ΒΑΣΙΚΗ ΑΛΓΕΒΡΑ

Συμπληρωματικές Ασκήσεις
Εαρινό Εξάμηνο 2023

Χρήστος Α. Αθανασιάδης

Συμβολίζουμε με $\mathbb{Z}_m$ το δακτύλιο των ακεραίων modulo m, με $\bar{a} \in \mathbb{Z}_m$ την κλάση $(\mathrm{mod}\, m)$ του $a \in \mathbb{Z}$ και με $M_n(R)$ το δακτύλιο των $n \times n$ πινάκων με στοιχεία από το δακτύλιο R.

Δακτύλιοι, Ακέραιες Περιοχές, Σώματα

Συμβολίζουμε με 0_R το μηδενικό στοιχείο ενός δακτυλίου R, με 1_R το μοναδιαίο στοιχείο (μονάδα) του R (όταν αυτό υπάρχει) και με $U(R)$ το σύνολο των αντιστρέψιμων στοιχείων ενός δακτυλίου R με μονάδα. Υπενθυμίζουμε ότι ένα στοιχείο b ενός δακτυλίου με μονάδα R λέγεται *αριστερό* (αντίστοιχα, *δεξιό*) *αντίστροφο* του $a \in R$ αν $ba = 1_R$ (αντίστοιχα, $ab = 1_R$).

1. Να εξετάσετε αν το σύνολο $\mathbb{N}$ των φυσικών αριθμών, εφοδιασμένο με τις πράξεις πρόσθεσης $a \oplus b = \max\{a, b\}$ και πολλαπλασιασμού $a \otimes b = a + b$, αποτελεί δακτύλιο.

2. Δίνεται δακτύλιος R. Θεωρούμε το σύνολο $R^{\mathrm{op}} = R$, εφοδιασμένο με την πρόσθεση του R και πολλαπλασιασμό $\circ : R \times R \to R$ που ορίζεται θέτοντας $a \circ b = ba$ για $a, b \in R$ (όπου ab είναι το γινόμενο των a, b στο R).

(α) Δείξτε ότι το R^{op} αποτελεί δακτύλιο.
(β) Δείξτε ότι ο R έχει μονάδα (αντίστοιχα, είναι μεταθετικός δακτύλιος), αν και μόνο αν ο R^{op} έχει μονάδα (αντίστοιχα, είναι μεταθετικός δακτύλιος).
(γ) Δείξτε ότι ένα στοιχείο $a \in R$ έχει αριστερό (αντίστοιχα, δεξιό) αντίστροφο στο R αν και μόνο το a έχει δεξιό (αντίστοιχα, αριστερό) αντίστροφο στο R^{op}.
(δ) Δείξτε ότι το $a \in R$ είναι αριστερός (αντίστοιχα, δεξιός) μηδενοδιαιρέτης στο R αν και μόνο το a είναι δεξιός (αντίστοιχα, αριστερός) μηδενοδιαιρέτης στο R^{op}.

3. Δώστε παράδειγμα μη μεταθετικού δακτυλίου με μονάδα, ο οποίος έχει ακριβώς οκτώ στοιχεία.

4. Δίνεται δακτύλιος R και στοιχεία του a, b με $ab = ba$.

(α) Δείξτε ότι για κάθε θετικό ακέραιο n ισχύει η ταυτότητα

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k},$$

όπου $\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$ για $k \in \{0, 1, \ldots, n\}$.

(β) Συνάγετε ότι αν p είναι πρώτος αριθμός και ισχύει $pr = 0_R$ για κάθε $r \in R$, τότε $(a+b)^p = a^p + b^p$.

5. Δίνεται δακτύλιος R για τον οποίο ισχύει $a^2 = a$ για κάθε $a \in R$. Δείξτε ότι ο R είναι μεταθετικός και ότι $-a = a$ για κάθε $a \in R$.

6. Δίνεται δακτύλιος R με μονάδα.

(α) Δείξτε ότι ένα στοιχείο $a \in R$ είναι αντιστρέψιμο στοιχείο του R (δηλαδή ότι $a \in U(R)$) αν και μόνο αν το a έχει αριστερό αντίστροφο και δεξιό αντίστροφο στο R.

(β) Αν $a \in U(R)$, δείξτε ότι $a^{-1} \in U(R)$.

(γ) Αν $a, b \in U(R)$, δείξτε ότι $ab \in U(R)$.

7. Δίνεται δακτύλιος R με μονάδα και στοιχείο $a \in R$. Να εξετάσετε αν οι ακόλουθες προτάσεις είναι αληθείς:

(α) Αν το a έχει δεξιό αντίστροφο στο R, τότε το ίδιο ισχύει για το a^n για κάθε θετικό ακέραιο n.

(β) Αν το a έχει αριστερό αντίστροφο στο R, τότε το ίδιο ισχύει για το a^n για κάθε θετικό ακέραιο n.

8. Δίνεται δακτύλιος R με μονάδα και στοιχείο $a \in R$ το οποίο έχει δεξιό αντίστροφο στο R. Δείξτε ότι οι ακόλουθες συνθήκες είναι ισοδύναμες:

(i) Το a είναι αντιστρέψιμο στοιχείο του R.

(ii) Το a έχει μοναδικό δεξιό αντίστροφο στο R.

(iii) Το a έχει πεπερασμένου πλήθους δεξιούς αντιστρόφους στο R.

(iv) Το a δεν είναι αριστερός μηδενοδιαιρέτης στο R.

9. Δίνεται δακτύλιος R με μονάδα και $a, b \in R$. Αν το $1_R - ab$ είναι αντιστρέψιμο στοιχείο του R, δείξτε ότι το $1_R - ba$ είναι επίσης αντιστρέψιμο στοιχείο του R.

10. Δίνονται δακτύλιοι R, S και το ευθύ γινόμενο $R \times S$.

(α) Δείξτε ότι ο $R \times S$ είναι μεταθετικός δακτύλιος (αντίστοιχα, έχει μονάδα) αν και μόνο αν οι R και S είναι μεταθετικοί δακτύλιοι (αντίστοιχα, έχουν μονάδα).

(β) Αν οι R και S έχουν μονάδα, δείξτε ότι $U(R \times S) = U(R) \times U(S)$.

(γ) Πότε ο δακτύλιος $R \times S$ δεν έχει μηδενοδιαιρέτες;

11. Βρείτε:

(α) όλα τα αντιστρέψιμα στοιχεία του υποδακτυλίου $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ του $\mathbb{C}$,
(β) έναν υποδακτύλιο του $\mathbb{C}$ με μονάδα, διάφορο του $\mathbb{Z}$, ο οποίος να έχει ακριβώς δύο αντιστρέψιμα στοιχεία.

12. Δίνεται το σύνολο $R = \{a + 2b\sqrt{6} : a, b \in \mathbb{Z}\}$.

(α) Δείξτε ότι το R είναι υποδακτύλιος του $\mathbb{C}$ με μονάδα.
(β) Δείξτε ότι το R έχει άπειρο πλήθος αντιστρέψιμων στοιχείων.

13. Για φυσικούς αριθμούς m θέτουμε $m\mathbb{Z} = \{ma : a \in \mathbb{Z}\}$. Δείξτε ότι:

(α) Το σύνολο $m\mathbb{Z}$ είναι υποδακτύλιος του $\mathbb{Z}$ για κάθε φυσικό αριθμό m.
(β) Κάθε υποδακτύλιος του $\mathbb{Z}$ είναι της μορφής $m\mathbb{Z}$ για κάποιο φυσικό αριθμό m.

14. Δίνεται σώμα $\mathbb{F}$ και το υποσύνολο $R = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a, b \in \mathbb{F} \right\}$ του $M_2(\mathbb{F})$.

(α) Δείξτε ότι το R είναι υποδακτύλιος του $M_2(\mathbb{F})$ με μονάδα.
(β) Δείξτε ότι ο πίνακας

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

είναι αντιστρέψιμο στοιχείο του R αν και μόνο αν $a^2 + b^2 \neq 0$ στο $\mathbb{F}$.
(γ) Για ποια σώματα $\mathbb{F} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_3, \mathbb{Z}_5\}$ είναι ο δακτύλιος R σώμα;
(δ) Για ποια σώματα $\mathbb{F} = \mathbb{Z}_p$ είναι ο δακτύλιος R σώμα;

15. Δίνεται δακτύλιος R, στοιχείο $\alpha \in R$ και το σύνολο $S = \{x \in R : \alpha x = x\alpha\}$.

(α) Δείξτε ότι το S είναι υποδακτύλιος του R.
(β) Έστω ότι $R = M_2(\mathbb{F})$, όπου $\mathbb{F}$ είναι σώμα, και $\alpha = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Δείξτε ότι ο δακτύλιος S είναι μεταθετικός και βρείτε όλα τα αντιστρέψιμα στοιχεία και τους μηδενοδιαιρέτες του. Είναι το S ακέραια περιοχή;
(γ) Δώστε παράδειγμα δακτυλίου R και στοιχείου $\alpha \in R$ για τα οποία το S είναι γνήσιος και μη μεταθετικός υποδακτύλιος του R.

16. Συμβολίζουμε με $C(R)$ το σύνολο των στοιχείων x ενός δακτυλίου R για τα οποία ισχύει $\alpha x = x\alpha$ για κάθε $\alpha \in R$ (το $C(R)$ λέγεται *κέντρο* του R).

(α) Δείξτε ότι το $C(R)$ είναι μεταθετικός υποδακτύλιος του R.
(β) Δείξτε ότι για τυχαίους δακτυλίους R και S ισχύει $C(R \times S) = C(R) \times C(S)$.
(γ) Δώστε παράδειγμα μη μηδενικού δακτυλίου R με $C(R) = \{0_R\}$.
(δ) Δώστε παράδειγμα δακτυλίου R με τουλάχιστον τρία στοιχεία, για τον οποίο το $C(R)$ έχει ακριβώς δύο στοιχεία.
(ε) Δώστε παράδειγμα δακτυλίου R με τουλάχιστον τρία στοιχεία, για τον οποίο ισχύει $xy \neq yx$ για όλα τα $x, y \in R \setminus \{0_R\}$ με $x \neq y$.

17. Δίνεται ακέραια περιοχή R.

(α) Βρείτε όλα τα στοιχεία $a \in U(R)$ για τα οποία ισχύει $a^{-1} = a$.
(β) Έστω ότι το σύνολο $U(R)$ είναι πεπερασμένο. Δείξτε ότι το $U(R)$ έχει περιττό πλήθος στοιχείων αν και μόνο ισχύει $-x = x$ για κάθε $x \in R$.

18. Έστω δακτύλιος R και έστω S το σύνολο των μη μηδενικών στοιχείων του R τα οποία δεν είναι αριστεροί μηδενοδιαιρέτες στο R. Δείξτε ότι $ab \in S$ για όλα τα $a, b \in S$.

19. Δίνεται πεπερασμένος δακτύλιος R με μονάδα. Δείξτε ότι κάθε μη μηδενικός μη μηδενοδιαιρέτης στο R είναι αντιστρέψιμο στοιχείο του R.

20. Δίνεται δακτύλιος R.

(α) Αν το b είναι αριστερός μηδενοδιαιρέτης στο R και $a \in R$, δείξτε ότι $ab = 0_R$ ή το ab είναι αριστερός μηδενοδιαιρέτης στο R.
(β) Αν το b είναι αριστερός μηδενοδιαιρέτης στο R και το $a \in R \setminus \{0_R\}$ δεν είναι, δείξτε ότι το ab είναι επίσης αριστερός μηδενοδιαιρέτης στο R.
(γ) Αν το σύνολο των αριστερών μηδενοδιαιρετών του R είναι μη κενό και πεπερα-σμένο, δείξτε ότι ο R είναι πεπερασμένος δακτύλιος.

21. Δίνεται πεπερασμένος δακτύλιος R. Δείξτε ότι:

(α) Για κάθε $x \in R$ υπάρχουν ακέραιοι $1 \leq n < m$ τέτοιοι ώστε $x^n = x^m$.
(β) Υπάρχουν ακέραιοι $1 \leq n < m$ τέτοιοι ώστε να ισχύει $x^n = x^m$ για κάθε $x \in R$.

22. Ένα στοιχείο a ενός δακτυλίου R λέγεται *μηδενοδύναμο* αν $a^n = 0_R$ για κάποιο θετικό ακέραιο n.

(α) Αν a, b είναι μηδενοδύναμα στοιχεία του R και $ab = ba$, δείξτε ότι το $a + b$ είναι επίσης μηδενοδύναμο στοιχείο του R.

(β) Αν a, b είναι στοιχεία του R ένα τουλάχιστον από τα οποία είναι μηδενοδύναμο και $ab = ba$, δείξτε ότι το ab είναι επίσης μηδενοδύναμο στοιχείο του R.

(γ) Έστω ότι ο R είναι δακτύλιος με μονάδα. Αν $a \in U(R)$, το b είναι μηδενοδύναμο στοιχείο του R και $ab = ba$, δείξτε ότι $a+b \in U(R)$.

(δ) Έστω ότι ο R είναι δακτύλιος με μονάδα. Αν b είναι μηδενοδύναμο στοιχείο του R, δείξτε ότι $1_R + b \in U(R)$.

(ε) Ποια από τα (α), (β) και (γ) ισχύουν χωρίς την υπόθεση $ab = ba$;

23. Δίνεται σώμα $\mathbb{F}$.

(α) Έστω $R = M_n(\mathbb{F})$ και έστω 1_R ο $n \times n$ ταυτοτικός πίνακας με στοιχεία από το $\mathbb{F}$. Αν για τα $A, B \in R$ ισχύει $A^2 = B^2$ και $\lambda AB + \mu BA = 1_R$ για κάποια $\lambda, \mu \in \mathbb{F}$ με $\lambda \neq \mu$, δείξτε ότι $AB = BA$ και ότι $A, B \in U(R)$.

(β) Για ποια γενικότερη κατηγορία δακτυλίων R ισχύει το (α);

24. Δίνεται σώμα $\mathbb{F}$ με q στοιχεία, όπου q είναι περιττός αριθμός.

(α) Δείξτε ότι δεν υπάρχει μη μηδενικό στοιχείο $x \in \mathbb{F}$, τέτοιο ώστε $-x = x$.

(β) Αν $q \equiv 1 \pmod 4$, δείξτε ότι υπάρχει $x \in \mathbb{F}$, τέτοιο ώστε $x^2 = -1$.

Πολυωνυμικοί Δακτύλιοι

Συμβολίζουμε με $R[x]$ το δακτύλιο των πολυωνύμων στη μεταβλητή x με συντελεστές από το δακτύλιο R και με $\deg(f(x))$ το βαθμό ενός μη μηδενικού πολυωνύμου $f(x) \in R[x]$.

25. Δίνεται δακτύλιος R.

(α) Αν ο R δεν έχει μηδενοδιαιρέτες, δείξτε ότι ούτε ο $R[x]$ έχει μηδενοδιαιρέτες και ότι για τυχαία μη μηδενικά πολυώνυμα $f(x), g(x) \in R[x]$ ισχύει

$$\deg(f(x)g(x)) \;=\; \deg(f(x)) \;+\; \deg(g(x)).$$

(β) Έστω ότι ο R δεν έχει μηδενοδιαιρέτες. Αν ο δακτύλιος $R[x]$ έχει μονάδα, δείξτε ότι η μονάδα αυτή είναι σταθερό πολυώνυμο το οποίο είναι μονάδα του R.

(γ) Δείξτε ότι ο δακτύλιος $R[x]$ δεν είναι σώμα.

26. Να εξετάσετε αν υπάρχουν:

(α) πολυώνυμα $p(x), q(x) \in \mathbb{C}[x]$ τέτοια ώστε $(p(x))^{80} \cdot (q(x))^{64} = (x^{10} + x^5 + 1)^{2012}$.

(β) πολυώνυμα $p(x), q(x) \in \mathbb{C}[x]$ βαθμού $n \geq 1$, τέτοια ώστε $(p(x))^2 - (q(x))^2 = 1 + x + x^2 + \cdots + x^{n-1}$.

27. Δίνεται σώμα $\mathbb{F}$ στο οποίο $2 \neq 0$. Βρείτε όλα τα μη μηδενικά πολυώνυμα $p(x) \in \mathbb{F}[x]$ για τα οποία $p(x^2) = (p(x))^2$.

28. Δίνεται σώμα $\mathbb{F}$ και μονικό πολυώνυμο $p(x) \in \mathbb{F}[x]$ άρτιου βαθμού $2n \geq 2$.

(α) Αν ισχύει $-1 \neq 1$ στο $\mathbb{F}$, δείξτε ότι υπάρχουν πολυώνυμα $q(x), r(x) \in \mathbb{F}[x]$ τέτοια ώστε $p(x) = (q(x))^2 + r(x)$ και $\deg(r(x)) < n$.
(β) Ισχύει το (α) χωρίς την υπόθεση $-1 \neq 1$;

29. Δίνεται δακτύλιος R. Για $p(x) \in R[x]$ θέτουμε $\Delta(p(x)) = p(x) - p(x-1)$ και $\Delta^m(p(x)) = \Delta(\Delta^{m-1}(p(x)))$ για $m \geq 2$. Για παράδειγμα, έχουμε $\Delta^2(p(x)) = p(x) - 2p(x-1) + p(x-2)$.

(α) Αν $\deg(p(x)) \leq n$, δείξτε ότι $\deg(\Delta(p(x))) \leq n-1$.
(β) Δείξτε ότι

$$\Delta^m(p(x)) \;=\; \sum_{k=0}^{m} (-1)^k \binom{m}{k} p(x-k)$$

για κάθε θετικό ακέραιο m.
(γ) Αν $\deg(p(x)) \leq n$, δείξτε ότι $\sum_{k=0}^{n+1} (-1)^k \binom{n+1}{k} p(x-k) = 0$.
(δ) Δείξτε ότι

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} (x-k)^n \;=\; n!$$

για κάθε $n \in \mathbb{N}$.

30. Δίνεται μεταθετικός δακτύλιος R και $\alpha \in R$. Για $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ θέτουμε

$$\varphi_\alpha(f(x)) = f(\alpha) \;:=\; a_0 + a_1\alpha + \cdots + a_n\alpha^n \in R.$$

(α) Δείξτε ότι $\varphi_\alpha(f(x)+g(x)) = \varphi_\alpha(f(x)) + \varphi_\alpha(g(x))$ για όλα τα $f(x), g(x) \in R[x]$.
(β) Δείξτε ότι $\varphi_\alpha(f(x)\cdot g(x)) = \varphi_\alpha(f(x))\cdot\varphi_\alpha(g(x))$ για όλα τα $f(x), g(x) \in R[x]$.
(γ) Έστω $\psi(f(x)) \in R$ το άθροισμα των συντελεστών του $f(x) \in R[x]$. Δείξτε ότι $\psi(f(x)+g(x)) = \psi(f(x)) + \psi(g(x))$ και ότι $\psi(f(x)g(x)) = \psi(f(x))\psi(g(x))$ για όλα τα $f(x), g(x) \in R[x]$.
(δ) Υπολογίστε το άθροισμα των συντελεστών του $(1-3x+x^2)^n \in \mathbb{Z}[x]$ για κάθε θετικό ακέραιο n.

31. Δίνεται πολυώνυμο $p(x) \in \mathbb{C}[x]$ βαθμού n.

(α) Αν $p(m) \in \mathbb{Z}$ για κάθε $m \in \{0, 1, \ldots, n\}$, δείξτε ότι $p(m) \in \mathbb{Z}$ για κάθε $m \in \mathbb{Z}$.
(β) Αν $p(m) \in \mathbb{Z}$ για κάθε $m \in \{0, 1, 2^2, \ldots, n^2\}$, δείξτε ότι $p(m) \in \mathbb{Z}$ για κάθε τετράγωνο ακεραίου m.

(γ) Δώστε παράδειγμα πολυωνύμου $p(x)$ το οποίο λαμβάνει ακέραια τιμή σε κάθε τεράγωνο ακεραίου, αλλά όχι σε κάθε ακέραιο αριθμό.

32. Δίνεται θετικός ακέραιος k. Προσδιορίστε τον ελάχιστο θετικό ακέραιο $n = n(k)$ για τον οποίο υπάρχει μονικό πολυώνυμο $p(x) \in \mathbb{Z}[x]$ βαθμού n, τέτοιο ώστε το $p(m)$ να διαιρείται με το k για κάθε $m \in \mathbb{Z}$. Υπολογίστε επακριβώς το $n(k)$ για $k = 1000$.

33. Δίνεται μεταθετικός δακτύλιος R με μονάδα και πολυώνυμο $f(x) \in R[x]$.

(α) Αν το $f(x)$ είναι αντιστρέψιμο στοιχείο του $R[x]$, δείξτε ότι το $f(\alpha)$ είναι αντιστρέψιμο στοιχείο του R για κάθε $\alpha \in R$.
(β) Συνάγετε ότι το $1 + 5x + 3x^2$ δεν είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}_6[x]$.
(γ) Δώστε παράδειγμα μεταθετικού δακτυλίου R με μονάδα και μη αντιστρέψιμου πολυωνύμου $f(x) \in R[x]$ για το οποίο $f(\alpha)$ είναι αντιστρέψιμο στοιχείο του R για κάθε $\alpha \in R$.

34. Δίνεται μεταθετικός δακτύλιος R με μονάδα.

(α) Δείξτε ότι το πολυώνυμο $1_R + rx$ είναι αντιστρέψιμο στοιχείο του $R[x]$ αν και μόνο αν το r είναι μηδενοδύναμο στοιχείο του R.
(β) Γενικότερα, δείξτε ότι το πολυώνυμο $a + bx$ είναι αντιστρέψιμο στοιχείο του $R[x]$ αν και μόνο αν $a \in U(R)$ και το b είναι μηδενοδύναμο στοιχείο του R.
(γ) Συνάγετε ότι αν ο m διαιρείται με το τετράγωνο κάποιου πρώτου αριθμού, τότε ο δακτύλιος $\mathbb{Z}_m[x]$ έχει αντιστρέψιμα στοιχεία πρώτου βαθμού.

35. Να εξετάσετε αν ο δακτύλιος $\mathbb{Z}_m[x]$ έχει άπειρο πλήθος αντιστρέψιμων στοιχείων:

(α) για $m = 6$,
(β) για $m = 12$.

36. Δίνεται μεταθετικός δακτύλιος R με μονάδα. Για $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ ορίζουμε την παράγωγο

$$f'(x) \;=\; a_1 + 2a_2x + \cdots + na_nx^{n-1} \in R[x].$$

(α) Δείξτε ότι $(f(x)+g(x))' = f'(x)+g'(x)$ για όλα τα $f(x), g(x) \in R[x]$.
(β) Δείξτε ότι $(f(x)g(x))' = f'(x)g(x)+f(x)g'(x)$ για όλα τα $f(x), g(x) \in R[x]$.

37. Βρείτε όλα τα πολυώνυμα $p(x) \in \mathbb{C}[x]$ για τα οποία

$$(p(x))^2 - (p(y))^2 = p(x-y)p(x+y)$$

στο $\mathbb{C}[x, y]$.

38. Δείξτε ότι το πολυώνυμο $(x-1)^n q(x)$ έχει τουλάχιστον $n+1$ μη μηδενικούς συντελεστές για κάθε μη μηδενικό πολυώνυμο $q(x) \in \mathbb{C}[x]$.

Διαιρετότητα και Παραγοντοποίηση Πολυωνύμων

39. Δείξτε ότι το πολυώνυμο $x^{48} + x^{40} + x^{32} + x^{24} + x^{16} + x^8 + 1$ διαιρείται με το $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ στο $\mathbb{Z}[x]$.

40. Δίνεται μεταθετικός δακτύλιος R και πολυώνυμα $f(x), p(x), q(x) \in R[x]$.

(α) Δείξτε ότι το $f(p(x)) - f(q(x))$ διαιρείται με το $p(x) - q(x)$ στο $R[x]$.
(β) Αν $p(q(x)) = q(p(x))$, δείξτε το $p(p(x)) - q(q(x))$ διαιρείται με το $p(x) - q(x)$ στο $R[x]$.

41. Υπολογίστε το μέγιστο κοινό διαιρέτη των $x^6 - x^4 + 2x^2 - 2$ και $x^3 + x^2 + x + 1$:

(α) στο $\mathbb{Z}[x]$,
(β) στο $\mathbb{Z}_2[x]$,
(γ) στο $\mathbb{Z}_3[x]$.

42. Δίνονται θετικοί ακέραιοι m, n και ακέραια περιοχή R.

(α) Δείξτε ότι $\mu\kappa\delta(x^m - 1, x^n - 1) = x^d - 1$ στο $R[x]$, όπου $d = \mu\kappa\delta(m, n)$.
(β) Για ποιους ακεραίους m, n το $x^m - 1$ διαιρείται με το $x^n - 1$ στο $R[x]$;
(γ) Δείξτε ότι $\mu\kappa\delta(f_m(x), f_n(x)) = f_d(x)$ στο $R[x]$, όπου $d = \mu\kappa\delta(m, n)$ και $f_k(x) = 1 + x + x^2 + \cdots + x^{k-1}$ για $k \geq 1$.

43. Δίνονται σώμα $\mathbb{K}$, υπόσωμα $\mathbb{F} \subseteq \mathbb{K}$ αυτού και πολυώνυμα $f(x), g(x) \in \mathbb{F}[x]$ με $g(x) \neq 0$.

(α) Δείξτε ότι το πηλίκο και το υπόλοιπο της Ευκλείδειας διαίρεσης του $f(x)$ με το $g(x)$ στο $\mathbb{K}[x]$ είναι ίσα, αντίστοιχα, με το πηλίκο και το υπόλοιπο της Ευκλείδειας διαίρεσης του $f(x)$ με το $g(x)$ στο $\mathbb{F}[x]$.
(β) Συνάγετε ότι το $f(x)$ διαιρείται με το $g(x)$ στο $\mathbb{K}[x]$ αν και μόνο αν το $f(x)$ διαιρείται με το $g(x)$ στο $\mathbb{F}[x]$.
(γ) Δείξτε ότι ο μέγιστος κοινός διαιρέτης των $f(x)$ και $g(x)$ στο $\mathbb{K}[x]$ είναι ίσος με το μέγιστο κοινό διαιρέτη των $f(x)$ και $g(x)$ στο $\mathbb{F}[x]$.
(δ) Έστω ότι το $g(x)$ είναι ανάγωγο στο $\mathbb{F}[x]$. Αν τα $f(x)$ και $g(x)$ έχουν τουλάχιστον μία κοινή ρίζα στο $\mathbb{K}$, δείξτε ότι το $f(x)$ διαιρείται με το $g(x)$ στο $\mathbb{F}[x]$.

44. Αναλύστε το πολυώνυμο $f(x) = x + x^2 + \cdots + x^{p-1} \in \mathbb{Z}_p[x]$ σε γινόμενο ανάγωγων πολυωνύμων του $\mathbb{Z}_p[x]$ για τυχαίο πρώτο αριθμό p.

45. Δίνεται πρώτος αριθμός p και το πολυώνυμο $f(x) = 1 + x + \cdots + x^{p-1} \in \mathbb{Z}_p[x]$.

(α) Βρείτε όλες τις ρίζες του $f(x)$ στο $\mathbb{Z}_p$.
(β) Αναλύστε το $f(x)$ σε γινόμενο ανάγωγων πολυωνύμων του $\mathbb{Z}_p[x]$.

46. Θεωρούμε το πολυώνυμο $f(x) = (x^2 + x + 1)^p - (x^2 + x + 1) \in \mathbb{Z}_p[x]$.

(α) Δείξτε ότι υπάρχει πολυώνυμο $q(x) \in \mathbb{Z}_p[x]$ τέτοιο ώστε $f(x) = (x^p - x)q(x)$. Ποιος είναι ο βαθμός του $q(x)$;
(β) Υπολογίστε επακριβώς το πολυώνυμο $q(x)$.

47. Δίνονται πολυώνυμα $f(x), g(x) \in \mathbb{Z}[x]$ για τα οποία το $f(n)$ είναι ακέραιο πολλαπλάσιο του $g(n)$ για κάθε $n \in \mathbb{Z}$.

(α) Δείξτε ότι το $f(x)$ διαιρείται με το $g(x)$ στο $\mathbb{Q}[x]$.
(β) Δώστε παράδειγμα τέτοιων πολυωνύμων στο οποίο το $f(x)$ δε διαιρείται με το $g(x)$ στο $\mathbb{Z}[x]$.

48. Δίνονται μη μηδενικά πολυώνυμα $f(x), g(x) \in \mathbb{Z}[x]$. Δείξτε ότι τα $f(x), g(x)$ δεν έχουν κοινή μιγαδική ρίζα αν και μόνο αν υπάρχει $d \in \mathbb{Z}$ τέτοιο ώστε $\mu\kappa\delta(f(n), g(n)) \leq d$ για κάθε $n \in \mathbb{Z}$.

49. Δίνεται ακέραια περιοχή R με άπειρο πλήθος στοιχείων και πολυώνυμο $f(x, y) \in R[x, y]$.

(α) Αν ισύχει $f(a, a) = 0_R$ για κάθε $a \in R$, δείξτε ότι υπάρχει πολυώνυμο $q(x, y) \in R[x, y]$ τέτοιο ώστε $f(x, y) = (x - y)q(x, y)$.
(β) Έστω ότι $R = \mathbb{R}$. Αν ισύχει $f(a, b) = 0$ για κάθε $(a, b) \in \mathbb{R}^2$ με $a^2 + b^2 = 1$, δείξτε ότι υπάρχει πολυώνυμο $q(x, y) \in \mathbb{R}[x, y]$ τέτοιο ώστε $f(x, y) = (x^2 + y^2 - 1)q(x, y)$.

50. Δίνονται τα πολυώνυμα $f_n(q) = (q - 1)(q^2 - 1) \cdots (q^n - 1)$ για $n \in \mathbb{N}$, όπου $f_0(q) = 1$. Για $0 \leq k \leq n$ θέτουμε

$$\binom{n}{k}_q = \frac{f_n(q)}{f_k(q)\, f_{n-k}(q)}.$$

(α) Αν $1 \leq k \leq n$, δείξτε ότι $\binom{n}{k}_q = \binom{n-1}{k}_q + q^{n-k}\binom{n-1}{k-1}_q$.
(β) Συνάγετε ότι το $f_n(q)$ διαιρείται με το $f_k(q)f_{n-k}(q)$ στο $\mathbb{Z}[q]$ και ότι το πηλίκο $\binom{n}{k}_q$ είναι πολυώνυμο βαθμού $k(n-k)$ με μη αρνητικούς ακέραιους συντελεστές.

51. Δίνεται ακέραια περιοχή R. Ένα πολυώνυμο $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ βαθμού n έχει *παλινδρομικούς συντελεστές* αν $a_i = a_{n-i}$ για $0 \leq i \leq n$.

(α) Δείξτε ότι ένα πολυώνυμο $f(x) \in R[x]$ βαθμού n έχει παλινδρομικούς συντελεστές αν και μόνο αν $x^n f(1/x) = f(x)$ (η ισότητα αυτή έχει νόημα π.χ στο σώμα κλασμάτων του $R[x]$).
(β) Δείξτε ότι το γινόμενο δύο πολυωνύμων με παλινδρομικούς συντελεστές είναι επίσης πολυώνυμο με παλινδρομικούς συντελεστές.
(γ) Δείξτε ότι τα πολυώνυμα $f_n(q)$ της Άσκησης 50 έχουν παλινδρομικούς συντελεστές.

52. Δίνονται τα πολυώνυμα $f(x, y, z) = (x + y + z)^9 - x^9 - y^9 - z^9$ και $g(x, y, z) = (x + y + z)^3 - x^3 - y^3 - z^3$.

(α) Εκφράστε το $g(x, y, z)$ ως γινόμενο ανάγωγων πολυωνύμων του $\mathbb{Q}[x, y, z]$.
(β) Δείξτε ότι το $f(x, y, z)$ διαιρείται με το $g(x, y, z)$ στο $\mathbb{Q}[x, y, z]$.

53. Αναλύστε το $x^4 + 1$ σε γινόμενο ανάγωγων πολυωνύμων:

(α) στο $\mathbb{R}[x]$,
(β) στο $\mathbb{Q}[x]$,
(γ) στο $\mathbb{Z}_{17}[x]$,
(δ) επί ενός δακτυλίου R με $-1_R = 1_R$.

54. Δείξτε ότι:

(α) Το πολυώνυμο $x^4 + x^3 + x^2 - 2x + 1$ είναι ανάγωγο στο $\mathbb{Z}[x]$.
(β) Το πολυώνυμο $x^4 + x^3 + x + 3$ είναι ανάγωγο στο $\mathbb{Z}_5[x]$.

55. Βρείτε όλα τα ανάγωγα πολυώνυμα τετάρτου βαθμού στο $\mathbb{Z}_2[x]$.

56. Δίνονται διαφορετικοί ανά δύο ακέραιοι αριθμοί $a_1, a_2, \ldots, a_n$.

(α) Δείξτε ότι το $f(x) = (x - a_1)(x - a_2) \cdots (x - a_n) - 1$ είναι ανάγωγο στο $\mathbb{Z}[x]$.
(β) Δείξτε ότι το $g(x) = (x-a_1)^2(x-a_2)^2 \cdots (x-a_n)^2 + 1$ είναι ανάγωγο στο $\mathbb{Z}[x]$.
(γ) Ισχύει πάντοτε το ίδιο για το $h(x) = (x-a_1)(x-a_2) \cdots (x-a_n) + 1$;

57. Δίνεται σώμα $\mathbb{F}$.

(α) Δείξτε ότι υπάρχουν άπειρου πλήθους ανάγωγα πολυώνυμα στο $\mathbb{F}[x]$.
(β) Έστω ότι το $\mathbb{F}$ είναι πεπερασμένο. Δείξτε ότι για κάθε $n \in \mathbb{N}$ υπάρχει ανάγωγο πολυώνυμο στο $\mathbb{F}[x]$ βαθμού μεγαλύτερου του n.

(γ) Ισχύει το (β) χωρίς την υπόθεση ότι το $\mathbb{F}$ είναι πεπερασμένο;

58. Δίνονται πρώτος αριθμός p και το πολυώνυμο $f_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$. Για $n \in \mathbb{N}$, δείξτε ότι οι ακόλουθες συνθήκες είναι ισοδύναμες:

(i) το $f_p(x)$ διαιρεί το $f_p(x^n)$ στο $\mathbb{Z}[x]$,
(ii) το $f_p(x)$ διαιρεί το $f_p(x^n)$ στο $\mathbb{C}[x]$,
(iii) το n δε διαιρείται με το p.

59. Δίνεται φυσικός αριθμός n. Βρείτε:

(α) Όλα τα πολυώνυμα $p(x) \in \mathbb{C}[x]$ με $p(0) = 0$ τα οποία επαληθεύουν την ισότητα $p(x^4 + 1) = (p(x))^4 + 1$ στο $\mathbb{C}[x]$.
(β) Όλα τα πολυώνυμα $p(x) \in \mathbb{C}[x]$ βαθμού μικρότερου ή ίσου του n για τα οποία ισχύει $p(k) = 1/(k + 1)$ για $k \in \{0, 1, \ldots, n\}$.

60. Δίνεται πολυώνυμο $p(x) \in \mathbb{C}[x]$ βαθμού μικρότερου ή ίσου του n για το οποίο ισχύει $p(k) = 1/\binom{n+1}{k}$ για $k \in \{0, 1, \ldots, n\}$. Υπολογίστε το $p(n + 1)$.

61. Δίνεται ακέραια περιοχή R, πολυώνυμο $f(x) \in R[x]$ και $a \in R$. Λέμε ότι το a είναι *διπλή ρίζα* του $f(x)$ αν το $f(x)$ διαιρείται με το $(x - a)^2$ στο $R[x]$. Λέμε ότι το a είναι *ρίζα πολλαπλότητας* m του $f(x)$ αν το $f(x)$ διαιρείται με το $(x - a)^m$, αλλά όχι με το $(x - a)^{m+1}$, στο $R[x]$.

(α) Δείξτε ότι το a είναι διπλή ρίζα του $f(x)$ αν και μόνο αν $f(a) = f'(a) = 0_R$, όπου $f'(x)$ είναι η παράγωγος του $f(x)$ (Άσκηση 36).
(β) Έστω ότι $R = \mathbb{C}$ (ή οποιοδήποτε σώμα χαρακτηριστικής μηδέν). Δείξτε ότι αν a είναι ρίζα πολλαπλότητας m του $f(x)$, τότε το a είναι ρίζα πολλαπλότητας $m - 1$ του $f'(x)$.
(γ) Έστω ότι $R = \mathbb{Q}$ (ή οποιοδήποτε σώμα χαρακτηριστικής μηδέν) και ότι το R είναι υπόσωμα ενός σώματος $\mathbb{K}$. Αν $g(x) \in R[x]$ είναι ανάγωγο πολυώνυμο στο $R[x]$, δείξτε ότι το $g(x)$ δεν έχει διπλές ρίζες στο $\mathbb{K}$.

62. Δίνεται ανάγωγο πολυώνυμο τρίτου βαθμού $g(x) \in \mathbb{Q}[x]$. Δείξτε ότι αν r_1, r_2, r_3 είναι οι ρίζες του $g(x)$ στο $\mathbb{C}$, τότε κανένας από τους αριθμούς $r_1 - r_2$, $r_1 - r_3$ και $r_2 - r_3$ δεν είναι ρητός.

63. Δίνεται πολυώνυμο $f(x) \in \mathbb{R}[x]$ για το οποίο ισχύει $f(x) \geq 0$ για κάθε $x \in \mathbb{R}$.

(α) Δείξτε ότι το $f(x)$ μπορεί να γραφεί ως το γινόμενο ενός θετικού αριθμού και πολυωνύμων της μορφής $(x - a)^2 + b^2$, με $a, b \in \mathbb{R}$.
(β) Συνάγετε ότι υπάρχουν πολυώνυμα $p(x), q(x) \in \mathbb{R}[x]$ τέτοια ώστε $f(x) = (p(x))^2 + (q(x))^2$.

64. Δίνεται πολυώνυμο $p(x) = a_0+a_1x+\cdots+a_nx^n \in \mathbb{R}[x]$ με μη αρνητικούς συντελεστές για τους οποίους ισχύει $a_0 = 1$ και $a_i = a_{n-i}$ για $0 \leq i \leq n$. Υποθέτουμε ότι κάθε ρίζα του $p(x)$ είναι πραγματικός αριθμός.

(α) Δείξτε ότι το $p(x)$ μπορεί να γραφεί στη μορφή

$$p(x) \;=\; (1+x)^m \prod_{i=1}^{r} (x+b_i)(x+\frac{1}{b_i})$$

για κάποια $m, r \in \mathbb{N}$ και θετικούς πραγματικούς αριθμούς $b_1, b_2, \ldots, b_r$ διάφορους του 1.

(β) Συνάγετε ότι $(-1)^{\lfloor n/2 \rfloor} \sum_{i=0}^{n} (-1)^i a_i \geq 0$.

(γ) Συνάγετε ότι ισχύει $p(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} \gamma_i x^i (1+x)^{n-2i}$ για κάποιους μη αρνητικούς πραγματικούς αριθμούς $\gamma_0, \gamma_1, \ldots, \gamma_{\lfloor n/2 \rfloor}$.

65. Δίνονται ακέραιοι $1 \leq k \leq n$ και πολυώνυμο $p(x) \in \mathbb{C}[x]$ της μορφής $p(x) = a_0 + a_1x + \cdots + a_{n-k}x^{n-k} + x^n \in \mathbb{C}[x]$, διάφορο του x^n. Δείξτε ότι το $p(x)$ έχει τουλάχιστον k διακεκριμένες ρίζες στο $\mathbb{C}$.

66. Δίνεται θετικός ακέραιος n. Βρείτε το ελάχιστο δυνατό πλήθος στοιχείων του συνόλου $\{x \in \mathbb{C} : \; p(x) \in \{0,1\}\}$, όπου $p(x) \in \mathbb{C}[x]$ είναι πολυώνυμο βαθμού n.

67. Δίνονται πολυώνυμα $p(x), q(x) \in \mathbb{R}[x]$ τέτοια ώστε $p(x) \in \mathbb{Z} \Leftrightarrow q(x) \in \mathbb{Z}$, για $x \in \mathbb{R}$. Δείξτε ότι ένα τουλάχιστον από τα πολυώνυμα $p(x) - q(x)$ και $p(x) + q(x)$ είναι σταθερό.

68. Βρείτε το μέγιστο θετικό ακέραιο n για τον οποίο υπάρχει πολυώνυμο $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ βαθμού n με τις εξής ιδιότητες:

(i) $\{a_0, a_1, \ldots, a_n\} = \{0, 1, \ldots, n\}$,

(ii) το $f(x)$ αναλύεται σε γινόμενο πρωτοβάθμιων πολυωνύμων στο $\mathbb{Z}[x]$ (ισοδύναμα, κάθε μιγαδική ρίζα του $f(x)$ είναι ρητός αριθμός).

69. Βρείτε όλα τα πολυώνυμα $p(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{R}[x]$ με $a_i \in \{-1, 1\}$ για $1 \leq i \leq n$ κάθε μιγαδική ρίζα των οποίων είναι πραγματικός αριθμός.

Ομομορφισμοί, Ιδεώδη και Δακτύλιος Πηλίκο

Υπενθυμίζουμε ότι ένας ομομορφισμός δακτυλίων $\varphi : R \to R$ λέγεται *ενδομορφισμός* του R. Συμβολίζουμε με $T_n(R)$ το δακτύλιο των άνω τριγωνικών $n \times n$ πινάκων με στοιχεία από το R.

70. Να εξετάσετε αν οι παρακάτω απεικονίσεις είναι ομομορφισμοί δακτυλίων:

(α) $\varphi, \psi : M_2(\mathbb{Z}) \to \mathbb{Z}$ με

$$\varphi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a, \quad \psi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

για $a, b, c, d \in \mathbb{Z}$,

(β) ο περιορισμός της φ στον υποδακτύλιο $T_2(\mathbb{Z})$ του $M_2(\mathbb{Z})$,

(γ) $\sigma : \mathbb{Z}[i] \to \mathbb{Z}_5$ με $\sigma(a + bi) = \bar{a} + \bar{b}$, για $a, b \in \mathbb{Z}$,

(δ) $\tau : \mathbb{Z}[i] \to \mathbb{Z}_5$ με $\tau(a + bi) = \bar{a} + 2\bar{b}$, για $a, b \in \mathbb{Z}$,

(ε) $\rho : \mathbb{Z}[x] \to \mathbb{Z}$ με $\rho(f(x)) = f'(0)$, για $f(x) \in \mathbb{Z}[x]$.

71. Δίνεται το σύνολο $R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$.

(α) Δείξτε ότι το R είναι υποδακτύλιος του $M_2(\mathbb{Z})$.

(β) Βρείτε όλους τους ομομορφισμούς δακτυλίων $\varphi : R \to \mathbb{Z} \times \mathbb{Z}$.

72. Δίνεται το σύνολο $R = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$.

(α) Δείξτε ότι το R είναι υποδακτύλιος του $M_2(\mathbb{Z})$. Είναι ακέραια περιοχή;

(β) Βρείτε όλους τους ομομορφισμούς δακτυλίων $\varphi : R \to \mathbb{Z}$.

(γ) Δείξτε ότι ο R είναι ισόμορφος με έναν υποδακτύλιο του $\mathbb{Z} \times \mathbb{Z}$.

(δ) Βρείτα όλα τα στοιχεία $x \in R$ με $x^2 = x$. Είναι ο R ισόμορφός με τον $\mathbb{Z} \times \mathbb{Z}$;

73. Δίνεται δακτύλιος R με μονάδα.

(α) Δείξτε ότι για κάθε $\alpha \in U(R)$, η απεικόνιση $\varphi : R \to R$ με $\varphi(x) = \alpha x \alpha^{-1}$ για $x \in R$ είναι αυτομορφισμός του R.

(β) Δείξτε ότι η απεικόνιση $\varphi : M_2(R) \to M_2(R)$ με

$$\varphi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & c \\ b & a \end{pmatrix}$$

για $a, b, c, d \in R$ είναι αυτομορφισμός του $M_2(R)$. Ισχύει το ίδιο χωρίς την υπόθεση ότι ο R έχει μονάδα;

(γ) Συνάγετε ότι ο δακτύλιος των άνω τριγωνικών 2×2 πινάκων με στοιχεία από το R είναι ισόμορφος με το δακτύλιο των κάτω τριγωνικών 2×2 πινάκων με στοιχεία από το R.

74. Δίνεται ακέραια περιοχή R. Βρείτε:

(α) όλους τους ομομορφισμούς δακτυλίων $\varphi : \mathbb{Z} \to R$,

(β) όλους τους αυτομορφισμούς του δακτυλίου $\mathbb{Z}$,

(γ) όλους τους επιμορφισμούς δακτυλίων $\varphi : \mathbb{Z} \to \mathbb{Z}_p$, όπου p είναι πρώτος αριθμός,

(δ) όλους τους μονομορφισμούς δακτυλίων $\varphi : \mathbb{Z} \to \mathbb{Z}[x]$.

75. Δίνεται ομομορφισμός δακτυλίων $\varphi : R \to S$. Για $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ θέτουμε

$$\tilde{\varphi}(f(x)) \;=\; \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n \in S[x].$$

(α) Δείξτε ότι η απεικόνιση $\tilde{\varphi} : R[x] \to S[x]$ είναι ομομορφισμός δακτυλίων.
(β) Δείξτε ότι ο ομομορφισμός $\tilde{\varphi}$ είναι μονομορφισμός (αντίστοιχα, επιμορφισμός ή ισομορφισμός) αν και μόνο αν ο φ είναι μονομορφισμός (αντίστοιχα, επιμορφισμός ή ισομορφισμός).
(γ) Συνάγετε ότι υπάρχει επιμορφισμός δακτυλίων $\psi : \mathbb{Z}[x] \to \mathbb{Z}_n[x]$ για τον οποίο $\psi(a) = \bar{a} \in \mathbb{Z}_n$ (η κλάση του $a \pmod n$) για κάθε $a \in \mathbb{Z}$ (το $\psi(f(x))$ είναι η *αναγωγή του* $f(x) \pmod n$).
(δ) Έστω θετικοί ακέραιοι n, m και έστω ότι ο n διαιρεί τον m. Συνάγετε ότι υπάρχει επιμορφισμός δακτυλίων $\psi : \mathbb{Z}_m[x] \to \mathbb{Z}_n[x]$ για τον οποίο $\psi(\bar{a}) \in \mathbb{Z}_n$ είναι η κλάση του $a \pmod n$ για κάθε $\bar{a} \in \mathbb{Z}_m$.

76. Δίνεται ακέραιος $p \geq 2$. Δείξτε ότι το πολυώνυμο $1 + x + x^2 + \cdots + x^{p-1}$ είναι ανάγωγο στο $\mathbb{Z}[x]$ αν και μόνο αν ο p είναι πρώτος αριθμός.

77. Δείξτε ότι τα πολυώνυμα:

(α) $5x^8 + 132x^2 + 253x + 209$,
(β) $16x^4 + 11x^3 + 5x^2 + 21x + 48$,
(γ) $x^6 + x^5 + x^4 + 8x^3 + 8x^2 + x + 1$

είναι ανάγωγα στο $\mathbb{Z}[x]$.

78. Δίνεται πρώτος αριθμός p. Να εξετάσετε αν ισχύουν οι παρακάτω προτάσεις:

(α) Αν $f(x) \in \mathbb{Z}[x]$ και το $f(m)$ διαιρείται με το p για κάθε $m \in \mathbb{Z}$, τότε κάθε συντελεστής του $f(x)$ διαιρείται με το p.
(β) Αν $f(x) \in \mathbb{Z}[x]$ είναι πολυώνυμο βαθμού μικρότερου του p και το $f(m)$ διαιρείται με το p για κάθε $m \in \mathbb{Z}$, τότε κάθε συντελεστής του $f(x)$ διαιρείται με το p.

79. Δίνεται επιμομορφισμός δακτυλίων $\varphi : R \to S$ και θετικός ακέραιος n.

(α) Αν ο R είναι μεταθετικός, δείξτε ότι το ίδιο ισχύει για τον S.
(β) Αν ο R έχει μονάδα, δείξτε ότι το ίδιο ισχύει για τον S και ότι $\varphi(1_R) = 1_S$.
(γ) Αν $n \cdot a = 0_R$ για κάθε $a \in R$, δείξτε ότι $n \cdot b = 0_S$ για κάθε $b \in S$.
(δ) Αν κάθε στοιχείο του R είναι μηδενοδύναμο, δείξτε ότι το ίδιο ισχύει για τον S.

(ε) Έστω θετικός ακέραιος m. Αν κάθε πολυώνυμο στο $R[x]$ αναλύεται σε γινόμενο πολυωνύμων βαθμού μικρότερου του m, δείξτε ότι το ίδιο ισχύει για τα πολυώνυμα του $S[x]$.

80. Δίνεται ομομορφισμός $\varphi : R \to S$ δακτυλίων με μονάδα, με $\varphi(1_R) = 1_S$.

(α) Αν $a \in U(R)$, δείξτε ότι $\varphi(a) \in U(S)$. Συνάγετε ότι ο φ επάγει μια απεικόνιση $\bar{\varphi} : U(R) \to U(S)$.
(β) Αν ο φ είναι μονομορφισμός, δείξτε ότι η $\bar{\varphi}$ είναι 1–1.
(γ) Αν ο φ είναι ισομορφισμός, δείξτε ότι η $\bar{\varphi}$ είναι 1–1 και επί.
(δ) Δώστε παράδειγμα επιμορφισμού φ για τον οποίο η απεικόνιση $\bar{\varphi}$ δεν είναι επί.
(ε) Δείξτε ότι οι δακτυλίοι $\mathbb{Z}[i]$ και $\mathbb{Z}[x]$ δεν είναι ισόμορφοι.

81. Δίνεται μη μηδενικός ομομορφισμός $\varphi : R \to S$ δακτυλίων με μονάδα.

(α) Αν ο S δεν έχει μηδενοδιαιρέτες, δείξτε ότι $\varphi(1_R) = 1_S$.
(β) Δώστε παράδειγμα τέτοιου ομομορφισμού με $\varphi(1_R) \neq 1_S$.
(γ) Έστω $n \in \mathbb{Z}$. Αν ο S δεν έχει μηδενοδιαιρέτες και υπάρχει $a \in R$ με $n \cdot a = 1_R$, δείξτε ότι υπάρχει $b \in S$ με $n \cdot b = 1_S$.
(δ) Συνάγετε ότι δεν υπάρχει μη μηδενικός ομομορφισμός δακτυλίων $\varphi : \mathbb{Q} \to \mathbb{Z}$.

82. Να εξετάσετε αν είναι αληθείς οι παρακάτω προτάσεις:

(α) Υπάρχει πεπερασμένος δακτύλιος R και γνήσιος υποδακτύλιος αυτού ο οποίος είναι ισόμορφος με τον R.
(β) Υπάρχει γνήσιος υποδακτύλιος του $\mathbb{Z}$ ο οποίος είναι ισόμορφος με τον $\mathbb{Z}$.
(γ) Υπάρχει δακτύλιος R και γνήσιος υποδακτύλιος αυτού ο οποίος είναι ισόμορφος με τον R.

83. Βρείτε όλους τους ομομορφισμούς δακτυλίων $\varphi : \mathbb{Z}[i] \to S$, όπου:

(α) $S = \mathbb{Z}_9$.
(β) $S = \mathbb{Z}_{10}$.
(γ) $S = \mathbb{Z}[x]$.

84. Βρείτε όλους τους αυτομορφισμούς:

(α) του δακτυλίου $\mathbb{Q}$,
(β) του δακτυλίου $\mathbb{Z}[x]$,
(γ) του δακτυλίου $\mathbb{Q}[x]$.

85. Να εξετάσετε αν το I είναι ιδεώδες του δακτυλίου R στις παρακάτω περιπτώσεις:

(α) $R = M_2(\mathbb{Z})$ και $I = \left\{ \begin{pmatrix} 2a & b \\ c & d \end{pmatrix} : \ a, b, c, d \in \mathbb{Z} \right\}$.

(β) $R = T_2(\mathbb{Z})$ και $I = \left\{ \begin{pmatrix} 2a & b \\ 0 & c \end{pmatrix} : \ a, b, c \in \mathbb{Z} \right\}$.

(γ) $R = \mathbb{Z}[x]$ και $I = \{f(x) \in \mathbb{Z}[x] : f(\sqrt{2}) = 0\}$.

(δ) $R = \mathbb{Z}[x]$ και $I = \{f(x) \in \mathbb{Z}[x] : f(1) = f'(1) = 0\}$.

(ε) $R = \mathbb{Z}[x]$ και $I = \{f(x) \in \mathbb{Z}[x] : f(1) = f'(2) = 0\}$.

86. Δίνεται σώμα $\mathbb{F}$ και τα υποσύνολα

$$I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : \ b \in \mathbb{F} \right\}, \ J = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : \ a, b \in \mathbb{F} \right\}, \ K = \left\{ \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} : \ b, c \in \mathbb{F} \right\}$$

του δακτυλίου $R = T_2(\mathbb{F})$.

(α) Δείξτε ότι τα I, J, K είναι ιδεώδη του R.

(β) Δείξτε ότι τα I, J, K είναι τα μόνα μη τετριμμένα (δηλαδή διάφορα των $\{0_R\}$ και R) ιδεώδη του R.

87. Δίνονται ακέραιοι a, b, όχι και οι δύο μηδέν. Πόσους πρώτους αριθμούς μπορεί να περιέχει το σύνολο $\{ax + by : x, y \in \mathbb{Z}\}$;

88. Δίνεται σώμα $\mathbb{F}$. Δείξτε ότι κάθε ιδεώδες του δακτυλίου $\mathbb{F}[x]$ είναι κύριο.

89. Δίνεται το σύνολο $I = \{f(x) \in \mathbb{Q}[x] : f(1 + \sqrt{2}) = 0\}$.

(α) Δείξτε ότι το I είναι ιδεώδες του δακτυλίου $\mathbb{Q}[x]$.

(β) Βρείτε ομομορφισμό δακτυλίων $\varphi : \mathbb{Q}[x] \to S$ τέτοιον ώστε $\ker(\varphi) = I$.

(γ) Βρείτε πολυώνυμο $g(x) \in \mathbb{Q}[x]$ τέτοιο ώστε ότι $I = \langle g(x) \rangle$.

90. Δίνεται το σύνολο $I = \{f(x) \in \mathbb{Z}[x] : f(0) \in 2\mathbb{Z}\}$.

(α) Δείξτε ότι το I είναι ιδεώδες του δακτυλίου $\mathbb{Z}[x]$.

(β) Βρείτε ομομορφισμό δακτυλίων $\varphi : \mathbb{Z}[x] \to S$ τέτοιον ώστε $\ker(\varphi) = I$.

(γ) Δείξτε ότι $I = \langle 2, x \rangle \subseteq \mathbb{Z}[x]$.

(δ) Δείξτε ότι το I δεν είναι κύριο ιδεώδες του $\mathbb{Z}[x]$.

91. Υπολογίστε τον πυρήνα και την εικόνα των ομομορφισμών της Άσκησης 83. Για καθέναν από αυτούς, δείξτε ότι ο πυρήνας είναι κύριο ιδεώδες του $\mathbb{Z}[i]$ και βρείτε στοιχείο που τον παράγει.

92. Δίνεται σώμα $\mathbb{F}$.

(α) Δείξτε ότι τα τετριμμένα ιδεώδη $\{0\}$ και $\mathbb{F}$ είναι τα μόνα ιδεώδη του $\mathbb{F}$.

(β) Δείξτε, γενικότερα, ότι για κάθε θετικό ακέραιο n, τα τετριμμένα ιδεώδη $\{O\}$ και $M_n(\mathbb{F})$ είναι τα μόνα ιδεώδη του δακτυλίου $M_n(\mathbb{F})$.
(γ) Δείξτε ότι κάθε μη μηδενικός ομομορφισμός δακτυλίων $\varphi : M_n(\mathbb{F}) \to S$ είναι μονομορφισμός.

93. Δίνεται ομομορφισμός δακτυλίων $\varphi : R \to S$. Υπενθυμίζουμε ότι για $J \subseteq S$ ορίζεται η αντίστροφη εικόνα $\varphi^{-1}(J) = \{x \in R : \varphi(x) \in J\}$ του J ως προς φ.

(α) Αν το J είναι ιδεώδες του S, δείξτε ότι το $\varphi^{-1}(J)$ είναι ιδεώδες του R.
(β) Αν ο φ είναι επιμορφισμός και το I είναι ιδεώδες του R, δείξτε ότι το $\varphi(I)$ είναι ιδεώδες του S.
(γ) Έστω ότι οι R και S είναι μεταθετικοί δακτύλιοι. Αν ο φ είναι επιμορφισμός και $I = \langle a_1, a_2, \ldots, a_m\rangle \subseteq R$, δείξτε ότι $\varphi(I) = \langle \varphi(a_1), \varphi(a_2), \ldots, \varphi(a_m)\rangle \subseteq S$.
(δ) Έστω ότι οι R και S είναι μεταθετικοί δακτύλιοι. Αν ο φ είναι επιμορφισμός και κάθε ιδεώδες του R είναι κύριο, δείξτε ότι κάθε ιδεώδες του S είναι κύριο.
(ε) Συνάγετε ότι κάθε ιδεώδες του δακτυλίου $\mathbb{Z}_m$ είναι κύριο.
(στ) Ισχύει το (β) χωρίς την υπόθεση ότι ο φ είναι επιμορφισμός;

94. Δίνονται δακτύλιοι R, S και ιδεώδη I, J αυτών, αντίστοιχα.

(α) Δείξτε ότι το $I \times J$ είναι ιδεώδες του δακτυλίου $R \times S$.
(β) Αν οι R και S έχουν μονάδα, δείξτε ότι κάθε ιδεώδες του $R \times S$ είναι της μορφής $I \times J$, όπου I είναι ιδεώδες του R και J είναι ιδεώδες του S.
(γ) Ισχύει το (β) χωρίς την υπόθεση ότι οι R και S έχουν μονάδα;

95. Δίνεται δακτύλιος R και ιδεώδη I, J αυτού. Υπενθυμίζουμε ότι με IJ συμβολίζεται το σύνολο όλων των πεπερασμένων αθροισμάτων στοιχείων του R της μορφής ab, όπου $a \in I$ και $b \in J$.

(α) Δείξτε ότι το IJ είναι ιδεώδες του R και ότι $IJ \subseteq I \cap J$.
(β) Αν ο R είναι μεταθετικός με μονάδα και $I + J = R$, δείξτε ότι $IJ = I \cap J$.
(γ) Ισχύει το (β) χωρίς την υπόθεση ότι ο R έχει μονάδα;
(δ) Ισχύει το (β) χωρίς την υπόθεση ότι $I + J = R$;

96. Δίνεται δακτύλιος R και ιδεώδη I, J αυτού.

(α) Αν $I + J = R$ και $I \cap J = \{0_R\}$, δείξτε ότι ο R είναι ισόμορφος με το ευθύ γινόμενο $I \times J$ των υποδακτυλίων του I και J.
(β) Συνάγετε ότι αν m και n είναι σχετικώς πρώτοι θετικοί ακέραιοι, τότε ο δακτύλιος $\mathbb{Z}_{mn}$ είναι ισόμορφος με το ευθύ γινόμενο $\mathbb{Z}_m \times \mathbb{Z}_n$.

97. Δίνονται οι δακτυλίοι πηλίκο $R = \mathbb{Z}_p[x] \,/\, \langle x^2+1\rangle$ και $S = \mathbb{Z}_p[x] \,/\, \langle x^2+x+1\rangle$, όπου p είναι πρώτος αριθμός. Έστω α η κλάση του x στο R και β η κλάση του x στο S, οπότε $\alpha^2 = -1$ και $\beta^2+\beta+1 = 0$.

(α) Υπολογίστε το γινόμενο $\prod_{k=1}^{p}(k^2+1)$ στο R.
(β) Υπολογίστε το γινόμενο $\prod_{k=1}^{p}(k^2+k+1)$ στο S.
(γ) Για ποιους πρώτους p υπάρχει $k \in \mathbb{Z}$ τέτοιο ώστε $p \mid k^2+1$;
(δ) Για ποιους πρώτους p υπάρχει $k \in \mathbb{Z}$ τέτοιο ώστε $p \mid k^2+k+1$;

98. Δίνονται το ιδεώδες $I = \langle x^2+x+1\rangle$ του δακτυλίου $\mathbb{Z}[x]$, ο δακτύλιος πηλίκο $R = \mathbb{Z}[x] \,/\, I$ και τα πολυώνυμα $f_n(x) = (x+1)^n + x^n + 1$ για $n \in \mathbb{N}$.

(α) Βρείτε $a_n, b_n \in \mathbb{Z}$ ώστε να ισχύει $f_n(x) + I = (a_n + b_n x) + I$ στο R.
(β) Δείξτε ότι το $f_n(x)$ διαιρείται με το x^2+x+1 στο $\mathbb{Z}[x]$ αν και μόνο αν $n \equiv 2$ ή $4 \pmod 6$.

99. Δίνεται το υποσύνολο

$$R \;=\; \left\{ \begin{pmatrix} a & b \\ b & a+b \end{pmatrix} :\; a, b \in \mathbb{Z}_2 \right\}$$

του $M_2(\mathbb{Z}_2)$.

(α) Δείξτε ότι το R είναι μεταθετικός υποδακτύλιος του $M_2(\mathbb{Z}_2)$ με μονάδα.
(β) Δείξτε ότι ο R είναι ισόμορφος με το δακτύλιο πηλίκο $\mathbb{Z}_2[x] \,/\, \langle x^2+x+1\rangle$.
(γ) Συνάγετε ότι ο δακτύλιος R είναι σώμα με τέσσερα στοιχεία.

100. Δίνεται ο δακτυλίος πηλίκο $R = \mathbb{Z}_3[x] \,/\, \langle x^2+2\rangle$.

(α) Πόσα στοιχεία έχει ο R;
(β) Ποια είναι τα αντιστρέψιμα στοιχεία του;

101. Δίνεται σώμα $\mathbb{F}$, πολυώνυμα $f(x), g(x) \in \mathbb{F}[x]$ με $f(x) \neq 0$, το ιδεώδες $I = \langle g(x)\rangle$ του $\mathbb{F}[x]$ και ο δακτυλίος πηλίκο $R = \mathbb{F}[x] \,/\, I$.

(α) Δείξτε ότι κλάση $f(x) + I$ είναι αντιστρέψιμο στοιχείο του R αν και μόνο αν $\mu\kappa\delta(f(x), g(x)) = 1$.
(β) Πόσα αντιστρέψιμα στοιχεία έχει ο R, αν το $\mathbb{F}$ είναι πεπερασμένο σώμα με q στοιχεία και $g(x) = (x+1)^n$;

102. Δίνονται δακτύλιοι R, S και ιδεώδη I, J αυτών, αντίστοιχα.

(α) Δείξτε τον ισομορφισμό δακτυλίων $(R\times S) \,/\, (I\times J) \cong (R/I)\times(S/J)$.
(β) Συνάγετε ότι $(\mathbb{Z}\times\mathbb{Z}) \,/\, (m\mathbb{Z}\times n\mathbb{Z}) \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

103. Δείξτε ότι ισχύουν οι παρακάτω ισομορφισμοί δακτυλίων:

(α) $\mathbb{Z}[x] \,/\, \langle x^2+1\rangle \cong \mathbb{Z}[i]$,
(β) $R[x] \,/\, \langle x^2 - 1_R\rangle \cong R\times R$, όπου R είναι ακέραια περιοχή με $-1_R \neq 1_R$,

(γ) $\mathbb{Z}[i] \,/\, \langle 1 + 4i \rangle \cong \mathbb{Z}_{17}$.

104. Δίνεται δακτύλιος R και ιδεώδη I, J αυτού.

(α) Αν υπάρχει αυτομορφισμός φ του R τέτοιος ώστε $\varphi(I) = J$, δείξτε ότι ο δακτύλιος πηλίκο R/I είναι ισόμορφος με τον R/J.
(β) Δώστε παράδειγμα μεταθετικού δακτυλίου R με μονάδα και ιδεωδών I, J αυτού, τέτοιων ώστε τα I και J να είναι ισόμορφοι υποδακτύλιοι του R αλλά ο δακτύλιος πηλίκο R/I να μην είναι ισόμορφος με τον R/J.

105. Ποιοι από τους παρακάτω δακτυλίους είναι μεταξύ τους ισόμορφοι;

(α) $\mathbb{Z}_4$,
(β) $\mathbb{Z}_2 \times \mathbb{Z}_2$,
(γ) $\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : \ a, b \in \mathbb{Z}_2 \right\}$, ως υποδακτύλιος του $M_2(\mathbb{Z})$,
(δ) $\mathbb{Z}_2[x] \,/\, \langle x^2 \rangle$,
(ε) $\mathbb{Z}_2[x] \,/\, \langle x^2 + 1 \rangle$.

106. Ποιοι από τους παρακάτω δακτυλίους είναι μεταξύ τους ισόμορφοι;

(α) $\mathbb{Q}[x] \,/\, \langle x^2 - 1 \rangle$,
(β) $\mathbb{Q}[x] \,/\, \langle x^2 - 2 \rangle$,
(γ) $\mathbb{Q}[x] \,/\, \langle x^2 - 4 \rangle$,
(δ) $\mathbb{Q}[x] \,/\, \langle x^2 + 1 \rangle$,
(ε) $\mathbb{Q}[x] \,/\, \langle x^2 + 2 \rangle$,
(στ) $\mathbb{Q}[x] \,/\, \langle x^2 + 8 \rangle$.

107. Δίνονται οι πίνακες

$$\alpha = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \beta = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

και το σύνολο R των πινάκων $x \in M_3(\mathbb{F})$ για τους οποίους ισχύουν $\alpha x = x\alpha$ και $\beta x = x\beta$ (όπου $\mathbb{F}$ είναι σώμα).

(α) Δείξτε ότι το R είναι υποδακτύλιος του $M_3(\mathbb{F})$ με μονάδα.
(β) Δείξτε ότι ο δακτύλιος R είναι μεταθετικός.
(γ) Δείξτε ότι ο R είναι ισόμορφος με το δακτύλιο πηλίκο $\mathbb{F}[t] \,/\, \langle t^3 \rangle$.

108. Δίνεται σώμα $\mathbb{F}$, πολυώνυμο $g(x) \in \mathbb{F}[x]$ βαθμού n και ο δακτύλιος πηλίκο $R = \mathbb{F}[x]/\langle g(x) \rangle$. Ορίζουμε εξωτερικό πολλαπλασιασμό $\mathbb{F} \times R \to R$ ταυτίζοντας κάθε στοιχείο $a \in \mathbb{F}$ με την κλάση του αντίστοιχου σταθερού πολυωνύμου $a \in \mathbb{F}[x]$ στο R.

(α) Δείξτε ότι το R, εφοδιασμένο με την πρόσθεσή του και τον εξωτερικό αυτό πολλαπλασιασμό, είναι διανυσματικός χώρος επί του $\mathbb{F}$.

(β) Δείξτε ότι αν $\alpha = x + \langle g(x)\rangle$ είναι είναι η κλάση του x στο R, τότε το σύνολο $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ αποτελεί βάση του $\mathbb{F}$-διανυσματικού χώρου R. Συνάγετε ότι $\dim_{\mathbb{F}}(R) = n$.

(γ) Έστω τυχαίο υποσύνολο S του $\mathbb{N}$ με $n+1$ στοιχεία. Δείξτε ότι υπάρχει πολυώνυμο $h(x) \in \mathbb{F}[x]$ τέτοιο ώστε $g(x)h(x) = \sum_{i\in S} a_i x^i$ για κάποια $a_i \in \mathbb{F}$ (δηλαδή τέτοιο ώστε οι εκθέτες των μονωνύμων που εμφανίζονται στο $g(x)h(x)$ με μη μηδενικό συντελεστή να ανήκουν όλοι στο S).

109. Δίνεται σώμα $\mathbb{F}$. Ποιες από τις παρακάτω προτάσεις είναι αληθείς;

(α) Αν $f(x), g(x) \in \mathbb{F}[x]$ είναι μονικά πολυώνυμα και ο δακτύλιος $\mathbb{F}[x]/\langle f(x)\rangle$ είναι ισόμορφος με τον $\mathbb{F}[x]/\langle g(x)\rangle$, τότε $f(x) = g(x)$.

(β) Αν $f(x), g(x) \in \mathbb{F}[x]$ και οι δακτύλιος $\mathbb{F}[x]/\langle f(x)\rangle$ και $\mathbb{F}[x]/\langle g(x)\rangle$ είναι ισόμορφοι, τότε $\deg(f(x)) = \deg(g(x))$.

110. Δίνονται πρώτοι αριθμοί p και q και οι δακτύλιοι $R = \mathbb{Z}_p[x]/\langle x^p - x\rangle$ και $S = \mathbb{Z}_q[x]/\langle x^q + x\rangle$.

(α) Δείξτε ότι $y^p = y$ για κάθε $y \in R$.

(β) Δείξτε ότι αν οι οι δακτύλιοι R και S είναι ισόμορφοι, τότε $p = q = 2$.

Ομάδες: Βασικές Έννοιες

Θα συμβολίζουμε με e το ουδέτερο στοιχείο μιας ομάδας G. Υπενθυμίζουμε ότι η τάξη ενός στοιχείου $a \in G$ είναι ο ελάχιστος θετικός ακέραιος m για τον οποίο ισχύει $a^m = e$, αν τέτοιος ακέραιος υπάρχει (διαφορετικά το a έχει άπειρη τάξη).

111. Ποιες από τις ακόλουθες προτάσεις είναι αληθείς;

(α) Αν για τα στοιχεία a, b, c μιας ομάδας ισχύει $abc = e$, τότε $bca = e$.
(β) Αν για τα στοιχεία a, b, c μιας ομάδας ισχύει $abc = e$, τότε $bac = e$.

112. Δίνεται δακτύλιος R με μονάδα και το σύνολο $U(R)$ των αντιστρέψιμων στοιχείων του.

(α) Δείξτε ότι το $U(R)$, με πράξη τον πολλαπλασιασμό του R, αποτελεί ομάδα.
(β) Προσδιορίστε την ομάδα $U(R)$ για $R = \mathbb{Z}[i]$.
(γ) Περιγράψτε τα στοιχεία της ομάδας $U(R)$ αν R είναι ο δακτύλιος των άνω τριγωνικών $n \times n$ πινάκων με στοιχεία από μια ακέραια περιοχή F.

113. Δίνεται δακτύλιος R και το σύνολο $\mathrm{Aut}(R)$ των αυτομορφισμών του R.

(α) Δείξτε ότι το $\mathrm{Aut}(R)$, με πράξη τη σύνθεση απεικονίσεων, αποτελεί ομάδα.
(β) Προσδιορίστε την ομάδα $\mathrm{Aut}(R)$ για τον υποδακτύλιο $R = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ του $\mathbb{C}$.

114. Αποφανθείτε αν είναι αληθής η ακόλουθη πρόταση: Αν για τα στοιχεία a, b μιας ομάδας ισχύει $a^{13}b^8 = a^8b^5 = e$, τότε $a = b = e$.

115. Δίνονται στοιχεία a, b μιας ομάδας με $a^3b = ba^3$.

(α) Αν $a^2 = e$, δείξτε ότι $ab = ba$.
(β) Αν $a^4 = e$, δείξτε ότι $ab = ba$.
(γ) Αν $a^5 = e$, δείξτε ότι $ab = ba$.
(δ) Γενικότερα, αν $a^r = e$ για κάποιο θετικό ακέραιο r ο οποίος δεν είναι πολλαπλάσιο του 3, δείξτε ότι $ab = ba$.

116. Δίνονται στοιχεία a, b μιας ομάδας G.

(α) Αν $ab = ba$, δείξτε ότι $a^mb^n = b^na^m$ για όλα τα $m, n \in \mathbb{Z}$.
(β) Έστω ότι τα a και b έχουν πεπερασμένες τάξεις p και q στη G, αντίστοιχα. Αν $a^mb^n = b^na^m$ για κάποια $m, n \in \mathbb{Z}$ με $\mu\kappa\delta(m, p) = \mu\kappa\delta(n, q) = 1$, δείξτε ότι $ab = ba$.

117. Δίνονται πεπερασμένη ομάδα G, υποσύνολο S αυτής και θετικός ακέραιος n.

(α) Έστω ότι το S περιέχει περισσότερα από τα μισά στοιχεία της G. Δείξτε ότι για κάθε $x \in G$ υπάρχουν $a, b \in S$ τέτοια ώστε $x = ab$.
(β) Δώστε παράδειγμα ομάδας G τάξης $2n$ και συνόλου $S \subseteq G$ με n στοιχεία, για τα οποία δεν υπάρχει $x \in G \setminus S$ το οποίο να μπορεί να γραφεί ως γινόμενο στοιχείων του S.

118. Δίνεται πεπερασμένη ομάδα G με τουλάχιστον δύο στοιχεία. Υποθέτουμε ότι για οποιαδήποτε στοιχεία $a, b \in G$, διάφορα του e, υπάρχει $x \in G$ τέτοιο ώστε $b = xax^{-1}$. Δείξτε ότι η G έχει ακριβώς δύο στοιχεία.

119. Δίνεται πεπερασμένο σώμα $\mathbb{F}_q$ με q στοιχεία.

(α) Υπολογίστε την τάξη της ομάδας των αντιστρέψιμων άνω τριγωνικών $n \times n$ πινάκων με στοιχεία από το $\mathbb{F}_q$.
(β) Υπολογίστε την τάξη της ομάδας $\mathrm{GL}_n(\mathbb{F}_q)$ των αντιστρέψιμων $n \times n$ πινάκων με στοιχεία από το $\mathbb{F}_q$.

120. Δίνεται πεπερασμένη ομάδα G.

(α) Δείξτε ότι το πλήθος των στοιχείων τάξης 2 της G είναι περιττός αριθμός αν και μόνο αν η τάξη της G είναι άρτιος αριθμός.
(β) Υπολογίστε το πλήθος των στοιχείων τάξης 2 της ομάδας των συμμετριών του κανονικού n-γώνου για κάθε ακέραιο $n \geq 3$.

121. Δείξτε ότι δεν υπάρχει ομάδα που να έχει ακριβώς δύο στοιχεία τάξης 2.

122. Δίνεται ομάδα G και στοιχείο $a \in G$ πεπερασμένης τάξης n.

(α) Έστω $m \in \mathbb{Z}$. Δείξτε ότι $a^m = e$ αν και μόνο αν το m είναι ακέραιο πολλαπλάσιο του n.
(β) Υπολογίστε την τάξη του στοιχείου 2 της πολλαπλασιαστικής ομάδας $U(\mathbb{Z}_{25})$.
(γ) Υπολογίστε την τάξη του στοιχείου 2 της πολλαπλασιαστικής ομάδας $U(\mathbb{Z}_{5^m})$ για κάθε θετικό ακέραιο m.

123. Δίνονται στοιχεία μιας ομάδας a και b τάξης p και q, αντίστοιχα, με $ab = ba$.

(α) Αν οι p και q είναι σχετικώς πρώτοι, δείξτε ότι η τάξη του ab είναι ίση με pq.
(β) Έστω ότι $p = q = 5$. Ποιες είναι οι δυνατές τιμές της τάξης του ab;
(γ) Έστω ότι $p = q = 4$. Ποιες είναι οι δυνατές τιμές της τάξης του ab;

124. Δίνεται ομάδα G, στοιχείο a αυτής και η απεικόνιση $f_a : G \to G$ με $f_a(x) = xax^{-1}$ για $x \in G$. Η εικόνα $\{xax^{-1} : x \in G\}$ της f_a λέγεται *κλάση συζυγίας* του a στη G και συμβολίζεται με C_a.

(α) Ποια είναι η κλάση συζυγίας C_e του ουδέτερου στοιχείου $e \in G$;
(β) Δείξτε ότι οι κλάσεις συζυγίας της G αποτελούν διαμέριση του συνόλου G (δηλαδή ότι είναι μη κενές, ξένες ανά δύο και ότι η ένωσή τους είναι ίση με G).
(γ) Δείξτε ότι η G είναι αβελιανή αν και μόνο αν κάθε κλάση συζυγίας της G έχει ακριβώς ένα στοιχείο.
(δ) Δώστε παράδειγμα μη τετριμμένης πεπερασμένης ομάδας, οι κλάσεις συζυγίας της οποίας έχουν ανά δύο διαφορετικούς πληθάριθμους.
(ε) Δείξτε ότι ο πληθάριθμος της αντίστροφης εικόνας $\{x \in G : f_a(x) = b\}$ του $\{b\}$ ως προς την f_a είναι ανεξάρτητος του $b \in C_a$.
(στ) Δείξτε ότι αν η G είναι πεπερασμένη, τότε το πλήθος των στοιχείων οποιασδήποτε κλάσης συζυγίας της G διαιρεί την τάξη της G.
(ζ) Δώστε μια λύση στην Άσκηση 118 χρησιμοποιώντας το (στ).

Συμμετρικές Ομάδες

Συμβολίζουμε με $S(X)$ την ομάδα των μεταθέσεων του συνόλου X και με S_n την ομάδα των μεταθέσεων του συνόλου $\{1, 2, \ldots, n\}$.

125. Ορίζουμε την απεικόνιση $\sigma : \{1, 2, \ldots, 20\} \to \{1, 2, \ldots, 20\}$ θέτοντας

$$\sigma(k) = \begin{cases} 2k, & \text{αν } k \leq 10 \\ 2k - 11, & \text{αν } k \geq 11 \end{cases}$$

για $k \in \{1, 2, \ldots, 20\}$.

(α) Δείξτε ότι $\sigma \in S_{20}$.
(β) Υπολογίστε την τάξη της σ.
(γ) Υπολογίστε τις μεταθέσεις σ^{2000} και σ^{2013}.

126. Υπολογίστε την τάξη του στοιχείου

$$(1\ 2\ \cdots\ n)\,(1\ 2\ \cdots\ n-1)\ \cdots\ (1\ 2\ 3)\,(1\ 2)$$

της S_n για κάθε $n \geq 2$.

127. Βρείτε τον ελάχιστο θετικό ακέραιο n για τον οποίο υπάρχει ακέραιος $r \geq 2$ με την εξής ιδιότητα: η συμμετρική ομάδα S_n έχει τουλάχιστον ένα στοιχείο τάξης r αλλά δεν έχει στοιχείο τάξης $r - 1$.

128. Δίνεται η μετάθεση $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 8 & 1 & 5 & 3 & 4 & 2 \end{pmatrix} \in S_8$.

(α) Υπολογίστε την τάξη της σ.
(β) Βρείτε στοιχεία x, y τάξης 2 της S_8 τέτοια ώστε $xy = \sigma$.
(γ) Υπάρχουν στοιχεία x, y τάξης 3 της S_8 τέτοια ώστε $xy = \sigma$;

129. Ποιες από τις παρακάτω προτάσεις είναι αληθείς;

(α) Υπάρχουν δύο στοιχεία τάξης 15 της συμμετρικής ομάδας S_8 το γινόμενο των οποίων έχει επίσης τάξη 15.
(β) Υπάρχουν δύο στοιχεία τάξης 30 της συμμετρικής ομάδας S_{10} το γινόμενο των οποίων έχει επίσης τάξη 30.

130. Δείξτε ότι:

(α) Κάθε μετάθεση $w \in S_n$ περιττής τάξης είναι άρτια.
(β) Κάθε άρτια μετάθεση $w \in S_n$ μπορεί να γραφεί ως γινόμενο μεταθέσεων περιττής τάξης.

131. Ποια στοιχεία της S_4 μπορούν να γραφούν στη μορφή $\sigma\tau\sigma^2\tau^2\sigma^3\tau^3$, με $\sigma, \tau \in S_4$;

132. Θεωρούμε μεταθέσεις $\sigma, \tau \in S_n$.

(α) Αν μία από τις σ, τ είναι ίση με κάποια δύναμη της άλλης, δείξτε ότι $\sigma\tau = \tau\sigma$. Ισχύει το αντίστροφο;
(β) Αν $\sigma\tau = \tau\sigma$ και η τ είναι κύκλος μήκους n, δείξτε ότι η σ είναι ίση με κάποια δύναμη της τ.

133. Πόσα στοιχεία της S_{2n} μετατίθενται με το στοιχείο $(1\ 2)(3\ 4)\cdots(2n-1\ 2n)$;

134. Για $\sigma \in S_n$ συμβολίζουμε με $c(\sigma)$ το πλήθος των κύκλων (συμπεριλαμβανομένων εκείνων μήκους ένα) της σ. Για παράδειγμα, έχουμε $c(e) = n$ και $c(\sigma) = 1$ αν και μόνο αν η σ είναι κύκλος μήκους n.

(α) Έστω ότι η σ είναι κύκλος μήκους n. Δείξτε ότι η $c(\sigma^2) = 1$, αν ο n είναι περιττός αριθμός και ότι $c(\sigma^2) = 2$, αν ο n είναι άρτιος.
(β) Δείξτε ότι $c(\sigma) \leq c(\sigma^2) \leq 2c(\sigma)$ για κάθε $\sigma \in S_n$.
(γ) Δείξτε ότι $c(\sigma^2) = c(\sigma)$ αν και μόνο αν η τάξη της σ είναι περιττός αριθμός.

135. Δίνεται κύκλος $\tau \in S_n$ μήκους n.

(α) Δείξτε ότι κάθε μετάθεση $\sigma \in S_n$ με $\sigma^2 = \tau$ είναι κύκλος μήκους n.
(β) Βρείτε όλες τις μεταθέσεις $\sigma \in S_n$ με $\sigma^2 = \tau$.
(γ) Γενικότερα, για δοσμένο θετικό ακέραιο m, βρείτε όλες τις μεταθέσεις $\sigma \in S_n$ με $\sigma^m = \tau$.

136. Θεωρούμε τα στοιχεία $\sigma = (1\ 2)$ και $\tau = (1\ 2\ \cdots\ n)$ της S_n. Δείξτε ότι κάθε στοιχείο της S_n μπορεί να γραφεί ως γινόμενο πεπερασμένου πλήθους στοιχείων, καθένα από τα οποία είναι ίσο με σ ή με τ.

137. Για $n \geq 2$, δείξτε ότι κάθε στοιχείο της S_n μπορεί να γραφεί ως γινόμενο δύο στοιχείων τάξης 2 της S_n.

138. Για $\sigma \in S_n$ συμβολίζουμε με $f(\sigma)$ τον ελάχιστο φυσικό αριθμό k για τον οποίο η μετάθεση σ μπορεί να γραφεί ως γινόμενο k αντιμεταθέσεων (κύκλων μήκους 2). Για παράδειγμα, έχουμε $f(e) = 0$ και $f(\sigma) = 1$ αν και μόνο αν η σ είναι αντιμετάθεση. Συμβολίζουμε επίσης με $c(\sigma)$ το πλήθος των κύκλων της σ, όπως στην Άσκηση 134.

(α) Δείξτε ότι $f(\sigma) \leq n - c(\sigma)$ για κάθε $\sigma \in S_n$.
(β) Δείξτε ότι $c(\sigma t) = c(\sigma) \pm 1$ για κάθε $\sigma \in S_n$ και κάθε αντιμετάθεση $t \in S_n$.
(γ) Δείξτε ότι $f(\sigma) = n - c(\sigma)$ για κάθε $\sigma \in S_n$.

Υποομάδες

Υπενθυμίζουμε ότι οι αριστερές (αντίστοιχα, δεξιές) κλάσεις της υποομάδας H μιας ομάδας G είναι τα σύνολα $aH = \{ax : x \in H\}$ (αντίστοιχα, $Ha = \{xa : x \in H\}$) για $a \in G$. Θα συμβολίζουμε με $\mathbb{F}^\times$ την πολλαπλασιαστική ομάδα των μη μηδενικών στοιχείων ενός σώματος $\mathbb{F}$.

139. Δίνεται ομάδα G. Για $A, B \subseteq G$ θα γράφουμε $AB = \{ab : a \in A,\ b \in B\}$ και $A^{-1} = \{a^{-1} : a \in A\}$.

(α) Δείξτε ότι ένα σύνολο $H \subseteq G$ είναι υποομάδα της G αν και μόνο αν $e \in H$ και $HH = H^{-1} = H$.
(β) Έστω ότι H, K είναι υποομάδες της G. Δείξτε ότι το HK είναι υποομάδα της G αν και μόνο αν $HK = KH$.

140. Δίνονται ομάδες G και G' με ταυτοτικά στοιχεία e και e', αντίστοιχα. Στο $G \times G'$ ορίζουμε μια πράξη θέτοντας $(a, a')(b, b') = (ab, a'b')$ για $a, b \in G$ και $a', b' \in G'$.

(α) Δείξτε ότι με την πράξη αυτή, το $G \times G'$ καθίσταται ομάδα με ταυτοτικό στοιχείο (e, e') και ότι τα σύνολα $G \times \{e'\}$ και $\{e\} \times G$ είναι υποομάδες της ομάδας αυτής.
(β) Δώστε παράδειγμα ομάδων G και G', η καθεμιά με τουλάχιστον δύο στοιχεία, για τις οποίες οι $G \times \{e'\}$ και $\{e\} \times G'$ είναι οι μόνες υποομάδες της $G \times G'$ εκτός της τετριμμένης $\{e\} \times \{e'\}$ και της $G \times G'$.
(γ) Δείξτε ότι για κάθε ομάδα G με τουλάχιστον δύο στοιχεία, η ομάδα $G \times G$ έχει τουλάχιστον τρεις υποομάδες εκτός της τετριμμένης $\{e\} \times \{e\}$ και της $G \times G$.

141. Μια υποομάδα H μιας ομάδας G λέγεται γνήσια αν η H είναι γνήσιο υποσύνολο της G. Ποιες από τις παρακάτω προτάσεις είναι αληθείς;

(α) Υπάρχει ομάδα η οποία είναι ίση με την ένωση δύο γνήσιων υποομάδων της.
(β) Υπάρχει ομάδα η οποία είναι ίση με την ένωση τριών γνήσιων υποομάδων της.

142. Θεωρούμε το σύνολο $E_n = \{z \in \mathbb{C} : z^n = 1\}$.

(α) Δείξτε ότι το E_n είναι υποομάδα τάξης n της $\mathbb{C}^\times$ για κάθε θετικό ακέραιο n.
(β) Δείξτε ότι το E_n είναι η μόνη υποομάδα τάξης n της $\mathbb{C}^\times$.

143. Δίνονται ακέραιοι $1 \leq k \leq n$. Συμβολίζουμε με H το σύνολο των μεταθέσεων $\sigma \in S_n$ για τις οποίες ισχύει $\sigma(i) \in \{1, 2, \ldots, k\}$ για κάθε $i \in \{1, 2, \ldots, k\}$.

(α) Δείξτε ότι το H είναι υποομάδα της S_n.
(β) Υπολογίστε την τάξη της H και το δείκτη $[S_n : H]$.
(γ) Περιγράψτε τις αριστερές κλάσεις της H στην S_n.
(δ) Περιγράψτε τις δεξιές κλάσεις της H στην S_n.

144. Θεωρούμε το σύνολο $X = \{1, -1, 2, -2, \ldots, n, -n\}$, όπου n είναι θετικός ακέραιος, και συμβολίζουμε με K το σύνολο των μεταθέσεων $\sigma \in S(X)$ για τις οποίες ισχύει $\sigma(-x) = -\sigma(x)$ για κάθε $x \in X$.

(α) Δείξτε ότι το K είναι υποομάδα της $S(X)$.
(β) Υπολογίστε την τάξη της K και το δείκτη $[S(X) : K]$.

145. Για ποιους θετικούς ακεραίους d υπάρχει υποομάδα της S_4 τάξης d;

146. Δώστε παράδειγμα ομάδας τάξης 12 η οποία δεν έχει υποομάδες τάξης 6.

147. Δίνεται ομάδα G τάξης 4.

(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 η G είναι αβελιανή. Ισχύει το ίδιο για τις ομάδες τάξης 8;
(γ) Βρείτε όλες τις υποομάδες της ομάδας των συμμετριών του τετραγώνου.

148. Για ομάδα G και στοιχείο $a \in G$ θέτουμε $C_G(a) = \{x \in G : ax = xa\}$.

(α) Δείξτε ότι το $C_G(a)$ είναι υποομάδα της G για κάθε $a \in G$.

(β) Αν η ομάδα G είναι πεπερασμένη δείξτε ότι $|G| = |C_G(a)| \cdot |C_a|$ για κάθε $a \in G$, όπου $C_a = \{xax^{-1} : x \in G\}$ είναι η κλάση συζυγίας του a που ορίστηκε στην Άσκηση 124.
(γ) Βρείτε όλες τις υποομάδες της μορφής $C_G(a)$, αν G είναι η ομάδα των συμμετριών του τετραγώνου.
(δ) Έστω ότι η ομάδα G είναι πεπερασμένη τάξης n. Δείξτε ότι το πλήθος των ζευγών (a, b) στοιχείων της G με $ab = ba$ είναι ίσο με mn, όπου m είναι το πλήθος των κλάσεων συζυγίας της G.

149. Το κέντρο $Z(G)$ μιας ομάδας G αποτελείται από όλα τα στοιχεία $x \in G$ για τα οποία ισχύει $ax = xa$ για κάθε $a \in G$.

(α) Δείξτε ότι το $Z(G)$ είναι υποομάδα της G.
(β) Δείξτε ότι το $Z(G)$ περιέχει την τομή των μη τετριμμένων υποομάδων της G.
(γ) Υπολογίστε το κέντρο της ομάδας των συμμετριών του κανονικού n-γώνου.

150. Για υποσύνολο H ομάδας G και $x \in G$ θέτουμε $xHx^{-1} = \{xax^{-1} : a \in H\}$.

(α) Αν το H είναι υποομάδα της G, δείξτε ότι το ίδιο ισχύει για το xHx^{-1} για κάθε $x \in G$. Κάθε τέτοια υποομάδα λέγεται *συζυγής* της H.
(β) Έστω υποομάδες H, K της G. Αν η K είναι συζυγής της H, δείξτε ότι η τάξη της K είναι ίση με εκείνη της H. Ισχύει το αντίστροφο;
(γ) Έστω $a, b \in G$. Αν τα a, b ανήκουν στην ίδια κλάση συζυγίας της G, δείξτε ότι η υποομάδα $C_G(b)$ που ορίστηκε στην Άσκηση 148 είναι συζυγής της $C_G(a)$. Ισχύει το αντίστροφο;

151. Έστω γνήσια υποομάδα H μιας πεπερασμένης ομάδας G.

(α) Δείξτε ότι το πλήθος των υποομάδων της G της μορφής xHx^{-1} με $x \in G$ είναι μικρότερο ή ίσο του δείκτη $[G : H]$.
(β) Δείξτε ότι υπάρχει στοιχείο της G που δεν είναι συζυγές με κανένα στοιχείο της υποομάδας H.

152. Δίνονται θετικός ακέραιος n και πρώτος αριθμός p. Πόσες υποομάδες τάξης p έχει μια ομάδα G τάξης n, αν $x^p = e$ για κάθε $x \in G$;

153. Δείξτε ότι για πεπερασμένη ομάδα G, οι ακόλουθες συνθήκες είναι ισοδύναμες:

(i) Η εξίσωση $x^2 = a$ έχει λύση στη G για κάθε $a \in G$.
(ii) Η εξίσωση $x^2 = a$ έχει μοναδική λύση στη G για κάθε $a \in G$.
(iii) Η τάξη της G είναι περιττός αριθμός.

154. Μια ομάδα G περιέχει στοιχεία a, b τάξης 3 για τα οποία το ab έχει τάξη 2.

(α) Δείξτε ότι η G δεν είναι αβελιανή.
(β) Ποια είναι η μικρότερη δυνατή τάξη της G;

155. Δίνεται ομάδα G τάξης ≥ 2 κάθε στοιχείο της οποίας διάφορο του ταυτοτικού $e \in G$ έχει τάξη p.

(α) Δείξτε ότι ο p είναι πρώτος αριθμός.
(β) Έστω ότι μεταξύ οποιωνδήποτε $p^2 - 1$ στοιχείων της G υπάρχουν p στοιχεία τα οποία ανά δύο μετατίθενται. Δείξτε ότι η ομάδα G είναι αβελιανή.

156. Δίνεται υποομάδα H της συμμετρικής ομάδας S_n που περιέχει μια αντιμετάθεση και έναν κύκλο μήκους n.

(α) Αν ο n είναι πρώτος αριθμός, δείξτε ότι $H = S_n$.
(β) Ισχύει το ίδιο χωρίς την υπόθεση ότι ο n είναι πρώτος;

157. Δίνονται ομάδα G και υποομάδα H αυτής.

(α) Δείξτε ότι οι αριστερές και οι δεξιές κλάσεις της H στη G έχουν όλες το ίδιο πλήθος στοιχείων.
(β) Δείξτε ότι το πλήθος των αριστερών κλάσεων της H στη G είναι ίσο με το πλήθος των δεξιών κλάσεων.

158. Δίνονται ομάδα G και υποομάδες H, K αυτής.

(α) Αν $H \subseteq K$, δείξτε ότι $[G : H] = [G : K][K : H]$.
(β) Δείξτε ότι για κάθε $a \in G$ το σύνολο $(aH) \cap K$ είναι κενό, ή ίσο με μια αριστερή κλάση της $K \cap H$ στην K.
(γ) Δείξτε ότι $[K : K \cap H] \leq [G : H]$.

159. Θεωρούμε υποομάδες H, K μιας ομάδας G. Βρείτε τις δυνατές τιμές του δείκτη $[G : K \cap H]$ στις εξής περιπτώσεις:

(α) $[G : K] = 2$ και $[G : H] = 3$.
(β) $[G : K] = [G : H] = 3$.

160. Δίνονται ομάδα G και υποομάδα της H πεπερασμένου δείκτη n.

(α) Δείξτε ότι για κάθε $x \in G$ υπάρχει $k \in \{1, 2, \ldots, n\}$ τέτοιο ώστε $x^k \in H$.
(β) Αν η ομάδα G είναι αβελιανή, δείξτε ότι $x^n \in H$ για κάθε $x \in G$.
(γ) Ισχύει το (β) χωρίς την υπόθεση ότι η G είναι αβελιανή;

161. Δείξτε ότι:

(α) Η προσθετική ομάδα $\mathbb{Q}$ δεν έχει μη τετριμμένες πεπερασμένες υποομάδες.
(β) Η προσθετική ομάδα $\mathbb{Q}$ δεν έχει γνήσιες υποομάδες πεπερασμένου δείκτη.
(γ) Η ομάδα $\mathbb{C}^\times$ δεν έχει γνήσιες υποομάδες πεπερασμένου δείκτη.

162. Δίνονται υποομάδες H, K μιας ομάδας G. Τα σύνολα της μορφής $HxK = \{axb : a \in H,\ b \in K\}$ για $x \in G$ λέγονται *διπλές κλάσεις* των H, K στη G.

(α) Δείξτε ότι διακεκριμένες διπλές κλάσεις των H, K στη G είναι ξένες μεταξύ τους και ότι η ένωση των κλάσεων αυτών είναι ίση με G.
(β) Βρείτε τις διπλές κλάσεις των H, K στη G, αν $G = \mathrm{GL}_2(\mathbb{F})$ για κάποιο σώμα $\mathbb{F}$ και $H = K$ είναι η υποομάδα των 2×2 αντιστρέψιμων άνω τριγωνικών πινάκων με στοιχεία από το $\mathbb{F}$.

Κυκλικές Ομάδες

163. Ποιες από τις ακόλουθες ομάδες είναι κυκλικές;

(α) $U(\mathbb{Z}_{50})$.
(β) $U(\mathbb{Z}_{65})$.
(γ) $\mathrm{SL}_n(\mathbb{F})$, όπου $\mathbb{F}$ είναι πεπερασμένο σώμα.
(δ) $\mathrm{GL}_n(\mathbb{F})$, όπου $\mathbb{F}$ είναι πεπερασμένο σώμα.

164. Δίνεται θετικός ακέραιος n και η ομάδα $G = U(\mathbb{Z}_{2^n})$.

(α) Βρείτε όλα τα στοιχεία τάξης 2 της G.
(β) Αν $n \geq 3$, δείξτε ότι η G δεν είναι κυκλική.
(γ) Συνάγετε ότι αν $n \geq 3$, τότε $a^{2^{n-2}} \equiv 1 \pmod{2^n}$ για κάθε περιττό ακέραιο a.

165. Θεωρούμε σώμα $\mathbb{F}_q$ με q στοιχεία και την ομάδα $G = U(R)$ των αντιστρέψιμων στοιχείων του δακτυλίου $R = \mathbb{F}_q[x]/\langle x^2 \rangle$.

(α) Υπολογίστε την τάξη της G.
(β) Για ποιες δυνάμεις πρώτων αριθμών q είναι η ομάδα G κυκλική;

166. Θεωρούμε την ομάδα $G = U(\mathbb{Z}_2[x]/\langle x^n \rangle)$.

(α) Υπολογίστε την τάξη της G.
(β) Για ποιους θετικούς ακεραίους n είναι η ομάδα G κυκλική;

167. Πόσα ιδεώδη έχει ο δακτύλιος $\mathbb{Z}_n$;

168. Θεωρούμε κυκλική ομάδα G τάξης n.

(α) Έστω d ένας θετικός διαιρέτης του n. Πόσα στοιχεία τάξης d έχει η G;
(β) Δείξτε ότι

$$\sum_{d\,|\,n} \varphi(d) \;=\; n$$

για κάθε θετικό ακέραιο n, όπου στο άθροισμα το d διατρέχει όλους τους θετικούς διαιρέτες d του n.

169. Θεωρούμε κυκλική ομάδα G τάξης n, θετικό διαιρέτη d του n και $x \in G$.

(α) Έστω H η μοναδική υποομάδα τάξης d της G. Δείξτε ότι η τάξη του x διαιρεί το d αν και μόνο αν $x \in H$.
(β) Συνάγετε ότι υπάρχουν ακριβώς d στοιχεία της ομάδας G, η τάξη των οποίων διαιρεί το d.
(γ) Πόσα στοιχεία άρτιας τάξης έχει η G;

170. Δίνεται πεπερασμένη ομάδα G.

(α) Αν για κάθε θετικό ακέραιο d υπάρχουν το πολύ d στοιχεία $x \in G$ με $x^d = e$, δείξτε ότι η ομάδα G είναι κυκλική.
(β) Συνάγετε ότι η υποομάδα $E_n = \{z \in \mathbb{C} : z^n = 1\}$ της $\mathbb{C}^\times$ είναι κυκλική για κάθε θετικό ακέραιο n.
(γ) Συνάγετε ότι η πολλαπλασιαστική ομάδα $\mathbb{F}^\times$ είναι κυκλική για κάθε πεπερασμένο σώμα $\mathbb{F}$.

171. Δείξτε ότι η πολλαπλασιαστική ομάδα $\mathbb{F}^\times$ ενός σώματος $\mathbb{F}$ είναι κυκλική αν και μόνο αν το σώμα $\mathbb{F}$ είναι πεπερασμένο.

172. Ένα στοιχείο a μιας ομάδας G λέγεται *τέλειο τετράγωνο* αν ισχύει $a = x^2$ για κάποιο $x \in G$.

(α) Αν G είναι κυκλική ομάδα και τα $a, b \in G$ δεν είναι τέλεια τετράγωνα, δείξτε ότι το γινόμενο ab είναι τέλειο τετράγωνο.
(β) Ισχύει το ίδιο χωρίς την υπόθεση ότι η ομάδα G είναι κυκλική;

Ομομορφισμοί, Κανονικές Υποομάδες και Ομάδα Πηλίκο

Υπενθυμίζουμε ότι με $\mathbb{F}^\times$ συμβολίζεται η πολλαπλασιαστική ομάδα των μη μηδενικών στοιχείων ενός σώματος $\mathbb{F}$.

173. Βρείτε όλους τους ενδομορφισμούς $\varphi : \mathbb{Q} \to \mathbb{Q}$ της προσθετικής ομάδας $\mathbb{Q}$. Ποιοι από αυτούς είναι αυτομορφισμοί;

174. Θεωρούμε ομάδα G και την απεικόνιση $\varphi : G \to G$ με $\varphi(x) = x^2$ για $x \in G$.

(α) Δείξτε ότι η φ είναι ενδομορφισμός της G αν και μόνο αν η G είναι αβελιανή.
(β) Για ποιες πεπερασμένες ομάδες G η απεικόνιση φ είναι αυτομορφισμός της G;

175. Έστω ομομορφισμός ομάδων $\varphi : G \to K$.

(α) Αν x, y είναι συζυγή στοιχεία της G, δείξτε ότι τα $\varphi(x)$ και $\varphi(y)$ είναι συζυγή στοιχεία της K.
(β) Θεωρούμε τα στοιχεία $u = (1\ 2\ 3\ 4)$ και $v = (1\ 2\ 4\ 3)$ της S_4. Υπάρχει ομομορφισμός ομάδων $\varphi : S_4 \to S_4$ με $\varphi(u) = (1\ 2)$ και $\varphi(v) = (1\ 3)(2\ 4)$;

176. Θεωρούμε ομάδα G με ταυτοτικό στοιχείο e, ομομορφισμό ομάδων $\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to G$ και τα στοιχεία $a = \varphi(\bar{1}, \bar{0})$ και $b = \varphi(\bar{0}, \bar{1})$ της G.

(α) Δείξτε ότι $a^2 = b^2 = e$ και $ab = ba$.
(β) Αντιστρόφως, δείξτε ότι για κάθε ζεύγος (a, b) στοιχείων της G με $a^2 = b^2 = e$ και $ab = ba$, υπάρχει μοναδικός ομομορφισμός ομάδων $\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to G$ τέτοιος ώστε $\varphi(\bar{1}, \bar{0}) = a$ και $\varphi(\bar{0}, \bar{1}) = b$.
(γ) Πόσοι ομομορφισμοί ομάδων $\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to S_3$ υπάρχουν συνολικά;

177. Έστω κυκλική ομάδα G τάξης n με γεννήτορα a και ομάδα K.

(α) Για $b \in K$, δείξτε ότι υπάρχει ομομορφισμός ομάδων $\varphi : G \to K$ με $\varphi(a) = b$ αν και μόνο αν η τάξη του b διαιρεί το n.
(β) Συνάγετε ότι αν η K είναι κυκλική τάξης m, τότε υπάρχουν ακριβώς $\mu\kappa\delta(n, m)$ ομομορφισμοί ομάδων $\varphi : G \to K$.

178. Θεωρούμε την αντιμετάθεση $t = (n+1\ \ n+2) \in S_{n+2}$ και ορίζουμε την απεικόνιση $\varphi : S_n \to S_{n+2}$ θέτοντας

$$\varphi(\sigma) = \begin{cases} \sigma, & \text{αν η } \sigma \text{ είναι άρτια} \\ \sigma \cdot t, & \text{αν η } \sigma \text{ είναι περιττή} \end{cases}$$

για $\sigma \in S_n$, όπου έχουμε ταυτίσει κάθε μετάθεση $\sigma \in S_n$ με την επέκτασή της με $\sigma(n+1) = n+1$ και $\sigma(n+2) = n+2$ στην S_{n+2}.

(α) Δείξτε ότι η φ είναι μονομορφισμός ομάδων.
(β) Συνάγετε ότι η S_n είναι ισόμορφη με μια υποομάδα της εναλλάσσουσας ομάδας A_{n+2}.

179. Θεωρούμε ομάδα G και για $g \in G$ θεωρούμε την απεικόνιση $\psi_g : G \to G$ που ορίζεται θέτοντας $\psi_g(x) = gxg^{-1}$ για κάθε $x \in G$. Θέτουμε $\mathrm{Inn}(G) = \{\psi_g : g \in G\}$.

(α) Δείξτε ότι η ψ_g είναι αυτομορφισμός της G για κάθε $g \in G$.
(β) Δείξτε ότι $\psi_g \circ \psi_h = \psi_{gh}$ και ότι $(\psi_g)^{-1} = \psi_{g^{-1}}$ για όλα τα $g, h \in G$.

(γ) Συνάγετε ότι το σύνολο $\mathrm{Inn}(G)$ είναι υποομάδα της ομάδας $\mathrm{Aut}(G)$ των αυτομορφισμών της G.

180. Δίνεται υποομάδα H μιας ομάδας G. Θεωρούμε το σύνολο $X = \{xH : x \in G\}$ των αριστερών κλάσεων της H στη G και την ομάδα $S(X)$ των μεταθέσεων του X.

(α) Δείξτε ότι για κάθε $g \in G$, η απεικόνιση $\varphi_g : X \to X$ με $\varphi_g(xH) = (gx)H$ για $x \in G$ είναι είναι μια καλά ορισμένη μετάθεση του συνόλου X.
(β) Δείξτε ότι η απεικόνιση $\varphi : G \to S(X)$ που ορίζεται θέτοντας $\varphi(g) = \varphi_g$ για κάθε $g \in G$ είναι ομομορφισμός ομάδων, ο πυρήνας του οποίου περιέχεται στην H.

181. Βρείτε όλους τους ομομορφισμούς ομάδων $\varphi : S_n \to \mathbb{C}^\times$.

182. Δίνεται πεπερασμένο σώμα $\mathbb{F}_q$ με q στοιχεία.

(α) Δείξτε ότι η απεικόνιση της ορίζουσας $\det : \mathrm{GL}_n(\mathbb{F}_q) \to \mathbb{F}_q^\times$ είναι επιμορφισμός ομάδων.
(β) Συνάγετε ότι το σύνολο $\mathrm{SL}_n(\mathbb{F}_q)$ των $n \times n$ πινάκων ορίζουσας 1 με στοιχεία από το $\mathbb{F}_q$ είναι κανονική υποομάδα της $\mathrm{GL}_n(\mathbb{F}_q)$ και υπολογίστε την τάξη της.

183. Βρείτε όλες τις κανονικές υποομάδες της συμμετρικής ομάδας S_4.

184. Βρείτε όλους τους ακεραίους $n \geq 2$ για τους οποίους η συμμετρική ομάδα S_n είναι ισόμορφη με το ευθύ γινόμενο της S_{n-1} με την κυκλική ομάδας τάξης n.

185. Θεωρούμε ομομορφισμό ομάδων $\varphi : G \to K$ και θέτουμε, ως συνήθως, $\varphi(H) = \{\varphi(x) : x \in H\}$ και $\varphi^{-1}(N) = \{x \in G : \varphi(x) \in N\}$ για $H \subseteq G$ και $N \subseteq K$.

(α) Δείξτε ότι το $\varphi(H)$ είναι υποομάδα της K για κάθε υποομάδα H της G.
(β) Δείξτε ότι το $\varphi^{-1}(N)$ είναι υποομάδα της G για κάθε υποομάδα N της K.
(γ) Αν ο $\varphi : G \to K$ είναι επιμορφισμός ομάδων, δείξτε ότι το $\varphi(H)$ είναι κανονική υποομάδα της K για κάθε κανονική υποομάδα H της G. Ισχύει το ίδιο για τυχαίο ομομορφισμό ομάδων $\varphi : G \to K$;
(δ) Δείξτε ότι το $\varphi^{-1}(N)$ είναι κανονική υποομάδα της G για κάθε κανονική υποομάδα N της K.

186. Δίνεται η υποομάδα

$$G = \left\{ \begin{pmatrix} x & y \\ 0 & 1/x \end{pmatrix} : x, y \in \mathbb{R},\ x \neq 0 \right\}$$

της $\mathrm{GL}_2(\mathbb{R})$ και η υποομάδα

$$N = \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} : y \in \mathbb{R} \right\}$$

της G.

(α) Δείξτε ότι η N είναι κανονική υποομάδα της G.
(β) Βρείτε μια κανονική γνήσια υποομάδα της G που περιέχει γνήσια τη N.
(γ) Δείξτε ότι δεν υπάρχει μη τετριμμένη κανονική υποομάδα της G που περιέχεται γνήσια στη N.

187. Ποιες από τις ακόλουθες προτάσεις είναι αληθείς;

(α) Αν N είναι κανονική υποομάδα μιας ομάδας G, τότε κάθε κανονική υποομάδα της N είναι κανονική υποομάδα της G.
(β) Αν N είναι κυκλική υποομάδα μιας ομάδας G η οποία είναι κανονική υποομάδα της G, τότε κάθε υποομάδα της N είναι κανονική υποομάδα της G.

188. Δίνεται περιττός ακέραιος n και πεπερασμένη ομάδα G με υποομάδα N τάξης 2 και υποομάδα K τάξης n.

(α) Δείξτε ότι $|G| \geq 2n$.
(β) Δώστε παράδειγμα τέτοιας ομάδας τάξης $2n$, η οποία δεν είναι κυκλική.
(γ) Αν $|G| = 2n$, η υποομάδα N της G είναι κανονική και ο n είναι πρώτος, δείξτε ότι η ομάδα G είναι κυκλική.

189. Αν H, K είναι κανονικές υποομάδες μιας ομάδας G και $H \cap K = \{e\}$, δείξτε ότι $ab = ba$ για όλα τα $a \in H$ και $b \in K$.

190. Έστω μη τετριμμένη, πεπερασμένη ομάδα G και έστω p ο μικρότερος πρώτος διαιρέτης της τάξης της G. Δείξτε ότι κάθε υποομάδα H της G με δείκτη $[G : H] = p$ είναι κανονική υποομάδα της G.

191. Δίνονται ομάδα G και το υποσύνολο $N = \{(x, x) : x \in G\}$ της ομάδας $G \times G$.

(α) Δείξτε ότι το N είναι υποομάδα της $G \times G$.
(β) Περιγράψτε τις αριστερές και τις δεξιές κλάσεις της N στη $G \times G$.
(γ) Δείξτε ότι η υποομάδα N της G είναι κανονική αν και μόνο αν η G είναι αβελιανή.

(δ) Αν η G είναι αβελιανή, δείξτε ότι η ομάδα $(G \times G)/N$ είναι ισόμορφη με τη G.

192. Δίνονται υποομάδες H, N μιας ομάδας G, τέτοιες ώστε $G = \{ab : a \in H, b \in N\}$ και $H \cap N = \{e\}$.

(α) Δείξτε ότι $|G| = |H| \cdot |N|$.
(β) Αν η N είναι κανονική υποομάδα της G, δείξτε ότι η ομάδα πηλίκο G/N είναι ισόμορφη με την H.
(γ) Αν οι H, N είναι και οι δύο κανονικές υποομάδες της G, δείξτε ότι η G είναι ισόμορφη με την $H \times N$.
(δ) Βρείτε παράδειγμα στο οποίο η N είναι κανονική υποομάδα της G, αλλά η G δεν είναι ισόμορφη με την $H \times N$.

193. Θεωρούμε την υποομάδα $\mathrm{Inn}(G)$ (Άσκηση 179) της ομάδας $\mathrm{Aut}(G)$ των αυτομορφισμών μιας ομάδας G.

(α) Δείξτε ότι η $\mathrm{Inn}(G)$ είναι κανονική υποομάδα της $\mathrm{Aut}(G)$.
(β) Δείξτε ότι η $\mathrm{Inn}(G)$ είναι ισόμορφη με την ομάδα πηλίκο $G/Z(G)$, όπου με $Z(G)$ συμβολίζεται το κέντρο (Άσκηση 149) της ομάδας G.

194. Δίνεται η υποομάδα

$$H = \left\{ m\begin{pmatrix} 3 \\ 2 \end{pmatrix} + n\begin{pmatrix} 1 \\ 3 \end{pmatrix} : m, n \in \mathbb{Z} \right\}$$

της προσθετικής ομάδας $\mathbb{Z}^2$ και η απεικόνιση $\varphi : \mathbb{Z}^2 \to \mathbb{Z}_7$ που ορίζεται θέτοντας

$$\varphi\begin{pmatrix} a \\ b \end{pmatrix} = 2\bar{a} - 3\bar{b} \in \mathbb{Z}_7$$

για $a, b \in \mathbb{Z}$.

(α) Δείξτε ότι η φ είναι επιμορφισμός ομάδων, ο πυρήνας του οποίου περιέχει την H.
(β) Δείξτε ότι $\ker(\varphi) = H$.
(γ) Συνάγετε ότι η ομάδα πηλίκο $\mathbb{Z}^2/H$ είναι ισόμορφη με τη $\mathbb{Z}_7$.

195. Ποιες από τις ακόλουθες προτάσεις είναι αληθείς;

(α) Υπάρχουν πεπερασμένη ομάδα G και μη τετριμμένη κανονική υποομάδα N της G για τις οποίες η ομάδα πηλίκο G/N είναι ισόμορφη με τη G.
(β) Υπάρχουν ομάδα G και μη τετριμμένη κανονική υποομάδα N της G για τις οποίες η ομάδα πηλίκο G/N είναι ισόμορφη με τη G.

196. Αποφανθείτε αν είναι αληθής η παρακάτω πρόταση: Αν N είναι κανονική υποομάδα πεπερασμένου δείκτη n μιας ομάδας G, τότε $x^n \in N$ για κάθε $x \in G$.

197. Δείξτε ότι η μόνη γνήσια κανονική υποομάδα N της συμμετρικής ομάδας S_n για την οποία η ομάδα πηλίκο S_n/N είναι αβελιανή, είναι η εναλλάσσουσα υποομάδα A_n.

198. Έστω υποομάδα H πεπερασμένου δείκτη μιας ομάδας G. Δείξτε ότι υπάρχει κανονική υποομάδα πεπερασμένου δείκτη της G η οποία περιέχεται στην H.

199. Δείξτε ότι η ομάδα $\mathrm{Aut}(S_n)$ των αυτομορφισμών της συμμετρικής ομάδας S_n είναι ισόμορφη με την S_n για κάθε θετικό ακέραιο n με $n \neq 2, 6$.

Διάφορα Προβλήματα

200. Δίνεται $n \times n$ πίνακας A με στοιχεία ακέραιους αριθμούς και ορίζουσα $\det(A) = 1$.

(α) Δείξτε ότι για κάθε θετικό ακέραιο m υπάρχουν θετικός ακέραιος k και $n \times n$ πίνακας C με στοιχεία ακέραιους αριθμούς, τέτοιοι ώστε $A^k = I + mC$.

(β) Έστω $B = P^{-1}AP$, όπου P είναι $n \times n$ πίνακας με στοιχεία ακέραιους αριθμούς και $\det(P) \neq 0$. Συνάγετε ότι υπάρχει θετικός ακέραιος k για τον οποίο όλα τα στοιχεία του πίνακα B^k είναι ακέραιοι αριθμοί.

Υποδείξεις - Λύσεις

(1) Παρατηρήστε ότι ο αριθμός μηδέν είναι ουδέτερο στοιχείο της πρώτης πράξης (πρόσθεσης) αλλά ότι κανένα άλλο στοιχείο του $\mathbb{N}$ δεν έχει αντίθετο, οπότε η απάντηση στο ερώτημα είναι αρνητική. Δείξτε μάλιστα ότι οι δύο προτεινόμενες πράξεις στο $\mathbb{N}$ επαληθεύουν όλα τα αξιώματα του δακτυλίου, εκτός από την ύπαρξη του αντιθέτου στοιχείου.

(2) Για το (α) παρατηρήστε ότι για $a, b, c \in R$ έχουμε $(a \circ b) \circ c = (ba) \circ c = c(ba) = (cb)a = a \circ (cb) = a \circ (b \circ c)$ και επαληθεύστε ομοίως ότι $(a+b) \circ c = a \circ c + b \circ c$ και ότι $c \circ (a+b) = c \circ a + c \circ b$. Τα (β), (γ) και (δ) αφήνονται στον αναγνώστη.

(3) Δείξτε ότι ο δακτύλιος των 2×2 άνω τριγωνικών πινάκων με στοιχεία από το $\mathbb{Z}_2$ έχει τις ζητούμενες ιδιότητες.

(4) Για το (α) χρησιμοποιήστε επαγωγή στο n (αυτή είναι η συνήθης αλγεβρική απόδειξη του Διωνυμικού Θεωρήματος). Για το (β) δείξτε ότι ο συντελεστής $\binom{p}{k}$ διαιρείται με το p για κάθε πρώτο αριθμό p και $k \in \{1, 2, \ldots, p-1\}$ και εφαρμόστε το (α).

(5) Αναπτύσσοντας το $(a+a)^2$ και χρησιμοποιώντας τη δοσμένη σχέση $a^2 = a$, συνάγετε πρώτα από την ισότητα $(a+a)^2 = a + a$ ότι $-a = a$ για κάθε $a \in R$. Εργαζόμενοι με παρόμοιο τρόπο, συνάγετε έπειτα από την ισότητα $(a+b)^2 = a + b$ ότι $ab = -ba$ και συμπεράνετα ότι $ab = ba$ για όλα τα $a, b \in R$.

(6) Για το (α), υποθέστε ότι το a έχει αριστερό αντίστροφο c και δεξιό αντίστροφο b, οπότε $ca = ab = 1_R$. Παρατηρήστε τότε ότι $c = c \cdot 1_R = c \cdot (ab) = (ca) \cdot b = 1_R \cdot b = b$ και συνάγετε ότι το είναι a αντιστρέψιμο στοιχείο του R με αντίστροφο $a^{-1} = b = c$. Τα αντίστροφο είναι τετριμμένο. Το (β) αφήνεται στον αναγνώστη. Για το (γ), επαληθεύστε ότι το στοιχείο $b^{-1}a^{-1}$ είναι το αντίστροφο του ab.

(7) Δείξτε ότι οι δύο προτάσεις είναι αληθείς ως εξής. Για το (α) θεωρήστε δεξιό αντίστροφο b του a, οπότε $ab = 1_R$. Παρατηρήστε ότι $a^n b^n = a^{n-1}(ab)\, b^{n-1} = a^{n-1} \cdot 1_R \cdot b^{n-1} = a^{n-1} b^{n-1}$ και εφαρμόστε επαγωγή στο n για να δείξετε ότι το b^n είναι δεξιό αντίστροφο του a^n για κάθε θετικό ακέραιο n. Για το (β) εργαστείτε ομοίως, ή εφαρμόστε το (α) στο δακτύλιο της Άσκησης 2 και χρησιμοποιήστε το ερώτημα (γ) της ίδιας άσκησης.

(8) Έστω b ένα δεξιό αντίστροφο του a, οπότε $ab = 1_R$. Για τη συνεπαγωγή (i) $\Rightarrow$ (ii), υποθέστε ότι $a \in U(R)$ και ότι το $c \in R$ είναι επίσης δεξιό αντίστροφο του a, δηλαδή ότι $ac = 1_R$. Δείξτε ότι $b = c$ παρατηρώντας ότι $a(b-c) = 0_R$ και πολλαπλασιάζοντας την ισότητα αυτή από αριστερά με a^{-1}. Για να δείξετε ότι (ii) $\Rightarrow$ (iv), υποθέστε ότι το a είναι αριστερός μηδενοδιαιρέτης στο R, οπότε υπάρχει μη μηδενικό στοιχείο $u \in R$ με $au = 0_R$. Παρατηρήστε ότι $ab = a(b+u) = 1_R$ και συμπεράνετε ότι το a έχει δύο διαφορετικούς δεξιούς αντιστρόφους στο R. Για τη συνεπαγωγή (iv) $\Rightarrow$ (i), υποθέστε ότι το a δεν είναι αριστερός μηδενοδιαιρέτης στο R. Παρατηρήστε ότι $a(ba - 1_R) = a(ba) - a = (ab)a - a = 1_R \cdot a - a = 0_R$. Συμπεράνετε ότι $ba = 1_R$ και ότι το a είναι αντιστρέψιμο στοιχείο του R με αντίστροφο στοιχείο το b. Για τη συνεπαγωγή (iii) $\Rightarrow$ (i), δείξτε πρώτα ότι το στοιχείο $b_n := b + (ba - 1_R)a^n$ είναι δεξιό αντίστροφο του a για κάθε θετικό ακέραιο n. Υποθέτοντας ότι το a έχει πεπερασμένου πλήθους δεξιούς αντιστρόφους στο R, συμπεράνετε ότι υπάρχουν ακέραιοι $1 \leq n < m$ τέτοιοι ώστε $b_n = b_m$, οπότε $(ba - 1_R)a^n = (ba - 1_R)a^m$. Πολλαπλασιάστε έπειτα από δεξιά αυτή την ισότητα με b^m για να καταλήξετε στην ισότητα $ba = 1_R$. Η αντίστροφη συνεπαγωγή (i) $\Rightarrow$ (iii) είναι τετριμμένη.

(9) Υποθέστε ότι το $1_R - ab$ είναι αντιστρέψιμο στοιχείο του R με αντίστροφο $x \in R$, δηλαδή ότι ισχύει $(1_R - ab)x = x(1_R - ba) = 1_R$ στο R, και δείξτε ότι $(1_R - ba)y = y(1_R - ba) = 1_R$ για $y = 1_R + bxa \in R$.

(10) Για το (α) παρατηρήστε ότι ισχύει $(a, b)(c, d) = (c, d)(a, b)$ στο $R \times S$ αν και μόνο αν $ac = ca$ στο R και $bd = db$ στο S και ότι το (a, b) είναι μοναδιαίο στοιχείο στο $R \times S$ αν και μόνο αν το a είναι μοναδιαίο στοιχείο στο R και το b είναι μοναδιαίο στοιχείο στο S. Για το (β) δείξτε ότι το (a, b) είναι αντίστροφο του (c, d) στο $R \times S$ αν και μόνο αν το a είναι αντίστροφο του c στο R και το b είναι αντίστροφο του d στο S και συμπεράνετε ότι $(a, b) \in U(R \times S)$ αν και μόνο αν $a \in U(R)$ και $b \in U(S)$. Για το (γ) παρατηρήστε ότι ισχύει $(a, 0_S)(0_R, d) = (0_R, 0_S)$ στο $R \times S$ και συμπεράνετε ότι ο $R \times S$ δεν έχει μηδενοδιαιρέτες αν και μόνο αν ένας τουλάχιστον από τους R και S είναι ο μηδενικός δακτύλιος και ο άλλος δεν έχει μηδενοδιαιρέτες.

(11) Για το (α) δείξτε ότι $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$ ως εξής. Θεωρήστε αντιστρέψιμο στοιχείο $x = a + bi$ του $\mathbb{Z}[i]$, έστω με αντίστροφο $y = c + di$. Από την ισότητα $xy = 1$ συμπεράνετε ότι $1 = |xy|^2 = |x|^2|y|^2 = (a^2 + b^2)(c^2 + d^2)$ (όπου με $|z|$ συμβολίζουμε το μέτρο του μιγαδικού αριθμού z) και επομένως ότι $a^2 + b^2 = c^2 + d^2 = 1$. Συμπεράνετε ότι $x \in \{1, -1, i, -i\}$ και ότι $U(\mathbb{Z}[i]) \subseteq \{1, -1, i, -i\}$. Ο αντίστροφος εγκλεισμός είναι προφανής. Για το (β), θεωρήστε τον υποδακτύλιο $\mathbb{Z}[2i] = \{a + 2bi : a, b \in \mathbb{Z}\}$ του $\mathbb{Z}[i]$ και χρησιμοποιήστε το αποτέλεσμα του ερωτήματος (α).

(12) Το (α) αφήνεται στον αναγνώστη. Για το (β) παρατηρήστε ότι το $5 + 2\sqrt{6}$ είναι αντιστρέψιμο στοιχείο του R (με αντίστροφο $5 - 2\sqrt{6}$) και συμπεράνετε ότι το $(5 + 2\sqrt{6})^n$ είναι αντιστρέψιμο στοιχείο του R για κάθε ακέραιο n.

(13) Το (α) αφήνεται στον αναγνώστη. Για το (β) υποθέστε ότι R είναι μη μηδενικός υποδακτύλιος του $\mathbb{Z}$ και θεωρήστε τον ελάχιστο θετικό ακέραιο m που ανήκει στο R. Παρατηρήστε ότι $m\mathbb{Z} \subseteq R$ και δείξτε τον αντίστροφο εγκλεισμό θεωρώντας την Ευκλείδεια διαίρεση τυχαίου στοιχείου $a \in R$ με το m.

(14) Το (α) αφήνεται στον αναγνώστη. Για το (β) θυμηθείτε ότι αν A είναι αντιστρέψιμο στοιχείο του $M_n(\mathbb{F})$, τότε $\det(A) \neq 0$ και παρατηρήστε ότι αν $a^2 + b^2 \neq 0$ στο $\mathbb{F}$, τότε ο πίνακας

$$\frac{1}{a^2 + b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

ανήκει στο R και αποτελεί αντίστροφο του $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Για το (γ), συμπεράνετε από το (β) ότι το R είναι σώμα αν και μόνο αν στο $\mathbb{F}$ ισχύει $a^2 + b^2 = 0 \Rightarrow a = b = 0$. Συνάγετε ότι το R είναι σώμα αν $\mathbb{F} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{Z}_3\}$, ενώ δεν είναι αν $\mathbb{F} \in \{\mathbb{C}, \mathbb{Z}_5\}$. Για το (δ) χρησιμοποιήστε γνώσεις από τη θεωρία αριθμών για να δείξετε ότι για $\mathbb{F} = \mathbb{Z}_p$, το R είναι σώμα αν και μόνο αν για τον πρώτο p ισχύει $p \equiv 3 \pmod 4$.

(15) Για το (α) παρατηρήστε ότι $0_R \in S$ και δείξτε ότι αν $\alpha x = x\alpha$ και $\alpha y = y\alpha$ για κάποια $x, y \in R$, τότε $\alpha(x + y) = (x + y)\alpha$ και $\alpha(xy) = (xy)\alpha$. Για το (β), θέτοντας $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R$, δείξτε πρώτα ότι ισχύει $\alpha x = x\alpha$ αν και μόνο αν $a = d$ και $c = 0$ και συμπεράνετε ότι

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{F} \right\}$$

και ότι

$$U(S) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a \in \mathbb{F} \setminus \{0\}, b \in \mathbb{F} \right\}.$$

Τέλος, θέτοντας

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

με $a, b, c, d \in \mathbb{F}$, δείξτε ότι $xy = yx$ και ότι ισχύει $xy = 0_S$ αν και μόνο αν $a = 0$ ή $c = 0$. Συμπεράνετε ότι ο δακτύλιος S είναι μεταθετικός, ότι οι μηδενοδιαιρέτες του S είναι οι πίνακες $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$ με $b \in \mathbb{F}\setminus\{0\}$ και ότι το S δεν είναι ακέραια περιοχή. Για το (γ) θεωρήστε το δακτύλιο $R = M_3(\mathbb{F})$ και το στοιχείο του

$$\alpha = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

(16) Για το (α) εργασθείτε όπως στην Άσκηση 15 (α). Για το (β) δείξτε ότι ισχύει $(\alpha,\beta)(x,y) = (x,y)(\alpha,\beta)$ στο $R \times S$ αν και μόνο αν $\alpha x = x\alpha$ και $\beta y = y\beta$ και συμπεράνετε ότι $(x,y) \in C(R \times S)$ αν και μόνο αν $x \in C(R)$ και $y \in C(S)$. Για τα (γ) και (ε), θεωρήστε τον υποδακτύλιο

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : \ a, b \in \mathbb{F} \right\}$$

του $M_2(\mathbb{F})$. Δείξτε ότι ο R έχει τις ζητούμενες ιδιότητες στο (γ) για κάθε σώμα (ή ακόμη, κάθε δακτύλιο με μονάδα) $\mathbb{F}$ και τις ζητούμενες ιδιότητες στο (ε) για $\mathbb{F} = \mathbb{Z}_2$. Για το (δ), δείξτε ότι τέτοιο παράδειγμα είναι ο δακτύλιος $M_2(\mathbb{Z}_2)$.

(17) Για το (α) παρατηρήστε ότι $a^{-1} = a \Leftrightarrow a^2 = 1_R \Leftrightarrow (a - 1_R)(a + 1_R) = 0_R$ και συμπεράνετε ότι τα μόνα τέτοια στοιχεία του $U(R)$ είναι το 1_R και το -1_R. Για το (β) παρατηρήστε ότι το $U(R)$ διαμερίζεται από τα υποσύνολά του της μορφής $\{a, a^{-1}\}$ και συνάγετε από το (α) ότι το $U(R)$ έχει περιττό πλήθος στοιχείων αν και μόνο $-1_R = 1_R$.

(18) Παρατηρήστε ότι $ab \neq 0_R$ και χρησιμοποιώντας την ισότητα $(ab)x = a(bx)$, δείξτε ότι $(ab)x = 0_R \Rightarrow x = 0_R$ για $x \in R$.

(19) Έστω μη μηδενοδιαιρέτης $a \in R\setminus\{0_R\}$. Θα δείξουμε ότι $a \in U(R)$. Θεωρούμε την απεικόνιση $f : R \to R$ με $f(x) = ax$ για $x \in R$. Από την υπόθεση ότι το a δεν είναι αριστερός μηδε-νοδιαιρέτης στο R προκύπτει ότι η f είναι 1–1. Αφού το R είναι πεπερασμένο σύνολο, έπεται ότι η f είναι και επί. Επομένως, υπάρχει $x \in R$ τέτοιο ώστε $ax = 1_R$, δηλαδή το a έχει δεξιό αντίστροφο στο R. Με παρόμοιο τρόπο δείχνουμε ότι το a έχει και αριστερό αντίστροφο στο R. Από την Άσκηση 6 (α) έπεται ότι το a είναι αντιστρέψιμο στοιχείο του R.

(20) Για το (α) παρατηρήστε ότι αν $bu = 0_R$ με $u \in R\setminus\{0_R\}$, τότε $(ab)u = a(bu) = a \cdot 0_R = 0_R$. Το (β) έπεται από το (α). Έστω τώρα B το σύνολο των αριστερών μηδενοδιαιρετών του R και έστω $X = R\setminus(B \cup \{0_R\})$. Υποθέτοντας ότι το B έχει πεπερασμένο και μη μηδενικό πλήθος στοιχείων, έστω n, αρκεί για το (γ) να δείξουμε ότι το σύνολο X είναι πεπερασμένο. Θεωρούμε τυχαίο στοιχείο $b \in B$ και παρατηρούμε ότι, λόγω του (β), ορίζεται η απεικόνιση $f : X \to B$ με $f(x) = xb$ για $x \in X$. Παρατηρούμε επίσης ότι αν $f(x) = f(y)$ για κάποια $x, y \in X$, τότε $(x - y)b = 0_R$ και επομένως $x - y \in B \cup \{0_R\}$. Συμπεραίνουμε ότι η f λαμβάνει κάθε τιμή στο B το πολύ $n + 1$ φορές και συνεπώς ότι το πλήθος των στοιχείων του X δεν υπερβαίνει το $n(n + 1)$. Από αυτό έπεται το ζητούμενο.

(21) Για το (α) παρατηρήστε ότι τα στοιχεία $x, x^2, x^3, \ldots$ του R είναι πεπερασμένα σε πλήθος. Για το (β) υποθέστε ότι $R = \{x_1, x_2, \ldots, x_q\}$ και θεωρήστε το δακτύλιο γινόμενο $S = R^q := R \times R \times \cdots \times R$ (όπου το πλήθος των παραγόντων είναι ίσο με q). Παρατηρήστε ότι ο S είναι επίσης πεπερασμένος δακτύλιος και εφαρμόστε το (α) στο στοιχείο $x = (x_1, x_2, \ldots, x_q) \in S$.

(22) Για το (α) υποθέστε ότι $a^n = b^m = 0_R$. Χρησιμοποιώντας την Άσκηση 4 (α), δείξτε ότι $(a+b)^{n+m-1} = 0_R$. Για το (β) παρατηρήστε ότι $(ab)^p = a^p b^p$ για κάθε θετικό ακέραιο p. Για το (δ) υποθέστε ότι $b^m = 0_R$ και δείξτε ότι το στοιχείο $1_R - b + b^2 - \cdots + (-b)^{m-1}$ του R είναι αντίστροφο του $1_R + b$. Για το (γ) παρατηρήστε ότι $a + b = a\,(1_R + a^{-1}b)$ και συνάγετε το ζητούμενο από τα (β) και (δ). Για το (ε), δείξτε ότι κανένα από τα (α), (β), (γ) δεν ισχύει χωρίς την υπόθεση $ab = ba$ θεωρώντας το δακτύλιο $R = M_2(\mathbb{Z})$ και θέτοντας

$$a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

για τα (α) και (β), και

$$a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}$$

για το (γ).

(23) Για το (α), πολλαπλασιάζοντας από αριστερά και από δεξιά την ισότητα $\lambda AB + \mu BA = 1_R$ με A, αφαιρώντας κατά μέλη, παρατηρώντας ότι $BA^2 = B^3 = A^2B$ και λαμβάνοντας υπόψην ότι $\lambda - \mu \neq 0$ βρίσκουμε ότι $A(AB - BA) = O$. Εργαζόμενοι ομοίως βρίσκουμε $B(AB - BA) = O$. Επομένως,

$$AB - BA \;=\; 1_R \cdot (AB - BA) \;=\; (\lambda AB + \mu BA) \cdot (AB - BA) \;=\; O.$$

Συμπεραίνουμε ότι $(\lambda + \mu)AB = (\lambda + \mu)BA = 1_R$ και συνεπώς ότι τα A, B είναι αντιστρέψιμα στοιχεία του R. Για το (β), παρατηρούμε ότι η παραπάνω λύση ισχύει για κάθε δακτύλιο R με μονάδα ο οποίος είναι ταυτόχρονα $\mathbb{F}$-διανυσματικός χώρος και ισχύει $\lambda(ab) = (\lambda a)b = a(\lambda b)$ για $a, b \in R$ και $\lambda \in \mathbb{F}$. Ένας τέτοιος δακτύλιος R λέγεται $\mathbb{F}$-*άλγεβρα* με μονάδα.

(24) Για το (α), υποθέστε ότι υπάρχει τέτοιο $x \in \mathbb{F}$ και δείξτε ότι τα σύνολα της μορφής $\{a, a + x\}$, για $a \in \mathbb{F}$, αποτελούν τα μέρη μιας διαμέρισης του $\mathbb{F}$. Αυτό δείχνει ότι το πλήθος των στοιχείων του $\mathbb{F}$ είναι άρτιος αριθμός, σε αντίθεση με την υπόθεση. Για το (β), έστω ότι $q \equiv 1 \pmod 4$. Δείξτε πρώτα ότι τα σύνολα $\{x, -x, x^{-1}, -x^{-1}\}$, για μη μηδενικά $x \in \mathbb{F}$, αποτελούν τα μέρη μιας διαμέρισης του $\mathbb{F}\setminus\{0\}$. Κάποια από τα σύνολα αυτά ενδέχεται να έχουν λιγότερα από τέσσερα στοιχεία. Παρατηρήστε ότι αφού $-x \neq x$ για κάθε $x \in \mathbb{F}\setminus\{0\}$, όπως προκύπτει από το (α), αυτό συμβαίνει μόνο όταν $x^{-1} = x$, ή $x^{-1} = -x$, και ότι στην πρώτη περίπτωση υπάγεται μόνο το σύνολο $\{1, -1\}$. Από τα προηγούμενα και το γεγονός ότι το πλήθος των στοιχείων του $\mathbb{F}\setminus\{0\}$ είναι ακέραιο πολλαπλάσιο του 4, συνάγετε το ζητούμενο.

(25) Για το (α) υποθέστε ότι $\deg(f(x)) = n$ και $\deg(g(x)) = m$ και εκφράστε τα $f(x), g(x)$ στη μορφή $f(x) = a_0 + a_1x + \cdots + a_nx^n$ και $g(x) = b_0 + b_1x + \cdots + b_mx^m$, με $a_n, b_m \neq 0_R$. Παρατηρήστε ότι $f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_mx^{n+m}$ και ότι $a_nb_m \neq 0_R$ και συνάγετε ότι $f(x)g(x) \neq 0_{R[x]}$ και ότι $\deg(f(x)g(x)) = n + m$. Για το (β), υποθέστε ότι $r(x)$ είναι η μονάδα του $R[x]$ και συμπεράνετε από το (α) και την ισότητα $(r(x))^2 = r(x)$ ότι το $r(x)$ είναι σταθερό πολυώνυμο (και προφανώς μονάδα του R). Για το (γ), παρατηρήστε πρώτα ότι αν ο $R[x]$ δεν έχει μηδενοδιαιρέτες, τότε το ίδιο ισχύει για τον R, και χρησιμοποιήστε τα (α) και (β) για να δείξετε ότι δεν υπάρχει μη σταθερό πολυώνυμο $f(x) \in R[x]$ το οποίο να είναι αντιστρέψιμο στοιχείο του $R[x]$.

(26) Χρησιμοποιήστε την Άσκηση 25 (α) για να δείξτε ότι δεν υπάρχουν τέτοια πολυώνυμα ως εξής. Για το (α) παρατηρήστε ότι ο βαθμός του αριστερού μέλους της προτεινόμενης ισότητας είναι ακέραιο πολλαπλάσιο του 16, ενώ εκείνος του δεξιού μέλους δεν είναι. Για το (β) παρατηρήστε ότι $(p(x))^2 - (q(x))^2 = (p(x) - q(x))(p(x) + q(x))$ και ότι ένα τουλάχιστον από τα πολυώνυμα $p(x) - q(x)$ και $p(x) + q(x)$ έχει βαθμό n και συμπεράνετε ότι αν το πολυώνυμο

$(p(x))^2 - (q(x))^2$ είναι μη μηδενικό, τότε ο βαθμός του είναι μεγαλύτερος ή ίσος του n.

(27) Θα δείξουμε ότι τα μόνα πολυώνυμα με την ιδιότητα αυτή είναι εκείνα της μορφής $p(x) = x^n$, με $n \in \mathbb{N}$. Αφού το $p(x)$ είναι μη μηδενικό, μπορούμε να το γράψουμε στη μορφή $p(x) = x^n q(x)$ για κάποιο $q(x) \in \mathbb{F}[x]$ με $q(0) \neq 0$. Έχουμε $q(x^2) = (q(x))^2$ και θέλουμε να δείξουμε ότι $q(x) \equiv 1$. Γράφουμε $q(x) = a_0 + a_1 x + \cdots + a_m x^m$. Εξισώνουμε τους σταθερούς όρους στα δύο μέλη της $q(x^2) = (q(x))^2$ και συμπεραίνουμε ότι $a_0 = a_0^2$, οπότε $a_0 = 1$. Ομοίως, εξισώνουμε διαδοχικά τους συντελεστές των $x, x^2, \ldots$ και παίρνουμε $0 = 2a_0a_1 = 2a_1$, οπότε $a_1 = 0$, $0 = 2a_0a_2 = 2a_2$, οπότε $a_2 = 0$ και ούτω καθεξής. Έπεται ότι $q(x) \equiv 1$.

(28) Για το (α), έστω $p(x) = x^{2n} + a_1 x^{2n-1} + \cdots + a_{2n}$ και $q(x) = x^n + b_1 x^{n-1} + \cdots + b_n$. Τότε $(q(x))^2 = x^{2n} + c_1 x^{2n-1} + \cdots + c_{2n}$ με $c_k = b_0 b_k + b_1 b_{k-1} + \cdots + b_k b_0$ για $1 \leq k \leq n$, όπου $b_0 = 1$. Παρατηρήστε ότι οι εξισώσεις $c_1 = a_1$, $c_2 = a_2, \ldots, c_n = a_n$ έχουν μοναδική λύση $b_1 = a_1/2$, $b_2 = (a_2 - b_1^2)/2, \ldots, b_n = (a_n - b_1 b_{k-1} - \cdots b_{k-1} b_1)/2$ ως προς $b_1, b_2, \ldots, b_n$ και συνάγετε το ζητούμενο. Για το (β) δώστε αρνητική απάντηση, δοκιμάζοντας το πολυώνυμο $p(x) = 1 + x + x^2 \in \mathbb{Z}_2[x]$.

(29) Το (α) αφήνεται στον αναγνώστη. Για το (β) χρησιμοποιήστε επαγωγή στο m. Για το (γ) εφαρμόστε τα (α) και (β), καθώς και το γεγονός ότι $\Delta(q(x)) = 0$ για κάθε σταθερό πολυώνυμο $q(x) \in R[x]$. Για το (δ), χρησιμοποιώντας τα (β) και (γ), παρατηρήστε ότι

$$\begin{aligned}\sum_{k=0}^{n} (-1)^k \binom{n}{k} (x-k)^n &= \Delta^n(x^n) = \Delta^{n-1}(x^n - (x-1)^n) \\ &= \Delta^{n-1}\left(nx^{n-1} - \binom{n}{2} x^{n-2} + \cdots\right) = \Delta^{n-1}(nx^{n-1}) \\ &= n\Delta^{n-1}(x^{n-1})\end{aligned}$$

και καταλήξετε στο ζητούμενο με επαγωγή στο n.

(30) Για το (α), εκφράστε τα $f(x), g(x)$ στη μορφή $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ και $g(x) = b_0 + b_1 x + \cdots + b_n x^n$, όπου $\deg(f(x)), \deg(g(x)) \leq n$, και παρατηρήστε ότι

$$\begin{aligned}(f+g)(\alpha) &= (a_0 + b_0) + (a_1 + b_1)\alpha + \cdots + (a_n + b_n)\alpha^n \\ &= (a_0 + a_1\alpha + \cdots + a_n\alpha^n) + (b_0 + b_1\alpha + \cdots + b_n\alpha^n) \\ &= f(\alpha) + g(\alpha).\end{aligned}$$

Για το (β) δείξτε πρώτα την ειδική περίπτωση $g(x) = b_m x^m$. Στη συνέχεια, γράψτε $g(x) = h(x) + b_m x^m$ με $\deg(h(x)) < m$ και χρησιμοποιήστε το (α), την προηγούμενη ειδική περίπτωση και επαγωγή στο βαθμό του $g(x)$ για να καταλήξετε στη ζητούμενη ισότητα. Το (γ) είναι η ειδική περίπτωση $\alpha = 1_R$ των (α) και (β), όταν ο R έχει μονάδα. Στη γενική περίπτωση, μπορεί κανείς να μιμηθεί την απόδειξη των (α) και (β) που περιγράψαμε. Για το (δ) εφαρμόστε το (γ) και συμπεράνετε ότι το ζητούμενο άθροισμα είναι ίσο με $(-1)^n$.

(31) Για το (α) χρησιμοποιήστε την Άσκηση 29 (γ). Για το (β) εφαρμόστε το (α) στο πολυώνυμο $q(x) = p(x^2)$ βαθμού $2n$, παρατηρώντας ότι $q(m) \in \mathbb{Z}$ για κάθε $m \in \{-n, -n+1, \ldots, n\}$. Για το (γ) δοκιμάστε το πολυώνυμο $p(x) = x(x-1)/12$.

(32) Δείξτε πρώτα ότι αν $p_n(x) = x(x-1)(x-2)\cdots(x-n+1)$, τότε το $p_n(m)$ διαιρείται με το $n!$ για κάθε $m \in \mathbb{Z}$. Υποθέστε έπειτα ότι $p(x) \in \mathbb{Z}[x]$ είναι μονικό πολυώνυμο βαθμού n και παρατηρήστε ότι αν το $p(m)$ διαιρείται με το k για κάθε $m \in \mathbb{Z}$, τότε το ίδιο ισχύει για το πολυώνυμο $\Delta^n(p(x))$. Συνάγετε από την Άσκηση 29 (δ) ότι το k διαιρεί το $n!$. Από τα παραπάνω συμπεράνετε

ότι το $n(k)$ είναι ο ελάχιστος θετικός ακέραιος n για τον οποίο το $n!$ διαιρείται με το k. Ειδικότερα, για $k = 1000 = 2^3 \cdot 5^3$ έχουμε $n(k) = 15$.

(33) Για το (α) θεωρήστε το πολυώνυμο $g(x)$ για το οποίο ισχύει $f(x)\,g(x) = 1$ στο $R[x]$ και εφαρμόστε την Άσκηση 30 (β) για να δείξετε ότι το $g(\alpha)$ είναι το αντίστροφο στοιχείο του $f(\alpha)$ για κάθε $\alpha \in R$. Για το (β) εφαρμόστε το (α) με $\alpha = 1 \in \mathbb{Z}_6$. Για το (γ) να θέσετε $R = \mathbb{Z}_2$ και $f(x) = 1 + x + x^2$.

(34) Για το (α), υποθέστε πρώτα ότι το $1_R + rx$ είναι αντιστρέψιμο στοιχείο του $R[x]$, οπότε υπάρχουν $c_0, c_1, \ldots, c_n \in R$ με $(1_R + rx)(c_0 + c_1x + \cdots + c_nx^n) = 1_R$ στο $R[x]$. Από τις εξισώσεις $c_0 = 1_R$, $c_1 + rc_0 = c_2 + rc_1 = \cdots = c_n + rc_{n-1} = rc_n = 0_R$ που προκύπτουν συνάγετε ότι $r^{n+1} = 0_R$ και συνεπώς ότι το r είναι μηδενοδύναμο στοιχείο του R. Το αντίστροφο έπεται από την Άσκηση 22 (δ). Για το (β), υποθέστε πρώτα ότι το $a + bx$ είναι αντιστρέψιμο στοιχείο του $R[x]$ και, εργαζόμενοι όπως στο (α), δείξτε ότι το a είναι αντιστρέψιμο στοιχείο του R. Έπειτα, γράφοντας $a + bx = a(1_R + a^{-1}bx)$, συνάγετε το (β) ερώτημα από το (α). Για το (γ) συνάγετε από το (β) ότι αν ο m διαιρείται με p^2, τότε το πολυώνυμο $1 + (m/p)x$ είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}_m[x]$.

(35) Για το (α), δείξτε ότι τα μόνα αντιστρέψιμα στοιχεία του $\mathbb{Z}_6[x]$ είναι τα σταθερά πολυώνυμα 1 και -1 ως εξής. Θεωρήστε πολυώνυμα $f(x), g(x)$ με ακέραιους συντελεστές για τα οποία ισχύει $f(x)g(x) = 1$ στο $\mathbb{Z}_6[x]$. Αυτό σημαίνει ότι ο σταθερός όρος του $f(x)g(x)$ είναι ισότιμος με 1 mod 6 και οι υπόλοιποι με μηδέν. Επομένως, έχουμε $f(x)g(x) = 1$ στο $\mathbb{Z}_3[x]$ επίσης. Αφού όμως τα μόνα αντιστρέψιμα στοιχεία του $\mathbb{Z}_3[x]$ είναι τα 1 και -1, έπεται ότι κάθε συντελεστής των $f(x)$ και $g(x)$ εκτός των σταθερών όρων διαιρείται με το 3. Με αυτό το δεδομένο καταλήξτε σε άτοπο. Για το (β), παρατηρήστε ότι ισχύει $(1 + 6f(x))^2 = 1$ για κάθε πολυώνυμο $f(x) \in \mathbb{Z}_{12}[x]$ και συνάγετε ότι το πολυώνυμο $1 + 6x + \cdots + 6x^n$ είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}_{12}[x]$ για κάθε φυσικό αριθμό n.

(36) Αφήνουμε την επαλήθευση στον αναγνώστη.

(37) Θα δείξουμε ότι τα πολυώνυμα με την επιθυμητή ιδιότητα είναι εκείνα της μορφής $p(x) = ax$, με $a \in \mathbb{C}$. Θέτοντας πρώτα $x = y = 0$ στη δοσμένη ταυτότητα προκύπτει ότι $p(0) = 0$. Έπειτα, παραγωγίζοντας ως προς x και θέτοντας $x = y$ παίρνουμε ότι $2p'(x)p(x) = p'(0)p(2x)$. Αν $p'(0) = 0$, τότε το $p(x)$ είναι σταθερό πολυώνυμο και συνεπώς ταυτοτικά ίσο με $p(0) = 0$. Διαφορετικά, το $p(x)$ έχει θετικό βαθμό, έστω n. Εξισώνοντας τους βαθμούς των $2p'(x)p(x)$ και $p'(0)p(2x)$ βρίσκουμε ότι $2n - 1 = n$, οπότε $n = 1$. Άρα, $p(x) = ax$ με $a = p'(0) \in \mathbb{C}$.

(38) Εφαρμόστε επαγωγή στο n. Έστω $f(x) = (x - 1)^n q(x)$ και έστω ότι $n \geq 1$ (το ζητούμενο είναι τετριμμένο για $n = 0$). Μπορείτε να υποθέσετε χωρίς βλάβη της γενικότητας ότι $q(0) \neq 0$ (εξηγήστε γιατί), οπότε $f(0) \neq 0$. Παρατηρήστε ότι $f'(x) = (x - 1)^{n-1} r(x)$ για κάποιο $r(x) \in \mathbb{C}[x]$ και εφαρμόστε την υπόθεση της επαγωγής στο $f'(x)$.

(39) Δείξτε ότι η διαφορά των δύο πολυωνύμων διαιρείται με το $x^7 - 1$, άρα και με το $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, στο $\mathbb{Z}[x]$ και συμπεράνετε το ζητούμενο.

(40) Για το (α) εκφράστε το $f(x)$ στη μορφή $f(x) = a_0 + a_1x + \cdots + a_nx^n$ και χρησιμοποιήστε την ταυτότητα $y^m - z^m = (y - z)(y^{m-1} + y^{m-2}z + \cdots + z^{m-1})$ (όπου $yz = zy$). Για το (β) παρατηρήστε ότι $p(p(x)) - q(q(x)) = (p(p(x)) - p(q(x))) + (q(p(x)) - q(q(x)))$ και εφαρμόστε το (α).

(41) Απάντηση: (α) $x + 1$, (β) $x^2 + 1$, (γ) $x^3 + x^2 + x + 1$.

(42) Για το (α) υποθέστε ότι $m \geq n$ και θεωρήστε την Ευκλείδεια διαίρεση $m = qn + r$ του m με το n, όπου $0 \leq r < n$. Δείξτε ότι $x^m - 1 = (x^n - 1)q(x) + (x^r - 1)$ για κάποιο πολυώνυμο $q(x) \in R[x]$. Συμπεράνετε ότι $\mu\kappa\delta(x^m - 1, x^n - 1) = \mu\kappa\delta(x^n - 1, x^r - 1)$ και εφαρμόστε επαγωγή στο $\max\{m, n\}$ για να δείξετε το ζητούμενο. Για το (β),

συνάγετε από το (α) ότι το $x^m - 1$ διαιρείται με το $x^n - 1$ στο $R[x]$ αν και μόνο αν το m διαιρείται με το n στο $\mathbb{Z}$. Για το (γ) παρατηρήστε ότι $x^k - 1 = (x-1)f_k(x)$ για $k \geq 1$ και χρησιμοποιήστε το (α).

(43) Για το (α) θεωρήστε την Ευκλείδεια διαίρεση $f(x) = q(x)g(x) + r(x)$ του $f(x)$ με το $g(x)$ στο $\mathbb{F}[x]$. Παρατηρήστε ότι η προηγούμενη ισότητα ισχύει και στο $\mathbb{K}[x]$ και χρησιμοποιήστε τη μοναδικότητα της Ευκλείδειας διαίρεσης στο $\mathbb{K}[x]$. Το (β) έπεται από το (α). Για το (γ) χρησιμοποιήστε το (β) και τον Ευκλείδειο αλγόριθμο για τον υπολογισμό του μέγιστου κοινού διαιρέτη (ή επαγωγή στο βαθμό του $f(x)$). Για το (δ), θεωρήστε το μέγιστο κοινό διαιρέτη $d(x)$ των $f(x)$ και $g(x)$ στο $\mathbb{K}[x]$ και χρησιμοποιήστε το (γ), καθώς και την υπόθεση ότι το $g(x)$ είναι ανάγωγο στο $\mathbb{F}[x]$, για να δείξετε ότι $d(x) = g(x)$.

(44) Χρησιμοποιώντας το μικρό Θεώρημα του Fermat, δείξτε ότι κάθε στοιχείο του $\mathbb{Z}_p$ εκτός του 1 είναι ρίζα του $f(x)$ και συμπεράνετε ότι στο $\mathbb{Z}_p[x]$ ισχύει $f(x) = x(x-2)\cdots(x-p+1)$.

(45) Για το (α) παρατηρήστε ότι $f(1) = 0$ και, χρησιμοποιώντας το μικρό Θεώρημα του Fermat, ότι $f(\alpha) = (\alpha^p - 1)/(\alpha - 1) = 1$ για $\alpha \neq 1$ και συμπεράνετε ότι η μοναδική ρίζα του $f(x)$ στο $\mathbb{Z}_p$ είναι η $\alpha = 1$. Για το (β) δείξτε ότι $f(x) = (x-1)^{p-1}$ στο $\mathbb{Z}_p[x]$ ως εξής. Αντικθιστώντας το x με το $-x$, έχουμε να δείξουμε ότι $(1+x)^{p-1} = 1 - x + \cdots + (-x)^{p-1}$ στο $\mathbb{Z}_p[x]$, δηλαδή ότι

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}$$

για $k \in \{0, 1, \ldots, p-1\}$. Αυτό προκύπτει με επαγωγή στο k, παρατηρώντας ότι

$$\binom{p-1}{k} = \binom{p}{k} - \binom{p-1}{k-1} \equiv -\binom{p-1}{k-1} \pmod{p}$$

για $k \in \{1, 2, \ldots, p-1\}$.

(46) Από το μικρό Θεώρημα του Fermat συνάγετε ότι κάθε στοιχείο του $\mathbb{Z}_p$ είναι ρίζα του $f(x)$ και συνεπώς ότι το $f(x)$ διαιρείται με το γινόμενο $x(x-1)(x-2)\cdots(x-p+1) = x^p - x$ στο $\mathbb{Z}_p[x]$. Άρα, ισχύει το (α). Αφού τα $f(x)$ και $x^p - x$ έχουν βαθμό $2p$ και p, αντίστοιχα, ο βαθμός του πηλίκου $q(x)$ είναι ίσος με $2p - p = p$. Για το (β), χρησιμοποιώντας την Άσκηση 4 (β), παρατηρήστε ότι

$$\begin{aligned} f(x) &= (x^{2p} + x^p + 1) - (x^2 + x + 1) = (x^{2p} - x^2) + (x^p - x) \\ &= (x^p - x)(x^p + x) + (x^p - x) = (x^p - x)(x^p + x + 1) \end{aligned}$$

και συμπεράνετε ότι $q(x) = x^p + x + 1$.

(47) Υποθέτουμε ότι το $g(x)$ είναι πολυώνυμο θετικού βαθμού (διαφορετικά το ζητούμενο είναι τετριμμένο) και θεωρούμε την Ευκλείδεια διαίρεση $f(x) = g(x)q(x) + r(x)$ του $f(x)$ με το $g(x)$ στο $\mathbb{Q}[x]$, οπότε έχουμε $q(x), r(x) \in \mathbb{Q}[x]$ και $\deg(r(x)) < \deg(g(x))$. Αφού $q(x) \in \mathbb{Q}[x]$, υπάρχει θετικός ακέραιος m τέτοιος ώστε $m \cdot q(x) \in \mathbb{Z}[x]$. Από την υπόθεση έχουμε ότι $q(n) + r(n)/g(n) = f(n)/g(n) \in \mathbb{Z}$ για κάθε αρκετά μεγάλο ακέραιο n. Λαμβάνοντας υπόψην ότι $\lim_{x\to\infty} r(x)/g(x) = 0$, άρα ότι $|r(x)/g(x)| < 1/m$ για αρκετά μεγάλο x, και ότι $q(n) \in \frac{1}{m}\mathbb{Z}$ για κάθε ακέραιο n, προκύπτει ότι $r(n) = 0$ για κάθε αρκετά μεγάλο ακέραιο n. Συμπεραίνουμε ότι το $r(x)$ είναι το μηδενικό πολυώνυμο του $\mathbb{Q}[x]$, δηλαδή ότι ισχύει το (α). Για το (β) αρκεί να θέσει κανείς $f(x) = x(x-1)$ και $g(x) = 2$.

(48) Υποθέτουμε πρώτα ότι τα $f(x), g(x)$ δεν έχουν κοινή μιγαδική ρίζα. Τότε $\mu\kappa\delta(f(x), g(x)) = 1$ στο $\mathbb{Q}[x]$ και συνεπώς υπάρχουν $a(x), b(x) \in \mathbb{Q}[x]$ τέτοια ώστε $a(x)f(x) + b(x)g(x) = 1$. Πολλαπλασιάζοντας με κατάλληλο θετικό ακέραιο d βρίσκουμε $p(x), q(x) \in \mathbb{Z}[x]$ τέτοια ώστε $p(x)f(x) + q(x)g(x) = d$ και προφανώς $\mu\kappa\delta(f(n), g(n)) \leq d$ για κάθε $n \in \mathbb{Z}$. Αντιστρόφως, έστω ότι τα $f(x), g(x)$ έχουν κοινή ρίζα στο $\mathbb{C}$. Τότε $\mu\kappa\delta(f(x), g(x)) \neq 1$ στο $\mathbb{C}[x]$ και

συνεπώς, σύμφωνα με την Άσκηση 43 (γ), το ίδιο ισχύει στο $\mathbb{Q}[x]$. Άρα, υπάρχει πολυώνυμο $h(x) \in \mathbb{Z}[x]$ θετικού βαθμού και $a(x), b(x) \in \mathbb{Q}[x]$ τέτοια ώστε $f(x) = a(x)h(x)$ και $g(x) = b(x)h(x)$. Πολλαπλασιάζοντας με κατάλληλο ακέραιο r βρίσκουμε $p(x), q(x) \in \mathbb{Z}[x]$ τέτοια ώστε $r\,f(x) = p(x)h(x)$ και $r\,g(x) = q(x)h(x)$. Συμπεραίνουμε ότι $r\,\mu\kappa\delta(f(n), g(n)) \geq |h(n)|$ για κάθε $n \in \mathbb{Z}$, από όπου έπεται ότι $\lim_{n\to\infty} \mu\kappa\delta(f(n), g(n)) = \infty$.

(49) Θεωρήστε το $f(x, y)$ ως πολυώνυμο στο x με συντελεστές από το $R[y]$. Για το (α) εφαρμόστε την Ευκλείδεια διαίρεση για να γράψετε το $f(x, y)$ στη μορφή $f(x, y) = (x - y)q(x, y) + r(y)$ για κάποια πολυώνυμα $q(x, y) \in R[x, y]$ και $r(y) \in R[y]$. Θέτοντας $x = y = a \in R$, παρατηρήστε ότι $r(a) = 0_R$ για κάθε $a \in R$ και συμπεράνετε ότι το $r(y)$ είναι το μηδενικό πολυώνυμο του $R[y]$. Για το (β) εφαρμόστε την Ευκλείδεια διαίρεση για να γράψετε το $f(x, y)$ στη μορφή $f(x, y) = (x^2 + y^2 - 1)q(x, y) + g(y)x + h(y)$ για κάποια πολυώνυμα $q(x, y) \in \mathbb{R}[x, y]$ και $g(y), h(y) \in \mathbb{R}[y]$. Παρατηρήστε έπειτα ότι για κάθε $(a, b) \in \mathbb{R}^2$ με $a^2 + b^2 = 1$ το $(-a, b)$ επαληθεύει την ίδια ισότητα και επομένως ότι $g(b)a + h(b) = -g(b)a + h(b) = 0$. Συνάγετε ότι $g(y) = h(y) = 0$ στο $\mathbb{R}[y]$.

(50) Το (α) αφήνεται στον αναγνώστη. Το (β) προκύπτει από το (α) με επαγωγή στο n.

(51) Για το (α) παρατηρήστε ότι $x^n f(1/x) = a_n + a_{n-1}x + \cdots + a_0x^n$, αν $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Για το (β) εφαρμόστε το (α), ή χρησιμοποιήστε κατευθείαν τον ορισμό του γινομένου πολυωνύμων. Για το (γ) χρησιμοποιήστε τον ορισμό των πολυωνύμων $f_n(q)$ και εφαρμόστε το (α).

(52) Για το (α) επαληθεύστε ότι $g(x, y, z) = 3(x + y)(x + z)(y + z)$. Για το (β) θεωρήστε το $f(x, y, z)$ ως πολυώνυμο στο x με συντελεστές από το $\mathbb{Q}[y, z]$. Παρατηρήστε ότι $f(x, y, z) = 0$ για $x = -y$ και θεωρήστε την Ευκλείδεια διαίρεση $f(x, y, z) = (x+y)\,q(x, y, z)+r(x, y)$ του $f(x, y, z)$ με το $x+y$ στο $\mathbb{Q}[x, y, z]$ για να συμπεράνετε ότι $f(x, y, z) = (x + y)\,q(x, y, z)$ για κάποιο πολυώνυμο $q(x, y, z) \in \mathbb{Q}[x, y, z]$. Δείξτε με παρόμοιο τρόπο ότι το $q(x, y, z)$ διαιρείται με το $x + z$ και ότι το πηλίκο της διαίρεσης διαιρείται με το $y + z$ στο $\mathbb{Q}[x, y, z]$.

(53) Έστω $f(x) = x^4+1$. Στο $\mathbb{R}[x]$ έχουμε $f(x) = (x^2+1)^2-2x^2 = (x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1)$. Στο $\mathbb{Z}_{17}[x]$ έχουμε $f(x) = x^4-16 = (x^2-4)(x^2+4) = (x^2-4)(x^2-64) = (x-2)(x+2)(x-8)(x+8)$. Για το (β) παρατηρήστε ότι κάθε παραγοντοποίηση του $f(x)$ στο $\mathbb{Q}[x]$ ισχύει και στο $\mathbb{R}[x]$ και συνάγετε ότι το $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$. Για το (δ) παρατηρήστε ότι αν $-1_R = 1_R$, τότε $f(x) = (x + 1)^4$ στο $R[x]$.

(54) Έστω $f(x) = x^4+x^3+x^2-2x+1$ και $g(x) = x^4+x^3+x+3$. Για το (α), δείξτε ότι το $f(x)$ δεν έχει ρίζες στο $\mathbb{Z}$ και συμπεράνετε ότι αν το $f(x)$ δεν είναι ανάγωγο στο $\mathbb{Z}[x]$, τότε υπάρχει παραγοντοποίηση της μορφής $f(x) = (x^2+ax+1)(x^2+bx+1)$ ή $f(x) = (x^2 + ax - 1)(x^2 + bx - 1)$. Για την πρώτη περίπτωση, παρατηρήστε ότι ο συντελεστής του x^3 στο γινόμενο $(x^2 + ax + 1)(x^2 + bx + 1)$ είναι ίσος με εκείνον του x και συμπεράνετε ότι μια τέτοια παραγοντοποίηση για το $f(x)$ είναι αδύνατη. Εργαστείτε παρόμοια για τη δεύτερη περίπτωση. Για το (β), δείξτε ότι το $g(x)$ δεν έχει ρίζες στο $\mathbb{Z}_5$. Συμπεράνετε ότι αν το $g(x)$ δεν είναι ανάγωγο στο $\mathbb{Z}_5[x]$, τότε υπάρχει παραγοντοποίηση της μορφής $g(x) = (x^2 + ax + 1)(x^2 + bx + 3)$ ή $g(x) = (x^2 + ax - 1)(x^2 + bx - 3)$ και δείξτε ότι και οι δύο παραγοντοποιήσεις είναι αδύνατες στο $\mathbb{Z}_5[x]$.

(55) Δείξτε πρώτα ότι το x^2+x+1 είναι το μόνο ανάγωγο πολυώνυμο δευτέρου βαθμού στο $\mathbb{Z}_2[x]$. Συμπεράνετε ότι τα ανάγωγα πολυώνυμα τετάρτου βαθμού στο $\mathbb{Z}_2[x]$ είναι αυτά που έχουν μη μηδενικό σταθερό όρο (ισοδύναμα, δε διαιρούνται με το x), έχουν περιττό πλήθος μη μηδενικών συντελεστών (ισοδύναμα, δε διαιρούνται με το $x - 1$) και είναι διάφορα του $(x^2 + x + 1)^2 = x^4 + x^2 + 1$, δηλαδή τα $x^4 + x + 1$, $x^4 + x^3 + 1$ και $x^4 + x^3 + x^2 + x + 1$.

(56) Για το (α) υποθέστε ότι $f(x) = p(x)q(x)$ για κάποια πολυώνυμα $p(x), q(x) \in \mathbb{Z}[x]$ βαθμού μικρότερου του n. Παρατηρήστε τότε ότι $p(a_i)q(a_i) = -1$ για $1 \leq i \leq n$ και θεωρήστε το πολυώνυμο $r(x) = p(x) + q(x)$. Παρατηρήστε ότι οι $a_1, a_2, \ldots, a_n$ είναι ρίζες του πολυωνύμου $r(x)$ και ότι $\deg(r(x)) \leq n-1$ και συμπεράνετε ότι το $r(x)$ είναι το μηδενικό πολυώνυμο. Επομένως, έχουμε $q(x) = -p(x)$ και $f(x) = -(p(x))^2$. Θυμηθείτε τώρα ότι το $f(x)$ είναι μονικό πολυώνυμο για να καταλήξετε σε άτοπο. Εργασθείτε ομοίως για το (β). Υποθέστε ότι $g(x) = p(x)q(x)$ για κάποια πολυώνυμα $p(x), q(x) \in \mathbb{Z}[x]$ βαθμού μικρότερου του $2n$. Παρατηρήστε τότε ότι $p(a_i)q(a_i) = 1$ για $1 \leq i \leq n$ και ότι τα $p(x), q(x)$ δεν έχουν πραγματικές ρίζες. Συμπεράνετε ότι είτε $p(a_i) = q(a_i) = 1$ για $1 \leq i \leq n$, οπότε $p(x) = q(x) = (x-a_1)(x-a_2)\cdots(x-a_n)+1$, είτε $p(a_i) = q(a_i) = -1$ για $1 \leq i \leq n$, οπότε $p(x) = q(x) = (x-a_1)(x-a_2)\cdots(x-a_n)-1$ και καταλήξτε σε άτοπο. Για το (γ) δώστε αρνητική απάντηση θεωρώντας π.χ. το πολυώνυμο $h(x) = (x-1)(x-3)+1$.

(57) Για το (α) μιμηθείτε την απόδειξη του Ευκλείδη για την απειρία των πρώτων αριθμών. Για το (β) παρατηρήστε ότι αν το $\mathbb{F}$ είναι πεπερασμένο, τότε για κάθε $n \in \mathbb{N}$ υπάρχουν μόνο πεπερασμένου πλήθους πολυώνυμα στο $\mathbb{F}[x]$ βαθμού μικρότερου ή ίσου του n και χρησιμοποιήστε το (α). Για το (γ) δώστε αρνητική απάντηση θέτοντας $\mathbb{F} = \mathbb{R}$, ή $\mathbb{F} = \mathbb{C}$.

(58) Για τη συνεπαγωγή (i) $\Rightarrow$ (iii) δείξτε ότι αν το n διαιρείται με το p, τότε το

$$f_p(x^n) - p \;=\; (x^n-1) \,+\, (x^{2n}-1) \,+\, \cdots \,+\, (x^{(p-1)n}-1)$$

διαιρείται με το $x^p - 1$, άρα και με το $f_p(x)$, στο $\mathbb{Z}[x]$ και συμπεράνετε ότι το $f_p(x^n)$ δε διαιρείται με το $f_p(x)$. Για την (iii) $\Rightarrow$ (ii) δείξτε ότι αν το n δε διαιρείται με το p, τότε κάθε ρίζα του $f_p(x) = (x^p-1)/(x-1)$ είναι και ρίζα του $f_p(x^n)$ (θα χρειαστεί η υπόθεση ότι ο p είναι πρώτος αριθμός). Αφού το $f_p(x)$ έχει p διακεκριμένες μιγαδικές ρίζες (εξηγήστε γιατί), συμπεράνετε ότι το $f_p(x)$ διαιρεί το $f_p(x^n)$ στο $\mathbb{C}[x]$. Η συνεπαγωγή (ii) $\Rightarrow$ (i) προκύπτει από τη μοναδικότητα της Ευκλείδειας διαίρεσης του $f_p(x^n)$ με το $f_p(x)$ στα $\mathbb{Z}[x]$ και $\mathbb{C}[x]$, αντίστοιχα.

(59) Για το (α) δείξτε με επαγωγή στο m ότι ισχύει $p(m^4+1) = m^4+1$ για κάθε $m \in \mathbb{N}$. Συμπεράνετε ότι το πολυώνυμο $p(x) - x$ έχει άπειρες ρίζες στο $\mathbb{C}$ και επομένως ότι το $p(x) = x$ είναι το μοναδικό πολυώνυμο με τις ζητούμενες ιδιότητες. Για το (β) παρατηρήστε ότι το πολυώνυμο $q(x) = (x+1)p(x) - 1$ έχει βαθμό μικρότερο ή ίσο του $n+1$ και τις ρίζες $0, 1, \ldots, n$. Συμπεράνετε ότι $q(x) = cx(x-1)\cdots(x-n)$ για κάποιο $c \in \mathbb{C}$. Θέτοντας $c = -1$ στην προηγούμενη ισότητα, δείξτε ότι $c = (-1)^n/(n+1)!$ και συνάγετε ότι το

$$p(x) \;=\; \left(1 \,+\, \frac{(-1)^n}{(n+1)!}\, x(x-1)\cdots(x-n)\right) / \,(x+1)$$

είναι το μοναδικό πολυώνυμο με τις ζητούμενες ιδιότητες.

(60) Από τον τύπο παρεμβολής του Lagrange έχουμε

$$\begin{aligned} p(x) \;&=\; \sum_{k=0}^{n} p(k) \prod_{i\neq k} \frac{x-i}{k-i} \;=\; \sum_{k=0}^{n} \frac{1}{\binom{n+1}{k}} \cdot \frac{\prod_{i\neq k}(x-i)}{(-1)^{n-k}k!\,(n-k)!} \\ &=\; \sum_{k=0}^{n} (-1)^{n-k}\, \frac{n-k+1}{(n+1)!} \prod_{i\neq k}(x-i), \end{aligned}$$

όπου στα γινόμενα το i διατρέχει τα στοιχεία του $\{0, 1, \ldots, n\}$ εκτός από το k. Θέτοντας $x = n+1$ στο τελευταίο άθροισμα, συμπεράνετε ότι $p(n+1) = 1$ ή 0, αν ο n είναι άρτιος ή περιττός, αντίστοιχα.

(61) Για το (α) υποθέστε ότι $f(a) = f'(a) = 0_R$, οπότε υπάρχει πολυώνυμο $q(x) \in R[x]$ με $f(x) = (x-a)q(x)$. Χρησιμοποιώντας την Άσκηση 36 (β), δείξτε ότι

$f'(x) = q(x) + (x-a)q'(x)$ και συμπεράνετε ότι $q(a) = 0_R$, ότι το $q(x)$ διαιρείται με το $x-a$ και ότι το $f(x)$ διαιρείται με το $(x-a)^2$ στο $R[x]$. Για το αντίστροφο χρησιμοποιήστε την Άσκηση 36 (β). Για το (β) γράψτε $f(x) = (x-a)^m q(x)$, όπου $q(x) \in R[x]$ με $q(a) \neq 0_R$, και δείξτε ότι $f'(x) = (x-a)^{m-1} r(x)$, όπου $r(x) \in R[x]$ με $r(a) \neq 0_R$. Για το (γ) παρατηρήστε ότι το $g'(x)$ είναι μη μηδενικό πολυώνυμο βαθμού μικρότερου από αυτόν του $g(x)$, οπότε δε διαιρείται από το $g(x)$ στο $R[x]$, και χρησιμοποιήστε το (α) και την Άσκηση 43 (δ).

(62) Υποθέστε ότι $r_1 - r_2 \in \mathbb{Q}$. Υποθέστε επίσης, χωρίς βλάβη της γενικότητας, ότι το $g(x)$ είναι μονικό πολυώνυμο. Παρατηρήστε, χρησιμοποιώντας την Άσκηση 61 (γ), ότι $r_1 - r_2 \neq 0$ και θεωρήστε το πολυώνυμο $f(x) = g(x + r_1 - r_2)$. Δείξτε ότι το $f(x)$ είναι μονικό πολυώνυμο τρίτου βαθμού με ρητούς συντελεστές διάφορο του $g(x)$ και ότι το r_2 είναι ριζα του $f(x)$ και καταλήξτε σε άτοπο, χρησιμοποιώντας την Άσκηση 43 (δ).

(63) Για το (α) θεωρήστε την ανάλυση του $f(x)$ σε γινόμενο ανάγωγων πολυωνύμων στο $\mathbb{R}[x]$. Δείξτε ότι κάθε πραγματική ρίζα του $f(x)$ έχει πολλαπλότητα άρτιο αριθμό και θυμηθείτε ότι τα μονικά ανάγωγα πολυώνυμα στο $\mathbb{R}[x]$ βαθμού ≥ 2 είναι εκείνα της μορφής $(x-a)^2 + b^2$, με $a, b \in \mathbb{R}$ και $b \neq 0$. Χρησιμοποιώντας επαγωγή στο βαθμό του $f(x)$, συνάγετε το (β) από το (α) και την ταυτότητα $(p^2+q^2)(r^2+s^2) = (pr+qs)^2 + (ps-qr)^2$, που ισχύει σε κάθε μεταθετικό δακτύλιο.

(64) Παρατηρούμε ότι το $p(x)$ δεν έχει μη αρνητικές πραγματικές ρίζες. Συνεπώς, από την υπόθεση του προβλήματος και την Άσκηση 51 (α) προκύπτει ότι $p(x) = (x+\beta_1)(x+\beta_2)\cdots(x+\beta_n)$ για κάποιους θετικούς πραγματικούς αριθμούς $\beta_1, \beta_2, \ldots, \beta_n$ με $\beta_1\beta_2\cdots\beta_n = 1$ και ότι $p(x) = x^n p(1/x)$. Αφού $\beta_1\beta_2\cdots\beta_n = 1$, η ισότητα $p(x) = x^n p(1/x)$ γράφεται

$$\prod_{i=1}^{n} (x+\beta_i) \;=\; \prod_{i=1}^{n} (x + \frac{1}{\beta_i}).$$

Από τα προηγούμενα προκύπτει το (α). Για το (β) έχουμε να δείξουμε ότι $(-1)^{\lfloor n/2 \rfloor} p(-1) \geq 0$. Αυτό ισχύει αν $m \geq 1$, αφού τότε $p(-1) = 0$. Διαφορετικά, έχουμε $n = 2r$ και

$$(-1)^{n/2}\, p(-1) \;=\; \prod_{i=1}^{r} \frac{(b_i - 1)^2}{b_i} > 0.$$

Για το (γ) χρησιμοποιούμε το (α) παρατηρώντας ότι $(x+b_i)(x+1/b_i) = (1+x)^2 + c_i x$, με $c_i > 0$, για $1 \leq i \leq r$.

(65) Έστω $\alpha_1, \ldots, \alpha_r$ οι διακεκριμένες ρίζες του $p(x)$, οπότε $p(x) = (x-\alpha_1)^{m_1} \cdots (x-\alpha_r)^{m_r}$ για κάποιους θετικούς ακεραίους $m_1, \ldots, m_r$. Όπως προκύπτει από την Άσκηση 61 (β), το πολυώνυμο $q(x) = (x-\alpha_1)^{m_1-1} \cdots (x-\alpha_r)^{m_r-1}$ διαιρεί τα $p(x)$ και $p'(x)$. Άρα, το $q(x)$ διαιρεί και το $np(x) - xp'(x)$. Έχουμε όμως $\deg(q(x)) = n - r$ και $\deg(np(x) - xp'(x)) \leq n - k$, επομένως $r \geq k$.

(66) Δείξτε ότι το ζητούμενο ελάχιστο είναι ίσο με $n+1$ ως εξής. Παρατηρήστε πρώτα ότι για $p(x) = x^n$, το δοσμένο σύνολο έχει ακριβώς $n+1$ στοιχεία. Θεωρήστε έπειτα τυχαίο πολυώνυμο $p(x) \in \mathbb{C}[x]$ βαθμού n. Παρατηρήστε ότι το άθροισμα των πολλαπλοτήτων των ριζών του $p(x)$ είναι ίσο με n, όπως και του $p(x) - 1$, ενώ για την κοινή τους παράγωγο $p'(x)$ το αντίστοιχο άθροισμα είναι ίσο με $n-1$. Χρησιμοποιώντας τα προηγούμενα και την Άσκηση 61 (γ), συμπεράνετε ότι τα $p(x)$ και $p(x) - 1$ έχουν συνολικά τουλάχιστον $n+1$ ρίζες.

(67) Δείξτε πρώτα ότι αν ένα από τα πολυώνυμα $p(x), q(x)$ είναι σταθερό, τότε είναι σταθερό και το άλλο. Υποθέστε τώρα ότι τα $p(x), q(x)$ δεν είναι σταθερά. Αντικαθιστώντας το $p(x)$ με το $-p(x)$, αν αυτό είναι απαραίτητο, και

ομοίως για το $q(x)$, μπορεί να υποθέσει κανείς ότι οι συντελεστές των μεγιστοβάθμιων όρων των $p(x)$ και $q(x)$ είναι θετικοί αριθμοί. Υπό αυτή την προϋπόθεση, υπάρχει $a \in \mathbb{R}$ τέτοιο ώστε τα $p(x)$ και $q(x)$ είναι γνησίως αύξουσες συναρτήσεις για $x > a$. Τότε το $p(x)$ παίρνει διαδοχικές ακέραιες τιμές $m, m+1, m+2, \ldots$ για $x = a_0, a_1, a_2, \ldots$ με $a < a_0 < a_1 < a_2 < \cdots$. Από την υπόθεση του προβλήματος προκύπτει ότι το $q(x)$ παίρνει επίσης διαδοχικές ακέραιες τιμές $n, n+1, n+2, \ldots$ για $x = a_0, a_1, a_2, \ldots$. Συμπεράνουμε ότι η διαφορά $p(x) - q(x)$ λαμβάνει την τιμή $m - n$ για άπειρες τιμές του x. Κατά συνέπεια, το $p(x) - q(x)$ είναι σταθερό πολυώνυμο με τιμή $m - n$.

(68) Δείξτε ότι ο μέγιστος δυνατός βαθμός ενός τέτοιου πολυωνύμου είναι ίσος με 3 ως εξής. Παρατηρήστε πρώτα ότι το $f(x) = x(x+1)(x+2)$ έχει τις ζητούμενες ιδιότητες. Θεωρήστε έπειτα τυχαίο πολυώνυμο $f(x) \in \mathbb{Z}[x]$ βαθμού n με τις ιδιότητες (i) και (ii), οπότε

$$f(x) \;=\; a_0 + a_1 x + \cdots + a_n x^n \;=\; \prod_{i=1}^{n} (b_i x + c_i)$$

για κάποιους ακεραίους b_i, c_i με $b_i \geq 1$ για $1 \leq i \leq n$. Δείξτε ότι $c_i \geq 0$ για $1 \leq i \leq n$, με $c_i = 0$ για έναν το πολύ δείκτη i. Χρησιμοποιώντας την Άσκηση 30 (γ) (δηλαδή θέτοντας $x = 1$ στην παραπάνω ισότητα), δείξτε ότι

$$\frac{n(n+1)}{2} \;=\; a_0 + a_1 + \cdots + a_n \;=\; \prod_{i=1}^{n} (b_i + c_i) \;\geq\; 2^{n-1}$$

και συμπεράνετε ότι $n \leq 4$ και ότι το $n(n+1)/2$ μπορεί να γραφεί ως γινόμενο $n-1$ ακεραίων ≥ 2. Από αυτά συνάγετε ότι $n \leq 3$.

(69) Υποθέστε ότι $a_n = 1$ και θεωρήστε τα τετράγωνα των ριζών του $f(x)$. Παρατηρήστε ότι οι αριθμοί αυτοί είναι μη αρνητικοί και ότι έχουν άθροισμα $a_{n-1}^2 - 2a_{n-2}$ και γινόμενο a_0^2. Εφαρμόστε την ανισότητα αριθμητικού - γεωμετρικού μέσου και χρησιμοποιήστε την υπόθεση $a_i \in \{-1, 1\}$ για να δείξετε ότι $n \leq 3$. Καταλήξτε ότι τα πολυώνυμα με τις ζητούμενες ιδιότητες είναι τα $\pm(x-1)$, $\pm(x+1)$, $\pm(x^2+x-1)$, $\pm(x^2-x-1)$, $\pm(x^3+x^2-x-1)$ και $\pm(x^3-x^2-x+1)$.

(70) Για το (α) δείξτε ότι οι φ, ψ δεν είναι ομομορφισμοί, αφού δε διατηρούν τον πολλαπλασιασμό και την πρόσθεση, αντίστοιχα. Για το (β) δείξτε ότι η δοσμένη απεικόνιση είναι ομομορφισμός. Για το (γ) δείξτε ότι η σ δεν είναι ομομορφισμός αφού, για παράδειγμα, έχουμε $\sigma(i) = 1$ και $\sigma(i^2) = \sigma(-1) = -1 \neq \sigma(i) \cdot \sigma(i)$. Για το (δ) δείξτε ότι η τ είναι ομομορφισμός, χρησιμοποιώντας την ισότητα $2 \cdot 2 = -1$ που ισχύει στο $\mathbb{Z}_5$ για να δείξετε ότι $\varphi(xy) = \varphi(x)\varphi(y)$ για $x, y \in \mathbb{Z}[i]$. Για το (ε) δείξτε ότι η ρ δεν είναι ομομορφισμός αφού, για παράδειγμα, έχουμε $\rho(x) = 1$ και $\rho(x^2) = 0 \neq \rho(x) \cdot \rho(x)$.

(71) Για το (β), θέτουμε

$$I \;=\; \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad J \;=\; \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

και παρατηρούμε ότι

$$\varphi\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \;=\; \varphi(aI + bJ) \;=\; a\varphi(I) + b\varphi(J)$$

για κάθε ομομορφισμό δακτυλίων $\varphi : R \to \mathbb{Z} \times \mathbb{Z}$ και όλα τα $a, b \in \mathbb{Z}$. Παρατηρούμε επίσης ότι $I^2 = I$ και $J^2 = O$ και συμπεραίνουμε ότι $(\varphi(I))^2 = \varphi(I)$ και $(\varphi(J))^2 = (0,0)$. Αφού όμως τα μόνα στοιχεία $x, y \in \mathbb{Z} \times \mathbb{Z}$ με $x^2 = x$ και $y^2 = (0,0)$ είναι τα $x \in \{(0,0), (1,0), (0,1), (1,1)\}$ και $y = (0,0)$, αντίστοιχα, συνάγουμε ότι οι μόνες δυνατότητες για τον $\varphi : R \to \mathbb{Z} \times \mathbb{Z}$ είναι να είναι ο

μηδενικός ομομορφισμός, ή ένας από τους

$$\varphi_1\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = (a,0), \quad \varphi_2\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = (0,a), \quad \varphi_3\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = (a,a).$$

(72) Θέτοντας

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

έχουμε $R = \{aI + bJ : a, b \in \mathbb{Z}\}$, όπου $J^2 = I$. Για το δεύτερο ζητούμενο στο (α), παρατηρήστε ότι $(I + J)(I - J) = O$. Για το (β), εργαστείτε όπως στη λύση της Άσκησης 71 και δείξτε ότι οι μόνοι μη μηδενικοί ομομορφισμοί είναι εκείνοι με $\varphi_1(aI + bJ) = a + b$ και $\varphi_2(aI + bJ) = a - b$. Για το (γ), συνάγετε από το (β) ότι υπάρχει ο μονομορφισμός δακτυλίων $\psi : R \to \mathbb{Z} \times \mathbb{Z}$ με $\psi(aI + bJ) = (a + b, a - b)$ και συμπεράνετε ότι ο R είναι ισόμορφος με τον υποδακτύλιο $\psi(R)$ του $\mathbb{Z} \times \mathbb{Z}$. Για το (δ), δείξτε ότι υπάρχουν μόνο δύο στοιχεία $x \in R$ με $x^2 = x$ και συμπεράνετε ότι ο R δεν είναι ισόμορφος με τον $\mathbb{Z} \times \mathbb{Z}$.

(73) Για το (α), επαληθεύστε ότι $\varphi(x+y) = \alpha(x+y)\alpha^{-1} = \alpha x\alpha^{-1} + \alpha y\alpha^{-1} = \varphi(x) + \varphi(y)$ και ότι $\varphi(xy) = \alpha(xy)\alpha^{-1} = (\alpha x)(\alpha^{-1}\alpha)(y\alpha^{-1}) = (\alpha x\alpha^{-1})(\alpha y\alpha^{-1}) = \varphi(x)\varphi(y)$ για όλα τα $x, y \in R$. Έπειτα δείξτε ότι η φ είναι 1–1 και επί, παρατηρώντας ότι για κάθε $y \in R$ η εξίσωση $\alpha x\alpha^{-1} = y$ έχει μοναδική λύση $x = \alpha^{-1}y\alpha$ ως προς x. Για το (β), εφαρμόστε το (α) στο δακτύλιο $M_2(R)$ και το αντιστρέψιμο στοιχείο του

$$\alpha = \begin{pmatrix} 0 & 1_R \\ 1_R & 0 \end{pmatrix}.$$

Εναλλακτικά, δείξτε κατευθείαν ότι η φ είναι 1–1 και επί και ότι $\varphi(x + y) = \varphi(x) + \varphi(y)$ και $\varphi(xy) = \varphi(x)\varphi(y)$ για όλα τα $x, y \in M_2(R)$. Αυτό δείχνει ότι η υπόθεση ότι ο R έχει μονάδα δεν είναι απαραίτητη. Για το (γ) παρατηρήστε ότι κατάλληλος περιορισμός του φ είναι ισομορφισμός μεταξύ των δύο δακτυλίων που αναφέρονται.

(74) Για το (α) θεωρήστε τυχαίο ομομορφισμό δακτυλίων $\varphi : \mathbb{Z} \to R$, όπου R είναι ακέραια περιοχή. Θέτοντας $\varphi(1) = a \in R$ και χρησιμοποιώντας την ιδιότητα $\varphi(x + y) = \varphi(x) + \varphi(y)$, δείξτε ότι $\varphi(x) = ax$ για κάθε $x \in \mathbb{Z}$. Χρησιμοποιώντας την ιδιότητα $\varphi(xy) = \varphi(x)\varphi(y)$, συμπεράνετε ότι $a = 0_R$ ή $a = 1_R$ και συνάγετε ότι οι μόνοι ομομορφισμοί $\varphi : \mathbb{Z} \to R$ είναι ο μηδενικός και εκείνος με $\varphi(n) = n \cdot 1_R$ για κάθε $n \in \mathbb{Z}$. Για τα (β), (γ) και (δ), συνάγετε από το (α) ότι ο ταυτοτικός ενδομορφισμός είναι ο μόνος αυτομορφισμός του $\mathbb{Z}$, ότι ο φυσικός επιμορφισμός $\mathbb{Z} \to \mathbb{Z}_p$ είναι ο μόνος μη μηδενικός ομομορφισμός δακτυλίων $\varphi : \mathbb{Z} \to \mathbb{Z}_p$ και ότι η φυσική εμβάπτιση $\iota : \mathbb{Z} \to \mathbb{Z}[x]$ είναι ο μόνος μονομορφισμός δακτυλίων $\varphi : \mathbb{Z} \to \mathbb{Z}[x]$.

(75) Για το (α) εργαστείτε όπως στην Άσκηση 30 (α) και (β). Για παράδειγμα, για πολυώνυμα $f(x) = a_0 + a_1x + \cdots + a_nx^n$ και $g(x) = b_0 + b_1x + \cdots + b_nx^n$ του $R[x]$ έχουμε

$$\begin{aligned} \tilde{\varphi}(f(x) + g(x)) &= \varphi(a_0 + b_0) + \varphi(a_1 + b_1)x + \cdots + \varphi(a_n + b_n)x^n \\ &= (\varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n) + (\varphi(b_0) + \varphi(b_1)x + \cdots + \varphi(b_n)x^n) \\ &= \tilde{\varphi}(f(x)) + \tilde{\varphi}(g(x)). \end{aligned}$$

Το (β) αφήνεται στον αναγνώστη. Για τα (γ) και (δ), εφαρμόστε το (α) στους φυσικούς επιμορφισμούς $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ και $\varphi : \mathbb{Z}_m \to \mathbb{Z}_n$, αντίστοιχα, και θέστε $\psi = \tilde{\varphi}$.

(76) Έστω $f(x) = 1 + x + x^2 + \cdots + x^{p-1}$. Δείξτε πρώτα ότι ένα πολυώνυμο $g(x) \in \mathbb{Z}[x]$ είναι ανάγωγο στο $\mathbb{Z}[x]$ αν και μόνο αν το ίδιο ισχύει για το

$g(x+1)$. Παρατηρήστε έπειτα ότι

$$f(x+1) \;=\; \frac{(x+1)^p - 1}{x} \;=\; \sum_{k=1}^{p} \binom{p}{k} x^{k-1}$$

και εφαρμόστε το κριτήριο του Eisenstein για να δείξετε ότι το $f(x+1)$, άρα και το $f(x)$, είναι ανάγωγο στο $\mathbb{Z}[x]$ για κάθε πρώτο p. Αντιστρόφως, αν $p = rs$ για ακεραίους $r, s \geq 2$, παρατηρήστε ότι $f(x) = (1 + x + x^2 + \cdots + x^{r-1})(1 + x^r + x^{2r} + \cdots + x^{r(s-1)})$ και συμπεράνετε ότι το $f(x)$ δεν είναι ανάγωγο στο $\mathbb{Z}[x]$.

(77) Για το (α) εφαρμόστε το κριτήριο του Eisenstein για $p = 11$. Για το (β) θεωρήστε την αναγωγή του δοσμένου πολυωνύμου στο $\mathbb{Z}_5[x]$ και χρησιμοποιήστε την Άσκηση 54 (β). Για το (γ) εφαρμόστε το κριτήριο του Eisenstein για $p = 7$ στο πολυώνυμο $f(x+1)$, όπως στην Άσκηση 76, όπου $f(x)$ είναι το δοσμένο πολυώνυμο.

(78) Για το (α) θεωρήστε το πολυώνυμο $f(x) = x^p - x$ και δείξτε ότι η πρόταση είναι ψευδής. Αντιθέτως, δείξτε ότι η πρόταση στο (β) είναι αληθής ως εξής. Θεωρήστε την αναγωγή $\bar{f}(x)$ του $f(x)$ στο $\mathbb{Z}_p[x]$. Παρατηρήστε ότι το $\bar{f}(x)$ έχει p σε πλήθος ρίζες στο $\mathbb{Z}_p$ και βαθμό μικρότερο του p. Συμπεράνετε ότι το $\bar{f}(x)$ είναι το μηδενικό πολυώνυμο στο $\mathbb{Z}_p[x]$ και συνεπώς ότι κάθε συντελεστής του $f(x)$ διαιρείται με το p.

(79) Για το (α) για τυχαία $c, d \in S$, θεωρήστε $a, b \in R$ με $c = \varphi(a)$ και $d = \varphi(b)$ και παρατηρήστε ότι $cd = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = dc$. Για το (β) δείξτε ότι αν 1_R είναι η μονάδα του R, τότε το $\varphi(1_R)$ είναι μονάδα του S. Για το (γ) θυμηθείτε ότι $\varphi(n \cdot a) = n \cdot \varphi(a)$ για κάθε $a \in R$. Για το (δ) για τυχαίο $b \in S$, θεωρήστε $a \in R$ με $b = \varphi(a)$ και παρατηρήστε ότι αν $a^m = 0_R$, τότε $b^m = (\varphi(a))^m = \varphi(a^m) = \varphi(0_R) = 0_S$. Για το (ε) χρησιμοποιήστε την Άσκηση 75.

(80) Για το (α) δείξτε ότι αν $a \in U(R)$, τότε το $\varphi(a)$ είναι αντιστρέψιμο στοιχείο του S με αντίστροφο το $\varphi(a^{-1})$. Το (β) είναι τετριμμένο (εξηγήστε γιατί). Για το (γ) εφαρμόστε το (α) στους ομομορφισμούς $\varphi : R \to S$ και $\varphi^{-1} : S \to R$. Για το (δ) δικιμάστε τους φυσικούς επιμορφισμούς $\varphi : \mathbb{Z} \to \mathbb{Z}_p$, όπου p είναι πρώτος αριθμός. Για το (ε) χρησιμοποιήστε το (γ) και θυμηθείτε ότι οι δακτύλιοι $\mathbb{Z}[i]$ και $\mathbb{Z}[x]$ έχουν τέσσερα και δύο αντιστρέψιμα στοιχεία, αντίστοιχα.

(81) Για το (α) παρατηρήστε ότι υπάρχει $a \in R$ με $\varphi(a) \neq 0_S$. Συμπεράνετε ότι $\varphi(a) \cdot \varphi(1_R) = \varphi(a \cdot 1_R) = \varphi(a) \neq 0_S$ και συνεπώς ότι $\varphi(1_R) \neq 0_S$. Παρατηρήστε έπειτα ότι $(\varphi(1_R))^2 = \varphi(1_R) \cdot \varphi(1_R) = \varphi(1_R \cdot 1_R) = \varphi(1_R)$, δηλαδή ότι το $\varphi(1_R)$ επαληθεύει την εξίσωση $y^2 = y$ στο S, και συμπεράνετε ότι $\varphi(1_R) = 1_S$. Για το (β) θεωρήστε την απεικόνιση $\varphi : \mathbb{Z} \to \mathbb{Z}_6$ με $\varphi(x) = 3\bar{x}$ για $x \in \mathbb{Z}$. Για το (γ) χρησιμοποιήστε το (α) και την ιδιότητα $\varphi(n \cdot x) = n \cdot \varphi(x)$ του ομομορφισμού φ. Το (δ) έπεται από το (γ), για παράδειγμα με $n = 2$.

(82) Το (α) έχει αρνητική απάντηση αφού κάθε δακτύλιος που είναι ισόμορφος με έναν πεπερασμένο δακτύλιο R πρέπει να έχει το ίδιο πλήθος στοιχείων με εκείνο του R. Για το (β) δώστε αρνητική απάντηση, παρατηρώντας ότι οι γνήσιοι υποδακτύλιοι του $\mathbb{Z}$ είναι οι $m\mathbb{Z}$ με $m \geq 2$ (Άσκηση 13) και χρησιμοποιώντας την Άσκηση 79 (α). Για το (γ) παρατηρήστε ότι για κάθε μη μηδενικό δακτύλιο S υπάρχει ο μονομορφισμός δακτυλίων $\varphi : S[x] \to S[x]$ με $\varphi(f(x)) = f(x^2)$ για κάθε $f(x) \in S[x]$. Η εικόνα αυτού του μονομορφισμού είναι γνήσιος υποδακτύλιος του $S[x]$ ο οποίος είναι ισόμορφος με τον $S[x]$.

(83) Θεωρήστε τυχαίο ομομορφισμό δακτυλίων $\varphi : \mathbb{Z}[i] \to S$, όπου ο S είναι όπως στις τρεις δοθείσες περιπτώσεις. Από την ιδιότητα $\varphi(mx+ny) = m\varphi(x)+n\varphi(y)$ του ομομορφισμού φ συμπεράνετε ότι $\varphi(a + bi) = au + bv$ για $a, b \in \mathbb{Z}$, όπου $u = \varphi(1)$ και $v = \varphi(i)$. Από τις ισότητες $1 \cdot 1 = 1$ και $i \cdot i = -1$ που ισχύουν στο $\mathbb{Z}[i]$

συμπεράνετε ότι τα $u, v \in S$ ικανοποιούν τις εξισώσεις $u^2 = u$ και $v^2 = -u$ στο S. Για το (α) δείξτε ότι οι μη μηδενικές λύσεις των εξισώσεων για το ζεύγος (u, v) στο $\mathbb{Z}_9 \times \mathbb{Z}_9$ είναι οι $(\bar{0}, \bar{3})$ και $(\bar{0}, -\bar{3})$. Δείξτε όμως ότι οι δύο απεικονίσεις που προκύπτουν, δηλαδή οι $\varphi_1, \varphi_2 : \mathbb{Z}[i] \to \mathbb{Z}_9$ με $\varphi_1(a + bi) = 3\bar{b}$ και $\varphi_2(a + bi) = -3\bar{b}$, για $a, b \in \mathbb{Z}$, δεν είναι ομομορφισμοί δακτυλίων (δε διατηρούν το γινόμενο) και συμπεράνετε ότι ο μόνος ομομορφισμός $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_9$ είναι ο μηδενικός. Για το (β) δείξτε ότι οι μη μηδενικές λύσεις των εξισώσεων για το ζεύγος (u, v) είναι οι $(\bar{1}, \bar{3})$, $(\bar{1}, -\bar{3})$ και $(\bar{5}, \bar{5})$. Επαληθεύστε ότι και οι τρείς απεικονίσεις που προκύπτουν, δηλαδή οι $\varphi_1, \varphi_2, \varphi_3 : \mathbb{Z}[i] \to \mathbb{Z}_{10}$ με $\varphi_1(a+bi) = \bar{a}+3\bar{b}$, $\varphi_2(a+bi) = \bar{a}-3\bar{b}$ και $\varphi_3(a+bi) = 5(\bar{a}+\bar{b})$, για $a, b \in \mathbb{Z}$, είναι ομομορφισμοί δακτυλίων. Για το (γ) δείξτε ότι οι εξισώσεις αυτές δεν έχουν μη μηδενικές λύσεις στο $\mathbb{Z}[x]$ και συμπεράνετε ότι ο μόνος ομομορφισμός $\varphi : \mathbb{Z}[i] \to \mathbb{Z}[x]$ είναι ο μηδενικός.

(84) Έστω αυτομορφισμός $\varphi : R \to R$, όπου $R = \mathbb{Q}$, ή $\mathbb{Z}[x]$, ή $\mathbb{Q}[x]$. Από την Άσκηση 79 (β) προκύπτει ότι $\varphi(1) = 1$ και από την ιδιότητα $\varphi(n \cdot x) = n \cdot \varphi(x)$ του ομομορφισμού φ ότι $\varphi(n) = n$ για κάθε $n \in \mathbb{Z}$. Για το (α) χρησιμοποιήστε την ίδια ιδιότητα για να δείξετε πρώτα ότι $\varphi(1/n) = 1/n$ για κάθε θετικό ακέραιο n και έπειτα ότι $\varphi(r) = r$ για κάθε $r \in \mathbb{Q}$. Συμπεράνετε ότι ο μόνος αυτομορφισμός του δακτυλίου $\mathbb{Q}$ είναι ο ταυτοτικός αυτομορφισμός. Για το (β), θέτοντας $\varphi(x) = p(x) \in \mathbb{Z}[x]$, δείξτε ότι $\varphi(f(x)) = f(p(x))$ για κάθε $f(x) \in \mathbb{Z}[x]$. Παρατηρήστε έπειτα ότι για να είναι η φ επί, θα πρέπει να υπάρχει $f(x) \in \mathbb{Z}[x]$ με $\varphi(f(x)) = x$. Συπεράνεται ότι $p(x) = x + a$ ή $p(x) = -x + a$ για κάποιο $a \in \mathbb{Z}$ και ότι οι αυτομορφισμοί του $\mathbb{Z}[x]$ είναι ακριβώς οι απεικονίσεις $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[x]$ με $\varphi(f(x)) = f(x + a)$ για $f(x) \in \mathbb{Z}[x]$ και εκείνες με $\varphi(f(x)) = f(-x + a)$ για $f(x) \in \mathbb{Z}[x]$, όπου $a \in \mathbb{Z}$. Για το (γ), εργαζόμενοι με παρόμοιο τρόπο, δείξτε ότι $\varphi(r) = r$ για κάθε αυτομορφισμό φ του $\mathbb{Q}[x]$ και $r \in \mathbb{Q}$ και ότι οι αυτομορφισμοί του $\mathbb{Q}[x]$ είναι ακριβώς οι απεικονίσεις $\varphi : \mathbb{Q}[x] \to \mathbb{Q}[x]$ με $\varphi(f(x)) = f(a + bx)$ για $f(x) \in \mathbb{Q}[x]$, όπου $a, b \in \mathbb{Q}$ και $b \neq 0$.

(85) Δείξτε ότι το I είναι ιδεώδες στις περιπτώσεις (β), (γ) και (δ), ενώ δεν είναι στις (α) και (ε). Για το (δ) χρησιμοποιήστε την Άσκηση 61 (α) για να δείξετε ότι το I είναι το κύριο ιδεώδες του $\mathbb{Z}[x]$ που παράγεται από το $(x-1)^2$. Για το (ε) παρατηρήστε ότι το I περιέχει το πολυώνυμο $g(x) = x^2 - 4x + 3$ αλλά όχι το $xg(x)$.

(86) Το (α) αφήνεται στον αναγνώστη. Για το (β) θεωρήστε τυχαίο μη μηδενικό ιδεώδες L του R. Παρατηρήστε πρώτα ότι $a \cdot 1_R \in R$ για κάθε $a \in \mathbb{F}$, όπου 1_R είναι ο 2×2 ταυτοτικός πίνακας, και συμπεράνετε ότι $ax \in L$ για κάθε $a \in \mathbb{F}$ και $x \in L$. Από τις ισότητες

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix}$$

συμπεράνετε ότι το L περιέχει κάποιο μη μηδενικό στοιχείο του I και επομένως ότι $I \subseteq L$. Υποθέτοντας ότι $L \neq I$, δείξτε ότι το L περιέχει κάποιον μη μηδενικό διαγώνιο πίνακα και διακρίνετε δύο περιπτώσεις. Αν υπάρχουν $a, c \in \mathbb{F} \setminus \{0\}$ τέτοια ώστε $\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \in L$, δείξτε ότι $L = R$ χρησιμοποιώντας τις ισότητες

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix}.$$

Αν όχι, τότε παρατηρήστε ότι είτε

$$\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{F}\right\} \subseteq L,$$

οπότε $L = J$, είτε

$$\left\{\begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix} : c \in \mathbb{F}\right\} \subseteq L,$$

οπότε $L = K$.

(87) Παρατηρούμε ότι το δοσμένο σύνολο, έστω I, είναι ιδεώδες του $\mathbb{Z}$. Αφού κάθε ιδεώδες του $\mathbb{Z}$ είναι κύριο, έχουμε $I = \{dx : x \in \mathbb{Z}\}$ για κάποιο θετικό ακέραιο d. Μάλιστα, ο d είναι ο μέγιστος κοινός διαιρέτης των a και b (εξηγήστε γιατί). Από αυτά συμπεραίνουμε ότι το I περιέχει είτε άπειρους, είτε ακριβώς έναν, είτε κανέναν πρώτο αριθμό, αναλόγως αν $d = 1$, ή αν ο d είναι πρώτος ή σύνθετος αριθμός, αντίστοιχα.

(88) Θεωρήστε τυχαίο ιδεώδες I του $\mathbb{F}[x]$. Υποθέτοντας ότι το I είναι μη μηδενικό, επιλέξτε πολυώνυμο $g(x)$ ελάχιστου βαθμού που ανήκει στο I. Παρατηρήστε ότι $\langle g(x)\rangle \subseteq I$ και δείξτε τον αντίστροφο εγκλεισμό θεωρώντας την Ευκλείδεια διαίρεση στο $\mathbb{F}[x]$ τυχαίου στοιχείου $f(x) \in I$ με το $g(x)$.

(89) Το (α) προκύπτει από το (β). Για το (β) θεωρήστε τον ομομορφισμό εκτίμησης $\varphi : \mathbb{Q}[x] \to \mathbb{C}$ με $\varphi(f(x)) = f(1 + \sqrt{2})$ για $f(x) \in \mathbb{Q}[x]$ (το ότι η απεικόνιση φ είναι ομομορφισμός δακτυλίων έπεται από την Άσκηση 30). Για το (γ) θεωρήστε το $g(x) = (x - 1 - \sqrt{2})(x - 1 + \sqrt{2}) = x^2 - 2x - 1 \in \mathbb{Q}[x]$ και παρατηρήστε ότι $\langle g(x)\rangle \subseteq I$. Για τον αντίστροφο εγκλεισμό, θεωρήστε τυχαίο πολυώνυμο $f(x) \in I$. Παρατηρήστε ότι το $g(x)$ είναι ανάγωγο πολυώνυμο στο $\mathbb{Q}[x]$ και ότι έχει την κοινή ρίζα $1 + \sqrt{2}$ με το $f(x)$. Συμπεράνετε από την Άσκηση 43 (δ) ότι το $g(x)$ διαιρεί το $f(x)$ στο $\mathbb{Q}[x]$, δηλαδή ότι $f(x) \in \langle g(x)\rangle$.

(90) Το (α) προκύπτει από το (β) (η απευθείας επαλήθευσή του αφήνεται στον αναγνώστη). Για το (β) θεωρήστε τον ομομορφισμό δακτυλίων $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_2$ με $\varphi(f(x)) = \overline{f(0)}$ για $f(x) \in \mathbb{Z}[x]$. Για το (γ) παρατηρήστε πρώτα ότι $\langle 2, x\rangle \subseteq I$, αφού το I είναι ιδεώδες που περιέχει το 2 και το x. Δείξτε έπειτα τον αντίστροφο εγκλεισμό, γράφοντας τυχαίο στοιχείο $f(x) \in I$ στη μορφή $f(x) = x\,q(x) + a$, όπου $q(x) \in \mathbb{Z}[x]$ και $a = f(0)$ είναι άρτιος αριθμός. Για το (δ) υποθέστε ότι $I = \langle g(x)\rangle$ για κάποιο $g(x) \in \mathbb{Z}[x]$. Παρατηρήστε τότε ότι το $g(x)$ διαιρεί κάθε στοιχείο του I, ειδικότερα το 2 και το x, στο $\mathbb{Z}[x]$ και καταλήξτε σε άτοπο.

(91) Για το μηδενικό ομομορφισμό $\varphi : \mathbb{Z}[i] \to S$ έχουμε $\ker(\varphi) = \mathbb{Z}[i]$ και $\operatorname{im}(\varphi) = \{0_S\}$. Για $S = \mathbb{Z}_{10}$, έστω $\varphi_1, \varphi_2, \varphi_3$ οι μη μηδενικοί ομομορφισμοί που βρέθηκαν στη λύση της Άσκησης 83. Παρατηρήστε ότι $\ker(\varphi_3) = \{a + bi \in \mathbb{Z}[i] : a + b \equiv 0 \pmod 2\}$ και $\operatorname{im}(\varphi_3) = \{\bar{0}, \bar{5}\} \subseteq \mathbb{Z}_{10}$. Λαμβάνοντας υπόψην ότι $2 = (1 + i)(1 - i) \in \langle 1 + i\rangle$, δείξτε ότι ο πυρήνας $\ker(\varphi_3)$ είναι ίσος με το κύριο ιδεώδες του $\mathbb{Z}[i]$ που παράγεται από το $1 + i$. Με ανάλογο τρόπο, δείξτε ότι οι πυρήνες των φ_1 και φ_2 παράγονται από τα $3 - i$ και $3 + i$, αντίστοιχα, και ότι $\operatorname{im}(\varphi_1) = \operatorname{im}(\varphi_2) = \mathbb{Z}_{10}$.

(92) Για το (α) παρατηρήστε ότι αν $I \subseteq \mathbb{F}$ είναι ιδεώδες που περιέχει ένα μη μηδενικό στοιχείο $a \in \mathbb{F}$, τότε $b = (ba^{-1}) \cdot a \in I$ για κάθε $b \in \mathbb{F}$ και συνεπώς $I = \mathbb{F}$. Για το (β) θεωρήστε τυχαίο μη μηδενικό ιδεώδες J του $M_n(\mathbb{F})$ και δείξτε ότι $J = M_n(\mathbb{F})$ ως εξής. Για $1 \le i, j \le n$, έστω E_{ij} ο $n \times n$ πίνακας που έχει το (i, j) στοιχείο του ίσο με 1 και τα υπόλοιπα ίσα με μηδέν. Επιλέξτε πίνακα $A = (a_{ij}) \in J$ με $a_{k\ell} = a \neq 0$ και παρατηρήστε ότι, αφού το J είναι ιδεώδες, έχουμε $a^{-1}E_{ik}AE_{\ell i} \in J$ για $1 \le i \le n$. Παρατηρήστε τώρα ότι ο $a^{-1}E_{ik}AE_{\ell i}$ είναι ο πίνακας που έχει το (i, i) στοιχείο του ίσο με 1 και τα υπόλοιπα ίσα με μηδέν. Συμπεράνετε ότι το άθροισμα αυτών των πινάκων για $1 \le i \le n$, δηλαδή ο

ταυτοτικός $n \times n$ πίνακας, ανήκει στο J και συνεπώς ότι $J = M_n(\mathbb{F})$. Για το (γ) θυμηθείτε ότι ο πυρήνας του φ είναι ιδεώδες του $M_n(\mathbb{F})$ και εφαρμόστε το (β) για να καταλήξετε στο ζητούμενο.

(93) Για το (α) παρατηρήστε ότι $0_R \in \varphi^{-1}(J)$ και θεωρήστε στοιχεία $r \in R$ και $a, b \in \varphi^{-1}(J)$, οπότε $\varphi(a), \varphi(b) \in J$. Παρατηρήστε ότι $\varphi(a+b) = \varphi(a)+\varphi(b) \in J$, ότι $\varphi(ra) = \varphi(r)\varphi(a) \in J$ και ότι $\varphi(ar) = \varphi(a)\varphi(r) \in J$ και συμπεράνετε ότι $a + b, ra, ar \in \varphi^{-1}(J)$. Για το (β) παρατηρήστε ότι $0_S = \varphi(0_R) \in \varphi(I)$ και θεωρήστε στοιχεία $s \in S$ και $\varphi(a), \varphi(b) \in \varphi(I)$ (όπου $a, b \in I$). Παρατηρήστε ότι $\varphi(a) + \varphi(b) = \varphi(a + b) \in \varphi(I)$ και επιλέξτε στοιχείο $r \in R$ με $\varphi(r) = s$ για να δείξετε ότι $s\varphi(a) = \varphi(r)\varphi(a) = \varphi(ra) \in \varphi(I)$ και ότι $\varphi(a)s = \varphi(a)\varphi(r) = \varphi(ar) \in \varphi(I)$. Εργαστείτε με παρόμοιο τρόπο για το (γ). Για το (δ) υποθέστε ότι το J είναι ιδεώδες του S και θεωρήστε το ιδεώδες $I = \varphi^{-1}(J)$ του R. Παρατηρήστε ότι $J = \varphi(I)$ (αφού η φ είναι επί, η ισότητα αυτή ισχύει για κάθε υποσύνολο J του S) και εφαρμόστε το (γ) για $m = 1$ για να συμπεράνετε ότι το J είναι κύριο ιδεώδες του S. Για το (ε) εφαρμόστε το (δ) στο φυσικό επιμορφισμό $\varphi : \mathbb{Z} \to \mathbb{Z}_m$. Για το (στ) δώστε αρνητική απάντηση, θεωρώντας το μονομορφισμό $\varphi : \mathbb{Z} \to \mathbb{Q}$ με $\varphi(n) = n$ για κάθε $n \in \mathbb{Z}$.

(94) Το (α) αφήνεται στον αναγνώστη. Για το (β) θεωρήστε τυχαίο ιδεώδες K του $R \times S$. Θεωρήστε τους φυσικούς επιμορφισμούς δακτυλίων $\varphi : R \times S \to R$ και $\psi : R \times S \to S$ με $\varphi(a, b) = a$ και $\psi : (a, b) = b$ για $(a, b) \in R \times S$ και συμπεράνετε από την Άσκηση 93 (β) ότι το $I = \varphi(K)$ είναι ιδεώδες του R και ότι το $J = \psi(K)$ είναι ιδεώδες του S. Παρατηρήστε ότι $K \subseteq I \times J$ και δείξτε τον αντίστροφο εγκλεισμό ως εξής. Θεωρήστε τυχαίο στοιχείο $(a, b) \in I \times J$. Παρατηρήστε ότι αφού $a \in I$, υπάρχει $b' \in S$ τέτοιο ώστε $(a, b') \in K$. Αφού το K είναι ιδεώδες του $R \times S$, συμπεράνετε ότι $(a, 0_S) = (1_R, 0_S)(a, b') \in K$. Δείξτε με παρόμοιο τρόπο ότι $(0_R, b) \in K$ και συμπεράνετε ότι $(a, b) = (a, 0_S) + (0_R, b) \in K$. Για το (γ) θεωρήστε το δακτύλιο $2\mathbb{Z} \times 2\mathbb{Z}$ και το υποσύνολό του K που αποτελείται από τα ζεύγη $(a, b) \in 2\mathbb{Z} \times 2\mathbb{Z}$ για τα οποία το $a + b$ είναι ακέραιο πολλαπλάσιο του 4. Επαληθεύστε ότι το K είναι ιδεώδες του $2\mathbb{Z} \times 2\mathbb{Z}$ το οποίο περιέχει το ζεύγος $(2, 2)$ αλλά όχι το $(2, 0)$ και συμπεράνετε ότι το K δεν είναι της μορφής $I \times J$.

(95) Το (α) αφήνεται στον αναγνώστη (και θεωρείται γνωστό). Για το (β) επιλέξτε στοιχεία $a \in I$ και $b \in J$ με $a + b = 1_R$. Παρατηρήστε ότι για κάθε $x \in I \cap J$ ισχύει $x = x \cdot 1_R = x(a + b) = xa + xb = ax + xb \in IJ$ και συμπεράνετε ότι $I \cap J \subseteq IJ$. Για το (γ) θεωρήστε τον υποδακτύλιο $R = 2\mathbb{Z}$ του $\mathbb{Z}$ και τα ιδεώδη $I = 4\mathbb{Z}$ και $J = 6\mathbb{Z}$ του R. Για το (δ) θεωρήστε το δακτύλιο $R = \mathbb{Z}$ και τα ιδεώδη $I = 2\mathbb{Z}$ και $J = 4\mathbb{Z}$.

(96) Για το (α), χρησιμοποιώντας τις υποθέσεις $I + J = R$ και $I \cap J = \{0_R\}$, δείξτε ότι για κάθε $x \in R$ υπάρχει μοναδικό ζεύγος $(a, b) \in I \times J$ τέτοιο ώστε $x = a+b$. Θεωρήστε την απεικόνιση $\varphi : R \to I \times J$ που ορίζεται θέτοντας $\varphi(x) = (a, b)$ για $x \in R$, όπου τα $a \in I$ και $b \in J$ είναι όπως πριν. Παρατηρήστε ότι η φ είναι 1–1 και επί και δείξτε ότι $\varphi(x + y) = \varphi(x) + \varphi(y)$ για $x, y \in R$. Έπειτα, συμπεράνετε από την υπόθεση $I \cap J = \{0_R\}$ ότι ισχύει $ab = ba = 0_R$ για όλα τα $a \in I$ και $b \in J$ και δείξτε ότι $\varphi(xy) = \varphi(x)\varphi(y)$ για $x, y \in R$. Το (β) προκύπτει από το (α).

(97) Αφού οι R και S περιέχουν το $\mathbb{Z}_p$ ως υποδακτύλιο, το πολυώνυμο $f(t) = t^p - t$ παραγοντοποιείται στα $R[t]$ και $S[t]$ κατά τα γνωστά ως

$$f(t) \;=\; t(t-1)\cdots(t-p+1) \;=\; \prod_{k=1}^{p}(t+k).$$

Αφού $k^2+1 = k^2-\alpha^2 = (k-\alpha)(k+\alpha)$ στο R, υπολογίζουμε ότι

$$\prod_{k=1}^{p}(k^2+1) \;=\; \prod_{k=1}^{p}(k-\alpha)(k+\alpha) \;=\; \prod_{k=1}^{p}(k-\alpha)\prod_{k=1}^{p}(k+\alpha) \;=\; f(-\alpha)f(\alpha)$$

$$=\; ((-\alpha)^p+\alpha)\cdot(\alpha^p-\alpha) \;=\; -(\alpha^p-\alpha)^2 \;=\; 2+2\alpha^{p+1}$$

στο R. Διακρίνοντας τις περιπτώσεις $p=2$, $p\equiv 1 \pmod 4$ και $p\equiv 3 \pmod 4$, συμπεραίνουμε για το (α) ότι

$$\prod_{k=1}^{p}(k^2+1) \;=\; \begin{cases} 0, & \text{αν } p=2 \text{ ή } p\equiv 1 \pmod 4,\\ 4, & \text{αν } p\equiv 3 \pmod 4. \end{cases}$$

Εργαζόμαστε ομοίως για το (β) με την παραγοντοποίηση $k^2+k+1 = (k-\beta)(k-\beta^2)$ που ισχύει στο S και βρίσκουμε ότι

$$\prod_{k=1}^{p}(k^2+k+1) \;=\; \begin{cases} 0, & \text{αν } p=3 \text{ ή } p\equiv 1 \pmod 3,\\ 3, & \text{αν } p\equiv 2 \pmod 3 \end{cases}$$

στο S. Αφού οι παραπάνω ταυτότητες πρέπει να ισχύουν και στο $\mathbb{Z}_p$, έπεται ότι η απάντηση στο (γ) είναι οι πρώτοι $p=2$ και $p\equiv 1 \pmod 4$ και στο (δ) οι πρώτοι $p=3$ και $p\equiv 1 \pmod 3$.

(98) Έστω $y = x+I$ η κλάση του x στο R. Παρατηρήστε ότι ισχύει $y^2+y+1=0$ στο R, οπότε $y^2=-y-1$ και $y^3=1$. Γράψτε το n στη μορφή $n=6q+r$ με $q\in\mathbb{N}$ και $r\in\{0,1,2,3,4,5\}$ και παρατηρήστε ότι στο R έχουμε

$$f_n(y) \;=\; (y+1)^n+y^n+1 \;=\; (-y^2)^n+y^n+1 \;=\; (-1)^r y^{2r}+y^r+1,$$

αφού $y^6=1$. Εξετάζοντας κάθε τιμή του r ξεχωριστά, συμπεράνετε ότι $f_n(y) = 3, 2+2y, 0, 1, 0, -2y$, οπότε $a_n+b_nx = 3, 2+2x, 0, 1, 0, -2x$, αν $r=0,1,2,3,4,5$, αντίστοιχα. Για το (β) παρατηρήστε ότι το $f_n(x)$ διαιρείται με το x^2+x+1 στο $\mathbb{Z}[x]$ αν και μόνο αν $a_n=b_n=0$ και χρησιμοποιήστε το αποτέλεσμα του (α).

(99) Το (α) αφήνεται στον αναγνώστη. Για το (β), δείξτε ότι η απεικόνιση $\varphi : R \to \mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ που ορίζεται θέτοντας

$$\varphi\begin{pmatrix} a & b \\ b & a+b \end{pmatrix} \;=\; a+bx+\langle x^2+x+1\rangle$$

είναι ισομορφισμός δακτυλίων. Το (γ) έπεται από το (β), αφού το x^2+x+1 είναι ανάγωγο πολυώνυμο στο $\mathbb{Z}_2[x]$ και συνεπώς ο δακτύλιος $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ είναι σώμα.

(100) Έστω α η κλάση του x στον R, οπότε έχουμε $\alpha^2=-2=1$ στο R. Για το (α) θυμηθείτε ότι τα στοιχεία του R είναι τα $a+b\alpha$ με $a,b\in\{-1,0,1\}$, άρα ακριβώς 9 σε πλήθος. Για το (β) δείξτε ότι $U(R)=\{\pm 1,\pm\alpha\}$ παρατηρώντας ότι τα $\pm 1, \pm\alpha$ είναι αντιτρέψιμα στοιχεία του R, αφού ισχύει $(-1)^2=\alpha^2=1$ στο R, ενώ τα $\pm(\alpha-1), \pm(\alpha+1)$ δεν είναι, αφού $(\alpha-1)(\alpha+1)=0$.

(101) Για το (α) παρατηρήστε πρώτα ότι $\mu\kappa\delta(f(x),g(x))=1$ αν και μόνο αν υπάρχουν πολυώνυμα $a(x), b(x)\in\mathbb{F}[x]$ με $a(x)f(x)+b(x)g(x)=1$. Δείξτε έπειτα ότι το τελευταίο ισχύει αν και μόνο αν υπάρχει $a(x)\in\mathbb{F}[x]$ τέτοιο ώστε να ισχύει $(a(x)+I)(f(x)+I)=1+I$ στο R. Για το (β) συνάγετε από το (α) ότι το $f(x)+I$ είναι αντιστρέψιμο στοιχείο του R αν και μόνο αν το -1 δεν είναι ρίζα του $f(x)$ και συμπεράνετε ότι το ζητούμενο πλήθος είναι ίσο με q^n-q^{n-1}.

(102) Για το (α) εφαρμόστε το Θεώρημα του Ισομορφισμού στον ομομορφισμό δακτυλίων $\varphi : R\times S \to (R/I)\times(S/J)$ που ορίζεται θέτοντας $\varphi(a,b)=(\pi(a),\rho(b))$ για $a\in R$ και $b\in S$, όπου $\pi : R\to R/I$ και $\rho : S\to S/J$ είναι οι φυσικοί επιμορφισμοί. Το (β) είναι η ειδική περίπτωση $R=S=\mathbb{Z}$, $I=m\mathbb{Z}$, $J=n\mathbb{Z}$ του (α).

(103) Για το (α) εφαρμόστε το Θεώρημα του Ισομορφισμού στον ομομορφισμό δακτυλίων $\varphi : \mathbb{Z}[x] \to \mathbb{C}$ με $\varphi((f(x)) = f(i)$ για $f(x) \in \mathbb{Z}[x]$. Παρατηρήστε πρώτα ότι $\mathrm{im}(\varphi) = \mathbb{Z}[i]$ και θεωρήστε έπειτα την Ευκλείδεια διαίρεση τυχαίου πολυωνύμου $f(x) \in \mathbb{Z}[x]$ με το $x^2 + 1$ για να δείξετε ότι $\ker(\varphi) = \langle x^2 + 1 \rangle$. Εργασθείτε με παρόμοιο τρόπο για τα (β) και (γ), χρησιμοποιώντας τους ομομορφισμούς $\varphi : R[x] \to R \times R$ με $\varphi((f(x)) = (f(1_R), f(-1_R))$ για $f(x) \in R[x]$ και $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_{17}$ με $\varphi(a + bi) = \bar{a} + 4\bar{b}$ για $a, b \in \mathbb{Z}$, αντίστοιχα.

(104) Για το (α) θεωρήστε τον ομομορφισμό δακτυλίων $\psi = \pi \circ \varphi : R \to R/J$, όπου $\pi : R \to R/J$ είναι ο κανονικός επιμορφισμός. Δείξτε ότι ο ψ είναι επιμορφισμός δακτυλίων με $\ker(\psi) = I$ και συνάγετε το ζητούμενο από το Θεώρημα του Ισομορφισμού. Για το (β) θεωρήστε το δακτύλιο $R = \mathbb{F}[x, y] / \langle x^3, xy, y^2 \rangle$, όπου $\mathbb{F}$ είναι τυχαίο σώμα, και τα κύρια ιδεώδη I και J του R που παράγονται από τις κλάσεις των x^2 και y, αντίστοιχα. Παρατηρήστε ότι ως υποδακτύλιοι του R, τα I και J είναι ισόμορφα με το δακτύλιο $\mathbb{F}$, στον οποίο η πρόσθεση είναι η πρόσθεση του σώματος $\mathbb{F}$ και ο πολλαπλασιασμός ορίζεται θέτοντας $ab = 0$ για όλα τα $a, b \in \mathbb{F}$. Δείξτε έπειτα ότι ο δακτύλιος πηλίκο R/I δεν είναι ισόμορφος με τον R/J, για παράδειγμα αφού τα στοιχεία α του R/I με $\alpha^2 = 0$ αποτελούν $\mathbb{F}$-διανυσματικό υπόχωρο του R διάστασης 2, ενώ τα αντίστοιχα στοιχεία του R/J αποτελούν $\mathbb{F}$-διανυσματικό υπόχωρο του R διάστασης 1.

(105) Παρατηρήστε πρώτα ότι ο $\mathbb{Z}_4$ δεν είναι ισόμορφος με κανέναν από τους υπόλοιπους δακτυλίους, αφού σε αυτούς ισχύει $-x = x$ για κάθε στοιχείο τους x, ενώ στον $\mathbb{Z}_4$ έχουμε $-1 \neq 1$. Παρατηρήστε επίσης ότι ο $\mathbb{Z}_2 \times \mathbb{Z}_2$ δεν είναι ισόμορφος με κανέναν από τους υπόλοιπους δα-κτυλίους, αφού ισχύει $x^2 = x$ για κάθε $x \in \mathbb{Z}_2 \times \mathbb{Z}_2$, ενώ τους υπόλοιπους δεν ισχύει το ίδιο. Δείξτε ότι οι δακτύλιοι στα (γ), (δ) και (ε) είναι μεταξύ τους ισόμορφοι ως εξής. Δείξτε ότι οι (δ) και (ε) είναι ισόμορφοι θεωρώντας τον αυτομορφισμό φ του $\mathbb{Z}_2[x]$ με $\varphi(f(x)) = f(x + 1)$ για $f(x) \in \mathbb{Z}_2[x]$, παρατηρώντας ότι ισχύει $(x + 1)^2 = x^2 + 1$ στο $\mathbb{Z}_2[x]$ και χρησιμοποιώντας την Άσκηση 104 (α). Τέλος, αν R είναι ο δακτύλιος του (γ), δείξτε ότι η απεικόνιση $\psi : R \to \mathbb{Z}_2[x] / \langle x^2 \rangle$ που ορίζεται θέτοντας

$$\psi\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = a + bx + \langle x^2 \rangle$$

είναι ισομορφισμός δακτυλίων.

(106) Δείξτε πρώτα ότι οι δακτύλιοι (α) και (γ) είναι ισόμορφοι θεωρώντας τον αυτομορφισμό φ του $\mathbb{Q}[x]$ που ορίζεται θέτοντας $\varphi(f(x)) = f(2x)$ για $f(x) \in \mathbb{Q}[x]$ και εφαρμόζοντας την Άσκηση 104 (α) (ή παρατηρώντας ότι και οι δύο δακτύλιοι είναι ισόμορφοι με το γινόμενο $\mathbb{Q} \times \mathbb{Q}$). Δείξτε με τον ίδιο τρόπο ότι οι δακτύλιοι (ε) και (στ) είναι επίσης ισόμορφοι. Παρατηρήστε έπειτα ότι οι δακτύλιοι (α) και (γ) δεν είναι ακέραιες περιοχές και επομένως ότι δεν είναι ισόμορφοι με κανέναν από τους υπόλοιπους δακτυλίους (οι οποίοι είναι όλοι σώματα). Στη συνέχεια, δείξτε ότι ο δακτύλιος (β) είναι ισόμορφος με τον υποδακτύλιο (υπόσωμα) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ του $\mathbb{R}$ και συμπεράνετε ότι ο δακτύλιος αυτός δεν είναι ισόμορφος με κανέναν από τους (δ) και (ε), αφού αυτοί περιέχουν στοιχεία α και β, αντίστοιχα, με $\alpha^2 = -1$ και $\beta^2 = -2$. Δείξτε τέλος ο δακτύλιος (ε) δεν περιέχει στοιχείο α με $\alpha^2 = -1$ και συμπεράνετε ότι δεν είναι ισόμορφος με τον (δ).

(107) Το (α) αφήνεται στον αναγνώστη. Για το (γ), εκτελώντας τις σχετικές πράξεις, δείξτε πρώτα ότι

$$R = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & c \end{pmatrix} : a, b, c \in \mathbb{F} \right\}.$$

Δείξτε έπειτα ότι η απεικόνιση $\varphi : R \to \mathbb{F}[t] / \langle t^3 \rangle$ που ορίζεται θέτοντας

$$\varphi \begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & c \end{pmatrix} = a + bt + ct^2 + \langle t^3 \rangle$$

είναι ισομορφισμός δακτυλίων. Το (β) είναι άμεση συνέπεια του (γ).

(108) Το (α) είναι τετριμμένο. Για το (β) χρησιμοποιήστε την Ευκλείδεια διαίρεση στο $\mathbb{F}[x]$ για να δείξετε ότι για κάθε $f(x) \in \mathbb{F}[x]$ υπάρχουν μοναδικά $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}$ τέτοια ώστε να ισχύει $f(x) + \langle g(x) \rangle = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ στο R και συμπεράνετε ότι το σύνολο $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ αποτελεί βάση του $\mathbb{F}$-διανυσματικού χώρου R. Για το (γ), χρησιμοποιώντας το (β), παρατηρήστε ότι το $\{\alpha^i : i \in S\}$ είναι γραμμικώς εξαρτημένο υποσύνολο του R και συνάγετε το ζητούμενο.

(109) Για το (α) παρατηρήστε ότι $\mathbb{F}[x] / \langle x - a \rangle \cong \mathbb{F}$ για κάθε $a \in \mathbb{F}$ και συμπεράνετε ότι η πρόταση είναι ψευδής. Για το (β), υποθέστε ότι οι δακτύλιοι πηλίκο $\mathbb{F}[x] / \langle f(x) \rangle$ και $\mathbb{F}[x] / \langle g(x) \rangle$ είναι ισόμορφοι. Δείξτε τότε ότι αυτοί είναι ισόμορφοι και ως $\mathbb{F}$-διανυσματικοί χώροι και χρησιμοποιήστε την Άσκηση 108 (β) για να συμπεράνετε ότι $\deg(f(x)) = \deg(g(x))$.

(110) Έστω $\alpha = x + \langle x^p - x \rangle$ η κλάση του x στο δακτύλιο R. Τότε $\alpha^p = \alpha$ και κάθε $y \in R$ γράφεται (μοναδικά) στη μορφή $y = a_0 + a_1\alpha + \cdots + a_{p-1}\alpha^{p-1}$ για κάποιους συντελεστές $a_i \in \mathbb{Z}_p$. Χρησιμοποιώντας την Άσκηση 4 (β) και το γεγονός ότι $a^p = a$ για κάθε $a \in \mathbb{Z}_p$, δείξτε ότι $y^p = y$ και συμπεράνετε ότι ισχύει το (α). Για το (β), ας υποθέσουμε ότι οι δακτύλιοι R και S είναι ισόμορφοι. Αφού οι R και S έχουν p^p και q^q στοιχεία, αντίστοιχα, έχουμε αναγκαστικά $p = q$. Επομένως, αν $\beta = x + \langle x^p + x \rangle$ είναι η κλάση του x στον S, τότε $\beta^p = -\beta$. Αφού όμως οι R και S είναι ισόμορφοι, από το (α) προκύπτει ότι $y^p = y$ για κάθε $y \in S$, οπότε και $\beta^p = \beta$. Άρα, $-\beta = \beta$. Αφού το β είναι μη μηδενικό στοιχείο του S, από την τελευταία ισότητα έπεται ότι $p = 2$.

(111) Δείξτε ότι η πρόταση στο (α) είναι αληθής, πολλαπλασιάζοντας πρώτα την ισότητα $abc = e$ από αριστερά με a^{-1} και έπειτα την ισότητα που προκύπτει από δεξιά με a. Δείξτε επίσης ότι η πρόταση στο (β) είναι ψευδής, θεωρώντας τυχαία στοιχεία a, b μιας μη αβελιανής ομάδας για τα οποία ισχύει $ab \neq ba$ και θέτοντας $c = (ab)^{-1}$.

(112) Για το (α) χρησιμοποιήστε την Άσκηση 6 (β) και (γ). Το ουδέτερο στοιχείο της $U(R)$ είναι η μονάδα του R. Για το (β) θυμηθείτε από την Άσκηση 11 (α) ότι $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$. Αφού $i^2 = -1$, $i^3 = -i$ και $i^4 = 1$, η ομάδα αυτή είναι κυκλική τάξης 4. Για το (γ) δείξτε ότι για έναν άνω τριγωνικό πίνακα $A \in M_n(F)$ ισχύει $A \in U(R)$ αν και μόνο αν το γινόμενο των διαγωνίων στοιχείων του A είναι αντιστρέψιμο στοιχείο του F ως εξής. Παρατηρήστε πρώτα ότι αν υπάρχει πίνακας $B \in M_n(F)$ με $AB = 1_R$, τότε $\det(A)\det(B) = \det(AB) = \det(1_R) = 1_F$ και συμπεράνετε ότι $\det(A) \in U(F)$. Αντιστρόφως, αν $\det(A) \in U(F)$, χρησιμοποίστε το Θεώρημα Cayley-Hamilton για να δείξετε ότι υπάρχει πολυώνυμο $p(x) \in F(x)$ τέτοιο ώστε $A \cdot p(A) = p(A) \cdot A = 1_R$. Παρατηρήστε ότι $p(A) \in R$ και συμπεράνετε ότι $A \in U(R)$.

(113) Για το (α) δείξτε ότι η σύνθεση αυτομορφισμών, καθώς και η αντίστροφη απεικόνιση ενός αυτομορφισμού, του R είναι επίσης αυτομορφισμοί του R. Ουδέτερο στοιχείο για τη σύνθεση αυτομορφισμών του R είναι ο ταυτοτικός αυτομορφισμός του R. Για το (β) δείξτε ότι $\mathrm{Aut}(R)$ είναι η ομάδα με δύο στοιχεία ως εξής. Θεωρήστε τυχαίο αυτομορφισμό φ του $\mathbb{Q}[\sqrt{2}]$ και δείξτε, όπως στη λύση της Άσκησης 84, ότι $\varphi(x) = x$ για κάθε $x \in \mathbb{Q}$. Θέτοντας $\alpha = \sqrt{2}$, παρατηρήστε ότι $\alpha^2 = 2$ και συνεπώς ότι $(\varphi(\alpha))^2 = 2$. Συμπεράνετε

ότι $\varphi(\alpha) \in \{\alpha, -\alpha\}$ και ότι οι μόνοι αυτομορφισμοί του $\mathbb{Q}[\sqrt{2}]$ είναι ο ταυτοτικός και η απεικόνιση $\varphi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]$ με $\varphi(a + b\sqrt{2}) = a - \sqrt{2}$ για $a, b \in \mathbb{Q}$.

(114) Η πρόταση είναι αληθής. Από την ισότητα $a^{13} b^8 = e$ παίρνουμε $b^8 = a^{-13}$ και $b^{40} = a^{-65}$. Ομοίως, από την ισότητα $a^8 b^5 = e$ παίρνουμε $b^5 = a^{-8}$ και $b^{40} = a^{-64}$. Συμπεραίνουμε ότι $a^{-65} = a^{-64}$ και συνεπώς ότι $a = e$. Με παρόμοιο τρόπο βρίσκουμε ότι $b = e$.

(115) Το (α) αφήνεται στον αναγνώστη. Για το (β) παρατηρήστε ότι $a^3 = a^{-1}$ και συμπεράνετε ότι $a^{-1}b = ba^{-1}$. Πολλαπλασιάστε την τελευταία σχέση από αριστερά και από δεξιά με το a και καταλήξτε στην ισότητα $ab = ba$. Για το (γ) γράψτε τη δοσμένη σχέση $a^3 b = ba^3$ ως $a^3 = ba^3 b^{-1}$. Υψώνοντας στο τετράγωνο, δείξτε ότι

$$a^6 \;=\; (ba^3b^{-1})(ba^3b^{-1}) \;=\; ba^3(b^{-1}b)a^3b^{-1} \;=\; ba^6b^{-1}$$

και χρησιμοποιήστε την ισότητα $a^6 = a$. Για το (δ) παρατηρήστε ότι $r = 3q + 1$ ή $r = 3q + 2$ για κάποιο φυσικό αριθμό q και εργασθείτε όπως προηγουμένως στο (γ).

(116) Για το (α) παρατηρούμε ότι $a = bab^{-1}$. Υψώνουμε στη δύναμη m και βρίσκουμε ότι

$$\begin{aligned} a^m &= (bab^{-1})(bab^{-1}) \cdots (bab^{-1}) \\ &= ba(b^{-1}b)a(b^{-1}b) \cdots (b^{-1}b)ab^{-1} \;=\; ba^m b^{-1}, \end{aligned}$$

δηλαδή ότι $a^m b = ba^m$. Επαναλαμβάνουμε το ίδιο επιχείρημα και υψώνουμε στη δύναμη n την $b = a^m b a^{-m}$. Για το (β) εφαρμόζουμε το (α) και συμπεραίνουμε ότι $a^{km} b^{\ell n} = b^{\ell n} a^{km}$ για όλα τα $k, \ell \in \mathbb{Z}$. Επιλέγουμε τα k και ℓ έτσι ώστε $km \equiv 1 \pmod{p}$ και $\ell n \equiv 1 \pmod{q}$ και συμπεραίνουμε ότι $ab = ba$.

(117) Για το (α) θεωρήστε το σύνολο $T = \{a^{-1}x : a \in S\}$. Δείξτε ότι το πλήθος των στοιχείων του T είναι ίσο με εκείνο του S και συμπεράνετε ότι $S \cap T \neq \varnothing$. Επιλέξτε στοιχείο $b \in S \cap T$ και παρατηρήστε ότι $x = ab$ για κάποιο $a \in S$. Για το (β) θεωρήστε, για παράδειγμα, τη διεδρική ομάδα G των συμμετριών του κανονικού n-γώνου και το υποσύνολο S που αποτελείται από όλες τις στροφές στη G (συμπεριλαμβανομένης της στροφής κατά γωνία μηδέν).

(118) Αρκεί να δείξουμε ότι η ομάδα G είναι αβελιανή, αφού τότε για οποιαδήποτε $a, b \in G\setminus\{e\}$ θα έχουμε $b = xax^{-1} = xx^{-1}a = a$ για κάποιο $x \in G$, και συνεπώς $a = b$. Θεωρούμε τυχαίο στοιχείο $a \in G$ και την απεικόνιση $f : G\setminus\{e\} \to G\setminus\{e\}$ που ορίζεται θέτοντας $f(x) = xax^{-1}$ για $x \in G\setminus\{e\}$. Από την υπόθεση της άσκησης έχουμε ότι η f είναι επί. Αφού το σύνολο $G\setminus\{e\}$ είναι πεπερασμένο, η f είναι και 1–1. Συμπεραίνουμε ότι $a^2 = e$, αφού διαφορετικά θα είχαμε $f(a^2) = a = f(a)$ και επομένως $a^2 = a$, σε αντίθεση με την υπόθεση $a \neq e$. Δείξαμε λοιπόν ότι $a^2 = e$ για κάθε $a \in G$. Ισοδύναμα, έχουμε $a^{-1} = a$ για κάθε $a \in G$. Έπεται ότι για όλα τα $a, b \in G$ ισχύει $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ και επομένως ότι η ομάδα G είναι αβελιανή.

(119) Για το (α) θυμηθείτε ότι ένας άνω τριγωνικός πίνακας $A \in M_n(\mathbb{F}_q)$ είναι αντιστρέψιμος αν και μόνο αν κάθε στοιχείο της κύριας διαγωνίου του A είναι μη μηδενικό. Άρα, υπάρχουν $q - 1$ επιλογές για κάθε τέτοιο στοιχείο του A και q επιλογές για καθένα από τα υπόλοιπα $\binom{n}{2}$ στοιχεία. Συμπεράνετε ότι η ζητούμενη τάξη είναι ίση με $(q-1)^n q^{\binom{n}{2}}$. Για το (β) παρατηρήστε ότι ένας πίνακας $A \in M_n(\mathbb{F}_q)$ είναι αντιστρέψιμος αν και μόνο αν δεν υπάρχει στήλη του A η οποία να είναι γραμμικός συνδυασμός των προηγουμένων. Συμπεράνετε ότι υπάρχουν $q^n - 1$ επιλογές για την πρώτη στήλη του A (ώστε αυτή να είναι μη μηδενική), υπάρχουν $q^n - q$ επιλογές για τη δεύτερη στήλη (ώστε αυτή να είναι μην είναι πολλαπλάσιο της πρώτης), υπάρχουν $q^n - q^2$ επιλογές για την τρίτη στήλη (ώστε αυτή να είναι μην είναι γραμμικός

συνδυασμός των δύο πρώτων) και ούτω καθεξής, και ότι η ζητούμενη τάξη είναι ίση με $q^{\binom{n}{2}}(q-1)(q^2-1)\cdots(q^n-1)$.

(120) Για το (α), παρατηρήστε ότι τα στοιχεία τάξης 2 της G, μαζί με το ουδέτερο στοιχείο, είναι ακριβώς τα στοιχεία $a \in G$ με $a^{-1} = a$. Παρατηρήστε επίσης ότι τα υπόλοιπα στοιχεία της G διαμερίζονται σε δισύνολα της μορφής $\{a^{-1}, a\}$, και συνεπώς ότι είναι άρτιου πλήθους, για να συμπεράνετε το ζητούμενο. Για το (β) παρατηρήστε ότι τα στοιχεία τάξης 2 της δοσμένης ομάδας είναι οι ανακλάσεις στους n άξονες συμμετρίας του κανονικού n-γώνου, καθώς και η στροφή κατά γωνία π, όταν αυτή είναι στοιχείο της ομάδας (δηλαδή όταν ο n είναι άρτιος). Συμπεράνετε ότι το ζητούμενο πλήθος είναι ίσο με n ή $n+1$, αν ο n είναι περιττός ή άρτιος αριθμός, αντίστοιχα.

(121) Θεωρήστε ομάδα G με δύο διαφορετικά στοιχεία a, b τάξης 2. Δείξτε πρώτα ότι αν $ab = ba$, τότε το ab είναι στοιχείο τάξης 2 της G διαφορετικό από τα a και b. Υποθέστε έπειτα ότι $ab \neq ba$ και δείξτε ότι το aba είναι στοιχείο τάξης 2 της G διαφορετικό από τα a και b.

(122) Για το (α) υποθέστε ότι $a^m = e$. Θεωρήστε την Ευκλείδεια διαίρεση $m = nq + r$ του m με το n, δείξτε ότι $a^r = e$ και συμπεράνετε ότι $r = 0$. Το αντίστροφο αφήνεται στον αναγνώστη. Για το (β) συμπεράνετε από το Θεώρημα του Euler και το (α) ότι η ζητούμενη τάξη είναι διαιρέτης του 20 και δείξτε έπειτα ότι είναι η τάξη αυτή ίση με 20. Για το (γ) εφαρμόστε επαγωγή στο m για να δείξετε ότι η ζητούμενη τάξη είναι ίση με $\phi(5^m) = 4 \cdot 5^{m-1}$ ως εξής. Παρατηρήστε πρώτα ότι το ζητούμενο ισχύει για $m = 1$ και, σύμφωνα την απάντηση στο (β), για $m = 2$ και υποθέστε ότι ισχύει για το $m \geq 2$. Θεωρήστε την τάξη n του 2 στην πολλαπλασιαστική ομάδα $U(\mathbb{Z}_{5^{m+1}})$. Από το Θεώρημα του Euler και το (α) συμπεράνετε ότι το n διαιρεί το $\phi(5^{m+1}) = 4 \cdot 5^m$. Από την παρατήρηση ότι $2^n \equiv 1 \pmod{5^m}$, το (α) και την υπόθεση της επαγωγής συμπεράνετε ότι το n διαιρείται με το $4 \cdot 5^{m-1}$. Επομένως αρκεί να αποκλειστεί η περίπτωση $n = 4 \cdot 5^{m-1}$. Υποθέστε, αντιθέτως, ότι $n = 4 \cdot 5^{m-1}$. Από το Θεώρημα του Euler έχουμε ότι $2^{4\cdot 5^{m-2}} = 1 + q \cdot 5^{m-1}$ για κάποιο θετικό ακέραιο q. Από την υπόθεση της επαγωγής συμπεράνετε ότι το q δε διαιρείται με το 5. Υπολογίστε τώρα ότι

$$\begin{aligned} 2^{4\cdot 5^{m-1}} &= (1 + q \cdot 5^{m-1})^5 \\ &= 5^{m+1}\,(q^5 \cdot 5^{4m-6} + q^4 \cdot 5^{3m-4} + 2q^3 \cdot 5^{2m-3} + 2q^2 \cdot 5^{m-2}) \;+\; q \cdot 5^m \;+\; 1, \end{aligned}$$

σε αντίθεση με την υπόθεση $2^{4\cdot 5^{m-1}} = 2^n \equiv 1 \pmod{5^{m+1}}$. Από την αντίφαση αυτή συμπεράνετε ότι $n = 4 \cdot 5^m$.

(123) Για το (α) παρατηρήστε πρώτα ότι $(ab)^{pq} = a^{pq}b^{pq} = e$. Υποθέστε έπειτα ότι $(ab)^m = e$ για κάποιο θετικό ακέραιο m και δείξτε ότι ο m είναι ακέραιο πολλαπλάσιο του pq ως εξής. Από την υπόθεση έχουμε $a^m b^m = e$. Θέτοντας $c = a^m = b^{-m}$ και χρησιμοποιώντας τις σχέσεις $a^p = b^q = e$, δείξτε ότι $c^p = c^q = e$. Από την Άσκηση 122 (α) συμπεράνετε ότι $c = e$. Από την ίδια άσκηση και τις σχέσεις $a^m = b^m = e$ συμπεράνετε ότι ο m είναι ακέραιο πολλαπλάσιο των p και q και συνάγετε το ζητούμενο. Απάντηση για το (β): οι πιθανές τιμές είναι οι 1 και 5. Απάντηση για το (γ): οι πιθανές τιμές είναι οι 1, 2 και 4. Για να δείξετε ότι η τιμή 2 είναι εφικτή θεωρήστε, για παράδειγμα, τα στοιχεία $a = b = (1\ 2\ 3\ 4)$ της S_4, ή τα στοιχεία $a = (1\ 2\ 3\ 4)$ και $b = (1\ 2\ 3\ 4)(5\ 6)$ της S_6.

(124) Για το (α) δείξτε ότι $C_e = \{e\}$. Για το (β) δείξτε ότι η διμελής σχέση στο σύνολο G που ορίζεται θέτοντας $a \sim b \Leftrightarrow b \in C_a$ είναι σχέση ισοδυναμίας στο G και συμπεράνετε το ζητούμενο. Το (γ) αφήνεται στον αναγνώστη. Για το (δ), δείξτε ότι η διεδρική ομάδα των συμμετριών του ισοπλεύρου τριγώνου έχει μία κλάση συζυγίας με ένα στοιχείο (την ταυτοτική συμμετρία), μία κλάση

συζυγίας με δύο στοιχεία (τις στροφές κατά γωνίες $2\pi/3$ και $-2\pi/3$) και μία κλάση συζυγίας με τρία στοιχεία (τις ανακλάσεις στους τρεις άξονες συμμετρίας του τριγώνου). Για το (ε) επιλέξτε τυχαίο στοιχείο $b = gag^{-1} \in C_a$ και δείξτε ότι $f_a(x) = b \Leftrightarrow g^{-1}x \in H_a \Leftrightarrow x \in gH_a$, όπου $H_a = \{x \in G : ax = xa\}$ και $gH_a = \{gx : x \in H_a\}$. Συμπεράνετε ότι το πλήθος των στοιχείων της αντίστροφης εικόνας του $\{b\}$ ως προς την f_a είναι ίσο με το πλήθος των στοιχείων του H_a και συνεπώς ανεξάρτητο του $b \in C_a$. Για το (στ) συνάγετε από το (ε) ότι η τάξη της G είναι ίση με το γινόμενο των πληθαρίθμων των C_a και H_a. Για το (ζ) παρατηρήστε ότι αν n είναι η τάξη μιας ομάδας G όπως στην Άσκηση 118, τότε η G έχει ακριβώς δύο κλάσεις συζυγίας με πλήθος στοιχείων 1 και $n-1$, αντίστοιχα. Συμπεράνετε από το (στ) ότι το $n-1$ είναι διαιρέτης του n και επομένως ότι $n = 2$.

(125) Για το (α) δείξτε ότι η απεικόνιση σ είναι 1–1, ή ότι είναι επί, ή περιγράψτε ευθέως την αντίστροφη απεικόνιση. Παρατηρήστε έπειτα ότι η σ γράφεται

$$\sigma = (1\ 2\ 4\ 8\ 16\ 11)\,(3\ 6\ 12)\,(5\ 10\ 20\ 19\ 17\ 13)\,(7\ 14)\,(9\ 18\ 15)$$

ως γινόμενο ξένων κύκλων και συμπεράνετε ότι η τάξη της είναι ίση με 6. Για το (γ) παρατηρήστε ότι $\sigma^{1998} = \sigma^{2010} = e$, αφού $\sigma^6 = e$, και συμπεράνετε ότι

$$\sigma^{2000} = \sigma^2 = (1\ 4\ 16)\,(2\ 8\ 11)\,(3\ 12\ 6)\,(5\ 20\ 17)\,(10\ 19\ 13)\,(9\ 15\ 18)$$

και ότι

$$\sigma^{2013} = \sigma^3 = (1\ 8)\,(2\ 16)\,(4\ 11)\,(5\ 19)\,(10\ 17)\,(20\ 13)\,(7\ 14).$$

(126) Δείξτε ότι το δοσμένο γινόμενο είναι ίσο με $(1\ n)(2\ n-1)(3\ n-2)\cdots$ και συμπεράνετε ότι η τάξη του είναι ίση με 2.

(127) Δείξτε ότι δεν υπάρχει τέτοιος ακέραιος r για $n \le 6$ και ότι η συμμετρική ομάδα S_7 έχει το στοιχείο (1 2 3 4 5)(6 7) τάξης 10 αλλά δεν έχει στοιχείο τάξης 9. Συμπεράνετε ότι ο ζητούμενος ελάχιστος ακέραιος είναι ο $n = 7$.

(128) Για το (α) παρατηρήστε ότι $\sigma = (1\ 7\ 4)(2\ 6\ 3\ 8)$ και συμπεράνετε ότι η σ έχει τάξη 12. Για το (β) παρατηρήστε ότι

$$\sigma = (1\ 7)\,(7\ 4)\,(2\ 6)\,(6\ 3)\,(3\ 8) = (1\ 7)\,(4\ 7)\,(2\ 6)\,(3\ 8)\,(6\ 8)$$

και συμπεράνετε ότι $\sigma = xy$, όπου $x = (1\ 7)(2\ 6)(3\ 8)$ και $y = (4\ 7)(6\ 8)$ είναι στοιχεία της S_8 τάξης 2. Για το (γ) δείξτε ότι κάθε μετάθεση τάξης 3 είναι άρτια και συμπεράνετε ότι το ερώτημα έχει αρνητική απάντηση.

(129) Τα στοιχεία (1 2 3 4 5)(6 7 8) και (1 3 5 2 4)(6 7 8) τάξης 15 της S_8 δείχνουν ότι η πρόταση στο (α) είναι αληθής. Για το (β), παρατηρήστε ότι κάθε στοιχείο τάξης 30 της S_{10} είναι ίσο με το γινόμενο τριών ξένων κύκλων μήκους 2, 3 και 5, αντίστοιχα, και συνεπώς είναι περιττή μετάθεση. Συμπεράνετε ότι το γινόμενο δύο τέτοιων στοιχείων είναι άρτια μετάθεση και συνεπώς έχει τάξη διάφορη του 30.

(130) Για το (α), υποθέτοντας ότι η $w \in S_n$ έχει περιττή τάξη, έχουμε $w^k = e$ για κάποιο περιττό k. Εφαρμόζοντας τον ομομορφισμό του προσήμου $\varepsilon : S_n \to \{1, -1\}$, παίρνουμε $(\varepsilon(w))^k = 1$ και συμπεραίνουμε ότι $\varepsilon(w) = 1$, δηλαδή ότι η w είναι άρτια μετάθεση. Για το (β), γνωρίζουμε ότι κάθε άρτια μετάθεση $w \in S_n$ μπορεί να γραφεί ως γινόμενο άρτιου πλήθους ξένων ανά δύο αντιμεταθέσεων. Παρατηρώντας ότι $(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d)$ για διακεκριμένα $a, b, c, d \in \{1, 2, \ldots, n\}$, συμπεραίνουμε ότι η w μπορεί να γραφεί ως γινόμενο κύκλων μήκους 3, οι οποίοι είναι μεταθέσεις περιττής τάξης.

(131) Παρατηρήστε πρώτα ότι κάθε μετάθεση της μορφής $\sigma\tau\sigma^2\tau^2\sigma^3\tau^3$ είναι άρτια. Δείξτε έπειτα ότι κάθε άρτια μετάθεση της S_4 μπορεί να γραφεί σε αυτή τη μορφή ως εξής. Για το ταυτοτικό στοιχείο $e \in S_4$ αρκεί να θέσει κανείς $\sigma = \tau = e$. Για τα στοιχεία (1 2)(3 4), (1 3)(2 4) και (1 4)(2 3) να θέσετε $\sigma = e$

και να θεωρήσετε κατάλληλο κύκλο τ μήκους 4. Για τους κύκλους μήκους 3 να θεωρήσετε κατάλληλες αντιμεταθέσεις σ και τ.

(132) Για το (α) παρατηρήστε ότι αν, για παράδειγμα, $\tau = \sigma^k$ για κάποιο $k \in \mathbb{N}$, τότε $\sigma\tau = \tau\sigma = \sigma^{k+1}$. Το αντίστροφο δεν ισχύει, όπως δείχνει το παράδειγμα $\sigma = (1\ 2)$ και $\tau = (3\ 4)$ για $n = 4$. Για το (β) παρατηρήστε πρώτα ότι αφού η $\tau \in S_n$ είναι κύκλος μήκους n, κάθε $x \in \{1, 2, \ldots, n\}$ γράφεται στη μορφή $x = \tau^m(1)$ με $m \in \mathbb{N}$. Θεωρήστε $k \in \mathbb{N}$ τέτοιο ώστε $\sigma(1) = \tau^k(1)$ και δείξτε ότι $\sigma = \tau^k$ ως εξής. Θεωρήστε τυχαίο $x \in \{1, 2, \ldots, n\}$ και επιλέξτε $m \in \mathbb{N}$ τέτοιο ώστε $x = \tau^m(1)$. Παρατηρήστε έπειτα ότι αφού η σ μετατίθεται με την τ, θα μετατίθεται και με κάθε δύναμη αυτής και υπολογίστε ότι

$$\begin{aligned} \sigma(x) &= \sigma(\tau^m(1)) = (\sigma\tau^m)(1) = (\tau^m\sigma)(1) = \tau^m(\sigma(1)) = \tau^m(\tau^k(1)) \\ &= \tau^{m+k}(1) = \tau^k(\tau^m(1)) = \tau^k(x). \end{aligned}$$

Συμπεράνετε ότι $\sigma(x) = \tau^k(x)$ για κάθε $x \in \{1, 2, \ldots, n\}$ και συνεπώς ότι $\sigma = \tau^k$.

(133) Θέτουμε $\tau = (1\ 2)(3\ 4)\cdots(2n-1\ 2n) \in S_{2n}$ και θεωρούμε μετάθεση $\sigma \in S_{2n}$. Παρατηρούμε ότι ισχύει $\sigma\tau = \tau\sigma$ αν και μόνο αν $\tau = \sigma\tau\sigma^{-1}$ και ότι η $\sigma\tau\sigma^{-1}$ γράφεται

$$\sigma\tau\sigma^{-1} = (\sigma(1)\ \sigma(2))\ (\sigma(3)\ \sigma(4))\ \cdots\ (\sigma(2n-1)\ \sigma(2n))$$

ως γινόμενο ξένων κύκλων. Συμπεραίνουμε ότι η σ μετατίθεται με την τ αν και μόνο αν η διαμέριση του συνόλου $\{1, 2, \ldots, 2n\}$ με μέρη $\{\sigma(1), \sigma(2)\}$, $\{\sigma(3), \sigma(4)\}, \ldots, \{\sigma(2n-1), \sigma(2n)\}$ συμπίπτει με εκείνη με μέρη $\{1, 2\}, \{3, 4\}, \ldots, \{2n-1, 2n\}$. Έπεται (εξηγήστε πώς) ότι το πλήθος των στοιχείων της S_{2n} που μετατίθενται με την τ είναι ίσο με $2^n n!$.

(134) Για το (α) θέτουμε $\sigma = (a_1\ a_2\ \cdots\ a_n)$ και υπολογίζουμε ότι $\sigma^2 = (a_1\ a_3 \cdots a_n\ a_2\ a_4 \cdots a_{n-1})$, αν ο n είναι περιττός αριθμός, και ότι $\sigma^2 = (a_1\ a_3 \cdots a_{n-1})(a_2\ a_4 \cdots a_n)$, αν ο n είναι άρτιος. Εκφράζουμε τώρα τη σ ως γινόμενο ξένων κύκλων $\sigma = \sigma_1\sigma_2\cdots\sigma_n$ και παρατηρούμε ότι $\sigma^2 = \sigma_1^2\sigma_2^2\cdots\sigma_n^2$ (εξηγήστε γιατί). Εφαρμόζοντας το (α) στους κύκλους σ_i προκύπτει το (β). Προκύπτει επίσης ότι $c(\sigma^2) = c(\sigma)$ αν και μόνο αν κάθε κύκλος σ_i έχει περιττό μήκος και συνεπώς ότι ισχύει το (γ).

(135) Συμβολίζουμε με $c(\sigma)$ το πλήθος των κύκλων της $\sigma \in S_n$, όπως στην Άσκηση 134. Για το (α) παρατηρήστε ότι αν $\sigma^2 = \tau$, τότε $c(\sigma^2) = 1$ και εφαρμόστε την Άσκηση 134 (β). Για το (β) διακρίνετε περιπτώσεις για το αν ο n είναι άρτιος ή περιττός. Στην πρώτη περίπτωση χρησιμοποιήστε το αποτέλεσμα του (α) και την Άσκηση 134 (α) για να δείξτε ότι δεν υπάρχει μετάθεση $\sigma \in S_n$ με $\sigma^2 = \tau$. Στη δεύτερη περίπτωση δείξτε ότι η μοναδική μετάθεση $\sigma \in S_n$ με $\sigma^2 = \tau$ είναι η $\sigma = \tau^{(n+1)/2}$. Επαληθεύστε πρώτα ότι για τη μετάθεση αυτή ισχύει $\sigma^2 = \tau$. Υποθέστε έπειτα ότι $\sigma^2 = \tau$, συνάγετε από το (α) ότι $\sigma^n = e$ και συμπεράνετε ότι $\sigma = \tau^{(n+1)/2}$. Για το (γ) εργασθείτε με παρόμοιο τρόπο για να δείξτε ότι η εξίσωση $\sigma^m = \tau$ έχει λύση $\sigma \in S_n$ αν και μόνο αν $\mu\kappa\delta(m, n) = 1$ και ότι όταν υπάρχει, η λύση είναι μοναδική. Στην περίπτωση που $\mu\kappa\delta(m, n) = 1$, δείξτε ότι η εξίσωση $\sigma^m = \tau$ έχει μοναδική λύση τη $\sigma = \tau^k$, όπου $k \pmod n$ είναι η μοναδική λύση της ισοτιμίας $mx \equiv 1 \pmod n$.

(136) Παρατηρήστε ότι $\tau^{i-1}\sigma\tau^{n-i+1} = (i\ i+1)$ για κάθε $i \in \{1, 2, \ldots, n-1\}$ και θυμηθείτε ότι κάθε στοιχείο της S_n μπορεί να γραφεί ως γινόμενο αντιμεταθέσεων της μορφής $(i\ i+1)$ με $i \in \{1, 2, \ldots, n-1\}$.

(137) Αφού κάθε στοιχείο της S_n γράφεται ως γινόμενο ξένων ανά δύο κύκλων, αρκεί να δείξουμε ότι κάθε κυκλική μετάθεση $\sigma \in S(X)$ ενός πεπερασμένου συνόλου X με τουλάχιστον δύο στοιχεία μπορεί να γραφεί ως γινόμενο δύο στοιχείων τάξης 2 της $S(X)$. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $X = \{1, 2, \ldots, m\}$, οπότε η $\sigma \in S_m$ είναι κύκλος μήκους $m \geq 2$. Παρατηρούμε πρώτα ότι υπάρχουν στοιχεία τ_1, τ_2 τάξης δύο της S_m τέτοια

ώστε το γινόμενο $\tau = \tau_1\tau_2$ να είναι κύκλος μήκους m. Για παράδειγμα, μπορούμε να θέσουμε

$$\tau_1 = (1\ 2)(3\ 4)\cdots(m-1\ m), \quad \tau_2 = (2\ 3)(4\ 5)\cdots(m-2\ m-1),$$

αν ο m είναι άρτιος και

$$\tau_1 = (1\ 2)(3\ 4)\cdots(m-2\ m-1), \quad \tau_2 = (2\ 3)(4\ 5)\cdots(m-1\ m),$$

αν ο m είναι περιττός (εξηγήστε γιατί). Αφού οι σ, τ είναι κύλοι μήκους m, οι μεταθέσεις αυτές είναι συζυγή στοιχεία της S_m και συνεπώς υπάρχει μετάθεση $\rho \in S_m$ τέτοια ώστε $\sigma = \rho\tau\rho^{-1}$. Συμπεραίνουμε ότι $\sigma = \rho(\tau_1\tau_2)\rho^{-1} = (\rho\tau_1\rho^{-1})(\rho\tau_2\rho^{-1})$ και συνεπώς η σ είναι ίση με το γινόμενο δύο στοιχείων τάξης 2 της S_m.

(138) Για το (α) δείξτε ότι κάθε κύκλος μήκους r μπορεί να γραφεί ως γινόμενο $r-1$ αντιμεταθέσεων και εφαρμόστε την παρατήρηση αυτή σε καθένα από τους κύκλους της σ. Για το (β) γράψτε $t = (a\ b)$ και δείξτε ότι $c(\sigma t) = c(\sigma) - 1$, αν τα a και b είναι στοιχεία του ίδιου κύκλου της σ και ότι $c(\sigma t) = c(\sigma) + 1$, αν τα a και b είναι στοιχεία διαφορετικών κύκλων της σ. Για το (γ) θεωρήστε μια παραγοντοποίηση $\sigma = t_1 t_2 \cdots t_k$ της σ ως γινόμενο $k = f(\sigma)$ αντιμεταθέσεων. Χρησιμοποιώντας το (β), δείξτε ότι $c(t_1 t_2 \cdots t_i) \geq n - i$ για κάθε $i \in \{0, 1, \ldots, k\}$ με επαγωγή στο i και συμπεράνετε ότι $c(\sigma) \geq n - f(\sigma)$. Από την ανισότητα αυτή και το (α) προκύπτει ότι $f(\sigma) = n - c(\sigma)$ για κάθε $\sigma \in S_n$.

(139) Το (α) αφήνεται στον αναγνώστη. Για το (β) υποθέστε πρώτα ότι το HK είναι υποομάδα της G και δείξτε, με τη βοήθεια του (α), ότι $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$. Αντιστρόφως, υποθέστε ότι $HK = KH$, δείξτε ότι $(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$ και ότι $(HK)^{-1} = HK$ και συμπεράνετε ότι το HK είναι υποομάδα της G.

(140) Το (α) αφήνεται στον αναγνώστη. Για το (β) θεωρήστε τις κυκλικές ομάδες με δύο και τρία στοιχεία, αντίστοιχα. Για το (γ) δείξτε ότι τα σύνολα $G \times \{e\}$, $\{e\} \times G$ και $\{(x, x) : x \in G\}$ είναι τρεις διακεκριμένες υποομάδες της $G \times G$ διάφορες της τετριμμένης $\{(e, e)\}$ και της $G \times G$.

(141) Αληθής είναι μόνο η πρόταση στο (β). Για το (α) θεωρήστε δύο γνήσιες υποομάδες H, K μιας ομάδας G και δείξτε ότι η ένωσή τους είναι γνήσιο υποσύνολο της G ως εξής. Παρατηρήστε πρώτα ότι το ζητούμενο είναι φανερό αν μία από τις H, K περιέχεται στην άλλη. Διαφορετικά, επιλέξτε στοιχεία $x \in H \setminus K$ και $y \in K \setminus H$ και δείξτε ότι το γινόμενο xy δεν ανήκει στο $H \cup K$. Για το (β) θεωρήστε τη μη κυκλική ομάδα με 4 στοιχεία.

(142) Το (α) αφήνεται στον αναγνώστη. Για να δείξετε ότι η τάξη της E_n είναι ίση με n, χρησιμοποιήστε το πολυώνυμο $p(x) = x^n - 1 \in \mathbb{C}[x]$ και την Άσκηση 61 (α). Για το (β) θεωρήστε υποομάδα H της $\mathbb{C}^\times$ τάξης n. Θεωρώντας την τάξη των στοιχείων της H, δείξτε ότι $x^n = 1$ για κάθε $x \in H$. Συμπεράνετε ότι $H \subseteq E_n$ και συνεπώς ότι $H = E_n$.

(143) Το (α) αφήνεται στον αναγνώστη. Για το (β) θέτουμε $X = \{1, 2, \ldots, k\}$ και $Y = \{k+1, \ldots, n\}$. Παρατηρήστε ότι οι περιορισμοί σ_X και σ_Y μιας μετάθεσης $\sigma \in H$ στα σύνολα X και Y είναι μεταθέσεις των συνόλων αυτών και δείξτε ότι η απεικόνιση $\varphi : H \to S(X) \times S(Y)$ που ορίζεται θέτοντας $\varphi(\sigma) = (\sigma_X, \sigma_Y)$ για $\sigma \in H$ είναι 1–1 και επί. Συμπεράνετε ότι η τάξη της H είναι ίση με $k!\,(n-k)!$ και ότι

$$[S_n : H] = \frac{n!}{k!\,(n-k)!} = \binom{n}{k}.$$

Για το (γ) παρατηρήστε ότι αν $\sigma, \tau \in S_n$ είναι μεταθέσεις που ανήκουν στην ίδια αριστερή κλάση της H στην S_n, τότε $\sigma(X) = \tau(X)$ και δείξτε ότι οι κλάσεις αυτές είναι ακριβώς τα σύνολα $\{\sigma \in S_n : \sigma(X) = S\}$, όπου το S διατρέχει τα υποσύνολα του $\{1, 2, \ldots, n\}$ με k στοιχεία. Ομοίως, δείξτε ότι οι δεξιές κλάσεις

της H στην S_n είναι τα σύνολα $\{\sigma \in S_n : \sigma(S) = X\}$, όπου το S διατρέχει τα υποσύνολα του $\{1, 2, \ldots, n\}$ με k στοιχεία.

(144) Το (α) αφήνεται στον αναγνώστη. Για το (β) παρατηρούμε ότι για κάθε $\sigma \in K$ η απεικόνιση $\tau : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ που ορίζεται θέτοντας $\tau(x) = |\sigma(x)|$ για $x \in \{1, 2, \ldots, n\}$ είναι μετάθεση $\{1, 2, \ldots, n\}$. Επιπλέον, κάθε μετάθεση $\tau \in S_n$ προκύπτει ακριβώς 2^n φορές με αυτόν τον τρόπο από στοιχεία της K. Συμπεραίνουμε ότι $|K| = 2^n n!$ και $[S_{2n} : K] = (2n)!/2^n n! = 1 \cdot 3 \cdots (2n-1)$ για κάθε θετικό ακέραιο n.

(145) Σύμφωνα με το Θεώρημα του Lagrange, τέτοιοι ακέραιοι πρέπει να διαιρούν το 24. Δείξτε ότι για κάθε θετικό διαιρέτη d του 24, υπάρχει υποομάδα της S_4 τάξης d. Για $d = 12$, η μόνη τέτοια είναι η εναλλάσσουσα ομάδα A_4. Για $d = 8$, δείξτε ότι το

$$H = \{e, (1\ 3), (2\ 4), (1\ 3)(2\ 4), (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 2\ 3\ 4), (1\ 4\ 3\ 2)\}$$

είναι υποομάδα της S_4 ως εξής. Θεωρήστε τη διεδρική ομάδα G των συμμετριών του τετραγώνου με κορυφές 1, 2, 3, 4, αριθμημένες κυκλικά. Κάθε στοιχείο $x \in G$ περιορίζεται σε μια μετάθεση $\varphi(x) \in S_4$ στο σύνολο των κορυφών του τετραγώνου. Παρατηρήστε ότι $\varphi(xy) = \varphi(x)\varphi(y)$ για $x, y \in G$ (δηλαδή, ότι η φ είναι ομομορφισμός ομάδων) και συμπεράνετε από αυτό ότι η εικόνα $\varphi(G) = H$ είναι υποομάδα της S_4.

(146) Δείξτε ότι η εναλλάσσουσα ομάδα A_4 έχει την επιθυμητή ιδιότητα.

(147) Για το (α) διακρίνετε τις περιπτώσεις για τις οποίες η G έχει ή δεν έχει στοιχείο τάξης 4. Παρατηρήστε ότι στη δεύτερη περίπτωση έχουμε $G = \{e, a, b, c\}$ για κάποια στοιχεία $a, b, c \in G$ με $a^2 = b^2 = c^2 = e$. Δείξτε ότι $ab = ba = c$, αποκλείοντας τις περιπτώσεις $ab \in \{e, a, b\}$ και $ba \in \{e, a, b\}$, και συνάγετε ότι η G είναι αβελιανή. Για το δεύτερο ερώτημα του (β) παρατηρήστε ότι η ομάδα, έστω K, των συμμετριών του τετραγώνου είναι μη αβελιανή ομάδα τάξης 8. Για το (γ) παρατηρήστε ότι οι μη τετριμμένες υποομάδες της K έχουν τάξη 2 ή 4. Συγκεκριμένα, υπάρχουν πέντε υποομάδες της K τάξης 2, όσες και τα στοιχεία τάξης 2, μία κυκλική υποομάδα τάξης 4 και δύο μη κυκλικές της ίδιας τάξης (καθεμιά από τις δύο τελευταίες περιέχει το ταυτοτικό στοιχείο, δύο ανακλάσεις a, b σε άξονες συμμετρίας του τετραγώνου που είναι κάθετοι μεταξύ τους και το γινόμενο $ab = ba$).

(148) Το (α) αφήνεται στον αναγνώστη. Για το (β) δείτε τη λύση της Άσκησης 124 (ε). Απάντηση για το (γ): είναι η ομάδα των συμμετριών του τετραγώνου και οι υποομάδες τάξης 4 αυτής. Για το (δ) παρατηρούμε ότι το ζητούμε πλήθος είναι ίσο με το άθροισμα $\sum_{a \in G} |C_G(a)|$. Από το αποτέλεσμα του (β) έχουμε $\sum_{a \in C} |C_G(a)| = |G|$ για κάθε κλάση συζυγίας C της G. Αθροίζοντας πάνω σε όλες τις κλάσεις συζυγίας της G παίρνουμε το ζητούμενο.

(149) Από τον ορισμό του κέντρου έχουμε $Z(G) = \bigcap_{a \in G} C_G(a)$. Το (α) προκύπτει από την ισότητα αυτή και την Άσκηση 148 (α). Από την ίδια ισότητα προκύπτει και το (β) αφού το $C_G(a)$ είναι υποομάδα της G διάφορη της τετριμμένης $\{e\}$ (εξηγήστε γιατί) για κάθε ομάδα G με τουλάχιστον δύο στοιχεία και κάθε $a \in G$. Για το (γ) έστω K η ομάδα των συμμετριών του κανονικού n-γώνου. Δείξτε ότι μία ανάκλαση της K μετατίθεται με μία στροφή αν και μόνο αν η τελευταία είναι στροφή κατά γωνία π. Συμπεράνετε ότι το κέντρο της K είναι τετριμμένο, αν ο είναι περιττός αριθμός και ότι αποτελείται από το ταυτοτικό στοιχείο και τη στροφή κατά γωνία π, αν ο n είναι άρτιος.

(150) Το (α) αφήνεται στον αναγνώστη. Για το (β) παρατηρήστε ότι αν $K = xHx^{-1}$, τότε η απεικόνιση $f : H \to K$ που ορίζεται θέτοντας $f(y) = xyx^{-1}$ για $y \in H$ είναι καλά ορισμένη, 1–1 και επί. Για να δείξετε ότι το αντίστροφο δεν ισχύει θεωρήστε, για παράδειγμα, τη μη κυκλική ομάδα τάξης 4 και τις υποομάδες τάξης 2 αυτής. Για το (γ) δείξτε ότι αν $b = xax^{-1}$ για κάποιο $x \in G$, τότε

$C_G(b) = xC_G(a)x^{-1}$. Για να δείξετε ότι το αντίστροφο δεν ισχύει θεωρήστε, για παράδειγμα, δύο τυχαία διακεκριμένα στοιχεία a και b μιας αβελιανής ομάδας G.

(151) Για το (α) παρατηρήστε ότι $(xh)H(xh)^{-1} = x(hHh^{-1})x^{-1} = xHx^{-1}$ για όλα τα $x \in G$ και $h \in H$ και συνάγετε το ζητούμενο. Για το (β) παρατηρήστε ότι η τάξη της υποομάδας xHx^{-1} είναι ίση με εκείνη της H για κάθε $x \in H$ και ότι κάθε υποομάδα xHx^{-1} περιέχει το ταυτοτικό στοιχείο της G. Συμπεράνετε από το (α) ότι η ένωση των συνόλων xHx^{-1} για $x \in G$ περιέχει λιγότερα από $|H| \cdot [G : H] = |G|$ στοιχεία, που σημαίνει ότι ισχύει το ζητούμενο.

(152) Παρατηρήστε ότι κάθε στοιχείο της G ανήκει σε υποομάδα τάξης p της G και δείξτε ότι για οποιεσδήποτε δύο τέτοιες διαφορετικές υποομάδες H και K ισχύει $H \cap K = \{e\}$. Συνάγετε ότι υπάρχουν ακριβώς $(n-1)/(p-1)$ υποομάδες τάξης p της G.

(153) Ορίζουμε την απεικόνιση $f : G \to G$ θέτοντας $f(x) = x^2$ για $x \in G$. Αφού το σύνολο G είναι πεπερασμένο, η απεικόνιση f είναι επί αν και μόνο αν η f είναι 1–1. Ως συνέπεια παίρνουμε την ισοδυναμία (i) $\Leftrightarrow$ (ii). Για τη συνεπαγωγή (iii) $\Rightarrow$ (i) υποθέτουμε ότι η τάξη της G είναι ίση με τον περιττό αριθμό $2n-1$. Παρατηρούμε τότε ότι για κάθε $a \in G$ ισχύει $a^{2n-1} = e$ (εξηγήστε γιατί) και συνεπώς ότι το στοιχείο $x = a^n$ της G είναι λύση της εξίσωσης $x^2 = a$. Η συνεπαγωγή (ii) $\Rightarrow$ (iii) προκύπτει από την Άσκηση 120 (α).

(154) Για το (α), ισχυριζόμαστε ότι $ab \neq ba$. Πράγματι, αν $ab = ba$, τότε από τις ισότητες $a^3 = b^3 = (ab)^2 = e$ προκύπτει ότι $ab = e$, σε αντίθεση με την υπόθεση ότι το ab έχει τάξη 2. Για το (β), ισχυριζόμαστε ότι η μικρότερη δυνατή τάξη της G είναι ίση με 12. Παρατηρούμε πρώτα ότι αφού η G περιέχει στοιχεία τάξης 2 και 3, η τάξη της είναι ακέραιο πολλαπλάσιο του 6. Δείχνουμε έπειτα ότι $\langle a\rangle \cap \langle b\rangle = \{e\}$ και ότι τα ab και ba, ως στοιχεία τάξης 2, δεν ανήκουν στην ένωση $\langle a\rangle \cup \langle b\rangle$ και συμπεραίνουμε ότι $|G| \geq 12$. Παράδειγμα ομάδας τάξης 12 με τις δοσμένες ιδιότητες είναι η A_4, με στοιχεία $a = (1\ 2\ 3)$, $b = (2\ 3\ 4)$ και $ab = (1\ 2)(3\ 4)$.

(155) Για το (α) υποθέστε ότι ο αριθμός p δεν είναι πρώτος και βρείτε στοιχείο της G τάξης μικρότερης του p. Για το (β), ας υποθέσουμε ότι υπάρχουν $a, b \in G$ με $ab \neq ba$. Αφού οι υποομάδες $\langle a\rangle$ και $\langle b\rangle$ είναι διακεκριμένες και έχουν τάξη p, θα πρέπει $\langle a\rangle \cap \langle b\rangle = \{e\}$. Έστω $T = \{a^i b^j : 0 \leq i, j \leq p-1\} \setminus \{e\}$. Λόγω της παρατήρησης, το T έχει ακριβώς $p^2 - 1$ σε πλήθος στοιχεία. Σύμφωνα με την υπόθεση, το T περιέχει υποσύνολο S με p στοιχεία τα οποία ανά δύο μετατίθενται. Διακρίνουμε τις εξής περιπτώσεις. Έστω ότι $a^k \in S$ για κάποιο $1 \leq k \leq p-1$. Αφού $|S| = p$, έχουμε $a^i b^j \in S$ για κάποια $0 \leq i \leq p-1$ και $1 \leq j \leq p-1$, οπότε $a^k(a^i b^j) = (a^i b^j)a^k$. Από την ισότητα αυτή έπεται ότι $a^k b^j = b^j a^k$ και από την Άσκηση 116 ότι $ab = ba$, σε αντίθεση με την υπόθεσή μας. Ομοίως καταλήγουμε σε άτοπο αν $b^k \in S$ για κάποιο $1 \leq k \leq p-1$. Διαφορετικά, το S περιέχει μόνο στοιχεία της μορφής $a^i b^j$ με $1 \leq i, j \leq p-1$. Τότε, υπάρχουν $1 \leq i, j, k \leq p-1$ με $j \neq k$ τέτοια ώστε $a^i b^j, a^i b^k \in S$ (εξηγήστε γιατί), οπότε $(a^i b^j)(a^i b^k) = (a^i b^k)(a^i b^j)$. Από την ισότητα αυτή έπεται ότι $a^i b^{j-k} = b^{j-k} a^i$ και από την Άσκηση 116, όπως προηγουμένως, ότι $ab = ba$.

(156) Για το (α) θεωρήστε χωρίς βλάβη της γενικότητας ότι τα $\sigma = (1\ 2\ \cdots\ n)$ και $\tau = (a\ b)$ είναι στοιχεία της H. Παρατηρήστε ότι οι αντιμεταθέσεις $\sigma^i \tau \sigma^{-i} = (a+i\ \ b+i)$, όπου η πρόσθεση των στοιχείων του $\{1, 2, \ldots, n\}$ γίνεται (mod n), ανήκουν επίσης στην H. Χρησιμοποιώντας την υπόθεση ότι ο n είναι πρώτος, δείξτε ότι κάθε αντιμετάθεση της S_n γράφεται ως γινόμενο των αντιμεταθέσεων $(a+i\ \ b+i)$ για $i \in \{0, 1, \ldots, n-1\}$. Συμπεράνετε ότι η H περιέχει όλες τις αντιμεταθέσεις της S_n και συνεπώς ότι $H = S_n$. Για το (β),

θεωρήστε τη διεδρική υποομάδα τάξης 8 της S_4 που βρέθηκε στη λύση της Άσκησης 145 και συμπεράνετε ότι το ερώτημα έχει αρνητική απάντηση.

(157) Το (α) θα πρέπει να σας είναι γνωστό. Για το (β) ας συμβολίσουμε με $L(G,H)$ και $R(G,H)$ τα σύνολα των αριστερών και δεξιών, αντίστοιχα, κλάσεων της H στη G. Δείξτε ότι η απεικόνιση $\varphi : L(G,H) \to R(G,H)$ που ορίζεται θέτοντας $\varphi(aH) = Ha^{-1}$ για $a \in G$ είναι καλά ορισμένη, 1–1 και επί και συμπεράνετε το ζητούμενο.

(158) Για το (α) παρατηρήστε ότι κάθε αριστερή κλάση H στην K είναι και αριστερή κλάση της H στη G και συμπεράνετε ότι η K γράφεται ως ξένη ένωση $[K : H]$ το πλήθος αριστερών κλάσεων της H στη G. Δείξτε ότι το ίδιο ισχύει για κάθε αριστερή κλάση της K στη G και συνάγετε το ζητούμενο. Για το (β) υποθέστε ότι το σύνολο $(aH) \cap K$ είναι με κενό, παρατηρήστε ότι $(aH) \cap K = (bH) \cap K$ για κάποιο $b \in K$ και δείξτε ότι το $(bH) \cap K$ είναι ίσο με την αριστερή κλάση $b(H \cap K)$ της $K \cap H$ στην K. Για το (γ) γράψτε τη $G = \bigcup_{i\in I} a_i H$ ως ξένη ένωση αριστερών κλάσεων της H, συμπεράνετε ότι $K = \bigcup_{i\in I}(a_i H) \cap K$ και εφαρμόστε το (β).

(159) Για το (α) εφαρμόστε την Άσκηση 158 (α) για να δείξετε πρώτα ότι ο δείκτης $[G : K \cap H]$ είναι ακέραιο πολλαπλάσιο του 6. Εφαρμόζοντας τα (α) και (β) της ίδιας άσκησης, δείξτε έπειτα ότι $[G : K \cap H] = [G : K][K : K \cap H] \leq [G : K][G : H] = 6$ και συνάγετε ότι $[G : K \cap H] = 6$ είναι η μόνη δυνατή τιμή για το $[G : K \cap H]$. Εργασθείτε ομοίως στο (β) για να δείξετε ότι $[G : K \cap H] \in \{3, 6, 9\}$ και επαληθεύστε ότι και οι τρεις αυτές τιμές είναι εφικτές.

(160) Για το (α) παρατηρήστε ότι υπάρχουν δύο στοιχεία μεταξύ των $e, a, a^2, \ldots, a^n$ που ανήκουν στην ίδια αριστερή κλάση της H στη G. Αν a^p και a^q είναι δύο τέτοια στοιχεία, δείξτε ότι $a^{q-p} \in H$ και συμπεράνετε το ζητούμενο. Για το (β) ας υποθέσουμε ότι $a_1H, a_2H, \ldots, a_nH$ είναι οι n αριστερές κλάσεις της H στη G. Δείξτε ότι τα στοιχεία $a_1x, a_2x, \ldots, a_nx$ ανήκουν σε διαφορετικές ανά δύο αριστερές κλάσεις της H στη G. Συμπεράνετε ότι το γινόμενό τους $(a_1x)(a_2x)\cdots(a_nx) = (a_1a_2\cdots a_n)\cdot x^n$ ανήκει στην αριστερή κλάση $(a_1a_2\cdots a_n)\,H$ και τελικά ότι $x^n \in H$. Για το (γ) θεωρήστε τη συμμετρική ομάδα S_3 και υποομάδα αυτής τάξης 2.

(161) Για το (α) παρατηρήστε ότι το μηδέν είναι το μόνο στοιχείο πεπερασμένης τάξης της προσθετικής ομάδας $\mathbb{Q}$ και θυμηθείτε ότι κάθε στοιχείο μιας πεπερασμένης ομάδας έχει πεπερασμένη τάξη. Για το (β) ας υποθέσουμε ότι υπάρχει γνήσια υποομάδα H πεπερασμένου δείκτη n της $\mathbb{Q}$. Από την Άσκηση 160 (β) προκύπτει ότι $nx \in H$ για κάθε $x \in \mathbb{Q}$. Αυτό μας οδηγεί στην αντίφαση $\mathbb{Q} = n \cdot \mathbb{Q} \subseteq H$ και αποδεικνύει το ζητούμενο. Το ίδιο σκεπτικό εφαρμόζεται και στο (γ).

(162) Για το (α) υποθέστε ότι οι διπλές κλάσεις HxK και HyK έχουν κοινό στοιχείο. Δείξτε ότι $x \in HyK$ και $y \in HxK$ και συμπεράνετε ότι $HxK \subseteq (HH)y(KK) = HyK$ και ότι $HyK \subseteq (HH)x(KK) = HxK$. Παρατηρήστε επίσης ότι $x \in HxK$ για κάθε $x \in G$ και συμπεράνετε το ζητούμενο. Για το (β) δείξτε ότι υπάρχουν ακριβώς δύο διπλές κλάσεις, συγκεκριμένα τα σύνολα H και $G \setminus H$.

(163) Για το (α) βρείτε στοιχείο που παράγει την ομάδα $U(\mathbb{Z}_{50})$. Για το (β) δείξτε ότι η $U(\mathbb{Z}_{65})$ έχει περισσότερα του ενός στοιχεία τάξης 2 (άρα περισσότερες από μία υποομάδες τάξης 2) και συμπεράνετε ότι η ομάδα αυτή δεν είναι κυκλική. Για τα (γ) και (δ) δείξτε ότι οι δοσμένες ομάδες είναι κυκλικές αν και μόνο αν $n = 1$ ως εξής. Δείξτε πρώτα ότι για $n \geq 2$ η ομάδα $\mathrm{SL}_n(\mathbb{F})$ δεν είναι αβελιανή, άρα ούτε κυκλική, και συμπεράνετε ότι το ίδιο ισχύει για τη $\mathrm{GL}_n(\mathbb{F})$. Παρατηρήστε έπειτα ότι για $n = 1$ η $\mathrm{SL}_n(\mathbb{F})$ είναι τετριμμένη, άρα κυκλική, και ότι η $\mathrm{GL}_n(\mathbb{F})$ ταυτίζεται με την πολλαπλασιαστική ομάδα $\mathbb{F}^\times$ του

πεπερασμένου σώματος $\mathbb{F}$, η οποία είναι κυκλική (δείτε, για παράδειγμα, την Άσκηση 170).

(164) Τα στοιχεία τάξης 2 είναι η κλάση του -1, αν $n \in \{1, 2\}$, και οι κλάσεις των $-1, 2^{n-1} \pm 1$, αν $n \geq 3$. Πράγματι, έστω στοιχείο $x = \bar{a} \in \mathbb{Z}_{2^n}$ με $x^2 = 1$, όπου $a \in \mathbb{Z}$ και $n \geq 2$. Τότε, το $a^2 - 1 = (a-1)(a+1)$ διαιρείται με το 2^n. Αφού τα $a-1$ και $a+1$ δε διαιρούνται ταυτόχρονα με το 4, θα πρέπει ένα από τα δύο να διαιρείται με το 2^{n-1}. Κατά συνέπεια, ένα από τα $x-1$ και $x+1$ ισούται με μία από τις κλάσεις των $0, 2^{n-1} \in \mathbb{Z}_{2^n}$, δηλαδή το x είναι μία από τις κλάσεις των $\pm 1, 2^{n-1} \pm 1 \in \mathbb{Z}_{2^n}$. Αντιστρόφως, έχουμε $x^2 = 1$ για καθεμιά από αυτές τις τιμές του $x \in \mathbb{Z}_{2^n}$. Το (β) είναι άμεση συνέπεια του αποτελέσματος του (α). Για το (γ), παρατηρήστε ότι αφού η G έχει τάξη $\varphi(2^n) = 2^{n-1}$ και δεν είναι κυκλική, η τάξη οποιουδήποτε στοιχείου της θα πρέπει να διαιρεί το 2^{n-2}. Εναλλακτικά, αποδείξτε τη ζητούμενη ισοτιμία με επαγωγή στο n.

(165) Γνωρίζουμε ότι κάθε στοιχείο του $R = \mathbb{F}_q[x] \,/\, \langle x^2 \rangle$ γράφεται με μοναδικό τρόπο στη μορφή $\alpha = a + bx + \langle x^2 \rangle$ με $a, b \in \mathbb{F}_q$. Από την Άσκηση 101 (α) προκύπτει ότι το α είναι αντιστρέψιμο στοιχείο του R αν και μόνο αν $a \neq 0$ και συνεπώς η τάξη της G είναι ίση με $q(q-1)$. Για το (β) γράφουμε $q = p^r$, όπου p είναι πρώτος αριθμός. Θα δείξουμε ότι η G είναι κυκλική αν και μόνο αν $q = p$. Παρατηρούμε ότι για τυχαίο θετικό ακέραιο n έχουμε $\alpha^n = a^n + na^{n-1}bx + \langle x^2 \rangle$. Συνεπώς έχουμε $\alpha^n = 1$ αν και μόνο αν ισχύει $a^n = 1$ στην ομάδα $\mathbb{F}_q^\times$ και είτε η χαρακτηριστική p του $\mathbb{F}_q$ διαιρεί το n, είτε $b = 0$. Αφού η ομάδα $\mathbb{F}_q^\times$ είναι κυκλική τάξης $q-1$, από τα προηγούμενα προκύπτει ότι ισχύει $\alpha^{p(q-1)} = 1$ για κάθε $\alpha \in G$ και ότι η G έχει στοιχείο τάξης $q(q-1)$ αν και μόνο αν $q = p$.

(166) Εργασθείτε όπως στη λύση της Άσκησης 165 και δείξτε πρώτα ότι κάθε στοιχείο της G γράφεται με μοναδικό τρόπο στη μορφή $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + \langle x^n \rangle$ με $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}_2$ και $a_0 = 1$. Για το (α) συμπεράνετε ότι η G έχει τάξη 2^{n-1} (οπότε είναι κυκλική για $n \leq 2$). Για το (β) δείξτε ότι η G έχει γεννήτορα το $1 + x + \langle x^3 \rangle$ για $n = 3$ και ότι έχει τουλάχιστον δύο στοιχεία τάξης 2, για παράδειγμα τα $1 + x^{n-2} + \langle x^n \rangle$ και $1 + x^{n-1} + \langle x^n \rangle$, για $n \geq 4$ και συνάγετε ότι η G δεν είναι κυκλική για αυτές τις τιμές του n.

(167) Κάθε ιδεώδες του δακτυλίου $\mathbb{Z}_n$ είναι και υποομάδα της προσθετικής του ομάδας. Αντιστρόφως, κάθε υποομάδα H της προσθετικής ομάδας του $\mathbb{Z}_n$ είναι και ιδεώδες, αφού $nx \in H$ για όλα τα $n \in \mathbb{Z}$ και $x \in H$. Κατά συνέπεια, το πλήθος των ιδεωδών του $\mathbb{Z}_n$ είναι ίσο με εκείνο των υποομάδων της προσθετικής ομάδας του $\mathbb{Z}_n$, δηλαδή ίσο με το πλήθος των θετικών διαιρετών του n.

(168) Για το (α) παρατηρήστε ότι τα στοιχεία τάξης d της G είναι ακριβώς οι γεννήτορες της μοναδικής κυκλικής υποομάδας τάξης d της G και συμπεράνετε ότι το πλήθος των στοιχείων αυτών είναι ίσο με $\varphi(d)$. Συνάγετε ότι το άθροισμα που δίνεται στο (β) είναι ίσο με την τάξη της G.

(169) Για το (α) υποθέτουμε ότι η τάξη, έστω k, του x διαιρεί το d. Αφού η H είναι κυκλική ομάδα τάξης d, υπάρχει μοναδική υποομάδα K της H τάξης k. Προφανώς η K συμπίπτει με τη μοναδική υποομάδα τάξης k της G. Αφού μια τέτοια είναι η υποομάδα $\langle x \rangle$ της G που παράγεται από το x, θα πρέπει να έχουμε $\langle x \rangle = K$. Άρα $x \in K \subseteq H$ και συνεπώς $x \in H$. Το αντίστροφο είναι φανερό αφού η τάξη οποιουδήποτε στοιχείου της H διαιρεί την τάξη d της H. Το (β) είναι άμεση συνέπεια του (α). Για το (γ), ας γράψουμε $n = 2^k \cdot q$ για κάποιο $k \in \mathbb{N}$ και κάποιο περιττό θετικό ακέραιο q. Τα στοιχεία περιττής τάξης της G είναι εκείνα η τάξη των οποίων διαιρεί το q και επομένως, σύμφωνα με το (β), ακριβώς $q = n/2^k$ σε πλήθος. Άρα, υπάρχουν ακριβώς $n - n/2^k$ στοιχεία άρτιας τάξης της G.

(170) Για το (α) συμβολίζουμε με n την τάξη και με r_d το πλήθος των στοιχείων τάξης d της G. Έστω ότι $x \in G$ είναι στοιχείο τάξης d της G. Από την υπόθεση γνωρίζουμε ότι υπάρχουν το πολύ d στοιχεία $y \in G$ με $y^d = e$. Κατά συνέπεια, τα στοιχεία αυτά είναι ακριβώς οι δυνάμεις του x και τα στοιχεία τάξης d της G είναι ακριβώς οι γεννήτορες της κυκλικής υποομάδας της G που παράγεται από το x. Από τα παραπάνω και την Άσκηση 168 (α) έπεται ότι $r_d \in \{0, \varphi(d)\}$ για κάθε θετικό διαιρέτη d του n. Επιπλέον, από το μέρος (β) της ίδιας άσκησης προκύπτει ότι το άθροισμα των αριθμών $\varphi(d)$ είναι ίσο με εκείνο των r_d (το οποίο είναι ίσο με n), όπου το d διατρέχει τους θετικούς διαιρέτες του n. Συμπεραίνουμε ότι $r_d = \varphi(d)$ για κάθε θετικό διαιρέτη d του n. Ειδικότερα, έχουμε $r_n = \varphi(n) \geq 1$ και συνεπώς η ομάδα G είναι κυκλική. Τα (β) και (γ) είναι άμεσες συνέπειες του (α).

(171) Είναι γνωστό (για παράδειγμα, από την Άσκηση 170) ότι αν το $\mathbb{F}$ είναι πεπερασμένο σώμα, τότε η ομάδα $\mathbb{F}^\times$ είναι κυκλική. Για το αντίστροφο υποθέστε ότι το $\mathbb{F}$ είναι άπειρο σώμα και ότι η ομάδα $\mathbb{F}^\times$ παράγεται από το στοιχείο a. Παρατηρήστε πρώτα ότι αφού $(-1)^2 = 1$, το -1 έχει πεπερασμένη τάξη στην $\mathbb{F}^\times$ και συνεπώς ισχύει $-1 = 1$ στο $\mathbb{F}$. Παρατηρήστε έπειτα ότι $1 + a = a^m$ για κάποιο $m \in \mathbb{Z}$ και συμπεράνετε ότι το σώμα $\mathbb{F}$ είναι πεπερασμένο, σε αντίθεση με την υπόθεση.

(172) Για το (α) παρατηρήστε ότι $a = c^m$ και $b = c^n$ για κάποιους περιττούς ακεραίους m και n, όπου c είναι γεννήτορας της G, και συμπεράνετε ότι το $ab = c^{m+n}$ είναι τέλειο τετράγωνο. Για το (β) θεωρήστε τη μη κυκλική ομάδα με τέσσερα στοιχεία για να δείξετε ότι η απάντηση στο ερώτημα είναι αρνητική.

(173) Ζητάμε να βρούμε όλες τις απεικονίσεις $\varphi : \mathbb{Q} \to \mathbb{Q}$ με την ιδιότητα $\varphi(x + y) = \varphi(x) + \varphi(y)$ για όλα τα $x, y \in \mathbb{Q}$. Δείξτε πρώτα ότι $\varphi(nx) = n\varphi(x)$ και $\varphi(x/m) = \varphi(x)/m$ για κάθε ακέραιο n, κάθε θετικό ακέραιο m και κάθε $x \in \mathbb{Q}$ και συμπεράνετε ότι $\varphi(x) = \alpha x$ για κάθε $x \in \mathbb{Q}$, όπου $\alpha = \varphi(1) \in \mathbb{Q}$. Αντιστρόφως, η απεικόνιση $\varphi_\alpha : \mathbb{Q} \to \mathbb{Q}$ με $\varphi_\alpha(x) = \alpha x$ έχει τη ζητούμενη ιδιότητα για κάθε $\alpha \in \mathbb{Q}$. Παρατηρήστε τέλος ότι η φ_α είναι αντιστρέψιμη, δηλαδή αυτομορφισμός, αν και μόνο αν $\alpha \neq 0$.

(174) Το (α) αφήνεται στον αναγνώστη. Για το (β) χρησιμοποιήστε την Άσκηση 153 για να δείξετε ότι οι πεπερασμένες ομάδες με τη ζητούμενη ιδιότητα είναι ακριβώς αυτές που έχουν περιττή τάξη.

(175) Για το (α) παρατηρήστε ότι αν $y = gxg^{-1}$ για κάποιο $g \in G$, τότε $\varphi(y) = \varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1}$ και συμπεράνετε ότι τα $\varphi(x)$ και $\varphi(y)$ είναι συζυγή στοιχεία της K. Εφαρμόστε έπειτα το (α) για να δείξετε ότι η απάντηση στο ερώτημα (β) είναι αρνητική.

(176) Για το (α) παρατηρήστε ότι $ab = \varphi(\bar{1}, \bar{0}) \cdot \varphi(\bar{0}, \bar{1}) = \varphi((\bar{1}, \bar{0}) + (\bar{0}, \bar{1})) = \varphi((\bar{0}, \bar{1}) + (\bar{1}, \bar{0})) = \varphi(\bar{0}, \bar{1}) \cdot \varphi(\bar{1}, \bar{0}) = ba$ και δείξτε ομοίως ότι $a^2 = e$ και $b^2 = e$. Για το (β) δείξτε ευθέως ότι η απεικόνιση $\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to G$ που ορίζεται θέτοντας $\varphi(\bar{0}, \bar{0}) = e$, $\varphi(\bar{1}, \bar{0}) = a$, $\varphi(\bar{0}, \bar{1}) = b$ και $\varphi(\bar{1}, \bar{1}) = ab$ είναι ομομορφισμός ομάδων. Εφαρμόζοντας τα (α) και (β) για $G = S_3$ προκύπτει ότι στο (γ) υπάρχουν ακριβώς δέκα ομομορφισμοί.

(177) Για το (α) παρατηρούμε ότι αν $\varphi : G \to K$ είναι ομομορφισμός ομάδων με $\varphi(a) = b$, τότε $b^n = \varphi(a)^n = \varphi(a^n) = e$ και συνεπώς η τάξη του b διαιρεί το n. Αντιστρόφως, αν η τάξη του $b \in K$ διαιρεί το n, δείνουμε ότι η απεικόνιση $\varphi : G \to K$ με $\varphi(a^p) = b^p$ για $p \in \mathbb{Z}$ είναι καλά ορισμένος ομομορφισμός ομάδων με $\varphi(a) = b$. Το (β) προκύπτει από το (α) και την Άσκηση 169 (β).

(178) Για το (α) επαληθεύστε ότι $\varphi(\sigma_1\sigma_2) = \varphi(\sigma_1)\varphi(\sigma_2)$ για $\sigma_1, \sigma_2 \in S_n$, διακρίνοντας περιπτώσεις για το αν οι σ_1, σ_2 είναι άρτιες ή περιττές μεταθέσεις. Το (β) είναι άμεση συνέπεια του (α).

(179) Για το (α) παρατηρούμε ότι $\psi_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \psi_g(x)\psi_g(y)$ και ότι $\psi_g(x) = y \Leftrightarrow gxg^{-1} = y \Leftrightarrow x = g^{-1}yg$ για $g, x, y \in G$. Για το (β) παρατηρούμε επίσης ότι $(\psi_g \circ \psi_h)(x) = \psi_g(\psi_h(x)) = \psi_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = \psi_{gh}(x)$ για $g, h, x \in G$ κ.ο.κ. Το (γ) είναι άμεση συνέπεια του (β).

(180) Για το (α) υποθέτουμε πρώτα ότι $xH = yH$ για κάποια $x, y \in G$. Παρατηρούμε ότι $y = xh$ για κάποιο $h \in H$ και συμπεραίνουμε ότι $(gy)H = g(xh)H = (gx)(hH) = (gx)H$ για $g \in G$. Αυτό δείχνει ότι η $\varphi_g : X \to X$ είναι καλά ορισμένη απεικόνιση για κάθε $g \in G$. Παρατηρούμε έπειτα ότι η $\varphi_{g^{-1}}$ είναι η αντίστροφη απεικόνιση της φ_g και συμπεραίνουμε ότι $\varphi_g \in S(X)$ για κάθε $g \in G$. Για το (β) παρατηρούμε ότι $\varphi_{g_1g_2} = \varphi_{g_1} \circ \varphi_{g_2}$ για $g_1, g_2 \in G$, αφού $\varphi_{g_1g_2}(xH) = (g_1g_2)xH = g_1(g_2x)H = \varphi_{g_1}(\varphi_{g_2}(xH))$ για κάθε $x \in H$, και συμπεραίνουμε ότι η $\varphi : G \to S(X)$ με $\varphi(g) = \varphi_g$ για $g \in G$ είναι ομομορφισμός ομάδων. Τέλος, υποθέτοντας ότι $g \in \ker(\varphi)$, έχουμε $(gx)H = xH$ για κάθε $x \in G$, άρα και για $x = e$, και συμπεραίνουμε ότι $g \in H$.

(181) Θα δείξουμε ότι οι μόνοι τέτοιοι ομομορφισμοί είναι ο τετριμμένος και ο ομομορφισμός του προσήμου $\epsilon : S_n \to \{1, -1\}$. Παρατηρούμε ότι για κάθε αντιμετάθεση $t \in S_n$ έχουμε $(\varphi(t))^2 = \varphi(t^2) = \varphi(e) = 1$ και συνεπώς ότι $\varphi(t) \in \{1, -1\}$. Θυμόμαστε έπειτα ότι οποιεσδήποτε δύο αντιμεταθέσεις $t_1, t_2 \in S_n$ είναι συζυγείς, δηλαδή ότι ισχύει $t_2 = \sigma t_1 \sigma^{-1}$ για κάποια μετάθεση $\sigma \in S_n$, οπότε $\varphi(t_2) = \varphi(\sigma t_1 \sigma^{-1}) = \varphi(\sigma)\varphi(t_1)\varphi(\sigma)^{-1} = \varphi(t_1)$. Από τα προηγούμενα προκύπτει ότι είτε $\varphi(t) = 1$ για κάθε αντιμετάθεση $t \in S_n$, είτε $\varphi(t) = -1$ για κάθε αντιμετάθεση $t \in S_n$. Στην πρώτη περίπτωση ο φ είναι ο τετριμμένος ομομορφισμός. Πράγματι, αφού κάθε μετάθεση $\sigma \in S_n$ γράφεται ως γινόμενο αντιμεταθέσεων $\sigma = t_1 t_2 \cdots t_m$, θα έχουμε $\varphi(\sigma) = \varphi(t_1)\varphi(t_2)\cdots\varphi(t_m) = 1$. Ομοίως, στη δεύτερη περίπτωση βρίσκουμε ότι $\varphi(\sigma) = \epsilon(\sigma)$ για κάθε $\sigma \in S_n$.

(182) Για το (α) χρησιμοποιήστε βασικές ιδιότητες των οριζουσών. Από το (α) προκύπτει ότι το σύνολο $\mathrm{SL}_n(\mathbb{F}_q)$ είναι κανονική υποομάδα της $\mathrm{GL}_n(\mathbb{F}_q)$ και ότι για την τάξη της ισχύει

$$|\mathrm{SL}_n(\mathbb{F}_q)| \;=\; |\mathrm{GL}_n(\mathbb{F}_q)| \,/\, |\mathbb{F}_q^{\times}| \;=\; |\mathrm{GL}_n(\mathbb{F}_q)| \,/\, (q-1).$$

Από αυτό και το αποτέλεσμα της Άσκησης 119 (β) προκύπτει ότι η τάξη της $\mathrm{SL}_n(\mathbb{F}_q)$ είναι ίση με $q^{\binom{n}{2}}(q^2-1)\cdots(q^n-1)$.

(183) Μια υποομάδα H μιας ομάδας G είναι κανονική αν και μόνο αν η H γράφεται ως ένωση κλάσεων συζυγίας της G. Οι κλάσεις συζυγίας της S_4 είναι εκείνη που αποτελείται μόνο από την ταυτοτική μετάθεση, εκείνη με στοιχεία τις έξι αντιμεταθέσεις της S_4, εκείνη με στοιχεία $(1\,2)(3\,4)$, $(1\,3)(2\,4)$ και $(1\,4)(2\,3)$, εκείνη με στοιχεία τους οκτώ κύκλους μήκους 3 της S_4 και εκείνη με στοιχεία τις έξι κυκλικές μεταθέσεις (κύκλους μήκους 4) του $\{1, 2, 3, 4\}$. Οι μόνες υποομάδες της S_4 που γράφονται ως ένωση αυτών των κλάσεων είναι οι τετριμμένες υποομάδες, η τεραεδρική ομάδα $\{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ και η εναλλάσσουσα ομάδα A_4.

(184) Θα δείξουμε ότι ο $n = 2$ είναι ο μόνος ακέραιος με αυτή την ιδιότητα. Πράγματι, ας υποθέσουμε ότι για κάποιο $n \geq 3$ η συμμετρική ομάδα S_n είναι ισόμορφη με το ευθύ γινόμενο $S_{n-1} \times C_n$, όπου C_n είναι η κυκλική ομάδα τάξης n. Τότε η S_n έχει μια κανονική κυκλική υποομάδα $H = \langle\sigma\rangle$ τάξης n, για κάποια $\sigma \in S_n$. Διακρίνουμε δύο περιπτώσεις. Έστω ότι η σ είναι κυκλική. Τότε όλες οι $(n-1)!$ κυκλικές μεταθέσεις της S_n είναι συζυγείς της σ και συνεπώς ανήκουν στην κανονική υποομάδα H τάξης n. Συμπεραίνουμε ότι $(n-1)! \leq n-1$, οπότε $n = 3$. Η περίπτωση αυτή αποκλείεται καθώς η ομάδα $S_2 \times C_3$ είναι αβελιανή, ενώ S_3 δεν είναι. Έστω τέλος ότι η σ δεν είναι κυκλική. Τότε υπάρχουν διακεκριμένα στοιχεία $a, b, c \in \{1, 2, \ldots, n\}$ με $\sigma(a) = b$, τέτοια ώστε το c δεν ανήκει στον κύκλο της σ που περιέχει τα a, b.

Τότε, η μετάθεση $\tau = (a\ c)\,\sigma\,(a\ c)$ είναι συζυγής της σ αλλά δεν ανήκει στην $H = \langle\sigma\rangle$, αφού $\tau(c) = b$, σε αντίθεση με την κανονικότητα της H. Μια άλλη λύση προκύπτει εφαρμόζοντας την Άσκηση 197.

(185) Για το (γ) υποθέτουμε ότι ο $\varphi : G \to K$ είναι επιμορφισμός ομάδων και θεωρούμε $w \in K$ και $y \in \varphi(H)$. Επιλέγουμε $g \in G$ και $x \in H$ τέτοια ώστε $w = \varphi(g)$ και $y = \varphi(x)$ και βρίσκουμε ότι $wyw^{-1} = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(gxg^{-1}) \in \varphi(H)$, αφού η H είναι κανονική υποομάδα της G και συνεπώς $gxg^{-1} \in H$. Αυτό δείχνει ότι η $\varphi(H)$ είναι κανονική υποομάδα της K. Για το δεύτερο ερώτημα θεωρούμε τυχαία μη κανονική υποομάδα H μιας ομάδας G και το μονομορφισμό ομάδων $\iota : H \to G$ με $\iota(x) = x$ για $x \in H$. Παρατηρούμε ότι η H είναι κανονική υποομάδα της H και ότι η $\iota(H)$ δεν είναι κανονική υποομάδα της G και συμπεραίνουμε ότι η απάντηση στο ερώτημα αυτό είναι αρνητική. Τα υπόλοιπα ερωτήματα αφήνονται στον αναγνώστη.

(186) Για το (α) δείξτε ότι η απεικόνιση $\varphi : G \to \mathbb{R}^\times$ που ορίζεται θέτοντας

$$\varphi\begin{pmatrix} x & y \\ 0 & 1/x \end{pmatrix} = x$$

είναι επιμορφισμός ομάδων με πυρήνα $\ker(\varphi) = N$. Για το (β) θεωρήστε την αντίστροφη εικόνα τυχαίας μη τετριμμένης υποομάδας της αβελιανής ομάδας $\mathbb{R}^\times$, για παράδειγμα την

$$K = \left\{ \begin{pmatrix} x & y \\ 0 & 1/x \end{pmatrix} : x > 0,\ y \in \mathbb{R} \right\}.$$

Σύμφωνα με το (δ) της Άσκησης 185, κάθε τέτοια αντίστροφη εικόνα είναι κανονική υποομάδα της G που περιέχει τη N. Για το (γ) θεωρήστε μη τετριμμένη κανονική υποομάδα H της G που περιέχεται στην N, υπολογίστε ότι

$$\begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a^2y \\ 0 & 1 \end{pmatrix}$$

και ότι

$$\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -y \\ 0 & 1 \end{pmatrix}$$

και συνάγετε ότι $H = N$.

(187) Για το (α) θεωρήστε την ομάδα G των συμμετριών του τετραγώνου (διεδρική ομάδα τάξης 8) και μια μη κυκλική υποομάδα $N = \{e, a, b, ab\}$, όπου $a, b \in G$ είναι δύο ανακλάσεις ως προς άξονες συμμετρίας κάθετους μεταξύ τους. Παρατηρήστε ότι η N είναι κανονική υποομάδα της G και ότι η $\{e, a\}$ είναι κανονική υποομάδα της N (ως υποομάδες δείκτη 2) αλλά ότι η $\{e, a\}$ δεν είναι κανονική υποομάδα της G και συμπεράνετε ότι η πρόταση στο (α) είναι ψευδής. Υποθέστε τώρα ότι η κυκλική υποομάδα $N = \langle a\rangle$ της G είναι κανονική υποομάδα της G και θεωρήστε υποομάδα H της N. Αφού κάθε υποομάδα κυκλικής ομάδας είναι κυκλική, έχουμε $H = \langle a^k\rangle$ για κάποιο $k \in \mathbb{N}$. Χρησιμοποιώντας την ισότητα $ga^kg^{-1} = (gag^{-1})^k$ δείξτε ότι $ga^kg^{-1} \in H$ για κάθε $g \in G$ και συμπεράνετε ότι η πρόταση στο (β) είναι αληθής.

(188) Για το (α) χρησιμοποιήστε το Θεώρημα του Lagrange για να δείξετε ότι η τάξη της G διαιρείται με το $2n$ και να συμπεράνετε το ζητούμενο. Για το (β) θεωρήστε τη διεδρική ομάδα τάξης $2n$. Για το (γ) θέτουμε $N = \{e, a\}$ και σκεφτόμαστε ως εξής. Αφού η K έχει τάξη τον πρώτο αριθμό n, η ομάδα αυτή είναι κυκλική, έστω με γεννήτορα $b \in K$ τάξης n. Από την κανονικότητα της N προκύπτει εύκολα ότι $ax = xa$ για κάθε $x \in G$ και ειδικότερα ότι $ab = ba$. Υπολογίζοντας ότι $(ab)^m = a^mb^m = ab^m$ για περιττούς ακεραίους και $(ab)^m = b^m$ για άρτιους, βρίσκουμε ότι η τάξη του ab είναι ίση με $2n$ και συμπεραίνουμε το ζητούμενο.

(189) Παρατηρούμε ότι $aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) \in H \cdot H \subseteq H$ και ότι $aba^{-1}b^{-1} = (aba^{-1})b^{-1} \in K \cdot K \subseteq K$ για $a \in H$ και $b \in K$ και συμπεραίνουμε ότι $aba^{-1}b^{-1} \in H \cap K = \{e\}$, δηλαδή ότι $ab = ba$, για $a \in H$ και $b \in K$.

(190) Θεωρήστε τον ομομορφισμό ομάδων $\varphi : G \to S(X)$ της Άσκησης 180 και τον πυρήνα αυτού $N = \ker(\varphi)$. Από το αποτέλεσμα αυτής της άσκησης έχουμε $N \subseteq H$. Παρατηρώντας ότι η ομάδα πηλίκο G/N είναι ισόμορφη με μια υποομάδα της $S(X)$, δείξτε ότι η τάξη της $[G : N]$ διαιρεί το $p!$. Από αυτό και την ισότητα $[G : N] = [G : H][H : N]$ συμπεράνετε ότι ο δείκτης $[H : N]$ διαιρεί το $(p-1)!$. Αφού ο δείκτης αυτός διαιρεί την τάξη της H, άρα και της G, από την υπόθεση της άσκησης συμπεράνετε ότι $[H : N] = 1$, δηλαδή ότι $H = N$, και συνάγετε ότι η H είναι κανονική υποομάδα της G.

(191) Το (α) αφήνεται στον αναγνώστη. Απάντηση στο (β): οι αριστερές κλάσεις είναι τα σύνολα της μορφής $\{(ax, x) : x \in G\}$ και οι δεξιές τα σύνολα της μορφής $\{(xa, x) : x \in G\}$, για $a \in G$. Για το (γ), υποθέτοντας ότι η N είναι κανονική, παρατηρήστε ότι $(axa^{-1}, x) = (a, e)(x, x)(a, e)^{-1} \in N$ και συμπεράνετε ότι $axa^{-1} = x$, για όλα τα $a, x \in G$. Για το αντίστροφο παρατηρήστε ότι αν η G είναι αβελιανή, τότε το ίδιο ισχύει και για τη $G \times G$ και συνεπώς κάθε υποομάδα της τελευταίας είναι κανονική. Για το (δ) χρησιμοποιήστε το (β) και τον ορισμό της ομάδας πηλίκο, ή τον επιμορφισμό ομάδων $\varphi : G \times G \to G$ που ορίζεται θέτοντας $\varphi(x, y) = xy^{-1}$ για $x, y \in G$.

(192) Για το (α), δείξτε ότι κάθε $x \in G$ γράφεται με μοναδικό τρόπο στη μορφή $x = ab$, με $a \in H$ και $b \in N$. Για το σκοπό αυτόν, παρατηρήστε ότι αν $ab = cd$ με $a, c \in H$ και $b, d \in K$, τότε $c^{-1}a = db^{-1} \in H \cap N = \{e\}$ και συμπεράνετε ότι $a = c$ και $b = d$. Για το (β), δείξτε ότι οι αριστερές κλάσεις της N στη G είναι ακριβώς τα σύνολα aN με $a \in H$ και ότι η απεικόνιση $\varphi : G/N \to H$ με $\varphi(aN) = a$ για $a \in H$ είναι ισομορφισμός ομάδων. Για το (γ), χρησιμοποιώντας τη λύση του (α) και την Άσκηση 189, δείξτε ότι η απεικόνιση $\psi : H \times N \to G$ με $\psi(a, b) = ab$ για $a \in H$ και $b \in N$ είναι ισομορφισμός ομάδων. Για το (δ), θεωρήστε τη συμμετρική ομάδα $G = S_3$ και τις υποομάδες της $H = \langle(1\ 2)\rangle$ και $N = \langle(1\ 2\ 3)\rangle$.

(193) Για το (α) δείξτε ότι $\alpha \circ \psi_g \circ \alpha^{-1} = \psi_{\alpha(g)}$ για κάθε $\alpha \in \mathrm{Aut}(G)$ και κάθε $g \in G$ και συμπεράνετε το ζητούμενο. Για το (β) θεωρήστε την απεικόνιση $\psi : G \to \mathrm{Inn}(G)$ με $\psi(g) = \psi_g$ για $g \in G$. Δείξτε ότι η ψ είναι επιμορφισμός ομάδων και με πυρήνα $Z(G)$ και εφαρμόστε το θεώρημα του ισομορφισμού για αυτόν τον επιμορφισμό.

(194) Το (α) αφήνεται στον αναγνώστη. Για το (β) παρατηρούμε ότι $a, b \in \mathbb{Z}$ έχουμε $2\bar{a} - 3\bar{b} = \bar{0} \Leftrightarrow \bar{a} = 5\bar{b} \Leftrightarrow a = 5b + 7c$ για κάποιο $c \in \mathbb{Z}$ και συμπεραίνουμε ότι

$$\ker(\varphi) = \left\{ \begin{pmatrix} 5b+7c \\ b \end{pmatrix} : b, c \in \mathbb{Z} \right\} = \left\{ b \begin{pmatrix} 5 \\ 1 \end{pmatrix} + c \begin{pmatrix} 7 \\ 0 \end{pmatrix} : b, c \in \mathbb{Z} \right\}.$$

Από την τελευταία έκφραση και τις ισότητες

$$\begin{pmatrix} 5 \\ 1 \end{pmatrix} = 2\begin{pmatrix} 3 \\ 2 \end{pmatrix} - \begin{pmatrix} 1 \\ 3 \end{pmatrix} \in H, \quad \begin{pmatrix} 7 \\ 0 \end{pmatrix} = 3\begin{pmatrix} 3 \\ 2 \end{pmatrix} - 2\begin{pmatrix} 1 \\ 3 \end{pmatrix} \in H$$

προκύπτει ότι $\ker(\varphi) \subseteq H$. Το (γ) έπεται από το (β) και το θεώρημα του ισομορφισμού.

(195) Αληθής είναι μόνο η πρόταση στο (β). Για το (α) παρατηρήστε ότι η G/N έχει μικρότερη τάξη από εκείνη της G για κάθε πεπερασμένη ομάδα G και κάθε μη τετριμμένη κανονική υποομάδα N αυτής. Για το (β) θεωρήστε την υποομάδα $G = \{z \in \mathbb{C} : |z| = 1\}$ της πολλαπλασιαστικής ομάδας $\mathbb{C}^\times$ και την υποομάδα $E_n = \{z \in \mathbb{C} : z^n = 1\}$ της G για τυχαίο ακέραιο $n \geq 2$. Δείξτε ότι η απεικόνιση $\varphi : G \to G$ που ορίζεται θέτοντας $\varphi(z) = z^n$ για $z \in G$ είναι επιμορφισμός

ομάδων με πυρήνα $N = E_n$ και συμπεράνετε ότι η ομάδα πηλίκο G/N είναι ισόμορφη με τη G.

(196) Η πρόταση είναι αληθής. Αφού η ομάδα πηλίκο G/N έχει τάξη n, η τάξη οποιουδήποτε στοιχείου της xN διαιρεί το n. Άρα ισχύει $x^nN = N$, δηλαδή $x^n \in N$, για κάθε $x \in G$. Το αποτέλεσμα αυτό είναι ισχυρότερο εκείνο της Άσκησης 160 (β).

(197) Έστω κανονική υποομάδα N της S_n για την οποία η $A := S_n/N$ είναι αβελιανή. Τότε, $N = \ker(\varphi)$ για κάποιον ομομορφισμό ομάδων $\varphi : S_n \to A$. Αρκεί να δείξουμε ότι $\tau \in \ker(\varphi)$ για κάθε άρτια μετάθεση $\tau \in S_n$. Λόγω της Άσκησης 130 (β), αρκεί να δείξουμε ότι $\sigma \in \ker(\varphi)$ για κάθε μετάθεση $\sigma \in S_n$ περιττής τάξης. Όμως, για κάθε τέτοια μετάθεση, η σ^2 είναι συζυγής με τη σ (εξηγήστε γιατί). Άρα, $\sigma^2 = w\sigma w^{-1}$ για κάποια $w \in S_n$. Εφαρμόζοντας τον ομομορφισμό φ, βρίσκουμε ότι $\varphi(\sigma)^2 = \varphi(w)\varphi(\sigma)\varphi(w)^{-1} = \varphi(\sigma)\varphi(w)\varphi(w)^{-1} = \varphi(\sigma)$ και συμπεραίνουμε ότι $\sigma \in \ker(\varphi)$.

(198) Θεωρήστε τον ομομορφισμό ομάδων $\varphi : G \to S(X)$ της Άσκησης 180 και τον πυρήνα αυτού $N = \ker(\varphi)$, ο οποίος είναι κανονική υποομάδα της G. Από το αποτέλεσμα αυτής της άσκησης έχουμε $N \subseteq H$. Από το θεώρημα του ισομορφισμού συμπεράνετε ότι $[G : N] \leq |S(X)| < \infty$.

(199) Λόγω της Άσκησης 193, και αφού η $Z(S_n)$ είναι η τετριμμένη υποομάδα της S_n για $n \geq 2$, αρκεί να δείξουμε ότι $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$ για $n \neq 6$. Έστω $\varphi \in \mathrm{Aut}(S_n)$. Θέλουμε να δείξουμε ότι υπάρχει μετάθεση $w \in S_n$, τέτοια ώστε $\varphi(\sigma) = w\sigma w^{-1}$ για κάθε $\sigma \in S_n$. Αφού η S_n παράγεται από αντιμεταθέσεις, αρκεί να δείξει κανείς (εξηγήστε γιατί) ότι ο αυτομορφισμός φ απεικονίζει αντιμεταθέσεις σε αντιμεταθέσεις. Παρατηρούμε ότι ο φ απεικονίζει κλάσεις συζυγίας σε κλάσεις συζυγίας, αφού $\varphi(u\sigma u^{-1}) = \varphi(u)\varphi(\sigma)\varphi(u)^{-1}$ για $u, \sigma \in S_n$. Επομένως, ο φ μεταθέτει τις κλάσεις συζυγίας της S_n δοσμένου πλήθους στοιχείων. Από αυτά συμπεραίνουμε ότι αν $\varphi \notin \mathrm{Inn}(S_n)$, τότε η κλάση συζυγίας των αντιμεταθέσεων της S_n θα πρέπει να έχει το ίδιο πλήθος στοιχείων με κάποια άλλη κλάση συζυγίας. Αφού προφανώς ο φ απεικονίζει αντιμεταθέσεις σε μεταθέσεις τάξης δύο, συμπεραίνουμε (εξηγήστε πως) ότι

$$\binom{n}{2} = 1 \cdot 3 \cdots (2k-1)\binom{n}{2k}$$

για κάποιο $k \geq 2$ ή, ισοδύναμα, ότι $(n-2)(n-3)\cdots(n-2k+1) = 2^{k-1}k!$ για κάποιο $k \geq 2$. Η μόνη δυνατότητα είναι η $k = 3$ και $n = 6$ (εξηγήστε γιατί). Για $n = 6$, θέτοντας $s_1 = (1\ 2)$, $s_2 = (2\ 3)$, $s_3 = (3\ 4)$, $s_4 = (4\ 5)$ και $s_5 = (5\ 6)$, υπάρχει πράγματι αυτομορφισμός φ της S_n με

$$\begin{aligned}
\varphi(s_1) &= (1\ 2)(3\ 4)(5\ 6),\\
\varphi(s_2) &= (1\ 4)(2\ 5)(3\ 6),\\
\varphi(s_3) &= (1\ 3)(2\ 4)(5\ 6),\\
\varphi(s_4) &= (1\ 2)(3\ 6)(4\ 5),\\
\varphi(s_5) &= (1\ 4)(2\ 3)(5\ 6).
\end{aligned}$$

Το παράδειγμα αυτό είναι παρμένο από το βιβλίο Abstract Algebra των D.S. Dummit και R.M. Foote. Ευχαριστώ το Νίκο Αδαλόγλου για τη διόρθωση της διατύπωσης αυτής της άσκησης και την υπόδειξη για τη βιβλιογραφία.

(200) Για το (α) παρατηρήστε ότι, αφού $\det(A) = 1$, με αναγωγή των στοιχείων του modulo m, ο A μπορεί να θεωρηθεί στοιχείο της πεπερασμένης ομάδας $\mathrm{GL}_n(\mathbb{Z}_m)$ και συμπεράνετε ότι ως τέτοιο στοιχείο, ο A έχει πεπερασμένη τάξη. Για το (β), εφαρμόστε το (α) για $m = |\det(P)|$ και συμπεράνετε ότι

$$B^k = P^{-1}A^kP = P^{-1}(I + mC)P = I + P^{-1}(mC)P = I + QCP,$$

όπου $Q = mP^{-1}$ είναι πίνακας με στοιχεία ακέραιους αριθμούς.