

Κεφάλαιο 3

3.1 3^η Εβδομάδα

Παρατήρηση 3.1. Έστω $\phi : K \rightarrow K'$ ισομορφισμός σωμάτων. Τότε ο ϕ επεκτείνεται σε ισομορφισμό δακτυλίων $K[X] \rightarrow K'[X]$ τέτοιον ώστε $X \mapsto X$. Συνήθως θα χρησιμοποιούμε και για αυτόν το γράμμα ϕ . Αυτός θα οριστεί να στέλνει

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

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 3.2. Έστω $\phi : F \rightarrow F'$ ισομορφισμός σωμάτων, $p \in F[X]$ ανάγωγο και $p' = \phi p \in F'[X]$. 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 $\tilde{\phi} : F[u] \rightarrow F'[u']$ τ.ω. $\tilde{\phi}(u) = u'$.

Απόδειξη. (Σκιτσάρισμα) Ο $\tilde{\phi}$ ορίζεται ως εξής:

$$\tilde{\phi}(c_0 + c_1u + \dots + c_nu^n) := \phi(c_0) + \phi(c_1)u' + \dots + \phi(c_n)u'^n.$$

Αποδεικτέο $\tilde{\phi}$ είναι ομομορφισμός σωμάτων, $\tilde{\phi}$ 1-1 και $\tilde{\phi}$ επί. Θα δείξω μόνο ότι ο $\tilde{\phi}$ είναι 1-1.

Αν έχω δείξει ότι ο $\tilde{\phi}$ είναι ομομορφισμός, τότε αρκεί να δείξω ότι $\ker \tilde{\phi} = \{0\}$. Έστω ότι $f(X) = c_0 + c_1X + \dots + c_nX^n \in F[X]$ και $\tilde{\phi}(c_0 + c_1u + \dots + c_nu^n) = 0$. Η σχέση αυτή συνεπάγεται ότι $\implies \phi(c_0) + \phi(c_1)u' + \dots + \phi(c_n)u'^n = 0$, που σημαίνει ότι το $u' \in F'$ είναι ρίζα του ϕf . Αφού ο $\phi : F[X] \rightarrow F'[X]$ είναι ισομορφισμός δακτυλίων (βλ. Παρατήρηση 3.1) και το p είναι ανάγωγο στο $F[X]$, έπεται και ότι το p' είναι ανάγωγο στο $F'[X]$.

Έχουμε λοιπόν ότι το ϕf έχει κοινή ρίζα με το p' , το οποίο είναι ανάγωγο. Άρα $p' \mid \phi f$. Άρα $\exists g' \in F'[X]$ τέτοιο ώστε $\phi p = p'g'$. Όμοια όντας ισομορφισμός ο ϕ , $f = pg$ άρα $f(u) = 0$. $\square$

Ορισμός 3.3. 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 $u_1, \dots, u_n \in K$ τ.ω. $f(X) = c(X - u_1) \dots (X - u_n)$.
- ii) $K = F[u_1, \dots, u_n] = F[u_1, \dots, u_n]$

Ορισμός 3.4. Τη συνθήκη (i) του παραπάνω ορισμού διατυπώνουμε ισοδύναμα λέγοντας ότι το f διασπάται στο F . Άρα, λέγοντας ότι το f διασπάται στο F , καταλαβαίνουμε ότι, αν αναλύσουμε το f σε ανάγωγα πολυώνυμα του $F[X]$, όλα αυτά τα πολυώνυμα είναι πρώτου βαθμού.

Πρόταση 3.5. Έστω K/F σώμα διάσπασης του $f \in K[X]$ και E ενδιάμεση επέκταση, δηλαδή, $F \subseteq E \subseteq K$. 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 $E = K$. $\square$

Θεώρημα 3.6. 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 $f = p_1 \cdots p_k$. 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 2.4. 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 $f(X) = (X - u_1) \cdots (X - u_{n-1})(X - u_n)c$ όπου $c \in F$. $\square$

Πρόταση 3.7. 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. Έχουμε τον παρακάτω «πύργο» επεκτάσεων:

$$\begin{array}{c}
 F[e_1, \dots, e_n] \\
 | \\
 F[e_1, \dots, e_{n-1}] \\
 | \\
 \vdots \\
 | \\
 F[e_1, \dots, e_{i-1}, e_i] \\
 | \\
 F[e_1, \dots, e_{i-1}] \\
 | \\
 \vdots \\
 | \\
 F[e_1, e_2] \\
 | \\
 F[e_1] \\
 | \\
 F
 \end{array}$$

Εφαρμόζουμε το Θεώρημα 2.13 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 2.9 συμπεραίνουμε ότι η επέκταση $F[e_1, \dots, e_n]/F$ είναι πεπερασμένη. $\square$

Θεώρημα 3.8. 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 πολωνύμου $f \in F[X]$ πάνω από το F και K' σώμα διάσπασης του πολωνύμου $\phi f = f' \in F'[X]$ πάνω από το F' , μπορεί να συμπληρωθεί με ένα ισομορφισμό $\tilde{\phi} : K \rightarrow K'$ ο οποίος επεκτείνει τον ϕ .

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

Αν $d = 1$, τότε (άσκηση 3.13 (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 3.5 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 μπορώ ο ϕ μπορεί να επεκταθεί σε ισομορφισμό $\tilde{\phi} : K \rightarrow K'$. 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 του p , έστω α στο K και μία οποιαδήποτε ρίζα α' του $p' = \phi p$ στο K' . Από την πρόταση 3.2, ξέρω ότι ο $\phi_1 : F_1 := F[\alpha] \rightarrow F'_1 := F'[\alpha']$, τ.ω. $\phi_1(\alpha) = \alpha'$.

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 3.13 (iii), το K είναι σώμα διάσπασης του f πάνω από το F_1 και το K' σώμα διάσπασης του f' πάνω από το F'_1 . Εφαρμόζεται η επαγωγική υπόθεση, άρα ο ϕ_1 επεκτείνεται σε ισομορφισμό $\tilde{\phi} : K \rightarrow K'$. Προφανώς ο $\tilde{\phi}$ είναι επέκταση του ϕ . $\square$

Πόρισμα 3.9. Αν το $f \in F[X]$ είναι μη μηδενικό, τότε όλα τα σώματα διάσπασης του f πάνω από το F είναι F -ισόμορφα, δηλαδή αν K, K' είναι σώματα διάσπασης του f πάνω από το F τότε υπάρχει ισομορφισμός $\psi : K \rightarrow K'$ τ.ω. $\psi(\alpha) = \alpha \forall \alpha \in F$.

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

Επόμενος στόχος: Να εξετάσω αν υπάρχει, για κάθε σώμα F , μια επέκταση C/F που να έχει ανάλογες “καλές” ιδιότητες όπως η επέκταση $\mathbb{C}/\mathbb{R}$. Δηλαδή ότι κάθε $f \in \mathbb{R}[X]$ μη σταθερό, αναλύεται σε πρωτοβάθμια του $\mathbb{C}[X]$. Δηλαδή θέλω να εξετάσω αν για κάθε σώμα F υπάρχει επέκταση C/F ώστε κάθε μη σταθερό πολυώνυμο του $F[X]$ να αναλύεται πλήρως σε πρωτοβάθμια του $C[X]$.

Θεώρημα 3.10. 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 $C[X]$.
3. Κάθε ανάγωγο του $C[X]$ είναι πρωτοβάθμιο.
4. Δεν υπάρχει γνήσια αλγεβρική επέκταση του C .

Ορισμός 3.11. Κάθε σώμα που ικανοποιεί τις παραπάνω ισοδύναμες συνθήκες χαρακτηρίζεται αλγεβρικά κλειστό.

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

(2) $\implies$ (3) : Απλούστατο.

(3) $\implies$ (4) : Έστω D/C αλγεβρική επέκταση του C . Έστω ένα $a \in D$ 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 ου p , ανήκει στο C .

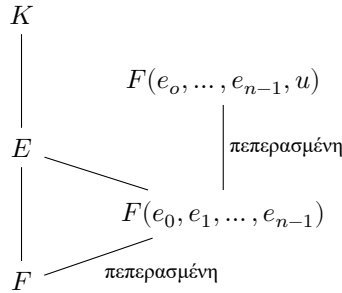
(4) $\implies$ (1) : Έστω μη σταθερό $f \in C[X]$ και έστω ότι δεν είχε καμία ρίζα στο C . Έστω p ανάγωγος παράγοντας του f . Τότε από το Θεώρημα 2.4 θα μπορούσα να βρω K/C για την οποία ισχύουν τα εξής. $\exists \alpha \in K$ τ.ω. $p(\alpha) = 0$ και $K = C[\alpha]$. Αλλά τότε $\deg(p) > 1$, αλλιώς το $\alpha \in C$. Επίσης, $[K : C] = \deg(p) > 1$ άρα το K είναι γνήσια αλγεβρική επέκταση του C , που αντιφάσκει στην υπόθεση. $\square$

Θεώρημα 3.12. 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

$$u^n + e_{n-1}u^{n-1} + \dots + e_1u + e_0 = 0$$

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



Η επέκταση $F(e_0, \dots, e_{n-1})/F$ είναι πεπερασμένη, καθώς όλα τα $e_0, \dots, e_{n-1}$ είναι αλγεβρικά πάνω από το F (Πρόταση 3.7). 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 . $\square$

Ασκήσεις

Άσκηση 3.13. Οι απαντήσεις στα 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 $f \in F[X]$ και $[K : F] = 1$, τότε $K = F$.
- (iii) Αν το K είναι σώμα διάσπασης του $f \in F[X]$ πάνω από το K και E είναι ενδιάμεση επέκταση (δηλαδή, $F \subseteq E \subseteq K$), τότε το K είναι σώμα διάσπασης του f και πάνω από το E .

Άσκηση 3.14. Αν $\phi : F \rightarrow F'$ είναι ισομορφισμός σωμάτων και το $f \in F[X]$ διασπάται στο F , τότε και το $\phi f = f' \in F'[X]$ διασπάται στο F' .

Άσκηση 3.15. 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 $\mathbb{C}$.)

- (ii) Δείτε το $X^2 - 2$ ως πολυώνυμο πάνω από το σώμα $\mathbb{Q}[\alpha]$ και, ως τέτοιο, δείξτε ότι είναι ανάγωγο.
- (iii) Έστω $E = \mathbb{Q}[\alpha, \beta]$. Βρείτε τον βαθμό μια βάσης της επέκτασης $E/\mathbb{Q}$ συναρτήσει των α, β

Άσκηση 3.16. Έστω $f(X) = X^3 - 3X - 1 \in \mathbb{Q}[X]$ και $K = \mathbb{Q}[u]$ όπου u είναι ρίζα του f .

- (i) Αποδείξτε ότι και τα στοιχεία $2 - u^2, -2 - u + u^2$ 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 $2 - u^2$ (τέτοιος αυτομορφισμός υπάρχει λόγω της Πρότασης 3.2). Υπολογίστε τα $\sigma(2 - u^2)$ και $\sigma^3(u)$.

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

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

Άσκηση 3.17. 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.

Άσκηση 3.18. 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 . Έστω $E = F[\alpha, \beta]$.

- (i) Αποδείξτε ότι $[E : F] \leq mn$.
(ii) 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 ;

