

**ΒΑΣΙΚΗ ΑΛΓΕΒΡΑ**  
**Χειμερινό Εξάμηνο 2017**

**Ασκήσεις**

1. Δείξτε ότι ο  $a - 1$  διαιρεί τον  $a^n - 1$  για κάθε  $a \in \mathbb{Z}$  και κάθε  $n \in \mathbb{N}$ .
2. Δίνονται οι ακέραιοι  $a = 126$  και  $b = 434$ .
  - (α) Υπολογίστε το  $\mu\kappa\delta(a, b)$ .
  - (β) Βρείτε  $x, y \in \mathbb{Z}$  τέτοια ώστε να ισχύει  $\mu\kappa\delta(a, b) = ax + by$ .
  - (γ) Υπάρχουν  $x, y$  όπως στο (β), για τα οποία το  $y$  είναι ακέραιο πολλαπλάσιο του 3;
3. Υπολογίστε το υπόλοιπο της διαίρεσης του  $2^{2012}$  με το 13. Υπόδειξη: Δείξτε πρώτα ότι  $2^6 \equiv -1 \pmod{13}$ .
4. Δίνεται θετικός ακέραιος  $n$ .
  - (α) Δείξτε ότι αν  $a, b$  είναι ακέραιοι οι οποίοι διαιρούν το  $5^n$ , τότε ο  $a$  διαιρεί τον  $b$ , ή ο  $b$  διαιρεί τον  $a$ .
  - (β) Για ποια  $c \in \{1, 2, \dots, 9\}$  η προηγούμενη πρόταση παύει να ισχύει αν το  $5^n$  αντικατασταθεί με το  $c^n$ ;
5. Δίνονται ακέραιοι  $a, b, m, n$  με  $m, n \geq 1$ .
  - (α) Αν  $a \equiv b \pmod{m}$ , δείξτε ότι  $\mu\kappa\delta(a, m) = \mu\kappa\delta(b, m)$ .
  - (β) Έστω ότι  $a \geq 2$ . Χρησιμοποιώντας το (α), δείξτε ότι
$$\mu\kappa\delta\left(\frac{a^n - 1}{a - 1}, a - 1\right) = \mu\kappa\delta(n, a - 1).$$
  - (γ) Έστω ότι  $a \geq 2$ . Δείξτε ότι  $\mu\kappa\delta(a^m - 1, a^n - 1) = a^d - 1$ , όπου  $d = \mu\kappa\delta(m, n)$ .
  - (δ) Συνάγετε από το (γ) ότι  $\mu\kappa\delta(2^m - 1, 2^n - 1) = 1$  αν και μόνο αν  $\mu\kappa\delta(m, n) = 1$ .
6. Δείξτε ότι  $5^n \equiv 1 + 4n \pmod{16}$  για κάθε  $n \in \mathbb{N}$ .

7. Για  $m = 14$  και  $m = 15$ :

- (α) Βρείτε όλα τα αντιστρέψιμα στοιχεία του  $\mathbb{Z}_m$ . Για καθένα από αυτά, υπολογίστε το αντίστροφο στοιχείο.
- (β) Υπολογίστε το άθροισμα και το γινόμενο των αντιστρέψιμων στοιχείων του  $\mathbb{Z}_m$ .

8. Για πόσους ακεραίους  $a \in \{1, 2, \dots, 1000\}$  ισχύει  $\mu\kappa\delta(a, 1000) = 4$ ;

9. Για πόσα ζεύγη  $(x, y)$  στοιχείων του  $\mathbb{Z}_{200}$  ισχύει  $x^3y = 1$  στο  $\mathbb{Z}_{200}$ ;

10. Συμβολίζουμε με  $\varphi : \mathbb{Z}_{>0} \rightarrow \mathbb{Z}$  τη συνάρτηση του Euler.

- (α) Υπολογίστε το  $\varphi(100)$ .
- (β) Δείξτε ότι  $3^{1000} \equiv 1 \pmod{100}$ .
- (γ) Βρείτε όλα τα  $x \in \mathbb{Z}$  που επαληθεύουν την ισοτιμία  $3x \equiv 1 \pmod{100}$ .
- (δ) Χρησιμοποιώντας τα (β) και (γ), υπολογίστε τα δύο τελευταία δεκαδικά ψηφία του αριθμού  $3^{999}$ .

11. Χρησιμοποιώντας το Θεώρημα του Euler:

- (α) Δείξτε ότι το  $a^6 - 1$  διαιρείται με το 252 για κάθε  $a \in \mathbb{Z}$  με  $\mu\kappa\delta(a, 42) = 1$ .
- (β) Δείξτε ότι το  $a^8 - a^2$  διαιρείται με το 252 για κάθε  $a \in \mathbb{Z}$ .

Συνάγετε ότι ο 252 είναι ο μεγαλύτερος θετικός ακεραίος που διαιρεί το  $a^8 - a^2$  για κάθε  $a \in \mathbb{Z}$ .

12. Για ποιους θετικούς ακεραίους  $m$  είναι ο  $\varphi(m)$  περιττός αριθμός;

13. Ποιες από τις παρακάτω αντιστοιχίες ορίζουν πράξεις στο σύνολο  $S$  που δίνεται;

- (α)  $S = \mathbb{Z} \setminus \{0\}$  και  $a \circ b = a + b$ , για  $a, b \in S$ .
- (β)  $S = \mathbb{Z} \setminus \{0\}$  και  $a * b = ab$ , για  $a, b \in S$ .
- (γ)  $S = \mathbb{Z}_3$  και  $\bar{a} \circ \bar{b} = \overline{\max(a, b)}$ , για  $a, b \in \{0, 1, 2\}$  (όπου  $\bar{x}$  είναι η κλάση mod 3 του  $x \in \mathbb{Z}$ ).
- (δ)  $S = \mathbb{Z}_3$  και  $\bar{a} * \bar{b} = \overline{\max(a, b)}$ , για  $a, b \in \mathbb{Z}$ .

14. Δίνεται δακτύλιος  $R$  και το σύνολο  $S = R \times R$ , εφοδιασμένο με πράξεις πρόσθεσης  $\oplus : S \times S \rightarrow S$  και πολλαπλασιασμού  $\odot : S \times S \rightarrow S$  που ορίζονται θέτοντας

$$\begin{aligned}(a, b) \oplus (c, d) &= (a + c, b + d) \\ (a, b) \odot (c, d) &= (ac, ad + bc)\end{aligned}$$

για  $a, b, c, d \in R$ .

- (α) Δείξτε ότι, εφοδιασμένο με τις πράξεις αυτές, το σύνολο  $S$  αποτελεί δακτύλιο.
- (β) Δείξτε ότι ο  $S$  έχει μονάδα (αντίστοιχα, είναι μεταθετικός δακτύλιος) αν και μόνο αν ο  $R$  έχει μονάδα (αντίστοιχα, είναι μεταθετικός δακτύλιος).
- (γ) Έστω ότι ο  $S$  έχει μονάδα. Ποια είναι τα αντιστρέψιμα στοιχεία του  $S$ ;
- (δ) Υπάρχει δακτύλιος  $R$  για τον οποίο ο  $S$  είναι ακέραια περιοχή;

**15.** Δίνεται μεταθετικός δακτύλιος  $R$  με μονάδα και ο δακτύλιος  $M_2(R)$  των  $2 \times 2$  πινάκων με στοιχεία από το  $R$ .

- (α) Δείξτε ότι ισχύει η ταυτότητα

$$(ax + bz)(cy + dw) - (ay + bw)(cx + dz) = (ad - bc)(xw - yz)$$

για  $a, b, c, d, x, y, w, z \in R$ .

- (β) Για  $a, b, c, d \in R$ , δείξτε ότι

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U(M_2(R)) \Leftrightarrow ad - bc \in U(R).$$

- (γ) Πόσα στοιχεία έχει συνολικά ο  $M_2(R)$ , αν  $R = \mathbb{Z}_p$ ; Πόσα από αυτά είναι αντιστρέψιμα, αν  $R = \mathbb{Z}_p$  και ο  $p$  είναι πρώτος αριθμός;

**16.** Δώστε παράδειγμα μεταθετικού δακτυλίου με μονάδα, ο οποίος περιέχει τουλάχιστον τέσσερα αντιστρέψιμα στοιχεία  $a$  για τα οποία ισχύει  $a^{-1} = a$ . Υπάρχει ακέραια περιοχή με την ίδια ιδιότητα;

**17.** Ποια από τα παρακάτω σύνολα είναι υποδακτύλιοι του  $M_2(\mathbb{Z})$ ;

- (α)  $\left\{ \begin{pmatrix} a & a \\ 0 & a \end{pmatrix} : a \in \mathbb{Z} \right\}$ .
- (β)  $\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$ .
- (γ)  $\left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$ .
- (δ)  $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc \geq 0 \right\}$ .

**18.** Ποιες από τις παρακάτω προτάσεις είναι αληθείς;

- (α) Το σύνολο  $(m\mathbb{Z}) \times (n\mathbb{Z})$  είναι υποδακτύλιος του  $\mathbb{Z} \times \mathbb{Z}$  για όλα τα  $m, n \in \mathbb{N}$ .
- (β) Κάθε υποδακτύλιος του  $\mathbb{Z} \times \mathbb{Z}$  είναι της μορφής  $(m\mathbb{Z}) \times (n\mathbb{Z})$  για κάποια  $m, n \in \mathbb{N}$ .

**19.** Για καθένα από τα σώματα  $F \in \{\mathbb{R}, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5\}$  να εξετάσετε αν υπάρχουν μη μηδενικά πολυώνυμα  $f(x), g(x) \in F[x]$  για τα οποία ο βαθμός του  $(f(x))^2 + (g(x))^2$  είναι περιττός αριθμός.

**20.** Δίνεται μεταθετικός δακτύλιος  $R$  με μονάδα και πολυώνυμο  $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$  βαθμού  $n$ .

- (α) Αν το  $f(x)$  είναι αντιστρέψιμο στο  $R[x]$ , δείξτε ότι  $a_0 \in U(R)$  και ότι το  $a_n$  είναι μηδενοδιαίρετης στο  $R$ .
- (β) Δώστε παράδειγμα μεταθετικού δακτυλίου  $R$  με μονάδα και μη αντιστρέψιμου πολυωνύμου  $f(x) \in R[x]$ , τέτοια ώστε να ισχύει  $a_0 \in U(R)$  και το  $a_n$  να είναι μηδενοδιαίρετης στο  $R$ .

**21.** Δίνεται μεταθετικός δακτύλιος  $R$  και πολυώνυμο  $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$ . Για  $g(x) \in R[x]$  θέτουμε

$$f(g(x)) = a_0 + a_1g(x) + \dots + a_n(g(x))^n.$$

Δείξτε ότι για όλα τα πολυώνυμα  $p(x), q(x) \in R[x]$ :

- (α) Το  $p(x) - q(x)$  διαιρεί το  $(p(x))^k - (q(x))^k$  στο  $R[x]$  για κάθε θετικό ακέραιο  $k$ .
- (β) Το  $p(x) - q(x)$  διαιρεί το  $f(p(x)) - f(q(x))$  στο  $R[x]$ .

**22.** Ποιες από τις παρακάτω προτάσεις είναι αληθείς;

- (α) Αν  $f(x), g(x) \in \mathbb{Z}[x]$  και το  $g(x)$  διαιρεί το  $f(x)$  στο  $\mathbb{Z}[x]$ , τότε το  $g(m)$  διαιρεί το  $f(m)$  στο  $\mathbb{Z}$  για κάθε  $m \in \mathbb{Z}$ .
- (β) Αν  $f(x), g(x) \in \mathbb{Z}[x]$  και το  $g(m)$  διαιρεί το  $f(m)$  στο  $\mathbb{Z}$  για κάθε  $m \in \mathbb{Z}$ , τότε το  $g(x)$  διαιρεί το  $f(x)$  στο  $\mathbb{Z}[x]$ .

**23.** Υπολογίστε το μέγιστο κοινό διαιρέτη των  $f(x) = x^5 - x^2 - x + 1$  και  $g(x) = x^3 + 1$  στο  $\mathbb{Q}[x]$  και στο  $\mathbb{Z}_3[x]$ .

**24.** Δίνεται το πολυώνυμο  $f(x) = x^5 + 3x^4 + 3x^3 + 4x^2 + 2 \in \mathbb{Z}_5[x]$ .

(α) Βρείτε όλες τις ρίζες του  $f(x)$  στο  $\mathbb{Z}_5$ .

(β) Εκφράστε το  $f(x)$  ως γινόμενο ανάγωγων πολυωνύμων του  $\mathbb{Z}_5[x]$ .

**25.** Βρείτε όλα τα πολυώνυμα  $p(x) \in \mathbb{Z}[x]$  για τα οποία ισχύει  $(x+1)p(x) = xp(x+1)$ .

**26.** Ποιες από τις παρακάτω προτάσεις είναι αληθείς;

(α) Για μη μηδενικά πολυώνυμα  $f(x), g(x) \in \mathbb{R}[x]$  ισχύει  $\mu\kappa\delta(f(x), g(x)) \neq 1$  αν και μόνο αν τα  $f(x)$  και  $g(x)$  έχουν τουλάχιστον μία κοινή ρίζα στο  $\mathbb{R}$ .

(β) Για μη μηδενικά πολυώνυμα  $f(x), g(x) \in \mathbb{C}[x]$  ισχύει  $\mu\kappa\delta(f(x), g(x)) \neq 1$  αν και μόνο αν τα  $f(x)$  και  $g(x)$  έχουν τουλάχιστον μία κοινή ρίζα στο  $\mathbb{C}$ .

**27.** Δίνεται πρώτος αριθμός  $p$ .

(α) Βρείτε πολυώνυμο  $f(x) \in \mathbb{Q}[x]$  βαθμού  $p$  το οποίο δεν έχει ρίζες στο  $\mathbb{Q}$ .

(β) Βρείτε πολυώνυμο  $f(x) \in \mathbb{Z}_p[x]$  βαθμού  $p$  το οποίο δεν έχει ρίζες στο  $\mathbb{Z}_p$ .

(γ) Υπάρχει πολυώνυμο  $f(x) \in \mathbb{R}[x]$  βαθμού  $p$  το οποίο δεν έχει ρίζες στο  $\mathbb{R}$ ;

**28.** Ποιοι από τους παρακάτω υποδακτυλίους του  $M_2(\mathbb{Z})$  είναι ισόμορφοι με το δακτύλιο  $\mathbb{Z} \times \mathbb{Z}$ ;

(α)  $\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z} \right\}$ .

(β)  $\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$ .

**29.** Θεωρούμε τον υποδακτύλιο  $2\mathbb{Z}$  του  $\mathbb{Z}$ .

(α) Ποια είναι τα κύρια ιδεώδη του  $2\mathbb{Z}$ ;

(β) Είναι κάθε ιδεώδες του  $2\mathbb{Z}$  κύριο;

**30.** Δίνεται η απεικόνιση  $\varphi : \mathbb{Z}[\sqrt{2}] \rightarrow \mathbb{Z}_7$  που ορίζεται θέτοντας  $\varphi(a + b\sqrt{2}) = \bar{a} + 3\bar{b}$  για  $a, b \in \mathbb{Z}$  (όπου με  $\bar{x}$  συμβολίζουμε την κλάση mod 7 του  $x \in \mathbb{Z}$ ).

(α) Δείξτε ότι η  $\varphi$  είναι ομομορφισμός δακτυλίων.

(β) Υπολογίστε τον πυρήνα και την εικόνα του  $\varphi$ .

(γ) Είναι ο πυρήνας του  $\varphi$  κύριο ιδεώδες του  $\mathbb{Z}[\sqrt{2}]$ ;

**31.** Αν  $F$  είναι σώμα, δείξτε ότι κάθε μη μηδενικός ομομορφισμός δακτυλίων  $\varphi : F \rightarrow S$  είναι μονομορφισμός.

**32.** Για  $\alpha \in \mathbb{R}$  θέτουμε  $\mathcal{I}(\alpha) = \{f(x) \in \mathbb{Q}[x] : f(\alpha) = 0\}$ .

(α) Δείξτε ότι το  $\mathcal{I}(\alpha)$  είναι ιδεώδες του  $\mathbb{Q}[x]$  για κάθε  $\alpha \in \mathbb{R}$ .

(β) Δείξτε ότι για κάθε  $m \in \mathbb{N}$  υπάρχουν ακέραιοι  $a_m$  και  $b_m$  για τους οποίους ισχύει  $(1 + \sqrt{2})^m = a_m + b_m\sqrt{2}$  και  $(1 - \sqrt{2})^m = a_m - b_m\sqrt{2}$ .

(γ) Χρησιμοποιώντας το (β), δείξτε ότι  $\mathcal{I}(1 + \sqrt{2}) = \mathcal{I}(1 - \sqrt{2})$ .

(δ) Βρείτε πολυώνυμο  $g(x) \in \mathbb{Q}[x]$  τέτοιο ώστε  $\mathcal{I}(1 + \sqrt{2}) = \langle g(x) \rangle$ , όπου  $\langle g(x) \rangle$  είναι το κύριο ιδεώδες του  $\mathbb{Q}[x]$  που παράγεται από το  $g(x)$ .

**33.** Δίνεται ο δακτύλιος - πηλίκο  $R = \mathbb{Z}_2[x] / \langle x^3 + 1 \rangle$  και η κλάση  $\alpha = x + \langle x^3 + 1 \rangle$  του  $x$  στον  $R$ .

(α) Περιγράψτε τα στοιχεία του  $R$  ως πολυώνυμα στο  $\alpha$  με συντελεστές από το  $\mathbb{Z}_2$ .

(β) Δείξτε ότι  $\alpha^3 = 1$  και ότι  $(1 + \alpha)(1 + \alpha + \alpha^2) = 0$ .

(γ) Ποια στοιχεία του  $R$  είναι αντιστρέψιμα;

**34.** Ποιοι από τους παρακάτω δακτυλίους είναι μεταξύ τους ισόμορφοι;

(α)  $\mathbb{Z}_5[x] / \langle x^2 + 1 \rangle$

(β)  $\mathbb{Z}_5[x] / \langle x^2 + 2 \rangle$

(γ)  $\mathbb{Z}_7[x] / \langle x^2 + 2 \rangle$ .

**35.** Θεωρούμε το δακτύλιο  $R = T_2(\mathbb{Z})$  των  $2 \times 2$  άνω τριγωνικών πινάκων με στοιχεία από το  $\mathbb{Z}$  και το υποσύνολό του

$$\mathcal{I} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a \in m\mathbb{Z}, b \in \mathbb{Z}, c \in n\mathbb{Z} \right\},$$

όπου  $m, n$  είναι θετικοί ακέραιοι.

(α) Δείξτε ότι το  $\mathcal{I}$  είναι ιδεώδες του  $R$ .

(β) Δείξτε ότι ο δακτύλιος  $R/\mathcal{I}$  είναι ισόμορφος με τον  $\mathbb{Z}_m \times \mathbb{Z}_n$ .

**36.** Να εξετάσετε αν οι δακτύλιοι  $R$  και  $S$  είναι ισόμορφοι στις ακόλουθες περιπτώσεις:

(α)  $R = \mathbb{Z}_2[x] / \langle x^2 - 1 \rangle$  και  $S = \mathbb{Z}_2 \times \mathbb{Z}_2$ ,

(β)  $R = \mathbb{Z}_3[x] / \langle x^2 - 1 \rangle$  και  $S = \mathbb{Z}_3 \times \mathbb{Z}_3$ .

**37.** Ποιες από τις παρακάτω προτάσεις είναι αληθείς;

- (α) Αν  $p$  είναι πρώτος και για μονικά πολυώνυμα  $f(x), g(x) \in \mathbb{Z}_p[x]$  ισχύει  $\mathbb{Z}_p[x] / \langle f(x) \rangle \cong \mathbb{Z}_p[x] / \langle g(x) \rangle$ , τότε  $f(x) = g(x)$ .
- (β) Αν  $p$  είναι πρώτος και για μονικά πολυώνυμα  $f(x), g(x) \in \mathbb{Z}_p[x]$  ισχύει  $\mathbb{Z}_p[x] / \langle f(x) \rangle \cong \mathbb{Z}_p[x] / \langle g(x) \rangle$ , τότε  $\deg(f(x)) = \deg(g(x))$ .

**38.** Δίνονται οι μεταθέσεις

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 1 & 2 & 6 & 8 & 5 & 7 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 2 & 5 & 8 & 1 & 4 & 6 & 3 \end{pmatrix}$$

της  $\mathcal{S}_8$ .

- (α) Υπολογίστε τις  $\sigma\tau$ ,  $\tau\sigma$ ,  $\sigma^{-1}$  και  $\tau^{-1}$ .
- (β) Υπολογίστε τη μετάθεση  $(\sigma\tau)^{1000}$ .

**39.** Δίνεται η μετάθεση

$$\sigma = (1\ 2)(1\ 3)(1\ 4)(1\ 5)(2\ 3)(2\ 4)(2\ 5)(3\ 4)(3\ 5)(4\ 5) \in \mathcal{S}_5.$$

- (α) Γράψτε τη  $\sigma$  ως γινόμενο ξένων κύκλων.
- (β) Συνάγετε ότι η  $\sigma^2$  είναι η ταυτοτική μετάθεση.
- (γ) Βρείτε  $\tau \in \mathcal{S}_5$  για την οποία η μετάθεση  $\sigma\tau$  είναι κυκλική.

**40.** Μια μετάθεση  $\sigma \in \mathcal{S}_n$  έχει σταθερό σημείο αν υπάρχει  $i \in \{1, 2, \dots, n\}$  τέτοιο ώστε  $\sigma(i) = i$ . Βρείτε όλους τους θετικούς ακεραίους  $n$  για τους οποίους ισχύει η εξής πρόταση: Αν  $\sigma \in \mathcal{S}_n$  και η  $\sigma^2$  έχει σταθερό σημείο, τότε η  $\sigma$  έχει επίσης σταθερό σημείο.

**41.** Θεωρούμε μεταθέσεις  $\sigma, \tau \in \mathcal{S}_n$ .

- (α) Αν η  $\sigma\tau$  έχει σταθερό σημείο, δείξτε ότι η  $\tau\sigma$  έχει επίσης σταθερό σημείο.
- (β) Αν η  $\sigma\tau$  είναι κυκλική μετάθεση, δείξτε ότι η  $\tau\sigma$  είναι επίσης κυκλική μετάθεση.

42. Δίνεται ομάδα  $G$  και στοιχεία  $a, b, e \in G$  με  $a^2 = b^3 = e^2 = e$ .

(α) Δείξτε ότι το  $e$  είναι το ταυτοτικό στοιχείο της  $G$ .

(β) Αν  $ab = ba$ , δείξτε ότι  $(ab)^6 = e$ .

(γ) Ισχύει το (β) χωρίς την υπόθεση  $ab = ba$ ;

43. Δίνεται η μετάθεση

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 1 & 4 & 7 & 10 & 13 & 2 & 5 & 8 & 11 & 14 & 3 & 6 & 9 & 12 & 15 \end{pmatrix} \in \mathcal{S}_{15}.$$

(α) Υπολογίστε την τάξη της  $\sigma$  και της  $\sigma^{64}$ .

(β) Βρείτε μετάθεση  $\tau \in \mathcal{S}_{15}$  τέτοια ώστε  $\sigma = \tau^2$ .

44. Πόσα στοιχεία της συμμετρικής ομάδας  $\mathcal{S}_5$  έχουν τάξη ίση με 3;

45. Δίνεται ομάδα  $G$  τάξης 4 με ταυτοτικό στοιχείο  $e \in G$ .

(α) Δείξτε ότι είτε  $G = \{e, a, a^2, a^3\}$  για κάποιο  $a \in G$  με  $a^4 = e$ , είτε  $G = \{e, a, b, ab\}$  για κάποια  $a, b \in G$  με  $a^2 = b^2 = e$  και  $ab = ba$ .

(β) Συνάγετε ότι κάθε ομάδα τάξης 4 είναι αβελιανή.

46. Δίνεται η ομάδα  $G = \text{GL}_2(\mathbb{R})$  των αντιστρέψιμων  $2 \times 2$  πινάκων με στοιχεία από το  $\mathbb{R}$ . Ποια από τα παρακάτω σύνολα είναι υποομάδες της  $G$ ; Ποια είναι κυκλικές υποομάδες της  $G$ ;

(α)  $\left\{ \begin{pmatrix} 1 & 2a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{Z} \right\}$ .

(β)  $\left\{ \begin{pmatrix} 1+a & -a \\ a & 1-a \end{pmatrix} : a \in \mathbb{R} \right\}$ .

(γ)  $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \geq 1 \right\}$ .

47. Δίνεται η ομάδα  $G$  των συμμετριών του τετραγώνου (θεωρούμε γνωστό ότι η τάξη της  $G$  είναι ίση με 8). Ποιες από τις παρακάτω προτάσεις είναι αληθείς;

(α) Υπάρχει κυκλική υποομάδα της  $G$  τάξης 4.

(β) Κάθε γνήσια υποομάδα της  $G$  είναι αβελιανή.

(γ) Κάθε γνήσια υποομάδα της  $G$  είναι κυκλική.



48. Δίνεται ομάδα  $G$  τάξης  $2n$  και υποομάδα  $H$  αυτής τάξης  $n$ .

- (α) Πόσες είναι οι αριστερές κλάσεις της  $H$  στη  $G$ ;
- (β) Δείξτε ότι  $a, b \in G \setminus H \Rightarrow ab \in H$ .

49. Δίνονται οι μεταθέσεις

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$$

της  $S_6$ .

- (α) Υπολογίστε τη μετάθεση  $\sigma\tau\sigma^{-1}$ .
- (β) Δείξτε ότι οι  $\sigma$  και  $\tau$  ανήκουν σε μια υποομάδα τάξης 6 της  $S_6$ .
- (γ) Υπάρχει υποομάδα τάξης 8 της  $S_6$  που περιέχει τις  $\sigma$  και  $\tau$ ;

50. Δίνεται ομάδα  $G$  τάξης 25 η οποία δεν έχει στοιχεία τάξης 25.

- (α) Δείξτε ότι κάθε γνήσια υποομάδα της  $G$  είναι κυκλική.
- (β) Πόσες γνήσιες υποομάδες μπορεί να έχει η  $G$ ;

51. Θεωρούμε την ομάδα  $G = GL_n(\mathbb{R})$  των αντιστρέψιμων  $n \times n$  πινάκων με στοιχεία από το  $\mathbb{R}$  και την απεικόνιση  $\varphi : G \rightarrow G$  που ορίζεται θέτοντας  $\varphi(A) = \det(A) \cdot A$  για  $A \in G$ .

- (α) Δείξτε ότι η  $\varphi$  είναι ομομορφισμός ομάδων.
- (β) Βρείτε όλους τους θετικούς ακεραίους  $n$  για τους οποίους η  $\varphi$  είναι αυτομορφισμός της  $G$ .

52. Δίνεται η μετάθεση

$$w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 4 & 3 & 8 & 1 & 2 & 5 & 6 \end{pmatrix} \in \mathcal{S}_8.$$

- (α) Είναι άρτια ή περιττή η  $w$ ;
- (β) Υπάρχουν μεταθέσεις  $\sigma, \tau \in \mathcal{S}_8$  τέτοιες ώστε  $w = \sigma\tau^2\sigma^{-1}$ ;

- 53.** Δίνεται η απεικόνιση  $\sigma : \mathbb{Z}_{12} \rightarrow \mathbb{Z}_{12}$  με  $\sigma(x) = x + 3$  για  $x \in \mathbb{Z}_{12}$ .
- (α) Δείξτε ότι η  $\sigma$  είναι μετάθεση του  $\mathbb{Z}_{12}$ .
  - (β) Είναι η μετάθεση αυτή άρτια ή περιπτή;
  - (γ) Υπάρχει απεικόνιση  $\tau : \mathbb{Z}_{12} \rightarrow \mathbb{Z}_{12}$  με  $\tau(\tau(x)) = \sigma(x)$  για κάθε  $x \in \mathbb{Z}_{12}$ ;
- 54.** Θεωρούμε ομομορφισμό ομάδων  $\varphi : \mathcal{S}_n \rightarrow \mathbb{C}^\times$ , όπου  $\mathbb{C}^\times$  είναι η πολλαπλασιαστική ομάδα των μη μηδενικών μιγαδικών αριθμών.
- (α) Δείξτε ότι  $\varphi(t) \in \{1, -1\}$  για κάθε αντιμετάθεση  $t \in \mathcal{S}_n$ .
  - (β) Δείξτε ότι  $\varphi(\sigma) \in \{1, -1\}$  για κάθε μετάθεση  $\sigma \in \mathcal{S}_n$ .
  - (γ) Βρείτε όλους τους ομομορφισμούς  $\varphi$  για  $n = 3$ .
- 55.** Ποιες από τις παρακάτω προτάσεις είναι αληθείς;
- (α) Αν ο δακτύλιος  $R$  είναι ισόμορφος με τον  $S$ , τότε η προσθετική ομάδα του  $R$  είναι ισόμορφη με την προσθετική ομάδα του  $S$ .
  - (β) Αν η προσθετική ομάδα ενός δακτυλίου  $R$  είναι ισόμορφη με την προσθετική ομάδα του  $S$ , τότε ο δακτύλιος  $R$  είναι ισόμορφος με τον  $S$ .
- 56.** Δίνεται πεπερασμένη ομάδα  $G$  η οποία περιέχει δύο διαφορετικά στοιχεία τάξης 2.
- (α) Δείξτε ότι η  $G$  δεν είναι κυκλική.
  - (β) Αν η  $G$  είναι αβελιανή, δείξτε ότι η τάξη της διαιρείται με το 4.
  - (γ) Ισχύει το (β) χωρίς την υπόθεση ότι η  $G$  είναι αβελιανή;
- 57.** Δίνεται κυκλική ομάδα  $G$  τάξης 24 με γεννήτορα  $a$ .
- (α) Βρείτε όλα τα στοιχεία των υποομάδων  $\langle a^{14} \rangle$  και  $\langle a^{42} \rangle$  της  $G$ .
  - (β) Βρείτε όλα τα στοιχεία της υποομάδας  $\langle a^{14} \rangle \cap \langle a^{39} \rangle$  της  $G$ .
- 58.** Ποιες από τις παρακάτω ομάδες είναι κυκλικές;
- (α)  $U(\mathbb{Z}_{18})$ .
  - (β)  $SL_2(\mathbb{Z}_2)$ .
  - (γ)  $U(\mathbb{Z}_2[x] / \langle x^3 \rangle)$ .
  - (δ)  $U(\mathbb{Z}_2[x] / \langle x^4 \rangle)$ .
- 59.** Δίνεται κυκλική ομάδα  $G$  τάξης 9 με γεννήτορα  $a$ .
- (α) Βρείτε όλους τους ομομορφισμούς ομάδων  $\varphi : G \rightarrow \mathcal{S}_3$ .
  - (β) Βρείτε όλους τους ομομορφισμούς ομάδων  $\psi : \mathcal{S}_3 \rightarrow G$ .

**60.** Δίνεται υποομάδα  $H = \{e, a\}$  τάξης 2 μιας ομάδας  $G$ .

- (α) Δείξτε ότι η  $H$  είναι κανονική υποομάδα της  $G$  αν και μόνο αν  $ax = xa$  για κάθε  $x \in G$ .
- (β) Βρείτε όλες τις κανονικές υποομάδες τάξης 2 της  $S_3$ , της ομάδας των συμμετριών του τετραγώνου και της  $SL_2(\mathbb{R})$ .

**61.** Δίνονται επιμορφισμός ομάδων  $\varphi : G \rightarrow K$  και ανά δύο διαφορετικά στοιχεία  $x, y, z$  της  $G$  τέτοια ώστε τα  $zxy^{-1}z^{-1}$  και  $xyz^{-1}x^{-1}$  να ανήκουν στον πυρήνα του  $\varphi$ .

- (α) Δείξτε ότι  $\varphi(x) = \varphi(y) = \varphi(z)$ .
- (β) Αν η  $G$  είναι πεπερασμένη, δείξτε ότι  $|G| \geq 3 \cdot |K|$ .

**62.** Θεωρούμε την ομάδα  $G = GL_n(\mathbb{Z}_p)$ , όπου  $p$  είναι πρώτος αριθμός, και την κανονική της υποομάδα  $N = SL_n(\mathbb{Z}_p)$ .

- (α) Δείξτε ότι η ομάδα πηλίκο  $G/N$  είναι ισόμορφη με την πολλαπλασιαστική ομάδα  $\mathbb{Z}_p^\times$  των μη μηδενικών στοιχείων του  $\mathbb{Z}_p$ . Ποια είναι η τάξη της  $G/N$ ;
- (β) Πόσες υποομάδες έχει η  $G/N$  για  $p = 31$ ;

**63.** Θεωρούμε την πολλαπλασιαστική ομάδα  $G = \mathbb{C}^\times$  των μη μηδενικών μιγαδικών αριθμών και την απεικόνιση  $\varphi : G \rightarrow G$  με  $\varphi(z) = z^2$  για  $z \in G$ .

- (α) Δείξτε ότι η  $\varphi$  είναι ομομορφισμός ομάδων και βρείτε τον πυρήνα και την εικόνα της.
- (β) Συνάγετε ότι υπάρχει γνήσια κανονική υποομάδα  $N$  της  $G$  για την οποία η ομάδα πηλίκο  $G/N$  είναι ισόμορφη με τη  $G$ .

**64.** Ποιες από τις παρακάτω προτάσεις είναι αληθείς;

- (α) Αν  $N_1$  και  $N_2$  είναι κανονικές υποομάδες μιας ομάδας  $G$  και η  $N_1$  είναι ισόμορφη με τη  $N_2$ , τότε η ομάδα πηλίκο  $G/N_1$  είναι ισόμορφη με τη  $G/N_2$ .
- (β) Αν  $N_1$  και  $N_2$  είναι κανονικές υποομάδες μιας ομάδας  $G$  και η ομάδα πηλίκο  $G/N_1$  είναι ισόμορφη με τη  $G/N_2$ , τότε η  $N_1$  είναι ισόμορφη με τη  $N_2$ .

## Σύντομες Λύσεις

1. Το ζητούμενο προκύπτει από την ταυτότητα  $a^n - 1 = (a - 1)(a^{n-1} + \dots + a + 1)$  για  $n \geq 1$  και είναι φανερό για  $n = 0$  (αφού τότε  $a^n - 1 = 0$ ).
2. Απάντηση για το (α):  $\mu\kappa\delta(a, b) = 14$ . Απάντηση για το (β):  $\mu\kappa\delta(a, b) = ax + by$ , όπου  $x = 7$  και  $y = -2$ . Το ερώτημα στο (γ) έχει αρνητική απάντηση αφού το 3 διαιρεί το  $a = 126$ , αλλά δε διαιρεί το  $\mu\kappa\delta(a, b) = 14$  (κατά συνέπεια, σε οποιαδήποτε ισότητα της μορφής  $\mu\kappa\delta(a, b) = ax + by$ , όπου  $x, y \in \mathbb{Z}$ , το  $y$  δεν είναι δυνατό να διαιρείται με το 3).
3. Παρατηρούμε ότι  $2^6 = 64 \equiv -1 \pmod{13}$ . Θεωρούμε την Ευκλείδεια διαίρεση  $2012 = 6q + 2$  του 2012 με το 6, όπου  $q = 335$ , και υπολογίζουμε ότι

$$2^{2012} = 2^{6q+2} = 4 \cdot (2^6)^q \equiv 4 \cdot (-1)^q = -4 \equiv 9 \pmod{13}.$$

Επομένως, το ζητούμενο υπόλοιπο είναι το 9.

4. Έστω ακέραιοι  $a$  και  $b$  οι οποίοι διαιρούν το  $5^n$ . Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι  $a, b \geq 1$ . Παρατηρούμε ότι ο μόνος πρώτος διαιρέτης του  $5^n$  είναι ο 5 (εξηγήστε γιατί). Αφού κάθε διαιρέτης του  $a$  είναι και διαιρέτης του  $5^n$ , το ίδιο πρέπει να ισχύει και για τον  $a$ . Από το Θεμελιώδες Θεώρημα της Αριθμητικής έπεται ότι  $a = 5^r$  για κάποιο  $r \in \mathbb{N}$ . Ομοίως βρίσκουμε ότι  $b = 5^s$  για κάποιο  $s \in \mathbb{N}$ , οπότε έχουμε  $b = a \cdot 5^{s-r}$  και  $a = b \cdot 5^{r-s}$ . Συμπεραίνουμε ότι ο  $a$  διαιρεί τον  $b$  αν  $r \leq s$ , και ότι ο  $b$  διαιρεί τον  $a$  αν  $s \leq r$ , και συνεπώς ότι ισχύει το (α). Το παραπάνω επιχείρημα εξακολουθεί να ισχύει αν το  $5^n$  αντικατασταθεί με το  $c^n$ , αρκεί το  $c$  να είναι δύναμη πρώτου αριθμού. Επιπλέον, στην περίπτωση  $c = 6$ , οι  $a = 2$  και  $b = 3$  είναι διαιρέτες του  $6^n$  κανέναν από τους οποίους δε διαιρεί τον άλλο. Άρα, η μόνη τιμή του  $c$  για το (β) είναι η  $c = 6$ .
5. (α) Υποθέτουμε ότι  $a - b = mq$  για κάποιο  $q \in \mathbb{Z}$  και θέτουμε  $d = \mu\kappa\delta(a, m)$  και  $e = \mu\kappa\delta(b, m)$ . Παρατηρούμε ότι το  $d$  διαιρεί το  $a$  και το  $m$  και συμπεραίνουμε ότι το  $d$  διαιρεί και το  $a - mq = b$ . Άρα, το  $d$  διαιρεί το  $b$  και το  $m$  και συνεπώς διαιρεί και το μέγιστο κοινό διαιρέτη αυτών  $e$ . Ομοίως βρίσκουμε ότι το  $e$  διαιρεί το  $d$  και συμπεραίνουμε ότι  $d = e$ .

(β) Σύμφωνα με το (α), αρκεί να δείξουμε ότι

$$\frac{a^n - 1}{a - 1} \equiv n \pmod{a - 1}.$$

Πράγματι, έχουμε  $a \equiv 1 \pmod{a - 1}$ , άρα  $a^k \equiv 1 \pmod{a - 1}$  για κάθε  $k \in \mathbb{N}$  και συνεπώς

$$\frac{a^n - 1}{a - 1} = a^{n-1} + a^{n-2} + \dots + a + 1 \equiv n \pmod{a - 1}.$$

(γ) Υποθέτουμε, χωρίς βλάβη της γενικότητας, ότι  $m \geq n$  και εφαρμόζουμε επαγωγή στο  $m$ . Το ζητούμενο είναι τετριμμένο για  $m = n$  (ειδικότερα για  $m = 1$ , οπότε και  $n = 1$ ). Υποθέτουμε ότι  $m > n \geq 1$  και ότι το ζητούμενο ισχύει για όλα τα ζεύγη θετικών ακεραίων μικρότερων του  $m$ . Σύμφωνα με την Ευκλείδεια διαίρεση, γράφουμε  $m = nq + r$  με  $q \in \mathbb{N}$  και  $r \in \{0, 1, \dots, n-1\}$ , οπότε  $d = \mu\kappa\delta(m, n) = \mu\kappa\delta(n, r)$ . Εργαζόμενοι όπως στο (β), έχουμε  $a^n \equiv 1 \pmod{a^n - 1}$ , άρα  $a^{nq} \equiv 1 \pmod{a^n - 1}$  και συνεπώς

$$a^m - 1 = a^{nq} \cdot a^r - 1 \equiv a^r - 1 \pmod{a^n - 1}.$$

Από την ισοτιμία αυτή και το (α) συμπεραίνουμε ότι

$$\mu\kappa\delta(a^m - 1, a^n - 1) = \mu\kappa\delta(a^r - 1, a^n - 1) = \mu\kappa\delta(a^n - 1, a^r - 1).$$

Από την υπόθεση της επαγωγής έχουμε  $\mu\kappa\delta(a^n - 1, a^r - 1) = a^d - 1$ . Από τις τελευταίες ισότητες έπεται ότι  $\mu\kappa\delta(a^m - 1, a^n - 1) = a^d - 1$ , συμπέρασμα το οποίο ολοκληρώνει την επαγωγή.

6. Χρησιμοποιούμε επαγωγή στο  $n$ . Το ζητούμενο ισχύει για  $n = 0$ . Έστω ότι ισχύει για το  $n$ . Πολλαπλασιάζοντας την ισοτιμία  $5^n \equiv 1 + 4n \pmod{16}$  με το 5, βρίσκουμε ότι

$$5^{n+1} \equiv 5 \cdot (1 + 4n) = 5 + 20n \equiv 5 + 4n = 1 + 4(n+1) \pmod{16}.$$

Συνεπώς το ζητούμενο ισχύει και για το  $n + 1$ . Από την αρχή της μαθηματικής επαγωγής συμπεραίνουμε ότι το ζητούμενο ισχύει για κάθε  $n \in \mathbb{N}$ .

7. Τα αντιστρέψιμα στοιχεία του  $\mathbb{Z}_{14}$  είναι οι κλάσεις  $\bar{1}, \bar{3}, \bar{5}, \bar{9}, \bar{11}$  και  $\bar{13}$ . Παρατηρώντας ότι  $\bar{1} + \bar{13} = \bar{3} + \bar{11} = \bar{5} + \bar{9} = \bar{0}$  στο  $\mathbb{Z}_{14}$  βρίσκουμε ότι το άθροισμα των αντιστρέψιμων στοιχείων του  $\mathbb{Z}_{14}$  είναι ίσο με  $\bar{0}$ . Παρατηρώντας ότι  $\bar{1} \cdot \bar{1} = \bar{3} \cdot \bar{5} = \bar{9} \cdot \bar{11} = \bar{13} \cdot \bar{13} = \bar{1}$  στο  $\mathbb{Z}_{14}$  βρίσκουμε ότι το αντίστροφο στοιχείο των  $\bar{1}, \bar{3}, \bar{5}, \bar{9}, \bar{11}$  και  $\bar{13}$  είναι το  $\bar{1}, \bar{5}, \bar{3}, \bar{11}, \bar{9}$  και  $\bar{13}$ , αντίστοιχα, και ότι το γινόμενο των αντιστρέψιμων στοιχείων του  $\mathbb{Z}_{14}$  είναι ίσο με  $\bar{13} = -\bar{1}$ . Ομοίως, τα αντιστρέψιμα στοιχεία του  $\mathbb{Z}_{15}$  είναι οι κλάσεις  $\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}$  και  $\bar{14}$ , το άθροισμά τους είναι ίσο με  $\bar{0}$ , το γινόμενό τους είναι ίσο με  $\bar{1}$  και το αντίστροφο στοιχείο των  $\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}$  και  $\bar{14}$  είναι το  $\bar{1}, \bar{8}, \bar{4}, \bar{13}, \bar{2}, \bar{11}, \bar{7}$  και  $\bar{14}$ , αντίστοιχα.
8. Για να ισχύει  $\mu\kappa\delta(a, 1000) = 4$  προφανώς θα πρέπει το  $a$  να διαιρείται με το 4. Θέτοντας  $a = 4b$  με  $b \in \mathbb{Z}$  (οπότε  $b \in \{1, 2, \dots, 250\}$ , αφού  $a \in \{1, 2, \dots, 1000\}$ ), έχουμε  $\mu\kappa\delta(a, 1000) = \mu\kappa\delta(4b, 1000) = 4 \mu\kappa\delta(b, 250)$  και συνεπώς  $\mu\kappa\delta(a, 1000) = 4$  αν και μόνο αν  $\mu\kappa\delta(b, 250) = 1$ . Συμπερίνουμε ότι το ζητούμενο πλήθος είναι ίσο με το πλήθος των  $b \in \{1, 2, \dots, 250\}$  για τα οποία ισχύει  $\mu\kappa\delta(b, 250) = 1$ . Από τον ορισμό της συνάρτησης του Euler, το πλήθος αυτό είναι ίσο με  $\varphi(250) = \varphi(2) \cdot \varphi(125) = 1 \cdot 100 = 100$ .

9. Για κάθε τέτοιο ζεύγος  $(x, y)$  το  $x$  είναι αντιστρέψιμο στοιχείο του  $\mathbb{Z}_{200}$ , αφού  $x \cdot (x^2y) = 1$ . Αντιστρόφως, αν το  $x \in \mathbb{Z}_{200}$  είναι αντιστρέψιμο, τότε το ίδιο ισχύει και για το  $x^3$  και η εξίσωση  $x^3y = 1$  έχει μοναδική λύση  $y = (x^3)^{-1} = (x^{-1})^3$  ως προς  $y$  στο  $\mathbb{Z}_{200}$ . Επομένως, το ζητούμενο πλήθος είναι ίσο με το πλήθος των αντιστρέψιμων στοιχείων του  $\mathbb{Z}_{200}$ , δηλαδή με  $\varphi(200) = \varphi(8) \cdot \varphi(25) = 4 \cdot 20 = 80$ .
10. Για το (α) υπολογίζουμε ότι  $\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2)\varphi(5^2) = 2 \cdot 20 = 40$ . Για το (β) εφαρμόζουμε το Θεώρημα του Euler και το (α) για να συμπεράνουμε ότι  $3^{40} \equiv 1 \pmod{100}$  και συνεπώς ότι  $3^{1000} = 3^{40 \cdot 25} = (3^{40})^{25} \equiv 1^{25} = 1 \pmod{100}$ . Για το (γ) παρατηρούμε ότι η δοσμένη ισοτιμία έχει μοναδική λύση mod 100 (αφού  $\mu\kappa\delta(3, 100) = 1$ ) και ότι η  $x \equiv 67 \pmod{100}$  είναι λύση της ισοτιμίας αυτής. Επομένως, οι ακέραιοι  $x$  που επαληθεύουν την ισοτιμία είναι ακριβώς εκείνοι με  $x \equiv 67 \pmod{100}$ . Για το (δ) θέτουμε  $x = 3^{999}$  και παρατηρούμε ότι  $3x = 3^{1000}$ . Από τα (β) και (γ) προκύπτει ότι  $x \equiv 67 \pmod{100}$ . Άρα, στο δεκαδικό σύστημα αρίθμησης ο  $x$  λήγει στα ψηφία 67.
11. Παρατηρούμε ότι  $252 = 4 \cdot 7 \cdot 9$  και ότι οι αριθμοί 4, 7 και 9 είναι ανά δύο σχετικώς πρώτοι. Επομένως, αρκεί να δείξουμε ότι ο  $a^6 - 1$  (όταν  $\mu\kappa\delta(a, 42) = 1$ ) και ο  $a^8 - a^2$  διαιρούνται με καθέναν από τους 4, 7 και 9. Υποθέτουμε ότι  $\mu\kappa\delta(a, 42) = 1$ , οπότε  $\mu\kappa\delta(a, 2) = \mu\kappa\delta(a, 3) = \mu\kappa\delta(a, 7) = 1$  και συνεπώς  $\mu\kappa\delta(a, 4) = \mu\kappa\delta(a, 7) = \mu\kappa\delta(a, 9) = 1$ . Αφού  $\varphi(4) = 2$  και  $\varphi(7) = \varphi(9) = 6$ , από το Θεώρημα του Euler παίρνουμε  $a^2 \equiv 1 \pmod{4}$ ,  $a^6 \equiv 1 \pmod{7}$  και  $a^6 \equiv 1 \pmod{9}$ . Από την πρώτη ισοτιμία προκύπτει ότι  $a^6 \equiv 1 \pmod{4}$ . Άρα, ο  $a^6 - 1$  διαιρείται με καθέναν από τους 4, 7 και 9 και συνεπώς ισχύει το (α). Δείξαμε προηγουμένως ότι αν  $\mu\kappa\delta(a, 2) = 1$ , τότε το  $a^6 - 1$  διαιρείται με το 4. Αν όχι, τότε το  $a$  διαιρείται με το 2 και συνεπώς το  $a^2$  διαιρείται με το 4. Επομένως το  $a^8 - a^2 = a^2(a^6 - 1)$  διαιρείται με το 4 για κάθε  $a \in \mathbb{Z}$ . Ομοίως βρίσκουμε ότι το  $a^8 - a^2$  διαιρείται με το 7 και το 9 για κάθε  $a \in \mathbb{Z}$  και συμπεραίνουμε ότι ισχύει το (β). Ο τελευταίος ισχυρισμός της άσκησης προκύπτει από το (β) και την παρατήρηση ότι  $a^8 - a^2 = 252$  για  $a = 2$ .
12. Θα δείξουμε ότι ο  $\varphi(m)$  είναι περιττός μόνο για  $m = 1$  και  $m = 2$ . Πράγματι, για αυτές τις τιμές του  $m$  έχουμε  $\varphi(1) = \varphi(2) = 1$ . Αν  $m \geq 3$ , τότε είτε  $m = 2^k$  για κάποιο ακέραιο  $k \geq 2$ , είτε ο  $m$  διαιρείται με κάποιον περιττό πρώτο  $p$ . Στην πρώτη περίπτωση έχουμε  $\varphi(m) = 2^{k-1}$  και συνπώς ο  $\varphi(m)$  είναι άρτιος. Στη δεύτερη περίπτωση μπορούμε να γράψουμε  $m = p^k q$ , όπου  $q$  είναι ακέραιος που δε διαιρείται με το  $p$ . Τότε  $\mu\kappa\delta(p^k, q) = 1$  και συνπώς  $\varphi(m) = \varphi(p^k)\varphi(q) = (p^k - p^{k-1})\varphi(q)$ . Άρα, ο  $\varphi(m)$  διαιρείται με τον άρτιο αριθμό  $p^k - p^{k-1}$  και επομένως είναι και πάλι άρτιος αριθμός.
13. Οι αντιστοιχίες (β), (γ) ορίζουν πράξεις στο  $S$ , ενώ οι (α), (δ) όχι. Πράγματι, για  $S = \mathbb{Z} \setminus \{0\}$  και  $a, b \in S$  έχουμε  $ab \in S$ , αλλά όχι αναγκαστικά  $a+b \in S$  (π.χ. για  $a = 1$  και  $b = -1$ ), οπότε η  $*$ :  $S \times S \rightarrow S$  είναι καλά ορισμένη απεικόνιση, ενώ η

$\circ : S \times S \rightarrow S$  δεν είναι. Επίσης, για  $S = \mathbb{Z}_3$  η  $\circ : S \times S \rightarrow S$  είναι καλά ορισμένη απεικόνιση, ενώ η  $*$  :  $S \times S \rightarrow S$  δεν είναι αφού, για παράδειγμα, στο  $\mathbb{Z}_3$  ισχύει  $\bar{1} = \bar{4}$  και συνεπώς έχουμε τα αντιφατικά αποτελέσματα  $\bar{1} * \bar{2} = \max(1, 2) = \bar{2}$  και  $\bar{1} * \bar{2} = \bar{4} * \bar{2} = \max(4, 2) = \bar{4} = \bar{1}$ .

14. (α) Τα τέσσερα αξιώματα που αφορούν μόνο την πρόσθεση επαληθεύονται εύκολα. Για παράδειγμα, το μηδενικό στοιχείο του  $S$  είναι το  $0_S = (0_R, 0_R)$  και το αντίθετο του  $(a, b) \in S$  είναι το  $(-a, -b) \in S$ . Για να επαληθεύσουμε την προσεταιριστική ιδιότητα του πολλαπλασιασμού, θεωρούμε στοιχεία  $x = (a, b)$ ,  $y = (c, d)$  και  $z = (e, f)$  του  $S$  και υπολογίζουμε ότι

$$(x \odot y) \odot z = (ac, ad + bc) \odot (e, f) = ((ac)e, (ac)f + (ad + bc)e)$$

και ότι

$$x \odot (y \odot z) = (a, b) \odot (ce, cf + de) = (a(ce), a(cf + de) + b(ce)).$$

Εφαρμόνοντας τις ιδιότητες (προσεταιριστική, επιμεριστική) του πολλαπλασιασμού στο  $R$ , από τις παραπάνω εκφράσεις προκύπτει ότι  $(x \odot y) \odot z = x \odot (y \odot z)$ . Με παρόμοιο τρόπο επαληθεύουμε ότι  $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$  και ότι  $(y \oplus z) \odot x = (y \odot x) \oplus (z \odot x)$ .

(β) Υποθέτουμε πρώτα ότι ο  $S$  έχει μονάδα, έστω  $1_S = (u, v) \in S$ . Τότε για όλα τα  $a, b \in R$  ισχύει

$$(a, b) \odot (u, v) = (u, v) \odot (a, b) = (a, b),$$

δηλαδή  $(au, av + bu) = (ua, ub + va) = (a, b)$ . Από τις ισότητες αυτές παίρνουμε  $au = ua = a$  για κάθε  $a \in R$  και συμπεραίνουμε ότι το  $u$  είναι μονάδα του  $R$ . Αντιστρόφως, αν το  $R$  έχει μονάδα  $1_R$ , τότε για το στοιχείο  $1_S = (1_R, 0_R)$  του  $S$  επαληθεύουμε ότι  $x \odot 1_S = 1_S \odot x = x$  για κάθε  $x \in S$  και συμπεραίνουμε ότι το  $1_S$  είναι μονάδα του  $S$ . Εργαζόμαστε ομοίως για τη μεταθετικότητα.

(γ) Θα δείξουμε τα αντιστρέψιμα στοιχεία του  $S$  είναι εκείνα τα ζεύγη  $(a, b) \in S$  για τα οποία το  $a$  είναι αντιστρέψιμο στοιχείο του  $R$ , δηλαδή ότι για  $a, b \in R$  ισχύει  $(a, b) \in U(S) \Leftrightarrow a \in U(R)$ . Πράγματι, έστω  $x = (a, b) \in S$ . Από τη λύση του (β) γνωρίζουμε ότι ο  $R$  έχει μονάδα, έστω  $1_R$ , και ότι το ζεύγος  $1_S = (1_R, 0_R)$  είναι η μονάδα του  $S$ . Επομένως έχουμε  $x \in U(S)$  αν και μόνο αν υπάρχουν  $u, v \in R$  τέτοια ώστε

$$(a, b) \odot (u, v) = (u, v) \odot (a, b) = (1_R, 0_R)$$

ή, ισοδύναμα,

$$(au, av + bu) = (ua, ub + va) = (1_R, 0_R).$$

Από τις ισότητες αυτές προκύπτει ότι  $au = ua = 1_R$  και συνεπώς ότι  $a \in U(R)$ . Δείξαμε λοιπόν ότι  $(a, b) \in U(S) \Rightarrow a \in U(R)$ . Αντιστρόφως, έστω ότι  $a \in U(R)$

και έστω  $u = a^{-1} \in R$ , οπότε  $au = ua = 1_R$ . Παρατηρούμε ότι το σύστημα των εξισώσεων  $av + bu = ub + va = 0_R$  έχει τη μοναδική λύση  $v = -a^{-1}ba^{-1}$  ως προς  $v$ . Σύμφωνα με τα προηγούμενα, για το ζεύγος  $y = (u, v)$  ισχύει  $x \odot y = y \odot x = 1_S$  και συνεπώς  $(a, b) = x \in U(S)$ .

(δ) Το ερώτημα έχει αρνητική απάντηση. Πράγματι, αφού ο μηδενικός δακτύλιος δεν είναι ακέραια περιοχή, μπορούμε να υποθέσουμε ότι το  $S$  έχει τουλάχιστον δύο στοιχεία. Τότε το ίδιο ισχύει για το  $R$ , οπότε υπάρχει  $b \in R$  με  $b \neq 0_R$ . Θέτοντας  $x = (0_R, b)$ , έχουμε  $x \neq 0_S$  και  $x \odot x = (0_R, b) \odot (0_R, b) = (0_R, 0_R) = 0_S$ . Κατά συνέπεια, το  $S$  δεν είναι ακέραια περιοχή.

15. (αβ) Για το (α), η προτεινόμενη ταυτότητα επαληθεύεται εύκολα με χρήση της επιμεριστικής ιδιότητας στο  $R$  μετά από πράξεις ρουτίνας. Για το (β), υποθέτουμε πρώτα ότι

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U(M_2(R)).$$

Τότε, υπάρχουν  $x, y, z, w \in R$  τέτοια ώστε

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 1_R & 0_R \\ 0_R & 1_R \end{pmatrix}.$$

Αυτό σημαίνει ότι  $ax + bz = cy + dw = 1_R$  και  $ay + bw = cx + dz = 0_R$ . Από την ταυτότητα στο (α) προκύπτει ότι  $(ad - bc)(xw - yz) = 1_R$  και συνεπώς ότι  $ad - bc \in U(R)$ . Αντιστρόφως, έστω ότι  $ad - bc \in U(R)$ . Θέτοντας

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad B = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

επαληθεύουμε ότι  $AB = BA = I_2(R)$  και συμπεραίνουμε ότι  $A \in U(M_2(R))$ .

(γ) Παρατηρούμε πρώτα ότι το πλήθος των στοιχείων του  $M_2(\mathbb{Z}_p)$  είναι ίσο με εκείνο των διατεταγμένων τετράδων  $(a, b, c, d) \in \mathbb{Z}_p^4$  και συνεπώς ίσο με  $p^4$ . Σύμφωνα με το (β), το πλήθος των αντιστρέψιμων στοιχείων του  $M_2(\mathbb{Z}_p)$  είναι ίσο με εκείνο των διατεταγμένων τετράδων  $(a, b, c, d) \in \mathbb{Z}_p^4$  για τις οποίες ισχύει  $ad - bc \neq \bar{0}$ . Για να απαριθμήσουμε τις τετράδες αυτές, θέτουμε  $ad - bc = e \in \mathbb{Z}_p \setminus \{\bar{0}\}$  και διακρίνουμε δύο περιπτώσεις. Αν  $a \neq \bar{0}$ , τότε η εξίσωση  $ad - bc = e$  έχει μοναδική λύση ως προς  $d$  για όλα τα  $b, c \in \mathbb{Z}_p$  και  $a, e \in \mathbb{Z}_p \setminus \{\bar{0}\}$ . Επομένως, το πλήθος των τετράδων αυτών είναι ίσο με  $p^2(p - 1)^2$ . Αν  $a = \bar{0}$ , τότε η εξίσωση γράφεται  $bc = -e$  και έχει μόνο λύσεις με  $b, c \neq \bar{0}$ . Επιπλέον, για τυχαία  $b, e \in \mathbb{Z}_p \setminus \{\bar{0}\}$  η εξίσωση  $bc = -e$  έχει μοναδική λύση ως προς  $c$ , ενώ η τιμή του  $d \in \mathbb{Z}_p$  είναι αδιάφορη. Επομένως, υπάρχουν ακριβώς  $p(p - 1)^2$  λύσεις στην περίπτωση αυτή. Κατά συνέπεια, υπάρχουν συνολικά ακριβώς

$$p^2(p - 1)^2 + p(p - 1)^2 = p(p - 1)^2(p + 1)$$

αντιστρέψιμα στοιχεία του  $M_2(\mathbb{Z}_p)$ .



16. Για το πρώτο ερώτημα παρατηρούμε ότι για το δακτύλιο  $\mathbb{Z}_8$  ισχύει  $a^2 = \bar{1}$ , άρα  $a^{-1} = a$ , για κάθε  $a \in \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ . Για το δεύτερο ερώτημα παρατηρούμε ότι για τυχαίο δακτύλιο  $R$  με μονάδα και για  $a \in R$ , έχουμε

$$a^{-1} = a \Leftrightarrow a^2 = 1_R \Leftrightarrow a^2 - 1_R = 0_R \Leftrightarrow (a + 1_R)(a - 1_R) = 0_R.$$

Αν ο  $R$  είναι ακέραια περιοχή, προκύπτει ότι  $a^{-1} = a \Leftrightarrow a \in \{-1_R, 1_R\}$  και συνεπώς ότι υπάρχουν το πολύ δύο στοιχεία  $a \in R$  με  $a^{-1} = a$ .

17. Το σύνολο, έστω  $S$ , που δίνεται είναι υποδακτύλιος του  $M_2(\mathbb{Z})$  στις περιπτώσεις (β) και (γ). Για παράδειγμα, για το (β), για τυχαία στοιχεία

$$X = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, \quad Y = \begin{pmatrix} c & d \\ 0 & c \end{pmatrix}$$

του  $S$  έχουμε

$$X - Y = \begin{pmatrix} a - c & b - d \\ 0 & a - c \end{pmatrix} \in S, \quad XY = \begin{pmatrix} ac & ad + bc \\ 0 & ac \end{pmatrix} \in S.$$

Αφού, επιπλέον, είναι μη κενό, το  $S$  αποτελεί υποδακτύλιο του  $M_2(\mathbb{Z})$ . Εργαζόμαστε παρόμοια για το (γ). Στις περιπτώσεις (α) και (δ) το  $S$  δεν είναι υποδακτύλιος του  $M_2(\mathbb{Z})$  διότι δεν είναι κλειστό ως προς το πολλαπλασιασμό και την πρόσθεση, αντίστοιχα. Για παράδειγμα, για το (α) έχουμε

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in S$$

αλλά

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \notin S.$$

Για το (δ) έχουμε

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in S$$

αλλά

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \notin S.$$

18. Στο (α) η πρόταση είναι αληθής (η επαλήθευση είναι εύκολη και παραλείπεται). Γενικότερα, αν  $R_0$  είναι υποδακτύλιος του  $R$  και  $S_0$  είναι υποδακτύλιος του  $S$ , τότε το σύνολο  $R_0 \times S_0$  είναι υποδακτύλιος του  $R \times S$ . Στο (β) η πρόταση είναι ψευδής, αφού το σύνολο  $\{(a, a) : a \in \mathbb{Z}\}$  είναι υποδακτύλιος του  $\mathbb{Z} \times \mathbb{Z}$  ο οποίος δεν είναι της μορφής  $(m\mathbb{Z}) \times (n\mathbb{Z})$ .

19. Θα δείξουμε ότι τέτοια πολυώνυμα υπάρχουν μόνο στην περίπτωση  $F = \mathbb{Z}_5$ . Πράγματι, για  $F = \mathbb{Z}_5$  αρκεί να θέσουμε  $f(x) = 1 + x$  και  $g(x) = 1 + 2x$ , αφού τότε

$$(f(x))^2 + (g(x))^2 = 2 + 6x + 5x^2 = 2 + x.$$

Έστω τώρα ότι  $F \in \{\mathbb{R}, \mathbb{Z}_2, \mathbb{Z}_3\}$  και έστω μη μηδενικά πολυώνυμα  $f(x), g(x) \in F[x]$  με βαθμούς  $n$  και  $m$ , αντίστοιχα. Γράφουμε  $f(x) = a_0 + a_1x + \dots + a_nx^n$  και  $g(x) = b_0 + b_1x + \dots + b_mx^m$ , με  $a_n, b_m \in F \setminus \{0\}$ . Στην περίπτωση  $F = \mathbb{Z}_2$  έχουμε

$$(f(x))^2 = (a_0 + a_1x^2 + \dots + a_nx^{2n})^2 = a_0^2 + a_1^2x^2 + \dots + a_n^2x^{2n},$$

$$(g(x))^2 = (b_0 + b_1x^2 + \dots + b_mx^{2m})^2 = b_0^2 + b_1^2x^2 + \dots + b_m^2x^{2m}.$$

Επομένως, το  $(f(x))^2 + (g(x))^2$  γράφεται ως άθροισμα μονωνύμων στα οποία η δύναμη του  $x$  είναι άρτιος αριθμός. Προφανώς, ένα τέτοιο πολυώνυμο δεν μπορεί να έχει περιττό βαθμό. Υποθέτουμε, τέλος, ότι  $F \in \{\mathbb{R}, \mathbb{Z}_3\}$ . Αν  $n \neq m$ , τότε ο μεγαλύτερος όρος του  $(f(x))^2 + (g(x))^2$  είναι ίσος με  $a_n^2x^{2n}$  ή με  $b_m^2x^{2m}$  και συνεπώς ο βαθμός του  $(f(x))^2 + (g(x))^2$  είναι άρτιος αριθμός. Αν  $n = m$ , τότε

$$(f(x))^2 + (g(x))^2 = c_0 + c_1x^2 + \dots + c_{2n}x^{2n}$$

για κάποια  $c_0, c_1, \dots, c_{2n} \in F$  με  $c_{2n} = a_n^2 + b_n^2$ . Αφού όμως  $a_n, b_n \neq 0$ , έχουμε  $a_n^2 + b_n^2 > 0$  στην περίπτωση  $F = \mathbb{R}$  και  $a_n, b_n \in \{-1, 1\}$ , οπότε  $a_n^2 + b_n^2 = 2$ , στην περίπτωση  $F = \mathbb{Z}_3$ . Άρα, και στις δύο περιπτώσεις ισχύει  $c_{2n} \neq 0$  και συνεπώς ο βαθμός του  $(f(x))^2 + (g(x))^2$  είναι ίσος με τον άρτιο αριθμό  $2n$ .

20. Για το (α) υποθέτουμε ότι υπάρχει πολυώνυμο  $g(x) = b_0 + b_1x + \dots + b_mx^m \in R[x]$  με  $f(x)g(x) = 1$ , όπου  $b_m \neq 0_R$ . Εξισώνοντας τους σταθερούς όρους και τους συντελεστές του  $x^{n+m}$  στην ισότητα  $f(x)g(x) = 1$  παίρνουμε  $a_0b_0 = 1_R$  και  $a_nb_m = 0_R$  και συμπεραίνουμε ότι  $a_0 \in U(R)$  και ότι το  $a_n$  είναι μηδενοδιαίρετης στο  $R$ . Για το (β) θέτουμε  $R = \mathbb{Z}_6$  και  $f(x) = 1 + 2x$ . Μπορούμε να δείξουμε ότι το  $f(x)$  δεν είναι αντιστρέψιμο στο  $\mathbb{Z}_6[x]$  ως εξής. Έστω ότι  $f(x)g(x) = 1$  για κάποιο  $g(x) \in \mathbb{Z}_6[x]$ . Θέτοντας  $x = \bar{1} \in \mathbb{Z}_6$  παίρνουμε  $f(\bar{1})g(\bar{1}) = \bar{1}$  στο  $\mathbb{Z}_6$ , όπου προκύπτει ότι το  $f(\bar{1})$  είναι αντιστρέψιμο στοιχείο του  $\mathbb{Z}_6$ . Στην περίπτωση μας αυτό δεν ισχύει, αφού  $f(\bar{1}) = \bar{3}$ . Από την αντίφαση αυτή συμπεραίνουμε ότι το  $f(x)$  δεν είναι αντιστρέψιμο στοιχείο του  $\mathbb{Z}_6[x]$ .

21. Το (α) προκύπτει από την ταυτότητα  $a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \dots + b^{k-1})$  για  $a = p(x)$  και  $b = q(x)$ . Για το (β) παρατηρούμε ότι

$$f(p(x)) - f(q(x)) = \sum_{k=1}^n a_k ((p(x))^k - (q(x))^k).$$

Εφαρμόζοντας το (α) για  $k \in \{1, 2, \dots, n\}$  συμπεραίνουμε ότι το  $p(x) - q(x)$  διαιρεί το δεξιό μέλος της προηγούμενης ισότητας στο  $R[x]$ , οπότε το  $p(x) - q(x)$  διαιρεί και το  $f(p(x)) - f(q(x))$  στο  $R[x]$ .

22. Αληθής είναι μόνο η πρόταση στο (α). Πράγματι, έστω ότι το  $g(x)$  διαιρεί το  $f(x)$  στο  $\mathbb{Z}[x]$ , οπότε υπάρχει  $q(x) \in \mathbb{Z}[x]$  με  $f(x) = g(x)q(x)$ . Τότε  $f(m) = g(m)q(m)$  για κάθε  $m \in \mathbb{Z}$ . Επιπλέον, αφού  $q(x) \in \mathbb{Z}[x]$ , έχουμε  $q(m) \in \mathbb{Z}$  για κάθε  $m \in \mathbb{Z}$ . Άρα, το  $g(m)$  διαιρεί το  $f(m)$  στο  $\mathbb{Z}$  για κάθε  $m \in \mathbb{Z}$  και συνεπώς ισχύει το (α). Για το (β) θέτουμε  $f(x) = x(x-1)$  και  $g(x) = 2$ . Παρατηρούμε ότι το  $g(x)$  δεν διαιρεί το  $f(x)$  στο  $\mathbb{Z}[x]$  (αφού οι συντελεστές του  $f(x)$  είναι περιττοί αριθμοί) και ότι το 2 διαιρεί το  $m(m-1)$  στο  $\mathbb{Z}$  για κάθε  $m \in \mathbb{Z}$ . Συνεπώς η πρόταση στο (β) είναι ψευδής.

23. Εκτελώντας τις διαδοχικές διαιρέσεις στο  $\mathbb{Q}[x]$  βρίσκουμε ότι

$$\begin{aligned} \mu\kappa\delta(f(x), g(x)) &= \mu\kappa\delta(x^3 + 1, -2x^2 - x + 1) = \mu\kappa\delta(2x^3 + 2, -2x^2 - x + 1) \\ &= \mu\kappa\delta(-2x^2 - x + 1, 3/2(x + 1)) \\ &= \mu\kappa\delta(x + 1, 0) = x + 1. \end{aligned}$$

Ομοίως υπολογίζουμε ότι

$$\begin{aligned} \mu\kappa\delta(f(x), g(x)) &= \mu\kappa\delta(x^3 + 1, -2x^2 - x + 1) = \mu\kappa\delta(x^3 + 1, x^2 + 2x + 1) \\ &= (x + 1)^2 \end{aligned}$$

στο  $\mathbb{Z}_3[x]$ .

24. Με δοκιμές βρίσκουμε ότι οι ρίζες του  $f(x)$  στο  $\mathbb{Z}_5$  είναι οι  $\bar{3}$  και  $\bar{4}$ . Επομένως, το  $f(x)$  διαιρείται με το  $(x-3)(x-4)$  στο  $\mathbb{Z}_5[x]$ . Εκτελώντας τη διαίρεση, βρίσκουμε ότι  $f(x) = (x-3)(x-4)(x^3+x+1) = (x+1)(x+2)(x^3+x+1)$  στο  $\mathbb{Z}_5[x]$ . Αφού το  $x^3+x+1$  είναι πολυώνυμο τρίτου βαθμού χωρίς ρίζες στο  $\mathbb{Z}_5$ , άρα ανάγωγο στο  $\mathbb{Z}_5[x]$ , η  $f(x) = (x+1)(x+2)(x^3+x+1)$  είναι η ζητούμενη παραγοντοποίηση του  $f(x)$ .

25. Θα δείξουμε ότι τα πολυώνυμα με τη ζητούμενη ιδιότητα είναι εκείνα της μορφής  $p(x) = cx$ , με  $c \in \mathbb{Z}$ . Θέτοντας  $x = 0$  στην ισότητα  $(x+1)p(x) = xp(x+1)$  παίρνουμε  $p(0) = 0$  και συμπεραίνουμε ότι  $p(x) = xq(x)$  για κάποιο  $q(x) \in \mathbb{Z}[x]$ . Για το πολυώνυμο  $q(x)$  προκύπτει ότι  $(x+1)xq(x) = x(x+1)q(x+1)$ , δηλαδή ότι  $q(x+1) = q(x)$ . Θέτοντας  $c = q(0)$ , βρίσκουμε ότι  $q(n) = c$  για κάθε  $n \in \mathbb{Z}$ . Άρα, το πολυώνυμο  $q(x) - c$  του  $\mathbb{Z}[x]$  έχει άπειρες ρίζες στο  $\mathbb{Z}$  και συνεπώς ταυτίζεται με το μηδενικό πολυώνυμο. Συμπεραίνουμε ότι ισχύει  $q(x) = c$ , και συνεπώς  $p(x) = cx$ , στο  $\mathbb{Z}[x]$ . Αντιστρόφως, κάθε τέτοιο πολυώνυμο  $p(x)$  επαληθεύει την ισότητα  $(x+1)p(x) = xp(x+1)$ .

26. Θέτοντας  $f(x) = g(x) = x^2 + 1$ , βρίσκουμε ότι η πρόταση στο (α) είναι ψευδής. Για το (β) θέτουμε  $d(x) = \mu\kappa\delta(f(x), g(x))$ , οπότε το  $d(x) \in \mathbb{C}[x]$  είναι μονικό πολυώνυμο. Υποθέτουμε πρώτα ότι  $d(x) \neq 1$ . Τότε το  $d(x)$  έχει θετικό βαθμό και συνεπώς μία τουλάχιστον ρίζα στο  $\mathbb{C}$ . Αφού το  $d(x)$  διαιρεί τα  $f(x)$  και  $g(x)$ , η ρίζα αυτή είναι κοινή ρίζα των  $f(x)$  και  $g(x)$ . Αντιστρόφως, έστω ότι  $\alpha \in \mathbb{C}$  είναι κοινή ρίζα των  $f(x)$  και  $g(x)$ . Τότε το  $x - \alpha$  διαιρεί τα  $f(x)$  και  $g(x)$ , άρα και το μέγιστο κοινό τους διαιρέτη  $d(x)$ , στο  $\mathbb{C}[x]$ . Συνεπώς  $d(x) \neq 1$ .

27. (αβ) Έστω  $f(x) = x^p - x + 1$ . Παρατηρούμε ότι το  $f(x)$  δεν έχει ρίζες στο  $\mathbb{Z}_p$  αφού  $f(a) = a^p - a + 1 = 1$  για κάθε  $a \in \mathbb{Z}_p$ . Ας υποθέσουμε ότι  $r/s$  είναι ρίζα του  $f(x)$ , όπου  $r$  και  $s$  είναι σχετικώς πρώτοι ακέραιοι με  $s \neq 0$ . Τότε, όπως είναι γνωστό, το  $r$  διαιρεί το σταθερό όρο και το  $s$  διαιρεί το συντελεστή του μεγιστοβαθμίου όρου του  $f(x)$ . Αφού οι συντελεστές αυτοί είναι ίσοι με 1, προκύπτει ότι  $r, s \in \{-1, 1\}$ . Αφού όμως τα  $-1$  και  $1$  δεν είναι ρίζες του  $f(x)$ , συμπεραίνουμε ότι το  $f(x)$  δεν έχει ρίζες ούτε στο  $\mathbb{Q}$ .

(γ) Τέτοιο πολυώνυμο υπάρχει μόνο για  $p = 2$  (για παράδειγμα, το  $x^2 + 1$ ). Διαφορετικά, ο  $p$  είναι περιττός αριθμός και κάθε πολυώνυμο  $f(x) \in \mathbb{R}[x]$  βαθμού  $p$  έχει ρίζα στο  $\mathbb{R}$  για τον εξής λόγο. Γνωρίζουμε ότι το  $f(x)$  μπορεί να γραφεί ως γινόμενο πολυωνύμων του  $\mathbb{R}[x]$  πρώτου ή δευτέρου βαθμού. Αφού οι βαθμοί των πολυωνύμων αυτών αθροίζουν στον περιττό αριθμό  $p$ , ένα τουλάχιστον από τα πολυώνυμα αυτά είναι πρώτου βαθμού και συνεπώς έχει ρίζα στο  $\mathbb{R}$ , η οποία είναι και ρίζα του  $f(x)$ .

28. Συμβολίζουμε με  $R$  το δακτύλιο στο (α) και με  $S$  το δακτύλιο στο (β). Ο δακτύλιος  $R$  είναι ισόμορφος με το γινόμενο  $\mathbb{Z} \times \mathbb{Z}$ , αφού η απεικόνιση  $\varphi : R \rightarrow \mathbb{Z} \times \mathbb{Z}$  με

$$\varphi \left( \begin{array}{cc} a & 0 \\ 0 & b \end{array} \right) = (a, b)$$

για  $a, b \in \mathbb{Z}$  είναι ισομορφισμός δακτυλίων (εξηγήστε γιατί). Θα δείξουμε ότι ο δακτύλιος  $S$  δεν είναι ισόμορφος με τον  $\mathbb{Z} \times \mathbb{Z}$ . Θεωρούμε τυχαίο ομομορφισμό δακτυλίων  $\varphi : S \rightarrow \mathbb{Z} \times \mathbb{Z}$ . Παρατηρούμε ότι για το μη μηδενικό στοιχείο

$$x = \left( \begin{array}{cc} 0 & 1 \\ 0 & 0 \end{array} \right) \in S$$

ισχύει  $x^2 = 0_S$ . Άρα, για το στοιχείο  $\varphi(x) \in \mathbb{Z} \times \mathbb{Z}$  έχουμε  $(\varphi(x))^2 = \varphi(x) \cdot \varphi(x) = \varphi(x \cdot x) = \varphi(x^2) = \varphi(0_S) = \mathbf{0}$  (όπου  $\mathbf{0} = (0, 0) \in \mathbb{Z} \times \mathbb{Z}$ ). Όμως στο δακτύλιο  $\mathbb{Z} \times \mathbb{Z}$  ισχύει  $y^2 = \mathbf{0} \Rightarrow y = \mathbf{0}$  και συνεπώς  $\varphi(x) = \mathbf{0} = \varphi(0_S)$ . Έπεται ότι η απεικόνιση  $\varphi$  δεν είναι 1-1 και συνεπώς ότι δεν υπάρχει ισομορφισμός (ούτε μονομορφισμός)  $\varphi : S \rightarrow \mathbb{Z} \times \mathbb{Z}$ .

29. Για το κύριο ιδεώδες του  $2\mathbb{Z}$  που παράγεται από το στοιχείο  $a \in 2\mathbb{Z}$  έχουμε  $\langle a \rangle = \{aq : q \in 2\mathbb{Z}\} = \{2ap : p \in \mathbb{Z}\} = (2a)\mathbb{Z}$ . Θέτοντας  $a = 2m$ , με  $m \in \mathbb{Z}$ ,

βρίσκουμε ότι  $\langle a \rangle = (4m)\mathbb{Z}$  και συμπεραίνουμε ότι τα κύρια ιδεώδη του  $2\mathbb{Z}$  είναι τα σύνολα της μορφής  $(4m)\mathbb{Z}$  για  $m \in \mathbb{Z}$ . Συμπεραίνουμε επίσης ότι το ιδεώδες  $2\mathbb{Z}$  του  $2\mathbb{Z}$  δεν είναι κύριο. Το ίδιο ισχύει για τα ιδεώδη  $6\mathbb{Z}, 10\mathbb{Z}, 14\mathbb{Z}, \dots$ .

30. (α) Για στοιχεία  $x = a + b\sqrt{2}$  και  $y = c + d\sqrt{2}$  του  $\mathbb{Z}[\sqrt{2}]$  έχουμε

$$\begin{aligned}x + y &= (a + c) + (b + d)\sqrt{2} \\xy &= (ac + 2bd) + (ad + bc)\sqrt{2}\end{aligned}$$

και συνεπώς

$$\begin{aligned}\varphi(x + y) &= \overline{a + c} + 3\overline{(b + d)} = (\bar{a} + 3\bar{b}) + (\bar{c} + 3\bar{d}) = \varphi(x) + \varphi(y) \\ \varphi(xy) &= \overline{ac + 2bd} + 3\overline{(ad + bc)} = \bar{a}\bar{c} + 3\bar{a}\bar{d} + 3\bar{b}\bar{c} + 2\bar{b}\bar{d} \\ &= \bar{a}\bar{c} + 3\bar{a}\bar{d} + 3\bar{b}\bar{c} + 9\bar{b}\bar{d} = (\bar{a} + 3\bar{b}) \cdot (\bar{c} + 3\bar{d}) \\ &= \varphi(x)\varphi(y).\end{aligned}$$

Άρα η  $\varphi : \mathbb{Z}[\sqrt{2}] \rightarrow \mathbb{Z}_7$  είναι ομομορφισμός δακτυλίων.

(βγ) Έχουμε  $im(\varphi) = \mathbb{Z}_7$ , αφού  $\bar{a} = \varphi(a) \in im(\varphi)$  για κάθε  $\bar{a} \in \mathbb{Z}_7$ . Θα δείξουμε ότι ο πυρήνας του  $\varphi$  είναι ίσος με το κύριο ιδεώδες του  $\mathbb{Z}[\sqrt{2}]$  που παράγεται από το  $3 - \sqrt{2}$ . Πράγματι, έχουμε  $\varphi(3 - \sqrt{2}) = \bar{3} + 3(-\bar{1}) = \bar{0}$ . Άρα  $3 - \sqrt{2} \in \ker(\varphi)$  και επομένως  $\langle 3 - \sqrt{2} \rangle \subseteq \ker(\varphi)$ . Αντιστρόφως, έστω  $x = a + b\sqrt{2} \in \ker(\varphi)$ , όπου  $a, b \in \mathbb{Z}$ . Τότε  $\varphi(x) = \bar{a} + 3\bar{b} = \bar{0}$  στο  $\mathbb{Z}_7$  και συνεπώς  $a = -3b + 7c$  για κάποιο  $c \in \mathbb{Z}$ . Συμπεραίνουμε ότι  $x = -b(3 - \sqrt{2}) + 7c \in \langle 3 - \sqrt{2} \rangle$ , αφού  $3 - \sqrt{2} \in \langle 3 - \sqrt{2} \rangle$  και  $7 = (3 - \sqrt{2})(3 + \sqrt{2}) \in \langle 3 - \sqrt{2} \rangle$ . Δείξαμε λοιπόν ότι  $\ker(\varphi) \subseteq \langle 3 - \sqrt{2} \rangle$  και συμπεραίνουμε ότι  $\ker(\varphi) = \langle 3 - \sqrt{2} \rangle$ .

31. Έστω μη μηδενικός ομομορφισμός δακτυλίων  $\varphi : F \rightarrow S$ . Παρατηρούμε ότι ο πυρήνας  $\ker(\varphi)$  είναι ιδεώδες του  $F$  διάφορο του  $F$ . Αφού όμως κάθε σώμα  $F$  έχει μόνο τα τετριμμένα ιδεώδη  $\{0_F\}$  και  $F$ , θα πρέπει  $\ker(\varphi) = \{0_F\}$ . Κατά συνέπεια, ο  $\varphi : F \rightarrow S$  είναι μονομορφισμός.

32. Για το (α), αφήνεται στον αναγνώστη να επαληθεύσει ότι το  $\mathcal{I}(\alpha)$  είναι (με κενό και) κλειστό ως προς την πρόσθεση και ως προς τον πολλαπλασιασμό με στοιχεία του  $\mathbb{Q}[x]$ . Για το (β) μπορούμε να χρησιμοποιήσουμε το Διωνυμικό Θεώρημα, ή επαγωγή στο  $m$ . Για παράδειγμα, με το δεύτερο τρόπο, παρατηρούμε πρώτα ότι το ζητούμενο ισχύει για  $m = 0$ , θέτοντας  $a_0 = 1$  και  $b_0 = 0$ . Υποθέτοντας ότι ισχύει για το  $m$ , βρίσκουμε ότι

$$\begin{aligned}(1 + \sqrt{2})^{m+1} &= (1 + \sqrt{2})^m (1 + \sqrt{2}) = (a_m + b_m\sqrt{2})(1 + \sqrt{2}) \\ &= (a_m + 2b_m) + (a_m + b_m)\sqrt{2} \\ (1 + \sqrt{2})^{m+1} &= (1 - \sqrt{2})^m (1 - \sqrt{2}) \\ &= (a_m - b_m\sqrt{2})(1 - \sqrt{2}) = (a_m + 2b_m) - (a_m + b_m)\sqrt{2}\end{aligned}$$

και επομένως, θέτοντας  $a_{m+1} = a_m + 2b_m$  και  $b_{m+1} = a_m + b_m$ , το ζητούμενο ισχύει και για το  $m + 1$ . Για το (γ) θεωρούμε πολυώνυμο  $f(x) = c_0 + c_1x + \dots + c_nx^n \in \mathbb{Q}[x]$ . Χρησιμοποιώντας το (α), βρίσκουμε ότι

$$f(1 + \sqrt{2}) = \sum_{k=0}^n c_k(1 + \sqrt{2})^k = \sum_{k=0}^n c_k(a_k + b_k\sqrt{2}) = a + b\sqrt{2},$$

$$f(1 - \sqrt{2}) = \sum_{k=0}^n c_k(1 - \sqrt{2})^k = \sum_{k=0}^n c_k(a_k - b_k\sqrt{2}) = a - b\sqrt{2},$$

όπου  $a = \sum_{k=0}^n c_k a_k \in \mathbb{Q}$  και  $b = \sum_{k=0}^n c_k b_k \in \mathbb{Q}$ . Από αυτό συμπεραίνουμε ότι  $f(1 + \sqrt{2}) = 0 \Leftrightarrow f(1 - \sqrt{2}) = 0 \Leftrightarrow a = b = 0$  και συνεπώς ότι  $\mathcal{I}(1 + \sqrt{2}) = \mathcal{I}(1 - \sqrt{2})$ . Συμπεραίνουμε επίσης, για το (δ), ότι  $f(x) \in \mathcal{I}(1 + \sqrt{2})$  αν και μόνο αν το  $f(x)$  διαιρείται με το  $(x - 1 - \sqrt{2})(x - 1 + \sqrt{2}) = x^2 - 2x - 1$  στο  $\mathbb{Q}[x]$  και συνεπώς ότι  $\mathcal{I}(1 + \sqrt{2}) = \langle g(x) \rangle$ , όπου  $g(x) = x^2 - 2x - 1 \in \mathbb{Q}[x]$ .

33. Για το (α), γνωρίζουμε ότι τα στοιχεία του  $R$  είναι τα πολυώνυμα βαθμού το πολύ δύο στο  $\alpha$  με συντελεστές από το  $\mathbb{Z}_2$ , οπότε  $R = \{0, 1, \alpha, 1 + \alpha, \alpha^2, 1 + \alpha^2, \alpha + \alpha^2, 1 + \alpha + \alpha^2\}$ . Για το (β) παρατηρούμε ότι στο  $R$  έχουμε  $-1 = 1$  και  $\alpha^3 + 1 = 0$  και συμπεραίνουμε ότι  $\alpha^3 = -1 = 1$  και ότι  $(1 + \alpha)(1 + \alpha + \alpha^2) = 1 + 2\alpha + 2\alpha^2 + \alpha^3 = 1 + \alpha^3 = 0$ . Για το (γ) παρατηρούμε ότι τα στοιχεία  $1, \alpha$  και  $\alpha^2$  του  $R$  είναι αντιστρέψιμα, αφού  $1 \cdot 1 = \alpha \cdot \alpha^2 = 1$ . Από την ισότητα  $(1 + \alpha)(1 + \alpha + \alpha^2) = 0$  προκύπτει ότι τα στοιχεία  $1 + \alpha$  και  $1 + \alpha + \alpha^2$  δεν είναι αντιστρέψιμα. Αφού  $\alpha + \alpha^2 = \alpha(1 + \alpha)$  και  $\alpha(1 + \alpha^2) = 1 + \alpha$ , έπεται ότι ούτε τα  $\alpha + \alpha^2$  και  $1 + \alpha^2$  είναι αντιστρέψιμα. Άρα  $U(R) = \{1, \alpha, \alpha^2\}$ .
34. Παρατηρούμε ότι το πολυώνυμο  $x^2 + 1$  δεν είναι ανάγωγο επί του  $\mathbb{Z}_5$ , αφού έχει ρίζα το  $\bar{2}$  (και το  $-\bar{2}$ ), ενώ το  $x^2 + 2$  είναι ανάγωγο επί των  $\mathbb{Z}_5$  και  $\mathbb{Z}_7$ . Άρα, ο δακτύλιος  $\mathbb{Z}_5[x] / \langle x^2 + 1 \rangle$  δεν είναι σώμα και συνεπώς δεν είναι ισόμορφος με τους  $\mathbb{Z}_5[x] / \langle x^2 + 2 \rangle$  ή  $\mathbb{Z}_7[x] / \langle x^2 + 2 \rangle$ , καθένας από τους οποίους είναι σώμα. Επίσης, οι δύο τελευταίοι δακτύλιοι δεν είναι μεταξύ τους ισόμορφοι, αφού ο πρώτος έχει 25 στοιχεία και ο δεύτερος έχει 49.
35. Θεωρούμε την απεικόνιση  $\varphi : R \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$  που ορίζεται θέτοντας

$$\varphi \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = (\bar{a}, \bar{c}) \in \mathbb{Z}_m \times \mathbb{Z}_n$$

για  $a, b, c \in \mathbb{Z}$ . Αφήνουμε στον αναγνώστη να επαληθεύσει ότι για  $x, y \in R$  έχουμε  $\varphi(x + y) = \varphi(x) + \varphi(y)$  και  $\varphi(xy) = \varphi(x)\varphi(y)$ , δηλαδή ότι η  $\varphi$  είναι ομομορφισμός δακτυλίων. Από τον ορισμό του πυρήνα και της εικόνας βρίσκουμε ότι  $\ker(\varphi) = \{x \in R : \varphi(x) = 0\} = \mathcal{I}$  και ότι  $\text{im}(\varphi) = \mathbb{Z}_m \times \mathbb{Z}_n$ . Συμπεραίνουμε ότι το  $\mathcal{I}$  είναι ιδεώδες του  $R$  και (από το Θεώρημα του Ισομορφισμού) ότι η  $\varphi$  επάγει ισομορφισμό δακτυλίων  $\bar{\varphi} : R/\mathcal{I} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ .

36. Στην περίπτωση του (β), το πολυώνυμο  $x^2 - 1 = (x - 1)(x + 1)$  έχει δύο διακεκριμένες ρίζες στο  $\mathbb{Z}_3$ . Έτσι, ο ομομορφισμός δακτυλίων  $\varphi : \mathbb{Z}_3[x] \rightarrow \mathbb{Z}_3 \times \mathbb{Z}_3$  με  $\varphi(f(x)) = (f(1), f(-1))$  για  $f(x) \in \mathbb{Z}_3[x]$  είναι επιμορφισμός δακτυλίων με πυρήνα  $\langle x^2 - 1 \rangle \subseteq \mathbb{Z}_3[x]$  (εξηγήστε γιατί). Από το θεώρημα του ισομορφισμού έπεται ότι ο δακτύλιος  $\mathbb{Z}_3[x] / \langle x^2 - 1 \rangle$  είναι ισόμορφος με τον  $\mathbb{Z}_3 \times \mathbb{Z}_3$ . Το ίδιο επιχείρημα δεν ισχύει στην περίπτωση του (α), αφού το πολυώνυμο  $x^2 - 1 = (x - 1)^2$  έχει μία διπλή ρίζα στο  $\mathbb{Z}_2$ . Μάλιστα  $\mathbb{Z}_2[x] / \langle x^2 - 1 \rangle = \{0, 1, \alpha, 1 + \alpha\}$  με  $\alpha^2 = 1$ , όπου  $\alpha = x + \langle x^2 - 1 \rangle$ , και συνεπώς ο  $\mathbb{Z}_2[x] / \langle x^2 - 1 \rangle$  έχει τα δύο αντιστρέψιμα στοιχεία 1 και  $\alpha$ , ενώ ο  $\mathbb{Z}_2 \times \mathbb{Z}_2$  έχει μόνο ένα αντιστρέψιμο στοιχείο. Κατά συνέπεια, οι δύο δακτύλιοι δεν είναι ισόμορφοι.

37. Έστω ότι  $\mathbb{Z}_p[x] / \langle f(x) \rangle \cong \mathbb{Z}_p[x] / \langle g(x) \rangle$  και ότι  $\deg(f(x)) = m$  και  $\deg(g(x)) = n$ . Αφού το πλήθος των στοιχείων των δακτυλίων  $\mathbb{Z}_p[x] / \langle f(x) \rangle$  και  $\mathbb{Z}_p[x] / \langle g(x) \rangle$  είναι ίσο με  $p^m$  και  $p^n$ , αντίστοιχα, θα πρέπει να ισχύει  $p^m = p^n$ , δηλαδή  $m = n$ . Άρα η πρόταση στο (β) είναι αληθής. Επίσης, αφού γνωρίζουμε ότι για όλα τα  $a, b \in \mathbb{Z}_p$  έχουμε  $\mathbb{Z}_p[x] / \langle x - a \rangle \cong \mathbb{Z}_p$  και  $\mathbb{Z}_p[x] / \langle x - b \rangle \cong \mathbb{Z}_p$ , άρα  $\mathbb{Z}_p[x] / \langle x - a \rangle \cong \mathbb{Z}_p[x] / \langle x - b \rangle$ , η πρόταση στο (α) είναι ψευδής.

38. Για το (α) υπολογίζουμε ότι

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 6 & 7 & 4 & 2 & 8 & 1 \end{pmatrix}, \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 5 & 7 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}$$

και ότι

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 2 & 1 & 7 & 5 & 8 & 6 \end{pmatrix}, \quad \tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 8 & 6 & 3 & 7 & 1 & 4 \end{pmatrix}.$$

Για το (β) παρατηρούμε ότι  $\sigma\tau = (1\ 5\ 4\ 7\ 8)(2\ 3\ 6)$  και συμπεραίνουμε ότι  $(\sigma\tau)^{1000} = (1\ 5\ 4\ 7\ 8)^{1000}(2\ 3\ 6)^{1000} = (2\ 3\ 6)$ .

39. Για τα (α) και (β) υπολογίζουμε ότι  $\sigma(1) = 5$ ,  $\sigma(2) = 4$ ,  $\sigma(3) = 3$ ,  $\sigma(4) = 2$  και  $\sigma(5) = 1$  και συμπεραίνουμε ότι  $\sigma = (1\ 5)(2\ 4)$  και ότι  $\sigma^2 = (1\ 5)^2(2\ 4)^2 = e$ . Για το (γ), αφού  $\sigma = (1\ 5)(2\ 4)$ , μια τέτοια μετάθεση  $\tau \in \mathcal{S}_5$  είναι η  $(1\ 2\ 3)$  και μία άλλη η  $(1\ 2)(3\ 4)$ .

40. Προφανώς ο  $n = 1$  έχει τη δοσμένη ιδιότητα. Το ίδιο ισχύει για τον  $n = 3$  αφού οι μεταθέσεις  $\sigma \in \mathcal{S}_3$  για τις οποίες η  $\sigma^2$  έχει σταθερό σημείο είναι η ταυτοτική και οι τρεις αντιμεταθέσεις  $(1\ 2)$ ,  $(1\ 3)$ ,  $(2\ 3)$ , καθεμιά από τις οποίες έχει σταθερό σημείο. Αντιθέτως, η αντιμετάθεση  $\sigma = (1\ 2) \in \mathcal{S}_2$  δεν έχει σταθερό σημείο, ενώ η  $\sigma^2$  έχει, και για  $n \geq 4$  η μετάθεση  $\sigma = (1\ 2)(3\ 4 \cdots n) \in \mathcal{S}_2$  δεν έχει σταθερό σημείο, ενώ η  $\sigma^2$  έχει. Άρα οι ζητούμενοι θετικοί ακέραιοι είναι οι 1 και 3.

41. Για το (α) παρατηρούμε ότι αν η  $\sigma\tau$  έχει σταθερό σημείο το  $i \in \{1, 2, \dots, n\}$ , τότε  $(\sigma(\tau(i))) = i$  και συνεπώς  $\tau(\sigma(\tau(i))) = \tau(i)$ , οπότε η  $\tau\sigma$  έχει σταθερό σημείο

το  $\tau(i) \in \{1, 2, \dots, n\}$ . Για το (α) υποθέτουμε ότι η  $\sigma\tau = (a_1 a_2 \cdots a_n)$  είναι κυκλική μετάθεση. Τότε  $(\sigma\tau)(a_i) = a_{i+1}$  για κάθε  $i$  και συνεπώς  $(\tau\sigma)(\sigma^{-1}(a_i)) = \tau(a_i) = \sigma^{-1}(\sigma\tau(a_i)) = \sigma^{-1}(a_{i+1})$  για κάθε  $i$ , οπότε η  $\tau\sigma$  είναι ίση με την κυκλική μετάθεση  $(\sigma^{-1}(a_1) \sigma^{-1}(a_2) \cdots \sigma^{-1}(a_n))$ .

42. (α) Αν  $c$  είναι το ταυτοτικό στοιχείο της  $G$ , τότε  $e^2 = e = c \cdot e$  και συνεπώς (διαγράφοντας τον παράγοντα  $e$  από τα δεξιά)  $c = e$ .

(β) Υποθέτουμε ότι  $ab = ba$  και δείχνουμε με επαγωγή ότι  $(ab)^n = a^n b^n = b^n a^n$  για κάθε θετικό ακέραιο  $n$  ως εξής. Το ζητούμενο είναι τετριμμένο για  $n = 1$  και υποθέτοντας ότι  $(ab)^n = a^n b^n = b^n a^n$ , βρίσκουμε ότι

$$\begin{aligned} (ab)^{n+1} &= a \cdot (ba)^n \cdot b = a \cdot (ab)^n \cdot b = a \cdot (a^n b^n) \cdot b = (a \cdot a^n)(b^n \cdot b) \\ &= a^{n+1} b^{n+1} \end{aligned}$$

και ομοίως ότι  $(ab)^{n+1} = (ba)^{n+1} = b^{n+1} a^{n+1}$ . Στην περίπτωση μας ειδικότερα, έχουμε  $(ab)^6 = a^6 b^6 = (a^2)^3 \cdot (b^3)^2 = e^3 \cdot e^2 = e$ .

(γ) Θέτοντας  $G = \mathcal{S}_4$ ,  $a = (1\ 2)$  και  $b = (2\ 3\ 4)$ , οπότε  $a^2 = b^3 = e$ ,  $ab = (1\ 2\ 3\ 4)$  και  $(ab)^6 = (ab)^2 = (1\ 3)(2\ 4)$ , βρίσκουμε ότι το (α) δεν ισχύει χωρίς την υπόθεση  $ab = ba$ .

43. Με τη γνωστή διαδικασία βρίσκουμε ότι

$$\sigma = (1)(2\ 4\ 10\ 14\ 12\ 6)(7\ 5\ 13\ 9\ 11\ 3)(8)(15).$$

Συμπεραίνουμε ότι η τάξη της  $\sigma$  είναι ίση με 6 και ότι η τάξη της  $\sigma^{64} = \sigma^4$  είναι ίση με 3. Μία μετάθεση με  $\tau \in \mathcal{S}_{15}$  με  $\tau^2 = \sigma$  είναι η

$$\tau = (2\ 7\ 4\ 5\ 10\ 13\ 14\ 9\ 12\ 11\ 6\ 3).$$

Μία άλλη είναι η  $\tau = (1\ 8)(2\ 9\ 4\ 11\ 10\ 3\ 14\ 7\ 12\ 5\ 6\ 13)$ .

44. Τα μόνα στοιχεία τάξης 3 της ομάδας  $\mathcal{S}_5$  είναι οι κύκλοι μήκους 3 (εξηγήστε γιατί). Υπάρχουν  $\binom{5}{3} = 10$  τρόποι να επιλέξει κανείς το σύνολο  $\{a, b, c\}$  των τριών στοιχείων ενός τέτοιου κύκλου και δύο τρόποι να επιλέξει κανείς τη φορά του, δηλαδή την  $(a\ b\ c)$  ή την  $(a\ c\ b)$ . Επομένως, υπάρχουν συνολικά 20 στοιχεία τάξης 3 στην  $\mathcal{S}_5$ .

45. Για το (α) θυμόμαστε ότι η τάξη οποιουδήποτε στοιχείου της  $G$  διαιρεί την τάξη της  $G$ . Άρα, στην περίπτωση μας τα στοιχεία της  $G$  έχουν τάξεις 1, 2 ή 4. Αν υπάρχει στοιχείο  $a \in G$  τάξης 4, τότε  $G = \{e, a, a^2, a^3\}$  με  $a^4 = e$ . Διαφορετικά έχουμε  $G = \{e, a, b, c\}$  με  $a^2 = b^2 = c^2 = e$ . Αποκλείοντας τις περιπτώσεις  $ab = e$  (αφού από αυτήν προκύπτει ότι  $b = a^{-1} = a$ ),  $ab = a$  και  $ab = b$  (αφού από αυτές προκύπτει ότι  $b = e$  και  $a = e$ , αντίστοιχα) για το  $ab$ , συμπεραίνουμε ότι  $ab = c$ . Ομοίως βρίσκουμε ότι  $ba = c$  και συμπεραίνουμε ότι  $G = \{e, a, b, ab\}$  με  $a^2 = b^2 = e$  και  $ab = ba$ . Το (β) είναι άμεση συνέπεια του (α).



46. Το σύνολο, έστω  $S$ , που δίνεται στο (γ) δεν είναι υποομάδα της  $G$  διότι για κάθε πίνακα  $A \in G$  με ορίζουσα μεγαλύτερη του 1 έχουμε  $A \in S$  αλλά  $\det(A^{-1}) = 1/\det(A) < 1$  και συνεπώς ο  $A^{-1}$  δεν ανήκει στο  $S$ . Οι ισότητες

$$\begin{pmatrix} 1+a & -a \\ a & 1-a \end{pmatrix} \begin{pmatrix} 1+b & -b \\ b & 1-b \end{pmatrix} = \begin{pmatrix} 1+a+b & -a-b \\ a+b & 1-a-b \end{pmatrix}$$

$$\begin{pmatrix} 1+a & -a \\ a & 1-a \end{pmatrix}^{-1} = \begin{pmatrix} 1-a & a \\ -a & 1+a \end{pmatrix}$$

δείχνουν ότι το σύνολο που δίνεται στο (β) είναι υποομάδα της  $G$ . Αφού το σύνολο αυτό είναι υπεραριθμησίμο, η υποομάδα αυτή δεν είναι κυκλική. Για το (γ) παρατηρούμε ότι

$$\begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^n$$

για  $n \in \mathbb{Z}$  και συμπεραίνουμε ότι το δοσμένο σύνολο είναι η κυκλική υποομάδα της  $G$  που παράγεται από τον πίνακα  $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ .

47. Οι στροφές ως προς το κέντρο του τετραγώνου κατά γωνίες  $0, \pi/2, \pi$  και  $3\pi/2$  αποτελούν τα στοιχεία μιας κυκλικής υποομάδας της  $G$  τάξης 4. Επίσης, σύμφωνα με το Θεώρημα του Lagrange, κάθε γνήσια υποομάδα της  $G$  έχει τάξη ίση με 2 ή 4. Από την Άσκηση 45 προκύπτει ότι κάθε τέτοια υποομάδα είναι αβελιανή. Συνεπώς οι προτάσεις στα (α) και (β) είναι αληθείς. Για το (γ), θεωρούμε τις ορθογώνιες ανακλάσεις  $a$  και  $b$  στους δύο άξονες συμμετρίας του τετραγώνου που είναι παράλληλοι στις ακμές του και παρατηρούμε ότι  $a^2 = b^2 = e$  και ότι  $ab = ba$ . Συμπεραίνουμε ότι η  $\{e, a, b, ab\}$  είναι μια μη κυκλική υποομάδα τάξης 4 της  $G$  και επομένως ότι η πρόταση στο (γ) είναι ψευδής.
48. Για το πλήθος των αριστερών κλάσεων  $[G : H]$  της  $H$  στη  $G$  έχουμε  $[G : H] = |G|/|H| = 2n/n = 2$ . Για το (β) θεωρούμε στοιχεία  $a, b \in G \setminus H$ , οπότε  $a^{-1} \in G \setminus H$ . Αφού υπάρχουν ακριβώς δύο αριστερές κλάσεις της  $H$  στη  $G$ , αυτές είναι οι  $H$  και  $aH = a^{-1}H$ . Αφού  $b \in G \setminus H$ , θα πρέπει να έχουμε  $b \in a^{-1}H$  και συνεπώς  $ab \in H$ .
49. Για το (α) παρατηρούμε ότι  $\sigma\tau = \tau\sigma$ , οπότε  $\sigma\tau\sigma^{-1} = (\sigma\sigma)(\tau\tau^{-1}) = \sigma^2 = e$ . Για το (β) παρατηρούμε ότι  $\sigma = \alpha^3$  και  $\tau = \alpha^2$ , όπου  $\alpha = (1\ 2\ 3\ 4\ 5\ 6)$  είναι κυκλική μετάθεση της  $S_6$  και συμπεραίνουμε ότι οι  $\sigma$  και  $\tau$  είναι στοιχεία της κυκλικής υποομάδας τάξης 6 της  $S_6$  που παράγεται από την  $\alpha$ . Το ερώτημα (γ) έχει αρνητική απάντηση, αφού η  $\tau$  έχει τάξη 3 και συνεπώς δεν περιέχεται σε υποομάδα τάξης 8 της  $S_6$ .
50. Σύμφωνα με το Θεώρημα του Lagrange, η τάξη κάθε γνήσιας υποομάδας της  $G$  είναι γνήσιος διαιρέτης της τάξης της  $G$  και συνεπώς ισούται με 5. Άρα, κάθε

γνήσια υποομάδα της  $G$  είναι κυκλική τάξης 5. Ειδικότερα (αφού η  $G$  δεν έχει στοιχεία τάξης 25), κάθε στοιχείο της  $G$  εκτός του ταυτοτικού  $e \in G$  έχει τάξη ίση με 5 και συνεπώς ανήκει σε κάποια γνήσια υποομάδα της  $G$  (συγκεκριμένα, στην κυκλική υποομάδα που παράγει το στοιχείο αυτό) και για διακεκριμένες γνήσιες υποομάδες  $H, K$  της  $G$  έχουμε  $H \cap K = \{e\}$ . Από τα προηγούμενα συμπεραίνουμε ότι καθένα από τα 24 στοιχεία της  $G$  εκτός του  $e$  ανήκει σε μία μοναδική γνήσια υποομάδα της  $G$ , καθεμιά από τις οποίες έχει ακριβώς 4 στοιχεία εκτός του  $e$ , και επομένως ότι η  $G$  έχει ακριβώς  $24/4 = 6$  γνήσιες υποομάδες.

51. Για το (α) παρατηρούμε ότι  $\varphi(AB) = \det(AB) \cdot (AB) = \det(A) \det(B) \cdot AB = \varphi(A)\varphi(B)$  για  $A, B \in G$  και συμπεραίνουμε το ζητούμενο. Για το (β) υπενθυμίζουμε ότι  $\det(\lambda A) = \lambda^n \det(A)$  για κάθε  $n \times n$  πίνακα  $A$  και  $\lambda \in \mathbb{R}$ . Θα δείξουμε ότι ο ομομορφισμός  $\varphi$  είναι αυτομορφισμός της  $G$  αν και μόνο αν ο  $n$  είναι άρτιος. Αν ο  $n$  είναι περιττός, τότε  $\det(\varphi(A)) = \det(\det(A)A) = \det(A)^{n+1} > 0$  για κάθε  $A \in G$  και συνεπώς η απεικόνιση  $\varphi : G \rightarrow G$  δεν είναι επί. Έστω ότι ο  $n$  είναι άρτιος. Αρκεί να δείξουμε ότι για κάθε  $B \in G$  υπάρχει μοναδικό  $A \in G$  τέτοιο ώστε  $\varphi(A) = \det(A) \cdot A = B$ . Προφανώς θα πρέπει να έχουμε  $A = \lambda B$  για κάποιο  $\lambda \in \mathbb{R}$ , οπότε

$$\varphi(A) = \det(A) \cdot A = \det(\lambda B) \cdot \lambda B = \lambda^{n+1} \det(B) \cdot B.$$

Αφού ο  $n + 1$  είναι περιττός, η εξίσωση  $\lambda^{n+1} = 1/\det(B)$  έχει μοναδική λύση  $\lambda \in \mathbb{R}$ . Κατά συνέπεια, η εξίσωση  $\varphi(A) = B$  έχει μοναδική λύση  $A \in G$ .

52. Για το (α), με τη συνήθη διαδικασία βρίσκουμε ότι

$$w = (1 \ 7 \ 5) (2 \ 4 \ 8 \ 6) (3)$$

και συμπεραίνουμε ότι  $\epsilon(w) = (-1)^2 \cdot (-1)^3 \cdot (-1)^0 = -1$ , δηλαδή ότι η  $w$  είναι περιττή μετάθεση. Το ερώτημα στο (β) έχει αρνητική απάντηση αφού

$$\epsilon(\sigma\tau^2\sigma^{-1}) = \epsilon(\sigma)\epsilon(\tau^2)\epsilon(\sigma^{-1}) = \epsilon(\sigma)\epsilon(\tau)^2\epsilon(\sigma)^{-1} = \epsilon(\tau)^2 = 1$$

και συνεπώς η  $\sigma\tau^2\sigma^{-1}$  είναι άρτια μετάθεση για όλες τις  $\sigma, \tau \in \mathcal{S}_n$ .

53. Για το (α) παρατηρούμε ότι η  $\sigma$  είναι αντιστρέψιμη, με αντίστροφη την  $\tau : \mathbb{Z}_{12} \rightarrow \mathbb{Z}_{12}$  με  $\tau(x) = x - 3$  για  $x \in \mathbb{Z}_{12}$ . Για το (β), με τη συνήθη διαδικασία βρίσκουμε ότι

$$\sigma = (\bar{1} \ \bar{4} \ \bar{7} \ \bar{10}) (\bar{2} \ \bar{5} \ \bar{8} \ \bar{11}) (\bar{3} \ \bar{6} \ \bar{9} \ \bar{12})$$

και συμπεραίνουμε ότι η  $\sigma$  είναι περιττή μετάθεση. Το ερώτημα στο (γ) έχει αρνητική απάντηση αφού η  $\tau^2 = \tau \circ \tau$  είναι άρτια μετάθεση για κάθε μετάθεση  $\tau$  οποιουδήποτε πεπερασμένου συνόλου.

54. Για το (α) παρατηρούμε ότι για κάθε αντιμετάθεση  $t \in S_n$  έχουμε  $(\varphi(t))^2 = \varphi(t^2) = \varphi(e) = 1$  και συνεπώς ότι  $\varphi(t) \in \{1, -1\}$ . Για το (β) θυμόμαστε ότι κάθε μετάθεση  $\sigma \in S_n$  γράφεται ως γινόμενο αντιμεταθέσεων  $\sigma = t_1 t_2 \cdots t_m$  οπότε, σύμφωνα με το (α),  $\varphi(\sigma) = \varphi(t_1) \varphi(t_2) \cdots \varphi(t_m) \in \{1, -1\}$ . Υποθέτουμε τώρα ότι  $n = 3$  και συμβολίζουμε με  $t_1 = (1\ 2)$ ,  $t_2 = (1\ 3)$ ,  $t_3 = (2\ 3)$ ,  $\alpha = (1\ 2\ 3)$  και  $\beta = (1\ 3\ 2)$  τα στοιχεία της  $S_3$  εκτός της ταυτοτική μετάθεσης. Από τις ισότητες  $\alpha = \beta^2$  και  $\beta = \alpha^2$  και το αποτέλεσμα στο (β) προκύπτει ότι  $\varphi(\alpha) = \varphi(\beta^2) = \varphi(\beta)^2 = 1$  και ομοίως ότι  $\varphi(\beta) = \varphi(\alpha^2) = \varphi(\alpha)^2 = 1$ . Επίσης, από τις σχέσεις  $\alpha t_1 = t_2$  και  $\alpha t_2 = t_3$  προκύπτει ότι  $\varphi(t_2) = \varphi(\alpha t_1) = \varphi(\alpha) \varphi(t_1) = \varphi(t_1)$  και  $\varphi(t_3) = \varphi(\alpha t_2) = \varphi(\alpha) \varphi(t_2) = \varphi(t_2)$ , οπότε  $\varphi(t_1) = \varphi(t_2) = \varphi(t_3) = \epsilon$  για κάποιο  $\epsilon \in \{1, -1\}$ . Συμπεραίνουμε ότι υπάρχουν ακριβώς δύο ομομορφισμοί  $\varphi : S_3 \rightarrow \mathbb{C}^\times$ : ο τετριμμένος (για  $\epsilon = 1$ ) και ο ομομορφισμός του προσήμου (για  $\epsilon = -1$ ).
55. Έστω ότι ο  $R$  είναι ισόμορφος με τον  $S$  και έστω ισομορφισμός δακτυλίων  $\varphi : R \rightarrow S$ . Τότε η απεικόνιση  $\varphi$  είναι 1-1 και επί και ισχύει  $\varphi(a + b) = \varphi(a) + \varphi(b)$  (και  $\varphi(ab) = \varphi(a)\varphi(b)$ ) για  $a, b \in R$ . Συνεπώς η  $\varphi$  είναι και ισομορφισμός των προσθετικών ομάδων των  $R$  και  $S$  και η πρόταση στο (α) είναι αληθής. Το αντίστροφο δεν ισχύει αφού, για παράδειγμα, οι δακτύλιοι  $\mathbb{Z}[i]$  και  $\mathbb{Z} \times \mathbb{Z}$  δεν είναι ισόμορφοι (ο πρώτος είναι ακέραια περιοχή, ενώ ο δεύτερος δεν είναι) αλλά έχουν ισόμορφες προσθετικές ομάδες (η απεικόνιση  $\varphi : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}[i]$  με  $\varphi(a, b) = a + bi$  για  $a, b \in \mathbb{Z}$  είναι ισομορφισμός προσθετικών ομάδων). Επίσης, οι  $\mathbb{Q}[x] / \langle x^2 + 1 \rangle$  και  $\mathbb{Q}[x] / \langle x^2 \rangle$  δεν είναι ισόμορφοι (ο πρώτος είναι σώμα, ενώ ο δεύτερος δεν είναι) αλλά έχουν ισόμορφες προσθετικές ομάδες.
56. Έστω  $a, b$  δύο διαφορετικά στοιχεία τάξης 2 της  $G$ . Για το (α) παρατηρούμε ότι η έχει δύο διαφορετικές υποομάδες τάξης 2, τις  $\{e, a\}$  και  $\{e, b\}$ , και συμπεραίνουμε το ζητούμενο. Για το (β) παρατηρούμε ότι  $ab = ba$  και ότι η  $\{e, a, b, ab\}$  είναι υποομάδα (εξηγήστε γιατί) τάξης 4 της  $G$ . Από το Θεώρημα του Lagrange έπεται ότι η τάξη της  $G$  διαιρείται με το 4. Το (γ) έχει αρνητική απάντηση διότι, για παράδειγμα, η συμμετρική ομάδα  $S_3$  έχει τάξη 6 και τρία στοιχεία τάξης 2.
57. Γνωρίζουμε ότι για κάθε γεννήτορα  $a$  κυκλικής ομάδας τάξης  $n$  και κάθε  $k \in \mathbb{Z}$  ισχύει  $\langle a^k \rangle = \langle a^d \rangle = \{a^d, a^{2d}, \dots, a^n\} = \{e, a^d, \dots, a^{n-d}\}$ , όπου  $d = \mu\kappa\delta(n, k)$ . Στην περίπτωση μας έχουμε  $n = 24$  και συνεπώς  $\langle a^{14} \rangle = \langle a^2 \rangle = \{e, a^2, a^4, \dots, a^{22}\}$  και  $\langle a^{39} \rangle = \langle a^3 \rangle = \{e, a^3, a^6, \dots, a^{21}\}$ , οπότε  $\langle a^{14} \rangle \cap \langle a^{39} \rangle = \{e, a^6, a^{12}, a^{18}\}$ .
58. Για το (α) παρατηρούμε ότι  $U(\mathbb{Z}_{18}) = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{13}, \bar{17}\}$  και ότι τα στοιχεία  $\bar{5}$  και  $\bar{11}$  είναι γεννήτορες της  $U(\mathbb{Z}_{18})$ , αφού  $\bar{5}^2 = \bar{7}$ ,  $\bar{5}^3 = \bar{17}$ ,  $\bar{5}^4 = \bar{13}$  και  $\bar{5}^5 = \bar{11}$ . Για το (β) παρατηρούμε ότι για τυχαίο σώμα  $\mathbb{F}$ , η ομάδα  $SL_2(\mathbb{F})$  δεν είναι αβελιανή (εξηγήστε γιατί), άρα ούτε κυκλική. Για το (γ) γνωρίζουμε ότι κάθε στοιχείο του  $\mathbb{Z}_2[x] / \langle x^3 \rangle$  γράφεται με μοναδικό τρόπο στη μορφή  $\alpha = a + bx + cx^2 + \langle x^3 \rangle$  με  $a, b, c \in \mathbb{Z}_2$ . Από τη σχετική θεωρία προκύπτει ότι το  $\alpha$  είναι αντιστρέψιμο αν και

μόνο αν το πολυώνυμο  $a + bx + cx^2$  είναι σχετικώς πρώτο προς το  $x^3$  στο  $\mathbb{Z}_2[x]$ , δηλαδή αν  $a \neq 0$ . Συνεπώς η δοσμένη ομάδα έχει τάξη 4 και παράγεται από το στοιχείο της  $\beta = 1 + x + \langle x^3 \rangle$ , αφού  $\beta^2 = 1 + x^2 + \langle x^3 \rangle$  και  $\beta^3 = 1 + x + x^2 + \langle x^3 \rangle$  (και φυσικά  $\beta^4 = 1$ ). Εργαζόμαστε ομοίως για το (δ), δείχνουμε ότι η δοσμένη ομάδα έχει τουλάχιστον δύο στοιχεία τάξης 2, για παράδειγμα τα  $1 + x^2 + \langle x^4 \rangle$  και  $1 + x^3 + \langle x^4 \rangle$ , και συμπεραίνουμε ότι η ομάδα αυτή δεν είναι κυκλική.

59. Για το (α) γνωρίζουμε ότι η τάξη του  $\varphi(a) \in \mathcal{S}_3$  πρέπει να διαιρεί την τάξη του  $a \in G$ , δηλαδή το 9. Τα στοιχεία της  $\mathcal{S}_3$  με την ιδιότητα αυτή είναι το ταυτοτικό στοιχείο  $e$  και οι δύο κυκλικές μεταθέσεις  $(1\ 2\ 3)$  και  $(1\ 3\ 2)$ . Αν  $\varphi(a) = e$ , τότε προκύπτει ο τετριμμένος ομομορφισμός  $\varphi : G \rightarrow \mathcal{S}_3$ . Αν  $\varphi(a) = (1\ 2\ 3)$  (αντίστοιχα,  $\varphi(a) = (1\ 3\ 2)$ ), τότε προκύπτει ο ομομορφισμός  $\varphi(a^k) = (1\ 2\ 3)^k$  (αντίστοιχα,  $\varphi(a^k) = (1\ 3\ 2)^k$ ) για  $k \in \mathbb{Z}$ . Για το (β) δείχνουμε ότι για κάθε θετικό ακέραιο  $n$  και κάθε πεπερασμένη ομάδα  $G$  περιττής τάξης, ο μόνος ομομορφισμός ομάδων  $\psi : \mathcal{S}_n \rightarrow G$  είναι ο τετριμμένος ως εξής. Σκεπτόμενοι όπως στο (α) δείχνουμε πρώτα ότι  $\psi(t) = e$  για κάθε αντιμετάθεση  $t \in \mathcal{S}_n$ . Γράφοντας τώρα τυχαία μετάθεση  $\sigma \in \mathcal{S}_n$  ως γινόμενο αντιμεταθέσεων  $\sigma = t_1 t_2 \cdots t_m$ , βρίσκουμε ότι  $\psi(\sigma) = \psi(t_1)\psi(t_2) \cdots \psi(t_m) = e$  και συμπεραίνουμε το ζητούμενο.
60. Για το (α) παρατηρούμε πρώτα ότι η  $H = \{e, a\}$  είναι κανονική υποομάδα της  $G$  αν και μόνο αν ισχύει  $axa^{-1} \in \{e, a\}$  για κάθε  $x \in G$ . Παρατηρούμε έπειτα ότι  $axa^{-1} \neq e$  για κάθε  $x \in G$  (αφού  $a \neq e$ ) και ότι  $axa^{-1} = a \Leftrightarrow ax = xa$  και συμπεραίνουμε το ζητούμενο. Για το (β) εφαρμόζουμε το (α) και συμπεραίνουμε ότι η  $\mathcal{S}_3$  δεν έχει κανονικές υποομάδες τάξης 2, ότι η μοναδική κανονική υποομάδα τάξης 2 της ομάδας των συμμετριών του τετραγώνου είναι αυτή που παράγεται από τη στροφή γύρω από το κέντρο του τετραγώνου κατά γωνία  $\pi$  και ότι η μοναδική κανονική υποομάδα τάξης 2 της  $SL_2(\mathbb{R})$  είναι η  $\{I_2, -I_2\}$ .
61. Αφού ο πυρήνας  $\ker(\varphi)$  είναι κανονική υποομάδα της  $G$  και  $zxy^{-1}z^{-1} \in \ker(\varphi)$ , θα πρέπει να έχουμε  $xy^{-1} \in \ker(\varphi)$ . Αυτό σημαίνει ότι  $\varphi(xy^{-1}) = e_K$  ή, ισοδύναμα, ότι  $\varphi(x)(\varphi(y))^{-1} = e_K$ , δηλαδή  $\varphi(x) = \varphi(y)$ . Ομοίως βρίσκουμε ότι  $\varphi(y) = \varphi(z)$ , οπότε προκύπτει το (α). Για το (β) γνωρίζουμε ότι  $|G| = |\ker(\varphi)| \cdot |K|$ , παρατηρούμε ότι ο πυρήνας  $\ker(\varphi)$  περιέχει τα τρία διαφορετικά ανά δύο (εξηγήστε γιατί) στοιχεία  $e_G$ ,  $xy^{-1}$  και  $xz^{-1} = (xy^{-1})(yz^{-1})$  και συμπεραίνουμε το ζητούμενο.
62. Γνωρίζουμε ότι η απεικόνιση  $\varphi : G \rightarrow \mathbb{Z}_p^\times$  που ορίζεται θέτοντας  $\varphi(X) = \det(X)$  για  $X \in G$  είναι επιμορφισμός ομάδων με πυρήνα την  $N$ . Από το Θεώρημα του ισομορφισμού έπεται ότι η ομάδα  $G/N$  είναι ισόμορφη με τη  $\mathbb{Z}_p^\times$ . Ειδικότερα, η τάξη της  $G/N$  είναι ίση με εκείνη της  $\mathbb{Z}_p^\times$ , δηλαδή με  $p - 1$ , και το πλήθος των υποομάδων της  $G/N$  είναι ίσο με εκείνο της  $\mathbb{Z}_p^\times$ . Αφού η τελευταία είναι κυκλική τάξης  $p - 1$ , το πλήθος των υποομάδων της είναι ίσο με το πλήθος των θετικών διακριτών του  $p - 1$ . Για  $p = 31$  το πλήθος αυτό είναι ίσο με 8.

63. Για το (α) παρατηρούμε ότι  $\varphi(z_1 z_2) = (z_1 z_2)^2 = z_1^2 z_2^2 = \varphi(z_1) \varphi(z_2)$  για όλα τα  $z_1, z_2 \in G$  και συμπεραίνουμε ότι η  $\varphi$  είναι ομομορφισμός ομάδων. Υπολογίζουμε έπειτα ότι  $\ker(\varphi) = \{z \in G : \varphi(z) = 1\} = \{z \in \mathbb{C} : z^2 = 1\} = \{1, -1\}$  και παρατηρούμε ότι η εξίσωση  $\varphi(z) = a$ , δηλαδή η  $z^2 = a$ , έχει λύση  $z \in \mathbb{C} \setminus \{0\} = G$  για κάθε  $a \in G$ , οπότε  $\text{im}(\varphi) = G$ . Για το (β) συνάγουμε από τα προηγούμενα και το Θεώρημα του ισομορφισμού ότι η υποομάδα  $N = \{1, -1\}$  της  $G$  έχει τις ζητούμενες ιδιότητες.
64. Οι προτάσεις αυτές είναι ψευδείς. Για το (α) θεωρούμε την προσθετική ομάδα  $\mathbb{Z}$  των ακεραίων και τις (κανονικές) υποομάδες  $2\mathbb{Z}$  και  $3\mathbb{Z}$ . Παρατηρούμε ότι οι τρεις αυτές ομάδες, ως άπειρες κυκλικές, είναι ισόμορφες και ότι οι  $\mathbb{Z}/2\mathbb{Z}$  και  $\mathbb{Z}/3\mathbb{Z}$  δεν είναι, αφού έχουν διαφορετικές τάξεις. Εναλλακτικά, θεωρούμε την αβελιανή ομάδα  $G = \mathbb{Z}_2 \times \mathbb{Z}_4$  και τις κυκλικές της υποομάδες  $N_1$  και  $N_2$  που παράγονται από τα στοιχεία  $(\bar{1}, \bar{0})$  και  $(\bar{0}, \bar{2})$  τάξης 2, αντίστοιχα. Παρατηρούμε ότι οι  $N_1$  και  $N_2$  είναι ισόμορφες, αφού έχουν τάξη 2, και ότι οι  $G/N_1$  και  $G/N_2$  δεν είναι αφού η πρώτη είναι κυκλική, ενώ η δεύτερη όχι (εξηγήστε γιατί). Για το (β) θεωρούμε την ομάδα  $G$  των συμμετριών του τετραγώνου. Γνωρίζουμε από προηγούμενη άσκηση ότι η  $G$  έχει κυκλική υποομάδα  $N_1$  τάξης 4 και μη κυκλική υποομάδα  $N_2$  της ίδιας τάξης. Οι υποομάδες αυτές της  $G$  είναι κανονικές (εξηγήστε γιατί) και η  $G/N_1$  είναι ισόμορφη με τη  $G/N_2$ , αφού και οι δύο αυτές ομάδες έχουν τάξη 2, αλλά προφανώς η  $N_1$  δεν είναι ισόμορφη με τη  $N_2$ .