

Κεφάλαιο 11

11.1 11^η Εβδομάδα

Υπερβατικότητα (συνέχεια)

Πρόταση 11.1. Έστω η επέκταση E/F και $S \subseteq E$. Τα εξής είναι ισοδύναμα:

$\alpha')$ Το S είναι βάση υπερβατικότητας της E/F .

$\beta')$ Το S είναι maximal μεταξύ των υποσυνόλων του E που είναι F -αλγεβρικά ανεξάρτητα.

$\gamma')$ Το S είναι minimal μεταξύ των υποσυνόλων του E που παράγουν αλγεβρικά την E/F .

Απόδειξη. $(\alpha') \implies (\beta')$: Έστω ότι το S είναι βάση υπερβατικότητας της E/F . Τότε το S είναι F -αλγεβρικά ανεξάρτητο. Έστω F -αλγεβρικά ανεξάρτητο σύνολο T με $T \supsetneq S$. Θεωρώ $t \in T \setminus S$. Το t είναι αλγεβρικό πάνω από το $F(S)$, άρα από την άσκηση 10.19 υπάρχουν $s_1, \dots, s_n$ ώστε το σύνολο $\{s_1, \dots, s_n, t\}$ να είναι F -αλγεβρικά εξαρτημένο. Προφανώς μπορώ να υποθέσω ότι τα $s_1, \dots, s_n$ είναι διαφορετικά, οπότε, λόγω του ότι $t \notin S$, τα $s_1, \dots, s_n, t$ είναι διαφορετικά και το F -αλγεβρικά εξαρτημένο σύνολο $\{s_1, \dots, s_n, t\}$ είναι υποσύνολο του F -αλγεβρικά ανεξάρτητου T · άτοπο.

$(\beta') \implies (\alpha')$: Εξ υποθέσεως το S είναι F -αλγεβρικά ανεξάρτητο άρα μένει να δείξω 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 -αλγεβρικά εξαρτημένο, οπότε από την άσκηση 10.20 το t είναι αλγεβρικό πάνω από το $F(S)$.

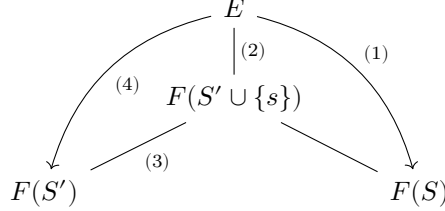
$(\alpha') \implies (\gamma')$: Το S παράγει αλγεβρικά την E/F . Έστω $T \subseteq S$, το οποίο παράγει αλγεβρικά την E/F . Θα δείξω ότι $T = S$. Το S είναι F -αλγεβρικά ανεξάρτητο άρα και το T είναι F -αλγεβρικά ανεξάρτητο, άρα το T είναι βάση υπερβατικότητας της E/F . Από την ισοδυναμία των (α') και (β') , έπεται ότι το T είναι maximal μεταξύ των F -αλγεβρικά ανεξάρτητων υποσυνόλων του E . Όμως $T \subseteq S$ και το S είναι F -αλγεβρικά ανεξάρτητο, άρα $T = S$.

$(\gamma') \implies (\alpha')$: Εξ υποθέσεως, το S παράγει αλγεβρικά την E/F , οπότε μένει να δείξω ότι το S είναι F -αλγεβρικά 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, μπορώ να υποθέσω 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 $f = g_n X_r^n + \dots + g_1 X_r + g_0$ με τα $g_i \in F[X_1, \dots, X_{r-1}]$ και $g_n(s_1, \dots, s_{r-1}) \neq 0$. Αυτό μου λέει ότι το s_r είναι ρίζα του πολωνύμου $g_n(s_1, \dots, s_{r-1})X_r^n + \dots + g_1(s_1, \dots, s_{r-1})X_r + g_0(s_1, \dots, s_{r-1}) \in F(s_1, \dots, s_{r-1})[X_r]$, άρα το s_r είναι αλγεβρικό πάνω από 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 και αυτό αντιβαίνει στην ελαχιστότητα του S . $\square$

Λήμμα 11.2 (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 δείξω ότι η επέκταση $E/F(S')$ είναι αλγεβρική.

Είναι $S' \cup \{s\} = S \cup \{t\}$, άρα $F(S) \leq F(S' \cup \{s\})$. Παρατηρώ 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 $F(S')$, συμπεραίνω ότι η επέκταση (3) είναι αλγεβρική. Αφού οι επεκτάσεις (2) και (3) είναι αλγεβρικές, έπεται ότι και η επέκταση (4) είναι αλγεβρική. $\square$

Δίνεται το παρακάτω θεώρημα χωρίς απόδειξη:

Θεώρημα 11.3. Κάθε επέκταση έχει μία (τουλάχιστον) βάση υπερβατικότητας.

Παρατήρηση 11.4. Αν η E/F είναι αλγεβρική, τότε βάση υπερβατικότητας αυτής είναι το $\emptyset$.

Θεώρημα 11.5. Έστω επέκταση E/F . Αν το $\{t_1, \dots, t_m\}$ παράγει αλγεβρικά το E/F και το $S \subseteq E$ είναι αλγεβρικός 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 $f_1(t_1, \dots, t_m, s_1) \neq 0$. 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 · άτοπο, διότι $s_1 \in S$ και το S είναι F -αλγεβρικός 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 $C_r(t_2, \dots, t_m, s_1)t_1^r + \dots + C_1(t_2, \dots, t_m, s_1)t_1 + C_0(t_2, \dots, t_m, s_1) = 0$, 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 11.2, το $\{s_1, t_2, \dots, t_m\}$ παράγει αλγεβρικός το E/F .

Επαγωγικό βήμα: Έστω $1 \leq i \leq m$ και το $\{s_1, \dots, s_i\} \cup \{m-i \text{ εκ των } t_1, \dots, t_m\}$ 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 $\{s_1, \dots, s_i, s_{i+1}\} \cup \{\text{ένα λιγότερο από τα } t_{i+1}, \dots, t_m\}$ 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 -αλγεβρικός 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 11.2, το $\{s_1, \dots, s_{i+1}, t_{i+2}, \dots, t_m\}$ παράγει αλγεβρικός το E/F .

Έτσι, επαγωγικά, καταλήγουμε 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 5, το $\{s_1, \dots, s_{m+1}\}$ είναι F -αλγεβρικός εξαρτημένο, συμπεράσμα το οποίο έρχεται σε αντίφαση με την υπόθεση ότι το S είναι F -αλγεβρικός ανεξάρτητο. $\square$

Πόρισμα 11.6. *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 -αλγεβρικός ανεξάρτητο. Επειδή η T είναι βάση υπερβατικότητας της E/F , παράγει αλγεβρικά 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 $|T| = |S|$. $\square$

Θεώρημα 11.7. *Δύο βάσεις υπερβατικότητας μίας οποιασδήποτε E/F είναι ισοπληθείς.*

Απόδειξη. Χάρη στο Πόρισμα 11.6, 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 $s \in S$ είναι 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 $F(T_{I_s})$, όπου $T_{I_s} = \{t_i : i \in I_s\}$.

Προφανώς $\bigcup_{s \in S} I_s \subseteq I$. Θα δείξω ότι ισχύει η ισότητα. Αν δεν ισχυε, 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 $T_s \subset T \setminus \{t_j\}$ · 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 11.1 (γ'). Συνεπώς $I = \bigcup_{s \in S} I(s)$.

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

Ορισμός 11.8. Ο πληθαιθμός μιας οποιασδήποτε βάση υπερβατικότητας μιας επέκτασης E/F ονομάζεται βαθμός υπερβατικότητας της E/F και συμβολίζεται $\text{trdeg}(E/F)$.

Θεώρημα 11.9. *Αν $F \leq K \leq E$ είναι διαδοχικές επεκτάσεις σωμάτων, τότε*

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

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 11.8, είναι $\text{trdeg}(K/F) = |S|$ και $\text{trdeg}(E/K) = |T|$. Από την άσκηση 11.10 είναι $S \cap T = \emptyset$. Συνεπώς, $|S \cup T| = |S| + |T| = \text{trdeg}(K/F) + \text{trdeg}(E/K)$, 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, συνάγουμε την αλγεβρικότητα της E/F .

Το $S \cup T$ είναι F -αλγεβρικός 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 $C_{i_1, \dots, i_m}(X_1, \dots, X_n)Y_1^{i_1} \dots Y_m^{i_m}$ 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 -αλγεβρικός ανεξάρτητο, άρα και $F(S)$ -αλγεβρικός 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 -αλγεβρικός ανεξάρτητο, συμπεραίνουμε ότι κάθε πολυώνυμο $C_{i_1, \dots, i_m}(X_1, \dots, X_n)$ είναι μηδενικό, άρα, το f είναι μηδενικό πολυώνυμο. $\square$

Ασκήσεις

Άσκηση 11.10. Έστω S, T όπως στην απόδειξη του Θεωρήματος 11.9. Αποδείξτε ότι $S \cap T = \emptyset$.

Άσκηση 11.11. 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 .

Άσκηση 11.12 (Σχετίζεται με την επίλυση τεταρτοβάθμιου πολυωνύμου). Έστω σώμα F του οποίου η χαρακτηριστική είναι 0 ή $\neq 2$ και ανάγωγο πολυώνυμο

$$f(X) = X^4 + qX^2 + rX + s \in F[X].^1$$

Έστω E σώμα διάσπασης του f πάνω από το F .

(1) Δείξτε ότι το f είναι διαχωρίσιμο και συμβολίστε με $t_1, \dots, t_4 \in E$ τις διαφορετικές ρίζες του. Έστω $G = \mathcal{G}(E/F)$. Δείτε την G ως υποομάδα της S_4 και την S_4 ως ομάδα μεταθέσεων των t_1, t_2, t_3, t_4 . Σύμφωνα με το Λήμμα 8.15 (ii), $S_4 = \langle (t_1 t_2), (t_2 t_3), (t_3 t_4) \rangle$. Έστω $V = \langle (t_1 t_2)(t_3 t_4), (t_1 t_3)(t_2 t_4) \rangle \leq S_4$. Παρατηρήστε ότι η V είναι «ομάδα των τεσσάρων» (του Klein) και αποδείξτε ότι είναι κανονική υποομάδα της S_4 .

Υπόδειξη. Δεν θα χρειαστεί να κάνετε πολλές πράξεις· αρκεί να ελέγξετε τα σύμπλοκα των γεννητόρων της S_4 .

Υπολογίστε $\phi_i \in S_4$, $i = 1, \dots, 6$ ώστε $S_4/V = \{\phi_i V : i = 1, \dots, 6\}$. Αποδείξτε ότι για κάθε $\sigma \in G$ υπάρχει $i \in \{1, \dots, 6\}$ και $\tau \in V$ ώστε $\sigma = \phi_i \tau$.

(2) Έστω

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

Δείξτε ότι τα u, v, w είναι διαφορετικά και, με τη βοήθεια του (1), αποδείξτε ότι $\mathcal{F}(G \cap V) = F(u, v, w)$. Δείξτε επίσης, ότι κάθε $\sigma \in G$ προκαλεί μετάθεση των u, v, w .

(3) Έστω

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

Με τη βοήθεια του (2) αποδείξτε ότι $g \in F[X]$. Δείξτε, επίσης, ότι $D(g) = D(f)$.

¹ 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.

(4) 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 γιατί

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

Εξισώνοντας τους συντελεστές στα δύο μέλη εκφράστε τα l, m, s συναρτήσει των q, r, k και δείξτε ότι $k^6 + 2qk^4 + (q^2 - 4s)k^2 - r^2 = 0$. 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 πολωνύμου, με $\sqrt{-v}, \sqrt{-w} \in E$, και συμπεράνετε ότι

$$g(X) = X^3 - 2qX^2 + (q^2 - 4s)X + r^2.$$

Ειδικότερα, οι τρεις ρίζες του g είναι διαφορετικές και ανήκουν στο E .

(5) Έστω $z \in E$ μια οποιαδήποτε 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 πολωνύμων του δεξιού μέλους μας δίνουν τις τέσσερις ρίζες του f . Εξηγήστε γιατί οι ρίζες του f εκφράζονται, συναρτήσει των συντελεστών του f , με τύπους που χρησιμοποιούν τις πράξεις του E και διάφορα ριζικά.

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