Κεφάλαιο 2

2.1 2^{η} Εβδομάδα

Σχόλιο 2.1 (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 2.2. Το $\mathbb{C} = \{(a, b) : a, b \in \mathbb{R}\}$ με πράξεις

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2 + b_1b_2, a_1b_2 + a_2b_1)$$

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 2.3. 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 υπάρει 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

$$p(X) = a_nX^n + \cdots + a_1X + a_0 \in F[X],$$

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

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

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

Θεώρημα 2.4. *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 του F) με τις εξής δυνατότητες:*

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 2.10.

Ορισμός 2.5. Έστω σώμα F. Το σώμα E χαρακτηρίζεται επέκταση του F (συμβολίζεται E/F) αν και μόνο αν το F είναι υπόσωμα του E.

Παρατήρηση 2.6. Η επέκταση E/F είναι F-διανυσματικός χώρος. Στην περίπτωση που $F \subseteq E$ και $i : F \mapsto E$ είναι ο μονομορφισμός μέσω του οποίου θεωρούμε το F υπόσωμα του E ορίζομε τον πολλαπλασιασμό επί βαθμωτό μέσω της $av = i(a)v$ για κάθε $a \in F, v \in E$.

Ορισμός 2.7. Τη διάσταση του F-διανυσματικού χώρου E (άπειρη ή πεπερασμένη) ονομάζουμε βαθμό της επέκτασης E/F και τη συμβολίζομε $[E : F]$.

Θεώρημα 2.8. *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. 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 $u = \sum'_{j\in J}\left(\sum'_{i\in I} f_{ji}a_i\right)b_j = \sum'_{i\in I, j\in J} f_{ji}a_ib_j$, οπότε το u είναι F-γραμμικός συνδυασμός των a_ib_j.

(ii) Το S είναι F-γραμμικά ανεξάρτητο.
Απόδειξη: Έστω ένα πεπερασμένο υποσύνολο του $\{a_ib_j\}_{i\in I, j\in J}$. Δηλαδή, έστω πεπερασμένο $I_0 \subseteq I$ και πεπερασμένο $J_0 \subseteq J$. Θα δείξω ότι το $\{a_ib_j\}_{i\in I_0, j\in J_0}$ είναι F-γραμμικώς ανεξάρτητο. Έστω $\sum_{i\in I_0, j\in J_0} c_{ij}a_ib_j = 0$ 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 2.9. Το Θεώρημα 2.8 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 $[E_{i+1} : E_i]$ είναι 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 2.8.

Ερώτημα 2.10. 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 2.4, ισχύει $F[u] = F(u)$.

Ορισμός 2.11. Έστω επέκταση E/F. Το $e \in E$ λέμε ότι είναι αλγεβρικό πάνω από το F αν υπάρχει μη μηδενικό πολυώνυμο $f \in F[X]$ τ.ω. $f(e) = 0$. Αν όχι, 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 2.12. *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 2.13. *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 $f \in F[X]$ τ.ω. $f(\alpha) = 0$. 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 2.12, δεν υπάρχει άλλο μονικό ανάγωγο στο F[X] με ρίζα το α.

(ii) Γενικά ισχύει

$$F[\alpha] \subseteq F(\alpha) \tag{2.1}$$

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 (2.1) 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 2.12. □

Ορισμός 2.14. Το ανάγωγο πολυώνυμο $p \in F[X]$ του πρώτου σκέλους του Θεωρήματος 2.13 καλείται ελάχιστο πολυώνυμο του α πάνω από το F.

Παρατήρηση 2.15. 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 $X-\sqrt{2}$.

Πρόταση 2.16. *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. $c_0+c_1e+\cdots+c_ne^n=0$. Δηλαδή το e είναι ρίζα του μη μηδενικού πολυωνύμου $c_0+c_1X+\cdots+c_nX^n\in F[X]$, άρα το e είναι αλγεβρικό πάνω από το F. □

Πρόταση 2.17. *Έστω επέκταση E/F. Θεωρώ το ενδιάμεσο υποσύνολο*

$$\bar{F}=\{\alpha\in E:\alpha \text{ αλγεβρικό πάνω από το } F\}.$$

Το $\bar{F}$ είναι σώμα, υπόσωμα του E και, φυσικά, η επέκταση $\bar{F}/F$ είναι αλγεβρική.

Το $\bar{F}$ λέγεται αλγεβρική κλειστότητα του F στο E.

Απόδειξη. Αρκεί να δείξω ότι για $a,b\in\bar{F}$ με $b\notin 0$ είναι και $a-b$ και $ab^{-1}\in\bar{F}$. 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 2.13 (iii). Τότε, από το Θεώρημα 2.8 συμπεραίνομε ότι η επέκταση $F(a,b)/F$ είναι πεπερασμένη, άρα αλγεβρική, βάσει της Πρότασης 2.16. Άλλα προφανώς, $a-b, ab^{-1}\in F(a,b)$ άρα είναι αλγεβρικά πάνω από το F και συνεπώς ανήκουν στο $\bar{F}$. □

Ορισμός 2.18. 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 $f[X_1,\dots,X_n]$, $g[X_1,\dots,X_n]\in F[X_1,\dots,X_n]$ τ.ω. $g(s_1,\dots,s_n)\neq 0$ 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 2.19. *Έστω επέκταση σωμάτων E/F, S μη κενό υποσύνολο του E και το σύνολο $F(S)$ του Ορισμού 2.18. Ισχύουν το εξής: Το $F(S)$ σώμα και, μάλιστα, είναι το ελάχιστο υπόσωμα του E που περιέχει το F και το S.*

Απόδειξη. Κατ' αρχάς θα δείξουμε ότι πρόκειται για 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 ακολουθεί εύκολα, καθώς αν $\frac{f(s_1,\dots,s_n)}{g(s_1,\dots,s_n)}$ είναι μη μηδενικό στοιχείο του $F(S)$, τότε $f(s_1,\dots,s_n)\neq 0$ και το αντίστροφο του $\frac{g(s_1,\dots,s_n)}{f(s_1,\dots,s_n)}$ είναι επίσης στο $F(S)$.

Έχοντας αποδείξει ότι είναι υπόσωμα, μένει να αποδείξουμε ότι είναι το ελάχιστο υπόσωμα που περιέχει τα F και S. Αν E είναι υπόσωμα του E με $F\cup S\subseteq E$, θα δείξουμε ότι $F(S)\subseteq E$. Έστω

$\frac{f(s_1,\dots,s_n)}{g(s_1,\dots,s_n)}$ το τυπικό στοιχείο του $F(S)$. Αφού το E 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 $f(s_1,\dots,s_n), g(s_1,\dots,s_n) \in E$. Επίσης, αφού $g(s_1,\dots,s_n) \neq 0$ και το E είναι σώμα, έπεται ότι και το $g(s_1,\dots,s_n)^{-1}$ ανήκει στο E. Τελικά, απο αυτό συμπεραίνομε ότι και $\frac{f(s_1,\dots,s_n)}{g(s_1,\dots,s_n)} = f(s_1,\dots,s_n)g(s_1,\dots,s_n)^{-1} \in E$ και $F(S) \subseteq E$. □

Ασκήσεις

Άσκηση 2.20. Έστω πεπερασμένη επέκτταση 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.

Άσκηση 2.21. 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 2.22. Η άσκηση αυτή μας δίνει ένα παράδειγμα επέκτασης η οποία είναι αλγεβρική αλλά όχι πεπερασμένη.

Θεωρήστε την αλγεβρική κλειστότητα $\bar{\mathbb{Q}}$ του $\mathbb{Q}$ στο $\mathbb{R}$. Εξ ορισμού της αλγεβρικής κλειστότητας (δείτε την Πρόταση 2.17, η επέκταση $\bar{\mathbb{Q}}/\mathbb{Q}$ είναι αλγεβρική. Έστω πρώτος p και ακέραιος $n \geq 2$. Αποδείξτε τα εξής:

(i) Το ελάχιστο πολυώνυμο του $\sqrt[n]{p}$ πάνω από το $\mathbb{Q}$ είναι το $X^n - p$.

Υπόδειξη: Θυμηθήτε το *κριτήριο Eisenstein*.

(ii) Η επέκταση $\bar{\mathbb{Q}}/\mathbb{Q}$ δεν είναι πεπερασμένη.

Άσκηση 2.23. 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 2.13, ο βαθμός της επέκτασης είναι 3 και κάθε στοιχείο του $\mathbb{Q}(u)$ είναι της μορφής $c_0 + c_1u + c_2u^2$, με τα c_i ρητούς αριθμούς. Γράψτε το στοιχείο $(u^2 + u - 1)^{-1}$ με τη μορφή $c_0 + c_1u + c_2u^2$.

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.