

## ΑΛΓΕΒΡΑ II – ΛΥΣΕΙΣ ΕΡΓΑΣΙΑΣ 1

### Παράγραφος 3.2

Άσκηση 1: Τα σταθερά σύνολα  $X_\sigma$  για κάθε  $\sigma \in D_4$  είναι τα:

$$\begin{array}{ll} X_{\rho_0} = X & X_{\mu_1} = \{s_1, s_3, m_1, m_2, C, P_1, P_3\} \\ X_{\rho_1} = \{C\} & X_{\mu_2} = \{s_2, s_4, m_1, m_2, C, P_2, P_4\} \\ X_{\rho_2} = \{m_1, m_2, d_1, d_2, C\} & X_{\delta_1} = \{2, 4, d_1, d_2, C\} \\ X_{\rho_3} = \{C\} & X_{\delta_2} = \{1, 3, d_1, d_2, C\} \end{array}$$

Άσκηση 2: Οι υποομάδες ισοτροπίας  $G_x$  για κάθε  $x \in X$  είναι οι:

$$\begin{array}{ll} G_1 = \{\rho_0, \delta_2\} = G_3 & G_{m_1} = \{\rho_0, \rho_2, \mu_1, \mu_2\} = G_{m_2} \\ G_2 = \{\rho_0, \delta_1\} = G_4 & G_{d_1} = \{\rho_0, \rho_2, \delta_1, \delta_2\} = G_{d_2} \\ G_{s_1} = \{\rho_0, \mu_1\} = G_{s_3} = G_{P_1} = G_{P_3} & G_C = D_4 \\ G_{s_2} = \{\rho_0, \mu_2\} = G_{s_4} = G_{P_2} = G_{P_4} & \end{array}$$

Άσκηση 3: Οι τροχιές στο  $X$  υπό την  $D_4$  είναι οι:

$$\begin{aligned} G1 &= G2 = G3 = G4 = \{1, 2, 3, 4\} \\ GS_1 &= GS_2 = GS_3 = GS_4 = \{s_1, s_2, s_3, s_4\} \\ Gm_1 &= Gm_2 = \{m_1, m_2\} \\ Gd_1 &= Gd_2 = \{d_1, d_2\} \\ GC &= \{C\} \\ GP_1 &= GP_2 = GP_3 = GP_4 = \{P_1, P_2, P_3, P_4\}. \end{aligned}$$

### Άσκηση 7:

α) Θα δείξουμε ότι οι τροχιές  $S = \{s_1, s_2, s_3, s_4\}$  και  $P = \{P_1, P_2, P_3, P_4\}$  είναι ισόμορφα  $D_4$  – σύνολα. Έστω η απεικόνιση  $\phi: S \rightarrow P$  με  $\phi(s_i) = P_i$ ,  $i = 1, 2, 3, 4$ . Τότε από τον ορισμό της η  $\phi$  είναι 1-1 και επί, και από τον Πίνακα 3.1 (σελ. 216) μπορούμε να εξακριβώσουμε ότι έχουμε  $g\phi(s_i) = \phi(gs_i)$  για κάθε  $g \in D_4, s_i \in S$ . Άρα η  $\phi$  είναι ισομορφισμός μεταξύ των  $D_4$  – συνόλων.

β) Παρατηρούμε ότι τα στοιχεία  $\rho_0, \rho_1, \rho_2, \rho_3$  δρούν στα  $D_4$  – σύνολα  $\{1, 2, 3, 4\}$  και  $\{s_1, s_2, s_3, s_4\}$  επάγοντας την ίδια μετάθεση των στοιχείων του πρώτου συνόλου με την μετάθεση των δεικτών των στοιχείων του δεύτερου συνόλου. Έτσι ορίζουμε την απεικόνιση  $\phi: \{1, 2, 3, 4\} \rightarrow \{s_1, s_2, s_3, s_4\}$  με  $\phi(i) = s_i$ ,  $i = 1, 2, 3, 4$ . Τότε παρατηρούμε ότι η  $\phi$  είναι 1-1 και επί, όμως  $1 = \mu_1 \phi(1) \neq \phi(\mu_1 1) = 3$  άρα η  $\phi$  δεν είναι ισομορφισμός  $D_4$  – συνόλων.

Πιο γενικά, έστω ότι υπάρχει ένας τέτοιος ισομορφισμός  $\phi$ , μεταξύ των συνόλων  $\{1, 2, 3, 4\}$  και  $\{s_1, s_2, s_3, s_4\}$ . Τότε θα πρέπει  $\mu_1 \phi(i) = \phi(\mu_1 i)$ ,  $i = 1, 2, 3, 4$ . Όμως παρατηρούμε ότι  $\mu_1 s_1 = s_1$  ενώ το  $\mu_1$  όταν δρά επί του συνόλου  $\{1, 2, 3, 4\}$  επάγει μία

μετάθεση που δεν αφήνει κανένα στοιχείο σταθερό. Αφού η  $\phi$  είναι επί, θα έχουμε  $\phi(i) = s_1$  για κάποιο  $i \in \{1,2,3,4\}$ , όμως τότε

$\mu_1 \phi(i) = \phi(\mu_1 i) \Leftrightarrow \mu_1 s_1 = \phi(\mu_1 i) \Leftrightarrow s_1 = \phi(j)$  με  $j \neq i, j \in \{1,2,3,4\}$ . Δηλαδή τα  $i$  και  $j$  έχουν την ίδια εικόνα  $s_1$ .

Άτοπο, αφού η  $\phi$  είναι 1-1.

γ) Τα  $S = \{s_1, s_2, s_3, s_4\}, P = \{P_1, P_2, P_3, P_4\}$  είναι τα μόνα ισόμορφα  $D_4$  - υποσύνολα της  $X$ , αφού με παρόμοιο τρόπο όπως στο υποερώτημα β) μπορούμε να δείξουμε ότι ούτε τα  $\{m_1, m_2\}, \{d_1, d_2\}$  είναι ισομορφικά.

### Ασκηση 11:

α) Εστω ένα σημείο  $P \in \mathbb{R}^2$ , παρατηρούμε ότι η περιστροφή του επιπέδου γύρω από την αρχή των αξόνων κατά γωνία 0 ακτινίων αφήνει το σημείο  $P$  ακίνητο, άρα  $0 * P = P$ .

Επιπλέον, εάν περιστραφεί το επίπεδο γύρω από την αρχή των αξόνων κατά  $\theta_1 + \theta_2$  ακτίνια, το σημείο  $P$  θα βρεθεί στην ίδια θέση με αυτή μετά από περιστροφή κατά  $\theta_2$  ακτίνια αρχικά και στη συνέχεια κατά  $\theta_1$  ακτίνια. Άρα  $(\theta_1 + \theta_2) * P = \theta_1 * (\theta_2 * P)$ .

β) Η τροχιά που περιέχει το  $P$  γεωμετρικά είναι ο κύκλος με κέντρο το  $O = (0,0)$  και ακτίνα  $\|\overrightarrow{OP}\|$ .

γ) Η υποομάδα ισοτροπίας του  $P$  είναι

$$G_P = \{g \in \mathbb{R} : gP = P\} = \{g \in \mathbb{R} : g = 2k\pi, k \in \mathbb{N}\} = \langle 2\pi \rangle.$$

### Παράγραφος 3.3

Για Ασκήσεις 4, 5: Υπάρχουν 24 πιθανές θέσεις ενός κύβου πάνω σε ένα τραπέζι. Κάθε τέτοια θέση προκύπτει από μία άλλη με περιστροφή του κύβου. Οι 24 στροφές του κύβου αποτελούνται από την ταυτότητα, από τις 9 στροφές που διατηρούν ένα ζεύγος απέναντι πλευρών σταθερό, από τις 8 στροφές που αφήνουν ένα ζευγάρι απέναντι κορυφών σταθερό, και από τις 6 στροφές που διατηρούν ένα ζεύγος απέναντι ακμών σταθερό. Άρα η ομάδα  $G$  των στροφών του κύβου αποτελείται από τα παρακάτω στοιχεία:

$e$ : ο κύβος μένει σταθερός.

$g_1, g_2, g_3$ : κρατάμε σταθερό ένα ζεύγος απέναντι πλευρών και περιστρέφουμε τον κύβο κατά γωνία  $90^\circ$  (υπάρχουν τρία διαφορετικά ζεύγη απέναντι πλευρών).

$g_4, g_5, g_6$ : κρατάμε σταθερό ένα ζεύγος απέναντι πλευρών και περιστρέφουμε τον κύβο κατά γωνία  $180^\circ$ .

$g_7, g_8, g_9$ : κρατάμε σταθερό ένα ζεύγος απέναντι πλευρών και περιστρέφουμε τον κύβο κατά γωνία  $270^\circ$ .

$h_1, h_2, h_3, h_4$ : κρατάμε σταθερό ένα ζεύγος απέναντι κορυφών και περιστρέφουμε τον κύβο κατά γωνία  $120^\circ$  ως προς τον άξονα που ορίζουν οι δύο απέναντι κορυφές. Η συμμετρία τότε καθορίζεται από το ισόπλευρο τρίγωνο που σχηματίζουν οι τρείς γειτονικές κορυφές μίας από τις δύο σταθερές (υπάρχουν τέσσερα διαφορετικά ζεύγη απέναντι κορυφών).

$h_5, h_6, h_7, h_8$ : κρατάμε σταθερό ένα ζεύγος απέναντι κορυφών και περιστρέφουμε τον κύβο κατά γωνία  $240^\circ$ .

$k_1, k_2, \dots, k_6$ : κρατάμε σταθερό ένα ζεύγος απέναντι ακμών και περιστρέφουμε κατά γωνία  $180^\circ$  πάνω στο επίπεδο των δύο ακμών. Τότε οι δύο ακμές εναλλάσσονται μεταξύ τους και άρα το ζεύγος παραμένει σταθερό (υπάρχουν 6 διαφορετικά ζεύγη απέναντι ακμών).

Άσκηση 4: Υπάρχουν συνολικά  $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 = 20160$  τρόποι να χρωματίσουμε έναν κύβο με 8 χρώματα με διαφορετικό χρώμα σε κάθε έδρα. Κάποιοι όμως από τους παραπάνω χρωματισμούς θεωρούνται ισότιμοι αν υπάρχει μία στροφή του κύβου που να τους ταυτίζει. Θεωρώντας λοιπόν το σύνολο όλων των δυνατών χρωματισμών και την δράση της ομάδας  $G$  των στροφών του κύβου πάνω σε αυτό, ο καθορισμός του πλήθους διαφορετικών χρωματισμών είναι ισοδύναμος με το ερώτημα «πόσες είναι οι διαφορετικές τροχιές του  $G$ -συνόλου των χρωματισμών υπό την  $G$ ;». Παρατηρούμε ότι  $|X_g| = 0$ , επειδή κάθε στροφή που δεν είναι η ταυτοτική μετατρέπει οποιονδήποτε από τους 20160 χρωματισμούς σε κάποιον διαφορετικό. Ακόμη  $|X_e| = 20160$ , αφού η ταυτότητα διατηρεί σταθερό κάθε έναν από τους 20160 χρωματισμούς. Σύμφωνα λοιπόν με το Θεώρημα Burnside,

$$(\text{πλήθος τροχιών}) = \frac{1}{24} 20160 = 840,$$

δηλαδή υπάρχουν 840 διαφορετικοί χρωματισμοί ενός κύβου με 8 διαφορετικά χρώματα.

Άσκηση 5: Αφού μπορούμε να χρωματίσουμε τις έδρες του κύβου με το ίδιο χρώμα, υπάρχουν συνολικά  $8^6$  δυνατοί χρωματισμοί. Η ομάδα  $G$  δρά πάνω στο σύνολο  $X$  των χρωματισμένων κύβων.

Οι διαφορετικοί χρωματισμοί είναι όσοι το πλήθος των τροχιών του συνόλου  $X$  υπό του  $G$ . Πρέπει να υπολογίσουμε το πλήθος  $|X_g|$  για καθένα από τα 24 στοιχεία της  $G$ .

Όπως είπαμε  $|X_e| = 8^6$ , αφού όλοι οι κύβοι παραμένουν αναλλοίωτοι υπό την δράση του  $e$ .

Παρατηρούμε ότι για να παραμένει ένας κύβος ο ίδιος μετά από την δράση των  $g_1, g_2, g_3, g_7, g_8, g_9$  θα πρέπει όλες οι υπόλοιπες έδρες εκτός των δύο σταθερών, να έχουν το ίδιο χρώμα, άρα συνολικά έχουμε να επιλέξουμε χρώμα για 3 πλευρές, δηλαδή  $|X_{g_1}| = \dots = |X_{g_3}| = |X_{g_7}| = \dots = |X_{g_9}| = 8^3$ .

Για να παραμένει ένας κύβος αναλλοίωτος από την δράση των  $g_4, g_5, g_6$  πρέπει δύο απέναντι πλευρές, εκτός αυτών που μένουν σταθερές κατά την στροφή, να έχουν το ίδιο χρώμα. Άρα έχουμε να επιλέξουμε χρωματισμό για 4 πλευρές συνολικά, δηλαδή  $|X_{g_4}| = |X_{g_5}| = |X_{g_6}| = 8^4$ .

Για να παραμένει ένας κύβος αναλλοίωτος μετά από την δράση των  $h_i, i = 1, \dots, 8$ , θα πρέπει οι τρείς έδρες που συναντώνται στην κάθε κορυφή να έχουν το ίδιο χρώμα.

Άρα συνολικά έχουμε να επιλέξουμε χρώμα για δύο έδρες, δηλαδή  $|X_{h_i}| = 8^2, i = 1, \dots, 8$ .

Τέλος παρατηρούμε ότι για να παραμείνει ένας κύβος αναλλοίωτος από την δράση των  $k_j, j = 1, \dots, 6$ , θα πρέπει οι έδρες που έχουν ως κοινή τομή μία από τις σταθερές ακμές να έχουν το ίδιο χρώμα, δηλαδή δύο διαδοχικές έδρες για κάθε ακμή, και οι απέναντι έδρες που απομένουν να έχουν επίσης το ίδιο χρώμα. Άρα συνολικά έχουμε να επιλέξουμε χρώμα για τρείς πλευρές, δηλαδή

$$|X_{k_j}| = 8^3, j = 1, \dots, 6.$$

Επομένως από το Θεώρημα Burnside, έχουμε

$$(\text{πλήθος τροχιών}) = \frac{1}{|G|} \sum_{g \in G} |X_g| = \frac{1}{24} (8^6 + 6 \cdot 8^3 + 3 \cdot 8^4 + 8 \cdot 8^2 + 6 \cdot 8^3) = 11712,$$

δηλαδή δημιουργούνται 11712 διαφορετικά παιδικά τουβλάκια.

### Παράγραφος 3.4

Ασκηση 1: Από το Πρώτο Θεώρημα Sylow, αποδεικνύεται ότι οι για μία ομάδα τάξης  $|G| = p^n m$  οι  $p$ -υποομάδες Sylow της  $G$  είναι ακριβώς εκείνες που έχουν τάξη  $p^n$ . Αφού  $|G| = 12 = 2^2 \cdot 3$ , μία 3-υποομάδα Sylow της  $G$  έχει τάξη 3.

Ασκηση 2: Από το Πρώτο Θεώρημα Sylow, αφού  $|G| = 54 = 2 \cdot 3^3$ , η  $G$  περιέχει μία 3-υποομάδα τάξης 3, μία 3-υποομάδα τάξης  $3^2$  και μία 3-υποομάδα τάξης  $3^3$ . Άρα μία 3-υποομάδα Sylow της  $G$  έχει τάξη  $3^3$  αφού δεν υπάρχει μεγαλύτερη 3-υποομάδα που να την περιέχει.

Ασκηση 3: Από το Τρίτο Θεώρημα Sylow έχουμε ότι το πλήθος,  $x$ , των 2-υποομάδων Sylow είναι ισότιμο προς το  $1 \pmod{2}$  και διαιρεί την  $|G| = 24$ . Επειδή μόνο οι περιττοί αριθμοί  $1, 3, 5, \dots, 21, 23$  είναι οι μόνοι θετικοί αριθμοί που είναι μικρότεροι του 24 και ισότιμοι του  $1 \pmod{2}$  και επειδή από αυτούς μόνο οι 1 και 3 διαιρούν το 24, βλέπουμε ότι η  $G$  έχει μία ή τρείς 2-υποομάδες Sylow.

Ασκηση 4: Ομοίως από το Τρίτο Θεώρημα Sylow έχουμε ότι μία υποομάδα τάξης 255 πρέπει να έχει 1 ή 85 3-υποομάδες Sylow και 1 ή 51 5-υποομάδες Sylow.

Ασκηση 5: Από το Τρίτο Θεώρημα Sylow έχουμε ότι αφού  $|S_4| = 2^3 \cdot 3$  το πλήθος των 3-υποομάδων Sylow της  $S_4$  θα είναι 1 ή 4. Από το Πρώτο Θεώρημα Sylow επίσης έχουμε ότι κάθε 3-υποομάδα Sylow της  $S_4$  θα έχει τάξη 3.

Βρίσκουμε ότι οι 3-υποομάδες Sylow της  $S_4$  είναι οι

$$G_1 = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \right\},$$

$$G_2 = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \right\},$$

$$G_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \right\} \text{ και}$$

$$G_4 = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \right\}.$$

Παρατηρούμε ότι

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} G_1 \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}^{-1} = G_2,$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} G_1 \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}^{-1} = G_3 \text{ και}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} G_1 \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}^{-1} = G_4,$$

δηλαδή υπάρχει  $g_{ij} \in S_4$  τέτοιο ώστε  $g_{ij} G_i g_{ij}^{-1} = G_j$ . Άρα οι  $G_1, G_2, G_3, G_4$  είναι ανάδυο συζυγείς υποομάδες της  $S_4$ .

Άσκηση 8: Από το Πρώτο Θεώρημα Sylow έχουμε ότι αν  $P$  είναι μία  $p$ -υποομάδα Sylow μίας πεπερασμένης ομάδας  $G$ , τότε κάθε συζυγής ομάδα της  $P$  είναι επίσης μία  $p$ -υποομάδα Sylow της  $G$ . Αν όμως η  $P$  είναι η μοναδική  $p$ -υποομάδα Sylow της  $G$ , αυτό σημαίνει ότι  $gPg^{-1} = P$  για κάθε  $g \in G$ , δηλαδή η  $P$  είναι κανονική υποομάδα της  $G$ , επομένως η  $G$  δεν είναι απλή.

Άσκηση 9: Έστω  $G$  μία ομάδα με  $|G| = 45 = 5 \cdot 3^2$ . Σύμφωνα με το Τρίτο Θεώρημα Sylow, το πλήθος των 3-υποομάδων Sylow της  $G$  είναι 1. Από το Πρώτο Θεώρημα Sylow η  $G$  περιέχει μία υποομάδα τάξης  $3^2$ . Άρα η μοναδική 3-υποομάδα Sylow της  $G$  θα έχει τάξη 9 και από την προηγούμενη άσκηση ξέρουμε ότι είναι κανονική υποομάδα.

Άσκηση 16:

α) Το κέντρο της ομάδας  $G$  είναι το

$$Z(G) = \{a \in G : ag = ga \quad \forall g \in G\}. \text{ Από την Άσκηση 10 στη σελίδα 220 έχουμε ότι } G_G = \{g \in G : g * x = x \quad \forall x \in G\} = \{g \in G : gxg^{-1} = x \quad \forall x \in G\} = \{g \in G : gx = xg \quad \forall x \in G\} \\ \text{ Άρα } G_G = Z(G).$$

β) Έστω ότι η  $G$  είναι μία πεπερασμένη  $p$ -ομάδα, άρα έχει τάξη  $p^n$ . Θεωρώντας την δράση της  $G$  στον εαυτό της μέσω συζυγίας, η  $G$  είναι ένα  $G$ -σύνολο και από το Θεώρημα 3.9 έχουμε ότι  $|G| \equiv |G_G| \pmod{p}$ . Από την προηγούμενη άσκηση έχουμε όμως ότι  $|G| \equiv |Z(G)| \pmod{p}$ . Επειδή  $p \mid |G|$ , θα έχουμε  $p \mid |Z(G)|$  άρα  $|Z(G)| \neq 1$ , δηλαδή το κέντρο της  $G$  δεν είναι τετριμμένο.

## ΑΛΓΕΒΡΑ ΙΙ – ΛΥΣΕΙΣ ΕΡΓΑΣΙΑΣ 2

### Παράγραφος 4.2

Άσκηση 4: Ελέγχουμε την εξίσωση αντικαθιστώντας με κάθε στοιχείο του  $\mathbb{Z}_6$  και παρατηρούμε ότι μόνο για το 2 ισχύει  $2^2 + 2 \cdot 2 + 4 \equiv 0 \pmod{6}$ . Άρα το 2 είναι η μοναδική λύση.

Άσκηση 18: Ο αντιμεταθετικός δακτύλιος  $2\mathbb{Z}$  δεν έχει διαιρέτες του μηδενός, όμως δεν έχει ταυτοτικό στοιχείο για τον πολλαπλασιασμό, δηλαδή δεν έχει μοναδιαίο στοιχείο, άρα δεν είναι ακέραια περιοχή.

### Παράγραφος 4.4

#### Άσκηση 3:

- α) Σωστό, αφού κάθε στοιχείο του  $\mathbb{Q}$  γράφεται σαν πηλίκο δύο στοιχείων του  $\mathbb{Z}$ .
- β) Λάθος, αφού δεν είναι το ελάχιστο σώμα που περιέχει την ακέραια περιοχή  $\mathbb{Z}$  έτσι ώστε όλα τα στοιχεία του να είναι πηλίκα στοιχείων του  $\mathbb{Z}$ .
- γ) Σωστό, αφού το  $\mathbb{R}$  είναι σώμα και αφού κάθε στοιχείο του γράφεται σαν πηλίκο δύο στοιχείων του.
- δ) Λάθος, αφού δεν μπορεί κάθε στοιχείο του  $\mathbb{C}$  να γραφτεί σαν πηλίκο δύο στοιχείων του  $\mathbb{R}$ .
- ε) Σωστό, αφού  $D$  είναι ένα σώμα, το  $D$  είναι και ακέραια περιοχή και εκ κατασκευής είναι σώμα πηλίκων του εαυτού του. Επιπλέον, από το Θεώρημα 4.14 υπάρχει ισομορφισμός από το σώμα  $D$  (ως σώμα που περιέχει την ακέραια περιοχή  $D$ ) στο σώμα πηλίκων της  $D$ .
- στ) Σωστό.
- ζ) Λάθος, αφού το μηδενικό στοιχείο ανήκει στην ακέραια περιοχή  $D$  και δεν είναι αντιστρέψιμο σε κανένα σώμα πηλίκων της  $D$ .
- η) Σωστό, αφού η ακέραια περιοχή και το σώμα πηλίκο έχουν το μοναδιαίο στοιχείο και για κάθε στοιχείο  $a \in D$ , ορίζεται το  $\frac{1}{a} \in D$ .
- θ) Σωστό, αφού το  $F$  περιέχει την ακέραια περιοχή  $D'$ , από το Θεώρημα 4.14 υπάρχει ισομορφισμός από το  $F'$  σε ένα υπόσωμα του  $F$ .
- ι) Σωστό, από το Πόρισμα 2 του Θεωρήματος 4.14.

### Παράγραφος 4.6

Άσκηση 5: Αφού το πολυώνυμο  $x^4 + 4$  αναλύεται σε γραμμικούς παράγοντες στον  $\mathbb{Z}_5[x]$ , αυτό σημαίνει ότι διαιρείται από πολυώνυμα τις μορφής  $x + a$  στον  $\mathbb{Z}_5[x]$ .

Εκτελώντας λοιπόν την διαίρεση των πολυωνύμων  $x^4 + 4$  και  $x + a$  για κάθε  $a \in \mathbb{Z}_5$  (το  $\mathbb{Z}_5$  είναι σώμα), βρίσκουμε την εξής ανάλυση  $x^4 + 4 = (x - 1)(x + 1)(x - 2)(x + 2)$ .

Άσκηση 13: Χρησιμοποιώντας το Θεώρημα 4.20, θα δείξουμε ότι το

$$f(x) = x^4 - 22x^2 + 1$$

ως στοιχείο του  $\mathbb{Q}[x]$  είναι ανάγωγο πάνω από το  $\mathbb{Q}$ . Αν το  $f(x)$  έχει ένα γραμμικό παράγοντα στον  $\mathbb{Q}[x]$ , τότε, εφόσον  $f(x) \in \mathbb{Z}[x]$ , από το πόρισμα του Θεωρήματος 4.20, θα έχει μία ρίζα στον  $\mathbb{Z}$ , και αυτή η ρίζα πρέπει να είναι διαιρέτης του 1 στον  $\mathbb{Z}$ , δηλαδή να είναι  $\pm 1$ . Άλλα  $f(1) = -20$  και  $f(-1) = -20$ , επομένως δεν είναι δυνατή μία τέτοια ανάλυση.

Αν το  $f(x)$  αναλύεται σε δύο τετραγωνικούς παράγοντες στον  $\mathbb{Q}[x]$ , τότε από το Θεώρημα 4.20, αναλύεται στο γινόμενο

$$(x^2 + ax + b)(x^2 + cx + d)$$

στον  $\mathbb{Z}[x]$ . Εξισώνοντας τους συντελεστές των δυνάμεων του  $x$ , βρίσκουμε ότι πρέπει να ισχύουν οι

$$bd = 1, ad + bc = 0, ac + b + d = -22 \text{ και } a + c = 0$$

για τους ακεραίους  $a, b, c, d \in \mathbb{Z}$ . Από την  $bd = 1$ , βλέπουμε ότι  $b = d = 1$  ή  $b = d = -1$ . Σε κάθε περίπτωση,  $b = d$  και από την  $a + c = 0$  έχουμε  $a = -c$ . Τέλος από την  $ac + b + d = 0$ , έχουμε  $-a^2 + 2b = -22 \Rightarrow a^2 = 20$  ή  $a^2 = 24$ . Όμως κανένας  $a \in \mathbb{Z}$  δεν ικανοποιεί κάποια από τις παραπάνω ισότητες. Έτσι αποκλείεται η ανάλυση σε δύο τετραγωνικά πολυώνυμα, δηλαδή το  $f(x)$  είναι ανάγωγο πάνω από το  $\mathbb{Q}$ .

Άσκηση 20: Εκτελώντας την διαίρεση των πολυωνύμων  $x^4 + x^3 + x^2 - x + 1$  και  $x + 2$  στον  $\mathbb{Z}_p$  όπου  $p$  πρώτος, έχουμε στο πρώτο βήμα:

$$(x^4 + x^3 + x^2 - x + 1) \div (x + 2) = x^3(x + 2) + (-x^3 + x^2 - x + 1) \text{ για κάθε } p \neq 1.$$

Στο δεύτερο βήμα έχουμε τα εξής ενδεχόμενα:

α)  $(x^4 + x^3 + x^2 - x + 1) \div (x + 2) = (x^3 - x^2)(x + 2) + (3x^2 - x + 1)$  για κάθε  $p \neq 3$ , ενώ

β) για  $p = 3$  έχουμε  $(x^4 + x^3 + x^2 - x + 1) \div (x + 2) = (x^3 - x^2)(x + 2) + (-x + 1)$  και συνεχίζοντας την διαίρεση στο  $\mathbb{Z}_3$  παίρνουμε

$(x^4 + x^3 + x^2 - x + 1) \div (x + 2) = (x^3 - x^2 - 1)(x + 2)$ , δηλαδή το  $x + 2$  είναι παράγοντας του  $x^4 + x^3 + x^2 - x + 1$  στον  $\mathbb{Z}_3$ .

Συνεχίζοντας για κάθε  $p \neq 3$  έχουμε

$$(x^4 + x^3 + x^2 - x + 1) \div (x + 2) = (x^3 - x^2 + 3x)(x + 2) - 7x + 1, \text{ οπότε:}$$

α1) για  $p = 7$  έχουμε  $(x^4 + x^3 + x^2 - x + 1) \div (x + 2) = (x^3 - x^2 + 3x)(x + 2) + 1$ , ενώ

α2) για κάθε  $p \neq 3$  και  $p \neq 7$

$$(x^4 + x^3 + x^2 - x + 1) \div (x + 2) = (x^3 - x^2 + 3x - 7)(x + 2) + 15, \text{ οπότε για } p = 5 \text{ έχουμε πλήρη διαίρεση.}$$

Άρα οι μόνοι περιττοί πρώτοι  $p$  για τους οποίους το  $x + 2$  είναι παράγοντας του  $x^4 + x^3 + x^2 - x + 1$  είναι το 3 και το 5.

Άσκηση 26: Θα δείξουμε ότι για κάθε  $a \in \mathbb{Z}_p$  το πολυώνυμο  $x^p + a$  στον  $\mathbb{Z}_p[x]$  έχει λύση στο  $\mathbb{Z}_p$ . Προφανώς ισχύει για  $a = 0$ . Έστω λοιπόν  $a \neq 0$ . Διακρίνουμε τις περιπτώσεις  $p = 2$  και  $p \neq 2$ .

Για  $p = 2$  θα έχουμε  $a = 0$  ή  $1$ , οπότε για  $a = 1$ ,  $x^2 + 1 \equiv x^2 - 1 = (x-1)(x+1) \equiv (x+1)^2$ .

Για  $p \neq 2$ : Παρατηρούμε ότι για  $x = -a$  έχουμε  $(-a)^p + a = -a^p + a$ , αφού  $p$  περιττός. Στη συνέχεια αυτό γράφεται ως  $-a(a^{p-1} - 1)$ . Όμως αφού  $a \in \mathbb{Z}_p$ , είναι και  $a \in \mathbb{Z}$  και  $p$  είναι ένας πρώτος που δεν διαιρεί τον  $a$ . Από το Θεώρημα Fermat λοιπόν έπεται ότι ο  $p$  διαιρεί τον  $a^{p-1} - 1$ . Άρα θα είναι  $-a(a^{p-1} - 1) = 0$  στο  $\mathbb{Z}_p$ . Δηλαδή το  $x^p + a$  έχει πάντα λύση το  $-a \pmod p$  για κάθε  $a \in \mathbb{Z}_p$ .

Άσκηση 27: Αφού το  $F$  είναι σώμα, κάθε μη μηδενικό στοιχείο του  $b \in F$  έχει πολλαπλασιαστικό αντίστροφο  $\frac{1}{b} \in F$ .

Αφού το  $a \neq 0$  είναι ρίζα του  $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$  στον  $F[x]$ , θα είναι  $f(a) = 0 \Rightarrow a_0 + a_1a + a_2a^2 + \dots + a_na^n = 0$ .

Πολλαπλασιάζοντας τώρα και τα δύο μέλη της τελευταίας ισότητας με  $\frac{1}{a^n}$  και χρησιμοποιώντας τις ιδιότητες των διμελών πράξεων του σώματος  $F$ , παίρνουμε

$$\begin{aligned} \frac{1}{a^n} \cdot (a_0 + a_1a + a_2a^2 + \dots + a_na^n) &= \frac{1}{a^n} \cdot 0 = 0 \\ \Leftrightarrow a_0 \frac{1}{a^n} + a_1 \frac{1}{a^{n-1}} \cdot (\frac{1}{a} \cdot a) + a_2 \frac{1}{a^{n-2}} \cdot (\frac{1}{a^2} \cdot a^2) + \dots + a_n \frac{1}{a^n} \cdot a^n &= 0 \end{aligned} \quad (1)$$

Επειδή όμως  $\frac{1}{a} \cdot a = 1$  τότε έχουμε  $\frac{1}{a} \cdot \frac{1}{a} \cdot a \cdot a = \frac{1}{a} \cdot 1 \cdot a \Rightarrow \frac{1}{a^2} \cdot a^2 = 1$ , δηλαδή πιο γενικά, ο πολλαπλασιαστικός αντίστροφος του  $a^k$  είναι ο  $\frac{1}{a^k}$ .

Έτσι η (1) γίνεται

$$\begin{aligned} (1) &\Leftrightarrow a_0 \frac{1}{a^n} + a_1 \frac{1}{a^{n-1}} + a_2 \frac{1}{a^{n-2}} + \dots + a_n = 0 \\ (1) &\Leftrightarrow a_0 \left(\frac{1}{a}\right)^n + a_1 \left(\frac{1}{a}\right)^{n-1} + a_2 \left(\frac{1}{a}\right)^{n-2} + \dots + a_n = 0 \end{aligned} \quad (2)$$

Έστω τώρα το πολυώνυμο  $g(x) = a_n + a_{n-1}x + a_{n-2}x^2 + \dots + a_0x^n$ . Τότε από την (2)

$$g\left(\frac{1}{a}\right) = a_0 \left(\frac{1}{a}\right)^n + a_1 \left(\frac{1}{a}\right)^{n-1} + a_2 \left(\frac{1}{a}\right)^{n-2} + \dots + a_n = 0.$$

Άσκηση 28: Αφού το  $F$  είναι σώμα, τότε το  $f(x) \in F[x]$  αναλύεται σε γινόμενο ανάγωγων πολυωνύμων στον  $F[x]$ . Έστω λοιπόν

$f(x) = p_1(x)p_2(x) \cdots p_s(x)$ , όπου  $p_i(x)$  είναι ανάγωγο για  $i = 1, 2, \dots, s$ .

Υπάρχουν δύο περιπτώσεις για το  $(x-a)$ :

- a) το  $(x-a) = p_i(x)$  για κάποιο  $i$ : τότε το υπόλοιπο της διαίρεσης του  $f(x)$  με το  $(x-a)$  είναι μηδέν και  $f(a) = 0$ , και

β) το  $(x-a) \neq p_i(x)$  για κάθε  $i$ : τότε  $f(a) \neq 0$ , και το υπόλοιπο  $r(x)$  της διαιρεσης του  $f(x)$  με το  $(x-a)$ , δεν θα είναι μηδέν και θα έχουμε  
 $f(x) = g(x)(x-a) + r(x)$  (1).

Τότε από την (1) έχουμε  $f(a) = g(a)(a-a) + r(a) = g(a) \cdot 0 + r(a) = r(a)$

Όμως αφού το υπόλοιπο της διαιρεσης θα έχει βαθμό μικρότερο του βαθμού του  $(x-a)$ , αυτό σημαίνει ότι θα είναι ένα σταθερό πολυώνυμο, άρα θα ταυτίζεται με το  $r(a) = f(a)$ .

### Άσκηση 29:

α) Έστω  $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$  και  $g(x) = b_0 + b_1x + \dots + b_nx^n \in \mathbb{Z}[x]$ . Τότε  
 $\overline{\sigma_m}(f(x) + g(x)) = \overline{\sigma_m}(a_0 + b_0) + \overline{\sigma_m}(a_1 + b_1)x + \dots + \overline{\sigma_m}(a_n + b_n)x^n$ , ενώ έχουμε ότι  
 $\overline{\sigma_m}(f(x)) + \overline{\sigma_m}(g(x)) = \overline{\sigma_m}(a_0) + \overline{\sigma_m}(b_0) + (\overline{\sigma_m}(a_1) + \overline{\sigma_m}(b_1))x + \dots + (\overline{\sigma_m}(a_n) + \overline{\sigma_m}(b_n))x^n$   
 Όμως ως γνωστό  $(a+b) \text{ mod } m = a(\text{mod } m) + b(\text{mod } m)$  (1).  
 Επίσης  $a \cdot b(\text{mod } m) = a(\text{mod } m) \cdot b(\text{mod } m)$  (2).

Έστω τώρα το  $h(x) = f(x)g(x) = d_0 + d_1x + \dots + d_sx^s$ , όπου  $d_i = \sum_{i=0}^j a_i b_{j-i}$ .

Τότε  $\overline{\sigma_m}(h(x)) = \overline{\sigma_m}(d_0) + \overline{\sigma_m}(d_1)x + \dots + \overline{\sigma_m}(d_s)x^s$ . Όμως από (1) και (2)

$$\overline{\sigma_m}(d_i) = \sum_{i=0}^j \overline{\sigma_m}(a_i b_{j-i}) = \sum_{i=0}^j \overline{\sigma_m}(a_i) \overline{\sigma_m}(b_j) \text{ στον } \mathbb{Z}_m[x].$$

Άρα έχουμε ότι  $\overline{\sigma_m}(h(x)) = \overline{\sigma_m}(f(x)) \overline{\sigma_m}(g(x))$ . Άρα η  $\overline{\sigma_m}: \mathbb{Z}[x] \rightarrow \mathbb{Z}_m[x]$  είναι ομοιορφισμός και προφανώς είναι επί.

β) Από το Θεώρημα 4.20 γνωρίζουμε ότι αν το  $f(x) \in \mathbb{Z}[x]$  αναλυόταν σε γινόμενο δύο πολυωνύμων με μικρότερους βαθμούς, τότε δεν θα ήταν ανάγωγο πάνω από το  $\mathbb{Q}$ . Όμως αν ήταν  $f(x) = g(x)h(x)$ , όπου  $g(x), h(x) \in \mathbb{Z}[x]$  πολυώνυμα μικρότερου βαθμού, τότε θα είχαμε ότι  $\overline{\sigma_m}(f(x)) = \overline{\sigma_m}(g(x))\overline{\sigma_m}(h(x))$ . Δηλαδή τότε θα αναλυόταν και το  $\overline{\sigma_m}(f(x)) \in \mathbb{Z}_m[x]$  σε γινόμενο δύο πολυωνύμων μικρότερου βαθμού στον  $\mathbb{Z}_m[x]$  (δεδομένου ότι ο βαθμός του  $\overline{\sigma_m}(f(x))$  είναι ο ίδιος με τον βαθμό του  $f(x)$ ). Αφού όμως δεν αναλύεται το  $\overline{\sigma_m}(f(x)) \in \mathbb{Z}_m[x]$ , τότε το  $f(x)$  είναι ανάγωγο πάνω από το  $\mathbb{Q}$ .

γ) Κατ' αρχάς παρατηρούμε εύκολα ότι τα  $\overline{\sigma_2}(f(x)) = x^3 + x$  και  $\overline{\sigma_3}(f(x)) = x^3 + 2x$  αναλύονται σε μικρότερους παράγοντες. Στη συνέχεια παρατηρούμε ότι το  $\overline{\sigma_5}(f(x)) = x^3 + 2x + 1$  δεν αναλύεται σε γινόμενο δύο πολυωνύμων μικρότερου βαθμού στον  $\mathbb{Z}_5[x]$ . Άρα από το (β) έχουμε ότι το  $f(x)$  είναι ανάγωγο στον  $\mathbb{Q}[x]$ .

## ΑΛΓΕΒΡΑ II – ΛΥΣΕΙΣ ΕΡΓΑΣΙΑΣ 3

### Παράγραφος 7.1

#### Άσκηση 27:

α) Τα μη μηδενικά στοιχεία του  $\mathbb{Z}_p$  είναι τα  $1, 2, \dots, p-1$ . Έστω ότι ισχύει η υπόθεση, τότε τα στοιχεία  $1, 2^2, \dots, (p-1)^2$  θα έπρεπε να είναι όλα διαφορετικά και να είναι μία μετάθεση των  $1, 2, \dots, p-1$ . Όμως παρατηρούμε ότι  $1^2 = (p-1)^2 = 1$ . Άτοπο.

β) Για  $p \neq 2$ : Αφού από α) δεν είναι κάθε στοιχείο του  $\mathbb{Z}_p$  το τετράγωνο κάποιου στοιχείου του  $\mathbb{Z}_p$ , θα υπάρχει  $c \in \mathbb{Z}_p$  έτσι ώστε το πολυώνυμο  $p(x) = x^2 - c$  να είναι ανάγωγο στον  $\mathbb{Z}_p$ .

Από το Θεώρημα 7.1 γνωρίζουμε ότι υπάρχει μία επέκταση σώματος  $E$  του  $\mathbb{Z}_p$  που περιέχει μία ρίζα  $\alpha$  του  $p(x)$ . Από το Θεώρημα 7.4, το  $\mathbb{Z}_p(\alpha)$  έχει ως στοιχεία τα  $0 + 0\alpha, 0 + 1\alpha, \dots, 0 + (p-1)\alpha, 1 + 0\alpha, \dots, 1 + (p-1)\alpha, \dots, (p-1) + 0\alpha, \dots, (p-1) + (p-1)\alpha$ . Παίρνουμε έτσι ένα νέο σώμα με  $p^2$  στοιχεία.

Τέλος, για  $p = 2$  έχουμε (από το Παράδειγμα 9, σελ. 424) ότι το  $p(x) = x^2 + x + 1$  είναι ανάγωγο στον  $\mathbb{Z}_2[x]$  και ότι το αντίστοιχο σώμα  $\mathbb{Z}_2[\alpha]$  έχει 4 στοιχεία.

Άσκηση 28: Από την υπόθεση, το  $\alpha$  είναι υπερβατικό πάνω από το  $F$  και άρα το  $F(\alpha)$  είναι το μικρότερο υπόσωμα του  $E$  που το περιέχει. Έστω  $\beta \in F(\alpha)$ . Τότε  $\beta = \frac{p(\alpha)}{q(\alpha)} \in F(\alpha)$ , όπου  $p(x), q(x) \in F[x]$ . Αν υπήρχε  $g(x) = c_n x^n + \dots + c_0 \in F[x]$  τέτοιο ώστε  $g(\beta) = 0$ , θα είχαμε ισοδύναμα :

$$g\left(\frac{p(\alpha)}{q(\alpha)}\right) = 0 \Leftrightarrow c_n \left(\frac{p(\alpha)}{q(\alpha)}\right)^n + \dots + c_1 \left(\frac{p(\alpha)}{q(\alpha)}\right) + c_0 = 0 \quad (1)$$

και πολλαπλασιάζοντας με  $(q(\alpha))^n$  έχουμε

$$(1) \Leftrightarrow c_n (p(\alpha))^n + \dots + (q(\alpha))^{n-1} c_1 p(\alpha) + (q(\alpha))^n c_0 = 0$$

$\Leftrightarrow \alpha$  ρίζα κάποιου πολυωνύμου στο  $F[x]$ .

### Παράγραφος 7.4

#### Άσκηση 15:

ζ) Λάθος.

η) Λάθος, αφού από Θεώρημα 7.17 γνωρίζουμε ότι κάθε σώμα έχει αλγεβρική θήκη.

θ) Λάθος, για παράδειγμα η αλγεβρική θήκη του  $\mathbb{Z}_p$ . Αφού η αλγεβρική θήκη του  $\mathbb{Z}_p$  είναι σώμα και περιέχει ως υπόσωμα το  $\mathbb{Z}_p$ , θα έχει χαρακτηριστική  $p$ , από Θεώρημα 5.12.

Άσκηση 29: Έστω ένα πεπερασμένο σώμα  $F$  με  $n+1$  μη μηδενικά στοιχεία  $1, a_1, \dots, a_n$  και με περιττή χαρακτηριστική  $p$ . Αν το  $F$  ήταν αλγεβρικά κλειστό, τότε θα έπρεπε κάθε πολυώνυμο της μορφής  $x^2 - a$  για  $a \in F$  να έχει ρίζα στο  $F$ . Ισοδύναμα μπορούμε να πούμε ότι θα έπρεπε κάθε στοιχείο  $a$  του  $F$  να είναι το τετράγωνο κάποιου στοιχείου του  $F$ . Τότε τα  $1^2, a_1^2, \dots, a_n^2$  θα έπρεπε να είναι πάλι όλα τα μη μηδενικά στοιχεία του  $F$ , άρα διαφορετικά μεταξύ τους. Όμως στην Άσκηση 27 της Παραγράφου 7.1 δείξαμε ότι για  $p \neq 2$  έχουμε  $1^2 = (p-1)^2 = 1$  στο  $\mathbb{Z}_p$ . Επίσης από το Θεώρημα 5.12 γνωρίζουμε ότι το  $F$  περιέχει ένα υπόσωμα ισόμορφο με το  $\mathbb{Z}_p$ . Άρα θα υπάρχει ένα στοιχείο  $a_i^2 \in F$ , αντίστοιχο του  $p-1$ , τέτοιο ώστε  $a_i^2 = 1^2 = 1$ , άτοπο. Δηλαδή, δεν υπάρχει πεπερασμένο σώμα με περιττή χαρακτηριστική που να είναι αλγεβρικά κλειστό.

Άσκηση 30: Έστω η απλή επέκταση  $\mathbb{Q}(2^{1/2})$  του  $\mathbb{Q}$ . Στο Παράδειγμα 3 σελ. 451 υπολογίζεται ότι η βάση αυτής της επέκτασης έχει βαθμό 2 πάνω από το  $\mathbb{Q}$ . Επίσης, παρατηρούμε ότι το  $\{1, 2^{1/3}, 2^{2/3}\}$  είναι μία βάση του  $\mathbb{Q}(2^{1/3})$  πάνω από το  $\mathbb{Q}$ , καθώς και του  $\mathbb{Q}(2^{1/2}, 2^{1/3})$  πάνω από το  $\mathbb{Q}(2^{1/2})$ . Δηλαδή η επέκταση του  $\mathbb{Q}(2^{1/2}, 2^{1/3})$  πάνω από το  $\mathbb{Q}(2^{1/2})$  έχει βαθμό 3. Επίσης, έχουμε ότι  $\mathbb{Q}(2^{1/2}, 2^{1/3}) = \mathbb{Q}(2^{1/6})$ , εφόσον έχουν βάση 6 πάνω από το  $\mathbb{Q}$ .

Γενικά παρατηρούμε ότι η επέκταση της μορφής  $\mathbb{Q}(2^{1/p_1})$  πάνω από το  $\mathbb{Q}$ , όπου  $p_1$  πρώτος έχει βαθμό  $p_1$  και μία βάση του αποτελείται από τα στοιχεία  $\{1, 2^{1/p_1}, 2^{2/p_1}, \dots, 2^{(p_1-1)/p_1}\}$ . Τότε η βάση μίας επέκτασης  $\mathbb{Q}(2^{1/p_2})$  πάνω από το  $\mathbb{Q}(2^{1/p_1})$ , όπου  $p_1 \neq p_2$  και  $p_1, p_2$  πρώτοι, αποτελείται από τα στοιχεία  $\{1, 2^{1/p_2}, 2^{2/p_2}, \dots, 2^{(p_2-1)/p_2}\}$  και έχει βαθμό  $p_2$ . Άρα σύμφωνα με το σχόλιο που ακολουθεί το Θεώρημα 7.13, η βάση μίας επέκτασης της μορφής  $\mathbb{Q}(2^{1/p_1}, 2^{1/p_2})$  πάνω από το  $\mathbb{Q}$ , όπου  $p_1 \neq p_2$  πρώτοι, έχει βαθμό  $p_1 p_2$ . Έστω λοιπόν μία επέκταση  $\mathbb{Q}(2^{1/p_1}, 2^{1/p_2}, \dots, 2^{1/p_k})$  πάνω από το  $\mathbb{Q}$ , όπου  $p_i, i=1, \dots, k$  πρώτοι και όλοι διαφορετικοί μεταξύ τους. Τότε πάντα μπορεί να βρεθεί πρώτος αριθμός  $q > p_i, \forall i=1, \dots, k$ . Για αυτόν θα έχουμε ότι η επέκταση  $\mathbb{Q}(2^{1/p_1}, 2^{1/p_2}, \dots, 2^{1/p_k}, 2^{1/q})$  είναι επέκταση του  $\mathbb{Q}(2^{1/p_1}, 2^{1/p_2}, \dots, 2^{1/p_k})$ , διότι αν δεν ήταν θα είχαμε

$$\mathbb{Q} \leq \mathbb{Q}(2^{1/q}) \leq \mathbb{Q}(2^{1/p_1}, 2^{1/p_2}, \dots, 2^{1/p_k})$$

και από το Θεώρημα 7.13 έχουμε ότι

$$\begin{aligned} p_1 p_2 \dots p_k &= [\mathbb{Q}(2^{1/p_1}, 2^{1/p_2}, \dots, 2^{1/p_k}, 2^{1/q}) : \mathbb{Q}] \\ &= [\mathbb{Q}(2^{1/p_1}, 2^{1/p_2}, \dots, 2^{1/p_k}) : \mathbb{Q}(2^{1/q})] [\mathbb{Q}(2^{1/q}) : \mathbb{Q}] \\ &= [\mathbb{Q}(2^{1/p_1}, 2^{1/p_2}, \dots, 2^{1/p_k}) : \mathbb{Q}(2^{1/q})] (q) \\ &\Rightarrow [\mathbb{Q}(2^{1/p_1}, 2^{1/p_2}, \dots, 2^{1/p_k}) : \mathbb{Q}(2^{1/q})] = (p_1 p_2 \dots p_k) / q \end{aligned}$$

που είναι άτοπο, αφού ο βαθμός της επέκτασης θα πρέπει να είναι ακέραιος αριθμός. Άρα αυτή η διαδικασία μπορεί να συνεχίζεται επ'άπειρον.