

Κεφάλαιο 4

4.1 4^η Εβδομάδα

Ορισμός 4.1. Έστω F σώμα. Ένα σώμα C καλείται αλγεβρική κλειστότητα του F , αν η επέκταση C/F είναι αλγεβρική και το σώμα C είναι αλγεβρικά κλειστό.

Θεώρημα 4.2. Κάθε σώμα διαθέτει αλγεβρική κλειστότητα.

Παράδειγμα 4.3. Το $\mathbb{R}$ έχει αλγεβρική κλειστότητα το $\mathbb{C}$. Το $\mathbb{Q}$ έχει μια αλγεβρική κλειστότητα που συμβολίζεται $\bar{\mathbb{Q}}$.

Πρόταση 4.4. Αν C είναι αλγεβρική κλειστότητα του σώματος F και $\bar{F}$ είναι η αλγεβρική κλειστότητα του F στο C (βλ. Πρόταση 2.17), τότε $\bar{F} = C$.

Απόδειξη. Εξ ορισμού, το $\bar{F}$ είναι υποσύνολο του C και περιέχει όλα τα στοιχεία του C που είναι αλγεβρικά πάνω από το F . Αφετέρου, εξ ορισμού της αλγεβρικής κλειστότητας, η επέκταση C/F είναι αλγεβρική, άρα, $C \subseteq \bar{F}$ και, συνεπώς, $\bar{F} = C$. $\square$

Πρόταση 4.5. 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 αποδείξουμε 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 3.11 και Θεώρημα 3.10).

Αντιστρόφως, έστω ότι κάθε μη σταθερό πολυώνυμο του $F[X]$ διασπάται στο C . Θα δείξουμε ότι το C είναι αλγεβρικά κλειστό. Για τον σκοπό αυτό θεωρούμε ένα μη σταθερό $g \in C[X]$ και αρκεί να δείξουμε ότι το g έχει μια τουλάχιστον ρίζα στο C (Ορισμός 3.11 και Θεώρημα 3.10). Από το Θεώρημα 2.13 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 3.12). 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 $u_1, \dots, u_n \in C$. Επειδή $f(u) = 0$, συμπεραίνουμε ότι $u = u_i$ για κάποιο i , οπότε $u \in C$. $\square$

Θεώρημα 4.6. Σε κάθε διάγραμμα όπως το παρακάτω, στο οποίο η επέκταση E/F είναι αλγεβρική και το C είναι η αλγεβρική κλειστότητα του F , ο σ επεκτείνεται σε μονομορφισμό $\tilde{\sigma} : E \rightarrow F$.

$$\begin{array}{ccc} E & & C \\ | & \nearrow \sigma & \\ F & & \end{array}$$

Θεώρημα 4.7. Αν τα C, C' είναι αλγεβρικές κλειστότητες του ίδιου σώματος τότε είναι F -ισόμορφες, δηλαδή υπάρχει ισομορφισμός $\sigma : C \rightarrow C'$ τ.ω. $\sigma(a) = a \ \forall a \in F$.

Απόδειξη. Στο διάγραμμα του Θεωρήματος 4.6 θέτω C στη θέση του E , C' στη θέση του C και στη θέση του σ την ταυτοτική εμφύτευση $\iota : F \rightarrow C'$ ($\iota(c) = c \ \forall c \in F$). Συμπεραίνω ότι υπάρχει μονομορφισμός $\phi : C \hookrightarrow C'$. Το σώμα $K = \phi(C)$ είναι ισόμορφο με το C , άρα είναι αλγεβρικά κλειστό (άσκηση 4.29 (1)). Το K είναι αλγεβρικά κλειστό υπόσωμα του αλγεβρικά κλειστού C' , άρα $K = C'$ (άσκηση 4.29 (2)), δηλαδή, ο ϕ είναι «επί», άρα, τελικά, ο ϕ είναι ισομορφισμός. $\square$

Θεώρημα 4.8. Έστω $\sigma : F \rightarrow F'$ ισομορφισμός και C, C' αλγεβρικές κλειστότητες των F, F' τότε ο σ επεκτείνεται σε ισομορφισμό $C \rightarrow C'$.

Διαχωρισιμότητα

Ορισμός 4.9. 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 $u_1, \dots, u_n \in K$ διαφορετικά μεταξύ τους και $c \in F$ είναι ο συντελεστής του μεγιστοβαθμίου όρου του f .

Παρατήρηση 4.10. 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 $\sigma : K \rightarrow K'$ (Θεώρημα 3.8). Αυτός επεκτείνεται σε ισομορφισμό δακτυλίων $\sigma : K[X] \rightarrow K'[X]$ (Παρατήρηση 3.1). Άρα, εφαρμόζοντας στη σχέση $f = (X - \alpha)^r g$ αυτόν τον ισομορφισμό, παίρνουμε $f = \sigma f = (X - \sigma(\alpha))^r \sigma g$ (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 4.11. 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 «νομομοποιεί» τον ορισμό 4.9.

Ορισμός 4.12 (Συνέχεια του Ορισμού 4.9). Ένα μη σταθερό $f \in F[X]$ χαρακτηρίζεται διαχωρίσιμο αν όλοι οι ανάγωγοι παράγοντες του είναι διαχωρίσιμοι.

Παράδειγμα 4.13. 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 $\pm i\sqrt{3}$ αντιστοίχα).

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

Ορισμός 4.14. 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 πολλαπλασιασμό $(fg)' = f'g + fg'$. Οι αποδείξεις τους συμβολικές (formal).

Πρόταση 4.15. 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, $f'|g$.

Αντιστρόφως. Αν f και f' έχουν μη σταθερό κοινό διαιρέτη στο $F[X]$, θα δείξουμε ότι το f έχει πολλαπλή ρίζα. Ισοδύναμα (αντιστροφο-αντίθετη συνεπαγωγή): Αν το f δεν έχει πολλαπλή ρίζα (δηλαδή έχει μόνο απλές ρίζες) θα δείξουμε, με επαγωγή στον $\deg f$, ότι τα f και f' δεν έχουν μη σταθερό κοινό διαιρέτη. Αν $\deg f = 1$, ο ισχυρισμός είναι προφανής, αφού το f' είναι σταθερό πολυώνυμο. Έστω $d > 2$ και υποθέτουμε ότι κάθε πολυώνυμο στο $F[X]$ με βαθμό $< d$ που έχει μόνο απλές ρίζες, δεν έχει μη σταθερό κοινό διαιρέτη με την παράγωγό του. Τώρα, θεωρούμε $f \in K[X]$ με $\deg f = d$, που έχει μόνο απλές ρίζες. Έστω ότι τα f, f' είχαν μη σταθερό κοινό διαιρέτη $g \in K[X]$ (πάμε για άτοπο). Έστω $\beta \in C$ ρίζα του g . Τότε $f(\beta) = 0 = f'(\beta)$. Επίσης $f(X) = (X - \beta)h(X)$, όπου $h \in F(\beta)[X]$ και $h(\beta) \neq 0$, διότι το f δεν έχει πολλαπλές ρίζες. Παίρνοντας τυπική παράγωγο βρίσκουμε $f'(X) = (X - \beta)h'(X) + h(X)$ και από αυτή τη σχέση έπεται ότι $f'(\beta) = h(\beta) \neq 0$, οπότε οδηγηθήκαμε σε αντίφαση. $\square$

Πόρισμα 4.16. 1. Αν $\text{char}(F) = 0$, τότε κάθε ανάγωγο $f \in F[X]$ είναι διαχωρίσιμο.

2. Αν $\text{char}(F) = p$ (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

$$f(X) = c_0 + c_1 X^{m_1 p} + c_2 X^{m_2 p} + \dots + c_r X^{m_r p}, \quad c_1, c_2, \dots, c_r \neq 0. \quad (4.1)$$

Απόδειξη. 1. Αν $f = a_n X^n + \dots + a_0$, $n \geq 1$, $a_n \neq 0$, τότε $f' = n a_n X^{n-1} + \dots + a_1 \neq 0$ καθώς $n a_n \neq 0$. Αν το f δεν είναι διαχωρίσιμο, τότε (από την Πρόταση 4.15) 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 (4.1), τότε, παραγωγίζοντας, βλέπουμε 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 4.15, μας λέει ότι το f έχει πολλαπλή ρίζα.

Αντιστρόφως, έστω ότι το f έχει πολλαπλή ρίζα. Τότε, από την Πρόταση 4.15, 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 καταλήγουμε 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 γράψουμε μόνο τους μη μηδενικούς όρους του)

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

Παραγωγίζοντας έχουμε

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

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 $i = 1, \dots, r$ βλέπουμε ότι το f είναι της μορφής (4.1). $\square$

Την καλή ιδιότητα των σωμάτων χαρακτηριστικής 0, έχουν και τα πεπερασμένα σώματα, όπως θα δούμε, παρακάτω, στην Πρόταση 4.20. Πιο πριν υπενθυμίζουμε κάποια πράγματα.

Υπενθύμιση 4.17. Κάθε πεπερασμένο σώμα έχει πληθάρημο $q = p^n$, 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 4.18. (Freshman's Dream)¹ Αν $\text{char}(F) = p$, τότε $(a + b)^p = a^p + b^p$

Απόδειξη.

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

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

Ορισμός 4.19. Έστω σώμα F πεπερασμένο χαρακτηριστικής p . Η απεικόνιση $a \mapsto a^p$ λέγεται *αυτομορφισμός του Frobenius*.

Ο χαρακτηρισμός «αυτομορφισμός» δικαιολογείται ως εξής: Από την υπενθύμιση 4.18, η απεικόνιση $a \mapsto a^p$ 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 απεικόνιση είναι 1-1, θα είναι και επί.

Πρόταση 4.20. 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 Πρόσλημμα 4.16 (2), $f(X) = c_0 + c_1 X^{m_1 p} + c_2 X^{m_2 p} + \dots + c_r X^{m_r p}$. Από τον αυτομορφισμό του Frobenius, $\forall c_i \exists a_i \in F$ τ.ω. $a_i^p = c_i$. Οπότε

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

άτοπο διότι το f είναι ανάγωγο. □

Ορισμός 4.21. 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 4.22. Έστω διαδοχικές επεκτάσεις $K/E/F$. Αν η K/F είναι διαχωρίσιμη, τότε οι επεκτάσεις E/F και η K/E είναι 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 2.21), 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 4.23. 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 $\sigma : F(\alpha) \rightarrow F(\beta)$ με $\sigma(\alpha) = \beta$. (Ο σ επεκτείνει τον id_F). Έστω $\tau : C \rightarrow C$ που επεκτείνει τον σ η ύπαρξη του οποίου εξασφαλίζεται από το 4.8. Έστω $r \geq 1$ η πολλαπλότητα του α στο f , τότε $f = (X - \alpha)^r g(X)$ με $g \in F(\alpha)[X]$, $g(\alpha) \neq 0$. Τότε $f = \sigma f = (X - \sigma(\alpha))^r \sigma g = (X - \beta)^r \sigma g$. Όμως $g(\alpha) \neq 0$ άρα $\sigma g(\sigma(\alpha)) \neq 0$ άρα $\sigma g(\beta) \neq 0$ που σημαίνει ότι η β είναι πολλαπλότητας r στο f . □

¹Το «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....

Πόρισμα 4.24. 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 4.25. Έστω E/F πεπερασμένη και $a_1, \dots, a_n \in E$ είναι βάση της. Τότε $E = F(a_1, \dots, a_n)$.

Λήμμα 4.26. Έστω C αλγεβρική κλειστότητα του F , C' αλγεβρική κλειστότητα του F' , $\sigma : F \rightarrow F'$ ισομορφισμός και E/F πεπερασμένη. Τότε ο σ μπορεί να επεκταθεί σε μονομορφισμό $\tau : E \hookrightarrow C'$ με το πολύ, πεπερασμένο πλήθος τρόπων.

Άλλη διατύπωση : Υπάρχει πεπερασμένο πλήθος εμφυτεύσεων $\tau : E \hookrightarrow C'$ που επεκτείνουν τον σ .

$$\begin{array}{ccc} C & & C' \\ | & & | \\ E & \xrightarrow[\sim]{\tau} & \tau(E) \\ | & & | \\ F & \xrightarrow[\sim]{\sigma} & F' \end{array}$$

Απόδειξη. Έστω $\alpha_1, \dots, \alpha_n$ μία βάση της επέκτασης E/F . Έστω ο τυπικός $\tau : E \hookrightarrow C'$. Αφού κάθε στοιχείο στο E γράφεται ως $e = c_1\alpha_1 + \dots + c_n\alpha_n$ με $c_1, \dots, c_n \in F$. Άρα

$$\begin{aligned} \tau(e) &= \tau(c_1)\tau(\alpha_1) + \dots + \tau(c_n)\tau(\alpha_n) \\ &= \tau(c_1)\sigma(\alpha_1) + \dots + \sigma(c_n)\tau(\alpha_n) \end{aligned}$$

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 πιθανές τιμές του $\tau(\alpha)$ είναι πεπερασμένες το πλήθος. Πράγματι, έστω $X^k + c_{k-1}X^{k-1} + \dots + c_1X + c_0 \in F[X]$ το ελάχιστο πολυώνυμο του α . Τότε, $\alpha^k + c_{k-1}\alpha^{k-1} + \dots + c_1\alpha + c_0 = 0$ και εφαρμόζοντας τον τ ,

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

Άρα το $\tau(\alpha)$ είναι ρίζα του $\sigma \text{Irr}(\alpha, F)$, οπότε το πλήθος των δυνατών τιμών του $\tau(\alpha)$ είναι πεπερασμένο. $\square$

Θεώρημα 4.27. Έστω C αλγεβρική κλειστότητα του F , C' αλγεβρική κλειστότητα του F' , $\sigma : F \rightarrow F'$ ισομορφισμός και E/F πεπερασμένη ($E \subseteq C$). Τότε το πλήθος των μονομορφισμών $\tau : E \hookrightarrow C'$ που επεκτείνουν τον σ όπως στο διάγραμμα του Λήμματος 4.26 (ήδη ξέρω από το λήμμα ότι είναι πεπερασμένο) είναι ανεξάρτητο από των F', C', σ και εξαρτάται μόνο από την επέκταση E/F .

Ορισμός 4.28. Το πλήθος των τ που ικανοποιούν το δεξιά διάγραμμα είναι ίσο με το πλήθος των τ που ικανοποιούν το αριστερό. Δηλαδή το πλήθος των F -μονομορφισμών $\tau : E \hookrightarrow C$ είναι ίσο με το πλήθος των τ στο πρώτο διάγραμμα. Αυτό το πλήθος συμβολίζεται με $\{E : F\}$ και ονομάζεται δείκτης της E/F .

Απόδειξη. Στο παρακάτω διάγραμμα

$$\begin{array}{ccccc} & & \lambda & & \\ & C'_1 & & C & C'_2 \\ & | & & | & | \\ \tau_1(E) & \xleftarrow{\tau_1} & E & \xrightarrow{\tau_2} & \tau_2(E) \\ & | & & | & | \\ F'_1 & \xleftarrow{\sigma_1} & F & \xrightarrow{\sigma_2} & F'_2 \end{array}$$

θεωρώ δύο «αντίγραφα» του διαγράμματος του Λήμματος 4.26, το ένα αριστερά, με $(F', \sigma, C') = (F'_1, \sigma_1, C'_1)$ και το δεύτερο δεξιά, με $(F', \sigma, C') = (F'_2, \sigma_2, C'_2)$. Τα τ_1 και τ_2 επεκτείνουν τους σ_1 και σ_2 αντίστοιχα. Έστω $T_1 = \{\tau_1 \text{ του αριστερού διαγράμματος}\}$ και $T_2 = \{\tau_2 \text{ του δεξιού διαγράμματος}\}$. Θέλω να δείξω ότι $|T_1| = |T_2|$. Θα δείξω ότι σε κάθε $\tau_1 \in T_1$ αντιστοιχεί μονοσήμαντα ένα $\tau_2 \in T_2$. οπότε θα έχω δείξει ότι υπάρχει 1-1 απεικόνιση από το T_1 στο T_2 . Λόγω συμμετρίας, υπάρχει 1-1 απεικόνιση και από το T_2 στο T_1 άρα $|T_1| = |T_2|$.

Ποια είναι η 1-1 αντιστοιχία $T_1 \rightarrow T_2$;

Έχω τον ισομορφισμό $\sigma_2 \sigma_1^{-1} : F'_1 \rightarrow F'_2$. Βάσει του Θεωρήματος 4.8, ο $\sigma_2 \sigma_1^{-1}$ επεκτείνεται σε ισομορφισμό $\lambda : C'_1 \rightarrow C'_2$. Τότε ορίζω αντιστοιχία $\psi : T_1 \rightarrow T_2$ $\tau_1 \mapsto \lambda \tau_1 =: \tau_2$.

Πρέπει να δείξω ότι είναι 1-1 και επεκτείνει τον σ_2 . Επεκτείνει τον σ_2 καθώς

$$\tau_2(c) = \lambda \tau_1(c) = \lambda(\sigma_1(c)) = \lambda(\sigma_1(c)) = \lambda \tau_1(c) = \sigma_2(c)$$

για κάθε $c \in F$. Επίσης είναι 1-1, καθώς έχει αντίτροφη την $\tau_2 \mapsto \lambda^{-1} \tau_2$. □

Ασκήσεις

Άσκηση 4.29. 1. Αν δύο σώματα είναι ισόμορφα και το ένα είναι αλγεβρικά κλειστό, αποδείξτε ότι και το άλλο είναι αλγεβρικά κλειστό.

2. Αν το αλγεβρικά κλειστό σώμα K είναι υπόσωμα του αλγεβρικά κλειστού σώματος C και η επέκταση C/K είναι αλγεβρική, αποδείξτε ότι $K = C$.

3. Αν C είναι αλγεβρική κλειστότητα του F και το σώμα E είναι επέκταση του F η οποία περιέχεται στο C , δείξτε ότι C είναι αλγεβρική κλειστότητα του E .

Άσκηση 4.30. Έστω E/F αλγεβρική επέκταση και C αλγεβρική κλειστότητα του E . Αποδείξτε ότι το C είναι αλγεβρική κλειστότητα και για το F .

Άσκηση 4.31. Έστω C αλγεβρική κλειστότητα του F , ανάγωγο $f \in F[X]$ και $\alpha, \beta \in C$ ρίζες του f . Αποδείξτε ότι υπάρχει F -ισομορφισμός $C \rightarrow C$, που στέλνει το α στο β .

Άσκηση 4.32. Έστω πρώτος p και $a \in \mathbb{F}_p$. Παραγοντοποιήστε στο $\mathbb{F}_p[X]$ το πολυώνυμο $X^p - a$.

Άσκηση 4.33. Έστω πρώτος p , σώμα F χαρακτηριστικής p και $u \in F$. Υποθέτουμε 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 4.34. 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 $K = \mathbb{Q}(\rho, i)$ 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 .