνω, σε συνδυασμό με την Παρατήρηση 7.6, μας οδηγούν στο συμπέρασμα ότι τα δύο πολυώνυμα της εκφώνησης είναι ίσα. □

Παράδειγμα 7.8. 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 $1^{\text{η}}$ ρίζα του 1 είναι το 1, άρα $\Psi_1 = X-1$ και μοναδική πρωταρχική $2^{\text{η}}$ ρίζα του 1 (όταν $\operatorname{char} F \neq 2$) είναι το -1, άρα $\Psi_2 = X+1$. Όταν $\operatorname{char} F \neq 3$, τότε, από την Πρόταση 7.7, $\Phi_3 = \Psi_1\Psi_3$, άρα

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

Όταν $\operatorname{char} F \neq 2$, τότε, από την Πρόταση 7.7, $\Phi_4 = \Psi_1\Psi_2\Psi_4$, άρα

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

Όταν $\operatorname{char} F \neq 2, 3$, τότε, από την Πρόταση 7.7, $\Phi_6 = \Psi_1\Psi_2\Psi_3\Psi_6$, άρα

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

Λήμμα 7.9. *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 $h \in \mathbb{Z}[X]$. □

Πρόταση 7.10. $\Psi_n \in \mathbb{P}[X]$. *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 7.7,

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

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 7.9 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 $\Psi_n \in \mathbb{Z}[X]$. □

Σύμφωνα με την Πρόταση 7.10, το Ψ_n είναι μονικό πολυώνυμο του $\mathbb{Z}[X]$. Θα αποδείξομε ότι, επιπλέον, είναι και ανάγωγο πάνω από το $\mathbb{Q}$. Θα χρειασθούμε τα εξής (δίχως απόδειξη).

Λήμμα 7.11 (Παραλλαγή του «Λήμματος του Gauss»). *Αν τα $f, g \in \mathbb{Q}[X]$ είναι μονικά και $fg \in \mathbb{Z}[X]$, τότε $f, g \in \mathbb{Z}[X]$.*

Λήμμα 7.12 (Αναγωγή mod p). *Έστω p πρώτος. Για κάθε $a \in \mathbb{Z}$ συμβολίζω με $\overline{a}$ την κλάση $a \bmod p$. Η απεικόνιση*

$$\mathbb{Z}[X] \ni a_n X^n + \cdots + a_1 X + a_0 \mapsto \overline{a_n} X^n + \cdots + \overline{a_1} X + \overline{a_0} \in \mathbb{F}_p[X]$$

είναι ομορφισμός δακτυλίων $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ και λέγεται «αναγωγή mod p».
Επίσης, ισχύει $\overline{f(X^p)} = \overline{f(X)^p} = \overline{f(X)}^p$.

Θεώρημα 7.13. *Για κάθε $n \in \mathbb{N}$, το Ψ_n είναι ανάγωγο πάνω από το $\mathbb{Q}$.*

Απόδειξη. Έστω ω πρωταρχική n-οστή ρίζα της μονάδος, $\Phi_n(X) = X^n - 1$ και $f = \mathrm{Irr}\,(\omega, \mathbb{Q})$ (το f, εξ ορισμού, είναι μονικό). Στόχος να δείξω ότι $f = \Psi_n$. Το ω είναι κοινή ρίζα των Φ_n και f και το f είναι ανάγωγο, άρα $f \mid \Phi_n$. Συνεπώς, $\Phi_n = fg$ για κάποιο $g \in \mathbb{Q}[X]$. Τα Φ_n και f είναι μονικά, άρα και το g είναι μονικό. Από το Λήμμα 7.11 έπεται ότι $f, g \in \mathbb{Z}[X]$. Θα δείξω τα εξής:

(1) Για κάθε πρώτο p που δεν διαιρεί το n ισχύει $f(\omega^p) = 0$. (Η απόδειξη στο τέλος.)

(2) Για κάθε k πρώτο προς τον n ισχύει $f(\omega^k) = 0$.

Η απόδειξη του (2) βασίζεται στο (1): Έστω $k = p_1 \cdots p_r$ η ανάλυση του k σε πρώτους (δεν είναι, κατ' ανάγκη διαφορετικοί). Είναι $(p_i, n) = 1$ για κάθε $i = 1, \ldots, r$. Από το (1) έπεται ότι $f(\omega^{p_1}) = 0$. Το $\omega_1 := \omega^{p_1}$ είναι πρωταρχική n-οστή ρίζα της μονάδας, άρα, από το (1), $f(\omega_1^{p_2}) = 0$, δηλαδή, $f(\omega^{p_1 p_2}) = 0$. Το $\omega_2 := \omega^{p_1 p_2}$ είναι πρωταρχική n-οστή ρίζα της μονάδας, άρα, $f(\omega_2^{p_3}) = 0$, δηλαδή, $f(\omega^{p_1 p_2 p_3}) = 0$ κλπ, μέχρι να καταλήξω στη σχέση $f(\omega^k) = 0$.

Βασισμένος στο (2) θα αποδείξω ότι $\Psi_n = f$. Τα Ψ_n και f έχουν κοινή ρίζα την ω και το f είναι ανάγωγο, άρα $f \mid \Psi_n$. Αντίστροφως, κάθε ρίζα του Ψ_n είναι της μορφής ω^k με $1 \le k < n$ και $(k, n) = 1$ και είναι απλή. Λόγω του (2), $f(\omega^k) = 0$, άρα, $\Psi_n \mid f$. Τα Ψ_n και f είναι μονικά, άρα, $\Psi_n = f$.

Απόδειξη του (1). Είναι $\Phi_n = fg$ με τα $f, g \in \mathbb{Z}[X]$ μονικά (όπως είδαμε στην αρχή της απόδειξης), άρα $0 = \Phi_n(\omega^p) = f(\omega^p) g(\omega^p)$. Έστω $f(\omega^p) \neq 0$ (πάω σε άτοπο). Τότε $g(\omega^p) = 0$. Δηλαδή, το πολυώνυμο $g(X^p) \in \mathbb{Z}[X]$ έχει ρίζα το ω, άρα $f(X) \mid g(X^p)$. Έστω $g(X^p) = f(x)h(X)$. Από το Λήμμα 7.9, $h \in \mathbb{Z}[X]$. Στην τελευταία ισότητα πολυωνύμων εφαρμόζω την αναγωγή mod p (Λήμμα 7.12), οπότε $\overline{g(X)}^p = \overline{f(X)} \cdot \overline{h(X)}$, δηλαδή, στον δακτύλιο $\mathbb{F}_p[X]$, $\overline{g}^p = \overline{f} \cdot \overline{h}$. Έστω $\overline{q} \in \mathbb{F}_p$ ανάγωγος παράγων του $\overline{f}$ (το ότι το f είναι ανάγωγο πάνω από το $\mathbb{Q}$ δεν συνεπάγεται ότι και το $\overline{f}$ είναι ανάγωγο στο $\mathbb{F}_p$). Το $\overline{q}$ διαιρεί το $\overline{g}^p$ άρα $\overline{q} \mid \overline{g}$. Αυτό συνεπάγεται ότι τα $\overline{g}$ και $\overline{f}$ έχουν κοινή ρίζα (σε κάποια επέκταση του $\mathbb{F}_p$). Αλλά $\overline{\Phi}_n = \overline{f} \cdot \overline{g}$, άρα, λόγω του τελευταίου συμπεράσματος, το $\overline{\Phi}_n \in \mathbb{F}_p[X]$ έχει ρίζα πολλαπλότητας > 1, κάτι που αποκλείεται από το Πόρισμα 3.18 (2). □

Πόρισμα 7.14. *Αν E_n είναι το n-οστό κυκλοτομικό σώμα πάνω από το $\mathbb{Q}$, τότε $\mathcal{G}\,(E_n/\mathbb{Q}) \cong \mathbb{Z}_n^*$.*

Απόδειξη. Έστω ω πρωταρχική n-οστή ρίζα του 1 πάνω από το $\mathbb{Q}$, οπότε $E_n = \mathbb{Q}(\omega)$. Το ω είναι ρίζα του $\Psi_n \in \mathbb{Q}[X]$, το οποίο είναι ανάγωγο σύμφωνα με το Θεώρημα 7.13. Άρα $\mathrm{Irr}\,(\omega, \mathbb{Q}) = \Psi_n$ και, συνεπώς, $|\mathcal{G}\,(E_n/\mathbb{Q})| = [E_n : \mathbb{Q}] = \deg \Psi_n = \phi(n) = |\mathbb{Z}_n^*|$. Από την Πρόταση 7.4, η $\mathcal{G}\,(E_n/\mathbb{Q})$ είναι ισόμορφη με υποομάδα της $\mathbb{Z}_n^*$ και, στην περίπτωσή μας, οι δύο ομάδες έχουν την ίδια τάξη ($= \phi(n)$), άρα οι ομάδες είναι ισόμορφες. □

Ασκήσεις

Άσκηση 7.15. (1) Σε σώμα F χαρακτηριστικής $\neq 3, 5$ υπολογίστε το Ψ_{15} εκτελώντας μόνο μία ευκλείδεια διαίρεση.
(2) Σε σώμα F χαρακτηριστικής $\neq 2$ υπολογίστε το Ψ_{16} δίχως να εκτελέσετε καμμία ευκλείδεια διαίρεση.

Άσκηση 7.16. Έστω E_n το n-οστό κυκλοτομικό πολυώνυμο πάνω από το $\mathbb{Q}$. Για τις απαντήσεις στα ερωτήματα που ακολουθούν, σημαντικό ρόλο παίζει το Πόρισμα 7.14, καθώς και ο ορισμός του μονομορφισμού ψ, ο οποίος ορίσθηκε αμέσως πριν την εκφώνηση της Πρότασης 7.4.

(i) Προσδιορίστε με ποια ομάδα είναι ισόμορφη η $\mathcal{G}(E_5/\mathbb{Q})$ και διαπιστώστε ότι είναι κυκλική. Έστω $\mathcal{G}(E_5/\mathbb{Q}) = \langle\sigma\rangle$ και ω πρωταρχική 5^{η} ρίζα της μονάδας. Ποια είναι η τιμή του $\sigma(\omega)$; Διαπιστώστε ότι υπάρχει μία μόνο γνήσια υποομάδα H της $\mathcal{G}(E_5/\mathbb{Q})$ διαφορετική από την $\langle id\rangle$ και υπολογίστε το σταθεροποιούμενο σώμα της K. Η απάντησή σας θα είναι της μορφής $K = \mathbb{Q}(\sqrt{d})$.

(ii) Δείξτε ότι η $\mathcal{G}(E_8/\mathbb{Q})$ είναι ισόμορφη με την V_4 (ομάδα Klein). Έστω $\mathcal{G}(E_8/\mathbb{Q}) = \langle\sigma,\tau\rangle$ και ω πρωταρχική 8^{η} ρίζα της μονάδας. Ποια είναι η τιμή των $\sigma(\omega)$ και $\tau(\omega)$; Διαπιστώστε ότι υπάρχουν ακριβώς τρεις γνήσιες υποομάδες της $\mathcal{G}(E_8/\mathbb{Q})$ διαφορετικές από την $\langle id\rangle$ και υπολογίστε τα αντίστοιχα σταθεροποιούμενα σώματά τους. Και τα τρία θα είναι της μορφής $\mathbb{Q}(\sqrt{d})$.

(iii) Προσδιορίστε με ποια ομάδα είναι ισόμορφη η $\mathcal{G}(E_7/\mathbb{Q})$ και διαπιστώστε ότι είναι κυκλική. Έστω ω πρωταρχική 7^{η} ρίζα της μονάδας. Προσδιορίστε τον ελάχιστο θετικό ακέραιο k για τον οποίο ο $\sigma \in \mathcal{G}(E_7/\mathbb{Q})$ που ορίζεται από τη σχέση $\sigma(\omega) = \omega^k$ παράγει την ομάδα $\mathcal{G}(E_7/\mathbb{Q})$. Εξηγήστε γιατί υπάρχουν ακριβώς δύο γνήσιες υποομάδες της $\mathcal{G}(E_7/\mathbb{Q})$ διαφορετικές από την $\langle id\rangle$. Συμβολίστε τις με H_1, H_2, όπου H_1 είναι αυτή με τη μεγαλύτερη τάξη και με K_1, K_2 τα αντίστοιχα σταθεροποιούμενα σώματα. Γιατί οι επεκτάσεις $K_i/\mathbb{Q}$, $i = 1, 2$, είναι Galois;

(iii.1) Δείξτε ότι το $\zeta := \omega^4 + \omega^2 + \omega$ ανήκει στο K_1. Υπολογίστε το ζ^2 και βάσει αυτού του υπολογισμού σας βρείτε το $\mathrm{Irr}(\zeta, \mathbb{Q})$. Δίχως να χρησιμοποιήσετε αυτές τις ιδιότητες του ζ, αλλά εργαζόμενοι αποκλειστικά όπως στο Παράδειγμα 6.9, εκφράστε συναρτήσει του ζ τη μορφή των στοιχείων του K_1 και εκφράστε το K_1 απλά, με χρήση ριζικού (δίχως να εμφανίζεται το ω).

(iii.2) Δείξτε ότι το $\xi := \omega + \omega^{-1}$ ανήκει στο K_2. Υπολογίστε το $\xi^2 + \xi^3$ και βάσει αυτού του υπολογισμού σας βρείτε το $\mathrm{Irr}(\xi, \mathbb{Q})$. Δίχως να χρησιμοποιήσετε αυτές τις ιδιότητες του ξ, αλλά εργαζόμενοι αποκλειστικά όπως στο Παράδειγμα 6.9, εκφράστε συναρτήσει του ξ τη μορφή των στοιχείων του K_2. Ποιο είναι το σώμα K_2;

Διακρίνουσα Πολυωνύμου

Ορισμός 7.17. Θεωρώ $f \in F[X]$ με $\deg(f) = n$ και $\alpha_1, \dots, \alpha_n$ ρίζες του f σε κάποια αλγεβρική κλειστότητα του F. Ορίζω

$$\Delta(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)$$

και $\mathrm{D}(f) = \Delta(f)^2$. Το $\mathrm{D}(f)$ ορίζεται ως η διακρίνουσα του f.

Παρατήρηση 7.18 (Προφανής)**.** $\mathrm{D}(f) = 0 \iff f$ έχει τουλάχιστον μία ρίζα πολλαπλότητας > 1.

Ορισμός 7.19. Υποθέτω στο εξής ότι οι ρίζες του f είναι διαφορετικές και το $E = F(\alpha_1, \dots, \alpha_n)$ είναι σώμα διάσπασης του f (πάνω από το F), οπότε η E/F είναι Galois. Όταν λέμε «ομάδα Galois του f» εννοούμε την $\mathcal{G}(E/F)$.

Υπενθύμιση: Η ομάδα S_n δρα «φυσιολογικά» σε κάθε σύνολο με πληθάριθμο n. Αν

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \tag{7.1}$$

και $X = \{x_1, x_2, \dots, x_n\}$, τότε η δράση της σ στο X έχει ως αποτέλεσμα το $X^{\sigma} := \{x_{i_1}, x_{i_2}, \dots, x_{i_n}\}$, οπότε η δράση της σ σε κάθε παράσταση $h(x_1, x_2, \dots, x_n) \in F(x_1, x_2, \dots, x_n)$ έχει ως αποτέλεσμα την $h^{\sigma} := f(x_{i_1}, x_{i_2}, \dots, x_{i_n})$. Λέμε ότι μία υποομάδα H της S_n είναι *μεταβατική* αν για κάθε ζεύγος (i, j) με $i, j \in \{1, 2, \dots, n\}$ υπάρχει $\sigma \in H$, τέτοιο ώστε $\sigma(i) = j$.

Παρατήρηση 7.20 (Πολύ σημαντική!)**.** Έστω τώρα $\sigma \in \mathcal{G}(E/F)$. Τότε ο σ στέλνει κάθε ρίζα του f σε ρίζα του f και διαφορετικές ρίζες τις στέλνει σε διαφορετικές ρίζες. Έστω, λοιπόν,

$$\sigma(\alpha_1) = \alpha_{i_1},\ \sigma(\alpha_2) = \alpha_{i_2}, \dots, \sigma(\alpha_n) = \alpha_{i_n}.$$

Έτσι είναι «νόμιμο» να ταυτίζομε τον σ με τη μετάθεση (χρησιμοποιούμε το ίδιο γράμμα) (7.1) διότι, γνωρίζοντας τη μετάθεση (7.1) ξέρομε τη δράση του F-αυτομορφισμού σ σε καθένα από τα α_i και, συνεπώς, σε κάθε στοιχείο του $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$. Έτσι, μέσω αυτής της ταύτισης η $\mathcal{G}(E/F)$ θεωρείται ως υποομάδα της S_n.

Ορισμός 7.21. Αν $\sigma \in S_n$ και έχω μία παράσταση της μορφής $\Delta = \prod_{1 \le i < j \le n}(x_i - x_j)$, τότε, σύμφωνα με τα παράπάνω, η δράση της σ στη Δ είναι

$$\Delta^\sigma = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Αποδεικνύεται (στη Στοιχειώδη Άλγεβρα) ότι, αν η σ είναι αντιμετάθεση, δηλαδή της μορφής (i, j), τότε $\Delta^\sigma = -\Delta$, άρα γενικά

$$\Delta^\sigma = \begin{cases} \Delta & \text{αν η } \sigma \text{ είναι άρτια} \\ -\Delta & \text{αν η } \sigma \text{ είναι περιττή.} \end{cases} \tag{7.2}$$

Παρατήρηση 7.22 (επί του συμβολισμού)**.** Έστω $\delta = h(\alpha_1, \alpha_2, \dots, \alpha_n) \in E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ και $\sigma \in \mathcal{G}(E/F)$. Αν βλέπω το δ ως στοιχείο του E, δίχως αναφορά στα α_i, τότε, για τη δράση του σ στο δ προτιμώ τον συμβολισμό $\sigma(\delta)$. Αν, όμως, βλέπω το δ ως συγκεκριμένη έκφραση των α_i, τότε, είναι προτιμότερο να θεωρώ τον σ ως μετάθεση (στοιχείο της S_n) και για τη δράση του σ στο δ προτιμώ τον συμβολισμό δ^σ. Με τον πρώτο συμβολισμό,

$$\sigma(\delta) = \sigma(h(\alpha_1, \alpha_2, \dots, \alpha_n) = h(\sigma(\alpha_1), \sigma(\alpha_2), \dots, \sigma(\alpha_n)), \tag{7.3}$$

ενώ, με τον δεύτερο συμβολισμό,

$$\delta^\sigma = h(\alpha_1, \alpha_2, \dots, \alpha_n)^\sigma = h(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \dots, \alpha_{\sigma(n)}). \tag{7.4}$$

Οι δύο παραπάνω εκφράσεις είναι ίσες. Διότι, αν $\sigma(\alpha_1) = \alpha_{i_1}, \sigma(\alpha_2) = \alpha_{i_2}, \dots, \sigma(\alpha_n) = \alpha_{i_n}$, τότε, από την (7.3), $\sigma(\delta) = h(\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_n})$. Αφετέρου, ο σ ταυτίζεται με τη μετάθεση (7.1), σύμφωνα με όσα είπαμε πριν. Άρα, από την (7.4), $\delta^\sigma = h(\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_n})$.

Στα παρακάτω, G θα συμβολίζει την ομάδα Galois του f, δηλαδή, $G = \mathcal{G}(E/F)$.

Πρόταση 7.23.

1. $\sigma(\Delta(f)) = \prod_{1 \le i < j \le n}(\sigma(\alpha_i) - \sigma(\alpha_j)) = \begin{cases} \Delta(f), & \text{αν η } \sigma \text{ ταυτίζεται με άρτια μετάθεση} \\ -\Delta(f), & \text{αν η } \sigma \text{ ταυτίζεται με περιττή μετάθεση} \end{cases}$
2. $\mathrm{D}(f) \in F$.

Απόδειξη. (1) Άμεση συνέπεια της (7.2).
(2) $\sigma(\mathrm{D}(f)) = \sigma(\Delta(f)^2) = \sigma(\Delta(f))^2 = (\pm\Delta(f))^2 = \Delta(f)^2 = \mathrm{D}(f)$ για κάθε $\sigma \in G$, άρα $\mathrm{D}(f) \in \mathcal{F}(G) = F$. □

Πρόταση 7.24 (Θεωρώντας τη G υποομάδα της S_n)**.** *$G \le A_n$ αν και μόνο αν η διακρίνουσα $\mathrm{D}(f)$ είναι τετράγωνο κάποιου στοιχείου του F (συμβολικά $\mathrm{D}(f) \in F^2$).*[3]

[3] A_n είναι η υποομάδα αρτίων μεταθέσεων της S_n και τάξη της είναι $\frac{1}{2}n!$.

Απόδειξη. Αν $G \leq A_n$, τότε, από την Πρόταση 7.23, $\sigma(\Delta(f)) = \Delta(f), \forall \sigma \in G$. Άρα $\Delta(f) \in \mathcal{F}(G) = F$ και $\mathrm{D}(f) = \Delta(f)^2 \in F^2$.

Αντιστρόφως, έστω ότι $\mathrm{D}(f) = c^2$ για καποιο $c \in F$. Τότε $c^2 = \Delta(f)^2$ άρα $\Delta(f) = \pm c \in F$. Συνεπώς, για κάθε $\sigma \in G$, έχω $\sigma(\Delta(f)) = \Delta(f)$, άρα ο σ ταυτίζεται με άρτια μετάθεση. □

Παρατήρηση 7.25. Έστω ότι το f είναι ανάγωγο (υπενθυμίζεται ότι έχει ήδη υποτεθεί ότι οι ρίζες του f είναι διαφορετικές· βλ. Ορισμό 7.19). Αν $1 \leq i, j \leq n$, ξέρομε ότι υπάρχει F-ισομορφισμός από το $F(\alpha_i)$ στο $F\alpha_j$, που στελνει το α_i στο α_j και μπορεί να επεκταθεί σε $\sigma \in G$. Δηλαδή, διατυπωμένο με όρους μεταθέσεων $\forall i, j \in \{1, \dots, n\} \exists \sigma \in G : \sigma(\rho_i) = \rho_j$. Βλέποντας τη G σαν υποομάδα της S_n, το συμπέρασμα αυτό διατυπώνεται ως εξης: *Η G είναι μεταβατική υποομάδα της S_n.* (Βλ. τρεις γραμμές κάτω από τη (7.1).)

Παράδειγμα 7.26. Εφαρμογή στο κυβικό πολυώνυμο. Έστω σώμα F χαρακτηριστικής $\neq 3$ και ανάγωγο διαχωρίσιμο $g = X^3 + aX^2 + bX + c \in F[X]$. Το $f(X) := g(X - a/3)$ είναι της μορφής $f(X) = X^3 + pX + q \in F[X]$. Αν ρ_1, ρ_2, ρ_3 είναι οι ρίζες του g, τότε οι ρίζες του f είναι $\alpha_i := \rho_i + a/3$, άρα $\Delta(f) = \Delta(g)$. Επίσης, τα f, g έχουν την ίδια ομάδα Galois G γιατί $F(\rho_1, \rho_2, \rho_3) = F(\alpha_1, \alpha_2, \alpha_3)$. Συνεπώς, εστιάζομε τη μελέτη μας στο απλούστερης μορφής πολυώνυμο f. Υπολογίζεται ότι $\mathrm{D}(g) = -4p^3 - 27q^2$.

Η G είναι υποομάδα της $S_3 = \{id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$ τάξεως 6. Οι υποομάδες της είναι οι

$$\langle id \rangle, \langle (1,2) \rangle, \ \langle (1,3) \rangle, \ \langle (2,3) \rangle, \ A_3 = \langle (1,2,3) \rangle = \{id, (1,2,3), (1,3,2)\}.$$

Την απαίτηση της μεταβατικότητας ικανοποιούν μόνο η S_3 και η A_3. Άρα, βάσει της Παρατήρησης 7.25, $G \cong A_3$ ή $G \cong S_3$.

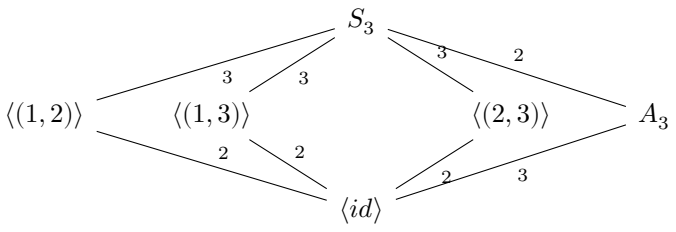
Έστω $G \cong A_3$. Η A_3 δεν έχει γνήσιες υποομάδες πλήν της $\langle id \rangle$, άρα δεν υπάρχει ενδιάμεση επέκταση μεταξύ των F και $E = F(\alpha_1, \alpha_2, \alpha_3)$. Αυτή η περίπτωση ισχύει αν και μόνο αν το $\mathrm{D}(f) \in F^2$ (Πρόταση 7.23). Επίσης, $[E : F] = |G| = 3$ άρα $E = F(\rho_1) = F(\rho_2) = F(\rho_3)$ αφού και $[F(\rho_i) : F] = \deg g = 3$. Άρα οι ρ_2, ρ_3 είναι πολυωνυμικές εκφράσεις του ρ_1 κλπ. Αριθμητικό παράδειγμα αυτής της περίπτωσης είδαμε στην άσκηση 2.17.

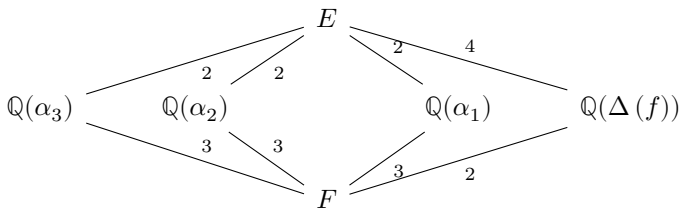
Έστω $G \cong S_3$. Τότε $[E : F] = |G| = 6$. Η G έχει ακριβώς τέσσερις γνήσιες υποομάδες πλήν της $\langle id \rangle$, άρα υπάρχουν ακριβώς τέσσερις γνήσιες ενδιάμεσες επεκτάσεις μεταξύ των F και E. Αυτές είναι τα σταθεροποιούμενα σώματα των $\langle (1,2) \rangle, \langle (1,3) \rangle, \langle (1,2) \rangle$ και A_3. Οι τρεις πρώτες είναι υποομάδες τάξης 2, άρα ο βαθμός της επέκτασης που αντιστοιχεί σε αυτές είναι βαθμού $6/2 = 3$.

Πιο συγκεκριμμένα, το $\mathcal{F}((1,2))$ είναι το $\mathbb{Q}(\alpha_3)$ η $\mathbb{Q}(\alpha_3)/\mathbb{Q}$ διότι αυτή ειναι βαθμού 3 και ο σ που αντιμεταθέτει τις α_1, α_2 αφήνει σταθερό το α_3. Αντίστοιχα, $\mathcal{F}((1,3)) = \mathbb{Q}(\alpha_2)$ και $\mathcal{F}((2,3)) = \mathbb{Q}(\alpha_1)$.

Μένει ο υπολογισμός του $K = \mathcal{F}(A_3)$. Για κάθε $\sigma \in A_3$ είναι $\sigma(\Delta(f)) = \Delta(f)$ (Πρόταση 7.23), άρα $\mathbb{Q}(\Delta(f)) \leq K$. Επίσης, $S_3 = G \not\leq A_3$, άρα, από την Πρόταση 7.24, $\Delta(f) \notin F$ και το $X^2 - \mathrm{D}(f)$ είναι ανάγωγο. Έπεται ότι η επέκταση $\mathbb{Q}(\Delta(f))/\mathbb{Q}$ είναι βαθμού 2, άρα $K = \mathbb{Q}(\Delta(f))$.

Έτσι, στην περίπτωση που $G \cong S_3$, καταλήγομε στα παρακάτω διαγράμματα υποομάδων και επεκτάσεων:





Στην περαιτέρω μελέτη των ομάδων Galois πολυωνύμων είναι χρήσιμο το εξής:

Λήμμα 7.27. *(i)* $S_n = \langle (1\,2), (1\,3), \dots, (1\,n) \rangle$

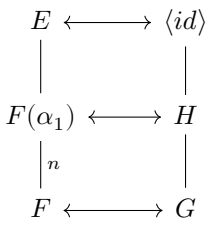
(ii) $S_n = \langle (1\,2), (2\,3), \dots, ((n-1)\,n) \rangle$

(iii) $S_n = \langle (1\,2), (1\,2\,3 \dots (n-1)\,n) \rangle$

(iv) $S_n = \langle (1\,2), (2\,3\ \dots\ (n-1)\,n) \rangle$

Λήμμα 7.28. *Έστω $f \in F[X]$ ανάγωγο, διαχωρίσιμο, βαθμού n και ομάδα Galois G . Τότε $n \mid |G|$. Επιπλέον, αν $n = p$ πρώτος, τότε η G (ως υποομάδα της S_n) περιέχει ένα p-κύκλο δηλαδή κάποιο $(i_1, \dots, i_p)$ με $i_1, \dots, i_p$ μετάθεση των $1, \dots, p$.*

Απόδειξη. Έστω $E = F(\alpha_1, \dots, \alpha_n)$ όπου $\alpha_1, \dots, \alpha_n$ ρίζες του f (διαφορετικές αφού το f είναι διαχωρίσιμο). Έχομε το παρακάτω διάγραμμα αντιστοιχίας Galois:



Η E/F είναι Galois ως σώμα διάσπασης του διαχωρίσιμου πολυωνύμου f πάνω από το f. Από το Θεμελιώδες Θεώρημα της Θεωρίας Galois 6.7, $n = [G : H]$. Είναι $|G| = |H|\,[G : H]$, άρα $n \mid |G|$.

Εξειδικεύω στην περίπτωση που $n = p$ πρωτος. Τότε έστω $|G| = p^r m$, όπου $r \geq 1$ και $p \nmid m$. Από το 1ο θεώρημα Sylow, υπάρχει υποομάδα P_i της G (p-ομάδα Sylow) τάξεως p^i για κάθε $i = 1, \dots, r$. Ειδικότερα $|P_1| = p$ άρα η P_1 είναι κυκλική τάξεως p, δηλαδη υπάρχει $sigma \in G$ τάξεως p οπότε οι $id, \sigma, \dots, \sigma^{p-1}$ είναι διαφορετικοί και $\sigma^p = id$. (Εναλλακτικά, το θεώρημα Cauchy για ομάδες λέει ότι αν η G είναι πεπερασμένη ομάδα και ο πρώτος p διαιρεί την τάξη $|G|$, τότε υπάρχει στοιχείο της G τάξεως p.)

Ο σ γράφεται σε γινόμενο ξένων κύκλων, έστω $\sigma = \kappa_1 \dots \kappa_2 \dots \kappa_m$ της S_p. Είναι $p = \mathrm{ord}\,(\sigma) = \mathrm{lcm}(\mathrm{ord}\,(\kappa_1), \dots \mathrm{ord}\,(\kappa_m))$. Άρα κάποιος κύκλος, έστω ο κ_1 έχει τάξη p. Αυτό, επίσης, σημαίνει ότι $\sigma = \kappa_1$, καθώς οι $\kappa_1, \dots, \kappa_m$ έχουν υποτεθεί ξένοι και αφού ο κ_1 έχει p στοιχεία, δεν υπάρχει ξένος προς αυτόν κύκλος. □

Πρόταση 7.29. *Έστω πρώτος $p \geq 3$, $f \in \mathbb{Q}(X)$ ανάγωγο, βαθμού p,[4] το οποίο έχει ένα ακριβώς ζεύγος συζυγών μιγαδικών ριζών και τις υπόλοιπες $p-2$ πραγματικές. Τότε η ομάδα Galois του f είναι ισόμορφη με την S_p.*

[4] Αφού είμαστε πάνω από το $\mathbb{Q}$, το f είναι διαχωρίσιμο.

Απόδειξη. Έστω ότι οι γνήσιες μιγαδικές ρίζες είναι $\alpha_1, \alpha_2 = \bar{\alpha_1}$ και οι πραγματικές οι $\alpha_3, \dots, \alpha_p$. Έχω τον $\mathbb{Q}$-αυτομορφισμό του $\mathbb{C}$ με $z \mapsto \bar{z}$. Περιορίζοντας αυτόν στο σώμα διάσπασης του f, έστω Ε παίρνω κάποιον $\tau \in G := \mathcal{G}(E/\mathbb{Q})$. Αν δω τον τ ως μετάθεση του S_p τότε αυτός είναι ο $(1,2)$. Από το Λήμμα 7.28 υπάρχει $\sigma \in G$ που είναι p-κύκλος. Αν αριθμήσω κατάλληλα τις πραγματικές ρίζες, τότε η G περιέχει τη μετάθεση $(1,2,\dots,p-1,p)$.[5] Καταλήγω στο συμπέρασμα ότι η G περιέχει τις μεταθέσεις $(1,2)$ και $(1,2,\dots,p-1,p)$, άρα, από το Λήμμα 7.27, $G \cong S_p$. □

Ασκήσεις

Άσκηση 7.30. Έστω $f = X^3 + aX + b \in F[X]$ και r_1, r_2, r_3 οι ρίζες του σε κάποιο σώμα διάσπασης του f πάνω από το F. Δείξτε ότι $(r_1 - r_2)^2 = (3b - ar_3)/r_3$. Ανάλογοι τύποι ισχύουν με κυκλική μετάθεση των r_1, r_2, r_3, οπότε, βασισμένοι σε αυτούς, αποδείξτε ότι

$$D(f) = -4a^3 - 27b^2.$$

Αναφερόμενοι στην άσκηση 7.16 (iii.2), υπολογίστε τη διακρίνουσα του $\mathrm{Irr}(\xi, \mathbb{Q})$ λαμβάνοντας υπόψη και την παρατήρηση στην αρχή του Παραδείγματος 7.26. Συμπεράνετε με τρόπο διαφορετικό από αυτόν της άσκησης 7.16 (iii) ότι η επέκταση $\mathbb{Q}(\xi)/\mathbb{Q}$ είναι Galois.

[5] Αυτό είναι εμφανές από το παρακάτω παράδειγμα. Έστω $p = 5$ και $\sigma = (1,3,4,2,5)$, τότε $\sigma^3 = (1,2,3,5,4)$. Οι $3,4,5$ αντιστοιχούν στις πραγματικές ρίζες οπότε αν αλλάξω την αρίθμηση των πραγματικών ριζών ($\alpha_4 \leftarrow a_5$ και $\alpha_5 \leftarrow a_4$) τότε ο σ ταυτίζεται με τον $(1,2,3,4,5)$.

Κεφάλαιο 8

8.1 $8^{η}$ Εβδομάδα

Επεκτάσεις κυκλικές και Kummer

Πρόταση 8.1. *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 $\lambda_1\sigma_1 + \cdots + \lambda_n\sigma_n = 0$ [1], τότε $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$.*

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 οποιουσδήποτε 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

$$\lambda_1\sigma_1 + \cdots + \lambda_n\sigma_n = 0 \tag{8.1}$$

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

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

$$\lambda_1\sigma_1(u) + \cdots + \lambda_{n-1}\sigma_{n-1}(u) + \lambda_n\sigma_n(u) = 0, \ \forall u \in K$$

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

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

Θέτοντας στην τελευταία ισότητα το αu στη θέση του u παίρνω και τη σχέση

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

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

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

Αυτή η σχέση λέει ότι

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

[1] Η μηδενική απεικόνιση $K \to K$.

[2] $\sigma_n(\alpha) = 0 \iff \alpha = 0 \iff \sigma_1(\alpha) = 0$.

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 (8.1), $\lambda_2\sigma_2+\cdots+\lambda_n\sigma_n = 0$. Λόγω της επαγωγικής υπόθεσης, η σχέση αυτή συνεπάγεται ότι $\lambda_i = 0$ για κάθε i. □

Κυκλικές επεκτάσεις

Ορισμός 8.2. Μια πεπερασμένη επέκταση E/F λέμε ότι είναι κυκλική αν και μόνο αν είναι Galois και η $\mathcal{G}(E/F)$ είναι κυκλική.

Θεώρημα 8.3. *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 έιναι Galois ως σώμα διάσπασης διαχωρίσιμου πολυωνύμου. Θεωρώ την εξής απεικόνιση ομάδων

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

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

Καθώς η ψ είναι μονομορφισμός, η $\mathcal{G}(E/F)$ είναι ισόμορφη με την εικόνα της μέσω του ψ, 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 θ, 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. □

Θεώρημα 8.4 (Αντίστροφο του Θεωρήματος 8.3)**.** *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 πολυωνύμου $f = X^n - \alpha$.*

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 $id, \sigma, \dots, \sigma^{n-1}$ είναι διαφορετικοί. Από την Πρόταση 8.1, αυτοί οι αυτομορφισμοί είναι γραμμικώς ανεξάρτητοι, άρα $\exists\beta \in E$ τέτοιο ώστε

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

Υπολογίζω $\sigma(\theta) = \sigma(\beta) + \omega\sigma^2(\beta) + \cdots + \omega^{n-2}\sigma^{n-1}(\beta) + \omega^{n-1}\beta$, 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 πολυώνυμο $f = X^n - \alpha \in F[X]$, το οποίο έχει ρίζα το θ.

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 τ είναι F-μονομορφισμός του $F(\theta)$. Η επέκταση $F(\theta)/F$ είναι Galois ως σώμα διάσπασης του διαχωρίσιμου f, άρα ο τ 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 $\text{ord}(\omega) = n$. □

Επεκτάσεις Kummer

Ορισμός 8.5. Μία πεπερασμένη επέκταση Galois, της οποίας η ομάδα Galois είναι αβελιανή ονομάζεται επέκταση Kummer

Θεώρημα 8.6. *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 $i \in 1, \dots, r$ και $j \in 0, \dots, n-1$ 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 k. 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,

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

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 $i = 1, \dots, r$. □

Υπενθύμιση 8.7. Έστω ότι $(G_i, \cdot)_{i=1,\dots,n}$ είναι αβελιανές ομάδες με ουδέτερα στοιχεία e_i. Το καρτεσιανό γινόμενο $G = \prod_{i=1}^n = G_1 \times G_2 \times \cdots \times G_n$, εφοδαδιασμένο με τον πολλαπλασιαμό 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 $H_i := G_1 \times \cdots \times G_{i-1} \times \{e_i\} \times G_{i+1} \times \cdots G_n$ της G ταυτίζεται με την $H_i \cong \prod_{j=1, j\neq i}^n G_j$ και $G/H_i \cong G_i$.

$1^η$ *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.

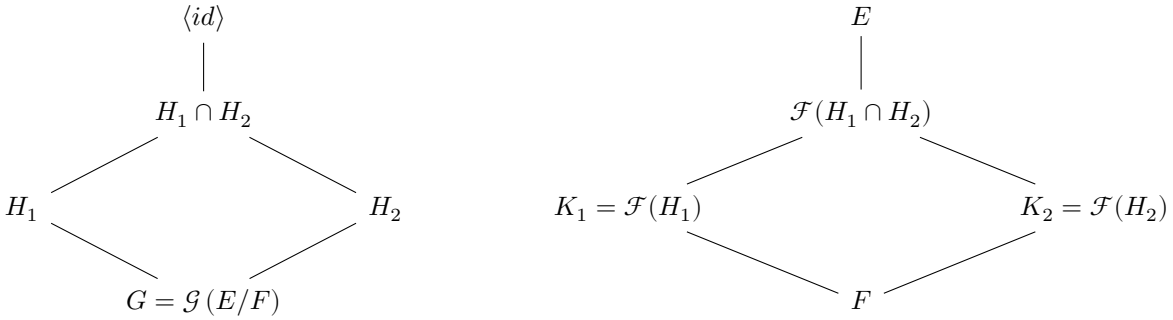
Το *Θεμελιώδες Θεώρημα των Πεπερασμένα Παραγόμενων Αβελιανών Ομάδων* λέει το εξής: Αν η G είναι (πεπερασμένα παραγόμενη) αβελιανή ομάδα, τότε $G \cong C_1 \times \cdots \times C_\mu \times \mathbb{Z}^\nu$, όπου C_i πεπερασμένη κυκλική ομάδα, δηλαδή αν $|C_i| = m_i$, $C_i \cong \mathbb{Z}_m$. Προφανώς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

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

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

Λήμμα 8.8. *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_1K_2, η λεγόμενη σύνθεση (compositum) των K_1K_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 $\mathcal{F}(H_1 \cap H_2) = K_1K_2$. Είναι $H_1 \cap H_2 \leq H_1$, άρα $\mathcal{F}(H_1 \cap H_2) \geq \mathcal{F}(H_i) = K_i$ για $i = 1, 2$. Συνεπώς, $\mathcal{F}(H_1 \cap H_2) \supseteq K_1 \cup K_2$ άρα και $\mathcal{F}(H_1 \cap H_2) \geq K_1K_2$.

Αντίστροφα, $K_i \leq K_1K_2$ για $i = 1, 2$ άρα $H_i = \mathcal{G}(E/K_i) \geq \mathcal{G}(E/K_1K_2)$ οπότε $H_1 \cap H_2 \geq \mathcal{G}(E/K_1K_2)$ άρα $\mathcal{F}(H_1 \cap H_2) \leq \mathcal{F}(\mathcal{G}(E/K_1K_2)) = K_1K_2$. □

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

Τώρα μπορούμε να αποδείξομε το (περίπου) αντίστροφο του Θεωρήματος 8.6.

Θεώρημα 8.9. *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 8.7, είναι $G/H_i \cong C_i$.

Επίσης, έστω $\mathcal{F}(H_i) := K_i$. Από το Θεμελιώδες Θεώρημα Galois 6.7 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 8.6, το K_i είναι σώμα διάσπασης του πολυωνύμου $X^{d_i} - \beta_i$ για κάποιο $\beta_i \in F$ και, μάλιστα, $K_i = F(\theta_i)$, όπου $\theta_i^{d_i} = \beta_i$.

Τώρα, από τη 2^{η} παρατήρηση της υπενθύμισης 8.7, η G έχει ένα στοιχείο, έστω τ, 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, $\theta_i^n = \left(\theta_i^{d_i}\right)^{n/d_i} = \beta_i^{n/d_i} = \alpha_i$, άρα το θ_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 $F(\theta_1, \dots, \theta_r) = K_1K_2 \dots K_r$. Από το Λήμμα 8.8, $\mathcal{G}(E/K_1 \cdots K_r) = H_1 \cap \cdots \cap H_r = \langle id_E \rangle$, όπου η τελευταία ισότητα ισχύει σύμφωνα με την 1^{η} παρατήρηση της υπενθύμισης 8.7. Άρα, $K_1 \cdots K_r = \mathcal{F}(\mathcal{G}(E/K_1 \cdots K_r)) = \mathcal{F}(\langle id_E \rangle) = E$, συνεπώς, $F(\theta_1, \dots, \theta_r) = K_1 \dots K_r = E$. □

Ριζικές επεκτάσεις

Ορισμός 8.10. 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 8.11. Αν αυτό συμβαίνει, τότε $\alpha_i^n \in F_{i-1}$ για $n = \text{lcm}(n_1, \dots, n_r)$. 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 8.12. 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 8.13. 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 8.14. *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 $\prod_{k=1}^{i} \text{Irr}\,(\alpha_k, F)$.
• 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 8.21 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 $\beta = \alpha_i', \alpha_i'', \dots$, 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 $\text{Irr}\,(\alpha_i, F)$ 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 8.12 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 8.15. 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 $i = 1, \dots, r$.

Ορισμός 8.16. 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 8.17. *Αν* $\text{char}(F) = 0$ *και το μη σταθερό $f \in F[X]$ είναι επιλύσιμο με ριζικά, τότε η ομάδα $\mathcal{G}\,(\text{K}/F)$ είναι επιλύσιμη.*

Απόδειξη. Έστω K σώμα διάσπασης του f πάνω από το F, 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 8.11), υπάρχει $n \in \mathbb{N}$ και αλυσίδα

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

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 $i = 0, 1, \dots, r$.

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 8.3, η επέκταση F_i/F_{i-1} είναι κυκλική. Η $N(\omega)/F$ είναι Galois, άρα και η $N(\omega)/F_{i-1}$ είναι Galois για $1 \leq i \leq r$ και έχω το εξής διάγραμμα αντιστοιχίας Galois:

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

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

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

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

Τώρα θεωρώ το διάγραμμα

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

Η K/F είναι Galois ως σώμα διάσπασης του f, άρα $\mathcal{G}\left(N(\omega)/K\right) \trianglelefteq \mathcal{G}\left(N(\omega)/F\right)$ και $\mathcal{G}\left(K/F\right) \cong \mathcal{G}\left(N(\omega)/F\right)/\mathcal{G}\left(N(\omega)/K\right)$. Άρα, η $\mathcal{G}\left(K/F\right)$ είναι πηλικοομάδα μιας επιλύσιμης ομάδας, οπότε, από την άσκηση 8.22 (2) είναι και αυτή επιλύσιμη. Αλλά επιλυσιμότητα της $\mathcal{G}\left(K/F\right)$ σημαίνει (Ορισμός 8.16) επιλυσιμότητα του f με ριζικά. □

Πρόταση 8.18. *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 7.29, ένα πολυώνυμο f όπως στην εκφώνηση έχει ομάδα Galois ισόμορφη με την S_p. Από την αμέσως παρακάτω Πρόταση 8.20, η S_p δεν είναι επιλύσιμη για $p \geq 5$, άρα, βάσει του Θεωρήματος 8.17, το f δεν είναι επιλύσιμο με ριζικά. □

Παράδειγμα 8.19. 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 8.18 είναι η εξής:

Πρόταση 8.20. *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 $i = 0, 1, \dots, r$, 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 $l, m \in \{1, \dots, n\} \setminus \{i, j, k\}$ 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 $(i, j, k) \in H_i$. □

Ασκήσεις

Άσκηση 8.21. 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 8.22. (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 $i = 1, \dots, n$. Θεωρήστε τις υποομάδες $f(G_i)$ $(i = 0, \dots, n)$ της H.

(2) Αν η G είναι επιλύσιμη ομάδα και $H \trianglelefteq G$ τότε και η G/H είναι επιλύσιμη.

Κεφάλαιο 9

9.1 9^{η} Εβδομάδα

Ριζικές επεκτάσεις (συνέχεια)

Θεώρημα 9.1 (Αντίστροφο του Θεωρήματος 8.17)**.** *Έστω* $\text{char}(F) = 0$ *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 $\text{char}(F) = 0$, 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 $i = 0, \ldots, r$, έστω $K_i = \mathcal{F}(H_i)$· 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

$$\begin{array}{ccc} K & \longleftarrow & H_r = \langle id \rangle \\ | & & | \\ K_i & \longleftarrow & H_i \\ | & & | \\ K_{i-1} & \longleftarrow & H_{i-1} \end{array}$$

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 $i = 0, \ldots, r$. Η F_i/F_{i-1} είναι Galois. Πράγματι, η 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 8.5). 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 8.9, 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 8.12 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 4.12). 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· 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 $\sigma = id_{F_i}$. □

Ασκήσεις

Άσκηση 9.2. (1) Γιατί κάθε αβελιανή ομάδα είναι επιλύσιμη;

(2) Αποδείξτε ότι η διεδρική ομάδα D_4 είναι επιλύσιμη.

Υπόδειξη. Δείτε το διάγραμμα υποομάδων του Παραδείγματος 6.9.

(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.

Ασκήσεις από προηγούμενη ύλη

Άσκηση 9.3. 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 9.4. 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 9.3). Υποθέτομε 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 ν' 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 9.5. Έστω σώμα F χαρακτηριστικής p, E/F κυκλική επέκταση (άρα Galois) βαθμού p και σ 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 $\tau : F(\theta) \to E$ είναι στοιχείο της $\mathcal{G}(F(\theta)/F)$ και $\mathrm{ord}(\tau) = p$. Βάσει αυτού αποδείξτε ότι $E = F(\theta)$.

(2) Αποδείξτε ότι το θ είναι ρίζα κάποιου πολυωνύμου $f = X^p - X - a \in F[X]$ και το f είναι ανάγωγο πάνω από το F.

Άσκηση 9.6. 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 παράγων 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 9.5 και 9.6 αποδεικνύει το εξής Θεώρημα: *Έστω σώμα F χαρακτηριστικής p. Η πεπερασμένη επέκταση E/F είναι κυκλική βαθμού p αν και μόνο αν το E είναι σώμα διάσπασης πάνω από το F ενός ανάγωγου πολυωνύμου της μορφής $f = X^p - X - a \in F[X]$. Όταν αυτή η συνθήκη ισχύει, τότε $E = F(\theta)$, όπου θ είναι ρίζα του f.*

Άσκηση 9.7. Η άσκηση αυτή δείχνει, μεταξύ άλλων, ότι στο Θεώρημα 8.3 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 9.3).

(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 $\mathrm{Irr}(\omega, F) = (X - \omega)(X - \omega^{-1})$ και $[E : L] = n$.[1] 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 $\mathrm{ord}(\sigma) = n$, $\mathrm{ord}(\tau) = 2$ 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 8.3, γιατί εκείνο το θεώρημα απαιτεί τη συνθήκη να περιέχει το F πρωταρχική n-οστή ρίζα της μονάδας, η οποία εδώ δεν ικανοποιείται.

Άσκηση 9.8. Η άσκηση αυτή δίνει ένα παράδειγμα στο οποίο όλες οι υποθέσεις της άσκησης 9.7 ικανοποιούνται, καθώς και οι υποθέσεις του ερωτήματος (3).

Έστω ω πρωταρχική 5^{η} 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^{η} ρίζα της μονάδας πλην του 1. Επίσης, δείξτε ότι $\mathrm{Irr}(\omega, F) = (X - \omega)(X - \omega^{-1}) = X^2 - \beta X + 1$.

(2) Δείξτε ότι $[E : \mathbb{Q}] = 20$ και $[E : L] = 5$. Από την άσκηση 9.7 συμπεράνετε ότι $\mathcal{G}(E/F) \cong D_5$.

Το τεταρτοβάθμιο πολυώνυμο

Έστω σώμα F με $\mathrm{char}(F) \neq 2$. Κάθε $X^4 + aX^3 + bX^2 + cX + d \in F[X]$ μπορεί να να μετασχηματισθεί σε πολυώνυμο της μορφής

$$f(X) = X^4 + qX^2 + rX + s, \quad q, r, s \in F, \tag{9.1}$$

[1] Στην άσκηση 9.8 θα δούμε παράδειγμα στο οποίο αυτές οι συνθήκες ικανοποιούνται.

δηλαδή, σε πολυώνυμο με μηδενικό συντελεστή στο X^3, μέσω της αντικατάστασης $X \leftarrow X - a/4$. Το f έχει το ίδιο σώμα διάσπασης και την ίδια διακρίνουσα με το αρχικό.

Σκοπός μας είναι να μελετήσομε την ομάδα Galois του f, *το οποίο υποθέτομε ανάγωγο.* Λόγω της υπόθεσης $\mathrm{char}\,(F) \neq 2$, το f είναι διαχωρίσιμο. Έστω E σώμα διάσπασης του f πάνω από το F και $t_1, \ldots, t_4 \in E$ οι (διαφορετικές) ρίζες του f. Την ομάδα S_4 βλέπομε ως ομάδα μεταθέσεων των t_1, t_2, t_3, t_4. Χρησιμοποιούμε τους εξής συμβολισμούς:

$$G = \mathcal{G}\,(E/F) \leq S_4 \quad \text{και} \quad V = \langle (t_1\,t_2)(t_3\,t_4), (t_1\,t_3)(t_2\,t_4) \rangle \leq S_4.$$

Η V είναι ομάδα Klein (τάξεως 4).

Επίσης, ορίζομε

$$u = (t_1 + t_2)(t_3 + t_4), \quad v = (t_1 + t_3)(t_2 + t_4), \quad w = (t_1 + t_4)(t_2 + t_3). \tag{9.2}$$

Με απλές πράξεις διαπιστώνομε ότι $u \neq v \neq w \neq u$, καθώς επίσης και ότι κάθε $\sigma \in S_4$ προκαλεί μια μετάθεση των u, v, w. Συνεπώς, το πολυώνυμο

$$g(X) := (X - u)(X - v)(X - w)$$

μένει αναλλοίωτο από κάθε $\sigma \in G$ (η συγκεκριμένη μορφή του υπολογίζεται στην άσκηση 9.18), άρα είναι πολυώνυμο του $F[X]$, με τρεις διαφορετικές ρίζες, όχι κατ' ανάγκη ανάγωγο πάνω από το F.

Τέλος, έστω

$$K := F(u, v, w) \leq E.$$

Η K/F είναι επέκταση Galois, αφού το K είναι σώμα διάσπασης του διαχωρίσιμου πολυωνύμου $g \in F[X]$.

Ένας υπολογισμός ρουτίνας δείχνει ότι $V \trianglelefteq S_4$ και

$$S_4/V = \{V,\ (t_1\,t_2)V,\ (t_2\,t_3)V,\ (t_1\,t_3)V,\ (t_1\,t_2\,t_3)V,\ (t_1\,t_3\,t_2)V\}. \tag{9.3}$$

Λήμμα 9.9. $\mathcal{G}\,(E/K) = G \cap V$. *Ισοδύναμα* $\mathcal{F}(G \cap V) = K$.

Απόδειξη. Ένας απλός έλεγχος δείχνει ότι κάθε $\sigma \in V$ αφήνει αναλλοίωτα τα u, v, w, επομένως, αφήνει αναλλοίωτο και κάθε στοιχείο του K. Άρα, $G \cap V \leq \mathcal{G}\,(E/K)$. Αντιστρόφως, έστω $\sigma \in \mathcal{G}\,(E/K)$. Λόγω της (9.3) είναι $\sigma = \tau\sigma_0$, όπου $\sigma_0 \in V$ και $\tau \in \{id,\ (t_1\,t_2),\ (t_2\,t_3),\ (t_1\,t_3),\ (t_1\,t_2\,t_3),\ (t_1\,t_3\,t_2)\}$. Το σ_0 αφήνει αναλλοίωτα τα u, v, w, άρα $\sigma(u) = \tau(u), \sigma(v) = \tau(v), \sigma(w) = \tau(w)$. Ένας απλός έλεγχος, και πάλι, αρκεί για να μας δείξει ότι από τους έξι αυτομορφισμούς του παραπάνω συνόλου, ο μόνος που αφήνει αναλλοίωτα και τα τρία u, v, w είναι ο id. Αλλά ο $\sigma \in \mathcal{G}\,(E/K)$ αφήνει αναλλοίωτα τα στοιχεία του K, άρα αφήνει αναλλοίωτα και τα τρία u, v, w· επομένως $\tau = id$ και $\sigma = \sigma_0 \in V$, άρα $\sigma \in G \cap V$. Συνεπώς, $\mathcal{G}\,(E/K) \leq G \cap V$, οπότε $\mathcal{G}\,(E/K) = G \cap V$. □

Έστω $[K : F] = m$. Έχομε το παρακάτω διάγραμμα αντιστοιχίας Galois:

$$\begin{array}{ccc} E & \longleftrightarrow & \langle id \rangle \\ \Big| & & \Big| \\ K & \longleftrightarrow & G \cap V \\ \Big| m & & \Big| \\ F & \longleftrightarrow & G \end{array}$$

Επειδή η K/F είναι επέκταση Galois, συμπεραίνομε ότι $G \cap V \trianglelefteq V$ και

$$\mathcal{G}\,(K/F) \cong G/(G \cap V) \quad \therefore \quad \frac{|G|}{|G \cap V|} = |G/(G \cap V)| = |\mathcal{G}\,(K/F)\,| = [K : F] = m. \tag{9.4}$$

Είναι η $G \cap V$ υποομάδα της V, άρα $|G \cap V| \in \{1, 2, 4\}$. Επίσης, επειδή m είναι ο βαθμός του σώματος διάσπασης κυβικού πολυωνύμου, είναι $m \in \{1, 2, 3, 6\}$. Συγκεκριμένα, αν το g είναι ανάγωγο πάνω από το F, τότε $m = 3$ ή $m = 6$, ανάλογα με το αν $\mathrm{D}(g)$ είναι ή δεν είναι ίση με τετράγωνο ενός στοιχείου του F (βλ. Παράδειγμα 7.26).
Ακόμη, είναι $F(t_1) \leq E$ και $[F(t_1) : F] = 4$ γιατί το f είναι ανάγωγο πάνω από το F, άρα $|G| = [E : F]$ είναι πολλαπλάσιο του 4. Όμως $|G|$ είναι και διαιρέτης του $|S_4| = 24$, άρα, συνοψίζοντας τα παραπάνω:

$$|G| \in \{4, 8, 12, 24\}, \quad |G \cap V| \in \{1, 2, 4\}, \quad m \in \{1, 2, 3, 6\}, \quad |G| = m \cdot |G \cap V|. \tag{9.5}$$

Στην απόδειξη του Θεωρήματος 9.13, το οποίο ταξινομεί τα τεταρτοβάθμια πολυώνυμα σε σχέση με τις ομάδες Galois αυτών, θα χρησιμοποιήσομε τις επόμενες καθαρά Ομαδο-θεωρητικές Προτάσεις 9.10 και 9.11, καθώς και το Λήμμα 9.12 που αφορά στην ειδική περίπτωση της G που μελετούμε.

Πρόταση 9.10. *Αν $H \leq S_n$ και $[S_n : H] = 2$, τότε $H = A_n$, δηλαδή, η μόνη υποομάδα της S_n με δείκτη 2 στην S_n είναι η εναλλάσουσα ομάδα A_n.*

Πρόταση 9.11. *Έστω πεπερασμένη ομάδα H τάξεως $p^n m$, όπου ο p είναι πρώτος, $n \geq 1$ και $p \nmid m$. Αν J_1, J_2 είναι υποομάδες της H τάξεως p^n (δηλαδή, οι J_1, J_2 είναι p-υποομάδες Sylow της H[2]), τότε αυτές είναι ισόμορφες* [3].

Λήμμα 9.12. *Αν η $G = \mathcal{G}(E/F)$ είναι τάξεως 4 και δεν είναι κυκλική, τότε $G = V$.*

Απόδειξη. Οι υποομάδες της S_4 τάξεως 4 είναι οι εξής:

$$\langle (1\,2\,3\,4) \rangle,\ \langle (1\,2\,4\,3) \rangle,\ \langle (1\,3\,2\,4) \rangle,\ \langle (1\,3), (2\,4) \rangle,\ \langle (1\,4), (2\,3) \rangle,\ \langle (1\,2), (3\,4) \rangle,\ \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle.$$

Οι τρεις πρώτες είναι κυκλικές, οπότε απορρίπτονται εξ υποθέσεως. Σύμφωνα με την Παρατήρηση 7.25, η G είναι μεταβατική, ενώ η τέταρτη και η πέμπτη από τις παραπάνω ομάδες είναι, προφανώς, μη μεταβατικές, άρα απορρίπτονται και αυτές και μένει δεκτή μόνο η τελευταία υποομάδα, η οποία είναι η V (διαπιστώστε ότι είναι μεταβατική). □

Στηριζόμενοι στα προηγούμενα είμαστε σε θέση τώρα να αποδείξομε το εξής:

Θεώρημα 9.13. (1) *Αν $m = 6$, τότε $G = S_4$.*
(2) *Αν $m = 3$, τότε $G = A_4$.*
(3) *Αν $m = 1$, τότε $G = V$.*
(4) *Αν $m = 2$ και το f είναι ανάγωγο πάνω από το K, τότε $G \cong D_4$.*
(5) *Αν $m = 2$ και το f δεν είναι ανάγωγο πάνω από το K, τότε $G \cong \mathbb{Z}_4$.*

Απόδειξη. Έστω $m \in \{3, 6\}$. Τότε, από την 4^{η} και την 1^{η} σχέσης στην (9.5), έπεται ότι $|G| \in \{12, 24\}$. Αν $|G| = 24$, τότε, προφανώς, $G = S_4$. Αν $|G| = 12$, τότε $[S_4 : G] = 2$ και από την Πρόταση 9.10 συμπεραίνομε ότι $G = A_4$. Τα στοιχεία της υποομάδας V είναι άρτιες μεταθέσεις, άρα, και στις δύο περιπτώσεις, $V \leq G$ και, συνεπώς, $G \cap V = V$, άρα $|G \cap V| = 4$. Τότε, από την 4^{η} σχέση στην (9.5), $|G| = 4m$. Από αυτή τη σχέση, σε συνδυασμό και με τα παραπάνω συμπεράσματα, γίνεται φανερό ότι, $m = 6 \Rightarrow G = S_4$ και $m = 3 \Rightarrow G = A_4$. Έτσι αποδείχθηκαν τα (1) και (2).

Έστω $m = 1$. Τότε, στο διάγραμμα αμέσως μετά την απόδειξη του Λήμματος 9.9, είναι $K = F$, άρα $G \cap V = V$. Αυτό σημαίνει ότι $G \leq V$. Η G δεν μπορεί να είναι γνήσια υποομάδα της $G \cap V$, διότι η τάξη της G είναι πολλαπλάσιο του 4, άρα $G = V$, οπότε αποδείχθηκε και το (3).

Έστω $m = 2$. Από την 1^{η}, 2^{η} και 4^{η} στη (9.5) έπεται ότι $|G| \in \{4, 8\}$. Σύμφωνα με την άσκηση 9.15, η S_4 έχει υποομάδες ισόμορφες με τη D_4, οπότε αν $|G| = 8$, τότε η G είναι 2-ομάδα Syllow της

[2] Η H περιέχει τέτοιες υποομάδες βάσει του *Πρώτου Θεωρήματος Sylow*.
[3] Βάσει του *Δεύτερου Θεωρήματος Sylow*.

S_4, όπως και η D_4, συνεπώς, από την Πρόταση 9.11, $G \cong D_4$ (δεν μπορούμε να ξέρομε με ποια από τις D_4-υποομάδες της S_4 είναι ίση η G). Αν $|G| = 4$ και η G δεν είναι κυκλική, τότε, από το Λήμμα 9.12, είναι $G = V$, κάτι που αποκλείεται για τον εξής λόγο: Αν $G = V$, τότε $|G \cap V| = 4$ και,συνεπώς, από την 4^{η} σχέση (9.5), $|G| = 8$, αντίφαση. Συνεπώς, μέχρι στιγμής καταλήξαμε στο εξής συμπέρασμα: Αν $m = 2$ τότε $G \cong D_4$ ή η G είναι κυκλική τάξεως 4, δηλαδή, $G \cong \mathbb{Z}_4$. Θα έχομε ολοκληρώσει την απόδειξη των (4) και (5) αν αποδείξομε ότι $G \cong D_4 \Leftrightarrow f$ είναι ανάγωγο πάνω από το K.

Απόδειξη του τελευταίου ισχυρισμού. Έστω ότι το f είναι ανάγωγο πάνω από το K. Τότε $[E : K] = 4$, άρα, από το διάγραμμα αμέσως μετά την απόδειξη του Λήμματος 9.9 είναι $[E : F] = 8$, οπότε $|G| = 8$, άρα $G \cong D_4$. Αντιστρόφως, έστω $G \cong D_4$. Τότε, η 4^{η} σχέση (9.5) συνεπάγεται ότι $|G \cap V| = 4$, άρα $G \cap V = V$, δηλαδή, $\mathcal{G}(E/K) = V$. Το E είναι, προφανώς, σώμα διάσπασης του f πάνω από το K και για κάθε $i \in \{1, 2, 3, 4\}$ υπάρχει $\sigma \in V$ με $\sigma(t_1) = t_i$, άρα, από την άσκηση 9.16, το f είναι ανάγωγο πάνω από το K. □

Παράδειγμα 9.14. Με τη βοήθεια του Θεωρήματος 9.13 θα υπολογίσομε τον ισομορφικό τύπο της ομάδας Galois G του $f(X) = X^4 + 5X + 5 \in \mathbb{Q}[X]$.

Βασισμένος στην άσκηση 9.18 υπολογίζω $g(X) = X^3 - 20X + 25 = (X + 5)(X^2 - 5X + 5)$. Άρα $m = 2$ και K είναι το σώμα διάσπασης του g πάνω από το $\mathbb{Q}$, δηλαδή, το σώμα διάσπασης του $X^2 - 5X + 5$. Συνεπώς, $K = \mathbb{Q}(\sqrt{5})$. Τώρα πρέπει να αποφασίσω αν $G \cong D_4$ ή $G \cong \mathbb{Z}_4$. Σύμφωνα με το θεώρημα, αυτό εξαρτάται από το αν το f είναι ή όχι ανάγωγο πάνω από το $\mathbb{Q}(\sqrt{5})$. Είναι $[F(t_i) : F] = 4$ για κάθε $i = 1, \dots, 4$, άρα το f δεν έχει ρίζα μέσα στο $K = \mathbb{Q}(\sqrt{5})$. Συνεπώς, το f δεν είναι ανάγωγο πάνω από το K αν και μόνο αν $f(X) = (X^2 + aX + b)(X^2 + cX + d)$ με τα $a, b, c, d \in K$. Αναπτύσσοντας το δεξιό μέλος και εξισώνοντας συντελεστές των ίσων δυνάμεων του X στα δύο μέλη, οδηγούμαι στις σχέσεις

$$c + a = 0, \quad ac + b + d = 0, \quad ad + bc = 5, \quad bd = 5.$$

Οι δύο πρώτες δίνουν $c = -a$ και $d = -b - ac = a^2 - b$. Αντικαθιστώντας στην τρίτη παίρνω $b = (a^3 - 5)/(2a)$ και τώρα η τελευταία γίνεται

$$5 = bd = \frac{a^3 - 5}{2a}(a^2 - b) = \frac{a^3 - 5}{2a}\left(a^2 - \frac{a^3 - 5}{2a}\right) = \frac{a^6 - 25}{4a^2}.$$

Έτσι, $a^6 - 20a^2 - 25 = 0$. Και παρατηρώ ότι η τιμή $a = \sqrt{5}$ επαληθεύει την τελευταία σχέση. Γι' αυτή την τιμή του a είναι και $c, b, d \in \mathbb{Q}(\sqrt{5}) = K$, άρα το f δεν είναι ανάγωγο πάνω από το K. Συνεπώς, σύμφωνα με το Θεώρημα 9.13 (5), είναι $G \cong \mathbb{Z}_4$.

Παρατήρηση. Αν και το πολυώνυμο $X^4 + 3X + 3 \in \mathbb{Q}[X]$ είναι «εντελώς όμοιο» με το f αυτού του παραδείγματος, έχει ομάδα Galois διαφορετικού ισομορφικού τύπου. Δείτε την άσκηση 9.19 (4).

Ασκήσεις

Άσκηση 9.15. Έστω $i, j, k \in \{2, 3, 4\}$ με $i \neq j \neq k \neq 1$. Αποδείξτε ότι η υποομάδα $\langle (1\,j),\ (1\,i\,j\,k) \rangle$ της S_4 είναι ισόμορφη με τη διεδρική ομάδα D_4.

Άσκηση 9.16. Έστω σώμα F και $f \in F[X]$ βαθμού $n > 1$ το οποίο έχει n διαφορετικές ρίζες $t_1, \dots, t_n$ σε ένα σώμα διάσπασής του E πάνω από το F. Αποδείξτε το εξής: Αν για κάθε $i = 1, \dots, n$ υπάρχει F-αυτομορφισμός του E που στέλνει το t_1 στο t_i, τότε το f είναι ανάγωγο πάνω από το F.

Άσκηση 9.17 (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. Παρατηρήστε ότι το α είναι μια οποιαδήποτε επιλογή κυβικής ρίζας του $\sqrt{R} - q/2$. Αν ω είναι 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.

Άσκηση 9.18 (Μέθοδος του Descartes για την εύρεση των ριζών του τεταρτοβάθμιου πολυωνύμου)**.** Έστω σώμα F του οποίου η χαρακτηριστική είναι $\neq 2, 3$ και ανάγωγο πολυώνυμο

$$f(X) = X^4 + qX^2 + rX + s \in F[X].^{4}$$

Έστω E σώμα διάσπασης του f πάνω από το F, $t_1, \ldots, t_4 \in E$ οι διαφορετικές (όπως έχομε ήδη 'δει) ρίζες του και τα στοιχεία $u, v, w \in E$ που ορίζονται στη σχέση (9.2). Τα u, v, w είναι διαφορετικά (αρκεί ένας απλός υπολογισμός), ορίσαμε το πολυώνυμο $g(X) = (X - u)(X - v)(X - w)$ και αποδείξαμε ότι $g \in F[X]$.

(1) Δείξτε ότι $\mathrm{D}(g) = \mathrm{D}(f)$.

(2) Έστω $t_1 + t_2 = -k$, $t_1 t_2 = l$ και $t_3 t_4 = m$ με $k, l, m \in E$. Παρατηρήστε ότι $t_3 + t_4 = k$ και εξηγήστε (δίχως καθόλου πράξεις) γιατί

$$f(X) = (X^2 + kX + l)(X^2 - kX + m).$$

(3) Εξισώνοντας τους συντελεστές στα δύο μέλη της παραπάνω ισότητας εκφράστε τα l, m, s συναρτήσει των q, r, k και στη συνέχεια δείξτε πώς, απαλείφοντας τα l, m μεταξύ των τριών αυτών σχέσεων, θα οδηγηθείτε στη στη σχέση $k^6 + 2qk^4 + (q^2 - 4s)k^2 - r^2 = 0$. Παρατηρήστε ότι $-k^2 = u$ και συμπεράνετε ότι το u είναι ρίζα του $X^3 - 2qX^2 + (q^2 - 4s)X + r^2$. Ειδικότερα, επειδή $-u = k^2 = (t_1 + t_2)^2$, είναι $\sqrt{-u} \in E$. Θεωρήστε δεδομένο ότι με εντελώς ανάλογο τρόπο μπορεί να αποδειχθεί ότι τα v και w είναι, επίσης, ρίζες του ίδιου πολυωνύμου, με $\sqrt{-v}, \sqrt{-w} \in E$, και εξηγήστε γιατί

$$g(X) = X^3 - 2qX^2 + (q^2 - 4s)X + r^2. \tag{9.6}$$

(4) Έστω $z \in E$ μια οποιαδήποτε μη μηδενική ρίζα του g. Αποδείξτε ότι

$$f(X) = \left(X^2 + \sqrt{-z}\, X + \frac{1}{2}\left(-z + q - \frac{r}{\sqrt{-z}}\right)\right) \cdot \left(X^2 - \sqrt{-z}\, X + \frac{1}{2}\left(-z + q + \frac{r}{\sqrt{-z}}\right)\right).$$

Συμπεράνετε ότι οι ρίζες των δύο δευτεροβάθμιων πολυωνύμων του δεξιού μέλους μας δίνουν τις τέσσερις ρίζες του f.

Σημείωση. Η κυβική εξίσωση $g(x) = 0$ λέγεται *επιλύουσα* της τεταρτοβάθμιας εξίσωσης $f(x) = 0$.

Άσκηση 9.19. Με τη βοήθεια του Θεωρήματος 9.13 υπολογίστε τον ισομορφικό τύπο των ομάδων Galois καθενός από τα παρακάτω πολυώνυμα του $\mathbb{Q}[X]$:

1. $X^4 + 8X + 12$
2. $X^4 + 4X^2 - 2$
3. $X^4 - X - 1$
4. $X^4 + 3X + 3$
5. $X^4 + 8X + 14$

[4] Κάθε $X^4 + aX^3 + bX^2 + cX + d \in F[X]$ μπορεί να πάρει αυτή τη μορφή (δηλαδή, με μηδενικό συντελεστή στο X^3), μέσω της αντικατάστασης $X \leftarrow X - a/4$ και το πολυώνυμο που προκύπτει έχει την ίδια διακρίνουσα με το αρχικό.

Τύποι για τις ρίζες του τεταρτοβάθμιου πολυωνύμου

Θεωρούμε το τεταρτοβάθμιο πολυώνυμο που ορίζεται στην (9.1) και συμβολίζουμε με $t_1, \dots, t_4$ τις ρίζες του. Επίσης, θεωρούμε τα u, v, w που ορίζονται στην (9.2).

Σύμφωνα με την άσκηση 9.18 είναι $t_1 + t_2 = \sqrt{-u}$ και, συνεπώς (λόγω της $t_1 + t_2 + t_3 + t_4 = 0$), $t_3 + t_4 = -\sqrt{-u}$. Προς το παρόν δεν προσδιορίζουμε ποια από τις δύο τετραγωνικές ρίζες του $-u$ συμβολίζει το $\sqrt{-u}$. Με ανάλογο τρόπο παίρνομε και τις σχέσεις $t_1 + t_3 = \sqrt{-v}$, $t_2 + t_4 = -\sqrt{-v}$ και $t_1 + t_4 = \sqrt{-w}$, $t_2 + t_3 = -\sqrt{-w}$. Όπως και στην περίπτωση του $\sqrt{-u}$, δεν προσδιορίζομε, προς το παρόν, ποια από τις δύο τετραγωνικές ρίζες των $-v$ και $-w$ προσδιορίζουν τα σύμβολα $\sqrt{-v}$ και $\sqrt{-w}$. Από την ίδια άσκηση, τα u, v, w είναι ρίζες του πολυωνύμου $g(X)$ που ορίζεται στην (9.6), άρα, από τους τύπους του Viète,

$$u + v + w = 2q, \quad uv + vw + wu = q^2 - 4s, \quad uvw = -r^2$$

Για απλούστευση του συμβολισμού θέτομε $\xi_1 = \sqrt{-u}, \xi_2 = \sqrt{-v}, \xi_3 = \sqrt{-w}$,[5] οπότε, βάσει των παραπάνω έχομε το σύστημα γραμμικών εξισώσεων

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \end{pmatrix} = \begin{pmatrix} \xi_1 \\ -\xi_1 \\ \xi_2 \\ -\xi_2 \\ \xi_3 \\ -\xi_3 \end{pmatrix}$$

Αυτό το μη ομογενές γραμμικό σύστημα έχει ακριβώς μία λύση, την

$$t_1 = \tfrac{1}{2}(\xi_1 + \xi_2 + \xi_3), \quad t_2 = \tfrac{1}{2}(\xi_1 - \xi_2 - \xi_3), \quad t_3 = \tfrac{1}{2}(-\xi_1 + \xi_2 - \xi_3), \quad t_4 = \tfrac{1}{2}(-\xi_1 - \xi_2 + \xi_3).$$

Μένει να προσδιορίσομε ποια από τις δύο τετραγωνικές ρίζες των $-u, -v, -w$ συμβολίζουν, αντιστοίχως, τα ξ, ξ_2, ξ_3. Σύμφωνα με τους τύπους του Viète, πρέπει και αρκεί να ισχύουν οι σχέσεις

$$\sum_{1 \le i \le 4} t_i = 0, \quad \sum_{1 \le i < j \le 4} t_i t_j = q, \quad \sum_{1 \le i < j < k \le 4} t_i t_j t_k = -r, \quad t_1 t_2 t_3 t_4 = s \tag{9.7}$$

Η πρώτη από τις σχέσεις (9.7) είναι προφανής και ισχύει ανεξαρτήτως επιλογής των τετραγωνικών ριζών $\xi_1, \dots, \xi_4$.
Υπολογίζομε

$$\sum_{1 \le i < j \le 4} t_i t_j = -\tfrac{1}{2}(\xi^2 + \xi_2^2 + \xi_3^2 = \tfrac{1}{2}(u + v + w) = q,$$

άρα ισχύει και η δεύτερη σχέση (9.7) ανεξαρτήτως επιλογής των τετραγωνικών ριζών $\xi_1, \dots, \xi_4$.
Υπολογίζομε

$$\begin{aligned} t_1 t_2 t_3 t_4 &= \tfrac{1}{16}\{\xi_1^4 + \xi_2^4 + \xi_3^4 - 2\left((\xi\xi_2)^2 + (\xi_2\xi_3)^2 + (\xi_3\xi_1)^2\right)\} = \tfrac{1}{16}\{u^2 + v^2 + w^2 - 2(uv + vw + wu)\} \\ &= \tfrac{1}{16}\{(u + v + w)^2 - 4(uv + vw + wu)\} = \tfrac{1}{16}\{4q^2 - 4(q^2 - 4s)\} = s, \end{aligned}$$

συνεπώς ισχύει και η τέταρτη σχέση (9.7) ανεξαρτήτως επιλογής των τετραγωνικών ριζών $\xi_1, \dots, \xi_4$ και μένει ο έλεγχος της τρίτης σχέσης. Υπολογίζομε $\sum_{1 \le i < j < k \le 4} t_i t_j t_k = \xi_1\xi_2\xi_3$. Είναι $(\xi_1\xi_2\xi_3)^2 = -uvw = r^2$, συνεπώς, στον ορισμό των $\xi_1 = \sqrt{-u}$, $\xi_2 = \sqrt{-v}$ και $\xi_3 = \sqrt{-w}$, η επιλογή των τετραγωνικών ριζών πρέπει να γίνει έτσι ώστε το γινόμενό τους να ισούται με $-r$ (προφανώς υπάρχουν περισσότερες από μία επιλογές).

[5] Τα ξ δεν είναι όλα 0 γιατί, σε αντίθετη περίπτωση, το $g(X)$ είναι μηδενικό πολυώνυμο, άρα $q = r = s = 0$, που αντιβαίνει στις υποθέσεις για το $f(X)$.

Συνοψίζοντας, οι ρίζες $t_1, \dots, t_4$ του $f(X) = X^4 + qX^2 + rX + s \in F[X]$ (char $(F) \neq 2, 3$), δίδονται από τις σχέσεις

$$\begin{aligned} t_1 &= \tfrac{1}{2}\left(\sqrt{-u} + \sqrt{-v} + \sqrt{-w}\right) \\ t_2 &= \tfrac{1}{2}\left(\sqrt{-u} - \sqrt{-v} - \sqrt{-w}\right) \\ t_3 &= \tfrac{1}{2}\left(-\sqrt{-u} + \sqrt{-v} - \sqrt{-w}\right) \\ t_4 &= \tfrac{1}{2}\left(-\sqrt{-u} - \sqrt{-v} + \sqrt{-w}\right) \end{aligned}$$

όπου u, v, w είναι οι ρίζες του $g(X) = X^3 - 2qX^2 + (q^2 - 4s)X + r^2$ και οι τετραγωνικές ρίζες $\sqrt{-u}, \sqrt{-v}, \sqrt{-w}$ είναι έτσι επιλεγμένες ώστε $\sqrt{-u}\sqrt{-v}\sqrt{-w} = -r$. Ο υπολογισμός των ριζών γίνεται με τη βοήθεια της άσκησης 9.17.[6]

Το Θεμελιώδες Θεώρημα της Άλγεβρας

Θεώρημα 9.20. *Το $\mathbb{C}$ είναι αλγεβρικά κλειστό σώμα.*

Απόδειξη. Έστω $K/\mathbb{C}$ πεπερασμένη επέκταση. Θα δείξομε ότι $K = \mathbb{C}$ (βλ. Ορισμό 3.2 και Θεώρημα 3.1).

Έστω N η κανονική κλειστότητα της πεπερασμένης επέκτασης $K/\mathbb{R}$ (Θεώρημα 5.2). Η πεπερασμένη επέκταση $N/\mathbb{R}$ είναι κανονική και διαχωρίσιμη (char $(\mathbb{R}) = 0$), άρα είναι επέκταση Galois. Έχομε τώρα την αλυσίδα επεκτάσεων $\mathbb{R} \leq \mathbb{C} \leq K \leq N$ και θα δείξομε ότι $N = \mathbb{C}$, οπότε και $K = \mathbb{C}$.

Θα εργασθούμε πρώτα στην επέκταση $N/\mathbb{R}$. Έστω $G = \mathcal{G}(N/\mathbb{R})$ και $|G| = 2^n m$ με m περιττό και $n \geq 0$. Από το 1ο Θεώρημα Sylow υπάρχει υποομάδα H της G τάξεως 2^n και έστω ότι αυτή αντιστοιχεί (μέσω της αντιστοιχίας Galois) στην ενδιάμεση επέκταση E. Η επέκταση $E/\mathbb{R}$ είναι απλή (θεώρημα 5.3) άρα υπάρχει $u \in \mathbb{R}$ ώστε $E = \mathbb{R}(u)$. Έχομε τώρα το διάγραμμα

$$\begin{array}{ccc} N & \longleftarrow & \langle id_N \rangle \\ \Big| {\scriptstyle 2^n} & & \Big| {\scriptstyle 2^n} \\ E = \mathbb{R}(u) & \longleftarrow & H \\ \Big| {\scriptstyle m} & & \Big| {\scriptstyle m} \\ \mathbb{R} & \longleftarrow & G \end{array}$$

Το Irr $(u, \mathbb{R})$ έχει βαθμό m περιττό. Αλλά κάθε πολυώνυμο του $\mathbb{R}[X]$ περιττού βαθμού έχει ρίζα στο $\mathbb{R}$, άρα τα μόνα ανάγωγα πολυώνυμα του $\mathbb{R}[X]$ περιττού βαθμού είναι τα πρωτοβάθμια. Συνεπώς $m = 1$, $H = G$ και $[N : \mathbb{R}] = |G| = 2^n$. Επειδή $[N : \mathbb{R}] \geq [\mathbb{C} : \mathbb{R}] = 2$, είναι $n \geq 1$. Τώρα θεωρούμε το διάγραμμα

$$\begin{array}{ccc} N & \longleftarrow & \langle id_N \rangle \\ \Big| {\scriptstyle 2^{n-1}} & & \Big| {\scriptstyle 2^{n-1}} \\ \mathbb{C} & \longleftarrow & \mathcal{G}(N/\mathbb{C}) \\ \Big| {\scriptstyle 2} & & \Big| {\scriptstyle 2} \\ \mathbb{R} & \longleftarrow & G \end{array}$$

Αν $n = 1$, τότε $N = \mathbb{C}$ η απόδειξη έχει ολοκληρωθεί.

[6] Η αλλαγή μεταβλητής $X \leftarrow X + 2q/3$ μετασχηματίζει το $g(X)$ σε κυβικό πολυώνυμο δίχως τον όρο X^2.

Μένει να αποδείξομε ότι η υπόθεση $n > 1$ μας οδηγεί σε άτοπο ως εξής. Εργαζόμαστε στην επέκταση Galois $N/\mathbb{C}$. Είναι $|\mathcal{G}(N/\mathbb{C}) = [N : \mathbb{C}] = 2^{n-1}$ και έστω υποομάδα J της $\mathcal{G}(N/\mathbb{C})$ τάξεως 2^{n-2} (την ύπαρξή της εξασφαλίζει το 1ο Θεώρημα Sylow) και M η ενδιάμεση επέκταση που αντιστοιχεί στην J. Τότε έχομε το διάγραμμα

$$\begin{array}{ccc} N & \longleftrightarrow & \langle id_N \rangle \\ \Big| 2^{n-2} & & \Big| 2^{n-2} \\ M & \longleftrightarrow & J \\ \Big| 2 & & \Big| 2 \\ \mathbb{C} & \longleftrightarrow & \mathcal{G}(N/\mathbb{C}) \end{array}$$

Η $M/\mathbb{C}$ είναι επέκταση του $\mathbb{C}$ βαθμού 2, συμπέρασμα άτοπο γιατί δεν υπάρχει τέτοια επάκταση του $\mathbb{C}$, αφού οι τετραγωνικές ρίζες καθενός μη μηδενικού μιγαδικού αριθμού ανήκουν στο $\mathbb{C}$. □

Ασκήσεις

Άσκηση 9.21. Αποδείξτε ότι κάθε γνήσια αλγεβρική επέκταση του $\mathbb{R}$ είναι ισόμορφη με το $\mathbb{C}$.
Υπόδειξη. Έστω K γνήσια αλγεβρική επέκταση του $\mathbb{R}$. Έχομε την παρακάτω κατάσταση:

$$\begin{array}{ccc} K & & \mathbb{C} \\ & \diagdown \quad \diagup & \\ & \mathbb{R} & \end{array}$$

Έστω $u \in K \setminus \mathbb{R}$ και $f = \text{Irr}(u, \mathbb{R})$. Το f έχει ρίζα $v \in \mathbb{C}$. Εξετάστε τα σώματα $\mathbb{R}(u)$ και $\mathbb{R}(v)$.

Κατασκευές με κανόνα και διαβήτη

- Ο όρος «κατασκευή» σημαίνει «γεωμετρική κατασκευή με αποκλειστική χρήση κανόνα και διαβήτη».
- Οι κατασκευές γίνονται πάνω στο επίπεδο xOy, άρα στους άξονες έχει ορισθεί το μοναδιαίο μήκος.
- Γίνεται διάκριση των όρων *ευθύγραμμο τμήμα* (γεωμετρικό αντικείμενο) από *μήκος ευθυγράμμου τμήματος* (πραγματικός αριθμός). Αν α συμβολίζει ένα ευθύγραμμο τμήμα, το $|\alpha|$ συμβολίζει το μήκος του.
- Κατασκευή πραγματικού αριθμού $x > 0$ σημαίνει κατασκευή ευθυγράμμου τμήματος α, ώστε $|\alpha| = x$ και μεταφορά, με τον διαβήτη, του α σε έναν από τους θετικούς ημιάξονες του επιπέδου με αρχή το 0. Κατασκευή πραγματικού αριθμού $x < 0$ σημαίνει κατασκευή ευθυγράμμου τμήματος α, ώστε $|\alpha| = -x$ και μεταφορά, με τον διαβήτη, του α σε έναν από τους αρνητικούς ημιάξονες του επιπέδου με αρχή το 0. Αν μπορεί να πραγματοποιηθεί η κατασκευή ενός πραγματικού αριθμού x, τότε ο x χαρακτηρίζεται *κατασκευάσιμος*.

Στοιχειώδεις γεωμετρικές κατασκευές

- *Δεδομένα:* Σημείο P και ευθεία ϵ που δεν περνά από το P.
  Κατασκευή: Ευθεία που περνά από το P και είναι κάθετη στην ϵ.
- *Δεδομένα:* Ευθεία ϵ και σημείο της P.
  Κατασκευή: Ευθεία κάθετη ϵ στο σημείο P.
- *Δεδομένα:* Σημείο P και ευθεία ϵ που δεν περνά από το P.
  Κατασκευή: Ευθεία που περνά από το P και είναι παράλληλη στην ϵ.
- *Δεδομένα:* Δύο τεμνόμενες ημιευθείες.
  Κατασκευή: Ευθεία που διχοτομεί τη γωνία που σχηματίζουν οι ημιευθείες αυτές.

- *Δεδομένο:* $m, n \in \mathbb{N}$.
  Κατασκευή: Ευθύγραμμο τμήμα μήκους m/n.
- *Δεδομένα:* Ευθύγραμμα τμήματα α, β.
  Κατασκευή: Το ευθύγραμμο τμήμα $\alpha + \beta$, δηλαδή, ευθύγραμμο τμήμα γ, ώστε $|\gamma| = |\alpha| + |\beta|$.
- *Δεδομένα:* Άνισα ευθύγραμμα τμήματα α, β.
  Κατασκευή: Το ευθύγραμμο τμήμα $\alpha - \beta$. Αυτό σημαίνει το εξής: Αν $|\alpha| > |\beta|$, κατασκευή ευθυγράμμου τμήματος γ, ώστε $|\gamma| = |\alpha| - |\beta|$. Αν $|\alpha| < |\beta|$, κατασκευή ευθυγράμμου τμήματος γ, ώστε $|\gamma| = |\beta| - |\alpha|$ και μεταφορά, με τον διαβήτη, του γ σε έναν από τους αρνητικούς ημιάξονες του επιπέδου
- *Δεδομένα:* Ευθύγραμμα τμήματα α, β.
  Κατασκευή: Το ευθύγραμμο τμήμα $\alpha \cdot \beta$, δηλαδή, ευθύγραμμο τμήμα γ, ώστε $|\gamma| = |\alpha| \cdot |\beta|$.
- *Δεδομένα:* Ευθύγραμμα τμήματα α, β.
  Κατασκευή: Το ευθύγραμμο τμήμα α/β, δηλαδή, ευθύγραμμο τμήμα γ, ώστε $|\gamma| = |\alpha|/|\beta|$.
- *Δεδομένα:* Ευθύγραμμο τμήμα α.
  Κατασκευή: Το ευθύγραμμο τμήμα $\sqrt{\alpha}$, δηλαδή, ευθύγραμμο τμήμα β, ώστε $|\beta| = \sqrt{|\alpha|}$.
- *Δεδομένα:* Κατασκευάσιμοι μη μηδενικοί πραγματικοί αριθμοί a, b.
  Κατασκευή: Λύση της $ax + b = 0$, δηλαδή, κατασκευή του πραγματικού αριθμού $-b/a$.
- *Δεδομένα:* Κατασκευάσιμοι πραγματικοί αριθμοί a, b, c με $a \neq 0$ και τουλάχιστον έναν από τους b, c μη μηδενικό.
  Κατασκευή: Λύση της $ax^2 + bx + c = 0$, δηλαδή, κατασκευή των πραγματικών αριθμών που παρέχουν οι τύποι επίλυσης της δευτεροβάθμιας εξίσωσης.

Έστω σώμα $F \geq \mathbb{Q}$. Όταν λέω «σημείο του F» εννοώ σημείο στο επίπεδο $x0y$, του οποίου οι συντεταγμένες x, y ανήκουν στο F. Κατ' αναλογίαν, «ευθεία του F» είναι κάθε ευθεία που ορίζεται από δύο διαφορετικά σημεία του F και «κύκλος του F» είναι κάθε κύκλος με κέντρο σημείο του F και ακτίνα ίση με την απόσταση δύο σημείων του F.

Εύκολα φαίνεται ότι οι ευθείες του F ορίζονται από εξισώσεις της μορφής

$$ax + by + c = 0, \quad a, b, c \in F$$

και οι κύκλοι του F ορίζονται από εξισώσεις της μορφής

$$x^2 + y^2 + ax + by + c = 0, \quad a, b, c \in F.$$

Αν επιχειρήσω να κάνω μία κατασκευή με κανόνα και διαβήτη βασισμένος στα σημεία του σώματος F, τότε κάθε νέο σημείο που προκύπτει είναι σημείο, ή του F ή μιας δευτεροβάθμιας επέκτασης του F. Αυτό εξηγείται ως εξής: Κάθε σημείο κατά τη διαδικασία μιας τέτοιας κατασκευής προκύπτει από τομές ευθειών ή κύκλων, άρα οι συντεταγμένες του προκύπτουν από επίλυση συστημάτων ζεύγους εξισώσεων όπως οι παραπάνω. Συνεπώς, οι συντεταγμένες του είναι λύσεις συστήματος που έχει μια από τις παρακάτω μορφές (σε όλες τις εξισώσεις εννοείται ότι οι συντελεστές ανήκουν στο F):

$$\begin{cases} a_1x + b_1y + c_1 = 0 \\ a_2x + b_2y + c_2 = 0 \end{cases} \tag{9.8}$$

$$\begin{cases} a_1x + b_1y + c_1 = 0 \\ x^2 + y^2 + a_2x + b_2y + c_2 = 0 \end{cases} \tag{9.9}$$

$$\begin{cases} x^2 + y^2 + a_1x + b_1y + c_1 = 0 \\ x^2 + y^2 + a_2x + b_2y + c_2 = 0 \end{cases} \tag{9.10}$$

Το 1ο σύστημα δίνει σημείο με συντεταγμένες στο F. Το 2ο σύστημα δίνει σημείο με συντεταγμένες σε επέκταση του F βαθμού το πολύ 2. Το 3ο σύστημα ανάγεται σε σύστημα της $2^{\eta\varsigma}$ μορφής, αν αντικαταστήσω τη μια από τις εξισώσεις του με εκείνη που προκύπτει από αφαίρεση των δύο εξισώσεων.
Σε μία κατασκευή πραγματικού αριθμού γίνονται πολλά τέτοια βήματα οπότε έχω αλυσίδα επεκτάσεων $\mathbb{Q} = F_0 \leq F_1 \leq ... \leq F_n$ στην οποία $[F_i : F_{i-1}] = 1$ ή 2 γ ια κάθε i και στο F_n βρίσκεται ο αριθμός που κατασκεύασα ως μία συντεταγμένη του τελικού σημείου κατασκευής. Συνεπώς, απέδειξα το εξής:

Θεώρημα 9.22. *Αν ο $\alpha \in \mathbb{R}$ είναι κατασκευάσιμος, τότε υπάρχει πεπερασμένη επέκταση $F/\mathbb{Q}$ με $\alpha \in F$ και $[F : \mathbb{Q}] = 2^k$ για κάποιο $k \in \mathbb{N}_0$. Συνεπώς, ο βαθμός $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ ισούται με δύναμη του 2.*

Παράδειγμα 9.23. Ο $\sqrt[3]{2}$ δεν κατασκευάζεται (με κανόνα και διαβήτη) (Δήλιον Πρόβλημα - Διπλασιασμός του Κύβου), καθώς αν υπάρχει τέτοιο σώμα F, τότε $3 = \left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] \mid [F : \mathbb{Q}] = 2^k$, άτοπο!

Για μια αναλυτικότερη παρουσίαση των παραπάνω παραπέμπω στην ενότητα 1.3 των Σημειώσεών μου για το προπτυχιακό μάθημα «Θεωρία Σωμάτων».

Κατασκευή Κανονικού n-γώνου (γενικά)

Πρόταση 9.24. (1) *Αν $n = 2^r m$, με τον m περιττό και $r \geq 0$, τότε το κανονικό n-γωνο κατασκευάζεται αν και μόνο αν το κανονικό m-γωνο κατασκευάζεται.*

(2) *Αν ο l είναι περιττός, όχι πρώτος και $l = mn$ με $m, n > 1$ και $\gcd(m, n) = 1$, τότε το κανονικό l-γωνο κατασκευάζεται αν και μόνο αν το κανονικό m-γωνο και το κανονικό n-γωνο κατασκευάζονται.*

Απόδειξη. (1) Αν κατασκευάζεται το κανονικό m-γωνο, τότε, φέρνοντας τη μεσοκάθετο κάθε πλευράς αυτού και ενώνοντας τις κορυφές του με τα σημεία τομής των μεσοκαθέτων με τον περιγεγραμμένο στο m-γωνο κύκλο, τότε κατασκευάζω το $2m$-γωνο. Επαναλαμβάνοντας τη διαδικασία στο νέο πολύγωνο κατασκευάζω το $4m$-γωνο, κλπ, μέχρι να κατασκευάσω το $2^r m$-γωνο.

Αντίστροφα, αν έχω κατασκευάσει το n-γωνο, ενώνω τις κορυφές του ανα 2^r. Το σχήμα που κατασκευάζω είναι κανονικό m-γωνο.

(2) Αν κατασκευάζεται το κανονικό l-γωνο, τότε, ενώνοντας τις κορυφές του ανα m (αντιστοίχως, ανά ν) κατασκευάζω το κανονικό ν-γωνο (αντιστοίχως, το κανονικό m-γωνο).

Αντίστροφα, έστω ότι κατασκευάζεται και το κανονικό m-γωνο και το κανονικό n-γωνο. Τα φαντάζομαι εγγεγραμμένα στον ίδιο κύκλο και έστω τ_m και τ_n τα τόξα που αντιστοιχούν σε μία πλευρά του m-γώνου και του n-γώνου αντιστοίχως. Τα μέτρα των τ_m και τ_n είναι, αντιστοίχως, $2\pi/m$ και $2\pi/n$.

Στον ίδιο κύκλο, το τόξο που αντιστοιχεί στο κανονικό mn-γωνο, έστω τ_{mn}, είναι αυτό που θέλω να κατασκευάσω. Το μέτρο του είναι $2\pi/(mn)$. Επειδή οι m, n είναι πρώτοι μεταξύ τους, από τη στοιχειώδη Θεωρία Αριθμών έχω ότι υπάρχουν θετικοί ακέραιοι a, b που επαληθεύουν τη σχέση $am - bn = 1$, άρα $a\frac{1}{n} - b\frac{1}{m} = \frac{1}{mn}$. Συνεπώς,

$$a\frac{2\pi}{n} - b\frac{2\pi}{m} = \frac{2\pi}{mn},$$

που σημαίνει ότι το τ_{mn} ισούται με a φορές το τ_n μείον b φορές το τ_m. Η κατασκευή τώρα του τ_{mn} είναι προφανής. □

Παρατήρηση 9.25. Έστω $m = p_1^{k_1} \cdots p_l^{k_l}$ η κανονική ανάλυση του m σε πρώτους (τα $k_i \geq 1$ και τα p_i διαφορετικά ανά 2) Από το παραπάνω, το m-γωνο κατακευάζεται αν και μόνο αν τα $p_i^{k_i}$ κατασκευάζονται. Άρα μένει να εξετάσω ποια q-γωνα με $q = p^k$, p περιττό πρώτο και $k \geq 1$ κατασκευάζονται. Έστω $\omega = \cos\theta + i\sin\theta \in \mathbb{C}$ (αρχική q-ρίζα της μονάδας). Το q-γωνο έχει κεντρική γωνία $\theta = \frac{2\pi}{q}$, συνεπώς το κανονικό q-γωνο κατασκευάζεται αν και μόνο αν το $\cos\theta$ κατασκευάζεται. Αλλά $2\cos\theta = \omega + \omega^{-1}$,

άρα $\omega^2 - (2\cos\theta)\omega + 1 = 0$. Το πολυώνυμο $X^2 - (2\cos\theta)X + 1 \in \mathbb{Q}(\cos\theta)[X]$ είναι ανάγωγο γιατί έχει ρίζες του τα $\omega, \omega^{-1} \notin \mathbb{R}$, ενώ $\mathbb{Q}(\cos\theta) \subset \mathbb{R}$. Επομένως

$$\begin{array}{c} E_q = \mathbb{Q}(\omega) \\ \Big| 2 \\ K = \mathbb{Q}(\cos(\theta)) \\ \Big| \\ \mathbb{Q} \end{array}$$

Η $E_q/\mathbb{Q}$ είναι κυκλοτομική, οπότε $\left[E_q : \mathbb{Q}\right] = \phi(q)$. Άρα $[K : \mathbb{Q}] = \frac{1}{2}\phi(q) = \frac{1}{2}p^{k-1}(p-1)$ ή $p^{k-1}(p-1)$. Για να κατασκευάζεται ο $\cos\theta$ πρέπει (Θεώρημα 9.22) ο αριθμός $[K : \mathbb{Q}]$ να είναι δύναμη του 2. Αυτό συνεπάγεται ότι $k = 1$ και ο $(p-1)$ είναι δύναμη του 2, δηλαδή, $p = 2^r + 1$ για κάποιο $r \in \mathbb{N}$. Η τελευταία ισότητα, με τη σειρά της, συνεπάγεται ότι ο r είναι δύναμη του 2, διότι, αν $r = l\nu$ με τον $\nu > 1$ και περιττό, τότε, λόγω της ταυτότητας

$$x^\nu + y^\nu = (x+y)(x^{\nu-1} - x^{\nu-2}y + \cdots - xy^{\nu-2} + y^{\nu-1})$$

(εφαρμόζόμενης στα $x = 2^l, y = 1$) ο $2^l + 1$ είναι διαιρέτης του πρώτου $p\cdot$ άτοπο.

Βάσει των παραπάνω καταλήγομε στο εξής:

Θεώρημα 9.26. *Το κανονικό n-γωνο κατασκευάζεται αν και μόνο αν $n = 2^r p_1 \cdots p_k$ όπου $r \geq 0$ και $p_1, \ldots, p_k$ είναι διαφορετικοί πρώτοι του Fermat, δηλαδή $p_i = 2^{2^{r_i}} + 1$ για κάποιο $r_i \geq 0$ για κάθε $i = 1, \ldots, k$.*

Κατασκευή του κανονικού 17-γώνου Η θεωρία των κυκλοτομικών σωμάτων πάνω από το $\mathbb{Q}$, εξειδικευμένη στο 17-ο κυκλοτομικό σώμα πάνω από το $\mathbb{Q}$, συνοψίζεται στα παρακάτω:

$$\theta = \frac{2\pi}{17}, \quad \omega = \cos\theta + i\sin\theta, \quad 2\cos\theta = \omega + \omega^{-1} = \omega + \omega^{16},$$

$$E_{17} = \mathbb{Q}(\omega), \quad \mathcal{G}\left(E_{17}/\mathbb{Q}\right) = \langle\sigma\rangle, \quad \sigma(\omega) = \omega^3, \quad \sigma^k(\omega) = \omega^{3^k}, \quad \sigma(\omega^k) = \omega^{3k}.$$

Το διάγραμμα της αντιστοιχίας Galois είναι το εξής:

$$\begin{array}{ccc} \langle id\rangle & \longleftrightarrow & L_4 = E_{17} \\ \Big| 2 & & \Big| 2 \\ \langle\sigma^8\rangle & \longleftrightarrow & L_3 \\ \Big| 2 & & \Big| 2 \\ \langle\sigma^4\rangle & \longleftrightarrow & L_2 \\ \Big| 2 & & \Big| 2 \\ \langle\sigma^2\rangle & \longleftrightarrow & L_1 \\ \Big| 2 & & \Big| 2 \\ \mathcal{G}\left(E_{17}/\mathbb{Q}\right)\langle\sigma\rangle & \longleftrightarrow & L_0 = \mathbb{Q} \end{array}$$

Επειδή η ομάδα $\mathcal{G}(E_{17}/\mathbb{Q})$ είναι κυκλική, οι μόνες υποομάδες της είναι αυτές των οποίων οι τάξεις είναι διαιρέτες του 16 και για κάθε διαιρέτη d υπάρχει ακριβώς μία υποομάδα της $\mathcal{G}(E_{17}/\mathbb{Q})$ τάξεως d. Συνεπώς, το «δίκτυο» υποομάδων της $\mathcal{G}(E_{17}/\mathbb{Q})$ είναι πολύ απλό: αυτό στην αριστερή στήλη του παραπάνω διαγράμματος. Συνεπώς, το «δίκτυο» υποσωμάτων του E_{17} είναι αυτό της δεξιάς στήλης του διαγράμματος. Οι αριθμοί 2, στην αριστερή στήλη δείχνουν τον δείκτη της υποομάδας στην αμέσως μεγαλύτερη υποομάδα και στη δεξιά στήλη δηλώνουν ότι $[L_i : L_{i-1}] = 2$ για $i = 1, \ldots, 4$. Επίσης $\sum_{i=1} \omega^{16} = -1$.

Βήμα 1. Ορίζω

$$\begin{aligned} \eta_1 &:= \omega + \omega^2 + \omega^4 + \omega^8 + \omega^9 + \omega^{13} + \omega^{15} + \omega^{16} \\ \eta_2 &:= \omega^3 + \omega^5 + \omega^6 + \omega^7 + \omega^{10} + \omega^{11} + \omega^{12} + \omega^{14} \end{aligned}$$

Με απλές πράξεις διαπιστώνεται ότι $\sigma(\eta_1) = \eta_2$ και $\sigma(\eta_2) = \eta_1$, άρα $\sigma^2(\eta_i) = \eta_i$ για $i = 1, 2$. Έπεται ότι $\mathbb{Q}(\eta_i) \leq \mathcal{F}(\sigma^2) = L_1$ για $i = 1, 2$. Αφετέρου, $\eta_1 + \eta_2 = \sum_{i=1} \omega^{16} = -1$ και $\eta_1\eta_2 = -4$. Έπεται ότι τα η_i είναι ρίζες του $X^2 + X - 4$, το οποίο είναι ανάγωγο πάνω από το $\mathbb{Q}$. Άρα $\mathbb{Q}(\eta_1) = \mathbb{Q}(\eta_2)$ και $[\mathbb{Q}(\eta_i) : \mathbb{Q}] = 2 = [L_1 : \mathbb{Q}]$, οπότε

$$L_1 = \mathbb{Q}(\eta_1) = \mathbb{Q}(\eta_2) = \mathbb{Q}(\sqrt{17}).$$

Ένας προσεγγιστικός υπολογισμός με υπολογιστή ταυτοποιεί τις ρίζες του $X^2 + X - 4$ με τα η_i:

$$\eta_1 = \tfrac{1}{2}(-1 + \sqrt{17}), \quad \eta_2 = \tfrac{1}{2}(-1 - \sqrt{17}).$$

Βήμα 2. Διασπώ τα η_i ως εξής:

$$\begin{aligned} \eta_1 &= \underbrace{(\omega + \omega^4 + \omega^{13} + \omega^{16})}_{\eta_{11}} + \underbrace{(\omega^2 + \omega^8 + \omega^9 + \omega^{15})}_{\eta_{12}} \\ \eta_2 &= \underbrace{(\omega^3 + \omega^5 + \omega^{12} + \omega^{14})}_{\eta_{21}} + \underbrace{(\omega^6 + \omega^7 + \omega^{10} + \omega^{11})}_{\eta_{22}} \end{aligned}$$

Εύκολα ελέγχω ότι, για $i = 1, 2$ ισχύει $\sigma^2(\eta_{i1} = \eta_{i2}$ και $\sigma^2(\eta_{i2}) = \eta_{i1}$, άρα, για $i, j \in \{1, 2\}$ ισχύει $\sigma^4(\eta_{ij}) = \eta_{ij}$, που σημαίνει ότι $\mathbb{Q}(\eta_{ij}) \leq \mathcal{F}(\sigma^4) = L_2$. Αφετέρου, για $i = 1, 2$ είναι $\eta_{i1} + \eta_{i2} = \eta_i$ (εκ κατασκευής) και διαπιστώνω, ακόμη, ότι $\eta_{i1}\eta_{i2} = -1$, άρα τα η_{i1}, η_{i2} είναι ρίζες του $X^2 - \eta_i X - 1 \in L_1[X]$. Οι ρίζες αυτές δεν μένουν αναλλοίωτες από τον σ^2, άρα δεν ανήκουν στο L_1· συνεπώς, το δευτεροβάθμιο αυτό πολυώνυμο είναι ανάγωγο πάνω από το L_1. Άρα, $\mathbb{Q}(\eta_{i1}) = \mathbb{Q}(\eta_{i2})$ και $[\mathbb{Q}(\eta_{i1}) : L_1] = 2 = [L_2 : L_1]$, οπότε

$$L_2 = \mathbb{Q}(\eta_{i1}) = \mathbb{Q}(\eta_{i2}), \quad i = 1, 2.$$

Ένας προσεγγιστικός υπολογισμός με υπολογιστή ταυτοποιεί, για κάθε $i = 1, 2$, τις ρίζες του $X^2 - \eta_i X - 1$ με τα η_{i1}, η_{21}. Έτσι,

$$\eta_{11} = -\frac{1}{4} + \frac{1}{4}\sqrt{17} + \frac{1}{4}\sqrt{34 - 2\sqrt{17}}, \quad \eta_{21} = -\frac{1}{4} - \frac{1}{4}\sqrt{17} + \frac{1}{4}\sqrt{34 + 2\sqrt{17}}$$

(τα η_{12}, η_{22} δεν θα μας χρειασθούν).

Βήμα 3. Διασπώ το η_{11} ως εξής:

$$\eta_{11} = \underbrace{(\omega + \omega^{16})}_{\eta_{111}} + \underbrace{(\omega^4 + \omega^{13})}_{\eta_{112}}.$$

Δουλεύοντας όπως στο προηγούμενο βήμα δείχνω ότι τα η_{111}, η_{112} είναι ρίζες του $X^2 - \eta_{11}X + \eta_{21}$, το οποίο είναι ανάγωγο πάνω από το L_2 και, συνεπώς,

$$L_3 = \mathbb{Q}(\eta_{111}) = \mathbb{Q}(\eta_{112}).$$

Οι ρίζες του τελευταίου δευτεροβάθμιου πολυωνύμου υπολογίζονται, αφού οι συντελεστές του έχουν ήδη υπολογισθεί στο βήμα 2. Ένας προσεγγιστικός υπολογισμός δείχνει με ποια ρίζα είναι ίσο το $\eta_{111} = \omega + \omega^6 = \omega + \omega^{-1} = 2\cos\theta$. Έτσι βρίσκω ότι

$$2\cos\theta = \frac{\eta_{11} + \sqrt{\eta_{11}^2 - 4\eta_{21}}}{2}.$$

Τώρα, όποιος έχει υπομονή (ή πακέτο συμβολικού υπολογισμού στον υπολογιστή του), υπολογίζει

$$\begin{aligned}\cos\frac{2\pi}{17} = &-\frac{1}{8} + \frac{1}{8}\sqrt{17} + \frac{1}{8}\sqrt{2(17-\sqrt{17})} \\ &+ \frac{1}{8}\sqrt{4(17+3\sqrt{17}) - 2\sqrt{2(17-\sqrt{17})} + 2\sqrt{17}\sqrt{2(17-\sqrt{17})} - 16\sqrt{2(17+\sqrt{17})}}.\end{aligned}$$

Είναι σαφές ότι καθένα από τα επιμέρους «κομμάτια» αυτού του αλγεβρικού αριθμού είναι κατασκευάσιμο.

Ασκήσεις Στις παρακάτω ασκήσεις, όπου ζητείται «γραφική» κατασκευή, εννοείται ότι πρέπει να την κάνετε σχεδιαστικά, πάνω σε χαρτί, χρησιμοποιώντας πραγματικά όργανα (κανόνα και διαβήτη), έχοντας επιλέξει αρχικά ένα ευθύγραμμο τμήμα του οποίου το μήκος είναι το μοναδιαίο (η επιλογή είναι, φυσικά, αυθαίρετη, αρκεί να βολεύει σχεδιαστικά).

Άσκηση 9.27. Έστω c το συνημίτονο της επίκεντρης γωνίας που αντιστοιχεί στην πλευρά κανονικού n-γώνου. Εκφράστε, συναρτήσει του c, το μήκος της πλευράς του κανονικού n-γώνου και εξηγήστε γιατί αυτό είναι κατασκευάσιμος αριθμός.

Άσκηση 9.28. Αναπτύξτε για το κανονικό 5-γωνο «θεωρία» ανάλογη με αυτήν του κανονικού 17-γώνου (είναι, φυσικά, πολύ απλούστερη) και, κατόπιν, κατασκευάστε γραφικά την πλευρά του κανονικού 5-γώνου.

Άσκηση 9.29. Κατασκευάστε γραφικά τον αριθμό $\frac{5}{3}\sqrt[4]{\sqrt{13}+\sqrt{11}}$.

Κεφάλαιο 10

10.1 10^{η} Εβδομάδα

Υπερβατικότητα

Ορισμός 10.1. Έστω 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 $t_1, \dots, t_n \in E$ λέμε ότι είναι αλγεβρικώς εξαρτημένα πάνω από το F (F-αλγεβρικώς εξαρτημένα) αν και μόνο αν υπάρχει κάποιο μη μηδενικό $f \in F[X_1, \dots, X_n]$ τέτοιο, ώστε να επαληθεύεται η ισότητα $f(t_1, \dots, t_n) = 0$. Αν δεν είναι F-αλγεβρικώς εξαρτημένα, τότε 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 $(s_1, \dots, s_n) \in S^n$ *διαφορετικών μεταξύ τους στοιχείων* και για κάθε μη μηδενικό $f \in F[X_1, \dots, X_n]$ ισχύει $f(s_1, \dots, s_n) \neq 0$.
Το $\emptyset$ οίζεται ως αλγεβρικώς ανεξάρτητο.

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

5. Το $S \subseteq E$ παράγει το αλγεβρικώς την 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 την E/F.

Ασκήσεις

Άσκηση 10.2. Έστω E/F επέκταση σωμάτων, $\emptyset \neq S \subseteq E$ και $t \in S$. Δείξτε ότι το $\{t\}$ είναι αλγεβρικώς εξαρτημένο πάνω από το $F(S)$.

Άσκηση 10.3. 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 $n, r \in \mathbb{N}$, $s_1, \dots, s_r \in S$ διαφορετικά μεταξύ τους 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 10.4. Έστω E/F επέκταση σωμάτων και $\emptyset \neq S \subseteq E$. Αν το $t \in E \setminus S$ είναι αλγεβρικό πάνω από το $F(S)$, αποδείξτε ότι υπάρχουν $s_1, \dots, s_r \in S$ διαφορετικά μεταξύ τους τέτοια, ώστε το $\{s_1, \dots, s_r, t\}$ να είναι F-αλγεβρικώς εξαρτημένο.

Άσκηση 10.5. 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 $F(S)$.

Λήμμα 10.6. *Έστω E/F επέκταση σωμάτων, το $S \subseteq E$ παράγει αλγεβρικά την E/F και το $s \in S$ είναι αλγεβρικό πάνω από το $F(S \setminus \{s\})$, τότε και το $S \setminus \{s\})$ παράγει αλγεβρικά την E/F.*

Απόδειξη. Έστω $K = F(S \setminus \{s\})$, οπότε $F(S) = K(s)$. Έχομε τις διαδοχικές επεκτάσεις $F \leq K \leq K(s) = F(S) \leq E$. Εξ υποθέσεως, κάθε μία από τις $E/K(s)$ και $K(s)/K$ είναι αλγεβρική, άρα και η E/K είναι αλγεβρική. Αυτό σημαίνει ότι το $S \setminus \{s\}$ παράγει αλγεβρικά την E/F. □

Πρόταση 10.7. *Έστω η επέκταση E/F και $S \subseteq E$. Τα εξής είναι ισοδύναμα:*

α΄) Το S είναι βάση υπερβατικότητας της E/F.

β΄) Το S είναι maximal μεταξύ των υποσυνόλων του E που είναι F-αλγεβρικώς ανεξάρτητα.

γ΄) Το S είναι minimal μεταξύ των υποσυνόλων του E που παράγουν αλγεβρικώς την E/F.

Απόδειξη. (α΄) $\implies$ (β΄): Έστω ότι το S είναι βάση υπερβατικότητας της E/F. Τοτε το S είναι F-αλγεβρικώς ανεξάρτητο. Έστω F-αλγεβρικώς ανεξάρτητο σύνολο T με $T \supsetneq S$. Έστω $t \in T \setminus S$. Το t είναι αλγεβρικό πάνω από το $F(S)$, άρα από την άσκηση 10.4, υπάρχουν διαφορετικά $s_1, \dots, s_n$ τέτοια που το σύνολο $\{s_1, \dots, s_n, t\}$ να είναι F-αλγεβρικώς εξαρτημένο. Λόγω του ότι $t \notin S$, τα $s_1, \dots, s_n, t$ είναι διαφορετικά και ανήκουν στο F-αλγεβρικώς ανεξάρτητο σύνολο T· άτοπο.

(β΄) $\implies$ (α΄): Εξ υποθέσεως το S είναι F-αλγεβρικώς ανεξάρτητο άρα μένει να δείξομε ότι η επέκταση $E/F(S)$ είναι αλγεβρική. Έστω $t \in E$. Από τη maximal ιδιότητα του S, το σύνολο $S \cup \{t\}$ είναι F-αλγεβρικώς εξαρτημένο, οπότε από την άσκηση 10.5 το t είναι αλγεβρικό πάνω από το $F(S)$.

(α΄) $\implies$ (γ΄): Το S παράγει αλγεβρικά την E/F. Έστω $T \subseteq S$, το οποίο παράγει αλγεβρικά την E/F. Θα δείξομε ότι $T = S$. Το S είναι F-αλγεβρικώς ανεξάρτητο άρα και το T είναι F-αλγεβρικώς ανεξάρτητο, άρα το T είναι βάση υπερβατικότητας της E/F. Από την ισοδυναμία των (α΄) και (β΄), έπεται ότι το T είναι maximal μεταξύ των F-αλγεβρικώς ανεξάρτητων υποσυνόλων του E. Όμως $T \subseteq S$ και το S έιναι F-αλγεβρικώς ανεξάρτητο, άρα $T = S$.

(γ΄) $\implies$ (α΄) : Εξ υποθέσεως, το S παράγει αλγεβρικά την E/F, οπότε μένει να δείξομε ότι το S είναι F-αλγεβρικώς ανεξάρτητο. Αν αυτό δεν ισχύει, τότε υπάρχουν $s_1, \dots, s_r \in S$ διαφορετικά και μη μηδενικό $f \in F[X_1, \dots, X_r]$ ώστε $f(s_1, \dots, s_r) = 0$. Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσομε ότι το s_r όντως εμφανίζεται στην τελευταία ισότητα και έστω $n \geq 1$ ο μέγιστος εκθέτης του s_r στην ισότητα αυτή. Αυτό σημαίνει ότι $f = g_n X_r^n + \cdots + g_1 X_r + g_0$ με τα $g_i \in F[X_1, \dots, X_{r-1}]$ και $g_n(s_1, \dots, s_{r-1}) \neq 0$. Αυτό μας λέει ότι το s_r είναι ρίζα του μη μηδενικού πολυωνύμου

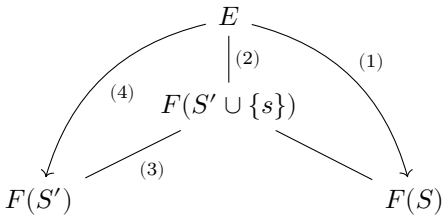
$$g_n(s_1, \dots, s_{r-1}) X_r^n + \cdots + g_1(s_1, \dots, s_{r-1}) X_r + g_0(s_1, \dots, s_{r-1}) \in F(s_1, \dots, s_{r-1})[X_r],$$

άρα το s_r είναι αλγεβρικό πάνω απο το $F(s_1, \dots, s_{r-1})$ άρα αλγεβρικό και πάνω από το $F(S)$. Αλλά τότε, το $T := S \setminus \{s_r\}$ παράγει αλγεβρικά την E/F λόγω του Λημματος 10.6. Αυτό αντιβαίνει στο ότι το S είναι minimal μεταξύ των υποσυνόλων του E που παράγουν αλγεβρικά την E/F. □

Λήμμα 10.8 (Αντικατάσταση στοιχείου σε σύνολο που παράγει αλγεβρικά μια επέκταση)**.** *Έστω επέκταση E/F και $S \subseteq E$ το οποίο την παράγει αλγεβρικά. Έστω $t \in E$ και $s \in S$ αλγεβρικό πάνω από το $S' := (S \setminus \{s\}) \cup \{t\}$. Τότε, το S' παράγει αλγεβρικά την E/F.*

Απόδειξη. Πρέπει και αρκεί να δείξομε ότι η επέκταση $E/F(S')$ είναι αλγεβρική.

Είναι $S' \cup \{s\} = S \cup \{t\}$, άρα $F(S) \leq F(S' \cup \{s\})$. Παρατηρούμε το παρακάτω διάγραμμα:



Η επέκταση (1) είναι αλγεβρική γιατί το S παράγει αλγεβρικά την E/F. Έπεται ότι η επέκταση (2) είναι αλγεβρική. Προφανώς, $F(S' \cup \{s\}) = F(S')(s)$, άρα, από την υπόθεση ότι το s είναι αλγεβρικό πάνω από το $F(S')$, έπεται ότι η επέκταση (3) είναι αλγεβρική. Αφού οι επεκτάσεις (2) και (3) είναι αλγεβρικές, έπεται ότι και η επέκταση (4) είναι αλγεβρική. □

Δίνεται το παρακάτω θεώρημα χωρίς απόδειξη:

Θεώρημα 10.9. *Κάθε επέκταση έχει μία (τουλάχιστον) βάση υπερβατικότητας.*

Παρατήρηση 10.10. Αν η E/F είναι αλγεβρική, τότε βάση υπερβατικότητας αυτής είναι το $\emptyset$.

Θεώρημα 10.11. *Έστω επέκταση E/F. Αν το $\{t_1, \dots, t_m\}$ παράγει αλγεβρικά το E/F και το $S \subseteq E$ είναι F-αλγεβρικώς ανεξάρτητο, τότε $|S| \leq m$.*

Απόδειξη. Έστω ότι το S περιέχει τουλάχιστον $m+1$ στοιχεία (πάω για άτοπο), έστω $s_1, \dots, s_{m+1}$. Πρώτα θα αποδείξω επαγωγικά ότι το $\{s_1, \dots, s_m\}$ παράγει αλγεβρικά την E/F.

Η επέκταση $E/F(t_1, \dots, t_m)$ είναι αλγεβρική, άρα το s_1 είναι αλγεβρικό πάνω από το $F(t_1, \dots, t_m)$, δηλαδή υπάρχει μη μηδενικό πολυώνυμο $f_1 \in F[X_1, \dots, X_{m+1}]$, ώστε $f_1(t_1, \dots, t_m, s_1) = 0$. Μία από τις μεταβλητές $X_1, \dots, X_m$ εμφανίζεται με βαθμό ≥ 1 στο f_1 καθώς, αν αυτό δεν αλήθευε, το πολυώνυμο f_1 θα ήταν μη μηδενικό πολυώνυμο μόνο της μεταβλητής X_{m+1} και θα είχα $f_1(s_1) = 0$, δηλαδή το s_1 θα ήταν αλγεβρικό πάνω από το $F\cdot$ άτοπο, διότι $s_1 \in S$ και το S είναι F-αλγεβρικώς ανεξάρτητο. Δίχως βλάβη της γενικότητας, θεωρώ ότι ο βαθμός του X_1 στο f_1 είναι $r \geq 1$. Τότε η σχέση $f_1(t_1, \dots, t_m, s_1) = 0$ μπορεί να γραφτεί στη μορφή $C_r(t_2, \dots, t_m, s_1)t_1^r + \cdots + C_1(t_2, \dots, t_m, s_1)t_1 + C_0(t_2, \dots, t_m, s_1) = 0$, με τα C_i πολυώνυμα m μεταβλητών πάνω από το F και $C_r(t_2, \dots, t_m, s_1) \neq 0$. Άρα το t_1 είναι αλγεβρικό πάνω από το $F(t_2, \dots, t_m, s_1)$. Από το Λήμμα 10.8, το $\{s_1, t_2, \dots, t_m\}$ παράγει αλγεβρικώς το E/F.

Επαγωγικό βήμα: Έστω $1 \leq i \leq m$ και το $\{s_1, \dots, s_i\} \cup \{m-i$ εκ των $t_1, \dots, t_m\}$ παράγει αλγεβρικά την E/F. Χωρίς βλάβη της γενικότητας μπορώ να υποθέσω ότι το $\{s_1, \dots, s_i\} \cup \{t_{i+1}, \dots, t_m\}$ παράγει αλγεβρικά την E/F. Θα δείξω ότι το $\{s_1, \dots, s_i, s_{i+1}\} \cup \{$ένα λιγότερο από τα $t_{i+1}, \dots, t_m\}$ παράγει αλγεβρικά το E/F. Από την επαγωγική υπόθεση, το s_{i+1} είναι αλγεβρικό πάνω από το $F(s_1, \dots, s_i, t_{i+1}, \dots, t_m)$ άρα υπάρχει μη μηδενικό πολυώνυμο $g \in F[X_1, \dots, X_{m+1}]$ ώστε $g(s_1, \dots, s_i, t_{i+1}, \dots, t_m, s_{i+1}) = 0$. Στο g, κάποια από τις μεταβλητές $X_{i+1}, \dots, X_m$ πρέπει να εμφανίζεται με εκθέτη ≥ 1, αλλιώς θα είχαμε ότι $g(s_1, \dots, s_i, s_{i+1}) = 0$, το οποίο είναι άτοπο καθώς το S είναι F-αλγεβρικώς ανεξάρτητο. Χωρίς βλάβη της γενικότητας, υποθέτω ότι αυτή η μεταβλητή είναι η X_{i+1}. Αυτό, όπως πριν, μας λέει ότι το t_{i+1} είναι ρίζα μη μηδενικού πολυωνύμου του $F[X_1, \dots, X_i, X_{i+1}, \dots, X_m, X_{m+1}]$ άρα το t_{i+1} είναι αλγεβρικό πάνω από το $F(s_1, \dots, s_i, t_{i+2}, \dots, t_m, s_{i+1})$. Εφαρμόζοντας το Λήμμα 10.8, το $\{s_1, \dots, s_{i+1}, t_{i+2}, \dots, t_m\}$ παράγει αλγεβρικώς το E/F.

Έτσι, επαγωγικά, καταλήγομε στο συμπέρασμα ότι το $\{s_1, \dots, s_m\}$ παράγει αλγεβρικά την E/F. Τότε όμως, κάθε στοιχείο του E, άρα και το s_{m+1}, είναι αλγεβρικό πάνω από το $F(s_1, \dots, s_m)$. Τότε, από την άσκηση 10.4, το $\{s_1, \dots, s_m, s_{m+1}\}$ είναι F-αλγεβρικώς εξαρτημένο, συμπέρασμα το οποίο έρχεται σε αντίφαση με την υπόθεση ότι το S είναι F-αλγεβρικώς ανεξάρτητο. □

Πόρισμα 10.12. *Αν S, T είναι βάσεις υπερβατικότητας της E/F και μία από τις δύο είναι πεπερασμένη, τότε και η άλλη είναι πεπερασμένη και σ' αυτή την περίπτωση οι βάσεις είναι ισοπληθείς.*

Απόδειξη. Έστω ότι η T είναι πεπερασμένη. Επειδή το S είναι βάση υπερβατικότητας της E/F άρα είναι F-αλγεβρικώς ανεξάρτητο. Επειδή η T είναι βαση υπερβατικότητας της E/F, παράγει αλγεβρικώς το E/F, άρα $|S| \leq |T|$.

Ξέρω πλέον ότι το S είναι πεπερασμένο. Καθώς οι ρόλοι των S και T είναι πλέον συμμετρικοί, θα έχω και $|T| \leq |S|$ άρα τελικά $|T| = |S|$ □

Θεώρημα 10.13. *Δύο βάσεις υπερβατικότητας μίας οποιασδήποτε E/F είναι ισοπληθείς.*

Απόδειξη. Χάρη στο Πόρισμα 10.12, μένει να εξετάσω την περίπτωση δύο βάσεων υπερβατικότητας, που είναι και οι δύο άπειρες.

Έστω $T = \{t_i : i \in I\}$ όπου το I είναι κάποιο άπειρο σύνολο δεικτών. Κάθε $a \in E$ και ειδικότερα κάθε $s \in S$ ειναι αλγεβρικό πάνω από το $F(T)$, άρα υπάρχουν $i_1, \dots, i_r \in I$ τέτοιο ώστε το S να είναι αλγεβρικό πάνω από το $F(t_{i_1}, \dots, t_{i_r})$. Διαφορετική διατύπωση: Για κάθε $s \in S$ υπάρχει κάποιο πεπερασμένο $I_s \subset I$ με την ιδιότητα: το s είναι αλγεβρικό πάνω από το $F(T_s)$, όπου $T_s = \{t_i : i \in I_s\}$.

Προφανώς $\bigcup_{s\in S} I_s \subseteq$ I. Θα δείξω ότι ισχύει η ισότητα. Αν δεν ίσχυε, τότε υπάρχει κάποιο $j \in I$ με $j \notin I_s \ \forall s \in S$, άρα $t_j \notin T_s \ \forall s \in S$. Συνεπώς, για κάθε $s \in S$ ισχύει $T_s \subset T \setminus \{t_j\}\cdot$ αλλά το s είναι αλγεβρικό πάνω από το $F(T_s)$, άρα είναι αλγεβρικό και πάνω από το $F(T \setminus \{t_j\})$. Έπεται ότι η επέκταση $F(S)/F(T \setminus \{t_j\})$ είναι αλγεβρική. Είναι, όμως, αλγεβρική και η $E/F(S)$ (γιατί το S παράγει αλγεβρικά την E/F), άρα η $E/F(T \setminus \{t_j\})$ είναι αλγεβρική, που σημαίνει ότι το σύνολο $T \setminus \{t_j\}$ παράγει αλγεβρικά την E/F. Καθώς, όμως, το σύνολο αυτό είναι γνήσιο υποσύνολο του T, ερχόμαστε σε αντίφαση με την Πρόταση 10.7 (γ΄). Συνεπως $I = \bigcup_{s\in S} I(s)$.

Στην επόμενη παράγραφο, το σύμβολο $\leq$ είναι μεταξύ άπειρων πληθαρίθμων για τους οποίους ισχύει το (διόλου τετριμμένο) Θεώρημα Schröder-Bernstein: *Αν* $\mathfrak{a} \leq \mathfrak{b}$ *και* $\mathfrak{b} \leq \mathfrak{a}$, *τότε* $\mathfrak{a} = \mathfrak{b}$. Προφανώς, το θεώρημα περιλαμβάνει την περίπτωση πεπερασμένων πληθαρίθμων. Επίσης, $\aleph_0$ («άλεφ μηδέν») είναι ο μικρότερος άπειρος πλήθάριθμος, δηλαδή, αυτός του $\mathbb{N}$ και ισχύει $\mathfrak{a}\aleph_0 = \mathfrak{a}$ για κάθε άπειρο πληθάριθμο $\mathfrak{a}$.

Καθώς τα I_s είναι πεπερασμένα, $|I_s| \leq \aleph_0$, άρα $|T| \leq |S|\aleph_0 = |S|$. Συμμετρικά, ισχύει και το $|S| \leq |T|$, άρα από το Θεώρημα Schröder-Bernstein $|S| = |T|$. □

Ορισμός 10.14. Ο πληθάριθμος μιας οποιαδήποτε βάση υπερβατικότητας μιας επέκτασης E/F ονομάζεται βαθμός υπερβατικότητας της E/F και συμβολίζεται $\operatorname{trdeg}(E/F)$.

Θεώρημα 10.15. *Αν $F \leq K \leq E$ είναι διαδοχικές επεκτάσεις σωμάτων, τότε*

$$\operatorname{trdeg}(E/F) = \operatorname{trdeg}(E/K) + \operatorname{trdeg}(K/F).$$

Η σχέση ισχύει και στην περίπτωση που ένα ή και τα δύο εκ των S, T είναι άπειρα.

Απόδειξη. Έστω S βάση υπερβατικότητας της K/F και T βάση υπερβατικότητας της E/K. Από τον Ορισμό 10.14, είναι $\operatorname{trdeg}(K/F) = |S|$ και $\operatorname{trdeg}(E/K) = |T|$. Από την άσκηση 10.16 είναι $S \cap T = \emptyset$. Συνεπώς, $|S \cup T| = |S| + |T| = \operatorname{trdeg}(K/F) + \operatorname{trdeg}(E/K)$, σχέση η οποία ισχύει και στην περίπτωση που ένα ή και τα δύο εκ των S, T είναι άπειρα. Συνεπώς, αρκεί να δείξω ότι το $S \cup T$ είναι βάση υπερβατικότητας της E/F.

Το $S \cup T$ παράγει αλγεβρικά την E/F. Ισοδύναμα, θα δείξω ότι η επέκταση $E/F(S \cup T)$ είναι αλγεβρική. Πράγματι, το S, ως βάση υπερβατικότητας της K/F, παράγει αλγεβρικά αυτή την επέκταση, άρα η επέκταση $K/F(S)$ είναι αλγεβρική, οπότε και η $K/F(S \cup T)$ είναι αλγεβρική. Επίσης, είναι προφανές ότι κάθε στοιχείο του T είναι αλγεβρικό πάνω από το $F(S \cup T)$, άρα η $K(T)/F(S \cup T)$ είναι αλγεβρική. Τώρα, το T, ως βάση υπερβατικότητας της E/K, παράγει αλγεβρικά αυτή την επέκταση, άρα η $E/K(T)$ είναι αλγεβρική. Συνδυάζοντας τα δύο συμπεράσματα, συνάγομε την αλγεβρικότητα της E/F.

Το $S \cup T$ είναι F-αλγεβρικώς ανεξάρτητο. Πράγματι, έστω ένα οποιοδήποτε πεπερασμένο υποσύνολο $\{s_1, \dots, s_n, t_1, \dots, t_m\}$ του $S \cup T$, με τα s_i διαφορετικά στοιχεία του S και τα t_j διαφορετικά στοιχεία του T, και $f(s_1, \dots, s_n, t_1, \dots, t_m) = 0$ με $f \in F[X_1, \dots, X_n, Y_1, \dots, Y_m]$. Θα δείξω ότι το f είναι το μηδενικό πολυώνυμο.
Το f είναι άθροισμα όρων της μορφής $C_{i_1,\dots,i_m}(X_1, \dots, X_n)Y_1^{i_1} \cdots Y_m^{i_m}$ όπου $C_{i_1,\dots,i_m}(X_1, \dots, X_n) \in F[X_1, \dots, X_n]$. Έστω $g(Y_1, \dots, Y_m) = f(s_1, \dots, s_n, Y_1, \dots, Y_m) \in F(S)[Y_1, \dots, Y_m]$.
Είναι $g(t_1, \dots, t_m) = f(s_1, \dots, s_n, t_1, \dots, t_m) = 0$. Αλλά το $\{t_1, \dots, t_m\}$ είναι K-αλγεβρικώς ανεξάρτητο, άρα και $F(S)$-αλγεβρικώς ανεξάρτητο (αφού $F(S) \leq K$), οπότε η τελευταία ισότητα συνεπάγεται ότι το g είναι το μηδενικό πολυώνυμο του $F(S)[Y_1, \dots, Y_m]$. Άρα καθένα από τα $C_{i_1,\dots,i_m}(s_1, \dots, s_n)$ είναι ίσο με 0. Επειδή το $\{s_1, \dots, s_n\}$ είναι F-αλγεβρικώς ανεξάρτητο, συμπεραίνομε ότι κάθε πολυώνυμο $C_{i_1,\dots,i_m}(X_1, \dots, X_n)$ είναι μηδενικό, άρα, το f είναι μηδενικό πολυώνυμο. □

Ασκήσεις

Άσκηση 10.16. Έστω S, T όπως στην απόδειξη του Θεωρήματος 10.15. Αποδείξτε ότι $S \cap T = \emptyset$.

Άσκηση 10.17. Έστω επέκταση E/F και $S = \{s_1, \dots, s_n\} \subset E$ βάση υπερβατικότητας της E/F. Έστω $m_1, \dots, m_n \in \mathbb{N}$. Αποδείξτε ότι το σύνολο $T = \{s_1^{m_1}, \dots, s_n^{m_n}\}$ είναι, επίσης, βάση υπερβατικότητας της E/F.