Βασική Άλγεβρα

Ασκήσεις

2013-14 (εκδοχή 15-3-2014)

Βασική Άλγεβρα

Ασκήσεις
Υποδείξεις/Απαντήσεις

Περιεχόμενα

		σελίδα
Ασκήσεις1	Διαιρετότητα στους ακέραιους, ισοτιμίες	1
Ασκήσεις2	Ακέραιοι modulo n, Θεώρημα του Euler	7
Ασκήσεις3	Δακτύλιοι: ορισμοί, παραδείγματα, βασικές ιδιότητες	14
Ασκήσεις4	Πολυώνυμα	25
Ασκήσεις5	Ομομορφισμοί και ιδεώδη	36
Ασκήσεις6	Ομάδες συμμετρίας, συμμετρικές ομάδες, βασικές ιδιότητες ομάδων	53
Ασκήσεις7	Υποομάδες, Θεώρημα του Lagrange	63
Ασκήσεις8	Ομομορφισμοί ομάδων, περισσότερα για κυκλικές ομάδες	76
Ασκήσεις9	Κανονικές υποομάδες, ομάδα πηλίκο	89

Εκδοχή 15/3/2014

Ασκήσεις1
Διαιρετότητα στους ακέραιους, ισοτιμίες

1. Δείξτε τις εξής προτάσεις.
   a. Αν $a,b\in\mathbb{Z}$ και $d=\text{μκδ}(a,b)$ [1], τότε $\text{μκδ}(a/d,b/d)=1$.
   b. Αν ο $n\in\mathbb{N}$ δεν είναι τετράγωνο ακεραίου, τότε $\sqrt{n}\notin\mathbb{Q}$.

2. Έστω $a,b,c\in\mathbb{Z}$ με $\mu\kappa\delta(a,b)=1$. Δείξτε τις εξής προτάσεις.
   a. Αν $a\mid bc$, τότε $a\mid c$.
   b. Αν $a\mid c$ και $b\mid c$, τότε $ab\mid c$.
   c. $\mu\kappa\delta(a,bc)=\mu\kappa\delta(a,c)$.

3. Έστω $a,b,c\in\mathbb{Z}, c>0$. Δείξτε τις εξής προτάσεις.
   a. $\mu\kappa\delta(a,b)\cdot\varepsilon\kappa\pi(a,b)=ab$
   b. $\mu\kappa\delta(ac,bc)=c\cdot\mu\kappa\delta(a,b)$.

4. Έστω $a,b,p\in\mathbb{Z}$ όπου p πρώτος. Δείξτε ότι αν $p\mid a^4$ και $p\mid a^2+b^2$, τότε $p\mid b$.

5. Δείξτε ότι αν $a,b,k\in\mathbb{Z}$, τότε
   a. $\mu\kappa\delta(a,b)=\mu\kappa\delta(a+kb,b)$ και
   b. $\mu\kappa\delta(a,b)=1\Leftrightarrow\mu\kappa\delta(a+b,ab)=1$.

6.
   a. Για κάθε $n\in\mathbb{Z}$ ισχύει $\mu\kappa\delta(3n+1,10n+3)=1$.
   b. Να βρεθούν όλοι οι πρώτοι που διαιρούν το $\text{μκδ}(n^2+n+5,n+6)$ για κάποιο $n\in\mathbb{Z}$.

7. Να υπολογιστεί ο $\mu\kappa\delta(165,418)$ και ακέραιοι x,y τέτοιοι ώστε $\mu\kappa\delta(165,418)=165x+418y$.

8. Να βρεθούν όλες οι τριάδες $(p,p+2,p+4)$, όπου οι $p,p+2,p+4$ είναι πρώτοι αριθμοί.

9. Ποιο είναι το ελάχιστο στοιχείο του συνόλου $\{24a+36b>0\mid a,b\in\mathbb{Z}\}$ και ποιο είναι το μέγιστο στοιχείο του $\{24a+36b+42c<0\mid a,b,c\in\mathbb{Z}\}$;

10. Αν $a,b\in\mathbb{Z}$ είναι τέτοια ώστε $a^3\mid b^7$, τότε $a\mid b^3$.

11. Έστω $a,b,n\in\mathbb{Z}_{>0}$ με $n>1$. Δείξτε ότι $\mu\kappa\delta(n^a-1,n^b-1)=n^d-1$, όπου $d=\mu\kappa\delta(a,b)$.

12. Να βρεθούν όλοι οι πρώτοι p,q με $49p+72q=pq^2$.

13. Δείξτε ότι
   a. $21\mid 4^{n+2}+5^{2n+1}$ για κάθε $n\in\mathbb{N}$,
   b. $10^n+3\cdot 4^{n+2}\equiv 4 \bmod 9$ για κάθε $n\in\mathbb{N}$.

14. Έστω m,n περιττοί θετικοί ακέραιοι. Τότε $1^m+2^m+\ldots+(n-1)^m\equiv 0 \bmod n$

15. Αν $a,b\in\mathbb{Z}, n\in\mathbb{Z}_{>0}$ και $a\equiv b \bmod n$, τότε
   a. $a^n\equiv b^n \bmod n^2$ και
   b. $\mu\kappa\delta(a^k,n)=\mu\kappa\delta(b^k,n)$ για κάθε θετικό ακέραιο k.

16. Αληθεύει ότι ο ακέραιος $2^{1000}+5$ είναι πρώτος;

17. Δείξτε ότι δεν υπάρχουν $n,x,y\in\mathbb{N}$ τέτοιοι ώστε $x^2+y^2=4n+3$.

18. Δείξτε ότι δεν υπάρχουν ακέραιοι x,y τέτοιοι ώστε $x^2-5y^2=13$.

19. Δείξτε ότι δεν υπάρχουν $x,y\in\mathbb{Q}$ τέτοιοι ώστε $x^2+y^2=3$.

20. *[2]Δείξτε ότι δεν υπάρχουν $m,n,x\in\mathbb{N}$ τέτοιοι ώστε $3^m+3^n+1=x^2$.

21. Εξετάστε ποιες από τις ακόλουθες προτάσεις αληθεύουν. Έστω $a,b,c,m\in\mathbb{Z}$.

---

[1] Όταν γράφουμε μκδ(a,b) ή εκπ(a,b) υποθέτουμε ότι τουλάχιστον ένας από τους a,b είναι μη μηδενικός (χωρίς να το αναφέρουμε ρητώς).
[2] Με * σημειώνονται οι ασκήσεις που ίσως είναι οι πιο απαιτητικές της ομάδας.

a. Αν $a|c$ και $b|c$, τότε $ab|c$.

b. Αν $a^2|b^3$, τότε $a|b$.

c. Αν $ac \equiv bc \bmod cm$ και $c \neq 0$, τότε $a \equiv b \bmod m$.

d. Αν $ac \equiv bc \bmod m$ και $\mu\kappa\delta(m,c)=1$, τότε $a \equiv b \bmod m$.

e. $\mu\kappa\delta(a,b)\cdot\mu\kappa\delta(a,c)=\mu\kappa\delta(a,bc)$.

f. Αν $\mu\kappa\delta(b,c)=1$, τότε $\mu\kappa\delta(a,b)\cdot\mu\kappa\delta(a,c)=\mu\kappa\delta(a,bc)$.

Υποδείξεις/Απαντήσεις
Ασκήσεις1

1.

a. Έστω $a_1 = a/d$, $b_1 = b/d$, οπότε $a_1, b_1 \in \mathbb{Z}$ και $a = da_1, b = db_1$. Αν $c \in \mathbb{Z}_{>0}$ είναι κοινός διαιρέτης των a_1, a_2, τότε ο dc είναι κοινός διαιρέτης των a, b. Άρα $dc \mid d$ καθώς $d = \text{μκδ}(a,b)$. Επειδή $d \neq 0$, παίρνουμε $c = 1$, οπότε $\text{μκδ}(a_1, b_1) = 1$.

b. Έστω $\sqrt{n} \in \mathbb{Q}$, δηλαδή $\sqrt{n} = \frac{a}{b}$ για κάποια $a, b \in \mathbb{Z}, b \neq 0$. Μπορούμε να υποθέσουμε ότι $\text{μκδ}(a,b) = 1$, γιατί διαφορετικά απλοποιούμε το κλάσμα ($\frac{a}{b} = \frac{a/d}{b/d}$, όπου $d = \text{μκδ}(a,b)$, και $\text{μκδ}(a/d, b/d) = 1$)). Έχουμε $a^2 = nb^2$. Από την υπόθεση, $b \neq \pm 1$, οπότε υπάρχει πρώτος p με $p \mid b$. Τότε $p \mid a^2$ και από το λήμμα του Ευκλείδη (βλ. Λήμμα 1.2.5 [3]), $p \mid a$. Δηλαδή έχουμε $p \mid a$ και $p \mid b$ πράγμα άτοπο αφού $\text{μκδ}(a,b) = 1$.

2.

Σύμφωνα με το Θεώρημα 1.2.4 υπάρχουν $x, y \in \mathbb{Z}$ με $1 = ax + by$. Άρα

$$c = acx + bcy. \tag{1}$$

a. Αν $a \mid bc$, τότε $a \mid acx + bcy$ και από τη σχέση (1) έπεται ότι $a \mid c$.

b. Αν $a \mid c$ και $b \mid c$, τότε $ab \mid bc$ και $ab \mid ac$. Συνεπώς $ab \mid acx + bcy$ δηλαδή $ab \mid c$ λόγω της (1).

c. Επειδή $\text{μκδ}(a,bc) \mid a$ και $\text{μκδ}(a,bc) \mid bc$, από την (1) έπεται ότι $\text{μκδ}(a,bc) \mid c$. [Σημείωση: Θα μπορούσαμε να φτάσουμε στο ίδιο συμπέρασμα εφαρμόζοντας το a.]
Επειδή $\text{μκδ}(a,bc) \mid a$ και $\text{μκδ}(a,bc) \mid c$, παίρνουμε $\text{μκδ}(a,bc) \mid \text{μκδ}(a,c)$.
Έχουμε $\text{μκδ}(a,c) \mid c$, οπότε $\text{μκδ}(a,c) \mid bc$. Από $\text{μκδ}(a,c) \mid a$ και $\text{μκδ}(a,c) \mid bc$ έπεται ότι $\text{μκδ}(a,c) \mid \text{μκδ}(a,bc)$.
Τελικά έχουμε $\text{μκδ}(a,bc) \mid \text{μκδ}(a,c)$ και $\text{μκδ}(a,c) \mid \text{μκδ}(a,bc)$. Επειδή οι ακέραιοι $\text{μκδ}(a,bc)$ και $\text{μκδ}(a,c)$ είναι θετικοί παίρνουμε $\text{μκδ}(a,bc) = \text{μκδ}(a,c)$.

3.

a. Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $a, b > 1$ (γιατί;). Έστω $a = p_1^{a_1} \ldots p_k^{a_k}$, $b = p_1^{b_1} \ldots p_k^{b_k}$, όπου $p_1, \ldots, p_k$ είναι πρώτοι διάφοροι ανά δύο και $a_i, b_i \in \mathbb{N}$. Ξέρουμε ότι $\text{μκδ}(a,b) = p_1^{c_1} \ldots p_k^{c_k}$ και $\text{εκπ}(a,b) = p_1^{d_1} \ldots p_k^{d_k}$, όπου $c_i = \min\{a_i, b_i\}$, $d_i = \max\{a_i, b_i\}$. Από τη σχέση $\min\{a_i, b_i\} + \max\{a_i, b_i\} = a_i + b_i$ έπεται ότι

$$\text{μκδ}(a,b) \cdot \text{εκπ}(a,b) = p_1^{c_1} \ldots p_k^{c_k} p_1^{d_1} \ldots p_k^{d_k} =$$
$$= p_1^{c_1 + d_1} \ldots p_k^{c_k + d_k} = p_1^{a_1 + b_1} \ldots p_k^{a_k + b_k} = ab.$$

b. Μπορεί να δοθεί μια απόδειξη όπως η προηγούμενη που να βασίζεται στη σχέση $\min\{a_i + c_i, b_i + c_i\} = c_i + \min\{a_i + b_i\}$ (άσκηση).
Μια άλλη απόδειξη είναι: Από το Θεώρημα 1.2.4 υπάρχουν ακέραιοι x, y με $ax + by = d$, όπου $d = \text{μκδ}(a,b)$. Άρα $acx + bcy = cd$. Επειδή $\text{μκδ}(ac,bc) \mid ac$ και $\text{μκδ}(ac,bc) \mid bc$, από την προηγούμενη ισότητα παίρνουμε $\text{μκδ}(ac,bc) \mid cd$.
Επειδή $d \mid a$ έχουμε $cd \mid ac$. Όμοια $cd \mid bc$. Άρα $cd \mid \text{μκδ}(ac,bc)$.

[3] Οι παραπομπές σε Θεωρήματα, Προτάσεις και Παραδείγματα αναφέρονται στο βιβλίο *Μια Εισαγωγή στην Άλγεβρα,* Δ. Βάρσος, Δ. Δεριζιώτης, Ι. Εμμανουήλ, Μ. Μαλιάκας, Ο. Ταλέλλη, Γ έκδοση, εκδόσεις Σοφία, 2012, ISBN 978-960-6706-37-0. Οι παραπομπές σε ασκήσεις αναφέρονται στις παρούσες σημειώσεις (πχ άσκηση 1.2 σημαίνει την άσκηση 2 από την ομάδα Ασκήσεις1.)

Τελικά έχουμε μκδ$(ac,bc)\,|\,cd$ και $cd\,|\,$μκδ(ac,bc). Επειδή οι ακέραιοι μκδ(ac,bc) και cd είναι θετικοί παίρνουμε μκδ$(ac,bc)=cd$.

4. Υπόδειξη: Από $p\,|\,a^4$ έπεται ότι $p\,|\,a$ γιατί ο p είναι πρώτος (Λήμμα 1.2.5).

5.

b. '$\Rightarrow$' Έστω ότι $\mu\kappa\delta(a,b)=1$. Έστω ότι υπάρχει πρώτος p με $p\,|\,\mu\kappa\delta(a+b,ab)$. Τότε $p\,|\,a+b$ και $p\,|\,ab$. Από την τελευταία σχέση έπεται ότι $p\,|\,a$ ή $p\,|\,b$, γιατί ο p είναι πρώτος (Λήμμα 1.2.5). Αν $p\,|\,a$, τότε από $p\,|\,a+b$ παίρνουμε $p\,|\,b$. Όμοια, αν $p\,|\,b$, τότε $p\,|\,a$. Σε κάθε περίπτωση έχουμε $p\,|\,a$ και $p\,|\,b$, οπότε $p\,|\,\mu\kappa\delta(a,b)$, δηλαδή $p\,|\,1$, άτοπο. Άρα $\mu\kappa\delta(a+b,ab)=1$.

'$\Leftarrow$' Έστω ότι $\mu\kappa\delta(a+b,ab)=1$. Έχουμε $\mu\kappa\delta(a,b)\,|\,a$ και $\mu\kappa\delta(a,b)\,|\,b$. Άρα $\mu\kappa\delta(a,b)\,|\,a+b$ και $\mu\kappa\delta(a,b)\,|\,ab$. Συνεπώς $\mu\kappa\delta(a,b)\,|\,\mu\kappa\delta(a+b,ab)$, δηλαδή $\mu\kappa\delta(a,b)\,|\,1$. Άρα $\mu\kappa\delta(a,b)=1$.

6.

a. Έχουμε (μιμούμενοι τον Ευκλείδειο αλγόριθμο)

$$10n+3=3\cdot(3n+1)+n$$
$$3n+1=3\cdot n+1$$
$$n=n\cdot 1+0.$$

Ξέρουμε ότι αν $b=qa+r$, όπου $a,b,q,r\in\mathbb{Z}$, τότε $\mu\kappa\delta(a,b)=\mu\kappa\delta(r,a)$, βλ. άσκηση 1.5a. Άρα παίρνουμε διαδοχικά $\mu\kappa\delta(10n+3,3n+1)=\mu\kappa\delta(3n+1,n)=\mu\kappa\delta(n,1)=1$.

b. Απάντηση: $p=5,7$.

7. Υπόδειξη: Βλ. Παράδειγμα σελίδα 22.

8.

Υπόδειξη: Αν p πρώτος και $p>3$, τότε $p=3k+1$ ή $p=3k+2$, όπου $k\in\mathbb{Z}$. Στην πρώτη περίπτωση ο $p+2$ δεν είναι πρώτος και στη δεύτερη ο $p+4$ δεν είναι πρώτος.

Υπάρχει μοναδική τριάδα, η $(3,5,7)$.

9. Υπόδειξη: Βλ. απόδειξη του Θεωρήματος 1.2.4.

Απάντηση: $12=$ μκδ$(24,36)$ και $-6=-$μκδ$(24,36,42)$ αντίστοιχα.

10.

Είναι σαφές ότι το ζητούμενο αληθεύει αν $a=0$ ή $b=0$. Έστω ότι $a,b\neq 0$ και έστω $a=\pm {p_1}^{a_1}\ldots {p_k}^{a_k}$, $b=\pm {p_1}^{b_1}\ldots {p_k}^{b_k}$, όπου $p_1,\ldots,p_k$ πρώτοι, $p_i\neq p_j$ για κάθε $i\neq j$ και $a_i,b_i\in\mathbb{N}$ για κάθε i. Από την υπόθεση έχουμε ${p_1}^{3a_1}\ldots {p_k}^{3a_k}\,|\,{p_1}^{7b_1}\ldots {p_k}^{7b_k}$ και άρα (σχέση 3 σελίδα 24)

$$3a_i\le 7b_i\Rightarrow a_i\le\frac{7}{3}b_i\le 3b_i \text{ για κάθε } i.$$

Από $a_i\le 3b_i$ για κάθε i έπεται ότι $a\,|\,b^3$.

11.

1η λύση (βασίζεται στον Ευκλείδειο αλγόριθμο). Παρατήρηση: Έστω $q,r\in\mathbb{N}$ με $b=qa+r$. Τότε υπάρχει $Q\in\mathbb{Z}$ τέτοιος ώστε $n^b-1=Q(n^a-1)+n^r-1$. Πράγματι, θέτοντας

$$Q=n^r\frac{n^{aq}-1}{n^a-1}=n^r(n^{a(q-1)}+n^{a(q-2)}+\ldots+1)\in\mathbb{Z},$$

εύκολα επαληθεύεται ότι $n^b-1=Q(n^a-1)+n^r-1$.

Εφαρμόζοντας τον Ευκλείδειο αλγόριθμο στα a,b υπάρχουν ακέραιοι $q,q_1,...,q_{k+1},r,r_1,...,r_k$ τέτοιοι ώστε

$$b=qa+r, \qquad 0\le r<a$$
$$a=q_1r+r_1, \qquad 0\le r_1<r$$
$$\vdots$$
$$r_{k-2}=q_kr_{k-1}+r_k, \quad 0\le r_k<r_{k-1}$$
$$r_{k-1}=q_{k+1}r_k+0.$$

Εφαρμόζοντας την παρατήρηση σε κάθε μία από τις παραπάνω ισότητες, υπάρχουν ακέραιοι $Q,Q_1,...,Q_{k+1}$ τέτοιοι ώστε

$$n^b-1=Q(n^a-1)+n^r-1$$
$$n^a-1=Q_1(n^r-1)+n^{r_1}-1$$
$$\vdots$$
$$n^{r_{k-2}}-1=Q_k(n^{r_{k-1}}-1)+n^{r_k}-1$$
$$n^{r_{k-1}}-1=Q_{k+1}(n^{r_k}-1)+0$$

Από τις ισότητες αυτές έπεται ότι

$$\mu\kappa\delta(n^a-1,n^b-1)=\mu\kappa\delta(n^a-1,n^r-1)=...$$
$$=\mu\kappa\delta(n^{r_{k-2}}-1,n^{r_{k-1}}-1)=\mu\kappa\delta(n^{r_{k-1}}-1,n^{r_k}-1)=$$
$$=\mu\kappa\delta(n^{r_k}-1,0)=n^{r_k}-1.$$

Από τον Ευκλείδειο αλγόριθμο ξέρουμε ότι $r_k=\mu\kappa\delta(a,b)$.

2η λύση: Αρχικά παρατηρούμε ότι αφού $d\,|\,a$ έχουμε $n^d-1\,|\,n^a-1$ λόγω της ταυτότητας $n^{dt}-1=(n^d-1)(n^{d(t-1)}+n^{d(t-2)}+...+n^d+1)$. Όμοια $n^d-1\,|\,n^b-1$ και συνεπώς $n^d-1\,|\,\mu\kappa\delta(n^a-1,n^b-1)$.

Έστω $c=\mu\kappa\delta(n^a-1,n^b-1)$. Τότε $n^a\equiv 1 \bmod c$ και $n^b\equiv 1 \bmod c$. Από το Θεώρημα 1.2.4 υπάρχουν ακέραιοι x, y με $d=ax+by.$ Χωρίς περιορισμό της γενικότητας υποθέτουμε ότι $x>0$ και $y\le 0.$ Έχουμε $n^{ax}\equiv 1 \bmod c$ και $n^{b(-y)}\equiv 1 \bmod c$. Άρα $n^d\equiv n^d 1\equiv n^d n^{b(-y)}\equiv n^{d+b(-y)}\equiv n^{ax}\equiv 1 \bmod c.$ Δηλαδή $c\,|\,n^d-1.$

Επειδή $n^d-1\,|\,c$, $c\,|\,n^d-1$ και $c>0,$ έχουμε $c=n^d-1.$

12. Απάντηση: $p=q=11.$

13.

a. Έχουμε $4^{n+2}+5^{2n+1}=16\cdot 4^n+5\cdot 25^n$ και $25\equiv 4 \bmod 21$. Άρα

$$4^{n+2}+5^{2n+1}\equiv 16\cdot 4^n+5\cdot 4^n \bmod 21.$$

Αλλά $16\cdot 4^n+5\cdot 4^n=21\cdot 4^n$ και $21\cdot 4^n\equiv 0 \bmod 21$. Άρα $4^{n+2}+5^{2n+1}\equiv 0 \bmod 21$, δηλαδή $21\,|\,4^{n+2}+5^{2n+1}$.

(Σημείωση. Φυσικά μπορεί να αποδειχτεί το ζητούμενο με επαγωγή στο n).

b. Επειδή $10\equiv 1 \bmod 9$ έχουμε $10^n\equiv 1^n\equiv 1 \bmod 9$ και άρα αρκεί να αποδειχτεί ότι $1+3\cdot 4^{n+2}\equiv 4 \bmod 9$.

Παρατηρούμε ότι $1+3\cdot 4^{n+2}-4=3(4^{n+2}-1)$ και $4^{n+2}\equiv 1 \bmod 3$. Άρα $9\,|\,3(4^{n+2}-1).$

14.

Έχουμε $n-i\equiv -i \bmod n$ για κάθε $i=1,...,n-1$ και άρα $i^m+(n-i)^m\equiv i^m+(-i)^m \bmod n$. Επειδή ο m είναι περιττός, $(-i)^m=(-1)^m i^m=-i^m$ και άρα

$$i^m+(n-i)^m\equiv 0 \bmod n.$$

Αθροίζοντας την τελευταία ισοτιμία για $i=1,2,...,\dfrac{n-1}{2}$, προκύπτει το ζητούμενο.

15.

Έχουμε $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1})$. Από την υπόθεση, $n \mid a-b$. Επίσης, $a^k \equiv b^k \bmod n$ για κάθε θετικό ακέραιο k (Πόρισμα 1.3.5). Συνεπώς

$$a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1} \equiv b^{n-1} + b^{n-2}b + ... + bb^{n-2} + b^{n-1} \equiv nb^{n-1} \equiv 0 \bmod n,$$

δηλαδή $n \mid a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1}$. Άρα $n^2 \mid (a-b)(a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1})$.

b. Από την υπόθεση, $a^k \equiv b^k \bmod n$. Συνεπώς $b^k = a^k + qn$, $q \in \mathbb{Z}$. Εύκολα αποδεικνύεται ότι $\text{μκδ}(a^k, n) = \text{μκδ}(a^k + qn, n)$ (άσκηση 1.5) και έχουμε το ζητούμενο.

16.

Όχι αφού $2^{1000} + 5 \equiv (-1)^{1000} + 5 \equiv 6 \equiv 0 \bmod 3$ και $2^{1000} + 5 > 3$.

17. Βλ. Εφαρμογή 1.3.8 1.

18.

Αν υπάρχουν ακέραιοι x, y τέτοιοι ώστε $x^2 - 5y^2 = 13$, τότε $x^2 \equiv 13 \bmod 5$, δηλαδή $x^2 \equiv 3 \bmod 5$. Επειδή $x \equiv 0,1,2,3,4 \bmod 5$ έχουμε $x^2 \equiv 0^2, 1^2, 2^2, 3^2, 4^2 \bmod 5$. Επειδή $3^2 \equiv 4 \bmod 5$ και $4^2 \equiv 1 \bmod 5$, παίρνουμε $x^2 \equiv 0,1,4 \bmod 5$. Δηλαδή σε κάθε περίπτωση, $x^2 \not\equiv 3 \bmod 5$, άτοπο.

19.

Υπόδειξη: Έστω $x = a/c$, $y = b/c$ με $a, b, c \in \mathbb{Z}, c \neq 0$. Μπορούμε να υποθέσουμε ότι δεν υπάρχει ακέραιος $d > 1$ τέτοιος ώστε $d \mid a, d \mid b, d \mid c$ (γιατί αλλιώς απλοποιούμε τα κλάσματα). Αν $x^2 + y^2 = 3$, τότε $a^2 + b^2 = 3c^2$. Εργαζόμενοι modulo 3, δείξτε ότι η τελευταία σχέση οδηγεί σε άτοπο.

20. Υπόδειξη: Αποδείξτε τα εξής:

a. Για κάθε $x \in \mathbb{Z}$, $x^2 \equiv 0,1,4 \bmod 8$.

b. Για κάθε $m \in \mathbb{N}$, $3^m \equiv 1,3 \bmod 8$.

Τώρα αν $3^m + 3^n + 1 = x^2$, όπου $m, n, x \in \mathbb{N}$, τα a. και b. οδηγούν σε άτοπο.

21. Απαντήσεις

a. Λ.
b. Λ.
c. Σ.
d. Σ.
e. Λ.
f. Σ.

Ασκήσεις2
Ακέραιοι modulo n, Θεώρημα του Euler

1. Εξετάστε αν το $[148]$ είναι αντιστρέψιμο στο $\mathbb{Z}_{303}$ και υπολογίστε το αντίστροφό του αν υπάρχει.

2. Να βρεθεί ένα στοιχείο $[a] \in U(\mathbb{Z}_5)$, έτσι ώστε κάθε στοιχείο του $U(\mathbb{Z}_5)$ να είναι της μορφής $[a]^n$, $n \in \mathbb{N}$. Αληθεύει ότι υπάρχει $[a] \in U(\mathbb{Z}_8)$, έτσι ώστε κάθε στοιχείο του $U(\mathbb{Z}_8)$ να είναι της μορφής $[a]^n$ όπου $n \in \mathbb{N}$;

3. Δείξτε ότι σε κάθε ημερολογιακό έτος (δίσεκτο ή μη) υπάρχει τουλάχιστον μία 'Τρίτη και 13'.

4. Υπολογίστε το άθροισμα A_n των στοιχείων του $\mathbb{Z}_n$, για $n = 3,4,5,6$. Δείξτε ότι $A_n = [0]$ αν n περιττός. Ποιο είναι το A_n αν n άρτιος και μη μηδενικός;

5. Εξετάστε ποιες από τις ακόλουθες προτάσεις αληθεύουν.

a. Υπάρχει $[a] \in \mathbb{Z}_{30}, [a] \neq [0]$, τέτοιο ώστε $[a]^2 = [0]$.

b. Υπάρχει $[a] \in \mathbb{Z}_{60}, [a] \neq [0]$, τέτοιο ώστε $[a]^2 = [0]$.

6. Ένα στοιχείο $[a] \in \mathbb{Z}_n$ λέγεται *μηδενοδύναμο* αν υπάρχει θετικός ακέραιος k με $[a]^k = [0]$.

a. Βρείτε τα μηδενοδύναμα στοιχεία του $\mathbb{Z}_{12}$.

b. Έστω $n = p_1^{n_1} \ldots p_s^{n_s}$, όπου p_i διάφοροι ανά δύο πρώτοι. Δείξτε ότι το $[a] \in \mathbb{Z}_n$ είναι μηδενοδύναμο αν και μόνο αν $p_1 \ldots p_s \mid a$.

c. Δείξτε ότι αν το $[a] \in \mathbb{Z}_n$ είναι μηδενοδύναμο, τότε το $[1-a]$ είναι αντιστρέψιμο.

d. Έστω $n > 1$ ακέραιος με την εξής ιδιότητα. Κάθε μη αντιστρέψιμο στοιχείο του $\mathbb{Z}_n$ είναι μηδενοδύναμο. Δείξτε ότι n είναι δύναμη πρώτου.

7. Έστω $a,b,m,n \in \mathbb{Z}$ με $m \mid n$. Έστω ότι το $[ab]_n \in \mathbb{Z}_n$ είναι αντιστρέψιμο. Δείξτε ότι το $[a]_m \in \mathbb{Z}_m$ είναι αντιστρέψιμο.

8. Βρείτε

a. το υπόλοιπο της διαίρεσης του 222^{555} με το 7,

b. τα τελευταία δύο ψηφία του 7^{100} στο δεκαδικό σύστημα.

9. Δείξτε ότι αν ο ακέραιος $n > 1$ δεν είναι πολλαπλάσιο του 5, τότε ο $n^4 + 4^n$ δεν είναι πρώτος.

10. Έστω n ο αριθμός μητρώου σας. Βρείτε το τελευταίο ψηφίο του $3^n + 7^n$ στο δεκαδικό σύστημα.

11. Δείξτε ότι για κάθε $n \in \mathbb{N}$,

a. $42 \mid n^7 - n$

b. $n^{49} \equiv n \bmod 1547$. Σημείωση: $1547 = 7 \cdot 13 \cdot 17$.

12. Δείξτε ότι για κάθε $n \in \mathbb{N}$, $(n+1)^9 + 4n^5 \equiv 1 \bmod 5$.

13. Έστω $n \in \mathbb{N}$. Δείξτε ότι $n^{12} + 12^n \equiv 5 \bmod 11 \Leftrightarrow n \equiv 2 \bmod 11$ ή $n \equiv 9 \bmod 11$.

14.

a. Έστω $n \in \mathbb{N}$. Δείξτε ότι $7^n \equiv 1 \bmod 20 \Leftrightarrow n \equiv 0 \bmod 4$.

b. Να βρεθούν όλοι οι $n \in \mathbb{N}$ τέτοιοι ώστε $9^n \equiv 1 \bmod 14$.

15. Έστω p πρώτος με $p \equiv 3 \bmod 4$. Δείξτε ότι δεν υπάρχει $a \in \mathbb{Z}$ με $a^2 \equiv -1 \bmod p$.

16. Έστω $a \in \mathbb{Z}$ με $\mu\kappa\delta(a,72) = 1$. Δείξτε ότι $a^{12} \equiv 1 \bmod 72$.

17. Δείξτε τα εξής.

a. Αν το $n \in \mathbb{Z}_{>0}$ είναι πολλαπλάσιο του 30, τότε το $\varphi(n)$ είναι πολλαπλάσιο του 8.

b. Έστω $n \in \mathbb{Z}_{>0}$ περιττός. Το $\varphi(n)$ είναι δύναμη του 2 αν και μόνο αν το n είναι γινόμενο διάφορων ανά δύο πρώτων της μορφής $2^{2^k} + 1$.

18. Έστω $m,n,k \in \mathbb{Z}_{>0}$. Δείξτε τα εξής.

a. $\varphi(mn) = \dfrac{d}{\varphi(d)}\varphi(m)\varphi(n)$, όπου $d = \mu\kappa\delta(m,n)$.

b. Αν $m \mid n$, τότε $\varphi(mn) = m\varphi(n)$.

c. $\varphi(n^k) = n^{k-1}\varphi(n)$.

19. Αν m,n είναι σχετικά πρώτοι θετικοί ακέραιοι, τότε $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \bmod(mn)$.

20. * Έστω $n \in \mathbb{Z}_{>0}$ με $n > 1$. Τότε $a^n \equiv a^{n-\varphi(n)} \bmod n$ για κάθε $a \in \mathbb{Z}_{>0}$.

21. Ο $2013^{2014} + 2014^{2013}$ δεν είναι τετράγωνο ακεραίου.

22. Έστω $p \neq 2,5$ πρώτος. Δείξτε ότι ο p διαιρεί άπειρο το πλήθος από τους $11, 111, 1111, \ldots$ (συνήθης δεκαδική γραφή).

23. Έστω $n \in \mathbb{Z}_{>0}$. Αν $d \in \mathbb{Z}_{>0}$ με $d \mid n$, θέτουμε $A_d = \left\{ m \in \{1,2,\ldots,n\} \,\middle|\, \mu\kappa\delta(m,n) = d \right\}$. Δείξτε τα εξής.

a. Το σύνολο A_d περιέχει ακριβώς $\varphi(n/d)$ στοιχεία.

b. Έχουμε την ξένη ένωση $\{1,2,\ldots,n\} = \bigcup_{d \mid n} A_d$.

c. $n = \sum_{d \mid n} \varphi(d)$.

24. Εξετάστε ποιες από τις ακόλουθες προτάσεις αληθεύουν.

a. Για κάθε $n \in \mathbb{N}$, το $[n+1] \in \mathbb{Z}_{2n+3}$ είναι αντιστρέψιμο.

b. Αν $a,b \in \mathbb{Z}_n$ και $ab \in U(\mathbb{Z}_n)$, τότε $a,b \in U(\mathbb{Z}_n)$.

c. Αν $a,n \in \mathbb{Z}$ με $n > 0$, τότε $a^n \equiv a \bmod n$.

d. Το αντίστροφο του $[7] \in \mathbb{Z}_{31}$ είναι το $[7^{29}]$.

Υποδείξεις/Απαντήσεις
Ασκήσεις2

1.
Εφαρμόζοντας τον Ευκλείδειο αλγόριθμο έχουμε

$$303 = 2\cdot 148 + 7$$
$$148 = 21\cdot 7 + 1$$
$$7 = 7\cdot 1 + 0.$$

Άρα μκδ(148,303)=1 και το $[148]\in\mathbb{Z}_{301}$ είναι αντιστρέψιμο σύμφωνα με την Πρόταση 1.4.5. Για τον υπολογισμό του αντίστροφου του [148] έχουμε

$$7 = 303 - 2\cdot 148$$
$$1 = 148 - 21\cdot 7$$

οπότε

$$1 = 148 - 21\cdot 7 =$$
$$= 148 - 21\cdot(303 - 2\cdot 148) =$$
$$= 43\cdot 148 + (-21)\cdot 303.$$

Δηλαδή

$$1 = 143\cdot 148 + (-21)\cdot 303.$$

Άρα το αντίστροφο του $[148]\in\mathbb{Z}_{303}$ είναι το $[143]\in\mathbb{Z}_{303}$.

2.
Απάντηση: Το στοιχείο $[2]\in\mathbb{Z}_5$ έχει τη ζητούμενη ιδιότητα αφού

$$[2]^1 = [2],$$
$$[2]^2 = [4],$$
$$[2]^3 = [8] = [3],$$
$$[2]^4 = [16] = [1].$$

Δηλαδή $U(\mathbb{Z}_5) = \left\{[2],[2]^2,[2]^3,[2]^4\right\}$.

Για το $\mathbb{Z}_8$ δεν αληθεύει, καθώς έχουμε $U(\mathbb{Z}_8) = \{[1],[3],[5],[7]\}$ και με πράξεις επαληθεύεται ότι για $[a]\in U(\mathbb{Z}_8)$ ισχύει $\left\{[a]^n \,\middle|\, n = 1,2,...\right\} = \begin{cases}\{[1]\}, & \text{αν } [a]=[1]\\ \{[1],[a]\}, & \text{αν } [a]\neq[1].\end{cases}$

3.
Υπόδειξη: Ας θεωρήσουμε μια 1-1 και επί αντιστοιχία μεταξύ των ημερών της εβδομάδας και των στοιχείων του $\mathbb{Z}_7$, πχ την ακόλουθη: Κυριακή $\leftrightarrow [1]$, Δευτέρα $\leftrightarrow [2]$ κλπ. Αν $[a_i]\in\mathbb{Z}_7$ αντιστοιχεί στην ημέρα της εβδομάδας με ημερομηνία 13 του i μήνα ($i = 1,2,...,12$), αρκεί να δείξουμε ότι $\{[a_i] | i = 1,2,...,12\} = \mathbb{Z}_7$.

Για να υπολογίσουμε τα $[a_i], i = 2,...,12,$ συναρτήσει του $[a_1]$ παρατηρούμε ότι, επειδή ο Ιανουάριος έχει 31 ημέρες και $31 \equiv 3 \bmod 7$, έχουμε $[a_2] = [a_1 + 31] = [a_1 + 3]$. Αν ο Φεβρουάριος έχει 28 ημέρες, τότε $[a_3] = [a_2 + 28] = [a_2] = [a_1 + 3]$. Όμοια $[a_4] = [a_3 + 31] = [a_3 + 3] = [a_1 + 6]$ κοκ. Βρίσκουμε τελικά

$$\{[a_i] | i = 1,2,...,12\} = \{[a_1],[a_1+1],[a_1+2],..,[a_1+6]\} = \mathbb{Z}_7.$$

Ο υπολογισμός για δίσεκτα έτη είναι παρόμοιος.

4. Απάντηση: Αν n άρτιος και μη μηδενικός, τότε $A_n = [n/2]$.

5.
a. Λάθος. Έχουμε

$[a]^2=[0]\Rightarrow[a^2]=[0]\Rightarrow 30\big|a^2\Rightarrow 2\big|a^2\ \ και\ \ 3\big|a^2\ \ και\ \ 5\big|a^2\overset{1}{\Rightarrow}$

$2\big|a\ \ και\ \ 3\big|a\ \ και\ \ 5\big|a\overset{2}{\Rightarrow}30\big|a\Rightarrow[a]=[0].$

1. Χρησιμοποιήσαμε ότι οι $2,3,5$ είναι πρώτοι (βλ. Λήμμα 1.2.5).
2. Χρησιμοποιήσαμε ότι οι $2,3,5$ είναι ανά δύο σχετικά πρώτοι (βλ Παράδειγμα 1.2.8 2 ή άσκηση 1.2b). Φυσικά θα μπορούσαμε να πούμε ότι το εκπ των $2,3,5$ διαιρεί το a.

b. Απάντηση: Σωστό. Το $[a]=[30]$ έχει τις ζητούμενες ιδιότητες. (Πως το βρήκαμε; Υπάρχει άλλο τέτοιο στοιχείο;)

6.

b. Έστω ότι $[a]^k=[0]$ για κάποιο θετικό ακέραιο k. Τότε $[a^k]=[0]\Rightarrow n\big|a^k\Rightarrow p_i\big|a^k$ για κάθε i, οπότε από το Λήμμα 1.2.5 έχουμε $p_i\big|a$ για κάθε i. Από την άσκηση 1.2b έπεται ότι $p_1...p_s\big|a$.

Αντίστροφα, έστω $p_1...p_s\big|a$. Για $k=\max\{n_1,...,n_s\}$ ισχύει $n\big|p_1^{\,k}...p_s^{\,k}$. Επειδή $p_1^{\,k}...p_s^{\,k}\big|a^k$, παίρνουμε $n\big|a^k$, δηλαδή $[a]^k=[0]$.

c. $1^{ος}$ τρόπος. Αν $[a]^k=[0]$, τότε

$$\begin{aligned}&\left([1]-[a]\right)\left([1]+[a]+[a]^2+...+[a]^{k-1}\right)=\\&=[1]+[a]+[a]^2+...+[a]^{k-1}-[a]-[a]^2-...-[a]^k=\\&=[1]-[a]^k=[1],\end{aligned}$$

και συνεπώς το $[1-a]=[1]-[a]$ είναι αντιστρέψιμο.

$2^{ος}$ τρόπος. Έστω ότι το $[a]$ είναι μηδενοδύναμο. Από το ερώτημα a. έχουμε $p_i\big|a$ για κάθε i. Από αυτό έπεται ότι $\text{μκδ}(1-a,n)=1$, γιατί διαφορετικά θα υπήρχε πρώτος p με $p\big|1-a$ και $p\big|n$, δηλαδή για κάποιο $j=1,...,s$ θα είχαμε $p_j\big|1-a$, οπότε $p_j\big|1$. Συνεπώς το $[1-a]$ είναι αντιστρέψιμο.

7.

Επειδή το $[ab]_n\in\mathbb{Z}_n$ είναι αντιστρέψιμο, έχουμε $\mu\kappa\delta(ab,n)=1$. Έστω $d\in\mathbb{Z}_{>0}$ με $d\big|a$ και $d\big|m$. Τότε $d\big|ab$ και $d\big|n$ (αφού $m\big|n$). Συνεπώς $d\big|\mu\kappa\delta(ab,n)$, οπότε $d=1$. Άρα $\mu\kappa\delta(a,m)=1$ και επομενως το $[a]_m\in\mathbb{Z}_m$ είναι αντιστρέψιμο.

$2^{ος}$ τρόπος. Αν υπάρχει $c\in\mathbb{Z}$ με $[ab]_n[c]_n=[1]_n$, τότε $[abc]_n=[1]_n$, δηλαδή $n\big|abc-1$. Επειδή $m\big|n$, έχουμε $m\big|abc-1$ από το οποίο έπεται ότι $[ab]_m[c]_m=[1]_m$ και άρα το $[ab]_m\in\mathbb{Z}_m$ είναι αντιστρέψιμο.

8.

a. Βλ. Παράδειγμα 1.4.9 1.

b. Λύση: Ζητάμε το υπόλοιπο της διαίρεσης του 7^{100} με το 100. Σύμφωνα με την Πρόταση 1.6.1 έχουμε $\varphi(100)=\varphi(2^2\cdot5^2)=\varphi(2^2)\varphi(5^2)=(2^2-2)(5^2-5)=40$. Επίσης $\mu\kappa\delta(7,100)=1$ αφού το 7 είναι πρώτος που δεν διαιρεί το 100. Άρα από το Θεώρημα του Euler,

$$7^{40}\equiv1\bmod100.$$

Επειδή $100=2\cdot40+20$, παίρνουμε $7^{100}=(7^{40})^2\,7^{20}$ και άρα

$$7^{100}\equiv7^{20}\bmod100.$$

Έχουμε $7^{20}=(7^4)^5=(2401)^5\equiv1^5\equiv1\bmod100$. Άρα $7^{100}\equiv1\bmod100$, δηλαδή το υπόλοιπο της διαίρεσης του 7^{100} με το 100 είναι 1 και επομένως τα δύο τελευταία ψηφία του 7^{100} στο δεκαδικό σύστημα είναι 01.

9.

Υπόδειξη: Για περιττό n εφαρμόστε το μικρό θεώρημα του Fermat για $p=5$.

10.

Υπόδειξη: Ζητάμε το υπόλοιπο της διαίρεσης του $3^n + 7^n$ με το 10.

$1^{ος}$ τρόπος. Έχουμε $\varphi(10) = 4$. Εφαρμόστε το Θεώρημα του Euler.

$2^{ος}$ τρόπος. Παρατηρούμε ότι $3^n + 7^n \equiv 3^n + (-3)^n \bmod 10$. Αν ο n είναι περιττός, τότε $3^n + (-3)^n \equiv 0 \bmod 10$ και το ζητούμενο υπόλοιπο είναι 0. Αν ο n είναι άρτιος, $n = 2m$, τότε $3^n + (-3)^n \equiv 9^m + 9^m \bmod 10$, οπότε $3^n + (-3)^n \equiv (-1)^m + (-1)^m \bmod 10$ και επομένως το ζητούμενο υπόλοιπο είναι 8 ή 2 αν ο m είναι περιττός ή άρτιος αντίστοιχα.

11.

a. Βλ. Παράδειγμα 1.4.9 3.

b. Υπόδειξη: Όπως το προηγούμενο υποερώτημα.

12.

Από το μικρό θεώρημα του Fermat για $p = 5$ έχουμε

$$n^5 \equiv n \bmod 5,$$

$$(n+1)^5 \equiv n+1 \bmod 5$$

για κάθε $n \in \mathbb{N}$. Παρατηρούμε ότι $(n+1)^9 = (n+1)^5 (n+1)^4 \equiv (n+1)(n+1)^4 \equiv n+1 \bmod 5$ και άρα

$$(n+1)^9 + 4n^5 \equiv n+1+4n \equiv 1+5n \equiv 1 \bmod 5.$$

13.

Επειδή $12 \equiv 1 \bmod 11$ έχουμε $12^n \equiv 1 \bmod 11$ για κάθε $n \in \mathbb{N}$. Επίσης, από το μικρό θεώρημα του Fermat, $n^{11} \equiv n \bmod 11$ για κάθε $n \in \mathbb{N}$ και άρα $n^{12} = n^{11} n \equiv nn \equiv n^2 \bmod 11$. Άρα

$$n^{12} + 12^n \equiv 5 \bmod 11 \Leftrightarrow n^2 + 1 \equiv 5 \bmod 11 \Leftrightarrow$$

$$n^2 - 4 \equiv 0 \bmod 11 \overset{1}{\Leftrightarrow} 11 \mid n^2 - 4 \Leftrightarrow$$

$$11 \mid (n-2)(n+2) \Leftrightarrow 11 \mid n-2 \quad \text{ή} \quad 11 \mid n+2 \Leftrightarrow$$

$$n \equiv 2 \bmod 11 \quad \text{ή} \quad n \equiv -2 \bmod 11 \Leftrightarrow$$

$$n \equiv 2 \bmod 11 \quad \text{ή} \quad n \equiv 9 \bmod 11.$$

1. Εναλλακτικά (πχ σε περίπτωση που δεν είχαμε τη βολική παραγοντοποίηση του $n^2 - 4$), θα μπορούσαμε στο σημείο αυτό να δοκιμάσουμε ποιες από τις περιπτώσεις $n \equiv 0,1,...,10 \bmod 11$ ικανοποιούν τη $n^2 - 4 \equiv 0 \bmod 11$.

14.

a. Από την Ευκλείδεια διαίρεση υπάρχουν $m, r \in \mathbb{N}$ με $n = 4m + r$, $0 \le r < 4$. Τότε $7^n = (7^4)^m 7^r$. Έχουμε $7^4 = 2401$ και άρα $7^4 \equiv 1 \bmod 20$. Τότε $7^n \equiv 7^r \bmod 20$. Συνεπώς

$$7^n \equiv 1 \bmod 20 \Leftrightarrow 7^r \equiv 1 \bmod 20.$$

Για $r = 0$, η τελευταία ισοτιμία αληθεύει, ενώ εύκολα επαληθεύεται ότι για $r = 1,2,3$ δεν αληθεύει. Συνεπώς $7^n \equiv 1 \bmod 20 \Leftrightarrow r = 0 \Leftrightarrow n \equiv 0 \bmod 4$.

Σημείωση: Από το Θεώρημα του Euler έχουμε $7^8 \equiv 1 \bmod 20$ ενώ είδαμε πριν ότι $7^4 \equiv 1 \bmod 20$. Έστω $a, m \in \mathbb{Z}, m > 0$, με $\mu\kappa\delta(a,m) = 1$. Η άσκηση αυτή δίνει ένα παράδειγμα όπου ο εκθέτης $\varphi(m)$ στο Θεώρημα του Euler, $a^{\varphi(m)} \equiv 1 \bmod m$, δεν είναι γενικά ο *μικρότερος* θετικός ακέραιος k τέτοιος ώστε $a^k \equiv 1 \bmod m$. Μπορεί να αποδειχθεί ότι ο μικρότερος τέτοιος θετικός ακέραιος k είναι διαιρέτης του $\varphi(m)$, βλ. Παράδειγμα 1.6.3 2. Μάλιστα το επιχείρημα του παραδείγματος δείχνει ότι κάθε άλλος θετικός ακέραιος n που ικανοποιεί $a^n \equiv 1 \bmod m$ είναι πολλαπλάσιο του k. Το θέμα αυτό θα το εξετάσουμε αργότερα στο εξάμηνο όταν μελετήσουμε τις ομάδες.

b. Απάντηση: $n \equiv 3 \bmod 6$.

15.

Υπόδειξη: Έστω $a^2 \equiv -1 \bmod p$. Αν $p \mid a$, τότε $p \mid -1$, άτοπο. Άρα το p δεν διαιρεί το a. Υψώστε τα μέλη της ισοτιμίας $a^2 \equiv -1 \bmod p$ σε κατάλληλη δύναμη και εφαρμόστε το μικρό θεώρημα του Fermat για να καταλήξετε σε άτοπο.

16. Βλ. Παράδειγμα 1.6.3 1.

17.

a. Αφού $30 \mid n$, έχουμε $n = 2^{n_1}3^{n_2}5^{n_3}m$, όπου $n_i \in \mathbb{Z}_{>0}$ και ο $m \in \mathbb{Z}_{>0}$ είναι σχετικά πρώτος με καθέναν από τους $2,3,5$. Άρα $\varphi(n) = \varphi(2^{n_1}3^{n_2}5^{n_3})\varphi(m) = (2^{n_1} - 2^{n_1-1})(3^{n_2} - 3^{n_2-1})(5^{n_3} - 5^{n_3-1})\varphi(m)$ (Πρόταση 1.6.1). Έχουμε $3^{n_2} - 3^{n_2-1} = 3^{n_2-1}(3-1)$ που είναι πολλαπλάσιο του 2 και $5^{n_3} - 5^{n_3-1} = 5^{n_3-1}(5-1)$ που είναι πολλαπλάσιο του 4. Άρα το $\varphi(n)$ είναι πολλαπλάσιο του 8.

b. Έστω $n = p_1^{m_1}...p_t^{m_t}$ όπου p_i διακεκριμένοι περιττοί πρώτοι. Τότε

$$\varphi(n) = \varphi(p_1^{m_1})...\varphi(p_t^{m_t}) = p_1^{m_1-1}(p_1-1)...p_t^{m_t-1}(p_t-1).$$

Το δεξί μέλος είναι δύναμη του 2 αν και μόνο αν για κάθε i

$$m_i = 1 \quad \text{και} \quad p_i = 2^{n_i} + 1.$$

Όμως αν ο $p_i = 2^{n_i} + 1$ είναι πρώτος, τότε το n_i είναι δύναμη του 2, γιατί αν $n_i = qr$ με $q > 1$ περιττό, τότε $p_i = 2^{n_i} + 1 = (2^r)^q + 1 = (2^r + 1)((2^r)^{q-1} - (2^r)^{q-2} + ... - 2^r + 1)$, πράγμα που αντιφάσκει ότι ο p_i είναι πρώτος.

18.

a. Από την Πρόταση 1.6.1 3, το ζητούμενο ισοδυναμεί με την ισότητα

$$\prod_{p \mid mn}(1-1/p) = \frac{1}{\prod_{p \mid d}(1-1/p)}\prod_{p \mid m}(1-1/p)\prod_{p \mid n}(1-1/p),$$

όπου σε κάθε γινόμενο το p διατρέχει τους πρώτους που έχουν την αναγραφόμενη ιδιότητα. Επειδή $d \mid m$ το ζητούμενο ισοδυναμεί με την ισότητα

$$\prod_{p \mid mn}(1-1/p) = \prod_{\substack{p \mid m \\ p \nmid d}}(1-1/p)\prod_{p \mid n}(1-1/p), \qquad (1)$$

όπου $p \nmid d$ σημαίνει p δεν διαιρεί το d. Έστω P_k το σύνολο των πρώτων διαιρετών ενός ακεραίου k. Με το Λήμμα του Ευκλείδη παίρνουμε $P_{mn} = P_m \cup P_n$ και από $d = \text{μκδ}(m,n)$ έπεται $P_d = P_m \cap P_n$. Συνεπώς έχουμε την ξένη ένωση $P_{mn} = (P_m - P_d) \cup P_n$. Από αυτό έπεται η (1).

b. Έπεται άμεσα από το a.

c. Έπεται άμεσα με επαγωγή στο k.

19.

Έχουμε $\mu\kappa\delta(m,n) = 1$. Εφαρμόζοντας δυο φορές το Θεώρημα του Euler παίρνουμε $m \mid n^{\varphi(m)} - 1$ και $n \mid m^{\varphi(n)} - 1$. Από την πρώτη σχέση έχουμε $m \mid m^{\varphi(n)} + n^{\varphi(m)} - 1$ και από τη δεύτερη $n \mid m^{\varphi(n)} + n^{\varphi(m)} - 1$. Από τις δύο τελευταίες σχέσεις και $\mu\kappa\delta(m,n) = 1$ έπεται ότι $mn \mid m^{\varphi(n)} + n^{\varphi(m)} - 1$, δηλαδή $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \bmod(mn)$.

20.

Υπόδειξη: Μπορούμε να υποθέσουμε ότι $n > 1$. Έστω $n = p_1^{k_1}...p_r^{k_r}$ η ανάλυση του n σε γινόμενο πρώτων. Δείξτε ότι για κάθε i, $p_i^{k_i} \mid a^{n-\varphi(n)}\left(a^{\varphi(n)} - 1\right)$ ως εξής:

- αν ο p_i δεν διαιρεί το a, δείξτε ότι $p_i^{k_i} \left| a^{\varphi(n)} - 1 \right.$ και
- αν $p_i \left| a \right.$, δείξτε ότι $p_i^{k_i} \left| a^{n-\varphi(n)} \right.$.

Από την άσκηση 1.2b έπεται το ζητούμενο.

21.

Υπόδειξη: Δείξτε ότι $2013^{2014} + 2014^{2013} \equiv 3 \bmod 10$ και παρατηρήστε ότι το 3 δεν είναι τετράγωνο modulo 10.

22.

Υπόδειξη: Έστω $a_n = \underbrace{11...1}_{n}$. Καθένας από τους $a_{3m}, m = 1,2,...$ διαιρείται με το 3 (γιατί;).

Έστω $p \neq 3$. Παρατηρήστε ότι $10^n - 1 = 9a_n$ και χρησιμοποιήστε το μικρό θεώρημα του Fermat για να δείξετε ότι $p \left| a_n \right.$ αν $p - 1 \left| n \right.$.

23.

a. Υπόδειξη: Έστω $d \in \mathbb{Z}_{>0}$ με $d \left| n \right.$ και έστω $m \in \{1, 2, ..., n\}$. Δείξτε ότι $m \in A_d$ αν και μόνο αν $d \left| m \right.$ και $\mu\kappa\delta(m/d, n/d) = 1$. Από αυτό έπεται ότι το πλήθος των στοιχείων του A_d είναι ίσο με $\varphi(n/d)$.

c. Έχουμε $\sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d)$, γιατί όταν το d διατρέχει τους θετικούς διαιρέτες του n, το ίδιο συμβαίνει με το n/d. Το ζητούμενο έπεται από την προηγούμενη παρατήρηση και τα υποερωτήματα a. και b.

23. Απαντήσεις:

a. Σ.
b. Σ.
c. Λ.
d. Σ.

Ασκήσεις3
Δακτύλιοι: ορισμοί, παραδείγματα, βασικές ιδιότητες

1. Δείξτε τα εξής.
   a. Η αντιστοιχία που ορίζεται από $\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2, ([a],[b]) \mapsto [c],$ όπου $c = \max\{a,b\}$, δεν είναι απεικόνιση.
   b. Το σύνολο $\mathbb{Z}$ είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο ως προς τις πράξεις $\oplus : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ και $\bullet : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ που ορίζονται από $a \oplus b = a + b - 1$ και $a \bullet b = ab - (a+b) + 2$. Το μηδενικό στοιχείο είναι το 1 και το μοναδιαίο στοιχείο είναι το 2.
   c. Το σύνολο $\mathbb{Z}$ δεν είναι δακτύλιος ως προς τις πράξεις $+ : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ και $\bullet : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ όπου η $+$ είναι η συνήθης πρόσθεση και η $\bullet$ ορίζεται από $a \bullet b = a - b$.

2. Έστω $R = \{a,b,c,d\}$ ένα σύνολο με 4 στοιχεία. Εξετάστε αν το R είναι δακτύλιος ως προς δύο πράξεις τέτοιες ώστε ο πίνακας της πρόσθεσης είναι ο ακόλουθος.

$+$	a	b	c	d
a	b	c	d	a
b	c	d	a	b
c	d	a	b	c
d	a	c	b	d

3. Εξετάστε αν ο S είναι υποδακτύλιος του R. Στις περιπτώσεις που ο S είναι υποδακτύλιος του R, εξετάστε αν είναι μεταθετικός, αν έχει μοναδιαίο στοιχείο, αν είναι περιοχή, και αν είναι σώμα.
   a. $S = 2\mathbb{Z}$, $R = \mathbb{Z}$.
   b. $S = \mathbb{Z}[\sqrt{2}] = \left\{a + b\sqrt{2} \in \mathbb{R} \middle| a,b \in \mathbb{Z}\right\}$, $R = \mathbb{R}$.
   c. $S = \left\{a + b\sqrt[3]{2} \in \mathbb{R} \middle| a,b \in \mathbb{Z}\right\}$, $R = \mathbb{R}$.
   d. $S = \left\{a + b\sqrt{2} \in \mathbb{R} \middle| a,b \in \mathbb{Z}, a \equiv 0 \bmod 3\right\}$, $R = \mathbb{Z}[\sqrt{2}]$.
   e. $S = \{[0],[4],[8]\}$, $R = \mathbb{Z}_{12}$.
   f. $S = \left\{\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} \in M_2(\mathbb{R})\right\}$, $R = M_2(\mathbb{R})$.
   g. $S = \left\{\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \in M_2(\mathbb{R})\right\}$, $R = M_2(\mathbb{R})$.
   h. $S = \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a,b,c \in \mathbb{R}, a+b+c = 0\right\}$, $R = M_2(\mathbb{R})$

4. Δείξτε ότι το σύνολο των αντιστρέψιμων στοιχείων του δακτυλίου
   a. $\mathbb{Z}[i] = \left\{a + bi \in \mathbb{C} \middle| a,b \in \mathbb{Z}\right\}$ είναι το $\{1,-1,i,-i\}$,
   b. $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \in \mathbb{R} \middle| a,b \in \mathbb{Q}\right\}$ είναι το $\mathbb{Q}[\sqrt{2}] - \{0\}$.

5. Δείξτε ότι ο πίνακας $A \in M_n(\mathbb{Z})$ είναι αντιστρέψιμο στοιχείο του δακτυλίου $M_n(\mathbb{Z})$ αν και μόνο αν $\det A = \pm 1$.

6. Έστω R δακτύλιος.
   a. Δείξτε ότι αν ο R έχει μοναδιαίο στοιχείο και $u, v \in U(R)$, τότε $uv \in U(R)$.
   b. Έστω ότι υπάρχει μοναδικό στοιχείο $e \in R$ με $er = r$ για κάθε $r \in R$. Δείξτε ότι $re = r$ για κάθε $r \in R$.

7. Δείξτε ότι το σύνολο $U(\mathbb{Z}[\sqrt{2}])$ είναι άπειρο.

8. Έστω $n \in \mathbb{Z}_{>0}$ και $T_2(\mathbb{Z}_n) = \left\{A \in M_2(\mathbb{Z}_n) \middle| A = \begin{pmatrix} [a] & [b] \\ [0] & [c] \end{pmatrix}\right\}$.

a. Δείξτε ότι το $T_2(\mathbb{Z}_n)$ είναι υποδακτύλιος του $M_2(\mathbb{Z}_n)$.

b. Αληθεύει ότι ο $T_2(\mathbb{Z}_n)$ είναι μεταθετικός;

c. Δείξτε ότι το σύνολο $U(T_2(\mathbb{Z}_n))$ των αντιστρέψιμων στοιχείων του $T_2(\mathbb{Z}_n)$ έχει $n\varphi(n)^2$ στοιχεία.

9. Δείξτε ότι το $R=\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\in M_2(\mathbb{R})\right\}$ είναι υποδακτύλιος του $M_2(\mathbb{R})$. Επίσης, το R είναι σώμα.

10. Πόσα στοιχεία του δακτυλίου $M_2(\mathbb{Z}_2)$ είναι αντιστρέψιμα; Αν p είναι ένας πρώτος αριθμός, πόσα στοιχεία του δακτυλίου $M_2(\mathbb{Z}_p)$ είναι αντιστρέψιμα;

11. Έστω $R=\left\{\frac{m}{2^a3^b}\in\mathbb{Q}\middle| m\in\mathbb{Z},\ a,b\in\mathbb{N}\right\}$.

a. Δείξτε ότι ο R είναι υποδακτύλιος του $\mathbb{Q}$.

b. Δείξτε ότι ο R περιέχεται σε κάθε υποδακτύλιο του $\mathbb{Q}$ που περιέχει τα $\frac{1}{2},\frac{1}{3}$.

c. Αληθεύει ότι το R είναι σώμα;

12. Έστω R υποδακτύλιος του $\mathbb{C}$ με $\mathbb{Q}\subseteq R$.

a. Δείξτε ότι το R είναι $\mathbb{Q}-$διανυσματικός χώρος με πρόσθεση $R\times R\to R$ τη πρόσθεση στο R, και εξωτερικό πολλαπλασιασμό $\mathbb{Q}\times R\to R$ τον περιορισμό του πολλαπλασιασμού του R.

b. Δείξτε ότι αν $\dim_{\mathbb{Q}} R<\infty$, τότε το R είναι σώμα.

13. Έστω $a\in\mathbb{C}$ με $a^3-a-1=0$. Θέτουμε $R=\{c_0+c_1a+c_2a^2\,|\,c_i\in\mathbb{Q}\}$.

a. Δείξτε ότι το R είναι υποδακτύλιος του $\mathbb{C}$.

b. Δείξτε ότι το R είναι σώμα.

c. Δείξτε ότι $2+a^2\neq 0$ και υπολογίστε $c_i\in\mathbb{Q}$ με $(2+a^2)^{-1}=c_0+c_1a+c_2a^2$.

14. Έστω R,S δύο δακτύλιοι.

a. Δείξτε ότι ο $R\times S$ είναι μεταθετικός αν και μόνο αν οι R,S είναι μεταθετικοί.

b. Δείξτε ότι ο $R\times S$ έχει μοναδιαίο στοιχείο αν και μόνο αν οι R,S έχουν μοναδιαία στοιχεία.

c. Έστω ότι οι R,S έχουν μοναδιαία στοιχεία. Δείξτε ότι $U(R\times S)=U(R)\times U(S)$.

d. Αληθεύει ότι αν οι R,S είναι περιοχές, τότε και ο $R\times S$ είναι περιοχή;

15. Δείξτε ότι κάθε υποδακτύλιος του $\mathbb{Z}$ είναι της μορφής $m\mathbb{Z}$, όπου $m\in\mathbb{N}$.

16.

a. Αν $R_i, i\in I,$ είναι υποδακτύλιοι του δακτυλίου R, τότε η τομή $\bigcap_{i\in I} R_i$ είναι υποδακτύλιος του R.

b. Να βρεθεί ένα $m\in\mathbb{N}$ τέτοιοι ώστε $m\mathbb{Z}=4\mathbb{Z}\cap 6\mathbb{Z}$.

c. Δείξτε ότι το σύνολο $2\mathbb{Z}\cup 3\mathbb{Z}$ δεν είναι υποδακτύλιος του $\mathbb{Z}$.

17. (*Διωνυμικό ανάπτυγμα*) Έστω R δακτύλιος και $a,b\in R$. Δείξτε ότι αν $ab=ba$, τότε για κάθε $n\in\mathbb{N}, n\geq 2$, έχουμε $(a+b)^n=a^n+\sum_{i=1}^{n-1}\binom{n}{i}a^{n-i}b^i+b^n$, όπου $\binom{n}{i}=\frac{n!}{i!(n-i)!}$, $k!=1\cdot 2\cdot\ldots\cdot k$ $(k\in\mathbb{Z}_{>0})$.

18. Έστω p πρώτος αριθμός και R μεταθετικός δακτύλιος τέτοιος ώστε $pr=0$ για κάθε $r\in R$. Δείξτε τα εξής.

a. $(a+b)^p=a^p+b^p$.

b. $(a+b)^{p^n}=a^{p^n}+b^{p^n}$ για κάθε $n\in\mathbb{N}$.

19.

a. Δείξτε ότι κάθε υπόσωμα του $\mathbb{C}$ περιέχει το $\mathbb{Q}$.

b. Δείξτε ότι τα σύνολα $\mathbb{Q}[\sqrt{2}]=\left\{a+b\sqrt{2}\in\mathbb{R}\middle| a,b\in\mathbb{Q}\right\}$ και $\mathbb{Q}[\sqrt{3}]=\left\{a+b\sqrt{3}\in\mathbb{R}\middle| a,b\in\mathbb{Q}\right\}$ είναι υποσώματα του $\mathbb{C}$.

c. Ποια είναι η τομή $\mathbb{Q}[\sqrt{2}]\cap\mathbb{Q}[\sqrt{3}]$;

20. Να βρεθούν οι υποδακτύλιοι του $M_n(\mathbb{R})$ που περιέχουν τους συμμετρικούς πίνακες.

21. Δείξτε ότι ο δακτύλιος R είναι μεταθετικός αν και μόνο αν $(a+b)^2 = a^2 + 2ab + b^2$ για κάθε $a,b \in R$.

22. Ένα στοιχείο r ενός δακτυλίου R λέγεται *ταυτοδύναμο* αν $r^2 = r$. Σε καθεμιά από τις ακόλουθες περιπτώσεις βρείτε όλα των ταυτοδύναμα στοιχεία του R.

a. $R = \mathbb{Z}_{10}$.

b. $R = \mathbb{Z}_{p^m}$, όπου p πρώτος και $m \in \mathbb{Z}_{>0}$.

c. $R =$ σώμα.

d. $R = M_2(\mathbb{R})$.

23. Ένα στοιχείο r ενός δακτυλίου R λέγεται *μηδενοδύναμο* αν $r^m = 0$ για κάποιο θετικό ακέραιο m.

a. Βρείτε όλα τα μηδενοδύναμα στοιχεία του $\mathbb{Z}_{30}$ και του $\mathbb{Z}_{60}$.

b. Συμπληρώστε την πρόταση: Έστω $n > 1$. Ο $\mathbb{Z}_n$ δεν έχει μη μηδενικό μηδενοδύναμο στοιχείο αν και μόνο αν ο n … .

24. Έστω R δακτύλιος.

a. Δείξτε ότι αν το $r \in R$ είναι μηδενοδύναμο (βλ. προηγούμενη άσκηση) και ο R έχει μοναδιαίο στοιχείο, τότε $1 - r \in U(R)$.

b. Δείξτε ότι αν τα $r, s \in R$ είναι μηδενοδύναμα και ο R μεταθετικός, τότε το rs είναι μηδενοδύναμο

c. Δείξτε ότι αν τα $r, s \in R$ είναι μηδενοδύναμα και ο R μεταθετικός, τότε το $r+s$ είναι μηδενοδύναμο. Συνεπώς το σύνολο των μηδενοδύναμων στοιχείων ενός μεταθετικού δακτυλίου R είναι υποδακτύλιος του R.

25. Έστω R υποδακτύλιος ενός σώματος και $a,b \in R$. Αν υπάρχουν σχετικά πρώτοι θετικοί ακέραιοι m,n τέτοιοι ώστε $a^m = b^m$ και $a^n = b^n$, τότε $a = b$.

26. Έστω R δακτύλιος. Αν $X \subseteq R$, θέτουμε $A(X) = \{ r \in R \,|\, rx = 0 \ \forall x \in X \}$.

a. Δείξτε ότι το $A(X)$ είναι υποδακτύλιος του R.

b. Για $R = M_2(\mathbb{R})$ και $X = \left\{ \begin{pmatrix} 2 & 3 \\ 0 & 0 \end{pmatrix} \right\}$ βρείτε τον $A(X)$ και εξετάστε αν είναι μεταθετκός και αν έχει μοναδιαίο στοιχείο.

27. Έστω $A \in M_2(\mathbb{Z})$ με $\det A = 0$. Θέτουμε $R = \{ mA \,|\, m \in \mathbb{Z} \}$.

a. Δείξτε ότι ο R είναι μεταθετικός υποδακτύλιος του $M_2(\mathbb{Z})$.

b. Δείξτε ότι ο R έχει μοναδιαίο στοιχείο αν και μόνο αν $A = 0$ ή $Tr(A) = \pm 1$. Στις περιπτώσεις αυτές βρείτε τα αντιστρέψιμα στοιχεία του R.

28. Αν R είναι δακτύλιος, έστω $C(R) = \{ a \in R \,|\, ar = ra \ \ \forall r \in R \}$. Το $C(R)$ ονομάζεται το *κέντρο* του δακτυλίου R.

a. Δείξετε ότι $C(R) = R \Leftrightarrow R$ μεταθετικός.

b. Δείξτε ότι το $C(R)$ είναι ένας υποδακτύλιος του R.

c. Δείξτε ότι $C\left(M_2(\mathbb{R})\right) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| a \in \mathbb{R} \right\}$.

d. Δείξτε ότι $C\left(M_n(\mathbb{R})\right) = \{ aI_n \,|\, a \in \mathbb{R} \}$, όπου I_n είναι ο ταυτοτικός $n \times n$ πίνακας.

e. Έστω R, S δυο δακτύλιοι. Εξετάστε αν $C(R \times S) = C(R) \times C(S)$.

29. * Έστω R δακτύλιος τέτοιος ώστε $r^2 + r \in C(R)$ για κάθε r (βλ. προηγούμενη άσκηση για τον ορισμό του $C(R)$). Δείξτε ότι ο R είναι μεταθετικός.

30. Έστω R πεπερασμένος δακτύλιος και $a \in R$ που δεν είναι μηδενοδιαιρέτης. Δείτε ότι ο R έχει μοναδιαίο στοιχείο και το a είναι αντιστρέψιμο.

31. Έστω R δακτύλιος με μοναδιαίο στοιχείο και $a,b \in R$. Δείξτε ότι αν το $1 - ab \in U(R)$, τότε $1 - ba \in U(R)$.

32. Έστω R ένας δακτύλιος τέτοιος ώστε $r^2 = r$ για κάθε $r \in R$. Δείξτε ότι ο R είναι μεταθετικός.

33. * Έστω R ένας δακτύλιος τέτοιος ώστε $r^3 = r$ για κάθε $r \in R$. Δείξτε ότι ο R είναι μεταθετικός.

34. Έστω R δακτύλιος με μοναδιαίο στοιχείο 1_R και S υποδακτύλιος του R με μοναδιαίο στοιχείο 1_S. Εξετάστε ποιες από τις ακόλουθες προτάσεις αληθεύουν.

a. $U(S) \subseteq U(R)$.

b. Αν $1_R = 1_S$, τότε $U(S) \subseteq U(R)$.

c. Αν ο R είναι περιοχή και ο S μη τετριμμένος, τότε ο S είναι περιοχή.

d. Αν ο R είναι σώμα και ο S πεπερασμένο σύνολο με τουλάχιστον δύο στοιχεία, τότε ο S είναι σώμα.

Υποδείξεις/Απαντήσεις
Ασκήσεις3

1.
a. Έχουμε $([0],[1]) = ([2],[1])$, $([0],[1]) \mapsto [1]$, $([2],[1]) \mapsto [2]$ και $[1] \neq [2]$.
b. Με πράξεις επαληθεύονται όλες οι ιδιότητες του ορισμού.
c. Δεν ισχύει η προσεταιριστική ιδιότητα της $\bullet$ καθώς $(a \bullet b) \bullet c = (a-b) \bullet c = (a-b) - c = a - b - c$ και $a \bullet (b \bullet c) = a - (b \bullet c) = a - (b - c) = a - b + c$. Για παράδειγμα, $(2 \bullet 2) \bullet 1 = -1$, ενώ $2 \bullet (2 \bullet 1) = 1$.

2.
Απάντηση: Η πράξη της άσκησης αυτής δεν μπορεί να είναι η πρόσθεση δακτυλίου, για παράδειγμα δεν υπάρχει ουδέτερο στοιχείο (δεν υπάρχει γραμμή της μορφής $a \;\; b \;\; c \;\; d$). (Επίσης, από τον πίνακα βλέπουμε ότι $b + d \neq d + b$).

3. Απαντήσεις:
a. Είναι μεταθετικός υποδακτύλιος και δεν έχει μοναδιαίο στοιχείο. Συνεπώς δεν είναι περιοχή ούτε σώμα.
b. Είναι περιοχή. Δεν είναι σώμα, αφού, για παράδειγμα, το $\sqrt{2}$ δεν είναι αντιστρέψιμο στο $\mathbb{Z}[\sqrt{2}]$ (αποδείξτε το).
c. Δεν είναι υποδακτύλιος. Δεν είναι κλειστό ως προς τον πολλαπλασιασμό, ειδικά $\left(\sqrt[3]{2}\right)^2 = \sqrt[3]{4} \notin S$ (γιατί;).
d. Δεν είναι υποδακτύλιος. Δεν είναι κλειστό ως προς τον πολλαπλασιασμό. Για παράδειγμα, ενώ $3 + \sqrt{2} \in S$, έχουμε $(3+\sqrt{2})^2 = 11 + 6\sqrt{2} \notin S$ αφού $11 \not\equiv 0 \bmod 3$.
e. Σώμα (με μοναδιαίο στοιχείο το [4]).
f. Σώμα (με μοναδιαίο στοιχείο το $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$).
g. Δεν είναι υποδακτύλιος (δεν περιέχει το μηδενικό πίνακα).
h. Δεν είναι υποδακτύλιος. Δεν είναι κλειστό ως προς τον πολλαπλασιασμό. Για παράδειγμα ενώ $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in S$, έχουμε $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin S$).

4.
a. Είναι σαφές ότι $\{1, -1, i, -i\} \subseteq U(\mathbb{Z}[i])$. (Για παράδειγμα, το αντίστροφο του i είναι το $-i$, αφού $i(-i) = (-i)i = 1$).
Έστω $a + bi \in \mathbb{C}, a, b \in \mathbb{Z}$, με $a + ib \in U(\mathbb{Z}[i])$. Τότε υπάρχουν $d, c \in \mathbb{Z}$ με $(a+ib)(c+di) = 1$. Λαμβάνοντας μέτρα μιγαδικών έχουμε $\left|(a+ib)(c+di)\right| = 1$, οπότε $\left|(a+ib)\right|\left|(c+di)\right| = 1$ και $\left|(a+ib)\right|^2 \left|(c+di)\right|^2 = 1$. Άρα $(a^2+b^2)(c^2+d^2) = 1$. Επειδή οι a^2+b^2 και c^2+d^2 είναι θετικοί ακέραιοι, έχουμε $a^2 + b^2 = 1$. Επειδή $a, b \in \mathbb{Z}$ παίρνουμε 1) $a = \pm 1$ και $b = 0$ ή 2) $a = 0$ και $b = \pm 1$. Συνεπώς ο $a + bi$ είναι ένας από τους $1, -1, i, -i$, πράγμα που σημαίνει ότι $U(\mathbb{Z}[i]) \subseteq \{1, -1, i, -i\}$. Άρα $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.
b. Βλ. σελίδα 81.

5.
Έστω ότι ο $A \in M_n(\mathbb{Z})$ είναι αντιστρέψιμο στοιχείο του δακτυλίου $M_n(\mathbb{Z})$. Τότε υπάρχει $B \in M_n(\mathbb{Z})$ με $AB = BA = I_n$. Λαμβάνοντας ορίζουσες έχουμε $\det(AB) = \det I_n$, οπότε
$$(\det A)(\det B) = 1.$$
Επειδή $A, B \in M_n(\mathbb{Z})$, έχουμε $\det A, \det B \in \mathbb{Z}$ και άρα $\det A = \pm 1$.

Αντίστροφα, έστω $A \in M_n(\mathbb{Z})$ με $\det A = \pm 1$. Από τη γραμμική άλγεβρα, ξέρουμε ότι ο A είναι αντιστρέψιμο στοιχείο του $M_n(\mathbb{R})$ και

$$A^{-1} = \frac{1}{\det A} adjA,$$

όπου στη θέση (i, j) του πίνακα $adjA$ υπάρχει το στοιχείο $(-1)^{i+j} \det A_{ij}$, όπου A_{ij} είναι ο $(n-1)\times(n-1)$ πίνακας που προκύπτει από τον A κατόπιν διαγραφής της j στήλης και i γραμμής του A. Επειδή τα στοιχεία του A είναι ακέραιοι, το ίδιο συμβαίνει με τον $adjA$. Επειδή $\det A = \pm 1$, βλέπουμε ότι τα στοιχεία του A^{-1} είναι ακέραιοι, δηλαδή $A^{-1} \in M_n(\mathbb{Z})$. Άρα υπάρχει $A^{-1} \in M_n(\mathbb{Z})$ τέτοιος ώστε $AA^{-1} = A^{-1}A = I_n = 1_{M_2(\mathbb{Z})}$. Δηλαδή το στοιχείο $A \in M_n(\mathbb{Z})$ είναι αντιστρέψιμο.

Σημείωση: Ο πίνακας $A = \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix} \in M_2(\mathbb{Z})$ είναι αντιστρέψιμο στοιχείο του δακτυλίου $M_2(\mathbb{R})$ (αφού $\det A = 2 \neq 0$) αλλά όχι του $M_2(\mathbb{Z})$ (αφού $\det A = 2 \neq \pm 1$). Στο $M_2(\mathbb{R})$, $A^{-1} = \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 3/2 \end{pmatrix}$.

6.

a. Έστω $u, v \in U(R)$. Τότε υπάρχουν $u', v' \in R$ τέτοια ώστε $uu' = u'u = 1_R$ και $vv' = v'v = 1_R$. Θέτοντας $w = v'u'$ παρατηρούμε ότι

$$(uv)w = (uv)(v'u') = ((uv)v')u' = (u(vv'))u' = (u1_R)u' = uu' = 1_R.$$

Όμοια $w(uv) = 1$. Άρα $uv \in U(R)$.

b. Υπόδειξη: Δείξτε ότι $(re - r + e)s = s$ για κάθε $r, s \in R$ και χρησιμοποιήστε τη μοναδικότητα της υπόθεσης.

7. Υπόδειξη: Δείξτε ότι το $3 + 2\sqrt{2}$ είναι αντιστρέψιμο. Άρα (βλ. προηγούμενη άσκηση) τα $\left(3 + 2\sqrt{2}\right)^n$, $n \in \mathbb{N}$, είναι αντιστρέψιμα.

8.

b. Δεν είναι γενικά μεταθετικός.

c. Υπόδειξη: Δείξτε ότι $\begin{pmatrix} [a] & [b] \\ [0] & [c] \end{pmatrix} \in U(T_2(\mathbb{Z}_n)) \Leftrightarrow [a], [c] \in U(\mathbb{Z}_n)$.

9. Βλ. Παράδειγμα 2.1.5 5.

10.

Έστω $A \in M_2(\mathbb{Z}_p)$, οπότε κάθε στοιχείο του πίνακα A είναι στοιχείο του συνόλου $\mathbb{Z}_p$. Έχουμε $|\mathbb{Z}_p| = p$. Ξέρουμε ότι ο A είναι αντιστρέψιμος αν και μόνο αν οι γραμμές του είναι γραμμικά ανεξάρτητες (ως στοιχεία του $\mathbb{Z}_p$-διανυσματικού χώρου $\mathbb{Z}_p \times \mathbb{Z}_p$). Έστω ότι ο A είναι αντιστρέψιμος. Τότε για την πρώτη γραμμή του A υπάρχουν $p^2 - 1$ δυνατές περιπτώσεις (όλες εκτός από τη μηδενική γραμμή). Για τη δεύτερη γραμμή υπάρχουν $p^2 - p$ περιπτώσεις (όλες οι περιπτώσεις εκτός από αυτές που η δεύτερη γραμμή είναι πολλαπλάσιο της πρώτης). Άρα το πλήθος των αντιστρέψιμων στοιχείων του $A \in M_2(\mathbb{Z}_p)$ είναι $(p^2 - 1)(p^2 - p)$.

11.

Υπόδειξη: a. Άμεσο από την Πρόταση 2.1.10.

b. Έστω S ένας υποδακτύλιος του $\mathbb{Q}$ με $\frac{1}{2}, \frac{1}{3} \in S$. Έχουμε $1 = \frac{1}{2} + \frac{1}{2} \in S$ λόγω της κλειστότητας της πρόσθεσης. Επειδή ο S είναι δακτύλιος, $-1 \in S$ και άρα κάθε άθροισμα της μορφής $a_1 + ... + a_k$, όπου $a_i = \pm 1$, ανήκει στο S. Άρα $\mathbb{Z} \subseteq S$.

Επίσης, $\frac{1}{2^a}=\frac{1}{2}...\frac{1}{2}\in S$ για κάθε $a\in\mathbb{Z}_{>0}$ λόγω της κλειστότητας του πολλαπλασιασμού. Όμοια, $\frac{1}{3^b}\in S$ για κάθε $b\in\mathbb{Z}_{>0}$. Άρα $\frac{m}{2^a3^b}=m\frac{1}{2^a}\frac{1}{3^b}\in S$, δηλαδή $R\subseteq S$.

c. Το R δεν είναι σώμα. Για παράδειγμα, το $7\in R$ δεν είναι αντιστρέψιμο . Πράγματι, αν το 7 ήταν αντιστρέψιμο στο R, τότε θα υπήρχαν $m\in\mathbb{Z},a,b\in\mathbb{N}$ με $1=\frac{m}{2^a3^b}7$, οπότε $7m=2^a3^b$ που σημαίνει ότι $7\left|2^a\right.$ ή $7\left|3^b\right.$, άτοπο.

12.

b. Έστω $a\in R-\{0\}$. Αρκεί να δείξουμε ότι ο μιγαδικός αριθμός a^{-1} ανήκει στο R. Θεωρούμε την απεικόνιση $f:R\to R, r\mapsto ar.$ Εύκολα επαληθεύεται ότι η f είναι $\mathbb{Q}$-γραμμική και 1-1. Επειδή $\dim_{\mathbb{Q}}R<\infty,$ είναι επί. Συνεπώς υπάρχει $s\in R$ με $as=1.$ Τότε $s=a^{-1},$ οπότε $a^{-1}\in R.$

13.

a. Είναι σαφές ότι

- $R\neq\varnothing$.

Έστω $c_0+c_1a+c_2a^2, d_0+d_1a+d_2a^2\in R$ όπου $c_i,d_i\in\mathbb{Q}.$ Τότε

- $c_0+c_1a+c_2a^2-(d_0+d_1a+d_2a^2)=c_0-d_0+(c_1-d_1)a+(c_2-d_2)a^2\in R$.

Από $a^3=a+1$ έχουμε $a^4=a^2+a$ και επομένως

- $(c_0+c_1a+c_2a^2)(d_0+d_1a+d_2a^2)=$
  $=c_0d_0+(c_0d_1+c_1d_0)a+(c_0d_2+c_1d_1+c_2d_0)a^2+(c_1d_2+c_2d_1)a^3+(c_2d_2)a^4=$
  $=c_0d_0+(c_0d_1+c_1d_0)a+(c_0d_2+c_1d_1+c_2d_0)a^2+(c_1d_2+c_2d_1)(a+1)+(c_2d_2)(a^2+a)=$
  $=c_0d_0+c_1d_2+c_2d_1+(c_0d_1+c_1d_0+c_2d_2+c_1d_2+c_2d_1)a+(c_0d_2+c_1d_1+c_2d_0+c_2d_2)a^2\in R.$

Άρα το R είναι υποδακτύλιος του $\mathbb{C}$.

b. Έπεται από το ερώτημα b της προηγούμενης άσκησης.

c. Αν $2+a^2=0,$ τότε $2a+a^3=0$ δηλαδή $2a+(a+1)=0$, οπότε $a=-1/3$ που όμως δεν ικανοποιεί τη σχέση $a^3-a-1=0.$ Άρα $2+a^2\neq0.$

Από το a έχουμε $(2+a^2)(c_0+c_1a+c_2a^2)=2c_0+c_1+(3c_1+c_2)a+(c_0+3c_2)a^2.$ Εύκολα επαληθεύεται ότι το σύστημα

$$\begin{cases}2c_0+c_1=1\\3c_1+c_2=0\\c_0+3c_2=0\end{cases}$$

έχει τη λύση $c_0=9/19, c_1=1/19,$ $c_2=-3/19$. Συνεπώς για τις τιμές αυτές έχουμε $(2+a^2)(c_0+c_1a+c_2a^2)=1,$ δηλαδή $(2+a^2)^{-1}=c_0+c_1a+c_2a^2.$

14.

b. Υπόδειξη: Αν τα R,S έχουν μοναδιαία στοιχεία $1_R,1_S$ αντίστοιχα, δείξτε ότι το $(1_R,1_S)$ είναι μοναδιαίο στοιχείο του $R\times S$. Αντίστροφα, αν το $R\times S$ έχει μοναδιαίο στοιχείο $1_{R\times S}$, τότε υπάρχουν $r_0\in R, s_0\in S$ με $1_{R\times S}=(r_0,s_0)$. Δείξτε ότι τα r_0,s_0 είναι μοναδιαία στοιχεία των R,S αντίστοιχα.

d. Δεν αληθεύει. Από την υπόθεση έχουμε $1_R\neq0_R$ και $1_S\neq0_S$, οπότε $(1_R,0_s)\neq(0_R,0_s)=0_{R\times S}$ και $(0_R,1_S)\neq(0_R,0_S)=0_{R\times S}$. Αλλά $(1_R,0_S)(0_R,1_S)=(1_R0_R,0_S1_S)=(0_R,0_s)=0_{R\times S}.$

15.

Έστω R ένας υποδακτύλιος του $\mathbb{Z}$. Τότε $R \neq \varnothing$ και αν $a \in R$, τότε $-a \in R$. Μπορούμε να υποθέσουμε ότι $R \neq \{0\}$. Τότε $R \cap \mathbb{Z}_{>0} \neq \varnothing$. Έστω m ο ελάχιστος θετικός ακέραιος με $m \in R$. Έχουμε $m\mathbb{Z} \subseteq R$ γιατί ο R είναι δακτύλιος.

Αν $n \in R$, τότε από την Ευκλείδεια διαίρεση υπάρχουν $q, r \in \mathbb{Z}$ με $n = qm + r, 0 \leq r < m$. Έχουμε $r = n - qm \in R$ γιατί $n, m \in R$ και R δακτύλιος. Λόγω του ελαχίστου του m παίρνουμε $r = 0$. Τότε $n = qm \in R$. Άρα $R \subseteq m\mathbb{Z}$. Συνεπώς $R = m\mathbb{Z}$

16. b. Απάντηση: $m = \varepsilon\kappa\pi(4,6) = 12.$

17. Βλ. Παράδειγμα 2.1.12 1.

18. Βλ. Παράδειγμα 2.1.12 2.

19.

c. Υπόδειξη: Δείξτε ότι αν $a + b\sqrt{2} = c + d\sqrt{3}$, όπου $a, b, c, d \in \mathbb{Q},$ τότε $b = d = 0.$ Άρα $\mathbb{Q}[\sqrt{2}] \cap \mathbb{Q}[\sqrt{3}] = \mathbb{Q}.$

20.

Υπόδειξη: Αν $A = (a_{ij}),$ τότε $E_{ss} A E_{tt} = a_{st} E_{st}$. Απάντηση: Υπάρχει μόνο ένας, ο $M_n(\mathbb{R})$.

21.

Έχουμε $(a+b)^2 = (a+b)(a+b) = a(a+b) + b(a+b) = a^2 + ab + ba + b^2.$ Άρα

$(a+b)^2 = a^2 + 2ab + b^2 \Leftrightarrow a^2 + ab + ba + b^2 = a^2 + 2ab + b^2 \Leftrightarrow ab = ba$.

22.

Απάντηση: a. [0],[1],[5],[6]. b. [0],[1]. c. $0_R, 1_R$. d. Βλ. παρακάτω.

Για το b. παρατηρούμε ότι αν $[a] \in \mathbb{Z}_{p^m}$ ικανοποιεί $[a]^2 = [a],$ τότε $p^k \mid a(a-1)$. Από αυτό έπεται ότι $p^k \mid a$ ή $p^k \mid a-1$ (δικαιολογήστε το). Άρα $[a] = [0],[1]$.

Για το d. χρησιμοποιούμε λίγη γραμμική άλγεβρα: Ο πίνακας $A \in M_2(\mathbb{R})$ ικανοποιεί $A^2 = A,$ αν και μόνο αν το ελάχιστο πολυώνυμο του A είναι ένα από τα $x, x-1, x(x-1)$. Αντίστοιχα έχουμε

$A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, A όμοιος με τον $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ (άσκηση).

Στην τελευταία περίπτωση, υπάρχει αντιστρέψιμος $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ με $A = P \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} P^{-1} = \frac{1}{ad-bc} \begin{pmatrix} -bc & ba \\ -dc & da \end{pmatrix}.$

23.

Απάντηση: a. Το $\mathbb{Z}_{30}$ έχει μοναδικό μηδενοδύναμο στοιχείο, το [0]. Το $\mathbb{Z}_{60}$ έχει δύο μηδενοδύναμα στοιχεία, τα $[0],[30]$.

b. Ο $\mathbb{Z}_n$ δεν έχει μη μηδενικό μηδενοδύναμο στοιχείο αν και μόνο αν ο n δεν διαιρείται με το τετράγωνο πρώτου (ή ισοδύναμα $n = p_1 \ldots p_k$, όπου $p_1, \ldots, p_k$ διακεκριμένοι πρώτοι).

Απόδειξη: Έστω $n = p_1 \ldots p_k$, όπου $p_1, \ldots, p_k$ διακεκριμένοι πρώτοι και έστω $[a] \in \mathbb{Z}_n$ με $[a]^m = [0]$, $m \in \mathbb{Z}_{>0}$. Τότε $[a^m] = [0]$ και άρα $n \mid a^m$, οπότε $p_i \mid a^m$ για κάθε i. Επειδή p_i πρώτος, $p_i \mid a$. Επειδή οι $p_1, \ldots, p_k$ είναι ανά δύο σχετικά πρώτοι, $p_1 p_2 \ldots p_k \mid a$, δηλαδή $n \mid a$. Άρα $[a] = [0]$.

Αντίστροφα, έστω ότι ο δακτύλιος $\mathbb{Z}_n$ δεν έχει μη μηδενικό μηδενοδύναμο στοιχείο και έστω $n = p_1^{n_1} \ldots p_k^{n_k}$ η ανάλυση του n σε γινόμενο πρώτων. Έστω $a = p_1 \ldots p_k$, οπότε $n \mid a^m$, όπου $m = \max\{n_1, \ldots, n_k\}$. Δηλαδή $[a]^m = [0].$ Από την υπόθεση παίρνουμε $[a] = [0]$, δηλαδή $n \mid a$, πράγμα που σημαίνει ότι $n_i = 1$ για κάθε i.

24.

a. Αν $r^m = 0$, τότε $(1-r)(1+r+...+r^{m-1}) = (1+r+...+r^{m-1})(1-r) = 1-r^m = 1$.

c. Υπόδειξη: Αν $r^m = s^n = 0$, βρείτε ένα N τέτοιο ώστε $(r+s)^N = 0$ με τη βοήθεια του διωνυμικού αναπτύγματος (άσκηση 3.17).

25.

Παρατήρηση: Από την υπόθεση υπάρχει σώμα F τέτοιο ώστε ο R είναι υποδακτύλιος του F. Άρα αν $r \in R-\{0\}$, τότε στο F υπάρχει το αντίστροφο r^{-1} του r. Συνεπώς, αν $x \in \mathbb{Z}$, τότε το a^x (ορίζεται και για αρνητικούς ακέραιους x) είναι ένα στοιχείο του F.

Με τους συμβολισμούς της άσκησης, αν $a = 0$, τότε $b^n = 0$ και άρα $b = 0$ (γιατί το F είναι σώμα). Υποθέτουμε ότι $a, b \neq 0$. Επειδή οι m, n είναι σχετικά πρώτοι, υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $1 = mx + ny$. Εργαζόμενοι στο F έχουμε $a = a^{mx+ny} = (a^m)^x (a^n)^y = (b^m)^x (b^n)^y = b^{mx+ny} = b$.

26.

b. Απάντηση: $A(X) = \left\{ \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} \middle| b, d \in \mathbb{R} \right\}$. Δεν είναι μεταθετικός και δεν έχει μοναδαίο στοιχείο.

27.

a. Υπόδειξη: Για να δείξουμε ότι το R είναι κλειστό ως προς τον πολλαπλασιασμό πινάκων παρατηρούμε ότι από το Θεώρημα των Cayley-Hamilton της Γραμμικής Άλγεβρας, $A^2 = Tr(A)A \in R$.

b. Απάντηση: Αν $Tr(A) = 1$, τότε $1_R = A$ και $U(R) = \{A, -A\}$. Αν $Tr(A) = -1$, τότε $1_R = -A$ και $U(R) = \{A, -A\}$.

28.

c. Έστω $A \in C(M_2(\mathbb{R}))$. Τότε $AB = BA$ για κάθε $B \in M_2(\mathbb{R})$. Έστω $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Επιλέγοντας $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ έχουμε

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \Rightarrow b = c = 0.$$

Επιλέγοντας $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ έχουμε

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow \begin{pmatrix} b & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} \Rightarrow a = d.$$

Άρα $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ και $C\left(M_2(\mathbb{R})\right) \subseteq \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| a \in \mathbb{R} \right\}$. Είναι σαφές ότι $\left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| a \in \mathbb{R} \right\} \subseteq C\left(M_2(\mathbb{R})\right)$ και άρα έχουμε ισότητα.

d. Ας αναπτύξουμε την ιδέα της προηγούμενης λύσης πιο συστηματικά. Έστω $E_{ij} \in M_n(\mathbb{R})$ ο πίνακας του οποίου όλα τα στοιχεία είναι 0 εκτός από το στοιχείο στη θέση (i, j) που είναι ίσιο με 1. Υπενθυμίζουμε ότι

$$E_{ij}E_{st} = \begin{cases} E_{it}, & \alpha\nu\ j = s \\ 0, & \alpha\nu\ j \neq s \end{cases}.$$

Έστω $A \in C(M_n(\mathbb{R}))$. Τότε $E_{ji}A = AE_{ji}$. Γράφοντας $A = \sum_{s,t} a_{st}E_{st}$ παίρνουμε $\sum_{s,t} a_{st}E_{ji}E_{st} = \sum_{s,t} a_{st}E_{st}E_{ji}$ και άρα

$$\sum_t a_{it}E_{jt} = \sum_s a_{sj}E_{si}. \qquad (1)$$

Πολλαπλασιάζοντας την (1) από δεξιά με το E_{ji} παίρνουμε $a_{ij}E_{jj} = \sum_s a_{st}E_{si}E_{ji}$. Αν $i \neq j$, το δεξί μέλος της τελευταίος ισότητας είναι 0 και άρα έχουμε $a_{ij} = 0$. Τότε η σχέση (1) γίνεται $a_{ii}E_{ji} = a_{jj}E_{ji}$ και άρα $a_{ii} = a_{jj}$.

Συνεπώς $A = \begin{pmatrix} a & & \\ & \ddots & \\ & & a \end{pmatrix} = aI_n$ και $C\left(M_n(\mathbb{R})\right) \subseteq \left\{aI_n \middle| a \in \mathbb{R}\right\}$.

Η σχέση $\left\{aI_n \middle| a \in \mathbb{R}\right\} \subseteq C\left(M_n(\mathbb{R})\right)$ είναι σαφής και άρα $\left\{aI_n \middle| a \in \mathbb{R}\right\} = C\left(M_n(\mathbb{R})\right)$.

e. Απάντηση: Αληθεύει.

29.

Από τη υπόθεση έπεται ότι $(r+s)^2 + r + s \in C(R)$ για κάθε $r, s \in R$. Άρα

$$r^2 + s^2 + rs + sr + r + s \in C(R).$$

Επειδή $r^2 + r, s^2 + s \in C(R)$ και ο $C(R)$ είναι δακτύλιος (βλ. προηγούμενη άσκηση) παίρνουμε $rs + rs \in C(R)$. Άρα $r(rs+sr) = (rs+sr)r$ δηλαδή $r^2s + rsr = rsr + sr^2$, οπότε $r^2s = sr^2$. Επειδή η τελευταία σχέση ισχύει για κάθε $s \in R$, έχουμε $r^2 \in C(R)$. Επειδή $r^2 + r \in C(R)$ και ο $C(R)$ είναι δακτύλιος, έχουμε $r \in C(R)$ για κάθε $r \in R$. Άρα ο R είναι μεταθετικός.

30.

Λύση: Επειδή το a δεν είναι μηδενοδιαιρέτης, η απεικόνιση $R \to R, r \mapsto ra$ είναι 1-1. Επειδή το σύνολο R είναι πεπερασμένο, αυτή είναι επί. Συνεπώς υπάρχει $e \in R$ με $ea = a$.

Από $(ae-a)a = (ae)a - a^2 = a(ea) - a^2 = a^2 - a^2 = 0$, έπεται ότι $ae - a = 0$, γιατί το a δεν είναι μηδενοδιαιρέτης. Συνεπώς έχουμε $ea = ae = a$.

Θα δείξουμε τώρα ότι $er = re = r$ για κάθε $r \in R$. Πράγματι, από $a(er - r) = a(er) - ar = (ae)r - ar = ar - ar = 0$ έπεται ότι $er - r = 0$ γιατί το a δεν είναι μηδενοδιαιρέτης. Όμοια, έχουμε $(re - r)a = 0$ και επομένως $re - r = 0$. Άρα $er = re = r$.

31.

Υπόδειξη: Δείξτε ότι αν c είναι το αντίστροφο του $1 - ab$, τότε το $1 + bca$ είναι το αντίστροφο του $1 - ba$.

32.

Από $(x+x)^2 = x + x$ έχουμε $4x^2 = 2x$ και άρα $4x = 2x$, δηλαδή

$$x = -x \text{ για κάθε } x \in R.$$

Από $(x+y)^2 = x + y$ παίρνουμε $x^2 + y^2 + xy + yx = x + y$ και αφού $x^2 = x$ και $y^2 = y$ παίρνουμε $xy + yx = 0$, δηλαδή $xy = -yx$. Άρα $xy = yx$.

33. Δύσκολη άσκηση. Υπόδειξη: Έστω $x, y \in R$.

1) Αναπτύσσοντας το αριστερό μέλος της $(x+y)^3 - (x-y)^3 = (x+y) - (x-y) = 2y$ δείξτε ότι $2x^2y + 2xyx + 2yx^2 = 0$. Έστω A το αριστερό μέλος της τελευταίας σχέσης. Χρησιμοποιώντας $xA - Ax = 0$ δείξτε ότι

$$2xy = 2yx.$$

2) Από $(x+x)^3 = x + x$ έπεται ότι

$$6x = 0.$$

3) Αναπτύσσοντας το $(x+y)^3 - (x^3 + y^3) = 0$, θέτοντας $y = x^2$ και χρησιμοποιώντας το 2) δείξτε ότι

$$3x^2 = 3x.$$

4) Από το 3) έχουμε $3(x+y)^2 - 3(x+y) = 0$. Αναπτύσσοντας το αριστερό μέλος και χρησιμοποιώντας το 2) δείξτε ότι

$$3xy = 3yx.$$

Το ζητούμενο έπεται από την προηγούμενη σχέση και το 1).

34.

a. Λ.
b. Σ.
c. Σ.
d. Σ.

Ασκήσεις4
Πολυώνυμα

Συμβολισμός: Στις παρακάτω ασκήσεις, θα ακολουθούμε συχνά συμβολισμό σύμφωνα με το παράδειγμα: το πολυώνυμο $[2]x^2+[5]x+[4]\in\mathbb{Z}_7[x]$ θα συμβολίζεται $2x^2+5x+4\in\mathbb{Z}_7[x]$.

1. Ποιοι από τους δακτυλίους $\mathbb{Z}_4[x]$, $\mathbb{Z}_5[x]$ είναι περιοχές; Ποιο είναι το $U(\mathbb{Z}_5[x])$; Δείξτε ότι $U(\mathbb{Z}_4[x])\neq U(\mathbb{Z}_4)$.

2. Δώστε ένα παράδειγμα $f(x)\in\mathbb{Z}_6[x]$ που έχει βαθμό 1 και δεν είναι ανάγωγο.

3.
   a. Έστω R μια περιοχή. Δείξτε ότι δεν υπάρχει $f(x)\in R[x]$ με $(x+1)^{2011}+(x^2+1)^{40}=f(x)^{30}$.
   b. Να βρεθούν όλα τα πολυώνυμα $f(x)\in\mathbb{Q}[x]$ με $f(x+2)-2f(x+1)=f(x)$.

4. Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Δείξτε ότι το $ax+b\in R[x]$ είναι αντιστρέψιμο αν και μόνο αν το b είναι αντιστρέψιμο στο R και υπάρχει $n\in\mathbb{Z}_{>0}$ με $a^n=0$.

5. Έστω F,K δύο σώματα τέτοια ώστε το F είναι υποδακτύλιος του K (για παράδειγμα $F=\mathbb{Q}$ και $K=\mathbb{C}$). Έστω $f(x),g(x)\in F[x]$.
   a. Αν στο $K[x]$ ισχύει $f(x)\mid g(x)$, τότε στο $F[x]$ ισχύει $f(x)\mid g(x)$.
   b. Ο μκδ των $f(x), g(x)$ όταν αυτά θεωρηθούν ως στοιχεία του $F[x]$ είναι ίσος με το μκδ των $f(x), g(x)$ όταν αυτά θεωρηθούν ως στοιχεία του $K[x]$.

6. Έστω F ένα σώμα, $a(x),b(x),f(x)\in F[x]$ και $\mu\kappa\delta(a(x),b(x))=1$.
   a. Αν $a(x)\mid b(x)f(x)$, τότε $a(x)\mid f(x)$.
   b. Αν $a(x)\mid f(x)$ και $b(x)\mid f(x)$, τότε $a(x)b(x)\mid f(x)$.
   c. $\mu\kappa\delta(a(x),b(x)f(x))=\mu\kappa\delta(a(x),f(x))$.
   d. $\mu\kappa\delta(a(x)b(x),f(x))=\mu\kappa\delta(a(x),f(x))\cdot\mu\kappa\delta(b(x),f(x))$.

7. Να βρεθούν
   a. όλα τα μονικά $f(x)\in\mathbb{R}[x]$ βαθμού 3 τέτοια ώστε $\mu\kappa\delta(f(x),x^2+1)\neq 1$ και $\deg\mu\kappa\delta(f(x),x^2-3x+2)=1$,
   b. όλα τα μονικά ανάγωγα $p(x),q(x)\in\mathbb{Q}[x]$ με $(x^2-1)p(x)+(x+2)q(x)=p(x)q(x)$.

8. Να βρεθεί ένα $f(x)\in\mathbb{Q}[x]$ με ρίζα το $1+\sqrt{1+\sqrt{2}}$.

9. Να βρεθούν όλα τα $f(x)\in\mathbb{Z}[x]$ τέτοια ώστε $xf(x-1)=(x-2014)f(x)$.

10. Δεν υπάρχει πολυώνυμο $f(x)\in\mathbb{Z}[x]$ θετικού βαθμού τέτοιο ώστε για κάθε $m\in\mathbb{N}$, το $f(m)$ να είναι πρώτος.

11. Έστω F ένα σώμα.
   a. Αποδείξτε ότι υπάρχουν άπειρα στο πλήθος ανάγωγα πολυώνυμα στο $F[x]$.
   b. Έστω ότι το F είναι πεπερασμένο σώμα. Αποδείξτε ότι για κάθε $n\in\mathbb{N}$ υπάρχει ανάγωγο πολυώνυμο του $F[x]$ βαθμού μεγαλύτερου ή ίσου του n.

12. Έστω F ένα σώμα και $m,n\in\mathbb{Z}_{>0}$. Τότε στο $F[x]$ έχουμε $\mu\kappa\delta(x^m-1,x^n-1)=x^d-1$, όπου $d=\mu\kappa\delta(m,n)$.

13. Έστω p πρώτος.
   a. Δείξτε ότι στο $\mathbb{Z}_p[x]$, $x^p-x=x(x-1)(x-2)...(x-(p-1))$.
   b. Δείξτε ότι $(p-1)!\equiv -1 \bmod p$.
   c. Βρείτε το υπόλοιπο της διαίρεσης του $98!$ με το 101.
   d. Αν $p>3$, δείξτε ότι $\sum_{0<i<j<p} ij\equiv 0 \bmod p$.

14. Έστω $n \in \mathbb{Z}_{>0}$ και $\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \in \mathbb{C}$.

a. Δείξτε ότι στο $\mathbb{C}[x]$, $x^n - 1 = (x-1)(x-\zeta)(x-\zeta^2)...(x-\zeta^{n-1})$.

b. Δείξτε ότι αν $n \geq 3$, τότε $\sum_{0 \leq i < j \leq n-1} \cos\frac{(i+j)2\pi}{n} = 0$.

15. Έστω p πρώτος. Δείξτε ότι για κάθε $f(x) \in \mathbb{Z}_p[x]$, $(f(x))^p = f(x^p)$.

16. Βρείτε την ανάλυση σε γινόμενο αναγώγων πολυωνύμων των ακόλουθων πολυωνύμων:

a. $x^3 + 2x^2 + 2 \in \mathbb{Z}_3[x]$,

b. $x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$,

c. $x^p + a \in \mathbb{Z}_p[x]$, όπου p πρώτος,

d. $x^2 + 1 \in \mathbb{Z}_p[x]$, όπου p πρώτος με $p \equiv 3 \bmod 4$.

17. Έστω p πρώτος . Βρείτε την ανάλυση του $x^{p^2} - x^p \in \mathbb{Z}_p[x]$ σε γινόμενο αναγώγων πολυωνύμων στο $\mathbb{Z}_p[x]$.

18. Εξετάστε αν το $x^4 + 2 \in \mathbb{Z}_5[x]$ είναι ανάγωγο.

19. Δείξτε ότι το $(x-1)(x-2)...(x-2011) - 1 \in \mathbb{Z}[x]$ είναι ανάγωγο.

20. Έστω p πρώτος και $n \in \mathbb{N}$. Ποια απεικόνιση $\mathbb{Z}_p \to \mathbb{Z}_p$ επάγει το πολυώνυμο $x^{p^n} - x \in \mathbb{Z}_p[x]$;

21. Έστω p πρώτος και $f(x) = x^p - x + 1 \in \mathbb{Z}_p[x]$.

a. Δείξτε ότι το $f(x)$ δεν έχει ρίζα στο $\mathbb{Z}_p$.

b. Έστω F ένα σώμα που περιέχει ως υποδακτύλιο το $\mathbb{Z}_p$.

i. Δείξτε ότι $1_F = 1_{\mathbb{Z}_p}$ και $pr = 0$ για κάθε $r \in F$.

ii. *Δείξτε ότι αν το F περιέχει μια ρίζα του $f(x)$, τότε περιέχει p διακεκριμένες ρίζες του $f(x)$.

22. Έστω p πρώτος και $f(x) = (x^2 + x + 1)^p - (x^2 + x + 1) \in \mathbb{Z}_p[x]$.

a. Δείξτε ότι $x^p - x \mid f(x)$.

b. Βρείτε την ανάλυση του $f(x)$ σε γινόμενο αναγώγων πολυωνύμων στο $\mathbb{Z}_p[x]$ για $p = 2$ και $p = 3$.

23. Έστω p πρώτος και $f(x) = x^p + x^{p-1} - x - 1$. Βρείτε την ανάλυση του $f(x)$ σε γινόμενο αναγώγων πολυωνύμων στο $\mathbb{Z}_p[x]$.

24. Ποιο είναι το υπόλοιπο της διαίρεσης του $f(x) = x^4 + 4x^2 + x + 1 \in \mathbb{Z}_5[x]$ με το $g(x) = 2x^2 + 1 \in \mathbb{Z}_5[x]$ και ποιος ο $\mu\kappa\delta(f(x), g(x))$;

25. Έστω $f(x) = 4x^4 + 2x^3 + 6x^2 + 4x + 5 \in \mathbb{Z}_7[x]$ και $g(x) = 3x^3 + 5x^2 + 6x \in \mathbb{Z}_7[x]$. Βρείτε το $\mu\kappa\delta(f(x), g(x))$ και πολυώνυμα $a(x), b(x) \in \mathbb{Z}_7[x]$ τέτοια ώστε $\mu\kappa\delta(f(x), g(x)) = a(x)f(x) + b(x)g(x)$.

26. Έστω $f(x), g(x) \in \mathbb{Z}_p[x]$, όπου p πρώτος και

$f(x) = x^4 + 2x^3 + 4x^2 + 8x + 9$, $g(x) = x^2 + 2x + 3$.

Για ποιους p ισχύει ότι $\deg \mu\kappa\delta(f(x), g(x)) = 2$;

27. Βρείτε όλα τα $f(x) \in \mathbb{Z}_2[x]$ βαθμού 7 τέτοια ώστε $\mu\kappa\delta(f(x), x^3 + x + 1) \neq 1$ και $\mu\kappa\delta(f(x), x^2 + 1) \neq 1$.

28. Έστω $f(x), g(x) \in \mathbb{C}[x]$, $f(x) = x(x^4 - 1)$, $g(x) = x^9 - 1$.

a. Βρείτε το $\mu\kappa\delta(f(x), g(x))$.

b. Βρείτε $a(x), b(x) \in \mathbb{C}[x]$ τέτοια ώστε $x^{2011} - 1 = a(x)f(x) + b(x)g(x)$.

29. Έστω p πρώτος. Δείξτε ότι το πλήθος των μονικών αναγώγων πολυωνύμων βαθμού 2 στο $\mathbb{Z}_p[x]$ είναι ίσο με $\frac{p(p-1)}{2}$.

30.

a. Βρείτε όλα τα ανάγωγα πολυώνυμα στο $\mathbb{Z}_2[x]$ βαθμού ≤ 4.

b. Έστω $f(x) \in \mathbb{Z}_2[x]$ βαθμού 5. Δείξτε ότι το $f(x)$ είναι ανάγωγο αν και μόνο αν το $f(x)$ δεν έχει ρίζα στο $\mathbb{Z}_2[x]$ και δεν διαιρείται με το x^2+x+1.

c. Εξετάστε αν το $x^5+x^4+1 \in \mathbb{Z}_2[x]$ είναι ανάγωγο.

31. Έστω $n \in \mathbb{Z}_{>0}$. Βρείτε στο $\mathbb{R}[x]$ το *μκδ* των $x^{n+1}-(n+1)x+n,\ x^n-nx+n-1$.

32. Έστω $n \in \mathbb{Z}_{>0}$. Δείξτε ότι το x^2+x+1 διαιρεί το $(x+1)^n+x^n+1$ στο $\mathbb{R}[x]$ αν και μόνο αν $n \equiv 2,4 \bmod 6$.

33. *Να βρεθούν όλα τα $f(x), g(x) \in \mathbb{R}[x]$ τέτοια ώστε $f(x)g(x+1)-f(x+1)g(x)=1$.

34. Να λυθεί στο $\mathbb{C}$ το σύστημα

$$\begin{aligned} a+b+c &= 6,\\ ab+ac+bc &= 11,\\ abc &= 6. \end{aligned}$$

35. Αν ένα πολυώνυμο $f(x) \in \mathbb{Z}[x]$ λαμβάνει την τιμή 7 για τέσσερις διαφορετικές ακέραιες τιμές του x, τότε το $f(x)$ δεν λαμβάνει την τιμή 14 για καμιά ακέραια τιμή του x.

36. Εξετάστε ποιες από τις ακόλουθες προτάσεις αληθεύουν. Δικαιολογήστε την απάντησή σας.

a. Το $x^2-2 \in \mathbb{Q}[x]$ είναι ανάγωγο.

b. Το $x^2-2 \in \mathbb{R}[x]$ είναι ανάγωγο.

c. Αν m,n είναι περιττοί ακέραιοι, το $x^3+mx+n \in \mathbb{Z}[x]$ είναι ανάγωγο.

d. Το $x^3+3x+1 \in \mathbb{Z}_5[x]$ είναι ανάγωγο.

e. Το $x^3+2x+1 \in \mathbb{Z}_5[x]$ είναι ανάγωγο.

f. Έστω F ένα σώμα. Ένα $f(x) \in F[x]$ βαθμού 4 είναι ανάγωγο αν και μόνο αν δεν έχει ρίζα στο F.

g. Έστω p πρώτος. Το $x^{100}-3x^3+5x^2-2x+1 \in \mathbb{Z}_p[x]$ διαιρείται με το $x+1 \in \mathbb{Z}_p[x]$ αν και μόνο αν $p=2,3$.

h. Έστω p πρώτος. Το $x^{100}-3x^3+5x^2-2x+1 \in \mathbb{Z}_p[x]$ διαιρείται με το $x^2-1 \in \mathbb{Z}_p[x]$ αν και μόνο αν $p=2$.

i. Υπάρχει μοναδικό μονικό ανάγωγο πολυώνυμο στο $\mathbb{R}[x]$ που έχει στο $\mathbb{C}$ ρίζα το $1-i$.

j. Κάθε μη μηδενικό $f(x) \in R[x]$, όπου R δακτύλιος με μονάδα, έχει το πολύ $\deg f(x)$ ρίζες στο R.

k. Αν p είναι περιττός πρώτος, τότε το $x^p+x+1 \in \mathbb{Z}_p[x]$ έχει ακριβώς μια ρίζα στο $\mathbb{Z}_p$.

l. Αν p είναι περιττός πρώτος και $a \in \mathbb{Z}_p$, τότε το $x^p+a \in \mathbb{Z}_p[x]$ δεν είναι ανάγωγο.

Υποδείξεις/Απαντήσεις
Ασκήσεις4

1.
Ο $\mathbb{Z}_5[x]$ είναι περιοχή αφού ο $\mathbb{Z}_5$ είναι περιοχή (βλ. Πρόταση 2.1.4 και Πρόταση 2.2.4). Ο $\mathbb{Z}_4[x]$ δεν είναι περιοχή αφού $2\cdot 2=0$ και $2\neq 0$. Στο $\mathbb{Z}_4[x]$ έχουμε $(2x+1)(2x+1)=1$. Άρα $2x+1\in U(\mathbb{Z}_4[x])$ και επομένως $U(\mathbb{Z}_4[x])\neq U(\mathbb{Z}_4)$.

2.
Στο $\mathbb{Z}_6[x]$ έχουμε $(2x+1)(3x+1)=5x+1$. Άρα το $5x+1$ δεν είναι ανάγωγο στο $\mathbb{Z}_6[x]$.

3.
a. Παρατηρούμε ότι

$$\deg(x+1)^{2014}=2014,\ \deg(x^2+1)^{40}=40,\ \deg(x+1)^{2014}\neq\deg(x^2+1)^{40}.$$

Άρα $\deg((x+1)^{2014}+(x^2+1)^{40})=2014$. Αν $(x+1)^{2014}+(x^2+1)^{40}=f(x)^{30}$, τότε $2014=\deg(f(x)^{30})=30\deg f(x)$ σύμφωνα με την Πρόταση 2.2.4 2. Αυτό είναι άτοπο αφού το 30 δεν διαιρεί το 2011.
b. Απάντηση: Συγκρίνοντας μεγιστοβάθμιους όρους προκύπτει $f(x)=0$.

4.
Έστω ότι το $b\in R$ είναι αντιστρέψιμο και υπάρχει $n\in\mathbb{Z}_{>0}$ με $a^n=0$. Τότε θέτοντας $r=b^{-1}ax$ έχουμε $r^n=(ab^{-1}x)^n=a^n(b^{-1})^n x^n=0$ γιατί ο R είναι μεταθετικός. Παρατηρούμε ότι

$$(r+1)\left((-r)^{n-1}+(-r)^{n-2}+\ldots+(-r)+1\right)=$$
$$\left((-1)^{n-1}r^n+(-1)^{n-2}r^{n-1}+\ldots+(-1)r^2+r\right)+\left((-1)^{n-1}r^{n-1}+(-1)^{n-2}r^{n-2}+\ldots+(-r)+1\right)=$$
$$(-1)^{n-1}r^n+1=1.$$

Άρα το $r+1$ είναι αντιστρέψιμο στο $R[x]$. Συνεπώς το $b(r+1)=ax+b$ είναι αντιστρέψιμο σύμφωνα με την άσκηση 3.6a.
Αντίστροφα, έστω ότι το $ax+b$ είναι αντιστρέψιμο. Τότε υπάρχουν $c_i\in R$ με $(ax+b)(c_nx^n+\ldots.+c_1x+c_0)=1$. Άρα

$$\begin{cases} ac_n=0 \\ ac_{n-1}+bc_n=0 \\ \quad\vdots \\ ac_1+bc_2=0 \\ ac_0+bc_1=0 \\ bc_0=1. \end{cases}$$

Από την τελευταία σχέση έπεται ότι το b και το c_0 είναι αντιστρέψιμα στο R. Με διαδοχικές αντικαταστάσεις εργαζόμενοι από την τελευταία σχέση προς τα πάνω μέχρι τη δεύτερη, παίρνουμε $c_n=(-1)^{n+1}c_0{}^{n+1}a^n$. Αντικαθιστώντας στην πρώτη σχέση έχουμε $(-1)^{n+1}c_0a^{n+1}=0$. Άρα $a^{n+1}=0$ γιατί το $(-1)^{n+1}c_0$ είναι αντιστρέψιμο στο R.

5.
a. Αν $f(x)=0,$ τότε $g(x)=0$ και είναι σαφές ότι ισχύει το αποτέλεσμα. Έστω ότι $f(x)\neq 0$. Από την υπόθεση υπάρχει $h(x)\in K[x]$ με

$$g(x)=h(x)f(x).$$

Από την Ευκλείδεια διαίρεση στο $F[x]$ υπάρχουν $q(x),r(x)\in F[x]$ με

$$g(x)=q(x)f(x)+r(x) \text{ και } \deg r(x)<\deg f(x).$$

Από τη μοναδικότητα στην Ευκλείδειας διαίρεσης στο $K[x]$ έπεται ότι $r(x)=0$.

b. Υπόδειξη: Και στις δυο περιπτώσεις οι αντίστοιχοι Ευκλείδειοι αλγόριθμοι ταυτίζονται.

6.

a. και b. Υπάρχουν $g(x),h(x)\in F[x]$ με $1=g(x)a(x)+h(x)b(x)$ σύμφωνα με το Θεώρημα 2.3.7. Άρα

$$f(x)=f(x)g(x)a(x)+f(x)h(x)b(x). \quad (1)$$

a. Από την υπόθεση έχουμε $a(x)\big|f(x)h(x)b(x)$. Είναι σαφές ότι $a(x)\big|f(x)g(x)a(x)$. Άρα $a(x)\big|f(x)g(x)a(x)+f(x)h(x)b(x)$, δηλαδή $a(x)\big|f(x)$.

b. Επειδή $b(x)\big|f(x)$ έχουμε $a(x)b(x)\big|f(x)g(x)a(x)$. Επειδή $a(x)\big|f(x)$ έχουμε $a(x)b(x)\big|f(x)h(x)b(x)$. Άρα $a(x)b(x)\big|f(x)g(x)a(x)+f(x)h(x)b(x)$, δηλαδή $a(x)b(x)\big|f(x)$.

c. Επειδή $\text{μκδ}(a(x),b(x)f(x))\big|a(x)$ και $\text{μκδ}(a(x),b(x)f(x))\big|b(x)f(x)$, από την (1) έπεται ότι $\text{μκδ}(a(x),b(x)f(x))\big|f(x)$. [Σημείωση: Θα μπορούσαμε να φτάσουμε στο ίδιο συμπέρασμα εφαρμόζοντας το a.]

Επειδή $\text{μκδ}(a(x),b(x)f(x)\big|a(x)$ και $\text{μκδ}(a(x),b(x)f(x))\big|f(x)$, παίρνουμε $\text{μκδ}(a(x),b(x)f(x))\big|\text{μκδ}(a(x),f(x))$.

Έχουμε $\text{μκδ}(a(x),f(x))\big|f(x)$, οπότε $\text{μκδ}(a(x),f(x))\big|b(x)f(x)$. Από $\text{μκδ}(a(x),f(x))\big|a(x)$ και $\text{μκδ}(a(x),f(x))\big|b(x)f(x)$ έπεται ότι $\text{μκδ}(a(x),f(x)\big|\text{μκδ}(a(x),b(x)f(x))$.

Τελικά έχουμε $\text{μκδ}(a(x),b(x)f(x))\big|\text{μκδ}(a(x),f(x))$ και $\text{μκδ}(a(x),f(x))\big|\text{μκδ}(a(x),b(x)f(x))$. Επειδή τα πολυώνυμα $\text{μκδ}(a(x),b(x)f(x))$ και $\text{μκδ}(a(x),f(x))$ είναι μονικά και το F είναι περιοχή παίρνουμε $\text{μκδ}(a(x),b(x)f(x))=\text{μκδ}(a(x),f(x))$.

[Σημείωση. Καλό είναι να συγκριθούν τα παραπάνω με την άσκηση 1.2]

d. Έστω $d(x)=\mu\kappa\delta(a(x)b(x),f(x))$, $d_1(x)=\mu\kappa\delta(a(x),f(x))$, $d_2(x)=\mu\kappa\delta(b(x),f(x))$. Έχουμε $d_1(x)\big|a(x)$ και $d_1(x)\big|f(x)$, άρα $d_1(x)\big|a(x)b(x)$ και $d_1(x)\big|f(x)$. Συνεπώς $d_1(x)\big|d(x)$.

Όμοια αποδεικνύεται ότι $d_2(x)\big|d(x)$.

Επειδή $d_1(x)\big|a(x)$, $d_2(x)\big|b(x)$ και $\mu\kappa\delta(a(x),b(x))=1$, έχουμε $\mu\kappa\delta(d_1(x),d_2(x))=1$. Από το υποερώτημα b. έπεται ότι

$$d_1(x)d_2(x)\big|d(x).$$

Επειδή $d(x)\big|a(x)b(x)$, έχουμε $d(x)=d_a(x)d_b(x)$, όπου $d_a(x)\big|a(x)$ και $d_b(x)\big|b(x)$. Επειδή $d(x)\big|f(x)$ έχουμε $d_a(x)\big|f(x)$. Άρα $d_a(x)\big|d_1(x)$. Όμοια $d_b(x)\big|d_2(x)$. Συνεπώς $d_a(x)d_b(x)\big|d_1(x)d_2(x)$, δηλαδή

$$d(x)\big|d_1(x)d_2(x).$$

Από $d_1(x)d_2(x)\big|d(x)$, $d(x)\big|d_1(x)d_2(x)$ και το γεγονός ότι τα $d(x),d_1(x)d_2(x)$ είναι μονικά παίρνουμε $d(x)=d_1(x)d_2(x)$ αφού το F είναι περιοχή.

7.

a. Ο $\mu\kappa\delta(f(x),x^2+1)$ διαιρεί το x^2+1. Επειδή το $x^2+1\in\mathbb{R}[x]$ είναι ανάγωγο και μονικό, από $\mu\kappa\delta(f(x),x^2+1)\neq 1$ έπεται ότι $\mu\kappa\delta(f(x),x^2+1)=x^2+1$. Άρα $x^2+1\big|f(x)$.

Έχουμε $x^2-3x+2=(x-1)(x-2)$. Από τη σχέση $\deg\mu\kappa\delta(f(x),x^2-3x+2)=1$ έπεται ότι ισχύει ακριβώς μία από τις εξής σχέσεις

$$\mu\kappa\delta(f(x),x^2-3x+2)=x-1 \text{ ή } \mu\kappa\delta(f(x),x^2-3x+2)=x-2,$$

οπότε $x-1\big|f(x)$ ή $x-2\big|f(x)$. Επειδή το x^2+1 είναι σχετικά πρώτο με καθένα από τα $x-1,x-2$ παίρνουμε $(x^2+1)(x-1)\big|f(x)$ ή $(x^2+1)(x-2)\big|f(x)$. Επειδή το $f(x)$ είναι βαθμού 3 και μονικό έχουμε τελικά $f(x)=(x^2+1)(x-1)$ ή $f(x)=(x^2+1)(x-2)$.

b. Απάντηση: $p(x)=q(x)=x^2+x+1$.

8.

Αν $\rho = 1+\sqrt{1+\sqrt{2}}$, τότε

$$(\rho-1)^2 = 1+\sqrt{2} \Rightarrow \rho^2 - 2\rho = \sqrt{2} \Rightarrow \rho^4 - 4\rho^3 + 4\rho^2 = 2 \Rightarrow \rho^4 - 4\rho^3 + 4\rho^2 - 2 = 0.$$

Το ρ είναι ρίζα του $x^4 - 4x^3 + 4x^2 - 2 \in \mathbb{Q}[x]$.

9.

Υπόδειξη: Δείξτε ότι $x-k \mid f(x)$ για κάθε $k = 0,1,...,2013$.

Απάντηση: $f(x) = cx(x-1)....(x-2013), c \in \mathbb{Z}$.

10.

Έστω $f(x) \in \mathbb{Z}[x]$ τέτοιο ώστε για κάθε $m \in \mathbb{Z}$ το $f(m)$ είναι πρώτος αριθμός. Έστω $m \in \mathbb{Z}$ και $f(m) = p$ πρώτος. Για κάθε $k \in \mathbb{Z}$ έχουμε $m + kp \equiv m \bmod p$ και άρα $f(m+kp) \equiv f(m) \equiv 0 \bmod p$ (Πρόταση 1.3.4). Αλλά ο ακέραιος $f(m+kp)$ είναι πρώτος. Συνεπώς από $f(m+kp) \equiv 0 \bmod p$ έπεται ότι $f(m+kp) = p$. Δηλαδή το πολυώνυμο $f(x) - p \in \mathbb{Z}[x]$ έχει άπειρες ρίζες. Άρα $f(x) = p$.

11.

a. Υπόδειξη: Η απόδειξη είναι όμοια με την απόδειξη του Ευκλείδη ότι υπάρχουν άπειροι πρώτοι.

b. Έστω ότι υπάρχει $n \in \mathbb{N}$ τέτοιο ώστε κάθε ανάγωγο πολυώνυμο του $F[x]$ έχει βαθμό μικρότερο του n. Επειδή το F είναι πεπερασμένο, το σύνολο $\{f(x) \in F[x] \mid \deg f(x) < n\}$ είναι πεπερασμένο. Άρα το σύνολο των αναγώγων πολυωνύμων του $F[x]$ είναι πεπερασμένο. Επίσης είναι μη κενό (πχ περιέχει το πολυώνυμο x). Έστω ότι το σύνολο των αναγώγων πολυωνύμων του $F[x]$ είναι το $\{p_1(x),..., p_m(x)\}$. Το $P(x) = p_1(x)p_2(x)...p_m(x)+1$ είναι θετικού βαθμού και άρα διαιρείται με κάποιο ανάγωγο πολυώνυμο σύμφωνα με το Θεώρημα 2.3.10, δηλαδή για κάποιο j έχουμε $p_j(x) \mid P(x)$. Επειδή $p_j(x) \mid p_1(x)p_2(x)...p_m(x)$ παίρνουμε $p_j(x) \mid 1$, άτοπο.

12.

Υπόδειξη: Τροποποιήστε κατάλληλα την πρώτη λύση της άσκησης 1.11.

13.

a. και b. Βλ. Εφαρμογές 2.4.6 2 και 3.

c. Ο 101 είναι πρώτος και από το προηγούμενο υποερώτημα έχουμε $100! \equiv -1 \bmod 101$, δηλαδή

$$[1 \cdot 2 \cdot ... \cdot 98 \cdot 99 \cdot 100] = [-1]$$

στο $\mathbb{Z}_{101}$. Με τη βοήθεια του Ευκλείδειου αλγορίθμου βρίσκουμε ότι το αντίστροφο του $[99 \cdot 100] \in \mathbb{Z}_{101}$ είναι το $[-50]$. Πολλαπλασιάζοντας κατά μέλη παίρνουμε $[1 \cdot 2 \cdot ... \cdot 98 \cdot 99 \cdot 100][-50] = [-1][-50]$, δηλαδή $[1 \cdot 2 \cdot ... \cdot 98] = [50]$. Άρα το ζητούμενο υπόλοιπο είναι 50.

d. Υπόδειξη: Συγκρίνετε τους συντελεστές του x^{p-2} στην ισότητα του υποερωτήματος a.

14.

a. Από το Παράδειγμα 1.1.4 4 έχουμε $\zeta^n = \cos(2\pi) + i\sin(2\pi) = 1$. Άρα για κάθε $j = 0,1,...,n-1$, το ζ^j ικανοποιεί $\left(\zeta^j\right)^n = \left(\zeta^n\right)^j = 1$. Δηλαδή κάθε ζ^j είναι ρίζα του $x^n - 1$. Τα $\zeta^0, \zeta^1, ..., \zeta^{n-1}$ είναι διακεκριμένα (γιατί;). Επειδή το πλήθος τους είναι $n = \deg(x^n - 1)$ και το $\mathbb{C}$ είναι σώμα, έχουμε $x^n - 1 = u(x-\zeta^0)(x-\zeta^1)...(x-\zeta^{n-1})$ για κάποιο $u \in \mathbb{C}$. Συγκρίνοντας μεγιστοβάθμιους όρους στα δύο μέλη παίρνουμε $u = 1$.

b. Συγκρίνοντας τους συντελεστές του x^{n-2} στην ισότητα του υποερωτήματος a. παίρνουμε

$$0 = \sum_{0 \le i < j \le n-1} \zeta^{i+j}.$$

Από το Παράδειγμα 1.1.4 4 έχουμε $\zeta^{i+j} = \cos\frac{(i+j)2\pi}{n} + i\sin\frac{(i+j)2\pi}{n}$. Άρα

$$0 = \sum_{0\le i<j\le n-1} \cos\frac{(i+j)2\pi}{n} + i\sum_{0\le i<j\le n-1} \sin\frac{(i+j)2\pi}{n} \Rightarrow$$

$$0 = \sum_{0\le i<j\le n-1} \cos\frac{(i+j)2\pi}{n} = \sum_{0\le i<j\le n-1} \sin\frac{(i+j)2\pi}{n}.$$

15.

Έστω $f(x) = f_n x^n + ... + f_1 x + f_0 \in \mathbb{Z}_p[x]$. Ο δακτύλιος $\mathbb{Z}_p[x]$ είναι μεταθετικός και ισχύει $pr = 0$ για κάθε $r \in \mathbb{Z}_p[x]$. Από την άσκηση 3.18a των παίρνουμε

$$f(x)^p = \left(f_n x^n\right)^p + ... + \left(f_1 x\right)^p + {f_0}^p = {f_n}^p (x^p)^n + ... + {f_1}^p x^p + {f_0}^p.$$

Από το μικρό θεώρημα του Fermat έχουμε ${f_i}^p = f_i$ για κάθε i. Άρα

$$f(x)^p = f_n (x^p)^n + ... + f_1 x^p + f_0 = f(x^p).$$

16.

a. Παρατηρούμε ότι το $2 \in \mathbb{Z}_3$ είναι ρίζα του $x^3 + 2x^2 + 2 \in \mathbb{Z}_3[x]$ αφού $2^3 + 2\cdot 2^2 + 2 = 18 = 0$. Άρα το $x^3 + 2x^2 + 2$ διαιρείται με το $x - 2$ (Θεώρημα 2.4.1). Με την Ευκλείδεια διαίρεση βρίσκουμε $x^3 + 2x^2 + 2 = (x-2)(x^2 + x + 2)$. Τώρα το $g(x) = x^2 + x + 2 \in \mathbb{Z}_3[x]$ έχει βαθμό 2 και δεν έχει ρίζα στο $\mathbb{Z}_3$ αφού $g(0) = 2 \neq 0, g(1) = 4 \neq 0, g(2) = 8 = 2 \neq 0$. Άρα το $g(x) \in \mathbb{Z}_3[x]$ είναι ανάγωγο. Η ζητούμενη παραγοντοποίηση είναι $x^3 + 2x^2 + 2 = (x-2)(x^2 + x + 2)$.

b. Παρατηρούμε ότι $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ (που επαληθεύεται με άμεσο υπολογισμό ή έπεται από την άσκηση 17a των Ακήσεων3 ή από την άσκηση 15). Επειδή το $x^2 + x + 1 \in \mathbb{Z}_2[x]$ έχει βαθμό 2 και δεν έχει ρίζα στο $\mathbb{Z}_2$, είναι ανάγωγο στο $\mathbb{Z}_2[x]$. Η ζητούμενη παραγοντοποίηση είναι $x^4 + x^2 + 1 = (x^2 + x + 1)^2$.

c. Από το μικρό θεώρημα του Fermat έχουμε $a = a^p$ για κάθε $a \in \mathbb{Z}_p$. Άρα $x^p + a = x^p + a^p = (x + a)^p$ σύμφωνα με την άσκηση 3.18a ή την άσκηση 4.15. Η ζητούμενη παραγοντοποίηση είναι $x^p + a = (x + a)^p$.

d. Θα δείξουμε ότι το $x^2 + 1 \in \mathbb{Z}_p[x]$, όπου p πρώτος με $p \equiv 3 \bmod 4$, είναι ανάγωγο και για το σκοπό αυτό αρκεί να δείξουμε ότι δεν έχει ρίζα στο $\mathbb{Z}_p$ γιατί είναι βαθμού 2. Από την άσκηση 2.15 δεν υπάρχει $a \in \mathbb{Z}_p$ με $a^2 + 1 = 0$.

17.

Από την άσκηση 4.15 (ή την άσκηση 3.18a) έχουμε $x^{p^2} - x^p = \left(x^p - x\right)^p$ και από την άσκηση 4.13a έχουμε $x^p - x = x(x-1)(x-2)...(x-(p-1))$. Άρα η ζητούμενη ανάλυση είναι

$$x^{p^2} - x^p = x^p (x-1)^p (x-2)^p ... (x-(p-1))^p.$$

18.

Υπόδειξη: Με πράξεις εύκολα επαληθεύεται ότι το $x^4 + 2 \in \mathbb{Z}_5[x]$ δεν έχει ρίζα στο $\mathbb{Z}_5$. Άρα το $x^4 + 2 \in \mathbb{Z}_5[x]$ δεν έχει πρωτοβάθμιο παράγοντα στην ανάλυσή του σε γινόμενο αναγώγων. Αν δεν είναι ανάγωγο, τότε υπάρχουν $a, b, c, d \in \mathbb{Z}_5$ με $x^4 + 2 = (x^2 + ax + b)(x^2 + cx + d)$, δηλαδή

$$\begin{cases} a + c = 0 \\ b + d + ac = 0 \\ ad + bc = 0 \\ bd = 2. \end{cases}$$

Δείξτε ότι το σύστημα δεν έχει λύση.

19.

Έστω ότι υπάρχουν $a(x), b(x) \in \mathbb{Z}[x]$ θετικού βαθμού με

$$(x-1)(x-2)...(x-2011)-1 = a(x)b(x).$$

Τότε $\deg(a(x)b(x)) = 2011$ και άρα $\deg a(x) + \deg b(x) = 2011$ σύμφωνα με την Πρόταση 2.2.4 2. Άρα $\deg a(x) < 2011$ και $\deg b(x) < 2011$. Για κάθε $n = 1, 2, ..., 2011$ έχουμε $a(n)b(n) = -1$ και άρα $a(n), b(n) \in \{1, -1\}$. Επομένως $a(n) = -b(n)$ για κάθε $n = 1, 2, ..., 2011$. Άρα το πολυώνυμο $a(x) + b(x)$ έχει τουλάχιστον 2011 διακεκριμένες ρίζες. Επειδή $\deg a(x) < 2011$ και $\deg b(x) < 2011$ συμπεραίνουμε ότι $\deg(a(x) + b(x)) < 2011$, οπότε από το Πόρισμα 2.4.2 έχουμε $a(x) + b(x) = 0$. Τότε

$$(x-1)(x-2)...(x-2011)-1 = -a(x)^2.$$

Συγκρίνοντας μεγιστοβάθμιους όρους έχουμε άτοπο.

20.

Έστω $a \in \mathbb{Z}_p$. Θα δείξουμε με επαγωγή στο n ότι $a^{p^n} = a$ για κάθε $n \in \mathbb{Z}_{>0}$. Από το μικρό θεώρημα του Fermat έχουμε $a^p = a$. Έστω $n > 1$ και $a^{p^{n-1}} = a$. Τότε

$$a^{p^n} = \left(a^{p^{n-1}}\right)^p = a^p = a.$$

Συνεπώς η ζητούμενη επαγόμενη συνάρτηση είναι η μηδενική.

21.

b. ii Υπόδειξη: Αν το $a \in F$ είναι ρίζα του $f(x)$, δείξτε ότι και το $a + b$ είναι ρίζα του $f(x)$ για κάθε $b \in \mathbb{Z}_p$.

22.

a. Από το μικρό θεώρημα του Fermat,

$$f(a) = (a^2 + a + 1)^p - (a^2 + a + 1) = (a^2 + a + 1) - (a^2 + a + 1) = 0$$

για κάθε $a \in \mathbb{Z}_p$. Άρα το $f(x)$ διαιρείται με καθένα από τα $x, x-1, ..., x-(p-1)$. Επειδή αυτά είναι ανά δύο σχετικά πρώτα, το $f(x)$ διαιρείται με το $x(x-1)...(x-(p-1))$ που ισούται με $x^p - x$ (άσκηση 4.13a).

$2^{ος}$ τρόπος. Από την άσκηση 4.15 έχουμε

$$f(x) = x^{2p} + x^p + 1 - x^2 - x - 1 = (x^p - x)(x^p + x) + x^p - x = (x^p - x)(x^p + x + 1).$$

b. Για $p = 2$ έχουμε

$$f(x) = (x^2 - x)(x^2 + x + 1) = x(x-1)(x^2 + x + 1).$$

Τα $x, x-1 \in \mathbb{Z}_2[x]$ είναι ανάγωγα (ως πρωτοβάθμια σε δακτύλιο της μορφής $R[x]$, όπου R περιοχή). Το $x^2 + x + 1 \in \mathbb{Z}_2[x]$ είναι ανάγωγο γιατί είναι δευτέρου βαθμού και δεν έχει ρίζα στο σώμα $\mathbb{Z}_2$ (Πρόταση 2.4.5).

Για $p = 3$ έχουμε

$$f(x) = (x^3 - x)(x^3 + x + 1) = x(x-1)(x+1)(x^3 + x + 1).$$

Το 1 είναι ρίζα του $x^3 + x + 1 \in \mathbb{Z}_3[x]$ οπότε διαιρώντας με το $x-1$ βρίσκουμε $x^3 + x + 1 = (x-1)(x^2 + x + 2)$. Το $x^2 + x + 2 \in \mathbb{Z}_3[x]$ είναι ανάγωγο γιατί είναι δευτέρου βαθμού και δεν έχει ρίζα στο σώμα $\mathbb{Z}_3$ (Πρόταση 2.4.5). Τελικά η ζητούμενη παραγοντοποίηση είναι $f(x) = x(x-1)^2(x+1)(x^2 + x + 2)$.

23.

Απάντηση: $(x-1)(x-2)...(x-(p-1))^2$.

24.

Απάντηση: Το υπόλοιπο είναι $x-2$ και ο μκδ είναι 1.

25.

Βλ. Παράδειγμα 2.3.11 1).

26.

Βλ. Παράδειγμα 2.3.11 2).

27.

Απάντηση: $f(x)=(x^3+x+1)(x+1)g(x)$, όπου $g(x)\in\mathbb{Z}_2[x]$ με $\deg g(x)=3$.

28.

a. Απάντηση: Ο μκδ είναι $x-1$. $x^{2011}-1=(x^{2010}+x^{2009}+...+1)g(x)+(x^{2010}+x^{2009}+...+1)(-x^4-1)f(x)$.

29.

Έστω

$$A=\left\{f(x)=x^2+ax+b\in\mathbb{Z}_p[x]\right\},$$

$$B=\left\{f(x)=x^2+ax+b\in\mathbb{Z}_p[x]\middle| f(x)\ \acute{o}\chi\iota\ \alpha\nu\acute{\alpha}\gamma\omega\gamma o\right\},$$

$$C=\left\{f(x)=x^2+ax+b\in\mathbb{Z}_p[x]\middle\| f(x)\ \alpha\nu\acute{\alpha}\gamma\omega\gamma o\right\}.$$

Τότε $|C|=|A|-|B|$. Έχουμε $|A|=p^2$. Επειδή $f(x)\in B\Leftrightarrow f(x)=(x-r)(x-s),\ r,s\in\mathbb{Z}_p$ (Πρόταση 2.4.5), έχουμε $|B|=\frac{p(p+1)}{2}$. Άρα $|C|=p^2-\frac{p(p+1)}{2}=\frac{p(p-1)}{2}$.

30.

a. Απάντηση: Τα ανάγωγα πολυώνυμα του $\mathbb{Z}_2[x]$ βαθμού ≤ 4 είναι τα ακόλουθα:

$$x,\ x+1$$

$$x^2+x+1,$$

$$x^3+x+1,\ x^3+x^2+1$$

$$x^4+x^3+1,\ x^4+x+1,\ x^4+x^3+x^2+x+1.$$

b. Αν το $f(x)$ δεν έχει ρίζα στο $\mathbb{Z}_2[x]$, τότε θεωρώντας βαθμούς συμπεραίνουμε ότι το $f(x)$ είναι ανάγωγο αν και μόνο αν δεν έχει δευτεροβάθμιο ανάγωγο παράγοντα. Αλλά υπάρχει μοναδικό δευτεροβάθμιο ανάγωγο πολυώνυμο σύμφωνα με το a., το x^2+x+1.

c. Το x^5+x^4+1 δεν είναι ανάγωγο, $x^5+x^4+1=(x^2+x+1)(x^3+x+1)$.

31.

Με την Ευκλείδεια διαίρεση βρίσκουμε $f(x)=xg(x)+n(x-1)^2$, όπου $f(x)=x^{n+1}-(n+1)x+n$, $g(x)=x^n-nx+n-1$, και συνεπώς ο ζητούμενος μκδ ισούται με τον μκδ$(g(x),(x-1)^2)$. Ο τελευταίος ισούται με $(x-1)^2$ γιατί εύκολα επαληθεύεται ότι το 1 είναι ρίζα του $g(x)$ και της παραγώγου του $g(x)$.

32.

Έστω $a\in\mathbb{C}$ ρίζα του x^2+x+1. Τότε $a\in\mathbb{C}-\mathbb{R}$ και από $x^3-1=(x-1)(x^2+x+1)$ έχουμε $a^3=1$.

Έστω $f(x)=(x+1)^n+x^n+1$. Επειδή $x^2+x+1=(x-a)(x-\bar{a})$ και $a\neq\bar{a}$, έχουμε $x^2+x+1\big|f(x)$ στο $\mathbb{C}[x]$ $\Leftrightarrow f(a)=f(\bar{a})=0$. Από την άσκηση 4.5, έχουμε $x^2+x+1\big|f(x)$ στο $\mathbb{C}[x]\ \Leftrightarrow\ x^2+x+1\big|f(x)$ στο $\mathbb{R}[x]$.

Επειδή $f(x)\in\mathbb{R}[x]$, έχουμε $f(a)=f(\bar{a})=0\Leftrightarrow f(a)=0$ (Θεώρημα 2.4.10). Συνεπώς έχουμε

$$x^2+x+1\big|f(x)\ \text{στο}\ \mathbb{R}[x]\Leftrightarrow f(a)=0.$$

Εξετάζουμε πότε ισχύει $f(a)=0$. Έχουμε $a^2+a+1=0\Rightarrow a+1=-a^2$ οπότε

$$f(a)=(-1)^n a^{2n}+a^n+1.$$

- Αν $n=6k,\ k\in\mathbb{N}$, τότε $f(a)=(a^3)^{4k}+(a^3)^{2k}+1=1+1+1\neq 0$.

- Αν $n=6k+1, k\in\mathbb{N}$, τότε $f(a)=-(a^3)^{4k}a^2+(a^3)^{2k}a+1=-a^2+a+1=2a+2\neq 0$.
- Αν $n=6k+2, k\in\mathbb{N}$, τότε $f(a)=(a^3)^{4k}a^4+(a^3)^{2k}a^2+1=a+a^2+1=0$.
- Αν $n=6k+3, k\in\mathbb{N}$, τότε $f(a)=-(a^3)^{4k+2}+(a^3)^{2k+1}+1=-1+1+1\neq 0$.
- Αν $n=6k+4, k\in\mathbb{N}$, τότε $f(a)=(a^3)^{4k+2}a^2+(a^3)^{2k+1}a+1=a^2+a+1=0$.
- Αν $n=6k+5, k\in\mathbb{N}$, τότε $f(a)=-(a^3)^{4k+3}a+(a^3)^{2k+1}a^2+1=-a+a^2+1=-2a\neq 0$.

Άρα $f(a)=0\Leftrightarrow n\equiv 2,4 \bmod 6$.

33.

Έστω ότι $f(x),g(x)\in\mathbb{R}[x]$ ικανοποιούν τη δοσμένη σχέση. Αρχικά παρατηρούμε ότι τα $f(x),g(x)$ είναι σχετικά πρώτα.

Θεωρώντας την αρχική σχέση για $x-1$ στη θέση του x και αφαιρώντας κατά μέλη παίρνουμε

$$f(x)(g(x+1)+g(x-1))=g(x)(f(x+1)+f(x-1)).$$

Άρα το $f(x)$ διαιρεί το $g(x)(f(x+1)+f(x-1))$ και επειδή τα $f(x),g(x)$ είναι σχετικά πρώτα υπάρχει $h(x)\in\mathbb{R}[x]$ με

$$f(x+1)+f(x-1)=h(x)f(x).$$

Συγκρίνοντας μεγιστοβάθμιους όρους στην τελευταία σχέση προκύπτει $h(x)=2$. Συνεπώς

$$f(x+1)-f(x)=f(x)-f(x-1).$$

Από αυτό έπεται ότι το πολυώνυμο $f(x)-f(x-1)$ παίρνει την ίδια τιμή για $x=1,2,3,...$ και συνεπώς είναι σταθερό πολυώνυμο, $f(x)-f(x-1)=b\in\mathbb{R}$. Από την τελευταία σχέση έχουμε

$$f(1)=f(0)+b,$$
$$f(2)=f(1)+c=f(0)+2b,$$
$$f(3)=f(2)+c=f(0)+3b,$$
κλπ

δηλαδή $f(m)=f(0)+mb$, $m=1,2,3,...$. Άρα $f(x)=f(0)+bx$. Δηλαδή $f(x)=a+bx, a,b\in\mathbb{R}$.

Με παρόμοιο τρόπο προκύπτει $g(x)=c+dx$, $c,d\in\mathbb{R}$.

Αντικαθιστώντας στην αρχική σχέση παίρνουμε μετά από πράξεις $ad-bc=1$.

Μέχρι στιγμής δείξαμε ότι αν τα $f(x),g(x)$ ικανοποιούν την αρχική σχέση, τότε $f(x)=a+bx$, $g(x)=c+dx$ και $ad-bc=1$. Το αντίστροφο επαληθεύεται άμεσα.

34.

Υπόδειξη: Θεωρήστε το πολυώνυμο

$$(x-a)(x-b)(x-c)=x^3-(a+b+c)x^2+(ab+ac+bc)x-abc=x^3-6x^2+11x-6$$

και παρατηρήστε ότι το 1 είναι ρίζα του.

Απάντηση: Υπάρχουν 6 λύσεις που προκύπτουν από τις μεταθέσεις της λύσης (1,2,3).

35.

Υπόδειξη: Δείξτε ότι από την υπόθεση έπεται ότι υπάρχουν διακεκριμένοι ακέραιοι a_1,a_2,a_3,a_4 και $g(x)\in\mathbb{Z}[x]$ με $f(x)-7=(x-a_1)(x-a_2)(x-a_3)(x-a_4)g(x)$. Αν υπάρχει $n\in\mathbb{Z}$ με $f(n)=14$, τότε

$$7=(n-a_1)(n-a_2)(n-a_3)(n-a_4)g(n).$$

Δείξτε ότι η τελευταία σχέση οδηγεί σε άτοπο.

36. Απαντήσεις:

a. Σ
b. Λ
c. Σ
d. Λ
e. Σ
f. Λ

g. Σ
h. Λ
i. Σ
j. Λ
k. Σ
l. Σ.

Ασκήσεις5
Ομομορφισμοί και ιδεώδη

1. Δείξτε ότι οι δακτύλιοι R και S είναι ισόμορφοι στις ακόλουθες περιπτώσεις .

a. $R=\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\in M_2(\mathbb{R})\middle| a,b\in\mathbb{R}\right\}$, $S=\mathbb{C}$.

b. $R=\left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\in M_2(\mathbb{Z})\middle| a,b\in\mathbb{Z}\right\}$, $S=\mathbb{Z}\times\mathbb{Z}$.

c. $R=\mathbb{Z}[\sqrt{2}]=\left\{a+b\sqrt{2}\in\mathbb{R}\middle| a,b\in\mathbb{Z}\right\}$, $S=\left\{\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}\in M_2(\mathbb{Z})\middle| a,b\in\mathbb{Z}\right\}$

d. $R=\mathbb{Z}_{mn}$, $S=\mathbb{Z}_m\times\mathbb{Z}_n$, όπου $\mu\kappa\delta(m,n)=1$.

2. Δείξτε ότι οι δακτύλιοι R και S δεν είναι ισόμορφοι στις ακόλουθες περιπτώσεις .

a. $R=\mathbb{C}$, $S=\mathbb{R}$.

b. $R=\mathbb{Z}[\sqrt{2}]$, $S=\mathbb{Z}[\sqrt{3}]$.

c. $R=2\mathbb{Z}$, $S=3\mathbb{Z}$.

3. Έστω $R\to S$ ένας επιμορφισμός δακτυλίων. Για κάθε μία από τις ακόλουθες ιδιότητες, δείξτε ότι αν ο R έχει την ιδιότητα, τότε και ο S έχει την ιδιότητα.

a. R έχει μοναδιαίο στοιχείο.

b. R είναι μεταθετικός.

4. Έστω R και S δυο ισόμορφοι δακτύλιοι. Για κάθε μία από τις ακόλουθες ιδιότητες, δείξτε ότι αν ο R έχει την ιδιότητα, τότε και ο S έχει την ιδιότητα.

a. R είναι περιοχή.

b. R είναι σώμα.

5. Για καθένα από τα παρακάτω ζεύγη δακτυλίων εξετάστε αν οι δακτύλιοι είναι ισόμορφοι.

a. $2\mathbb{Z},\mathbb{Z}$.

b. $\mathbb{R}\times\mathbb{R}$, $\mathbb{C}$

c. $\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\in M_2(\mathbb{Z})\middle| a\in\mathbb{Z}\right\}$, $\mathbb{Z}$.

d. $\left\{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}\in M_2(\mathbb{Z})\middle| b\in\mathbb{Z}\right\}$, $\mathbb{Z}$.

e. $\left\{\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}\in M_2(\mathbb{Z})\middle| a,b\in\mathbb{Z}\right\}$, $\left\{\begin{pmatrix} a & 2b \\ 2b & a \end{pmatrix}\in M_2(\mathbb{Z})\middle| a,b\in\mathbb{Z}\right\}$.

6. Έστω R και S δυο δακτύλιοι με μοναδιαία στοιχεία. Δείξτε ότι αν οι R και S είναι ισόμορφοι, τότε υπάρχει μια 1-1 και επί απεικόνιση $f:U(R)\to U(S)$ τέτοια ώστε $f(uv)=f(u)f(v)$ για κάθε $u,v\in U(R)$. Στη συνέχεια εξετάστε αν οι δακτύλιοι $\mathbb{Z}[x]$ και $\mathbb{Q}[x]$ είναι ισόμορφοι.

7. Για καθεμιά από τις ακόλουθες περιπτώσεις δείξτε ότι υπάρχει μοναδικός ισομορφισμός δακτυλίων $R\to R$.

a. $R=\mathbb{Z}$.

b. $R=\mathbb{Q}$.

c. * $R=\mathbb{R}$.

Αληθεύει ότι υπάρχει μοναδικός ισομορφισμός δακτυλίων $\mathbb{C}\to\mathbb{C}$;

8. Στις ακόλουθες περιπτώσεις βρείτε όλους τους ισομορφισμούς δακτυλίων $R\to R$.

a. $R=\mathbb{Z}[\sqrt{2}]$.

b. * $R=\mathbb{Z}_p[x]$, όπου p πρώτος.

9. Έστω $n\in\mathbb{N}, n>1,$ και p πρώτος. Δείξτε τα εξής.

a. Η απεικόνιση $\varphi:\mathbb{Z}_n\to\mathbb{Z}_n, \varphi(a)=2a$, είναι ομομορφισμός δακτυλίων αν και μόνο αν $n=2$.

b. Η απεικόνιση $\varphi:\mathbb{Z}_n\to\mathbb{Z}_n,\ \varphi(a)=a^2$, είναι ομομορφισμός δακτυλίων αν και μόνο αν $n=2$.

c. Η απεικόνιση $\varphi:\mathbb{Z}_p[x]\to\mathbb{Z}_p[x],\ \varphi(a)=a^p$, είναι μονομορφισμός δακτυλίων.

10. Να βρεθούν όλοι οι ομομορφισμοί δακτυλίων στις ακόλουθες περιπτώσεις και να υπολογιστούν οι πυρήνες τους.

a. $\mathbb{Z}_5\to\mathbb{Z}_3$.

b. $\mathbb{Z}_6\to\mathbb{Z}_3$.

c. $\mathbb{Z}\to\mathbb{Z}_3$.

11. Για καθεμιά από τις ακόλουθες περιπτώσεις εξετάστε αν το σύνολο I είναι ένα ιδεώδες του δακτυλίου R.

a. $I=\{f(x)\in\mathbb{Q}[x]\,|\,f(2)=0\},\ R=\mathbb{Q}[x]$.

b. $I=\{f(x)\in\mathbb{Q}[x]\,|\,f(2)=1\},\ R=\mathbb{Q}[x]$.

c. $I=\left\{\begin{pmatrix}0&b\\0&0\end{pmatrix}\in M_2(\mathbb{Z})\,|\,b\in\mathbb{Z}\right\},\ R=\left\{\begin{pmatrix}a&b\\0&c\end{pmatrix}\in M_2(\mathbb{Z})\,|\,a,b,c\in\mathbb{Z}\right\}$.

d. $I=\left\{\begin{pmatrix}0&b\\0&0\end{pmatrix}\in M_2(\mathbb{Z})\,|\,b\in\mathbb{Z}\right\},\ R=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in M_2(\mathbb{Z})\,|\,a,b,c,d\in\mathbb{Z}\right\}$.

e. $I=\left\{\begin{pmatrix}a&b\\0&0\end{pmatrix}\in M_2(\mathbb{Z})\,|\,a,b\in\mathbb{Z}\right\},\ R=\left\{\begin{pmatrix}a&b\\0&c\end{pmatrix}\in M_2(\mathbb{Z})\,|\,a,b,c\in\mathbb{Z}\right\}$.

f. $I=\left\{\begin{pmatrix}a&b\\0&0\end{pmatrix}\in M_2(\mathbb{Z})\,|\,a,b\in\mathbb{Z}\right\},\ R=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in M_2(\mathbb{Z})\,|\,a,b,c,d\in\mathbb{Z}\right\}$.

12.

a. Δείξτε ότι κάθε ιδεώδες του $\mathbb{Z}$ είναι κύριο.

b. Δείξτε ότι κάθε ιδεώδες του $F[x]$, όπου F σώμα, είναι κύριο.

c. Για τα ιδεώδη $\langle m\rangle,\langle n\rangle$ του $\mathbb{Z}$ δείξτε ότι $\langle m\rangle\subseteq\langle n\rangle$ αν και μόνο αν $n|m$.

d. Βρείτε όλα τα ιδεώδη I του $\mathbb{Z}$ τέτοια ώστε $20\mathbb{Z}\subseteq I\subseteq 2\mathbb{Z}$.

13. Στις ακόλουθες περιπτώσεις δίνεται ένα ιδεώδες I ενός δακτυλίου R. Εξετάστε αν υπάρχει $a\in I$ τέτοιο ώστε $I=\langle a\rangle$. Αν υπάρχει τέτοιο a, να βρεθεί ένα.

a. $I=\{24x+36y\,|\,x,y\in\mathbb{Z}\},\ R=\mathbb{Z}$.

b. $I=\{f(x)\in\mathbb{R}[x]\,|\,f(0)=f(2-3i)=0\},\ R=\mathbb{R}[x]$.

14. Έστω I,J δυο ιδεώδη ενός δακτυλίου R. Θέτουμε $I+J=\{a+b\,|\,a\in I,b\in J\}$ και

$IJ=\{a_1b_1+\ldots+a_nb_n\in R\,|\,a_i\in I,b\in J,n\in\mathbb{Z}_{>0}\}$.

a. Δείξτε ότι τα $I+J$, IJ και $I\cap J$ είναι ιδεώδη του R και ότι $IJ\subseteq I\cap J$.

b. Δείξτε ότι αν $R=\mathbb{Z}$, $I=\langle m\rangle$ και $J=\langle n\rangle$, όπου τουλάχιστον ένα από τα m,n είναι διάφορο του μηδενός, τότε

   i. $I+J=\langle d\rangle$, $d=\mu\kappa\delta(m,n)$,

   ii. $IJ=\langle mn\rangle$,

   iii. $I\cap J=\langle e\rangle$, $e=\varepsilon\kappa\pi(m,n)$.

c. Δείξτε με παράδειγμα ότι γενικά δεν αληθεύει ότι $IJ=I\cap J$.

d. Έστω ότι ο R έχει μοναδιαίο στοιχείο. Δείξτε ότι αν $I+J=R$, τότε $IJ=I\cap J$.

15.

a. Έστω F ένα σώμα. Δείξτε ότι τα μόνα ιδεώδη του F είναι τα $\{0_F\}$ και F.

b. Έστω R ένας μεταθετικός δακτύλιος με μονάδα $1_R \neq 0_R$. Δείξτε ότι αν τα μόνα ιδεώδη του R είναι τα $\{0_R\}$ και R, τότε ο R είναι σώμα.

16. * Έστω F ένα σώμα και $R = M_n(F)$. Δείτε ότι τα μόνα ιδεώδη του R είναι τα $\{0_R\}$ και R.

17. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο.

a. * Δείξτε ότι κάθε ιδεώδες I του $M_n(R)$ είναι της μορφής $I = M_n(J)$, όπου J ιδεώδες του R.

b. Βρείτε όλα τα ιδεώδη του $M_n(\mathbb{Z})$.

c. Χρησιμοποιώντας το υποερώτημα a. δείξτε το συμπέρασμα της άσκησης 5.16.

18.

a. Δείξτε ότι το σύνολο $I = \{xf(x) + 2g(x) | f(x), g(x) \in \mathbb{Z}[x]\}$ είναι ιδεώδες του $\mathbb{Z}[x]$ που δεν είναι κύριο.

b. Έστω $I \neq \{0\}$ ιδεώδες του $\mathbb{Z}[x]$ και n ο ελάχιστος φυσικός αριθμός τέτοιος ώστε υπάρχει $f(x) \in I$ βαθμού n. Δείξτε ότι αν το I περιέχει μονικό πολυώνυμο βαθμού n, τότε το I είναι κύριο.

19. Έστω R ένας μεταθετικός δακτύλιος, I ένα ιδεώδες του R και $\sqrt{I} = \{r \in R | r^n \in I, n \in \mathbb{Z}_{>0}\}$.

a. Δείξτε ότι το $\sqrt{I}$ είναι ένα ιδεώδες του R.

b. Έστω $R = \mathbb{Z}_{12}$ και $I = \langle [4] \rangle$. Βρείτε το $\sqrt{I}$.

c. Έστω $R = \mathbb{Z}_m$ και $I = \{[0]\}$. Δείξτε ότι αν $m = p_1^{m_1} .... p_k^{m_k}$, όπου p_i είναι διακεκριμένοι πρώτοι και $m_i \in \mathbb{Z}_{>0}$, τότε $\sqrt{I} = \langle [p_1 ... p_k] \rangle$.

d. Δείξτε ότι το I είναι ένα ιδεώδες του δακτυλίου $\sqrt{I}$ και ότι $\sqrt{I}/I = \{r + I \in R/I | (r+I)^n = I, n \in \mathbb{Z}_{>0}\}$.

20. Έστω R ένας δακτύλιος και I ένα ιδεώδες του R.

a. Δείξτε ότι ο R/I είναι μεταθετικός αν και μόνο αν $ab - ba \in I$ για κάθε $a, b \in R$.

b. Δείξτε ότι αν υπάρχουν $a, b \in R$ τέτοια ώστε $ab \in I$, $a \notin I$ και $b \notin I$, τότε ο R/I δεν είναι περιοχή.

21.

a. Δείξτε ότι το ο δακτύλιος πηλίκο $\mathbb{Z}_2[x]/I$, όπου $I = \langle x^2 + x + 1 \rangle$, είναι σώμα με 4 στοιχεία.

b. Αληθεύει ότι ο δακτύλιος πηλίκο $\mathbb{Z}_2[x]/J$, όπου $J = \langle x^2 + 1 \rangle$, είναι σώμα;

22. Θεωρούμε το πολυώνυμο $x^2 + 1 \in \mathbb{Z}_3[x]$ και το ιδεώδες $I = \langle x^2 + 1 \rangle$ του $\mathbb{Z}_3[x]$.

a. Δείξτε ότι ο δακτύλιος πηλίκο $\mathbb{Z}_3[x]/I$ είναι ένα σώμα με 9 στοιχεία.

b. Εξετάστε αν τα στοιχεία $(x^4 + x + 1) + I$, $(x^4 + 2) + I$ του $\mathbb{Z}_3[x]/I$ είναι αντιστρέψιμα και βρείτε τα αντίστροφά τους, αν υπάρχουν.

23. Έστω F ένα σώμα και $f(x), g(x) \in F[x]$. Δείξτε ότι οι ακόλουθες προτάσεις είναι ισοδύναμες.

a. $\mu\kappa\delta(f(x), g(x)) = 1$.

b. Το $f(x) + \langle g(x) \rangle \in F[x]/\langle g(x) \rangle$ είναι αντιστρέψιμο.

c. Το $g(x) + \langle f(x) \rangle \in F[x]/\langle f(x) \rangle$ είναι αντιστρέψιμο.

24. (Το συμπέρασμα στο b. είναι γνωστό ως το **Κινεζικό Θεώρημα Υπολοίπων**) Έστω R ένας δακτύλιος και I, J ιδεώδη του R.

a. Δείξτε ότι υπάρχει μονομορφισμός δακτυλίων $R/I \cap J \to R/I \times R/J$.

b. Δείξτε ότι αν $I + J = R$, τότε υπάρχει ισομορφισμός δακτυλίων $R/I \cap J \to R/I \times R/J$.

c. Αν $R = \mathbb{Z}$, $I = \langle m \rangle$, $J = \langle n \rangle$ με $\mu\kappa\delta(m, n) = 1$, τότε υπάρχει ισομορφισμός δακτυλίων $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$.

25. Θεωρούμε τους δακτυλίους $R = \dfrac{\mathbb{Z}_5[x]}{\langle x^2 + 2 \rangle}$ και $S = \dfrac{\mathbb{Z}_5[x]}{\langle x^2 + 1 \rangle}$.

a. Δείξτε ότι ο R είναι σώμα και ότι ο S δεν είναι ακέραια περιοχή.
b. Αληθεύει ότι οι δακτύλιοι R και $\mathbb{Z}_5 \times \mathbb{Z}_5$ είναι ισόμορφοι; Αληθεύει ότι οι δακτύλιοι S και $\mathbb{Z}_5 \times \mathbb{Z}_5$ είναι ισόμορφοι;
c. Πόσα στοιχεία έχει ο R ; Πόσα από τα στοιχεία του S είναι αντιστρέψιμα;

26. Έστω p πρώτος, $p > 2$. Δείξτε ότι αν οι δακτύλιοι $\dfrac{\mathbb{Z}_p[x]}{\langle x^2+1\rangle}$ και $\mathbb{Z}_p \times \mathbb{Z}_p$ είναι ισόμορφοι, τότε $p \equiv 1 \bmod 4$. Μπορείτε να αποδείξετε το αντίστροφο;

27. Θεωρούμε το δακτύλιο $R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{Z}) \middle| a,b,c \in \mathbb{Z} \right\}$ και το ιδεώδες $I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a,b \in \mathbb{Z} \right\}$ του R . Δείξτε ότι υπάρχει ισομορφισμός δακτυλίων $R/I \simeq \mathbb{Z}$.

28. Δείξτε ότι οι δακτύλιοι $\mathbb{R}[x]/\langle x^3 \rangle$ και $\left\{ \begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} \in M_3(\mathbb{R}) \middle| a,b,c \in \mathbb{R} \right\}$ είναι ισόμορφοι.

29. Θεωρούμε το ιδεώδες $I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) \middle| b \in \mathbb{Z} \right\}$ του δακτυλίου $R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{Z}) \middle| a,b,c \in \mathbb{Z} \right\}$. Δείξτε ότι υπάρχει ισομορφισμός δακτυλίων $R/I \simeq \mathbb{Z} \times \mathbb{Z}$.

30. Αποδείξτε ότι υπάρχουν ισομορφισμοί δακτυλίων
a. $\mathbb{Q}[x]/\langle x^2-1 \rangle \simeq \mathbb{Q} \times \mathbb{Q}$.
b. $\mathbb{Q}[x]/\langle x^2-2 \rangle \simeq \mathbb{Q}[\sqrt{2}]$, όπου $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{R} | a,b \in \mathbb{Q}\}$.

31. Έστω $a \in \mathbb{C}$ ρίζα του $x^3 - x - 1$ και $\mathbb{Q}[a] = \{ f(a) \in \mathbb{C} | f(x) \in \mathbb{Q}[x] \}$.
a. Δείξτε ότι το $x^3 - x - 1 \in \mathbb{Q}[x]$ είναι ανάγωγο.
b. Δείξτε ότι το $\mathbb{Q}[x]/\langle x^3 - x - 1 \rangle$ είναι σώμα ισόμορφο με το $\mathbb{Q}[a]$.
c. Βρείτε, αν υπάρχει, $f(x) \in \mathbb{Q}[x]$ με $x^6 f(x) - 1 \in \langle x^3 - x - 1 \rangle$.

32. Έστω $f(x) \in \mathbb{R}[x]$ ένα μονικό πολυώνυμο. Δείξτε ότι ο δακτύλιος πηλίκο $\mathbb{R}[x]/\langle f(x) \rangle$ είναι ισόμορφο με το σώμα $\mathbb{C}$ αν και μόνο αν $f(x) = x^2 + ax + b$ με $a^2 - 4b < 0$.

33. Έστω F σώμα και S περιοχή που δεν είναι σώμα. Δείξτε ότι κάθε επιμορφισμός δακτυλίων $F[x] \to S$ είναι ισομορφισμός.

34. Εξετάστε ποιες από τις ακόλουθες προτάσεις αληθεύουν. Δικαιολογήστε την απάντησή σας.
a. Αν $m,n \in \mathbb{Z}$ και $\mu\kappa\delta(m,n) = 1$, τότε κάθε ομομορφισμός δακτυλίων $\mathbb{Z}_m \to \mathbb{Z}_n$ είναι ο μηδενικός.
b. Κάθε μη μηδενικός ομομορφισμός δακτυλίων $F \to R$, όπου το F είναι σώμα, είναι μονομορφισμός.
c. Ο πυρήνας του ομομορφισμού δακτυλίων $f : \mathbb{R}[x] \to \mathbb{R}[x]$, $f(g(x)) = g(1-i)$ είναι το ιδεώδες $\langle x^2 - 2x + 2 \rangle$.
d. Υπάρχει δακτύλιος R και ομομορφισμός δακτυλίων $\mathbb{Q} \to R$ με πυρήνα το $\mathbb{Z}$.
e. Έστω $m,n \in \mathbb{N}$. Οι δακτύλιοι $m\mathbb{Z}$ και $n\mathbb{Z}$ είναι ισόμορφοι αν και μόνο αν $m = n$.
f. Έστω p πρώτος και $p(x) \in \mathbb{Z}_p[x]$ ένα ανάγωγο πολυώνυμο βαθμού n . Ο δακτύλιος $\mathbb{Z}_p[x]/\langle p(x) \rangle$ είναι ένα σώμα με p^n στοιχεία.
g. Ο δακτύλιος πηλίκο $\mathbb{R}[x]/\langle x^2 - 2 \rangle$ είναι σώμα.
h. Ο δακτύλιος πηλίκο $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$ είναι σώμα.
i. Αν R είναι δακτύλιος, S υποδακτύλιος του R και I ιδεώδες του R τέτοιο ώστε $I \subseteq S$, τότε το I είναι ιδεώδες του S .
j. Αν ο R είναι περιοχή, τότε για κάθε ιδεώδες I του R με $I \neq R$, ο δακτύλιος R/I είναι περιοχή.

Υποδείξεις/Απαντήσεις
Ασκήσεις5

1.
a. Βλέπε σελ. 126-7.
b. Είναι θέμα ρουτίνας να επαληθευτεί ότι η απεικόνιση $R \to S, \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mapsto (a,b)$ είναι ισομορφισμός δακτυλίων.
c. Βλέπε σελ. 134.
d. Βλέπε σελ. 132 Εφαρμογή.

2.
a. Βλ. Παράδειγμα 1 σελ. 134.
b. Βλ. Παράδειγμα 2 σελ. 134.
c. Έστω $\varphi : 2\mathbb{Z} \to 3\mathbb{Z}$ ένας ισομομρφισμός δακτυλίων. Έστω $\varphi(2) = a \in 3\mathbb{Z}$. Τότε $\varphi(4) = \varphi(2 \cdot 2) = 2\varphi(2) = 2a$. Επίσης $\varphi(4) = \varphi(2^2) = \varphi(2)^2 = a^2$. Άρα $2a = a^2$ οπότε $a = 0, 2$. Αλλά $2 \notin 3\mathbb{Z}$. Άρα $a = 0$. Τότε όμως ο φ δεν είναι μονομορφισμός καθώς $\varphi(0) = \varphi(2)$, άτοπο.

3.
a. Έστω $\varphi : R \to S$ ένας επιμορφισμός δακτυλίων και έστω ότι ο R έχει μοναδιαίο στοιχείο 1_R. Το $\varphi(1_R)$ είναι το μοναδιαίο στοιχείο του S. Πράγματι, έστω $s \in S$. Επειδή η απεικόνιση φ είναι επί, υπάρχει $r \in R$ με $s = \varphi(r)$. Τότε έχουμε $s\varphi(1_R) = \varphi(r)\varphi(1_R) = \varphi(r1_R) = \varphi(r) = s$. Όμοια $\varphi(1_R)s = s$.

4.
a. Έστω $\varphi : R \to S$ ισομορφισμός δακτυλίων και R περιοχή. Επειδή ο R έχει μοναδιαίο στοιχείο 1_R και είναι μεταθετικός, από την προηγούμενη άσκηση έπεται ότι ο S έχει μοναδιαίο στοιχείο το $1_S = \varphi(1_R)$ και είναι μεταθετικός.
Επειδή η απεικόνιση φ είναι 1-1 και ο δακτύλιος R είναι περιοχή, έχουμε
$0_R \neq 1_R \Rightarrow \varphi(0_R) \neq \varphi(1_R) \Rightarrow 0_S \neq 1_S$.
Έστω $s_1, s_2 \in S$ με $s_1 s_2 \in 0_S$. Επειδή η φ είναι επί υπάρχουν $r_1, r_2 \in R$ με $s_1 = \varphi(r_1), s_2 = \varphi(r_2)$. Τότε $0_S = s_1 s_2 = \varphi(r_1)\varphi(r_2) = \varphi(r_1 r_2) \Rightarrow r_1 r_2 = 0_R$ γιατί η φ είναι ομορφισμός και 1-1. Από την τελευταία ισότητα έπεται $r_1 = 0_R$ ή $r_2 = 0_R$ γιατί ο R είναι περιοχή. Άρα $s_1 = \varphi(0_R) = 0_S$ ή $s_2 = \varphi(0_R) = 0_S$.
Συνεπώς ο S είναι περιοχή.

5. Απαντήσεις:
a. Δεν είναι ισόμορφοι γιατί ο $2\mathbb{Z}$ δεν έχει μοναδιαίο στοιχείο ενώ ο $\mathbb{Z}$ έχει μοναδιαίο στοιχείο. Βλ. άσκηση 5.3a.
b. Δεν είναι ισόμορφοι γιατί ο $\mathbb{R} \times \mathbb{R}$ δεν είναι περιοχή (για παράδειγμα, έχουμε $(1,0)(0,1) = (0,0)$ ενώ $(1,0) \neq (0,0)$ και $(0,1) \neq (0,0)$) και ο $\mathbb{C}$ είναι περιοχή. Βλ. άσκηση 5.4a.
c. Η απεικόνιση $\left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) \middle| a \in \mathbb{Z} \right\} \to \mathbb{Z}, \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mapsto a$, είναι ισομορφισμός δακτυλίων.
d. Δεν είναι ισόμορφοι γιατί ο $\left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) \middle| b \in \mathbb{Z} \right\}$ δεν είναι περιοχή καθώς $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
Βλ. άσκηση 5.4a. (Επίσης, ο $\left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) \middle| b \in \mathbb{Z} \right\}$ δεν έχει μοναδιαίο στοιχείο. Βλ. άσκηση 5.3a.).
e. Βλ. Παράδειγμα 3 σελίδα 134.

6.

Υπόδειξη: Έστω $\varphi: R \to S$ ένας ισομορφισμός δακτυλίων. Δείξτε ότι αν $u \in U(R)$, τότε $\varphi(u) \in U(S)$. Συνεπώς ο περιορισμός στο $U(R)$ της απεικόνισης $\varphi: R \to S$ δίνει μια απεικόνιση $f: U(R) \to U(S), f(u) = \varphi(u)$, που είναι 1-1. Δείξτε ότι η f είναι επί.

Από την Πρόταση 2.2.4 3) έχουμε $U(\mathbb{Z}[x]) = \{1, -1\}$ και $U(\mathbb{Q}[x]) = \mathbb{Q} - \{0\}$. Το πρώτο σύνολο είναι πεπερασμένο, το δεύτερο άπειρο. Συνεπώς δεν υπάρχει 1-1 και επί απεικόνιση $U(\mathbb{Z}[x]) \to U(\mathbb{Q}[x])$, οπότε οι δακτύλιοι $\mathbb{Z}[x]$, $\mathbb{Q}[x]$ δεν είναι ισόμορφοι.

7.

a. Έστω $\varphi: \mathbb{Z} \to \mathbb{Z}$ ένας ισομορφισμός δακτυλίων. Τότε $\varphi(1) = 1$ (βλ. άσκηση 5.3a.). Άρα $\varphi(n) = n\varphi(1) = n$ για κάθε $n \in \mathbb{Z}$. Δηλαδή, η απεικόνιση $\varphi: \mathbb{Z} \to \mathbb{Z}$ είναι η ταυτοτική απεικόνιση.

b. Έστω $\varphi: \mathbb{Q} \to \mathbb{Q}$ ένας ισομορφισμός δακτυλίων. Τότε, όπως πριν, παίρνουμε $\varphi(n) = n$ για κάθε $n \in \mathbb{Z}$. Αν $n \in \mathbb{Z} - \{0\}$, τότε από $n\frac{1}{n} = 1$ παίρνουμε

$$\varphi\left(n\frac{1}{n}\right) = \varphi(1) \Rightarrow \varphi(n)\varphi\left(\frac{1}{n}\right) = \varphi(1) \Rightarrow n\varphi\left(\frac{1}{n}\right) = 1 \Rightarrow \varphi\left(\frac{1}{n}\right) = \frac{1}{n}.$$

Άρα, αν $m \in \mathbb{Z}$, τότε $\varphi\left(\frac{m}{n}\right) = \varphi\left(m\frac{1}{n}\right) = m\varphi\left(\frac{1}{n}\right) = m\frac{1}{n}$. Δηλαδή, η απεικόνιση $\varphi: \mathbb{Q} \to \mathbb{Q}$ είναι η ταυτοτική απεικόνιση.

c. Έστω $\varphi: \mathbb{R} \to \mathbb{R}$ ένας ισομορφισμός δακτυλίων. Όπως πριν παίρνουμε $\varphi(a) = a$ για κάθε $a \in \mathbb{Q}$.

Παρατήρηση: Αν $r, s \in \mathbb{R}$ με $r > s$, τότε $\varphi(r) > \varphi(s)$.

Πράγματι, από $r - s = \left(\sqrt{r-s}\right)^2$ έχουμε $\varphi(r-s) = \varphi\left(\left(\sqrt{r-s}\right)^2\right) = \left(\varphi\left(\sqrt{r-s}\right)\right)^2 \geq 0$. Επειδή ο φ είναι 1-1 και $r - s \neq 0$, έχουμε $\varphi(r-s) \neq \varphi(0) = 0$. Άρα $\varphi(r-s) > 0$, οπότε $\varphi(r) - \varphi(s) > 0$, δηλαδή $\varphi(r) > \varphi(s)$.

Έστω ότι υπάρχει $r \in \mathbb{R}$ με $r \neq \varphi(r)$.

- Αν $r > \varphi(r)$, τότε από την πυκνότητα του $\mathbb{Q}$ στο $\mathbb{R}$, υπάρχει $a \in \mathbb{Q}$ με $r > a > \varphi(r)$. Από την Παρατήρηση έχουμε $\varphi(r) > \varphi(a) = a$, άτοπο.
- Όμοια, αν $r < \varphi(r)$, τότε υπάρχει $a \in \mathbb{Q}$ με $\varphi(r) > a > r$. Από την Παρατήρηση, $\varphi(a) > \varphi(r) \Rightarrow a > \varphi(r)$, άτοπο.

Άρα $\varphi(r) = r$ για κάθε $r \in \mathbb{R}$, δηλαδή η απεικόνιση $\varphi: \mathbb{R} \to \mathbb{R}$ είναι η ταυτοτική απεικόνιση.

Η απεικόνιση $\mathbb{C} \to \mathbb{C}, a + bi \mapsto a - bi$, όπου $a, b \in \mathbb{R}$, είναι ισομορφισμός δακτυλίων (αποδείξτε το) και δεν είναι η ταυτοτική απεικόνιση.

8.

a. Η απεικόνιση $\psi: \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}], \psi(a + b\sqrt{2}) = a - b\sqrt{2}$, όπου $a, b \in \mathbb{Z}$, είναι ισομορφισμός δακτυλίων σύμφωνα με το Παράδειγμα 2.5.2 5. Θα δείξουμε ότι κάθε ισομορφισμός δακτυλίων $\mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ είναι ο ταυτοτικός ή ο ψ.

Έστω $\varphi: \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ ισομορφισμός δακτυλίων. Τότε $\varphi(1) = 1$ (βλ. άσκηση 5.3a) και επομένως για κάθε ακέραιο n, $\varphi(n) = n\varphi(1) = n$. Από τη σχέση $(\sqrt{2})^2 = 2$ έπεται ότι $\varphi((\sqrt{2})^2) = \varphi(2) \Rightarrow (\varphi(\sqrt{2}))^2 = 2$, δηλ. $\varphi(\sqrt{2}) = \sqrt{2}$ ή $\varphi(\sqrt{2}) = -\sqrt{2}$. Στην πρώτη περίπτωση η φ είναι η ταυτοτική απεικόνιση, αφού για κάθε $a, b \in \mathbb{Z}$,

$$\varphi(a + b\sqrt{2}) = \varphi(a) + \varphi(b\sqrt{2}) = \varphi(a) + b\varphi(\sqrt{2}) = a + b\sqrt{2},$$

και στη δεύτερη περίπτωση η φ είναι η ψ, αφού για κάθε $a, b \in \mathbb{Z}$,

$$\varphi(a + b\sqrt{2}) = \varphi(a) + \varphi(b\sqrt{2}) = \varphi(a) + b\varphi(\sqrt{2}) = a - b\sqrt{2} = \psi(a + b\sqrt{2}).$$

b. Έστω $a, b \in \mathbb{Z}_p$ με $a \neq 0_{\mathbb{Z}_p}$. Η απεικόνιση

$$\psi_{a,b}: \mathbb{Z}_p[x] \to \mathbb{Z}_p[x], f(x) \mapsto f(ax + b)$$

είναι ομομορφισμός δακτυλίων (αποδείξτε το). Καθώς το $\mathbb{Z}_p$ είναι σώμα, το a είναι αντιστρέψιμο. Εύκολα επαληθεύεται ότι

$$\psi_{a,b} \circ \psi_{a^{-1},-a^{-1}b} = \psi_{a^{-1},-a^{-1}b} \circ \psi_{a,b} = \text{ταυτοτική απεικόνιση στο } \mathbb{Z}_p[x].$$

Πράγματι, $\psi_{a,b} \circ \psi_{a^{-1},-a^{-1}b}(f(x)) = \psi_{a,b}(f(a^{-1}x - a^{-1}b)) = f(a(a^{-1}x - a^{-1}b) + b) = f(x)$ και όμοια η άλλη σχέση. Άρα η απεικόνιση $\psi_{a,b}$ είναι ισομορφισμός δακτυλίων. Θα δείξουμε τώρα ότι κάθε ισομορφισμός δακτυλίων $\mathbb{Z}_p[x] \to \mathbb{Z}_p[x]$ είναι ένας από τους $\psi_{a,b}$.

Έστω $\varphi : \mathbb{Z}_p[x] \to \mathbb{Z}_p[x]$ ισομορφισμός δακτυλίων. Τότε $\varphi(1_{\mathbb{Z}_p}) = 1_{\mathbb{Z}_p}$ (βλ. άσκηση 5.3a) και επομένως για κάθε ακέραιο n, $\varphi(n1_{\mathbb{Z}_p}) = n\varphi(1_{\mathbb{R}^{v\times v}}) = n1_{\mathbb{Z}_p}$, δηλαδή

$$\varphi(c) = c \text{ για κάθε } c \in \mathbb{Z}_p.$$

Παρατηρούμε ότι για κάθε $f(x) \in \mathbb{Z}_p[x]$ ισχύει $\varphi(f(x)) = f(\varphi(x))$, διότι αν $f(x) = c_n x^n + \ldots + c_1 x + c_0$, τότε

$$\begin{aligned}\varphi(f(x)) &= \varphi(c_n x^n) + \ldots + \varphi(c_1 x) + \varphi(c_0) = \\ &= \varphi(c_n)(\varphi(x^n)) + \ldots + \varphi(c_1)\varphi(x) + \varphi(c_0) = \\ &= c_n \varphi(x)^n + \ldots + c_1 \varphi(x) + c_0 = \\ &= f(\varphi(x)).\end{aligned}$$

Επειδή η απεικόνιση φ είναι επί, υπάρχει $g(x) \in \mathbb{Z}_p[x]$ με $\varphi(g(x)) = x$, δηλαδή $g(\varphi(x)) = x$ σύμφωνα με την προηγούμενη παρατήρηση. Λαμβάνοντας βαθμούς, η τελευταία σχέση δίνει $\deg g(x) \cdot \deg \varphi(x) = 1$ σύμφωνα με την Πρόταση 2.2.4 2 (το $\mathbb{Z}_p$ είναι περιοχή). Άρα $\deg \varphi(x) = 1$, δηλαδή $\varphi(x) = ax + b$ για κάποια $a, b \in \mathbb{Z}_p$ με $a \neq 0_{\mathbb{Z}_p}$. Έχουμε $\varphi = \psi_{a,b}$ αφού $\varphi(f(x)) = f(\varphi(x)) = f(ax + b) = \psi_{a,b}(f(x))$ για κάθε $f(x) \in \mathbb{Z}_p[x]$.

Σημείωση. Στην παραπάνω απόδειξη δεν χρησιμοποιήσαμε ότι η φ είναι 1-1 αλλά μόνο ότι είναι επιμορφισμός. Συνεπώς κάθε επιμορφισμός δακτυλίων $\mathbb{Z}_p[x] \to \mathbb{Z}_p[x]$ είναι ένας από τους $\psi_{a,b}$.

9.

a. Έστω ότι η απεικόνιση $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n, \varphi(a) = 2a$, είναι ομομορφισμός δακτυλίων. Τότε $[2] = \varphi([1]) = \varphi([1][1]) = \varphi([1])\varphi([1]) = [2][2] = [4]$. Άρα $[2] = [4] \Rightarrow [0] = [2] \Rightarrow n \mid 2$. Επειδή $n > 1$, παίρνουμε $n = 2$.

Αντίστροφα, αν $n = 2$, είναι άμεσο ότι η απεικόνιση $\varphi : \mathbb{Z}_2 \to \mathbb{Z}_2, \varphi(a) = 2a$ είναι ομομορφισμός δακτυλίων (ο μηδενικός).

b. Έστω ότι η απεικόνιση $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n, \varphi(a) = a^2$, είναι ομομορφισμός δακτυλίων. Τότε $[2] = [1] + [1] = \varphi([1]) + \varphi([1]) = \varphi([1] + [1]) = \varphi([2]) = [4]$. Άρα $[2] = [4]$ και όπως πριν έχουμε $n = 2$.

Αντίστροφα, αν $n = 2$, είναι άμεσο ότι η απεικόνιση $\varphi : \mathbb{Z}_2 \to \mathbb{Z}_2, \varphi(a) = a^2$ είναι ομομορφισμός δακτυλίων (ο ταυτοτικός).

c. Έστω $a, b \in \mathbb{Z}_p[x]$. Από την άσκηση 3.18a των Ασκήσεων3 έχουμε

$$\varphi(a + b) = (a + b)^p = a^p + b^p = \varphi(a) + \varphi(b).$$

Επειδή ο $\mathbb{Z}_p[x]$ είναι μεταθετικός, $(ab)^p = a^p b^p$. Άρα $\varphi(ab) = \varphi(a)\varphi(b)$.

Αν $\varphi(a) = 0$, τότε $a^p = 0 \Rightarrow a = 0$ γιατί ο $\mathbb{Z}_p[x]$ είναι περιοχή (Πρόταση 2.2.4 1)). Άρα $\ker \varphi = \{0\}$ και ο φ είναι 1-1 από την Πρόταση 2.5.4

10. Απάντηση:

a. Υπάρχει μόνο ο μηδενικός ομομορφισμός (που έχει πυρήνα το $\mathbb{Z}_5$).

b. Υπάρχουν μόνο δύο, ο μηδενικός ομομορφισμός (που έχει πυρήνα το $\mathbb{Z}_6$) και ο $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_3, \varphi([a]_6) = [a]_3$ (που έχει πυρήνα το $\{[0]_6, [3]_6\}$).

c. Υπάρχουν μόνο δύο, ο μηδενικός ομομορφισμός (που έχει πυρήνα το $\mathbb{Z}$) και ο $\varphi : \mathbb{Z} \to \mathbb{Z}_3, \varphi(a) = [a]$ (που έχει πυρήνα το $3\mathbb{Z}$).

11. Απάντηση
a. Ναι.
b. Όχι.
c. Ναι.
d. Όχι.
e. Ναι.
f. Όχι.

12.

a. Έστω I ένα ιδεώδες του $\mathbb{Z}$. Αν $I=\{0\}$, τότε $I=\langle 0\rangle$. Έστω $I\neq\{0\}$. Τότε υπάρχει $a\in\mathbb{Z}-\{0\}$ με $a\in I$. Επειδή το I είναι ιδεώδες έχουμε $-a\in I$ και άρα $I\cap\mathbb{Z}_{>0}\neq\varnothing$. Άρα το $I\cap\mathbb{Z}_{>0}$ έχει ελάχιστο στοιχείο, έστω a. Θα δείξουμε ότι $I=\langle a\rangle$. Η σχέση $\langle a\rangle\subseteq I$ είναι σαφής γιατί αν $b\in\langle a\rangle$, τότε $b=ca, c\in\mathbb{Z},$ και $ca\in I$ γιατί το I είναι ιδεώδες.
Έστω $d\in I$. Από την Ευκλείδεια διαίρεση υπάρχουν $q,r\in\mathbb{Z}$ με $d=qa+r, 0\leq r<a$. Έχουμε $r=d-qa.$ Από $a\in I$ έπεται ότι $qa\in I$ γιατί το I είναι ιδεώδες του $\mathbb{Z}$. Επειδή έχουμε και $d\in I$ συμπεραίνουμε ότι $r=d-qa\in I$. Επειδή $r<a$, ο ορισμός του a δίνει $r=0$, οπότε $d=qa\in\langle a\rangle$ Άρα $I\subseteq\langle a\rangle$. Συνεπώς $I=\langle a\rangle$.
b. Υπόδειξη: Τροποποιήστε κατάλληλα την προηγούμενη απόδειξη χρησιμοποιώντας τον αλγόριθμο διαίρεσης στο $F[x]$.
c. Άμεσο από τους ορισμούς.
d. Σύμφωνα με το a. έχουμε $I=\langle n\rangle$ για κάποιο $n\in\mathbb{N}$. Από $20\mathbb{Z}\subseteq I\subseteq 2\mathbb{Z}$, δηλαδή $\langle 20\rangle\subseteq I\subseteq\langle 2\rangle$, και το c. έχουμε $2|n$ και $n|20$. Άρα $n=2,4,10,20.$ Συνεπώς $I=\langle 2\rangle,\langle 4\rangle,\langle 10\rangle,\langle 20\rangle.$

13.
Από την προηγούμενη άσκηση ξέρουμε ότι υπάρχουν τέτοια a και στις δυο περιπτώσεις. Ανεξάρτητα από αυτό, μπορούμε να υπολογίσουμε τέτοια a.
a. Έστω $a=\mu\kappa\delta(24,36)=12$. Τότε $\langle a\rangle=I.$
Πράγματι, επειδή $12|24, 12|36$ έχουμε $12|24x+36y$ για κάθε $x,y\in\mathbb{Z}$. Άρα $I\subseteq\langle 12\rangle$. Από το Θεώρημα 1.2.4 έπεται ότι $12\in I$. Άρα $\langle 12\rangle\subseteq I$ γιατί το I είναι ιδεώδες. Συνεπώς $I=\langle 12\rangle$.
b. Έστω $f(x)=x(x^2-4x+13)\in\mathbb{R}[x].$ Θα δείξουμε ότι $I=\langle f(x)\rangle$.
Επειδή $f(0)=f(2-3i)=0$, έχουμε $f(x)\in I$. Αφού το I είναι ιδεώδες του $\mathbb{R}[x]$ έχουμε $\langle f(x)\rangle\subseteq I$.
Αντίστροφα, έστω $g(x)\in I$. Τότε $g(0)=g(2-3i)=0.$ Άρα $x|g(x)$ στο $\mathbb{R}[x]$. Από $g(2-3i)=0$ και $g(x)\in\mathbb{R}[x]$ έπεται ότι $g(2+3i)=0$ (Θεώρημα 2.4.10 1). Συνεπώς έχουμε $x-(2-3i)|g(x)$ στο $\mathbb{C}[x]$ και $x-(2+3i)|g(x)$ στο $\mathbb{C}[x]$. Επειδή τα πολυώνυμα $x, x-(2-3i), x-(2+3i)$ είναι ανά δύο σχετικά πρώτα, έχουμε $x(x-(2-3i))(x-(2+3i))|g(x)$ στο $\mathbb{C}[x]$, δηλαδή $f(x)|g(x)$ στο $\mathbb{C}[x]$. Επειδή $f(x),g(x)\in\mathbb{R}[x]$, από την άσκηση 4.5, έχουμε $f(x)|g(x)$ στο $\mathbb{R}[x]$, δηλαδή $g(x)\in\langle f(x)\rangle$. Άρα $I\subseteq\langle f(x)\rangle$. Συνεπώς $I=\langle f(x)\rangle$.

14. .
d. Από το a. έχουμε $IJ\subseteq I\cap J$, οπότε αρκεί να δείξουμε ότι $I\cap J\subseteq IJ$. Έστω $a\in I\cap J$. Τότε $a\in I$ και από την υπόθεση $I+J=R$ έπεται ότι $a+b=1$ για κάποιο $b\in J$. Τότε $a=a1=a(a+b)=a^2+ab$. Επειδή $a\in I$ και $a\in J$ έχουμε $a^2\in IJ$. Επειδή $a\in I$ και $b\in J$ έχουμε $ab\in IJ$. Άρα $a=a^2+ab\in IJ$.
Σημείωση: Στο βιβλίο, η άσκηση αυτή είναι η 18ii της Παραγράφου 2.5, αλλά η διατύπωση εκεί είναι λανθασμένη. Άσκηση: Βρείτε σχετικό αντιπαράδειγμα.

15.

a. Έστω I ένα μη μηδενικό ιδεώδες του σώματος F και $a \in I, a \neq 0$. Τότε $1 = aa^{-1} \in I$ γιατί το I είναι ιδεώδες και $a \in I$. Αν $b \in F$, τότε $b = b1 \in I$ γιατί το I είναι ιδεώδες και $1 \in I$. Άρα $F \subseteq I$ και συνεπώς $F = I$.

b. Έστω $a \in R, a \neq 0$. Τότε το ιδεώδες $\langle a \rangle$ του R είναι μη μηδενικό και άρα $\langle a \rangle = R$. Συνεπώς υπάρχει $b \in R$ με $ba = 1$. Επειδή ο R είναι μεταθετικός, έχουμε και $ab = 1$, οπότε το a είναι αντιστρέψιμο.

16.

Έστω $I \neq \{0\}$ ένα ιδεώδες του R. Θα δείξουμε ότι $I = R$. Έστω $A = (\alpha_{ij}) \in I$ με $A \neq 0$. Τότε $\alpha_{ke} \neq 0$ για κάποιους δείκτες k, ℓ. Έστω $E_{ij} \in R$ ο πίνακας του οποίου όλα τα στοιχεία είναι 0 εκτός από το στοιχείο στη θέση (i, j) που είναι ίσιο με 1. Υπενθυμίζουμε ότι

$$E_{ij}E_{pq} = \begin{cases} 0 & , \text{ αν } j \neq p \\ E_{iq}, & \text{ αν } j = p. \end{cases} \qquad (1)$$

Γράφοντας $A = \sum_{i,j} \alpha_{ij}E_{ij}$, από τη σχέση (1) παίρνουμε

$$E_{\ell k}AE_{\ell k} = \sum_{i,j} \alpha_{ij}(E_{\ell k}E_{ij})E_{\ell k} = \sum_{j} \alpha_{kj}E_{\ell j}E_{\ell k} = \alpha_{k\ell}E_{\ell k} \ .$$

Άρα

$$\alpha_{k\ell}E_{\ell k} \in I \qquad (2)$$

γιατί $A \in I$ και το I είναι ιδεώδες του R. Συνεπώς $E_{\ell k} = (\alpha_{k\ell}^{-1}E_{\ell\ell})(\alpha_{k\ell}E_{\ell k}) \in I$. Άρα έχουμε

$E_{ik} = E_{i\ell}E_{\ell k} \in I$ για κάθε i και άρα $E_{ii} = E_{ik}E_{ki} \in I$ για κάθε i. Τότε

$$1_R = E_{11} + \ldots + E_{nn} \in I \ .$$

Αν $B \in R$, τότε $B = B1_R \in I$ και επομένως $I = R$.

17.

a. Έστω I ένα ιδεώδες του $M_n(R)$. Έστω J το υποσύνολο του R που αποτελείται από τα $a \in R$ τέτοια ώστε υπάρχει πίνακας $A \in I$ του οποίου κάποιο στοιχείο είναι το a. Αρκεί να δείξουμε ότι

i. το J είναι ένα ιδεώδες του R και
ii. $I = M_n(J)$.

Για την απόδειξη του i., θα χρησιμοποιήσουμε την εξής παρατήρηση.

Παρατήρηση 1: Έστω $a \in J$ και $A \in I$ τέτοιο ώστε στη θέση (k, ℓ) του A υπάρχει το στοιχείο a. Τότε για κάθε i, j έχουμε $aE_{ij} \in I$.

Απόδειξη: Όπως ακριβώς στην απόδειξη της προηγούμενης άσκησης, έχουμε $aE_{\ell k} \in I$ (βλ. σχέση (2)).

Επειδή το I είναι ιδεώδες του $M_n(R)$, για κάθε i, j έχουμε $E_{i\ell}(rE_{\ell k})E_{kj} \in I$, δηλαδή $rE_{ij} \in I$.

Απόδειξη του i.: Επειδή το I είναι ιδεώδες του $M_n(R)$, το I περιέχει το μηδενικό πίνακα. Άρα $0_R \in J$ και $J \neq \varnothing$.

Έστω τώρα $a, b \in J$. Τότε από την Παρατήρηση 1 έπεται ότι $aE_{11} \in I$ και $bE_{11} \in I$, οπότε $(a-b)E_{11} = aE_{11} - bE_{11} \in I$ γιατί το I είναι ιδεώδες του $M_n(R)$. Άρα $a - b \in J$.

Έστω $a \in J$ και $r \in R$. Από την Παρατήρηση 1 έχουμε $aE_{11} \in I$. Άρα $(r1_{M_n(r)})(aE_{11}) \in I$ και $(aE_{11})(r1_{M_n(r)}) \in I$, γιατί το I είναι ιδεώδες του $M_n(R)$. Δηλαδή $(ra)E_{11} \in I$ και $(ar)E_{11} \in I$. Άρα $ra \in J$ και $ar \in J$. Συνεπώς το J είναι ιδεώδες του R.

Για την απόδειξη του ii. θα χρησιμοποιήσουμε την εξής παρατήρηση.

Παρατήρηση 2. Έστω $B=(b_{ij})\in M_n(R)$. Τότε $E_{ip}BE_{qj}=b_{pq}E_{ij}$.

Απόδειξη: $E_{ip}BE_{qj}=E_{ip}\left(\sum_{s,t}b_{st}E_{st}\right)E_{qj}=\sum_{s,t}b_{st}(E_{ip}E_{st})E_{qj}=\sum_{t}b_{pt}E_{it}E_{qj}=b_{pq}E_{ij}$.

Απόδειξη του ii.: Είναι σαφές από τον ορισμό του J ότι $I\subseteq M_n(J)$. Έστω $A=(a_{ij})\in M_n(J)$. Τότε για κάθε i,j υπάρχει πίνακας $B_{i,j}\in I$ (που εξαρτάται από τα i,j) που στη θέση $(p_{i,j},q_{i,j})$ έχει το στοιχείο a_{ij}. Γράφουμε $a_{ij}=\left(B_{i,j}\right)_{p_{i,j},q_{i,j}}$. Έχουμε

$$A=\sum_{i,j}a_{ij}E_{ij}=\sum_{i,j}\left(B_{i,j}\right)_{p_{i,j},q_{i,j}}E_{ij}\ .$$

Από την Παρατήρηση 2 παίρνουμε

$$A=\sum_{i,j}E_{ip_{i,j}}B_{i,j}E_{q_{i,j}j}\ .$$

Από την τελευταία σχέση έπεται ότι $A\in I$, γιατί $B_{i,j}\in I$ και το I είναι ιδεώδες του $M_n(J)$. Άρα $M_n(J)\subseteq I$ και συνεπώς $M_n(J)=I$.

b. Λύση: Από το προηγούμενο υποερώτημα έπεται ότι κάθε ιδεώδες του $M_n(\mathbb{Z})$ είναι της μορφής $M_n(J)$, όπου J ιδεώδες του $\mathbb{Z}$. Από την άσκηση 5.12a έχουμε $J=m\mathbb{Z}$, $m\in\mathbb{N}$, και άρα κάθε ιδεώδες του $M_n(\mathbb{Z})$ είναι της μορφής $M_n(m\mathbb{Z})$.

c. Λύση: Έστω F ένα σώμα. Από το προηγούμενο υποερώτημα έπεται ότι κάθε ιδεώδες του $M_n(F)$ είναι της μορφής $M_n(J)$, όπου J ιδεώδες του F. Από την άσκηση 5.15a έχουμε $J=\{0_F\}$ ή $J=F$. Άρα τα μόνα ιδεώδη του $M_n(F)$ είναι τα $\{0_{M_n(F)}\}$ και $M_n(F)$.

18.

a. Αν υπάρχει $h(x)\in\mathbb{Z}[x]$ με $I=<h(x)>$, τότε $x\in<h(x)>$ και $2\in<h(x)>$. Άρα $h(x)\mid x$ και $h(x)\mid 2$ στο $\mathbb{Z}[x]$. Τότε $h(x)=\pm1$ και συνεπώς $\pm1=xf(x)+2g(x)$ για κάποια $f(x),g(x)\in\mathbb{Z}[x]$. Θέτοντας $x=0$ προκύπτει $\pm1=$ άρτιος , άτοπο.

b. Υπόδειξη: Χρησιμοποιήστε τον αλγόριθμος διαίρεσης στο $\mathbb{Z}[x]$ (που ισχύει όταν ο διαιρέτης είναι μονικό πολυώνυμο, βλ. Πρόταση 2.3.5) κατά αναλογία με την απόδειξη της άσκησης 5. 12b.

19.

a. Θα δείξουμε τα εξής:

i. $\sqrt{I}\neq\varnothing$,

ii. αν $a,b\in I$, τότε $a+b\in\sqrt{I}$,

iii. αν $a\in\sqrt{I}$, τότε $-a\in\sqrt{I}$,

iv. αν $r\in R$ και $a\in I$, τότε $ra\in I$.

i. Επειδή $0\in I$ έχουμε $0\in\sqrt{I}$ και άρα $\sqrt{I}\neq\varnothing$.

ii. Έστω $a,b\in\sqrt{I}$. Τότε $a^m,b^n\in I$ για κάποια $m,n\in\mathbb{Z}_{>0}$. Παρατηρούμε ότι $a^{m+k}\in I$ και $b^{n+k}\in I$ για κάθε $k\in\mathbb{N}$. Πράγματι, αυτό είναι σαφές αν $k=0$, ενώ αν $k>0$, τότε $a^{m+k}=a^ma^k\in I$ γιατί $a^m\in I$ και το I είναι ιδεώδες. Όμοια $b^{n+k}=b^nb^k\in I$.

Επειδή ο R είναι μεταθετικός, έχουμε το διωνυμικό ανάπτυγμα (άσκηση 16 από τις Ασκήσεις3)

$$(a+b)^{m+n}=a^{m+n}+b^{m+n}+\sum_{i=1}^{m+n-1}\binom{m+n}{i}a^{m+n-i}b^i.$$

Από την προηγούμενη παρατήρηση έπονται τα εξής:

- a^{m+n}, $b^{m+n}\in I$.
- Αν $1\le i\le n$, τότε $a^{m+n-i}\in I$ και επειδή το I είναι ιδεώδες έχουμε $a^{m+n-i}b^i\in I$.
- Αν $n+1\le i\le m+n-1$, τότε $b^i\in I$ και επειδή το I είναι ιδεώδες έχουμε $a^{m+n-i}b^i\in I$.

Συνεπώς $(a+b)^{m+n} \in I$, δηλαδή $a+b \in \sqrt{I}$.

iii. Έστω $a \in \sqrt{I}$. Τότε $a^m \in I$ για κάποιο $m \in \mathbb{Z}_{>0}$. Επειδή το I είναι ιδεώδες έχουμε $-a^m \in I$. Άρα $(-a)^m = (-1)^m a^m \in I$, δηλαδή $-a \in \sqrt{I}$.

iv. Έστω $r \in R$ και $a \in \sqrt{I}$. Τότε $a^m \in I$ για κάποιο $m \in \mathbb{Z}_{>0}$. Επειδή ο R είναι μεταθετικός, έχουμε $(ra)^m = r^m a^m$. Άρα $(ra)^m \in I$ γιατί $a^m \in I$ και το I είναι ιδεώδες.

b. Απάντηση: $\sqrt{\langle [4] \rangle} = \langle [2] \rangle = \{[0],[2],[4],[6],[8],[10]\}$.

c. Αν $N = \max\{m_1,...,m_k\}$, τότε $m \mid {p_1}^N ... {p_k}^N$ και άρα στο $\mathbb{Z}_m$ έχουμε

$[p_1...p_k]^N = [{p_1}^N ... {p_k}^N] = [0] \Rightarrow [p_1...p_k] \in \sqrt{\langle [0] \rangle}$. Επειδή το $\sqrt{\langle [0] \rangle}$ είναι ιδεώδες, έχουμε

$$\langle [p_1...p_k] \rangle \subseteq \sqrt{\langle [0] \rangle}.$$

Αντίστροφα, έστω $[a] \in \sqrt{\langle [0] \rangle}$. Τότε υπάρχει $k \in \mathbb{Z}_{>0}$ με

$$[a]^k = [0] \Rightarrow [a^k] = [0] \Rightarrow m \mid a^k \Rightarrow p_1...p_k \mid a^k.$$

Από την τελευταία σχέση έχουμε $p_i \mid a^k$ για κάθε i και επομένως $p_i \mid a$ γιατί p_i είναι πρώτος. Επειδή οι p_i είναι διακεκριμένοι πρώτοι, παίρνουμε $p_1...p_k \mid a$, οπότε $[a] \in \langle [p_1...p_k] \rangle$. Άρα $\sqrt{\langle [0] \rangle} \subseteq \langle [p_1...p_k] \rangle$ και $\sqrt{\langle [0] \rangle} = \langle [p_1...p_k] \rangle$.

20.

a. Αν $a,b \in R$, έχουμε $(a+I)(b+I) = (b+I)(a+I) \Leftrightarrow ab+I = ba+I \Leftrightarrow ab-ba \in I$. Άρα ο R/I είναι μεταθετικός αν και μόνο αν $ab-ba \in I$ για κάθε $a,b \in I$.

b. Έστω ότι υπάρχουν $a,b \in R$ τέτοια ώστε $ab \in I$, $a \notin I$ και $b \notin I$. Από $ab \in I$ έχουμε $ab+I = I$ και άρα $0_{R/I} = I = ab+I = (a+I)(b+I)$. Από $a \notin I$ και $b \notin I$ έχουμε αντίστοιχα $a+I \neq I = 0_{R/I}$ και $b+I \neq I = 0_{R/I}$. Συνεπώς υπάρχουν δύο μη μηδενικά στοιχεία του δακτυλίου R/I που έχουν γινόμενο το μηδενικό στοιχείο.

21.

a. Βλ. Παράδειγμα 2.6.2 4).

b. Βλ. Παράδειγμα 2.6.2 5).

22.

a. Εύκολα επαληθεύεται ότι το $f(x) = x^2+1 \in \mathbb{Z}_3[x]$ δεν έχει ρίζα στο $\mathbb{Z}_3$. Επειδή $\deg f(x) = 2$, το $f(x)$ είναι ανάγωγο στο $\mathbb{Z}_3[x]$ σύμφωνα με την Πρόταση 2.4.5. Από το Θεώρημα 2.6.3 έπεται ότι ο δακτύλιος πηλίκο $\mathbb{Z}_3[x]/I$ είναι σώμα.

Θα δείξουμε ότι κάθε $g(x)+I \in \mathbb{Z}_3[x]/I$ έχει μοναδική παράσταση της μορφής $g(x)+I = r(x)+I$, όπου $r(x) \in \mathbb{Z}_3[x]$ και $\deg r(x) < 2$. Πράγματι, από τον Αλγόριθμο Διαίρεσης στο $\mathbb{Z}_3[x]$ υπάρχουν $q(x), r(x) \in \mathbb{Z}_3[x]$ τέτοια ώστε $g(x) = q(x)f(x) + r(x),\ \deg r(x) < \deg f(x) = 2$. Άρα στο $\mathbb{Z}_3[x]/I$ έχουμε $g(x)+I = r(x)+I$. Αν τώρα έχουμε $r(x), r_1(x) \in \mathbb{Z}_3[x]$ με

$$r(x)+I = r_1(x)+I,\ \deg r(x) < 2,\ \deg r_1(x) < 2,$$

τότε $r(x)-r_1(x) \in I = \langle x^2+1 \rangle$ και άρα $x^2+1 \mid r(x)-r_1(x)$. Επειδή $\deg(r(x)-r_1(x)) < 2$ και ο δακτύλιος $\mathbb{Z}_3[x]$ είναι περιοχή, η Πρόταση 2.3.1 4) δίνει $r(x)-r_1(x) = 0$.

Επειδή $r(x) = ax+b \in \mathbb{Z}_3[x]$, υπάρχουν $3 \cdot 3 = 9$ δυνατότητες για το $r(x)$. Άρα το σώμα $\mathbb{Z}_3[x]/I$ έχει 9 στοιχεία.

b. Εφαρμόζοντας τον Ευκλείδειο αλγόριθμο στα $x^4+x+1, x^2+1 \in \mathbb{Z}_3[x]$ βρίσκουμε:

$$x^4+x+1=(x^2-1)(x^2+1)+x+2,$$
$$x^2+1=(x+1)(x+2)-1.$$

Άρα $\mu\kappa\delta(x^4+x+1,x^2+1)=1$ και το $x^4+x+1+I$ είναι αντιστρέψιμο στο $\mathbb{Z}_3[x]/I$. Αντικαθιστώντας έχουμε

$$\begin{aligned}1&=(x+1)(x+2)-(x^2+1)=\\&=(x+1)(x^4+x+1-(x^2-1)(x^2+1))-(x^2+1)=\\&=(x+1)(x^4+x+1)+(-(x+1)(x^2-1)-1)(x^2+1).\end{aligned}$$

Επομένως στο $\mathbb{Z}_3[x]/I$ έχουμε $((x+1)+I)((x^4+x+1)+I)=1+I$. Άρα το αντίστροφο του $(x^4+x+1)+I$ είναι το $(x+1)+I$.

Το στοιχείο $(x^4+2)+I\in\mathbb{Z}_3[x]/I$ δεν είναι αντιστρέψιμο. Πράγματι, με τον αλγόριθμο διαίρεσης στο $\mathbb{Z}_3[x]$ βρίσκουμε $x^4+2=(x^2-1)(x^2+1)$. Άρα $(x^4+2)+I=I$ που είναι το μηδενικό στοιχείο του σώματος $\mathbb{Z}_3[x]/I$.

23.

‘ a $\Rightarrow$ b ’: Έστω ότι $\mu\kappa\delta(f(x),g(x))=1$. Από το Θεώρημα 2.3.7 υπάρχουν $a(x),b(x)\in F[x]$ με $a(x)f(x)+b(x)g(x)=1$. Τότε $a(x)f(x)-1\in\langle g(x)\rangle$ και άρα $a(x)f(x)+\langle g(x)\rangle=1+\langle g(x)\rangle$, δηλαδή $\big(a(x)+\langle g(x)\rangle\big)\big(f(x)+\langle g(x)\rangle\big)=1+\langle g(x)\rangle$. Επειδή ο δακτύλιος $F[x]/\langle g(x)\rangle$ είναι μεταθετικός, έχουμε ότι το στοιχείο $f(x)+\langle g(x)\rangle$ είναι αντιστρέψιμο.

‘ b $\Rightarrow$ a ’: Έστω ότι το $f(x)+\langle g(x)\rangle\in F[x]/\langle g(x)\rangle$ είναι αντιστρέψιμο. Τότε υπάρχει $a(x)\in F[x]$ με $\big(a(x)+\langle g(x)\rangle\big)\big(f(x)+\langle g(x)\rangle\big)=1+\langle g(x)\rangle$, οπότε $a(x)f(x)+\langle g(x)\rangle=1+\langle g(x)\rangle$ και άρα $a(x)f(x)-1\in\langle g(x)\rangle$. Επομένως υπάρχει $h(x)\in F[x]$ με

$$a(x)f(x)-1\in h(x)g(x).$$

Τώρα αν $d(x)\in F[x]$ ικανοποιεί $d(x)\big|f(x)$ και $d(x)\big|f(x)$, τότε $d(x)\big|1$. Άρα $\mu\kappa\delta(f(x),g(x))=1$.

Δείξαμε την ισοδυναμία των a και b. Εναλλάσσοντας τους ρόλους των $f(x),g(x)$ προκύπτει άμεσα η ισοδυναμία των a και c.

24. Υποδείξεις:

a. Δείξτε ότι η απεικόνιση $\varphi:R\to R/I\times R/J$, $\varphi(r)=\big(r+I,r+J\big)$, είναι ομομορφισμός δακτυλίων με πυρήνα το $I\cap J$.

b. Έστω ότι $I+J=R$. Έστω $(r+I,s+J)\in R/I\times R/J$. Υπάρχουν $r_I,s_I\in I$ και $r_J,s_J\in J$ με $r=r_I+r_J$, $s=s_I+s_J$. Θέτοντας $a=r_J+s_I$ δείξτε ότι $\varphi(a)=(r+I,s+J)$ και άρα η απεικόνιση φ είναι επί.

c. Επειδή $\mu\kappa\delta(m,n)=1$, έχουμε $\langle m\rangle+\langle n\rangle=\mathbb{Z}$ (βλ. άσκηση 5.14b) και άρα εφαρμόζει το Κινεζικό θεώρημα υπολοίπων.

25. Στα παρακάτω θα γράφουμε απλά a στη θέση του $[a]\in\mathbb{Z}_5$.

a. Με πράξεις εύκολα επαληθεύεται ότι το πολυώνυμο $x^2+2\in\mathbb{Z}_5[x]$ δεν έχει ρίζα στο $\mathbb{Z}_5$. Επειδή ο βαθμός του είναι δύο και το $\mathbb{Z}_5$ είναι σώμα, το $x^2+2\in\mathbb{Z}_5[x]$ είναι ανάγωγο. Από το Θεώρημα 2.6.3 έπεται ότι ο δακτύλιος R είναι σώμα.

Στο $\mathbb{Z}_5[x]$, έχουμε $x^2+1=(x-2)(x-3)$. Επειδή το $x-2$ είναι μη μηδενικό, $\deg(x-2)<\deg(x^2+1)$ και το $\mathbb{Z}_5$ είναι σώμα, έπεται ότι το x^2+1 δεν διαιρεί το $x-2$ στο $\mathbb{Z}_5[x]$. Άρα το στοιχείο $x-2+\langle x^2+1\rangle$ του S είναι μη μηδενικό. Όμοια το στοιχείο $x-3+\langle x^2+1\rangle$ του S είναι μη μηδενικό. Όμως το γινόμενό τους

είναι το μηδενικό στοιχείο του S καθώς
$\left(x-2+\left\langle x^2+1\right\rangle\right)\left(x-3+\left\langle x^2+1\right\rangle\right)=(x-2)(x-3)+\left\langle x^2+1\right\rangle=\left\langle x^2+1\right\rangle=0_S$. Άρα ο S δεν είναι περιοχή.

b. Είδαμε πριν ότι ο R είναι σώμα. Ξέρουμε ότι ο $\mathbb{Z}_5\times\mathbb{Z}_5$ δεν είναι σώμα (για παράδειγμα δεν είναι περιοχή αφού $(1,0)(0,1)=(0,0)$ ενώ $(1,0)\neq(0,0)$ και $(0,1)\neq(0,0)$). Άρα οι R και $\mathbb{Z}_5\times\mathbb{Z}_5$ δεν είναι ισόμορφοι.

Θα δείξουμε ότι οι S και $\mathbb{Z}_5\times\mathbb{Z}_5$ είναι ισόμορφοι. Θεωρούμε την απεικόνιση

$$\varphi:\mathbb{Z}_5[x]\to\mathbb{Z}_5\times\mathbb{Z}_5,\ f(x)\mapsto(f(2),f(3)).$$

Εύκολα επαληθεύεται ότι είναι ομομορφισμός δακτυλίων. Επειδή τα $2,3\in\mathbb{Z}_5$ είναι ρίζες του x^2+1, έχουμε $x^2+1\in\ker\varphi$ και άρα $\left\langle x^2+1\right\rangle\subseteq\ker\varphi$. Αν $f(x)\in\ker\varphi$, τότε $f(2)=f(3)=0$, οπότε $x-2\,|\,f(x)$ και $x-3\,|\,f(x)$ στο $\mathbb{Z}_5[x]$. Επειδή τα πολυώνυμα $x-2,x-3$ είναι σχετικά πρώτα, έχουμε $(x-2)(x-3)\,|\,f(x)$, δηλαδή $x^2+1\,|\,f(x)$. Άρα $f(x)\in\left\langle x^2+1\right\rangle$. Συνεπώς $\ker\varphi=\left\langle x^2+1\right\rangle$. Τώρα από το 1ο θεώρημα ισομορφισμών δακτυλίων έπεται ότι υπάρχει μονομορφισμός δακτυλίων
$S\to\mathbb{Z}_5\times\mathbb{Z}_5,\ f(x)+\left\langle x^2+1\right\rangle\mapsto(f(2),f(3))$.

Μένει να δείξουμε ότι η απεικόνιση αυτή είναι επί. Ένα τρόπος είναι, δεδομένου του $(a,b)\in\mathbb{Z}_5\times\mathbb{Z}_5$ να θεωρήσουμε το πολυώνυμο $g(x)=(b-a)x+3a-2b\in\mathbb{Z}_5[x]$ για το οποίο ισχύει $g(2)=a$ και $g(3)=b$ (πώς βρήκαμε το $g(x)$;).

Άλλος τρόπος για το επί είναι ο εξής. Το σύνολο $\mathbb{Z}_5\times\mathbb{Z}_5$ έχει 5^2 στοιχεία. Κάθε στοιχείο του S γράφεται μοναδικά στη μορφή $ax+b+\left\langle x^2+1\right\rangle$, όπου $a,b\in\mathbb{Z}_5$, λόγω της Ευκλείδειας διαίρεσης στο $\mathbb{Z}_5[x]$. Άρα και το σύνολο S έχει 5^2 στοιχεία. Επειδή τα πεπερασμένα σύνολα S και $\mathbb{Z}_5\times\mathbb{Z}_5$ έχουν το ίδιο πλήθος στοιχείων, κάθε 1-1 απεικόνιση $S\to\mathbb{Z}_5\times\mathbb{Z}_5$ είναι επί.

> Σημείωση. Ένας άλλος τρόπος να δειχθεί ότι οι S και $\mathbb{Z}_5\times\mathbb{Z}_5$ είναι ισόμορφοι είναι με χρήση του Κινεζικού θεωρήματος υπολοίπων, βλ. άσκηση 5.24.

c. Με παρόμοιο επιχείρημα που αναφέραμε πριν για τον S, έπεται ότι ο R έχει 5^2 στοιχεία.
Έχουμε ισομορφισμό δακτυλίων $S\to\mathbb{Z}_5\times\mathbb{Z}_5$ από το προηγούμενο ερώτημα. Από την άσκηση 5.6 έπεται ότι το πλήθος των στοιχείων του $U(S)$ είναι ίσο με το πλήθος των στοιχείων του $U(\mathbb{Z}_5)\times U(\mathbb{Z}_5)$. Άρα το ζητούμενο πλήθος είναι 4^2.

Ένας άλλος τρόπος να βρούμε το πλήθος των στοιχείων του $U(S)$ είναι να μετρήσουμε πόσα πολυώνυμα της μορφής $ax+b\in\mathbb{Z}_5[x]$ ικανοποιούν μκδ$(ax+b,x^2+1)=1$, βλ. άσκηση 5.23. Ισοδύναμα, πόσα πολυώνυμα της μορφής $ax+b\in\mathbb{Z}_5[x]$ δεν έχουν ρίζα ούτε το $2\in\mathbb{Z}_5$ ούτε το $3\in\mathbb{Z}_5$.

26.

Το ευθύ: Έστω $p\not\equiv1\bmod4$. Καθώς $p>2$ έχουμε $p\equiv3\bmod4$. Από την άσκηση 4.16 το $x^2+1\in\mathbb{Z}_p[x]$ είναι ανάγωγο. Άρα ο δακτύλιος $\mathbb{Z}_p[x]\big/\left\langle x^2+1\right\rangle$ είναι σώμα. Επειδή ο $\mathbb{Z}_p\times\mathbb{Z}_p$ δεν είναι σώμα, οι δακτύλιοι $\mathbb{Z}_p[x]\big/\left\langle x^2+1\right\rangle$ και $\mathbb{Z}_p\times\mathbb{Z}_p$ δεν είναι ισόμορφοι.

Υπόδειξη για το αντίστροφο: Έστω $p\equiv1\bmod4$. Το κριτήριο του Euler, βλ. Εφαρμογή 2.4.4, δίνει ότι το πολυώνυμο $x^2+1\in\mathbb{Z}_p[x]$, έχει ρίζα στο $\mathbb{Z}_p$, έστω a. Άρα $x^2+1=(x-a)(x+a)$. Το ζητούμενο έπεται από το Κινεζικό θεώρημα υπολοίπων (βλ. άσκηση 5.24) για $R=\mathbb{Z}_p[x],\ I=\left\langle x-a\right\rangle,\ J=\left\langle x+a\right\rangle$.

27.

Υπόδειξη: Δείξτε ότι η απεικόνιση $\varphi:R\to\mathbb{Z},\ \varphi\begin{pmatrix}a&b\\0&c\end{pmatrix}=c$ είναι ένας επιμορφισμός δακτυλίων και ότι $\ker\varphi=I$. Το ζητούμενο έπεται από το 1ο θεώρημα ισομορφισμών δακτυλίων.

28.

Υπόδειξη: Έστω $S=\left\{\begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix}\in M_3(\mathbb{R})\middle| a,b,c\in\mathbb{R}\right\}$. Δείξτε ότι η απεικόνιση

$\varphi:\mathbb{R}[x]\to S,\ \varphi(f(x))=\begin{pmatrix} f_0 & f_1 & f_2 \\ 0 & f_0 & f_1 \\ 0 & 0 & f_0 \end{pmatrix}$, $f(x)=f_nx^n+\ldots+f_1x+f_0$, είναι ένας επιμορφισμός δακτυλίων και ότι $\ker\varphi=\left\langle x^3\right\rangle$. Το ζητούμενο έπεται από το $1^{\text{ο}}$ θεώρημα ισομορφισμών δακτυλίων.

29.

Υπόδειξη: Θεωρήστε την απεικόνιση $R\to\mathbb{Z}\times\mathbb{Z},\ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\mapsto(a,b)$.

30.

a. Θεωρούμε την απεικόνιση

$$\varphi:\mathbb{Q}[x]\to\mathbb{Q}\times\mathbb{Q},\ \varphi(f(x))=\big(f(0),f(1)\big).$$

Εύκολα επαληθεύεται ότι είναι ομομορφισμός δακτυλίων.
Είναι επί απεικόνιση, γιατί αν $(a,b)\in\mathbb{Q}\times\mathbb{Q}$, τότε θέτοντας $f(x)=(b-a)x+a$ έχουμε $\varphi(f(x))=(a,b)$.
Έχουμε

$$f(x)\in\ker\varphi\Leftrightarrow f(0)=f(1)=0\Leftrightarrow$$
$$x\big|f(x)\ \text{και}\ x-1\big|f(x)\ (\text{Θεώρημα 2.4.2})\Leftrightarrow$$
$$\Leftrightarrow x(x-1)\big|f(x)\ (\text{Παράδειγμα 2.3.11 2})\Leftrightarrow$$
$$\Leftrightarrow x^2-1\big|f(x)\Leftrightarrow f(x)\in\left\langle x^2-1\right\rangle.$$

Άρα $\ker f=\left\langle x^2-1\right\rangle$. Το ζητούμενο έπεται από το $1^{\text{ο}}$ θεώρημα ισομορφισμών δακτυλίων.

Άλλος τρόπος: Θεωρήστε τα ιδεώδη $I=\left\langle x-1\right\rangle$ και $J=\left\langle x+1\right\rangle$ του $\mathbb{Q}[x]$ και εφαρμόστε το Κινεζικό θεώρημα υπολοίπων (βλ. άσκηση 5.24).

b. Αν $f(x)=a_nx^n+\ldots+a_1x+a_0\in\mathbb{Q}[x]$, τότε

$f(\sqrt{2})=\sum_{i\ge0}a_{2i}(\sqrt{2})^{2i}+\sum_{i\ge0}a_{2i+1}(\sqrt{2})^{2i+1}=\sum_{i\ge0}a_{2i}2^i+\sqrt{2}\sum_{i\ge0}a_{2i+1}2^i\in\mathbb{Q}[\sqrt{2}]$. Συνεπώς έχουμε την απεικόνιση

$$\varphi:\mathbb{Q}[x]\to\mathbb{Q}[\sqrt{2}],\ f(x)\mapsto f(\sqrt{2}).$$

Εύκολα επαληθεύεται ότι είναι ομομορφισμός δακτυλίων και επί απεικόνιση (δικαιολογήστε το). Για τον υπολογισμό του πυρήνα της φ, παρατηρούμε τα ακόλουθα.

- Έστω $f(x)\in\mathbb{Q}[x]$ με $f(\sqrt{2})=0$. Τότε $f(-\sqrt{2})=0$.
  Πράγματι, αν $f(x)=a_nx^n+\ldots+a_1x+a_0$, τότε από την σχέση που είδαμε πριν έχουμε
  $0=\sum_{i\ge0}a_{2i}2^i+\sqrt{2}\sum_{i\ge0}a_{2i+1}2^i$. Από αυτό έπεται ότι $\sum_{i\ge0}a_{2i+1}2^i=0$, γιατί αλλιώς το $\sqrt{2}$ θα ήταν ρητός αριθμός. Συνεπώς
  $$f(-\sqrt{2})=\sum_{i\ge0}a_{2i}(-\sqrt{2})^{2i}+\sum_{i\ge0}a_{2i+1}(-\sqrt{2})^{2i+1}=\sum_{i\ge0}a_{2i}2^i-\sqrt{2}\sum_{i\ge0}a_{2i+1}2^i=\sum_{i\ge0}a_{2i}2^i=0.$$
- Έστω $f(x)\in\mathbb{Q}[x]$. Αν το $x^2-2\big|f(x)$ στο $\mathbb{R}[x]$, τότε $x^2-2\big|f(x)$ στο $\mathbb{Q}[x]$.
  Αυτό έπεται από την άσκηση 4.5.

Έστω τώρα $f(x)\in\ker\varphi$, δηλαδή $f(x)\in\mathbb{Q}[x]$ και $f(\sqrt{2})=0$. Τότε $f(-\sqrt{2})=0$ όπως είδαμε πριν. Άρα στο $\mathbb{R}[x]$ έχουμε $x-\sqrt{2}\big|f(x)$ και $x+\sqrt{2}\big|f(x)$. Επειδή τα πολυώνυμα $x-\sqrt{2}, x+\sqrt{2}$ είναι σχετικά πρώτα, παίρνουμε $(x-\sqrt{2})(x+\sqrt{2})\big|f(x)$, δηλαδή $x^2-2\big|f(x)$ στο $\mathbb{R}[x]$. Άρα $x^2-2\big|f(x)$ στο $\mathbb{Q}[x]$ όπως

είδαμε πριν. Δηλαδή $f(x)\in\langle x^2+2\rangle$. Δείξαμε ότι $\ker\varphi\subseteq\langle x^2-2\rangle$. Η σχέση $\langle x^2-2\rangle\subseteq\ker\varphi$ είναι άμεση αφού $x^2-2\in\ker\varphi$ και το $\ker\varphi$ είναι ιδεώδες. Συνεπώς $\ker\varphi=\langle x^2-2\rangle$.

Είδαμε ότι η απεικόνιση $\varphi:\mathbb{Q}[x]\to\mathbb{Q}[\sqrt{2}]$ είναι επιμορφισμός δακτυλίων και έχει πυρήνα το $\langle x^2-2\rangle$. Από το 1ο θεώρημα ισομορφισμών δακτυλίων υπάρχει έπεται το ζητούμενο.

31.

a. Αρκεί να δείξουμε ότι το $p(x)=x^3-x-1$ δεν έχει ρητή ρίζα γιατί είναι τρίτου βαθμού. Έστω a/b ρίζα του $p(x)$, όπου $a,b\in\mathbb{Z}$ και μκδ$(a,b)=1$. Τότε $a^3/b^3-a/b-1=0$ οπότε $a^3-ab^2-b^3=0$. Αν υπάρχει πρώτος διαιρέτης του a, τότε αυτός διαιρεί τον b^3, οπότε από το Λήμμα του Ευκλείδη διαιρεί και τον b, άτοπο. Άρα $a=\pm1$. Με παρόμοιο επιχείρημα συμπεραίνουμε ότι $b=\pm1$. Συνεπώς οι μόνες πιθανές ρητές ρίζες του $p(x)$ είναι οι ±1. Επειδή $p(1)\neq0$ και $p(-1)\neq0$, το $p(x)$ δεν έχει ρητή ρίζα.

b. Από το προηγούμενο ερώτημα και το Θεώρημα 2.6.3 έπεται ότι ο $\mathbb{Q}[x]/\langle p(x)\rangle$ είναι σώμα.

Θεωρούμε την απεικόνιση $\varphi:\mathbb{Q}[x]\to\mathbb{Q}[a]$, $f(x)\mapsto f(a)$. Είναι σαφές ότι είναι ομομορφισμός δακτυλίων και επί απεικόνιση.

Επειδή το a είναι ρίζα του $p(x)$ έχουμε $\langle p(x)\rangle\subseteq\ker\varphi$. Έστω $f(x)\in\ker\varphi$, δηλαδή $f(x)\in\mathbb{Q}[x]$ και $f(a)=0$. Επειδή το $p(x)\in\mathbb{Q}[x]$ είναι ανάγωγο και μονικό, έχουμε

$$\text{μκδ}(p(x),f(x))=\begin{cases}1 \text{ ή}\\ p(x).\end{cases}$$

Από την άσκηση 4.5b έπεται ότι η πρώτη περίπτωση δεν ισχύει καθώς στο $\mathbb{C}[x]$ ο μκδ των $p(x)$, $f(x)$ διαιρείται με το $x-a$. Άρα $p(x)\big|f(x)$ και $f(x)\in\langle p(x)\rangle$. Συνεπώς $\langle p(x)\rangle=\ker\varphi$. Από το 1ο θεώρημα ισομορφισμών οι δακτύλιοι $\mathbb{Q}[x]/\langle p(x)\rangle$ και $\mathbb{Q}[a]$ είναι ισόμορφοι.

c. Απάντηση: Με τον Ευκλείδειο αλγόριθμο βρίσκουμε (οι πράξεις παραλείπονται εδώ)
$1=x^6f(x)+p(x)g(x)$, όπου $f(x)=2x^2-x-2,\quad g(x)=-2x^5+x^4-x^2+x-1$. Τότε μια ζητούμενη απάντηση είναι το $f(x)$.

32.

Υπόδειξη: Από το Θεώρημα 2.6.3 και το Θεώρημα 2.4.10 2) έπεται ότι ο δακτύλιος $\mathbb{R}[x]/\langle f(x)\rangle$ είναι σώμα αν και μόνο αν

$$f(x)=\begin{cases}x+a,\\ x^2+ax+b,\ a^2-4b<0.\end{cases}$$

Δείξτε ότι στην πρώτη περίπτωση έχουμε $\mathbb{R}[x]/\langle f(x)\rangle\simeq\mathbb{R}$ και στη δεύτερη $\mathbb{R}[x]/\langle f(x)\rangle\simeq\mathbb{C}$.

33.

Έστω I ο πυρήνας επιμορφισμού δακτυλίων $\varphi:F[x]\to S$, όπου F σώμα και S περιοχή που δεν είναι σώμα. Τότε οι δακτύλιοι $F[x]/I$ και S είναι ισόμορφοι σύμφωνα με το 1ο θεώρημα ισομορφισμών δακτυλίων. Από την άσκηση 5.12b, έχουμε $I=\langle f(x)\rangle$ για κάποιο $f(x)\in F[x]$. Επειδή το S δεν είναι σώμα, από το Θεώρημα 2.6.3 έπεται ότι το $f(x)$ δεν είναι ανάγωγο. Συνεπώς

ή $f(x)=a(x)b(x)$, όπου $a(x),b(x)\in F[x]$ με $1\le\deg a(x),\deg b(x)<\deg f(x)$
ή το $f(x)$ είναι σταθερό πολυώνυμο.

Στην πρώτη περίπτωση ο $F[x]/I$ δεν είναι περιοχή καθότι $a(x)+I\neq I$, $b(x)+I\neq I$ ενώ $(a(x)+I)(b(x)+I)=a(x)b(x)+I=f(x)+I=I$, οπότε και ο S δεν είναι περιοχή, άτοπο. Αν το σταθερό πολυώνυμο $f(x)$ είναι μη μηδενικό, τότε $I=F[x]$, γιατί το ιδεώδες I περιέχει αντιστρέψιμο στοιχείο του δακτυλίου $F[x]$, και επομένως ο δακτύλιος $F[x]/I$ είναι ο μηδενικός, πράγμα άτοπο καθώς ο S δεν είναι ο μηδενικός ως περιοχή. Τελικά $I=\{0\}$ και ο φ είναι ισομορφισμός.

34.

Απαντήσεις:

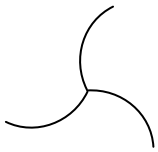
a. Σ.
b. Σ.
c. Σ.
d. Λ.
e. Σ.
f. Σ.
g. Λ.
h. Σ.
i. Σ.
j. Λ.

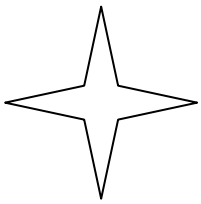
Ασκήσεις6
Ομάδες συμμετρίας, συμμετρικές ομάδες, βασικές ιδιότητες ομάδων

1. (Στις ασκήσεις 1, 2 και 3 δεν ζητείται αυστηρή δικαιολόγηση ότι οι συμμετρίες που βρήκατε εξαντλούν όλες τις συμμετρίες του σχήματος). Προσδιορίστε την ομάδα συμμετρίας για καθένα από τα ακόλουθα επίπεδα σχήματα.

a. A

b. H

c. 

d. 

2. Για κάθε $n \in \mathbb{Z}_{>0}$, βρείτε ένα επίπεδο σχήμα με ομάδα συμμετρίας αποτελούμενη από n στοιχεία.

3. Ποια είναι η ομάδα συμμετρίας μιας 2×2 σκακιέρας (με εναλλασσόμενα άσπρα-μαύρα τετραγωνίδια); Ίδιο ερώτημα για 3×3 σκακιέρα.

4. Θεωρούμε τις μεταθέσεις $\sigma, \tau \in S_5$ με $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix}$.

a. Να βρεθεί μια $\rho \in S_5$ με $\tau = \sigma\rho$. Είναι μοναδική η ρ;

b. Να παρασταθούν οι $\sigma, \tau, \sigma\tau$ ως γινόμενα ξένων κύκλων.

c. Αληθεύει ότι υπάρχει $\rho \in S_5$ με $\tau = \rho\sigma\rho^{-1}$;

5. Να παρασταθεί η μετάθεση $\sigma = (123)(234)(345)(456)(567) \in S_7$ ως γινόμενο ξένων κύκλων. Ίδιο ερώτημα για τη σ^{-1}.

6. Έστω $\sigma \in S_n$ και $\sigma = \sigma_1 ... \sigma_m$, όπου $\sigma_i \in S_n$ κύκλοι ξένοι ανά δύο. Δείξτε ότι $\sigma = \sigma^{-1}$ αν και μόνο αν για κάθε i ισχύει $k_i \le 2$, όπου k_i είναι το μήκος του κύκλου σ_i.

7. Έστω $\sigma = (1234)(3456) \in S_6$.

a. Να βρεθεί η τάξη του σ^{100}.

b. Αληθεύει ότι υπάρχει $\tau \in S_6$ με $\tau^3 = \sigma$;

8. Δείξτε ότι αν ένα στοιχείο $\sigma \in S_{10}$ έχει τάξη 14, τότε υπάρχει μοναδικό $i \in \{1,2,...,10\}$ τέτοιο ώστε $\sigma(i) = i$.

9. Έστω $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & a & 6 & 1 & b & 4 \end{pmatrix} \in S_6$. Υπολογίστε τη μετάθεση σ^m, $m \in \mathbb{Z}$.

10. Έστω $[a] \in \mathbb{Z}_n$, όπου $n \in \mathbb{Z}_{>0}$. Θεωρούμε την απεικόνιση $\sigma : \mathbb{Z}_n \to \mathbb{Z}_n, \sigma([b]) = [ab]$.

a. Δείξτε ότι η σ είναι μια μετάθεση του συνόλου $\mathbb{Z}_n$ αν και μόνο αν $\mu\kappa\delta(a,n) = 1$.

b. Για $n = 9$ και $a = 4$, βρείτε την ανάλυση της μετάθεσης σ^{2011} σε γινόμενο ξένων κύκλων.

11. Έστω $m, n \in \mathbb{Z}_{>0}$ με $m \mid n$. Δείξτε ότι αν $\sigma \in S_n$ είναι ένας κύκλος μήκους n, τότε η μετάθεση σ^m είναι γινόμενο m ξένων ανά δύο κύκλων μήκους n/m.

12. Έστω $\tau \in S_n$ κύκλος μήκους m. Δείξτε ότι δεν υπάρχει $\sigma \in S_n$ με $\sigma^m = \tau$.

13. Δείξτε ότι το πλήθος των κύκλων μήκους k που έχει η S_n, όπου $k \le n$, είναι ίσο με $\frac{n(n-1)...(n-k+1)}{k}$

.

14. Δείξτε ότι το σύνολο $G = \mathbb{Q} - \{0\}$ με πράξη $G \times G \to G, (a,b) \mapsto a * b,$ όπου $a * b = \frac{ab}{2}$, είναι μια αβελιανή ομάδα. Βρείτε ένα $x \in \mathbb{Q}$, τέτοιο ώστε $10 * x * 4 = 1$.

15. Δείξτε ότι το σύνολο $G = \mathbb{R} - \{-1\}$ με πράξη $G \times G \to G, (a,b) \mapsto a * b,$ όπου $a * b = a + b + ab$, είναι μια αβελιανή ομάδα. Γιατί το σύνολο $\mathbb{R}$ με πράξη $\mathbb{R} \times \mathbb{R} \to \mathbb{R}, (a,b) \mapsto a * b,$ όπου $a * b = a + b + ab$, δεν είναι ομάδα;

16. Έστω $n \in \mathbb{Z}_{>0}$ και $E_n = \left\{ z \in \mathbb{C} \middle| z^n = 1 \right\}$. Δείξτε τα εξής.

a. Το σύνολο E_n είναι αβελιανή ομάδα ως προς τον πολλαπλασιασμό μιγαδικών αριθμών.

b. $\left|E_n\right| = n$.

c. Υπάρχει στοιχείο στο E_n τάξης n.

17. Έστω $G = \left\{ \begin{pmatrix} [1] & [a] \\ [0] & [b] \end{pmatrix} \in M_2(\mathbb{Z}_n) \middle| \mu\kappa\delta(b,n) = 1 \right\}$. Δείξτε τα εξής.

a. Το σύνολο G είναι ομάδα ως προς τον πολλαπλασιασμό πινάκων.

b. $\left|G\right| = n\varphi(n)$.

18. Έστω $G = \left\{ A \in M_n(\mathbb{R}) \middle| AA^t = I_n \right\}$, όπου A^t συμβολίζει τον ανάστροφο του A και I_n τον $n \times n$ ταυτοτικό πίνακα. Δείξτε τα εξής.

a. Το σύνολο G είναι ομάδα ως προς τον πολλαπλασιασμό πινάκων.

b. Αν $n > 1$, τότε για κάθε $m \in \mathbb{Z}_{>0}$ υπάρχει στοιχείο της G τάξης m.

19. Δείξτε ότι αν μια ομάδα G έχει στοιχείο τάξης m, όπου $m \in \mathbb{Z}_{>0}$, τότε η G έχει τουλάχιστον $\varphi(m)$ στοιχεία τάξης m.

20.

a. Πόσα στοιχεία τάξης 2 έχει η ομάδα S_4;

b. Πόσα στοιχεία τάξης 3 έχει η ομάδα S_4;

c. Ποιο είναι το μέγιστο $m \in \mathbb{Z}_{>0}$, τέτοιο ώστε η S_5 έχει στοιχείο τάξης m;

d. Ποιο είναι το μέγιστο $m \in \mathbb{Z}_{>0}$, τέτοιο ώστε η S_{10} έχει στοιχείο σ τάξης m με $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$;

21. Έστω p περιττός πρώτος. Θεωρούμε την πολλαπλασιαστική ομάδα $U\left(\mathbb{Z}_p\right)$ των αντιστρέψιμων στοιχείων του δακτυλίου $\mathbb{Z}_p$. Δείξτε τα εξής.

a. Η $U\left(\mathbb{Z}_p\right)$ περιέχει μοναδικό στοιχείο τάξης 2.

b. Αν $p \equiv 3 \bmod 4$, τότε η $U\left(\mathbb{Z}_p\right)$ δεν περιέχει στοιχείο τάξης 4.

22. Έστω G μια ομάδα και $a, b \in G$. Δείξτε τα εξής:

a. $\left|a\right| = \left|a^{-1}\right|$.

b. $\left|a\right| = \left|b^{-1}ab\right|$.

c. $\left|ab\right| = \left|ba\right|$.

d. Αν $b^{-1}a^2b = a^3$ και $a \ne 1$, τότε $\left|a\right| \ge 5$.

23. Έστω G μια ομάδα που έχει μοναδικό στοιχείο a τάξης 2. Δείξτε ότι $ab = ba$ για κάθε $b \in G$.

24. Έστω G μια ομάδα και $a, b \in G$. Δείξτε τα εξής.

a. Αν $a^{-1}b^2a = ba$, τότε $a = b$.

b. Αν $a^{-1}b^2a=b^3$ και $a^2=1$, τότε $b^5=1$.

c. Αν $ba=a^mb^m$, όπου $m\in\mathbb{Z}$, τότε οι τάξεις των στοιχείων $a^mb^{m-2}, a^{m-2}b^m, ab^{-1}$ είναι ίσες.

25. Έστω G μια πεπερασμένη ομάδα και $A\subseteq G$ με $|A|>\frac{|G|}{2}$. Δείξτε ότι για κάθε $g\in G$ υπάρχουν $a,b\in A$ με $g=ab$.

26. Έστω G μια ομάδα. Δείξτε ότι από καθεμιά από τις ακόλουθες συνθήκες έπεται ότι η G είναι αβελιανή.

a. $(ab)^2=a^2b^2$ για κάθε $a,b\in G$.

b. $a^2=1$ για κάθε $a\in G$.

c. Υπάρχουν τρεις διαδοχικοί ακέραιοι i τέτοιοι ώστε $(ab)^i=a^ib^i$ για κάθε $a,b\in G$.

27. * Έστω G μια πεπερασμένη ομάδα που δεν περιέχει στοιχείο τάξης 3. Δείξτε ότι αν $(ab)^3=a^3b^3$ για κάθε $a,b\in G$, τότε η G είναι αβελιανή.

28. Έστω G ομάδα, $a,b\in G$ και m,n σχετικά πρώτοι ακέραιοι. Δείξτε ότι αν $a^m=b^m$ και $a^n=b^n$, τότε $a=b$.

29. Να βρεθούν όλες οι $\sigma\in S_7$ με $\sigma^2=(1234567)$.

30. Για ποια k η μετάθεση σ^k είναι κύκλος, όπου $\sigma=(1234)(34567)\in S_7$;

31. Θεωρούμε την ομάδα $GL_2(\mathbb{R})=\{A\in M_2(\mathbb{R})\,|\det A\neq 0\}$ με πράξη το συνήθη πολλαπλασιασμό πινάκων.

a. Δείξτε ότι το στοιχείο $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ έχει άπειρη τάξη.

b. Να βρεθούν στοιχεία $A,B\in GL_2(\mathbb{R})$ πεπερασμένης τάξης τέτοια ώστε το AB να έχει άπειρη τάξη.

32. Να βρεθούν όλοι οι θετικοί ακέραιοι n με $3^n\equiv 1 \bmod 56$.

33. *Ποια είναι η μέγιστη πεπερασμένη τάξη στοιχείου της ομάδας $\{A\in M_2(\mathbb{Z})\,|\det A=1\}$;

34. Στα παρακάτω, με G συμβολίζουμε μια ομάδα. Εξετάστε ποιες από τις ακόλουθες προτάσεις αληθεύουν. Δικαιολογήστε την απάντησή σας.

a. Αν $a,b\in G$ και $a^5=b^5$, τότε $a=b$.

b. Αν $a,b\in G$, $a^5=b^5$ και $a^{13}=b^{13}$, τότε $a=b$.

c. Αν $a,b\in G$ και $ab=1$, τότε $ba=1$.

d. Για κάθε $a\in G$, τα στοιχεία a, a^{-1} έχουν τις ίδιες τάξεις.

e. Υπάρχει G με μοναδικό στοιχείο τάξης 10.

f. Υπάρχει $\sigma\in S_{10}$ τάξης 21.

Υποδείξεις/Απαντήσεις
Ασκήσεις6

1.
Απάντηση:

a. $\{1,\rho\}$, όπου ρ είναι η ανάκλαση γύρω από τον άξονα συμμετρίας του σχήματος.

b. $\{1,\rho_1,\rho_2,\tau\}$, όπου ρ_1 είναι η ανάκλαση γύρω από τον οριζόντιο άξονα συμμετρίας, ρ_2 είναι η ανάκλαση γύρω από τον άλλο άξονα συμμετρίας και τ στροφή κατά γωνία π γύρω από το 'κέντρο συμμετρίας' του σχήματος.

c. $\{1,\tau,\tau^2\}$, όπου τ είναι στροφή κατά γωνία $\frac{2\pi}{3}$ γύρω από το 'κέντρο συμμετρίας' του σχήματος.

d. Είναι η ομάδα συμμετρίας του τετραγώνου.

2.
Υπόδειξη: Για $n=3$, ένα τέτοιο σχήμα είναι το σχήμα στην άσκηση 1c.

3.
Υπόδειξη: Στην πρώτη περίπτωση η ομάδα συμμετρίας έχει 4 στοιχεία και στη δεύτερη 8.

4.

a. Η ρ είναι μοναδική καθώς $\tau=\sigma\rho \Leftrightarrow \rho=\sigma^{-1}\tau$. Υπολογίζοντας έχουμε
$$\rho=\sigma^{-1}\tau=\begin{pmatrix}1&2&3&4&5\\5&1&4&3&2\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\3&5&2&4&1\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\4&2&1&3&5\end{pmatrix}.$$

b. Για τη σ έχουμε
$\sigma(1)=2,\sigma(2)=5,\sigma(5)=1,$
$\sigma(3)=4,\sigma(4)=3.$
Άρα $\sigma=(125)(34)$.
Για την τ έχουμε
$\tau(1)=3,\tau(3)=2,\tau(2)=5,\tau(5)=1,$
$\tau(4)=4.$
Άρα $\tau=(1325)(4)$.
Για τη $\sigma\tau$ έχουμε $\sigma\tau=\begin{pmatrix}1&2&3&4&5\\2&5&4&3&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\3&5&2&4&1\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\4&1&5&3&2\end{pmatrix}$, οπότε
$\sigma\tau(1)=4,\sigma\tau(4)=3,\sigma\tau(3)=5,\sigma\tau(5)=2,\sigma\tau(2)=1.$
Άρα $\sigma\tau=(14352)$.

c. Από το προηγούμενο υποερώτημα, η σ είναι τύπου $(2,3)$ και η τ είναι τύπου $(1,4)$, δηλαδή οι σ,τ είναι διαφορετικού τύπου. Από το Θεώρημα 4.2.15, δεν υπάρχει $\rho\in S_5$ με $\tau=\rho\sigma\rho^{-1}$.

5.
Απάντηση: $\sigma=(12)(67),\sigma^{-1}=(12)(67)$.

6.
Υπόδειξη: Αν $\sigma=\sigma^{-1}$, τότε $\sigma^2=1$, οπότε η τάξη της σ είναι 1 ή 2. Αν $k_1,...,k_m$ είναι τα μήκη των κύκλων στην ανάλυση της σ σε γινόμενο ξένων κύκλων, ξέρουμε ότι η τάξη της σ είναι το $\varepsilon\kappa\pi(k_1,...,k_m)$. Άρα $k_i\le 2$ για κάθε i. Αντίστροφα, αν $\sigma=\sigma_1...\sigma_m$, όπου οι $\sigma_1,...,\sigma_m$ είναι ανά δύο ξένοι κύκλοι μήκους 1 ή 2, τότε για κάθε i έχουμε $\sigma_i^{-1}=\sigma_i$. Άρα $\sigma^{-1}=\left(\sigma_1...\sigma_m\right)^{-1}=\sigma_m^{-1}...\sigma_1^{-1}=\sigma_m...\sigma_1$. Επειδή ξένες μεταθέσεις αντιμετατίθενται, $\sigma_m...\sigma_1=\sigma_1...\sigma_m=\sigma$.

7.

Υπόδειξη: Υπολογίζοντας της ανάλυση της σ σε γινόμενο ξένων ανά δύο κύκλων βρίσκουμε $\sigma = (123)(456)$. Άρα η τάξη της σ είναι ίση με το $\varepsilon\kappa\pi(3,3) = 3$ και τάξη της σ^{100} είναι ίση με $\frac{3}{\mu\kappa\delta(3,100)} = 3$.

Αν $\tau^3 = \sigma$, τότε $\tau^9 = (\tau^3)^3 = \sigma^3 = 1$ από το οποίο έπεται ότι η τάξη του τ είναι 1 ή 3 ή 9. Οι δυο πρώτες περιπτώσεις δεν ισχύουν αφού $\sigma \neq 1$ ενώ η τελευταία δεν ισχύει αφού η ομάδα S_6 δεν έχει στοιχείο τάξης 9 (δικαιολογήστε το θεωρώντας γινόμενα ξένων κύκλων, όπως στη λύση της άσκησης 6.19c).
Σημείωση: Για διαφορετική απόδειξη, βλ. άσκηση6.12

8.

Έστω $\sigma \in S_{10}$ με τάξη 14. Έστω $\sigma = \sigma_1 ... \sigma_m$, όπου οι $\sigma_1, ..., \sigma_m$ είναι ανά δύο ξένοι κύκλοι. Στην ανάλυση $\sigma = \sigma_1 ... \sigma_m$ υποθέτουμε ότι καταγράφονται και οι κύκλοι μήκους 1 (αν υπάρχουν). Αν k_i είναι το μήκος του κύκλου σ_i, τότε $k_1 + .. + k_m = 10$ και $\varepsilon\kappa\pi(k_1, ..., k_m) = 14$. Από την τελευταία σχέση έπεται ότι κάποιο k_s είναι πολλαπλάσιο του 7 και κάποιο k_t είναι πολλαπλάσιο του 2. Άρα από τη σχέση $k_1 + .. + k_m = 10$ παίρνουμε $k_s = 7$, $k_t = 2$ και $s \neq t$. Έχουμε $k_s + k_t = 9$. Από $k_1 + .. + k_m = 10$ έπεται ότι ανάμεσα στους $k_1, ..., k_m$ ακριβώς ένας είναι ίσος με 1. Άρα ανάμεσα στους κύκλους $\sigma_1, ..., \sigma_m$ υπάρχει μοναδικός κύκλος μήκους 1, δηλαδή υπάρχει μοναδικό $i \in \{1, 2, ..., 10\}$ με $\sigma(i) = i$.

9.

Υπόδειξη: Για το ζεύγος (a,b) έχουμε $(a,b) = (2,5)$ ή $(a,b) = (5,2)$. Υπολογίζοντας της ανάλυση της σ σε γινόμενο ξένων ανά δύο κύκλων βρίσκουμε $\sigma = (1364)$ ή $\sigma = (1364)(25)$ αντίστοιχα. Σε κάθε περίπτωση, η τάξη της σ είναι 4. Άρα $\sigma^m = \sigma^r$, όπου r είναι το υπόλοιπο της διαίρεσης του m με το 4.

10.

a. Έστω ότι η σ είναι μετάθεση και έστω ότι $\mu\kappa\delta(a,n) = d > 1$. Έχουμε $\frac{n}{d}, \frac{a}{d} \in \mathbb{Z}$ και $\sigma([\frac{n}{d}]) = [a\frac{n}{d}] = [\frac{a}{d}n] = [0]$. Επίσης $\sigma([0]) = ([0])$. Άρα $\sigma([\frac{n}{d}]) = \sigma([0])$ και η σ δεν είναι $1-1$, άτοπο.
Αντίστροφα, έστω ότι $\mu\kappa\delta(a,n) = 1$. Αν $\sigma([b_1]) = \sigma([b_2])$, τότε $[ab_1] = [ab_2]$ και άρα $n \mid a(b_1 - b_2)$. Επειδή $\mu\kappa\delta(a,n) = 1$, παίρνουμε $n \mid b_1 - b_2$, δηλαδή $[b_1] = [b_2]$ και η σ είναι 1-1. Επειδή το σύνολο $\mathbb{Z}_n$ είναι πεπερασμένο και η απεικόνιση $\sigma : \mathbb{Z}_n \to \mathbb{Z}_n$ είναι 1-1, η απεικόνιση σ είναι επί. Άρα η σ είναι μια μετάθεση.

b. Με υπολογισμούς βρίσκουμε $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 8 & 3 & 7 & 2 & 6 & 1 & 5 & 9 \end{pmatrix}$. Για παράδειγμα, $\sigma([5]) = [4 \cdot 5] = [20] = [2]$. Υπολογίζοντας την ανάλυση της σ σε γινόμενο ξένων κύκλων βρίσκουμε $\sigma = (147)(285)$. Άρα $\sigma^3 = 1$. Άρα $\sigma^{2011} = (\sigma^3)^{670}\sigma^1 = \sigma = (147)(285)$.

11.

Υπόδειξη: Αν $\sigma = (a_1 a_2 ... a_k)$ είναι ένας κύκλος μήκους k, τότε $\sigma^m(a_i) = (a_{[i+m]})$, όπου $[i+m]$ συμβολίζει το υπόλοιπο της διαίρεσης του $i+m$ με το k.

12.

Υπόδειξη: Από τη μοναδικότητα της ανάλυσης σε γινόμενο ξένων ανά δύο κύκλων μπορούμε να υποθέσουμε , χωρίς περιορισμό της γενικότητας, ότι σ είναι κύκλος.

Από τη σχέση $\sigma^m = \tau$, όπου τ κύκλος μήκος m, έπεται ότι $\frac{|\sigma|}{\mu\kappa\delta(|\sigma|, m)} = m$ και άρα $m \| \sigma|$. Επειδή η σ είναι κύκλος, η άσκηση 6.11 δίνει $m = |\sigma|$, άτοπο.

13.

Υπόδειξη:

1. Υπενθυμίζουμε ότι υπάρχουν $\binom{n}{k} = \frac{n(n-1)...(n-k+1)}{k!}$ υποσύνολα του $\{1, 2, ..., n\}$ που έχουν k στοιχεία.

2. Δείξτε ότι αν $\{b_1, ..., b_k\} \subseteq \{1, 2, ..., n\}$ είναι ένα υποσύνολο με k στοιχεία, τότε το πλήθος των κύκλων $(a_1 a_2 .... a_k) \in S_n$ με $\{a_1, ..., a_k\} = \{b_1, ..., b_k\}$ είναι ίσο με $(k-1)!$

14.

Απάντηση: $x = \frac{1}{10}$.

15.

Απάντηση: Το σύνολο $\mathbb{R}$ με πράξη $\mathbb{R} \times \mathbb{R} \to \mathbb{R}, (a, b) \mapsto a * b,$ όπου $a * b = a + b + ab$, δεν είναι ομάδα, γιατί το στοιχείο -1 δεν έχει αντίστροφο.

16.

Παρατηρούμε τα εξής.

- Έστω $x, y \in E_n$. Τότε $x^n = y^n = 1$ και άρα $(xy)^n = x^n y^n = 1$. Άρα $xy \in E_n$. Συνεπώς ο συνήθης πολλαπλασιασμός μιγαδικών αριθμών ορίζει πράξη στο σύνολο E_n.
- Αν $x, y, z \in E_n$, τότε $(xy)z = x(yz)$ από την προσεταιριστική ιδιότητα του πολλαπλασιασμού μιγαδικών αριθμών.
- Είναι σαφές ότι για τον αριθμό $1 \in \mathbb{C}$ έχουμε $1 \in E_n$ και $1z = z1 = z$ για κάθε $z \in E_n$.
- Αν $z \in E_n$, τότε $z^n = 1$ και άρα $\left(z^n\right)^{-1} = 1$, οπότε $\left(z^{-1}\right)^n = 1$. Άρα $z^{-1} \in E_n$ και φυσικά $z^{-1} z = z z^{-1} = 1$.

Από τα παραπάνω έπεται ότι το σύνολο E_n με το συνήθη πολλαπλασιασμό μιγαδικών αριθμών είναι ομάδα. Επειδή $xy = yx$ για κάθε $x, y \in E_n$, η ομάδα E_n είναι αβελιανή.

Από το Θεώρημα του De Moivre (Παράδειγμα 1.1.4 4) έπεται ότι οι μιγαδικοί αριθμοί $z_k = \cos\frac{2k\pi}{n} + i \sin\frac{2k\pi}{n} \in \mathbb{C}$, όπου $k = 0, 1, ..., n-1$, ικανοποιούν ${z_k}^n = 1$, δηλαδή $z_k \in E_n$. Οι $z_0, ..., z_{n-1}$ είναι διακεκριμένοι. Άρα $|E_n| \geq n$. Επειδή το $\mathbb{C}$ είναι σώμα, το πολυώνυμο $x^n - 1$ έχει το πολύ n διακεκριμένες ρίζες στο $\mathbb{C}$ (Πόρισμα 2.4.2). Άρα $|E_n| = n$.

> Σημείωση: Θα μπορούσε να αποδειχτεί ότι $|E_n| = n$ χρησιμοποιώντας 1) το κριτήριο της παραγώγου που λέει πότε ένα πολυώνυμο έχει απλές ρίζες και 2) ότι το σώμα $\mathbb{C}$ είναι αλγεβρικά κλειστό.

Ένα στοιχείο της ομάδας E_n τάξης n είναι το $z_1 = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$. Πράγματι, είδαμε πριν ότι ${z_1}^n = 1$ και παρατηρούμε ότι ${z_1}^k = z_k$ για κάθε $k = 1, 2, ..., n-1$ από το Θεώρημα του De Moivre. Άρα ${z_1}^k \neq 1$ για κάθε $k = 2, ..., n-1$.

17.

18.

b. Απάντηση: Ένα στοιχείο τάξης m είναι το $A=\begin{pmatrix}\cos\theta & -\sin\theta & & & \\ \sin\theta & \cos\theta & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1\end{pmatrix}$, όπου $\theta=\frac{2\pi}{m}$. Σημείωση:

Για $n=2$, έχουμε $A=\begin{pmatrix}\cos\theta & -\sin\theta \\ \sin\theta & \cos\theta\end{pmatrix}$ που (ως προς τη συνήθη βάση του διανυσματικού χώρου $\mathbb{R}^2$) παριστάνει στροφή κατά γωνία $\theta=\frac{2\pi}{m}$.

19.

Έστω ότι το g έχει τάξη m. Από την Πρόταση 4.3.11 2, κάθε στοιχείο της μορφής g^k, όπου $1\le k\le m$ και $\mu\kappa\delta(k,m)=1$, έχει τάξη m. Τα στοιχεία αυτά είναι ανά δύο διαφορετικά (γιατί;). Το πλήθος των στοιχείων αυτών είναι $\varphi(m)$.

20.

Απαντήσεις: a. Κάθε στοιχείο της S_4 τάξης 2 είναι ή κύκλος μήκους 2 ή γινόμενο δύο ξένων κύκλων μήκους 2. Συνολικά υπάρχουν $6+3=9$ τέτοια στοιχεία.

b. Κάθε στοιχείο της S_4 τάξης 3 είναι κύκλος μήκους 3. Υπάρχουν 8 τέτοια στοιχεία (βλ και άσκηση 12).

c. Λύση: Ξέρουμε ότι κάθε $\sigma\in S_5$ είναι γινόμενο ξένων ανά δύο κύκλων. Καταγράφουμε όλα τα $(k_1,k_2,...,k_m)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{>0}\times...\times\mathbb{Z}_{>0}$ όπου $\sigma=\sigma_1\sigma_2...\sigma_m$ είναι η ανάλυση της $\sigma\in S_5$ σε γινόμενο ξένων ανά δύο κύκλων και k_i είναι το μήκος του σ_i. Εδώ συμπεριλαμβάνουμε τους κύκλους μήκους 1 (άρα $k_1+...+k_m=5$) και υποθέτουμε ότι $k_1\ge k_2\ge...\ge k_m$ (επιτρεπτό αφού ξένες μεταθέσεις αντιμετατίθενται). Δίπλα καταγράφουμε την τάξη της σ χρησιμοποιώντας ότι είναι ίση με το $\varepsilon\kappa\pi(k_1,...,k_m)$.

(5)	5
(4,1)	4
(3,2)	6
(3,1,1)	3
(2,2,1)	2
(2,1,1,1)	2
(1,1,1,1,1)	1

Άρα το ζητούμενο μέγιστο είναι το 6.

d. Απάντηση: εκπ(3,5,2)=30.

21.

a. Το στοιχείο $[-1]\in U(\mathbb{Z}_p)$ ικανοποιεί $[-1]\ne[1]$, γιατί $p\ne 2$, και $[-1]^2=[1]$. Άρα η τάξη του $[-1]$ είναι ίση με 2. Έστω $[a]\in U(\mathbb{Z}_p)$ στοιχείο τάξης 2. Τότε

$$[a]^2=[1]\Rightarrow[a^2]=[1]\Rightarrow p\,|\,a^2-1\Rightarrow p\,|\,(a-1)(a+1).$$

Επειδή ο p είναι πρώτος, έχουμε $p\,|\,a-1$ ή $p\,|\,a+1$. Άρα $[a]=[1]$ ή $[a]=[-1]$. Συνεπώς το $[-1]$ είναι το μοναδικό στοιχείο τάξης 2 της ομάδας $U(\mathbb{Z}_p)$.

b. Βλ. άσκηση 2.15.

22.

a. Έχουμε $(a^{-1})^n = \left(a^n\right)^{-1}$ για κάθε $n \in \mathbb{Z}_{>0}$. Άρα $a^n = 1 \Leftrightarrow \left(a^{-1}\right)^n = 1$. Από την τελευταία ισοδυναμία και τον ορισμό της τάξης προκύπτει άμεσα ότι τα στοιχεία a, a^{-1} έχουν την ίδια τάξη.

b. Με μια εύκολη επαγωγή αποδεικνύεται ότι $(b^{-1}ab)^n = b^{-1}a^n b$ για κάθε $n \in \mathbb{Z}_{>0}$. Από τη σχέση αυτή έπεται ότι $(b^{-1}ab)^n = 1 \Leftrightarrow a^n = 1$. Από την τελευταία ισοδυναμία και τον ορισμό της τάξης προκύπτει άμεσα ότι τα στοιχεία $b^{-1}ab, a$ έχουν την ίδια τάξη.

c. Από τη σχέση $b^{-1}(ba)b = ab$ και το προηγούμενο ερώτημα έπεται το ζητούμενο.

23.

Από την προηγούμενη άσκηση, το $b^{-1}ab$ έχει τάξη 2 για κάθε $b \in G$. Από την υπόθεση της μοναδικότητας παίρνουμε $b^{-1}ab = a$. Άρα $ab = ba$ για κάθε $b \in G$.

24.

a. $a^{-1}b^2a = ba \Rightarrow a^{-1}b^2 = b \Rightarrow b^2 = ab \Rightarrow b = a.$

b. $a^{-1}b^2a = b^3 \Rightarrow b^2a = ab^3 \Rightarrow b^2 = ab^3a^{-1} = ab^3a = (ab)(b^2a) = (ab)(ab^3) = abab^3$. Από $b^2 = abab^3$ παίρνουμε

$$1 = abab \tag{1}$$

και επομένως

$$ab = (ab)^{-1} = b^{-1}a^{-1}. \tag{2}$$

Έχουμε $b^5 = b^3b^2 = (a^{-1}b^2a)b^2 = ab^2ab^2 = ab^2(ab)b \overset{(2)}{=} ab^2(b^{-1}a^{-1})b = abab \overset{(1)}{=} 1.$

c. Έχουμε

$$a^{-2}(a^m b^{m-2})a^2 = a^{-2}(a^m b^m)b^{-2}a^2 = a^{-2}(ba)b^{-2}a^2 = a^{-2}b(ab^{-1})b^{-1}a^2 = (b^{-1}a^2)^{-1}(ab^{-1})(b^{-1}a),$$

δηλαδή

$$a^{-2}(a^m b^{m-2})a^2 = (b^{-1}a^2)^{-1}(ab^{-1})(b^{-1}a).$$

Από την τελευταία σχέση και την άσκηση 21c παίρνουμε ότι τα στοιχεία $a^m b^{m-2}$, ab^{-1} έχουν την ίδια τάξη.

Έχουμε

$$b^{-2}(a^{m-2}b^m)b^2 = b^{-2}a^{-2}(a^m b^m)b^{-2}a^2 = b^{-2}a^{-2}(ba)b^{-2}a^2 = b^{-2}a^{-1}(a^{-1}b)ab^2 = (ab^2)^{-1}(a^{-1}b)ab^2,$$

δηλαδή

$$b^{-2}(a^{m-2}b^m)b^2 = (ab^2)^{-1}(a^{-1}b)ab^2.$$

Από την τελευταία σχέση και την άσκηση 6.21c παίρνουμε ότι τα στοιχεία $a^{m-2}b^m$, $a^{-1}b$ έχουν την ίδια τάξη.

Από την άσκηση 6.21a έπεται ότι η τάξη του $a^{-1}b$ είναι ίση με την τάξη του $(a^{-1}b)^{-1} = b^{-1}a$. Άρα οι τάξεις των $a^m b^{m-2}, a^{m-2}b^m, ab^{-1}$ είναι ίσες.

25.

Έστω $g \in G$. Θεωρούμε το σύνολο $B = \left\{a^{-1}g \in G \middle| a \in A\right\}$. Η απεικόνιση $A \to B, a \mapsto a^{-1}g$, είναι 1-1 γιατί αν $a_1^{-1}g = a_2^{-1}g$, όπου $a_1, a_2 \in A$, τότε πολλαπλασιάζοντας από δεξιά με g^{-1} προκύπτει $a_1^{-1} = a_2^{-1}$, οπότε $\left(a_1^{-1}\right)^{-1} = \left(a_2^{-1}\right)^{-1}$, δηλαδή $a_1 = a_2$. Είναι σαφές ότι η απεικόνιση είναι επί. Άρα για τα πεπερασμένα σύνολα A, B έχουμε $|A| = |B| > \frac{|G|}{2}$. Συνεπώς $A \cap B \neq \varnothing$. Άρα υπάρχουν $b \in A$ και $a \in A$ με $b = a^{-1}g$, οπότε $ab = g$.

26.

a. Για κάθε $a, b \in G$ έχουμε $(ab)^2 = a^2b^2 \Rightarrow abab = a^2b^2 \Rightarrow ba = ab$.

b. Για κάθε $a, b \in G$ έχουμε $(ab)^2 = 1 \Rightarrow (ab)^{-1} = ab \Rightarrow b^{-1}a^{-1} = ab \Rightarrow ba = ab$.

c. Από την υπόθεση υπάρχει $n \in \mathbb{Z}$ τέτοιος ώστε για κάθε $a, b \in G$,

$$(ab)^n = a^n b^n$$
$$(ab)^{n+1} = a^{n+1} b^{n+1}$$
$$(ab)^{n+2} = a^{n+2} b^{n+2}$$

Έχουμε $a^{n+2}b^{n+2} = (ab)^{n+2} = (ab)^{n+1}(ab) = a^{n+1}b^{n+1}ab.$ Από $a^{n+2}b^{n+2} = a^{n+1}b^{n+1}ab$ παίρνουμε

$$ab^{n+1} = b^{n+1}a. \quad (1)$$

Όμοια αποδεικνύεται ότι

$$ab^n = b^n a. \quad (2)$$

Επειδή $\mu\kappa\delta(n, n+1) = 1$, υπάρχουν $x, y \in \mathbb{Z}$ με $1 = x(n+1) + yn$. Άρα

$$ab = ab^{x(n+1)+yn} = a(b^x)^{n+1}(b^y)^n \overset{(1)}{=} (b^x)^{n+1}a(b^y)^n \overset{(2)}{=} (b^x)^{n+1}(b^y)^n a = ba.$$

27.

Υπόδειξη: Δείξτε τα εξής.

1. Η απεικόνιση $G \to G, a \mapsto a^3$, είναι επί.
2. $(ba)^2 = a^2b^2$ για κάθε $a, b \in G$.
3. $b^3a^2 = a^2b^3$ για κάθε $a, b \in G$.
4. Από τα 1 και 3 έπεται ότι $ba^2 = a^2b$ για κάθε $a, b \in G$.
5. Από τα 2 και 4 έπεται ότι $baba = b^2a^2$ και άρα $ab = ba$.

28.

Υπάρχουν ακέραιοι x, y με $mx + ny = 1$. Άρα $a = a^1 = (a^m)^x (a^n)^y = (b^m)^x (b^n)^y = b.$

29.

Υπόδειξη: Δείξτε ότι αν $\sigma \in S_7$ και $\sigma^2 = (1234567)$, τότε $|\sigma| = 7$ και άρα η σ είναι κύκλος μήκους 7.

Απάντηση: Υπάρχει μοναδική σ, $\sigma = (1526374)$.

30.

Απάντηση: $k \equiv 0, 3, 4, 8, 9 \bmod 12.$

31.

a. Δείξτε ότι για κάθε θετικό ακέραιο n, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$

b. Μια επιλογή είναι $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = AB,$ όπου $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ έχει τάξη 2 και $B = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ έχει τάξη 2.

32.

Με πράξεις διαπιστώνουμε ότι η τάξη του $[3] \in U(\mathbb{Z}_{56})$ είναι 6 και άρα η απάντηση είναι τα θετικά πολλαπλάσια του 6.

33.

Υπόδειξη: Αν $A^k = I_2$, δείξτε ότι το ελάχιστο πολυώνυμο του A (Γραμμική Άλγεβρα!) είναι ένα από τα ακόλουθα.

$$x - 1,\ x^2 + 1,\ x^2 + x + 1,\ x^2 - x + 1.$$

Παρατηρήστε ότι $x^2 + 1 \mid x^4 - 1,\ x^2 + x + 1 \mid x^3 - 1,\ x^2 - x + 1 \mid x^6 - 1.$

Απάντηση: Από τα παραπάνω έπεται ότι η μέγιστη πεπερασμένη τάξη είναι το πολύ 6. Ο πίνακας $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$ έχει τάξη 6 (πράξεις) και άρα η απάντηση στην άσκηση είναι 6.

34.

a. Λ. Για παράδειγμα, αν $a=(12345), b=(21345)\in S_5$, τότε $a^5=b^5=1$ και $a\neq b$.

b. Σ.

c. Σ.

d. Σ.

e. Λ. Αν το a έχει τάξη 10, τότε και το a^3 έχει τάξη $\frac{10}{\mu\kappa\delta(10,3)}=10$ και $a^3\neq a$.

f. Σ.

Ασκήσεις7
Υποομάδες, Θεώρημα του Lagrange

1. Έστω $G = GL_2(\mathbb{R}) = \{A \in M_2(\mathbb{R}) | \det A \neq 0\}$. Δείξτε ότι τα ακόλουθα σύνολα είναι υποομάδες της G.

a. $SL_2(\mathbb{R}) = \{A \in G | \det A = 1\}$.

b. $\{A \in G | AA^t = A^t A = I_2\}$.

c. $\left\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G | a, b \in \mathbb{R}\right\}$.

2. Έστω $H = \{\sigma \in S_n | \sigma(n) = n\}$.

a. Δείξτε ότι το H είναι υποομάδα της S_n.

b. Ποια είναι η τάξη της H;

c. Βρείτε ένα σύστημα αντιπροσώπων των αριστερών κλάσεων της H στη S_n, δηλαδή $a_1, a_2, ..., a_m \in S_n$ τέτοια ώστε να έχουμε την ξένη ένωση $G = a_1H \cup a_2H \cup ... \cup a_mH$.

3. Θεωρούμε τις ομάδες $E_n = \{z \in \mathbb{C} | z^n = 1\}$, $n \in \mathbb{Z}_{>0}$, (βλ.άσκηση 6.16).

a. Έστω $m, n \in \mathbb{Z}_{>0}$. Δείξτε ότι $m | n \Leftrightarrow E_m \leq E_n$.

b. Δείξτε ότι το σύνολο $\bigcup_{n=1}^{\infty} E_{2^n}$ είναι άπειρη υποομάδα της $\mathbb{C} - \{0\}$ και κάθε στοιχείο της έχει πεπερασμένη τάξη που είναι δύναμη του 2.

c. Αληθεύει ότι το σύνολο $E_m \cup E_n$ είναι υποομάδα της $\mathbb{C} - \{0\}$ για κάθε $m, n \in \mathbb{Z}_{>0}$;

d. Βρείτε μια ικανή και αναγκαία συνθήκη στους $m, n \in \mathbb{Z}_{>0}$ ώστε το σύνολο $E_m \cup E_n$ να είναι υποομάδα της $\mathbb{C} - \{0\}$.

4. Έστω G μια κυκλική ομάδα, $G = \langle a \rangle$, τάξης 12 και $H = \langle a^4 \rangle \leq G$. Βρείτε τις κλάσεις gH, $g \in G$. Για $G = E_{12}$ και $H = E_3$ (βλ. προηγούμενη άσκηση 3), σχεδιάστε τις κλάσεις σημειώνοντας τις αντίστοιχες κορυφές στο κανονικό κυρτό 12-γωνο.

5. Αν $f = f(x_1, x_2, x_3, x_4) \in \mathbb{Z}[x_1, x_2, x_3, x_4]$ (πολυώνυμο των x_1, x_2, x_3, x_4) και $\sigma \in S_4$, με $\sigma(f)$ συμβολίζουμε το πολυώνυμο $f(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$. Για παράδειγμα, αν $f = x_1x_2 + x_1^2x_3$ και $\sigma = (13)(24)$, τότε $\sigma(f) = x_{\sigma(1)}x_{\sigma(2)} + x_{\sigma(1)}^2 x_{\sigma(3)} = x_3x_4 + x_3^2x_1$. Έστω $S(f) = \{\sigma \in S_4 | \sigma(f) = f\}$.

a. Δείξτε ότι $S(f) \leq S_4$ για κάθε $f \in \mathbb{Z}[x_1, x_2, x_3, x_4]$.

b. Βρείτε την ομάδα $S(f)$ στις ακόλουθες περιπτώσεις.

i. $f = x_1x_2 + x_3^2$.

ii. $f = x_1x_2 + x_3x_4$. Δώστε μια γεωμετρική ερμηνεία για το αποτέλεσμα.

iii. $f = x_1 + x_2 + x_3 + x_4$.

c. Δείξτε ότι για κάθε $f, g \in \mathbb{Z}[x_1, x_2, x_3, x_4]$ ισχύει $S(f) \cap S(g) \leq S(f + g)$ και βρείτε παράδειγμα όπου δεν ισχύει η ισότητα.

6. Έστω G μια αβελιανή ομάδα και $H = \{g \in G | g^2 = 1\}$. Δείξτε ότι $H \leq G$. Αληθεύει το συμπέρασμα όταν η G δεν είναι αβελιανή;

7. Έστω G μια ομάδα και $Z(G) = \{a \in G | ag = ga \ \forall g \in G\}$. Το $Z(G)$ ονομάζεται το **κέντρο** της G.

a. Δείξτε ότι $Z(G) \leq G$ με ισότητα αν και μόνο αν η G είναι αβελιανή.

b. Δείξτε ότι $Z(S_n) = \{1\}$ αν $n \geq 3$.

c. Βρείτε το $Z(G)$ αν $G = GL_2(\mathbb{R})$.

8. Έστω G μια ομάδα και $H \leq G, K \leq G$.

a. Δείξτε ότι $H \cap K \le G$.

b. Αν οι H, K είναι πεπερασμένες και $\mu\kappa\delta(|H|,|K|) = 1$, δείξτε ότι $H \cap K = \{1\}$.

9. Εξετάστε ποιες από τις ακόλουθες ομάδες είναι κυκλικές.

a. $\mathbb{Z}$.

b. $\mathbb{Q}$.

c. $\mathbb{Z}_n$.

d. E_n.

e. $U(\mathbb{Z}_5)$.

f. $U(\mathbb{Z}_8)$.

g. S_3.

h. $\left\{ \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R}) \middle| m \in \mathbb{Z} \right\}$.

i. $\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R}) \middle| a \in \mathbb{R} \right\}$.

10. Δείξτε τα εξής.

a. Κάθε ομάδα που έχει τάξη πρώτο αριθμό είναι κυκλική.

b. Κάθε κυκλική ομάδα είναι αβελιανή.

c. Κάθε γνήσια υποομάδα μιας ομάδας τάξης pq, όπου p, q πρώτοι, είναι κυκλική.

11. Έστω G μια ομάδα και $a, b \in G$. Αν οι τάξεις των a, b είναι σχετικά πρώτοι ακέραιοι m, n αντίστοιχα και ισχύει $ab = ba$, δείξτε ότι η τάξη του ab είναι ίση με mn.

12. Έστω G μια πεπερασμένη υποομάδα της $\mathbb{C} - \{0\}$. Δείξτε ότι $G = E_n$ για κάποιο n.

13. Έστω G μια πεπερασμένη ομάδα και p ένας πρώτος αριθμός.

a. Έστω $a, b \in G$ με $|a| = |b| = p$. Δείξτε ότι $\langle a \rangle \cap \langle b \rangle = \{1\}$ ή $\langle a \rangle = \langle b \rangle$.

b. Δείξτε ότι το πλήθος των στοιχείων της G τάξης p είναι πολλαπλάσιο του $p-1$.

c. Δείξτε ότι αν $|G| = 33$, τότε η G έχει στοιχείο τάξης 3.

d. Έστω ότι η G έχει τάξη pq, όπου p, q πρώτοι. Δείξτε ότι αν $q \equiv 1 \bmod p$ και $n_p \not\equiv -1 \bmod p$, όπου n_p είναι το πλήθος των στοιχείων της G τάξης p, τότε η G είναι κυκλική.

14. Έστω G μια ομάδα τάξης $2m$, όπου $m \in \mathbb{Z}_{>0}$. Δείξτε τα εξής.

a. Το πλήθος των στοιχείων της G τάξης 2 είναι περιττός αριθμός.

b. Αν η G είναι αβελιανή και το m περιττός, τότε η G έχει μοναδικό στοιχείο τάξης 2.

15. Έστω G μια ομάδα τάξης $2m+1$, όπου $m \in \mathbb{Z}_{>0}$. Δείξτε τα εξής.

a. $\{g \in G \mid g^2 = 1\} = \{1\}$.

b. $\{g^2 \in G \mid g \in G\} = G$, δηλαδή κάθε στοιχείο της G είναι τετράγωνο.

16. Έστω G ομάδα τέτοια ώστε $a^2b^2 = b^2a^2$ για κάθε $a, b \in G$. Δείξτε ότι το υποσύνολο της G των στοιχείων περιττής τάξης είναι αβελιανή υποομάδα της G.

17. Έστω G ομάδα τάξης 105. Εξετάστε ποιες από τις ακόλουθες προτάσεις αληθεύουν.

a. Αν $H \le G$ και $|H| \ge 36$, τότε $H = G$.

b. Αν $g \in G$ και $g^{36} = 1$, τότε $g^3 = 1$.

18. Δείξτε ότι κάθε ομάδα τάξης p^n, όπου p πρώτος και $n \in \mathbb{Z}_{>0}$, έχει υποομάδα τάξης p.

19. Έστω G μια πεπερασμένη ομάδα τάξης n. Θεωρούμε την εξής ιδιότητα: (I) Για κάθε $m \in \mathbb{Z}_{>0}$ με $m \mid n$ και $m \ne n$ υπάρχει στοιχείο της G τάξης m. Εξετάστε ποιες από τις ακόλουθες ομάδες έχουν την ιδιότητα (I).

a. S_4.

b. A_4.

c. $\mathbb{Z}_n$.

d. D_4 (η ομάδα συμμετρίας του τετραγώνου).

20. Δώστε ένα παράδειγμα ομάδας G και υποομάδας $H \le G$ τέτοιες ώστε:

a. $[G:H]=\infty$, $|H|<\infty$, $H\neq\{1\}$.

b. $[G:H]=\infty$, $|H|=\infty$.

c. $[G:H]<\infty$, $|H|=\infty$.

21. Έστω G μια ομάδα και $H \le G$ με $[G:H]=n<\infty$. Δείξτε ότι για κάθε $g\in G$, υπάρχει $m\in\mathbb{Z}_{>0}$, $1\le m\le n$, τέτοιο ώστε $g^m\in H$.

22. Θεωρούμε την ομάδα $\mathbb{R}^*=\mathbb{R}-\{0\}$ με πράξη το συνήθη πολλαπλασιασμό πραγματικών.

a. Δείξτε ότι $\mathbb{R}_{>0}\le\mathbb{R}^*$ και $[\mathbb{R}^*:\mathbb{R}_{>0}]=2$.

b. Δείξτε ότι η $\mathbb{R}^*$ έχει μοναδική υποομάδα H με $[\mathbb{R}^*:H]=2$.

23. Έστω G μια ομάδα, $a,b\in G$, $H\le G$ και $K\le G$. Δείξτε ότι αν $aH\cap bK\neq\varnothing$, τότε υπάρχει $c\in G$ τέτοιο ώστε $aH\cap bK=c(H\cap K)$. Στην περίπτωση αυτή, δείξτε ότι $c(H\cap K)=cH\cap cK$.

24. (Θεώρημα του Poincare) Έστω G μια ομάδα, $H\le G$ και $K\le G$. Δείξτε ότι αν $[G:H]<\infty$, τότε $[K:H\cap K]\le[G:H]$.

25. Έστω G μια ομάδα, $H\le G$ και $K\le G$.

a. * Έστω ότι $H\subseteq K$ με $[G:H]<\infty$. Δείξτε ότι $[G:K],[K:H]<\infty$ και $[G:H]=[G:K][K:H]$.

b. Έστω ότι $[G:H]<\infty$ και $[G:K]<\infty$. Δείξτε ότι $[G:H\cap K]\le[G:H][G:K]$.

26. Έστω $\sigma=\begin{pmatrix}1&2&3&4&5&6&7\\4&7&5&2&6&3&1\end{pmatrix}\in S_7$.

a. Εξετάστε αν η σ είναι περιττή μετάθεση.

b. Να βρεθούν όλοι οι ακέραιοι m τέτοιοι ώστε $\langle\sigma^m\rangle\le A_7$.

c. Αληθεύει ότι υπάρχει $\tau\in S_7$ τέτοιο ώστε $\tau^{2000}=\sigma$;

27. Έστω $\sigma=\begin{pmatrix}1&2&3&4&5&6&7\\5&a&1&b&6&7&3\end{pmatrix}\in S_7$.

a. Να βρεθούν οι a,b ώστε η σ να είναι άρτια μετάθεση.

b. Αν η σ είναι άρτια μετάθεση, αληθεύει ότι $(15)(56)(67)\in\langle\sigma\rangle$;

c. Αληθεύει ότι $(12)\in\langle\sigma\rangle$;

28. Έστω $G\le S_n$. Δείξτε ότι αν η G περιέχει μια περιττή μετάθεση, τότε η τάξη της G είναι άρτιος ακέραιος και ακριβώς τα μισά στοιχεία της G είναι περιττές μεταθέσεις.

29. Δείξτε ότι κάθε υποομάδα της S_n, $n\ge 2$, περιττού δείκτη περιέχει τουλάχιστον μία περιττή μετάθεση.

30. Αληθεύει ότι η ομάδα A_6 έχει στοιχείο τάξης 6; Βρείτε όλα τα n ώστε η A_n να έχει στοιχείο τάξης 6.

31. Έστω $\sigma\in S_n$ με περιττή τάξη. Δείξτε ότι $\sigma\in A_n$.

32. Έστω G μια πεπερασμένη ομάδα τάξης n και $m\in\mathbb{Z}$ με $\mu\kappa\delta(m,n)=1$. Τότε $G=\{g^m\,|\,g\in G\}$.

33. Έστω $a,n\in\mathbb{Z}_{>0}$ με $a>1$. Δείξτε ότι $n\,|\,\varphi(a^n-1)$.

34. Έστω p πρώτος, $a\in\mathbb{Z}_p$, R ο δακτύλιος $\dfrac{\mathbb{Z}_p[x]}{\langle x^p+a\rangle}$ και G η ομάδα $U(R)$. Δείξτε τα εξής.

a. Το πλήθος των στοιχείων του R είναι ίσο με p^p.

b. Το πλήθος των στοιχείων της G είναι ίσο με p^p-p^{p-1}.

c. Αν $f(x)\in\mathbb{Z}_p[x]$ είναι τέτοιο ώστε $f(-a)\neq 0$, τότε $x^p+a\,|\,f(x)^n-1$, όπου $n=p^p-p^{p-1}$.

35. Στα παρακάτω, με G συμβολίζουμε μια ομάδα. Εξετάστε ποιες από τις ακόλουθες προτάσεις αληθεύουν. Δικαιολογήστε την απάντησή σας.

a. Αν $|G|=20$, $a\in G$ και $a^9=1$, τότε $a=1$.

b. Αν $|G|\le 29$, $H\le G$ και $|H|=10$, τότε $|G|=20$.

c. Αν $a,b\in G$, $|a|=8$ και $|b|=10$, τότε $\langle a\rangle\cap\langle b^4\rangle=\{1\}$.

d. Αν $G=\langle a\rangle$ και $|G|=100$, τότε $\langle a^{28}\rangle=\langle a^{36}\rangle$.

Υποδείξεις/Απαντήσεις
Ασκήσεις7

1.

b. Έστω $H = \{A \in G \,|\, AA^t = A^tA = I_2\}$.

- Έχουμε $H \neq \varnothing$ αφού $I_2 \in H$.
- Έστω $A, B \in H$. Τότε $AA^t = A^tA = I_2$ και $BB^t = B^tB = I_2$. Άρα $(AB)(AB)^t = ABB^tA^t = AI_2A^t = AA^t = I_2$. Όμοια αποδεικνύεται ότι $(AB)^t(AB) = I_2$. Άρα $AB \in H$.
- Έστω $A \in H$. Τότε $AA^t = A^tA = I_2$. Άρα ο A είναι αντιστρέψιμος και $A^{-1} = A^t$. Έχουμε $A^t(A^t)^t = A^tA = I_2$ και όμοια $(A^t)^tA^t = I_2$. Άρα $A^t \in H$, δηλαδή $A^{-1} \in H$.

Συνεπώς $H \leq G$.

2.

b. Απάντηση: $|H| = (n-1)!$.

c. Μια επιλογή των $a_1, a_2, ..., a_m \in S_n$ με τις ζητούμενες ιδιότητες είναι

$$a_1 = (1n), a_2 = (2n), a_3 = (3n), ..., a_n = (nn) = 1.$$

Πράγματι, παρατηρούμε ότι για την επιλογή αυτή, τα σύνολα $a_1H, a_2H, ..., a_nH$ είναι ανά δύο ξένα, αφού αν $\sigma \in a_iH$, τότε $\sigma(n) = i$. Επειδή $|a_iH| = |H| = (n-1)!$, το σύνολο $a_1H \cup a_2H \cup ... \cup a_nH$ έχει $n(n-1)! = n! = |G|$ στοιχεία. Άρα έχουμε $G = a_1H \cup a_2H \cup ... \cup a_nH$ (ξένη ένωση).

3.

d. Υπόδειξη: Αν $\zeta \in E_m - E_n$ και $\xi \in E_n - E_m$, θεωρήστε το γινόμενο $\zeta\xi \in E_m \cup E_n$.

Απάντηση: $E_m \subseteq E_n$ ή $E_m \subseteq E_n$. Ισοδύναμα $m|n$ ή $n|m$.

4.

Οι κλάσεις H, aH, a^2H, a^3H είναι διακεκριμένες. Πράγματι, αν $a^iH = a^jH$ με $0 \leq i, j \leq 3$ και $i > j$, παίρνουμε $a^{i-j} \in H$, όπου $i - j \in \{1, 2, 3\}$. Άρα υπάρχει $m \in \mathbb{Z}$ με $a^{i-j} = a^{4m}$. Επειδή $|a| = 12$, έχουμε $4m \equiv i - j \bmod 12$ και άρα $4|i - j$. Τότε όμως $i = j$.

[Εναλλακτικά, απλά υπολογίζουμε τις κλάσεις αυτές,
$H = \{1, a^4, a^8\}, aH = \{a, a^5, a^9\}, a^2H = \{a^2, a^6, a^{10}\}, a^3H = \{a^3, a^7, a^{11}\}$,
και παρατηρούμε ότι είναι διακεκριμένες καθώς τα στοιχεία $1, a, a^2, ..., a^{11}$ είναι διακεκριμένα, αφού η τάξη του a είναι 12.]

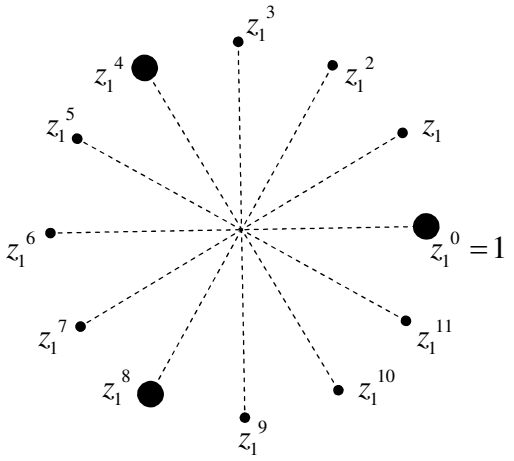
Συνεπώς το σύνολο $\{gH \,|\, g \in G\}$ έχει τουλάχιστον 4 στοιχεία. Ξέρουμε ότι το πλήθος των στοιχείων του συνόλου αυτού είναι $[G:H] = \frac{|G|}{|H|}$ και $|H| = |a^4| = \frac{|a|}{\mu\kappa\delta(|a|, 4)} = \frac{12}{\mu\kappa\delta(12, 4)} = 3$. Άρα $[G:H] = \frac{|G|}{|H|} = \frac{12}{3} = 4$. Άρα

$$\{gH \,|\, g \in G\} = \{H, aH, a^2H, a^3H\}.$$

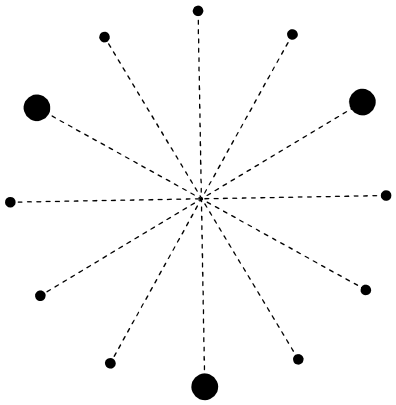
Σημείωση: Έστω $g \in G$. Τότε $g = a^m$ για κάποιο $m \in \mathbb{Z}$. Ισχύει $gH = a^rH$, όπου r είναι ο υπόλοιπο της διαίρεσης του m με το 4 (γιατί;). Αυτός είναι ο λόγος που επιλέξαμε τις κλάσεις H, aH, a^2H, a^3H στην αρχή της λύσης.

Ξέρουμε ότι $E_{12} = \{1, z_1, z_1^2, ..., z_1^{11}\}$, όπου $z_1 = \cos(2\pi/12) + i\sin(2\pi/12)$, και $E_3 = \{1, z_1^4, z_1^8\}$. Στην εικόνα α), οι 'μεγάλες' κορυφές αντιστοιχούν στα στοιχεία της E_3 και στη β) οι 'μεγάλες' κορυφές αντιστοιχούν στα στοιχεία της κλάσης $z_1E_3 = \{z_1, z_1^5, z_1^9\}$. Παρατηρούμε ότι οι κορυφές που αντιστοιχούν στην κλάση

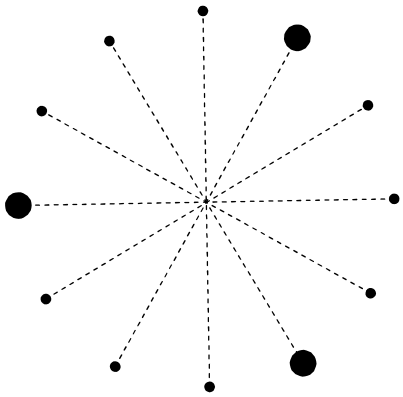
z_1E_3 προκύπτουν περιστρέφοντας τις κορυφές που αντιστοιχούν στην υποομάδα E_3 κατά γωνία $2\pi/12$ (στη φορά αντίθετη με την κίνηση των δεικτών ρολογιού), πράγμα που οφείλεται στον πολλαπλασιασμό με τον μιγαδικό αριθμό $z_1 = \cos(2\pi/12) + i\sin(2\pi/12)$



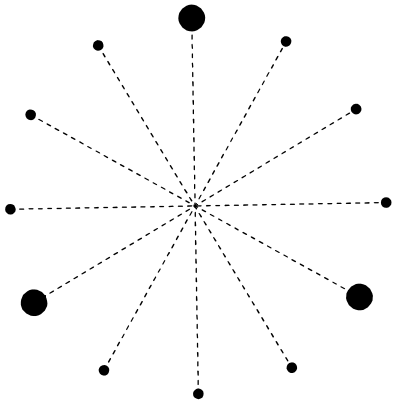
α) E_3 στην E_{12}



β) z_1E_3 στην E_{12}



γ) $z_1^{\,2}E_3$ στην E_{12}



δ) $z_1^{\,3}E_3$ στην E_{12}

5.

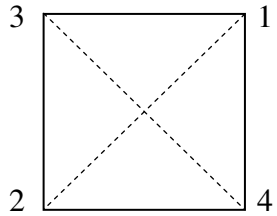
b) Απάντηση:

i) $S(f) = \{1, (12)\}$,

ii) $S(f) = \{1, (1324), (1324)^2, (1324)^3, (12), (34), (14)(23), (13)(24)\}$,

iii) $S(f) = S_4$.

Στην περίπτωση ii) πρόκειται για τις συμμετρίες του τετραγώνου με διαγώνιες 12 και 34 (βλ. σχήμα).



6.

- Έχουμε $H \neq \varnothing$ αφού $1 \in H$.
- Έστω $a,b \in H$. Τότε $a^2 = 1$ και $b^2 = 1$. Επειδή η G είναι αβελιανή έχουμε $(ab)^2 = a^2b^2$. Άρα $(ab)^2 = 1$ και $ab \in H$.
- Έστω $a \in H$. Τότε $a^2 = 1$ και άρα $a^{-1} = a \in H$.

Συνεπώς $H \leq G$.

Το συμπέρασμα γενικά δεν αληθεύει αν η G δεν είναι αβελιανή. Για παράδειγμα, έστω $G = S_3$. Τότε $(12),(13) \in H$, αλλά $(12)(13) = (132) \notin H$, αφού $(132)^2 = (123) \neq 1$.

7.

a. Βλ. σελίδα 288.

Έστω $\sigma \in S_n$, $\sigma \neq 1$. Τότε υπάρχουν $i, j \in \{1,2,...,n\}$ με $\sigma(i) = j$ και $i \neq j$. Επειδή $n \geq 3$, υπάρχει $k \in \{1,2,...,n\}$ με $k \neq i, j$. Έστω $\tau = (ik) \in S_n$. Τότε $\sigma\tau(i) = \sigma(k) \neq j$ γιατί η σ είναι 1-1. Επίσης, $\tau\sigma(i) = \tau(j) = j$. Άρα $\sigma\tau \neq \tau\sigma$ και επομένως $Z(S_n) = \{1\}$.

c. Θα δείξουμε ότι $Z(G) = \{aI_2 \,|\, a \in \mathbb{R} - \{0\}\}$. Έστω $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(G)$, $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in G$ και $C = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in G$. Τότε $AB = BA \Rightarrow \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} \Rightarrow c = 0, a = d$. Όμοια, από $AC = CA$ παίρνουμε $b = 0$. Άρα $Z(G) \subseteq \{aI_2 \,|\, a \in \mathbb{R} - \{0\}\}$. Είναι σαφές ότι ισχύει $\{aI_2 \,|\, a \in \mathbb{R} - \{0\}\} \subseteq Z(G)$ κι άρα έχουμε ισότητα.

8.

a. Βλ. σελίδες 287-288.

b. Επειδή $H \cap K \leq H$, το Θεώρημα του Lagrange δίνει $|H \cap K| \,||\, |H|$. Όμοια έχουμε $|H \cap K| \,||\, |K|$. Άρα $|H \cap K| \,||\, \mu\kappa\delta(|H|,|K|) \Rightarrow |H \cap K| \,|\, 1 \Rightarrow |H \cap K| = 1 \Rightarrow H \cap K = \{1\}$.

9.

Απάντηση:

a. $\mathbb{Z} = \{m1 \,|\, m \in \mathbb{Z}\} = \langle 1 \rangle$ είναι κυκλική.

b. Η ομάδα $\mathbb{Q}$ δεν είναι κυκλική. Πράγματι, αν $\mathbb{Q} = \left\langle \frac{a}{b} \right\rangle$, όπου $a,b \in \mathbb{Z}$ και $b \neq 0$, τότε επιλέγοντας $k \in \mathbb{Z} - \{0\}$ που δεν διαιρεί το b , έχουμε $\frac{1}{k} \in \mathbb{Q} = \left\langle \frac{a}{b} \right\rangle$, δηλαδή $\frac{1}{k} = m\frac{a}{b}$ για κάποιο $m \in \mathbb{Z}$. Τότε $kma = b \Rightarrow k \,|\, b$, άτοπο.

c. $\mathbb{Z}_n = \{[m] \,|\, m \in \mathbb{Z}\} = \langle [1] \rangle$ είναι κυκλική.

d. Είδαμε στην άσκηση 6.16 ότι $E_n = \langle z \rangle$, $z = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, δηλαδή η E_n είναι κυκλική.

e. Η $U(\mathbb{Z}_5)$ είναι κυκλική: Έχουμε $|U(\mathbb{Z}_5)| = \varphi(5) = 4$ και ένα στοιχείο της $U(\mathbb{Z}_5)$ τάξης 4 είναι το $[2]$.

f. Η $U(\mathbb{Z}_8)$ δεν είναι κυκλική: Έχουμε $U(\mathbb{Z}_8) = \{[a] \in \mathbb{Z}_n \,|\, \mu\kappa\delta(\alpha,8) = 1\} = \{[1],[3],[5],[7]\}$ (Πρόταση 1.4.5). Με υπολογισμούς αποδεικνύεται ότι $g^2 = 1$ για κάθε $g \in U(\mathbb{Z}_8)$. Ενδεικτικά, $[3]^2 = [9] = [1]$. Άρα δε υπάρχει στοιχείο της $g \in U(\mathbb{Z}_8)$ τάξης 4.

g. Η S_3 δεν είναι κυκλική, αφού $|S_3| = 6$ και η S_3 δεν έχει στοιχείο τάξης 6: Πράγματι, κάθε στοιχείο του $S_3 - \{1\}$ είναι κύκλος μήκους 2 ή 3 και άρα έχει τάξη 2 ή 3. (Το ότι η S_3 δεν είναι κυκλική, έπεται και από την άσκηση 10b παρακάτω, αφού η S_3 δεν είναι αβελιανή).

h. Η $H=\left\{\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix}\in GL_2(\mathbb{R})\middle| m\in\mathbb{Z}\right\}$ είναι κυκλική. Πράγματι εύκολα αποδεικνύεται ότι για κάθε $m\in\mathbb{Z}$, $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^m=\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix}$. Συνεπώς $H=\left\langle\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right\rangle$.

i. Η $\left\{\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\in GL_2(\mathbb{R})\middle| a\in\mathbb{R}\right\}$ δεν είναι κυκλική, αφού είναι μη αριθμήσιμο σύνολο.

10.

a. Έστω G ομάδα με $|G|=p$ πρώτος. Έστω $g\in G,\ g\neq 1$, και $H=\langle g\rangle$. Από το Θεώρημα του Lagrange, $|H|\,|p$ και άρα $|H|=1,p$. Επειδή $|H|\neq 1$, έχουμε $|H|=p$. Άρα $|H|=|G|$. Επειδή $|G|<\infty$ παίρνουμε $H=G$, δηλαδή η G είναι κυκλική.

b. Έστω $G=\langle g\rangle$ μια κυκλική ομάδα και $a,b\in G$. Τότε υπάρχουν $m,n\in\mathbb{Z}$ με $a=g^m, b=g^n$. Άρα $ab=g^mg^n=g^{m+n}=g^ng^m=ba$.

c. Έστω G ομάδα με $|G|=pq$, όπου p,q πρώτοι, και $H\leq G$, $H\neq G$. Από το Θεώρημα του Lagrange έπεται ότι $|H|=1,p,q$. Από το υποερώτημα a έπεται ότι η H είναι κυκλική.

11.

- Έχουμε $a^m=b^n=1$. Παρατηρούμε ότι $(ab)^{mn}=a^{mn}b^{mn}$, γιατί $ab=ba$. Άρα $(ab)^{mn}=(a^m)^n(b^n)^m=1$. Άρα $|ab|\leq mn$.
- Έστω $s\in\mathbb{Z}_{>0}$ με $(ab)^s=1$. Όπως πριν έχουμε $a^sb^s=1$ και άρα $a^s=b^{-s}\in\langle a\rangle\cap\langle b\rangle$. Έστω $c=a^s=b^{-s}$. Από $c\in\langle a\rangle$ έπεται ότι $|c|\,|m$ και από $c\in\langle b\rangle$ έπεται ότι $|c|\,|n$ (Πόρισμα 4.4.3). Επειδή οι m,n είναι σχετικά πρώτοι, παίρνουμε $|c|=1$, δηλαδή $a^s=b^{-s}=1$. Από $a^s=1$ έπεται ότι $m|s$ (Πρόταση 4.3.11 1). Από $b^{-s}=1$ έχουμε $b^s=\left(b^{-s}\right)^{-1}=1$ και όπως πριν έχουμε ότι $n|s$. Επειδή οι m,n είναι σχετικά πρώτοι, παίρνουμε $mn|s$. Άρα $mn\leq s$, οπότε $mn\leq|ab|$.
  Άρα $|ab|=mn$.

12.

Έστω $|G|=n$. Από το Πόρισμα 4.4. 23 έχουμε $g^n=1$ για κάθε $g\in G$. Άρα $G\subseteq E_n$. Επειδή $|G|=|E_n|<\infty$, παίρνουμε $G=E_n$.

13.

a. Έχουμε $\langle a\rangle\cap\langle b\rangle\leq\langle a\rangle$. Από το Θεώρημα του Lagrange παίρνουμε $|\langle a\rangle\cap\langle b\rangle|\,|\langle a\rangle|$, οπότε $|\langle a\rangle\cap\langle b\rangle|=1$, ή $|\langle a\rangle\cap\langle b\rangle|=p$. Άρα $\langle a\rangle\cap\langle b\rangle=\{1\}$ ή $\langle a\rangle\cap\langle b\rangle=\langle a\rangle$. Στη δεύτερη περίπτωση έχουμε $\langle a\rangle\subseteq\langle b\rangle$.
  Ξεκινώντας από $\langle a\rangle\cap\langle b\rangle\leq\langle b\rangle$, αποδεικνύεται όπως πριν ότι $\langle a\rangle\cap\langle b\rangle=\{1\}$ ή $\langle b\rangle\subseteq\langle a\rangle$. Άρα τελικά $\langle a\rangle\cap\langle b\rangle=\{1\}$ ή $\langle a\rangle=\langle b\rangle$.

b. Έστω $G_p=\{g\in G\,|\,|g|=p\}$. Παρατηρούμε ότι

$$G_p=\bigcup_{g\in G_p}\left(\langle g\rangle-\{1\}\right).$$

Πράγματι, η σχέση $G_p \subseteq \bigcup_{g\in G_p}\left(\langle g\rangle - \{1\}\right)$ είναι σαφής αφού $g \in \langle g\rangle$. Αν $g \in G_p$, τότε $\left|\langle g\rangle\right| = |g| = p$ και άρα κάθε στοιχείο της ομάδας $\langle g\rangle$ διάφορο του 1 έχει τάξη p. Άρα $\bigcup_{g\in G_p}\left(\langle g\rangle - \{1\}\right) \subseteq G_p$.

Από το προηγούμενο υποερώτημα, κάθε δύο σύνολα της μορφής $\langle g\rangle - \{1\}$, όπου $g \in G_p$, ή ταυτίζονται ή είναι ξένα. Άρα υπάρχει ξένη ένωση

$$G_p = \bigcup_{g\in A}\left(\langle g\rangle - \{1\}\right),$$

όπου $A \subseteq G$. Τότε $|G_p| = \sum_{g\in A}\left|\langle g\rangle - \{1\}\right|$. Έχουμε $\left|\langle g\rangle - \{1\}\right| = p-1$.

c. Οι πιθανές τάξης για ένα στοιχείο $g \in G, g \neq 1,$ είναι 33, 11, 3. Αν υπάρχει $g \in G$ τάξης 33, τότε το g^{11} έχει τάξη 3. Έστω ότι κάθε στοιχείο του $G - \{1\}$ έχει τάξη 11. Τότε από το υποερώτημα b το πλήθος των στοιχείων του σύνολο $G - \{1\}$ είναι πολλαπλάσιο του 10, άτοπο.

d. Από το Θεώρημα του Lagrange κάθε στοιχείο της G έχει τάξη $1, p, q, pq$. Από $q \equiv 1 \bmod p$ έχουμε $p \neq q$. Άρα

$$|G| = 1 + n_p + n_q + n_{pq}.$$

Από το υποερώτημα b και τη σχέση $q \equiv 1 \bmod p$ παίρνουμε $n_q \equiv 0 \bmod p$. Άρα $0 \equiv 1 + n_p + n_{pq} \bmod p$. Από $n_p \not\equiv -1 \bmod p$ παίρνουμε $n_{pq} \not\equiv 0 \bmod p$. Άρα $n_{pq} \neq 0$, δηλαδή η G έχει στοιχείο τάξης pq, δηλαδή η G είναι κυκλική.

14.

a. Έστω $G_2 = \{g \in G \,||g| = 2\}$ και $A = \{g \in G \,||g| > 2\}$. Τότε έχουμε την ξένη ένωση

$$G = \{1\} \cup G_2 \cup A.$$

Παρατηρούμε τα εξής:

- Αν $g, h \in G$, τότε $g = h \Leftrightarrow g^{-1} = h^{-1}$.
- Αν $g \in A$, τότε $g^{-1} \in A$ (αφού $|g| = |g^{-1}|$, βλ. άσκηση 6.22)
- Αν $g \in A$, τότε $g^{-1} \neq g$ (αφού $g^2 \neq 1$).

Άρα ο ακέραιος $|A|$ είναι άρτιος. Από την ξένη ένωση $G = \{1\} \cup G_2 \cup A$ και το ότι ο ακέραιος $|G|$ είναι άρτιος, έπεται το ζητούμενο.

Σημείωση. Λήμμα: Έστω A ένα πεπερασμένο σύνολο και $f : A \to A$ μια απεικόνιση τέτοια ώστε $f^2(a) = a$ για κάθε $a \in A$. Αν ο $|A|$ είναι περιττός, τότε υπάρχει $a \in A$ με $f(a) = a$. (Υπόδειξη για την απόδειξη: Επαγωγή στο m, $|A| = 2m+1$. Για το επαγωγικό βήμα έχουμε $A = \{a, f(a)\} \cup B$), όπου $a \in A$ και $B = A - \{a, f(a)\}$. Θεωρήστε τον περιορισμό της f στο σύνολο B).

Θα μπορούσαμε να διατυπώσουμε τη λύση της άσκησης με βάση το λήμμα ως εξής. Αν $a \in A$, τότε $a^{-1} \in A$ αφού $|a^{-1}| = |a| > 2$. Άρα έχουμε την απεικόνιση $f : A \to A$, $f(a) = a^{-1}$. Ισχύει $f^2(a) = a$ για κάθε $a \in A$. Δεν υπάρχει $a \in A$ με $f(a) = a$, γιατί διαφορετικά, $a^{-1} = a \Rightarrow a^2 = 1$. Άρα ο $|A|$ είναι άρτιος από το λήμμα.

b. Έστω $a, b \in G$ στοιχεία τάξης 2 και $a \neq b$. Παρατηρούμε ότι τα στοιχεία $1, a, b, ab$ είναι διακεκριμένα. (Για παράδειγμα, $ab = 1 \Rightarrow b = a^{-1} = a$). Έστω $H = \{1, a, b, ab\}$. Χρησιμοποιώντας τις σχέσεις $a^2 = 1$, $b^2 = 1$ και $ab = ba$, εύκολα επαληθεύεται ότι $H \leq G$. (Για παράδειγμα, $(ab)(ab) = abab = a^2b^2 = 1 \in H$). Από το Θεώρημα του Lagrange έχουμε $4 \,||G|$, άτοπο.

[Εναλλακτικά, το ζητούμενο έπεται από την άσκηση 6.28 (πώς;)]

15.

a. Αν $a^2=1$ και $a\neq 1,$ τότε η τάξη του a είναι 2 που δεν διαιρεί την τάξη της G, άτοπο.

b. Αρκεί να δείξουμε ότι η απεικόνιση $G\to G, a\mapsto a^2,$ είναι επί. Ισοδύναμα ότι είναι 1-1 (αφού G πεπερασμένο σύνολο). Έστω $a,b\in G$ με $a^2=b^2.$ Επειδή η τάξη της G είναι $2m+1$ έχουμε $a^{2m+1}=b^{2m+1}$. Από τις δύο ισότητες και την άσκηση 6.28 έπεται το ζητούμενο.

16.

Υπόδειξη: Με επιχείρημα παρόμοιο με τη λύση της προηγούμενης άσκησης έπεται ότι κάθε στοιχείο περιττής τάξης της G είναι τετράγωνο.

17.

a. Αληθεύει. Επειδή $105=3\cdot 5\cdot 7$, από του Θεώρημα του Lagrange έπεται ότι η μέγιστη τάξη που μπορεί να έχει γνήσια υποομάδα της G είναι $5\cdot 7=35$. Αφού $|H|>35,$ παίρνουμε $|H|=|G|$ και άρα $H=G.$

b. Αληθεύει. Υπάρχουν $x,y\in\mathbb{Z}$ με $36x+105y=\mu\kappa\delta(36,105)=3$ και επομένως αν $g^{36}=1$, τότε $g^3=(g^{36})^x(g^{105})^y=1^x1^y=1.$

18.

Υπόδειξη: Αν $g\in G-\{1\}$, και $|G|=p^n$, τότε $|g|=p^m, 1\leq m\leq n$. Θεωρήστε το $g^{p^{m-1}}$ και εφαρμόστε την Πρόταση 4.3.11 2.

19.

Απάντηση:

a. Η S_4 δεν έχει στοιχείο τάξης 6.

b. Η A_4 δεν έχει στοιχείο τάξης 6.

c. Η $\mathbb{Z}_n$ έχει την ιδιότητα (I). Πράγματι, η ομάδα $\left\langle \frac{n}{m}\right\rangle\leq\mathbb{Z}_n$ έχει τάξη m.

d. Η D_4 έχει την ιδιότητα (I). Πράγματι, η κυκλική υποομάδα που παράγεται από τη στροφή κατά γωνία $\frac{2\pi}{4}$ έχει τάξη m.

20.

Απάντηση: Μια επιλογή παραδειγμάτων είναι:

a. $G=\mathbb{C}-\{0\}$ και $H=E_n$, $n>1.$

b. $G=\mathbb{R}$ και $H=\mathbb{Z}$.

c. $G=\mathbb{Z}$ και $H=2\mathbb{Z}$.

21.

Ξέρουμε ότι $[G:H]=\left|\{gH\,|\,g\in G\}\right|$. Επειδή $[G:H]=n<\infty,$ ανάμεσα στα στοιχεία $H, gH, g^2H, ..., g^nH\in\{gH\,|\,g\in G\}$, υπάρχουν δύο που είναι ίσα. Άρα $g^iH=g^jH$, όπου $1\leq i,j\leq n$ και $i>j$. Άρα $g^{i-j}\in H$.

22.

a. Οι αριστερές κλάσεις της $\mathbb{R}_{>0}$ στην $\mathbb{R}^*$ είναι οι $\mathbb{R}_{>0}$ και $\mathbb{R}_{<0}$.

b. Έστω $H\leq\mathbb{R}^*$ με $[\mathbb{R}^*:H]=2$ και $\alpha\in\mathbb{R}_{>0}$. Έχουμε ξένη ένωση $\mathbb{R}^*=H\cup xH$ για κάποιο $x\in\mathbb{R}^*$. Παρατηρούμε ότι $x^2\in H$, γιατί διαφορετικά θα είχαμε $x^2\in xH\Rightarrow x\in H$ που δεν αληθεύει.

Αν $a \in \mathbb{R}_{>0}$, τότε θεωρώντας το $\sqrt{a}$, έχουμε $\sqrt{a} \in H$ ή $\sqrt{a} \in xH$. Στην πρώτη περίπτωση παίρνουμε $a = (\sqrt{a})^2 \in H$ γιατί $H \leq \mathbb{R}^*$. Ση δεύτερη περίπτωση παίρνουμε $\sqrt{a} = xh$ για κάποιο $h \in H$, οπότε $a = (\sqrt{a})^2 = x^2h^2 \in H$ σύμφωνα με την παρατήρηση. Συνεπώς σε κάθε περίπτωση $a \in \mathbb{R}_{>0}$ που σημαίνει ότι $\mathbb{R}_{>0} \subseteq H$.

Αν υπάρχει αρνητικός πραγματικός $b \in H$, τότε για κάθε αρνητικό πραγματικό c έχουμε $c = b\frac{c}{b} \in H$ αφού $\frac{c}{b} \in \mathbb{R}_{>0} \subseteq H$. Δηλαδή έχουμε $H = \mathbb{R}^*$, άτοπο αφού $[\mathbb{R}^* : H] \neq 1$.

23.

Έστω $aH \cap bK \neq \varnothing$. Τότε υπάρχει $c \in G$ με $c \in aH, c \in bK$. Από $c \in aH$ έχουμε $a^{-1}c \in H$ και άρα $cH = aH$ και όμοια από $c \in bK$ έχουμε $cK = bK$. Άρα $aH \cap bK = (cH) \cap (cK)$. Θα δείξουμε τώρα ότι $(cH) \cap (cK) = c(H \cap K)$. Είναι σαφές ότι $(cH) \cap (cK) \supseteq c(H \cap K)$. Έστω $a \in (cH) \cap (cK)$. Τότε υπάρχουν $h \in H, k \in K$ με $a = ch = ck$. Άρα $h = k \in H \cap K$. Συνεπώς $a \in c(H \cap K)$.

24.

Υπόδειξη: Δείξτε ότι η απεικόνιση $f : \{g(H \cap K) | g \in K\} \to \{gH | g \in G\}, f\left(g(H \cap K)\right) = gH$ είναι

- καλά ορισμένη, και
- 1-1.

25.

a. Υπόδειξη: Από $[G : H] < \infty$ και την προηγούμενη άσκηση έχουμε $[K : H \cap K] < \infty$, δηλαδή $[K : H] < \infty$.
Η απεικόνιση $f : \{gH | g \in G\} \to \{gK | g \in G\}, f(gH) = gK$ είναι καλά ορισμένη (αφού $H \subseteq K$) και επί.
Άρα από $[G : H] < \infty$ προκύπτει $[G : K] < \infty$.
Για την απόδειξη της σχέσης $[G : H] = [G : K][K : H]$, έστω $G = a_1K \cup ...a_sK$ (ξένη ένωση) και $K = b_1H \cup ...b_tH$ (ξένη ένωση). Δείξτε ότι $G = \bigcup_{i,j} a_ib_jH$ (ξένη ένωση).

b. Από το προηγούμενο υποερώτημα, $[G : H \cap K] = [G : K][K : H \cap K]$. Από την άσκηση 7.24, $[K : H \cap K] \leq [G : H]$. Άρα $[G : H \cap K] \leq [G : H][G : K]$.

26.

a. Υπολογίζοντας την ανάλυση της σ σε γινόμενο ξένων κύκλων, βρίσκουμε $\sigma = (1427)(356)$. Η μετάθεση (1427) είναι περιττή (ως κύκλος με άρτιο μήκος) και η μετάθεση (356) είναι άρτια (ως κύκλος με περιττό μήκος). Άρα η σ είναι περιττή μετάθεση.

b. Έχουμε $\langle \sigma^m \rangle \leq A_7 \Leftrightarrow \sigma^m \in A_7$. Είδαμε πριν ότι η σ είναι περιττή. Άρα και η σ^{-1} είναι περιττή. Επειδή $\sigma^m = \sigma\sigma...\sigma$ (m φορές, αν $m > 0$) ή $\sigma^m = \sigma^{-1}\sigma^{-1}...\sigma^{-1}$ ($-m$ φορές, αν $m < 0$) παίρνουμε $\sigma^m \in A_7 \Leftrightarrow$ m άρτιος.

c. Δεν αληθεύει ότι υπάρχει $\tau \in S_7$ τέτοιο ώστε $\tau^{2000} = \sigma$ γιατί η μετάθεση τ^{2000} είναι άρτια και η σ είναι περιττή.

27.

Έστω $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & a & 1 & b & 6 & 7 & 3 \end{pmatrix} \in S_7$.

a. Επειδή η σ είναι 1-1, για το ζεύγος (a,b) έχουμε τις δυνατότητες $(a,b) = (2,4)$ ή $(a,b) = (4,2)$.
Υπολογίζοντας την ανάλυση της σ σε γινόμενο ξένων κύκλων, βρίσκουμε αντίστοιχα $\sigma = (15673)$ ή

$\sigma = (15673)(24)$. Η $\sigma = (15673)$ είναι άρτια (ως κύκλος με περιττό μήκος) και η $\sigma = (15673)(24)$ είναι περιττή (γινόμενο άρτιας και περιττής). Άρα $(a,b) = (2,4)$.

b. Δεν αληθεύει. Εφόσον η σ είναι άρτια, κάθε στοιχείο της ομάδας $\langle\sigma\rangle$ είναι άρτια μετάθεση, ενώ η $(15)(56)(67)$ είναι περιττή.

c. Έστω $m \in \mathbb{Z}$. Από το πρώτο υποερώτημα έχουμε $\sigma = (15673)$ ή $\sigma = (15673)(24)$. Άρα $\sigma^m = (15673)^m$ ή $\sigma^m = (15673)^m (24)^m$ (γιατί ξένοι κύκλοι αντιμετατίθενται). Σε κάθε περίπτωση έχουμε $\sigma^m(1) \in \{1,5,6,7,3\}$. Άρα $\sigma^m(1) \neq 2$. οπότε δεν αληθεύει ότι $(12) \in \langle\sigma\rangle$.

28.

Έστω A το σύνολο των άρτιων μεταθέσεων της G, B το σύνολο των περιττών μεταθέσεων της G και $\tau \in B$. Τότε έχουμε την ξένη ένωση $G = A \cup B$. Για την απεικόνιση $f : A \to B, f(\sigma) = \tau\sigma$, παρατηρούμε τα εξής.

- $f(\sigma) \in B$ για κάθε $\sigma \in A$, αφού $\tau\sigma \in G$ (η G είναι ομάδα) και η $\tau\sigma$ είναι περιττή (ως γινόμενο περιττής και άρτιας).
- Η f είναι 1-1, αφού αν $\tau\sigma_1 = \tau\sigma_2$, $\sigma_i \in A$, παίρνουμε $\sigma_1 = \sigma_2$.
- Η f είναι επί: Έστω $\rho \in B$. Τότε $\tau^{-1}\rho \in A_n$ (το γινόμενο δύο περιττών μεταθέσεων είναι άρτια μετάθεση) και $\tau^{-1}\rho \in G$ (αφού η G είναι ομάδα). Άρα $\tau^{-1}\rho \in A$. Έχουμε $f(\tau^{-1}\rho) = \tau(\tau^{-1}\rho) = \rho$.

Άρα $|A| = |B|$. Το ζητούμενο έπεται από την ξένη ένωση $G = A \cup B$.

29.

Έστω $H \leq S_n$ με περιττό δείκτη $[S_n : H]$. Αν $H \leq A_n$, τότε από το Πόρισμα 4.4.25 (βλ. και άσκηση 21a) έχουμε $[S_n : H] = [S_n : A_n][A_n : H]$ και άρα $[S_n : H] = 2[A_n : H]$, άρτιος. Άρα η H περιέχει τουλάχιστον μία περιττή μετάθεση.

30.

Υπόδειξη: Κάθε στοιχείο $\sigma \in S_6$ τάξης 6 είναι

- κύκλος μήκους 6 ή
- γινόμενο ενός κύκλου μήκους 2 και ενός κύκλου μήκους 3.

Και στις δυο περιπτώσεις η σ είναι περιττή μετάθεση. Άρα η A_6 δεν έχει στοιχείο τάξης 6.

Υπόδειξη: Αν $\sigma = (12)(34)(567) \in S_n$, $n \geq 7$, τότε $\sigma \in A_n$ και η τάξη της σ είναι 6.

31.

Υπόδειξη: Κάθε $\sigma \in S_n$ με περιττή τάξη είναι γινόμενο κύκλων με περιττά μήκη.

32.

33.

Υπόδειξη: Ποια είναι η τάξη του $[a] \in U(\mathbb{Z}_{a^n-1})$;

34.

35. Απάντηση:

a. Σωστό. Από $a^9 = 1$ και τη Πρόταση 4.3.11 έπεται ότι $|a|\,|9$. Από το Πόρισμα 4.4.23 έπεται ότι $|a|\,|20$. Άρα $|a|\,|\mu\kappa\delta(9,20) \Rightarrow |a| = 1 \Rightarrow a = 1$.

b. Λάθος.

c. Σωστό. Έστω $H = \langle a \rangle \cap \langle b^4 \rangle$. Από το Θεώρημα του Lagrange, $|H| \big| |\langle a \rangle| \Rightarrow |H| \big| |a| \Rightarrow |H| \big| 8$. Επίσης, $|H| \big| |\langle b^4 \rangle| \Rightarrow |H| \big| |b^4| \Rightarrow |H| \Big| \frac{10}{\mu\kappa\delta(10,4)} \Rightarrow |H| \big| 5$. Άρα $|H| \big| \mu\kappa\delta(8,5) \Rightarrow |H| = 1 \Rightarrow H = \{1\}$.

d. Σωστό. Ένας τρόπος είναι να δείξουμε ότι $\langle a^{28} \rangle \subseteq \langle a^{36} \rangle$ και $\langle a^{36} \rangle \subseteq \langle a^{28} \rangle$. Ισοδύναμα, $a^{28} \in \langle a^{36} \rangle$ και $a^{36} \in \langle a^{28} \rangle$. Ισοδύναμα, υπάρχει $x \in \mathbb{Z}$ με $36x \equiv 28 \bmod 100$ και υπάρχει $y \in \mathbb{Z}$ με $28x \equiv 36 \bmod 100$. Υπάρχουν τέτοιοι x, y σύμφωνα με το Θεώρημα 1.5.3 2).

Σημείωση: Θα δούμε άλλη λύση όταν μελετήσουμε τις υποομάδες κυκλικών ομάδων.

Ασκήσεις8
Ομομορφισμοί Ομάδων, Κυκλικές Ομάδες ΙΙ

1. Θεωρούμε την απεικόνιση $\varphi:\mathbb{Z}_{24}\to S_5$, $\varphi([k])=\sigma^k$, όπου $\sigma=(12)(345)$. Δείξτε τα εξής.
   a. Η φ είναι καλά ορισμένη.
   b. Η φ είναι ομομορφισμός ομάδων.
   c. $\ker\varphi=\langle[6]\rangle$.
   d. $\mathrm{Im}\,\varphi=\langle\sigma\rangle$.

2. Θεωρούμε την απεικόνιση $\varphi:\mathbb{Z}_{24}\to\mathbb{Z}_{20}$, $\varphi([m]_{24})=[5m]_{20}$. Δείξτε τα εξής.
   a. Η φ είναι καλά ορισμένη.
   b. Η φ είναι ομομορφισμός ομάδων.
   c. $\ker\varphi=\langle[4]_{24}\rangle$.
   d. $\mathrm{Im}\,\varphi=\langle[5]_{20}\rangle$.

3. Θεωρούμε την απεικόνιση $\varphi:\mathbb{R}\to\mathbb{C}-\{0\}$, $\varphi(r)=\cos(2\pi r)+i\sin(2\pi r)$.
   a. Δείξτε ότι η φ είναι ομομορφισμός ομάδων.
   b. Βρείτε τον πυρήνα και την εικόνα της.
   c. Δώστε μια εποπτική ερμηνεία της απεικόνισης φ.

4. Δείξτε ότι οι ομάδες G,H είναι ισόμορφες στις ακόλουθες περιπτώσεις.
   a. $G=\mathbb{R}_{>0}$ (με πράξη τον πολλαπλασιασμό πραγματικών) και $H=\mathbb{R}$.
   b. $G=\mathbb{R}-\{0\}$ (με πράξη τον πολλαπλασιασμό πραγματικών) και $H=\mathbb{R}_{>0}\times\{1,-1\}$.
   c. $G=m\mathbb{Z}$ και $H=n\mathbb{Z}$, όπου m,n είναι μη μηδενικοί ακέραιοι

5. Έστω $\varphi:G\to H$ ένας ομομορφισμός πεπερασμένων ομάδων. Δείξτε τα εξής.
   a. Για κάθε $g\in G$, $|\varphi(g)|\,\big|\,|g|$.
   b. Αν η $\mathrm{Im}\,\varphi$ έχει στοιχείο τάξης m, τότε η G έχει στοιχείο τάξης m.
   c. Αν $\mu\kappa\delta(|G|,|H|)=1$, τότε $\varphi(g)=1_H$ για κάθε $g\in G$.
   d. Έστω ότι $G=S_6$ και $H=S_3$. Δείξτε ότι $\sigma\in\ker\varphi$, όπου $\sigma=\begin{pmatrix}1&2&3&4&5&6\\2&3&4&5&1&6\end{pmatrix}$.

6. Να βρεθούν όλοι οι ομομορφισμοί ομάδων $\mathbb{Z}\to\mathbb{Z}$. Ποιοι από αυτούς είναι
   a. μονομορφισμοί ομάδων;
   b. επιμορφισμοί ομάδων;
   c. ισομορφισμοί ομάδων;
   d. ομομορφισμοί δακτυλίων;

7. Αν $a\in\mathbb{Q}$, με φ_a συμβολίζουμε την απεικόνιση $\varphi_a:\mathbb{Q}\to\mathbb{Q},\varphi_a(x)=ax$.
   a. Δείξτε ότι για κάθε $a\in\mathbb{Q}$, η φ_a είναι ομομορφισμός ομάδων.
   b. Δείξτε ότι κάθε ομομορφισμός ομάδων $\mathbb{Q}\to\mathbb{Q}$ είναι της μορφής φ_a.

8. Έστω $n\in\mathbb{Z}_{>0}$.
   a. Πόσοι ομομορφισμοί ομάδων $\mathbb{Z}_n\to\mathbb{Z}$ υπάρχουν;
   b. Πόσοι ομομορφισμοί ομάδων $\mathbb{Z}\to\mathbb{Z}_n$ υπάρχουν; Πόσοι από αυτούς είναι επί;

9. Έστω G,H πεπερασμένες κυκλικές ομάδες με τάξεις αντίστοιχα m,n.
   a. Δείξτε ότι το πλήθος των ομομορφισμών ομάδων $G\to H$ είναι ίσο με το $\mu\kappa\delta(m,n)$.
   b. Έστω $G=\mathbb{Z}_{24}$ και $H=\mathbb{Z}_{20}$. Βρείτε όλους τους ομομορφισμούς ομάδων $G\to H$.

10. Έστω R,S,T δακτύλιοι με μονάδες.
   a. Δείξτε ότι αν υπάρχει ισομορφισμός δακτυλίων $R\simeq S$, τότε υπάρχει ισομορφισμός ομάδων $U(R)\simeq U(S)$.

b. Δείξτε ότι αν υπάρχει ισομορφισμός δακτυλίων $R \times S \simeq T$, τότε υπάρχει ισομορφισμός ομάδων $U(R) \times U(S) \simeq U(T)$.

11. Έστω m, n θετικοί ακέραιοι.

a. Δείξτε ότι οι ομάδες $\mathbb{Z}_m \times \mathbb{Z}_n$ και $\mathbb{Z}_{mn}$ είναι ισόμορφες αν και μόνο αν $\mu\kappa\delta(m,n) = 1$.

b. Για ποια m, n η ομάδα $\mathbb{Z}_m \times \mathbb{Z}_n$ είναι κυκλική;

12. Έστω p ένας περιττός πρώτος. Δείξτε ότι οι ομάδες $U(\mathbb{Z}_p)$ και $U(\mathbb{Z}_{2p})$ είναι ισόμορφες.

13. Για ποια n υπάρχει

a. επιμορφισμός ομάδων $G \to S_n$, όπου G αβελιανή;

b. μονομορφισμός ομάδων $S_n \to G$, όπου G αβελιανή;

14. Δείξτε ότι η ομάδα $G = \{2^m 3^n \in \mathbb{Q} \,|\, m, n \in \mathbb{Z}\}$ (με πράξη το συνήθη πολλαπλασιασμό ρητών) είναι ισόμορφη με την ομάδα $\mathbb{Z} \times \mathbb{Z}$.

15. Δείξτε ότι η απεικόνιση $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \varphi(x, y) = 28x + 49y$, είναι ομομορφισμός ομάδων. Ποια είναι η εικόνα της;

16. Υπάρχει ομάδα G τέτοια ώστε $G \times \mathbb{Z}_4 \simeq \mathbb{Z}_{40} \times \mathbb{Z}_2$;

17. Δείξτε ότι η ομάδα S_n περιέχει υποομάδα ισόμορφη με τη

a. $\mathbb{Z}_m$ για κάθε $m = 1, ..., n$,

b. S_m για κάθε $m = 1, ..., n$.

18. Έστω G μια ομάδα. Θεωρούμε το σύνολο $Aut(G)$ όλων των ισομορφισμών $G \to G$.

a. Δείξτε ότι με την πράξη της σύνθεσης συναρτήσεων, το $Aut(G)$ είναι ομάδα.

b. Δείξτε ότι αν $G = \mathbb{Z}_n$, τότε $Aut(G) \simeq U(\mathbb{Z}_n)$.

c. Ποια είναι η τάξη της ομάδας $Aut(E_{100})$, όπου $E_n = \left\{ z \in \mathbb{C} \,\middle|\, z^n = 1 \right\}$;

19. Έστω G μια κυκλική ομάδα τάξης 10.

a. Να βρεθούν όλες οι υποομάδες της G.

b. Για κάθε υποομάδα H της G να βρεθούν όλες οι κλάσεις gH.

20. Να βρεθούν όλες οι υποομάδες της $U(\mathbb{Z}_{25})$.

21. Έστω $G = \langle a \rangle$ μια κυκλική ομάδα τάξης 36 και $H = \langle a^{32} \rangle$.

a. Ποια είναι η τάξη της H;

b. Να βρεθούν όλα τα $g \in G$ τέτοια ώστε $\langle g \rangle = H$.

22. Έστω G μια πεπερασμένη κυκλική ομάδα και $H, K \leq G$. Δείξτε ότι $|H \cap K| = \mu\kappa\delta(|H|, |K|)$.

23. Έστω $G = \langle a \rangle$ μια κυκλική ομάδα τάξης 100.

a. Αληθεύει ότι $\langle a^{28} \rangle = \langle a^{36} \rangle$;

b. Να βρεθεί ένας γεννήτορας της ομάδας $\langle a^{22} \rangle \cap \langle a^{55} \rangle$ και η τάξη της.

c. Να βρεθούν όλοι οι γεννήτορες της $\langle a^{22} \rangle \cap \langle a^{55} \rangle$.

24. Έστω G πεπερασμένη κυκλική ομάδα τάξης n.

a. Δείξτε ότι για κάθε θετικό διαιρέτη d του n, το πλήθος των στοιχείων τάξης d της G ισούται με $\varphi(d)$, όπου φ είναι η συνάρτηση του Euler. Ειδικά, το πλήθος των γεννητόρων της G ισούται με $\varphi(n)$.

b. Χρησιμοποιώντας το προηγούμενο αποτέλεσμα, δείξτε ότι $n = \sum_{d|n} \varphi(d)$, όπου το d διατρέχει τους θετικούς διαιρέτες του n.

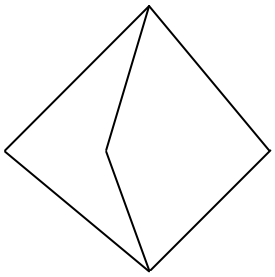
c. Έστω d θετικός διαιρέτης του n. Δείξτε ότι η εξίσωση $x^d = 1$ έχει ακριβώς d λύσεις στη G.

d. Δώστε ένα παράδειγμα ομάδας για την οποία το συμπέρασμα του προηγούμενου ερωτήματος δεν αληθεύει.

25. Για καθεμιά από τις ακόλουθες περιπτώσεις, σχεδιάστε το διάγραμμα υποομάδων μια κυκλικής ομάδας με τη δοσμένη τάξη. Για κάθε υποομάδα του διαγράμματος βρείτε ένα γεννήτορα.

a. 125
b. p^3, όπου p πρώτος
c. 18
d. pq^2, όπου p, q διαφορετικοί πρώτοι.

26. Υπάρχει κυκλική ομάδα με διάγραμμα υποομάδων της ακόλουθης μορφής;



27. Για κάθε μια από τις επόμενες ομάδες, να βρεθούν όλες οι υποομάδες της.

a. $\left\{\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix} \in GL_2(\mathbb{R}) \middle| m \in \mathbb{Z}\right\}$

b. $\left\{\begin{pmatrix}[1] & [m]\\ 0 & [1]\end{pmatrix} \in GL_2(\mathbb{Z}_{18}) \middle| m \in \mathbb{Z}_{18}\right\}$

28. Έστω G μια ομάδα με $|G| \le 180$ τέτοια ώστε η G έχει υποομάδα τάξης 7 και υποομάδα τάξης 13.

a. Δείξτε ότι κάθε γνήσια υποομάδα της G είναι κυκλική.
b. Δείξτε ότι αν η G είναι αβελιανή, τότε η G είναι κυκλική.
c. Είναι δυνατό η G να περιέχει στοιχείο τάξης 2;

29. Έστω $n \in \mathbb{Z}_{>0}$, $n > 1$. Δείξτε ότι κάθε κυκλική ομάδα τάξης $n^5 - n$ έχει υποομάδα τάξης 30.

Στις ασκήσεις 29-32 βρίσκουμε όλους τους $n \in \mathbb{Z}_{>0}$ για τους οποίους η ομάδα $U(\mathbb{Z}_n)$ είναι κυκλική. Το τελικό αποτέλεσμα είναι (Gauss):

Η $U(\mathbb{Z}_n)$ είναι κυκλική αν και μόνο αν $n = 1, 2, 4, p^m, 2p^m$, όπου p περιττός πρώτος.

Ο παρακάτω τρόπος απόδειξης είναι αυτός του άρθρου D.R. Guichard, When is $U(n)$ cyclic? An algebraic approach, *Mathematics Magazine* 72(2) (1999), 139-142. Μια άλλη απόδειξη υπάρχει στην Εφαρμογή 4.8.3.

30. Δείξτε ότι η ομάδα $U(\mathbb{Z}_n)$ δεν είναι κυκλική αν το n διαιρείται από 2 διαφορετικούς περιττούς πρώτους αριθμούς. Υπόδειξη: Έχουμε $n = ab$, όπου $a, b > 2$ και $\mu\kappa\delta(a,b) = 1$. Ξέρουμε ότι υπάρχει ισομορφισμός δακτυλίων $\mathbb{Z}_{ab} \simeq \mathbb{Z}_a \times \mathbb{Z}_b$. Εφαρμόστε την Άσκηση 10.

31. Δείξτε ότι για κάθε $m \ge 3$, η ομάδα $U(\mathbb{Z}_{2^m})$ δεν είναι κυκλική. Υπόδειξη: Αρκεί να δείξουμε ότι η $U(\mathbb{Z}_{2^m})$, $m \ge 3$, έχει τουλάχιστον 2 στοιχεία τάξης 2. Δείξτε ότι τα στοιχεία $[-1]$ και $[2^{m-1}+1]$ είναι διαφορετικά και έχουν τάξη 2.

32. * Έστω p περιττός πρώτος. Στην άσκηση αυτή δείχνουμε ότι οι ομάδες $U(\mathbb{Z}_{p^m}), m \ge 2,$ είναι κυκλικές χρησιμοποιώντας ότι η ομάδα $U(\mathbb{Z}_p)$ είναι κυκλική.

a. Έστω $[a]_p$ ένας γεννήτορας της κυκλικής ομάδας $U(\mathbb{Z}_p)$. Δείξτε ότι τουλάχιστον ένα από τα στοιχεία $[a]_{p^2}, [a+p]_{p^2}$ είναι γεννήτορας της $U(\mathbb{Z}_{p^2})$. Άρα η ομάδα $U(\mathbb{Z}_{p^2})$ είναι κυκλική.
b. Δείξτε ότι αν το $[b]_{p^2}$ είναι γεννήτορας της $U(\mathbb{Z}_{p^2})$, τότε το $[b]_{p^m}$ είναι γεννήτορας της $U(\mathbb{Z}_{p^m})$, $m \ge 3$. Άρα η ομάδα $U(\mathbb{Z}_{p^m})$ είναι κυκλική.

33. Η $U(\mathbb{Z}_n)$ είναι κυκλική αν και μόνο αν $n=1,2,4,p^m,2p^m$, όπου p περιττός πρώτος.

34. Για κάθε θετικό ακέραιο n θεωρούμε το δακτύλιο $R_n=\dfrac{\mathbb{Z}_2[x]}{\langle (x+1)^n\rangle}$ και την ομάδα $G_n=U(R_n)$. Δείξτε τα εξής.

a. $|G_n|=2^n-2^{n-1}$.

b. Η G_3 είναι κυκλική.

c. Η G_4 δεν είναι κυκλική.

35. Θεωρούμε το δακτύλιο $R=\left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\in M_2(\mathbb{Z})\,\middle|\, a,b,d\in\mathbb{Z}\right\}$.

a. Αληθεύει ότι $\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}\in U(R)$;

b. Αληθεύει ότι η ομάδα $U(R)$ είναι κυκλική;

36. Αν $\varphi: S_n\to G$ είναι ομομορφισμός ομάδων όπου η G είναι αβελιανή, τότε $A_n\subseteq \ker\varphi$.

37. Εξετάστε ποιες από τις ακόλουθες προτάσεις αληθεύουν. Δικαιολογήστε την απάντησή σας.

a. Υπάρχει n τέτοιο ώστε υπάρχει μονομορφισμός ομάδων $S_3\to\mathbb{Z}_n$.

b. Κάθε ομομορφισμός ομάδων $A_{n+1}\to S_n$, $n>1$, έχει μη τετριμμένο πυρήνα.

c. Αν η ομάδα G έχει τουλάχιστον 3 στοιχεία τάξης 6, τότε η G δεν είναι κυκλική.

d. Αν η ομάδα G έχει υποομάδα τάξης 20 και ακριβώς 3 γνήσιες μη τετριμμένες υποομάδες, τότε η G δεν είναι κυκλική.

e. Κάθε κύκλος μήκους 3 ή 5 της S_n ανήκει στον πυρήνα κάθε ομομορφισμού ομάδων $S_n\to\mathbb{Z}_{64}$.

f. Αν το διάγραμμα υποομάδων μια κυκλικής ομάδας G είναι της παρακάτω μορφής, τότε $|G|=p^3$ για κάποιο πρώτο p.

g. Αν G είναι πεπερασμένη ομάδα τέτοια ώστε κάθε γνήσια υποομάδα της είναι κυκλική, τότε η G είναι κυκλική.

Υποδείξεις/Απαντήσεις
Ασκήσεις8

1.

Αρχικά παρατηρούμε ότι $|\sigma| = \varepsilon\kappa\pi(2,3) = 6$, αφού το δεξί μέλος της $\sigma = (12)(345)$ είναι γινόμενο ξένων κύκλων με μήκη 2 και 3.

a. $[k] = [k'] \Rightarrow 24 | k - k' \Rightarrow 6 | k - k' \Rightarrow \sigma^k = \sigma^{k'}$.

b. Για κάθε $[k], [k'] \in \mathbb{Z}_{24}$ έχουμε, $\varphi([k] + [k']) = \varphi([k + k']) = \sigma^{k+k'} = \sigma^k \sigma^{k'} = \varphi([k])\varphi([k'])$.

c. $\ker\varphi = \left\{ [k] \in \mathbb{Z}_{24} \middle| \sigma^k = 1 \right\}$. Επειδή $|\sigma| = 6$ έχουμε $\sigma^k = 1 \Leftrightarrow 6 | k$. Άρα $\ker\varphi = \left\{ [k] \in \mathbb{Z}_{24} \middle|\ 6 | k \right\} = \langle [6] \rangle$.

d. $\mathrm{Im}\varphi = \left\{ \sigma^k \in S_5 \middle| [k] \in \mathbb{Z}_{24} \right\} = \left\{ \sigma^k \in S_5 \middle| k \in \mathbb{Z} \right\} = \langle \sigma \rangle$.

2.

a. $[k]_{24} = [k']_{24} \Rightarrow 24 | k - k' \Rightarrow 4 | k - k' \Rightarrow 20 | 5k - 5k' \Rightarrow [5k]_{20} = [5k']_{20}$.

b. Για κάθε $[k]_{24}, [k']_{24} \in \mathbb{Z}_{24}$ έχουμε,
$\varphi([k]_{24} + [k']_{24}) = \varphi([k + k']_{24}) = [k + k']_{20} = [k]_{20} + [k']_{20} = \varphi([k]_{24}) + \varphi([k']_{24})$.

c. $\ker\varphi = \left\{ [k]_{24} \in \mathbb{Z}_{24} \middle| [5k]_{20} = [0]_{20} \right\}$. Έχουμε $[5k]_{20} = [0]_{20} \Leftrightarrow 20 | 5k \Leftrightarrow 4 | k$. Άρα
$\ker\varphi = \left\{ [k]_{24} \in \mathbb{Z}_{24} \middle|\ 4 | k \right\} = \langle [4]_{24} \rangle$.

d. $\mathrm{Im}\varphi = \left\{ [5k]_{20} \in \mathbb{Z}_{20} \middle| [k]_{24} \in \mathbb{Z}_{24} \right\} = \left\{ [5k]_{20} \in \mathbb{Z}_{20} \middle| k \in \mathbb{Z} \right\} = \langle [5]_{20} \rangle$.

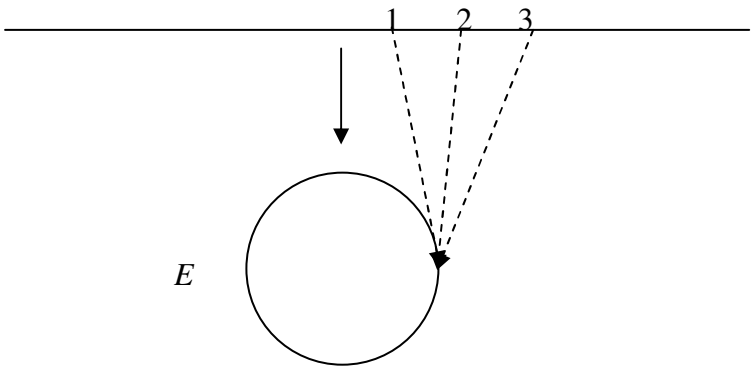
3.

a. Για κάθε $r, s \in \mathbb{R}$ έχουμε
$$\begin{aligned}\varphi(r+s) &= \cos(2\pi(r+s)) + i\sin(2\pi(r+s)) = \\ &= \cos(2\pi r)\cos(2\pi s) - \sin(2\pi r)\sin(2\pi s) + i\left(\sin(2\pi r)\cos(2\pi s) + \sin(2\pi s)\cos(2\pi r)\right) = \\ &= \left(\cos(2\pi r) + i\sin(2\pi r)\right)\left(\cos(2\pi s) + i\sin(2\pi s)\right) = \\ &= \varphi(r)\varphi(s).\end{aligned}$$
Στη δεύτερη ισότητα χρησιμοποιήσαμε τις ταυτότητες
$\cos(x+y) = \cos x \cos y - \sin x \sin y,\ \sin(x+y) = \sin x \cos y + \sin y \cos x$.

b. Έχουμε $Ker\varphi = \left\{ r \in \middle| \cos(2\pi r) + i\sin(2\pi r) = 0 \right\} = \mathbb{Z}$. Επίσης,
$\mathrm{Im}\varphi = \left\{ z \in \mathbb{C} \middle| z = \cos(2\pi r) + i\sin(2\pi r),\ r \in \mathbb{R} \right\} = \left\{ z \in \mathbb{C} \middle| |z| = 1 \right\} = E$, όπου με $|z|$ συμβολίζουμε το μέτρο του μιγαδικού z.

c. Η απεικόνιση φ 'επιμηκύνει' τον άξονα $\mathbb{R}$ κατά λόγο 2π και τον 'τυλίγει' γύρω από το μοναδιαίο κύκλο E έτσι ώστε τα σημεία του $\mathbb{R}$ που αντιστοιχούν στο $\mathbb{Z}$ να απεικονίζονται στο $(1,0)$

$\mathbb{R}$



4.

Βλ. Παραδείγματα 4.5.10 3,4.

5.

a. Έστω $g \in G$ και $|g| = k$. Τότε $g^k = 1_G \Rightarrow \varphi(g^k) = \varphi(1_G) \Rightarrow \varphi(g)^k = 1_H \Rightarrow |\varphi(g)| | k$, όπου στην τελευταία συνεπαγωγή χρησιμοποιήσαμε την Πρόταση 4.3.11 1.

b. Έστω $h = \varphi(g) \in \mathrm{Im}(\varphi)$ με $|h| = m$. Από το προηγούμενο υποερώτημα, $m | k$, όπου $k = |g|$. Το στοιχείο $g^{\frac{k}{m}}$ έχει τάξη m (αυτό έπεται άμεσα από τον ορισμό της τάξης).

c. Έστω $g \in G$. Έχουμε $|\varphi(g)| \| H|$ σύμφωνα με το Πόρισμα 4.4.23. Από το ίδιο Πόρισμα έχουμε $|g| \| G|$. Από το υποερώτημα a έχουμε $|\varphi(g)| \| g|$ και άρα $|\varphi(g)| \| G|$. Συνεπώς $|\varphi(g)| | \mu\kappa\delta(|G|, |H|)$, οπότε $|\varphi(g)| = 1 \Rightarrow \varphi(g) = 1_H$.

d. Έχουμε $\sigma = (12345)$, οπότε $|\sigma| = 5$. Από το υποερώτημα a, $|\varphi(\sigma)| | 5$. Από $\varphi(\sigma) \in S_3$, έχουμε $|\varphi(\sigma)| \| S_3|$, δηλαδή $|\varphi(\sigma)| | 6$. Άρα $|\varphi(\sigma)| = 1 \Rightarrow \varphi(\sigma) = 1 \Rightarrow \sigma \in \ker\varphi$.

6.

Απάντηση: Αν $a \in \mathbb{Z}$, με φ_a συμβολίζουμε την απεικόνιση $\varphi_a : \mathbb{Z} \to \mathbb{Z}, \varphi_a(x) = ax$. Οι ομομορφισμοί ομάδων $\mathbb{Z} \to \mathbb{Z}$ είναι οι φ_a, όπου $a \in \mathbb{Z}$.

a. φ_a μονομορφισμός ομάδων $\Leftrightarrow a \neq 0$.

b. φ_a επιμορφισμός ομάδων $\Leftrightarrow a = 1, -1$.

c. φ_a ισομορφισμός ομάδων $\Leftrightarrow a = 1, -1$.

d. φ_a ομομορφισμός δακτυλίων $\Leftrightarrow a = 0, 1$.

7.

b. Έστω $\psi : \mathbb{Q} \to \mathbb{Q}$ ομομορφισμός ομάδων. Για $m, n \in \mathbb{Z}, n \neq 0,$ έχουμε

$$\psi(1) = \psi\left(n\frac{1}{n}\right) = n\psi\left(\frac{1}{n}\right) \Rightarrow \psi\left(\frac{1}{n}\right) = \psi(1)\frac{1}{n},$$

οπότε

$$\psi\left(\frac{m}{n}\right) = \psi\left(m\frac{1}{n}\right) = m\psi\left(\frac{1}{n}\right) = \psi(1)\frac{m}{n}.$$

Δηλαδή $\psi = \varphi_a$, όπου $a = \psi(1)$.

8.

a. Έστω $\varphi:\mathbb{Z}_n\to\mathbb{Z}$ ομομορφισμός ομάδων. Τότε $0=\varphi([0])=\varphi([n])=\varphi(n[1])=n\varphi([1])\Rightarrow\varphi([1])=0,$ αφού $n\neq 0$. Άρα για κάθε $[a]\in\mathbb{Z}_n,$ έχουμε $\varphi([a])=a\varphi([1])=0.$ Συνεπώς υπάρχει μοναδικός ομομορφισμός ομάδων $\varphi:\mathbb{Z}_n\to\mathbb{Z}$, ο τετριμμένος, $\varphi([a])=0$ για κάθε $[a]\in\mathbb{Z}_n$.

b. Υπόδειξη: Αν $\varphi:\mathbb{Z}\to\mathbb{Z}_n$ είναι ομομορφισμός ομάδων, τότε ο φ καθορίζεται από την τιμή $\varphi(1)$, αφού $\varphi(m)=m\varphi(1)$ για κάθε $m\in\mathbb{Z}$.

Απάντηση: Οι ομομορφισμοί ομάδων $\mathbb{Z}\to\mathbb{Z}_n$ είναι οι $\varphi_0,\varphi_1,...,\varphi_{n-1}$, όπου $\varphi_i(m)=[im]$, $m\in\mathbb{Z}$. Το πλήθος αυτών είναι n. Ο φ_i είναι επί αν και μόνο αν $\mu\kappa\delta(i,n)=1$. Το πλήθος των φ_i, $i=0,1,...,n-1,$ που είναι επί είναι η τιμή της συνάρτησης του Euler στο n.

9.

a. Έστω $|G|=m, G=\langle g\rangle, |H|=n, H=\langle h\rangle$ και $d=\mu\kappa\delta(m,n)$. Έστω $\varphi:G\to H$ ομομορφισμός ομάδων. Επειδή $H=\{1,h,h^2,...,h^{n-1}\}$ έχουμε $\varphi(g)=h^a,$ για κάποιο $a\in\{0,1,...,n-1\}$. Τότε $\left(h^a\right)^m=\varphi(g)^m\Rightarrow h^{am}=\varphi(g^m)=\varphi(1_G)=1_H$, οπότε έχουμε $|h|\,|am$ σύμφωνα με την Πρόταση 4.3.11.

Δηλαδή $n|am$, αφού $|h|=|H|$. Επειδή $d|m$ και $d|n$, παίρνουμε $\frac{n}{d}\Big|a\frac{m}{d}$ και επειδή $\mu\kappa\delta(\frac{m}{d},\frac{n}{d})=1,$ παίρνουμε

$$\frac{n}{d}|a\,.$$

Άρα $a=\frac{n}{d}i$ για κάποιο $i\in\{0,1,...,d-1\}$. Για κάθε $k\in\mathbb{Z}$ έχουμε

$$\varphi(g^k)=(\varphi(g))^k=h^{ak}=h^{\frac{n}{d}ik}\,. \qquad (1)$$

Βλέπουμε δηλαδή ότι ο φ δίνεται από τη σχέση (1) για κατάλληλο i.

Για κάθε $i=0,1,...,d-1$, ορίζουμε μια απεικόνιση $\varphi_i:G\to H, \varphi_i(g^k)=h^{\frac{n}{d}ik}$.

Παρατηρούμε τα εξής:

- Η φ_i είναι καλά ορισμένη: Αν $g^k=g^{k'}$, τότε $m|k-k'$ και άρα $m\frac{n}{d}\Big|\frac{n}{d}i(k-k')\Rightarrow n\frac{m}{d}\Big|\frac{n}{d}i(k-k')\Rightarrow n\Big|\frac{n}{d}i(k-k')\Rightarrow h^{\frac{n}{d}ik}=h^{\frac{n}{d}ik'}$.
- Η φ_i είναι ομομορφισμός ομάδων: Αυτό είναι άμεσο.
- Αν $i\neq j$, τότε $\varphi_i\neq\varphi_j$: Αν $\varphi_i=\varphi_j$, τότε $\varphi_i(g)=\varphi_j(g)\Rightarrow h^{\frac{n}{d}i}=h^{\frac{n}{d}j}\Rightarrow n\Big|\frac{n}{d}(i-j)\Rightarrow i=j$ γιατί $0\le i,j\le d-1$.
- Αν $\varphi:G\to H$ είναι ομομορφισμός ομάδων, τότε υπάρχει $i\in\{0,1,...,d-1\}$ με $\varphi_i=\varphi$: Το αποδείξαμε πιο πάνω.

Από τα προηγούμενα έπεται οι ομομορφισμοί ομάδων $G\to H$ είναι οι φ_i, όπου $i=0,1,...,d-1$. Το πλήθος τους είναι d.

b. Με τους συμβολισμούς της απόδειξης του υποερωτήματος a, έχουμε:

$$m=24,\ n=20,\ d=\mu\kappa\delta(m,n)=4,\ \frac{n}{d}=5\,.$$

Άρα υπάρχουν ακριβώς 4 ομομορφισμοί ομάδων $\mathbb{Z}_{24}\to\mathbb{Z}_{20}$, οι $\varphi_0,\varphi_1,\varphi_2,\varphi_3$ που ορίζονται ως εξής (εδώ έχουμε προσθετικό συμβολισμό, π.χ. αντί της 'δύναμης' h^5 έχουμε το 'πολλαπλάσιο' $5h$):

$$\varphi_0([k]_{24}) = [0]_{20},$$
$$\varphi_1([k]_{24}) = [5k]_{20},$$
$$\varphi_2([k]_{24}) = [10k]_{20},$$
$$\varphi_3([k]_{24}) = [15k]_{20}.$$

[Σημείωση: Η απεικόνιση της άσκησης 8.1 ήταν η φ_1.]

10.

a. Βλ. άσκηση 5.6.
b. Υπόδειξη: Από την άσκηση 3.13c έχουμε $U(R\times S) = U(R)\times U(S)$. Από το προηγούμενο υποερώτημα, υπάρχει ισομορφισμός ομάδων $U(T) \simeq U(R)\times U(S)$.

11.

12.

Υπόδειξη: 1ος τρόπος. Έχουμε έναν ισομορφισμό δακτυλίων $\mathbb{Z}_{2p} \simeq \mathbb{Z}_2 \times \mathbb{Z}_p$ (βλ. Εφαρμογή σελ. 132). Εφαρμόζοντας την άσκηση 7.10 έχουμε έναν ισομορφισμό ομάδων $U(\mathbb{Z}_{2p}) \simeq U(\mathbb{Z}_2)\times(\mathbb{Z}_p)$. Παρατηρούμε ότι η $U(\mathbb{Z}_2)$ είναι η τετριμμένη ομάδα. Άρα $U(\mathbb{Z}_{2p}) \simeq U(\mathbb{Z}_p)$.

2ος τρόπος: Δείξτε ότι η απεικόνιση $\varphi : \mathbb{Z}_{2p} \to \mathbb{Z}_p, [a]_{2p} \mapsto [a]_p$, είναι καλά ορισμένη και έχει την ιδιότητα $\varphi(U(\mathbb{Z}_{2p})) \subseteq U(\mathbb{Z}_p)$. Δείξτε ότι ο περιορισμός της φ στο $U(\mathbb{Z}_{2p})$ δίνει έναν ισομορφισμό ομάδων $U(\mathbb{Z}_{2p}) \simeq U(\mathbb{Z}_p)$.

13.

Παρατηρούμε ότι αν $\varphi : G \to H$ είναι ένας επιμορφισμός ομάδων και η G είναι αβελιανή, τότε και η H είναι αβελιανή. Πράγματι, έστω $h_1, h_2 \in H$. Επειδή η φ είναι επί υπάρχουν $g_1, g_2 \in G$ με $h_i = \varphi(g_i)$. Άρα $h_1h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1g_2) = \varphi(g_2g_1) = \varphi(g_2)\varphi(g_1) = h_2h_1$.

a. Αν υπάρχει επιμορφισμός ομάδων $G \to S_n$, όπου G αβελιανή, τότε και η S_n είναι αβελιανή. Άρα $n = 1, 2$.
b. Αν υπάρχει μονομορφισμός ομάδων $S_n \to G$, όπου G αβελιανή, τότε η S_n είναι ισόμορφη με υποομάδα αβελιανής ομάδας και άρα η S_n είναι αβελιανή. Άρα $n = 1, 2$.

14.

Υπόδειξη: Η απεικόνιση $G \to \mathbb{Z}\times\mathbb{Z},\ 2^m3^n \mapsto (m,n),$ είναι καλά ορισμένη και ισομορφισμός ομάδων.

15.

Απάντηση: Η εικόνα είναι η υποομάδα $d\mathbb{Z} = \langle d \rangle$, όπου $d = \mu\kappa\delta(28,49) = 7$.

16.

Αν υπήρχε ομάδα G τέτοια ώστε $G\times\mathbb{Z}_4 \simeq \mathbb{Z}_{40}\times\mathbb{Z}_2$, τότε $|G\times\mathbb{Z}_4| \simeq |\mathbb{Z}_{40}\times\mathbb{Z}_2| \Rightarrow 4|G| = 80 \Rightarrow |G| = 20$. Στην ομάδα $\mathbb{Z}_{40}\times\mathbb{Z}_2$ υπάρχει στοιχείο τάξης 40, πχ το $([1]_{40},[1]_2)$, αλλά στην $G\times\mathbb{Z}_4$ δεν υπάρχει στοιχείο τάξης 40 αφού (χρησιμοποιώντας προσθετικό συμβολισμό) $20(a,b) = (0_G, 0_{\mathbb{Z}_4})$ για κάθε $(a,b) \in G\times\mathbb{Z}_4$.

17.

Απάντηση:

a. $\langle\sigma\rangle$, όπου $\sigma \in S_n$ είναι κύκλος μήκους m.
b. $\{\sigma \in S_n \,|\, \sigma(i) = i \ \ \forall i = m+1, ..., n\}$.

18.

b. Υπόδειξη: Δείξτε αν $\varphi \in Aut(\mathbb{Z}_n)$, τότε $\varphi([1]) \in U(\mathbb{Z}_n)$. Στη συνέχεια, δείξτε ότι η απεικόνιση $Aut(\mathbb{Z}_n) \to U(\mathbb{Z}_n), \varphi \mapsto \varphi(1)$, είναι μονομορφισμός ομάδων. Δείξτε ότι είναι επί (βλ. και άσκηση 9a).

19.

a. Σύμφωνα με το Θεώρημα 4.6.3 γ), αν d είναι θετικός διαιρέτης της τάξης μιας πεπερασμένης κυκλικής ομάδας $G = \langle a \rangle$, ξέρουμε ότι υπάρχει μοναδική υποομάδα H_d της G τάξης d και μάλιστα $H_d = \left\langle a^{\frac{n}{d}} \right\rangle$, $n = |G|$. Επίσης, οι παραπάνω υποομάδες ομάδες H_d είναι όλες οι υποομάδες της G.
Στη συγκεκριμένη άσκηση έχουμε $n = 10$. Άρα υπάρχουν 4 υποομάδες,
$$H_{10} = G, H_5 = \langle a^2 \rangle, H_2 = \langle a^5 \rangle, H_1 = \{1\}.,$$

b. Απάντηση: οι κλάσεις της $H_5 = \langle a^2 \rangle$ στη G είναι οι H_5, aH_5 και οι κλάσεις της $H_2 = \langle a^5 \rangle$ στη G είναι οι $H_2, aH_2, a^2H_2, a^3H_2, a^4H_2$.

20.

Υπόδειξη: Δείξτε ότι η $U(\mathbb{Z}_{25})$ είναι κυκλική (ένας γεννήτορας είναι το [2]) και εφαρμόστε το Θεώρημα 4.6.3 γ) όπως στην προηγούμενη άσκηση.

21.

a. Έχουμε $|H| = \left|\langle a^{32} \rangle\right| = |a^{32}|$. Από τη Πρόταση 4.3.11 2 έχουμε $|a^{32}| = \frac{|a|}{\mu\kappa\delta(|a|, 32)} = \frac{36}{\mu\kappa\delta(36, 32)} = 9$.
Άρα $|H| = 9$.

b. Επειδή η G είναι κυκλική έχουμε $\langle g \rangle = H \Leftrightarrow |\langle g \rangle| = |H|$ σύμφωνα με το Θεώρημα 4.6.3 γ). Έστω $g = a^k$. Τότε $|\langle g \rangle| = |g| = \frac{36}{\mu\kappa\delta(36, k)}$. Άρα
$$|\langle g \rangle| = |H| \Leftrightarrow \frac{36}{\mu\kappa\delta(36, k)} = 9 \Leftrightarrow \mu\kappa\delta(36, k) = 4 \Leftrightarrow$$
το 4 διαιρεί το k και το 3 δεν διαιρεί το k $\Leftrightarrow k \equiv 4, 8 \bmod 12$.
Συνεπώς ανάμεσα στα στοιχεία της $G = \{1, a, a^2, ..., a^{35}\}$, έχουμε $g = a^4, a^8, a^{16}, a^{20}, a^{28}, a^{32}$.

22.

Έστω $m = |H|, n = |K|$ και $d = \mu\kappa\delta(m, n)$. Θα δείξουμε ότι $|H \cap K| = d$
Επειδή $H \cap K \le H$, έχουμε $|H \cap K| | m$ σύμφωνα με το Θεώρημα του Lagrange. Όμοια, $|H \cap K| | n$. Άρα $|H \cap K| \le d$.
Υπενθύμιση: Αν k είναι θετικός διαιρέτης της τάξης μιας πεπερασμένης κυκλικής ομάδας $G = \langle a \rangle$, ξέρουμε ότι υπάρχει μοναδική υποομάδα H_k της G τάξης k και μάλιστα $H_k = \left\langle a^{\frac{t}{k}} \right\rangle$, $t = |G|$.
Συνεπώς $H = \left\langle a^{\frac{t}{m}} \right\rangle$ και $K = \left\langle a^{\frac{t}{n}} \right\rangle$. Επειδή $d | m$, έχουμε $\frac{t}{m} | \frac{t}{d}$ και άρα $a^{\frac{t}{d}} \in H$. Δηλαδή $H_d \subseteq H$. Όμοια $H_d \subseteq K$. Άρα $H_d \subseteq H \cap K$, πράγμα που σημαίνει ότι $d \le |H \cap K|$.
Άρα $d = |H \cap K|$.

23.

Έστω $G = \langle a \rangle$ μια κυκλική ομάδα τάξης 100.

a. $1^{ος}$ τρόπος. Από το Θεώρημα 4.6.3 γ) έπεται ότι $\langle a^{28}\rangle = \langle a^{36}\rangle \Leftrightarrow |a^{28}| = |a^{36}|$. Υπολογίζοντας τις τάξεις έχουμε $|a^{28}| = \dfrac{100}{\mu\kappa\delta(100,28)} = 25$ και $|a^{36}| = \dfrac{100}{\mu\kappa\delta(100,36)} = 25$. Άρα $\langle a^{28}\rangle = \langle a^{36}\rangle$.

$2^{ος}$ τρόπος. Από το Θεώρημα 1.5.3 2, έπεται ότι υπάρχει ακέραιος x με $28x \equiv 36 \bmod 100$. Άρα $a^{36} \in \langle a^{28}\rangle$. Όμοια, υπάρχει ακέραιος y με $36y \equiv 28 \bmod 100$. Άρα $a^{28} \in \langle a^{36}\rangle$. Συνεπώς $\langle a^{36}\rangle \subseteq \langle a^{28}\rangle$ και $\langle a^{28}\rangle \subseteq \langle a^{36}\rangle$, οπότε $\langle a^{28}\rangle = \langle a^{36}\rangle$.

b. Έχουμε $|a^{22}| = \dfrac{100}{\mu\kappa\delta(100,22)} = 50$ και $|a^{55}| = \dfrac{100}{\mu\kappa\delta(100,55)} = 20$. Από την άσκηση 8.22, η τάξη της $\langle a^{22}\rangle \cap \langle a^{55}\rangle$ είναι 10. Συνεπώς ένας γεννήτορας της $\langle a^{22}\rangle \cap \langle a^{55}\rangle$ είναι το στοιχείο $a^{\frac{100}{10}} = a^{10}$.

c. Από τη μοναδικότητα της υποομάδας τάξης 10 της G, έπεται ότι το a^k είναι γεννήτορας της $\langle a^{22}\rangle \cap \langle a^{55}\rangle$ αν και μόνο αν $|a^k| = |\langle a^{22}\rangle \cap \langle a^{55}\rangle| = 10$, δηλαδή $\dfrac{100}{\mu\kappa\delta(k,100)} = 10 \Leftrightarrow \mu\kappa\delta(k,100) = 10.$

Συνεπώς μεταξύ των στοιχείων της $G = \{1, a, a^2, ..., a^{99}\}$ οι γεννήτορες της $\langle a^{22}\rangle \cap \langle a^{55}\rangle$ είναι οι $a^{10}, a^{30}, a^{70}, a^{90}$.

24.

a. Έστω $G = \{1, a, a^2, ..., a^{n-1}\}$. Πρώτα δείχνουμε την ειδική περίπτωση $d = n$. Έχουμε $|a^k| = n \Leftrightarrow \dfrac{n}{\mu\kappa\delta(n,k)} = n \Leftrightarrow \mu\kappa\delta(n,k) = 1$. Συνεπώς το πλήθος των a^k, $0 \le k \le n-1$, με $|a^k| = n$ είναι ίσο με $\varphi(n)$.

Έστω τώρα d τυχαίος θετικός διαιρέτης του n. Επειδή κάθε στοιχείο της G τάξης d ανήκει στη μοναδική υποομάδα H_d της G τάξης d και επειδή η H_d είναι κυκλική, συμπεραίνουμε ότι το πλήθος των στοιχείων αυτών είναι ίσο με $\varphi(d)$, σύμφωνα με την ειδική περίπτωση που είδαμε πριν.

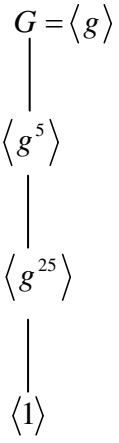
b. Έπεται άμεσα από το ερώτημα a.

c. Παρατηρήστε ότι αν $g \in G$, τότε $g^d = 1 \Leftrightarrow g \in H_d$.

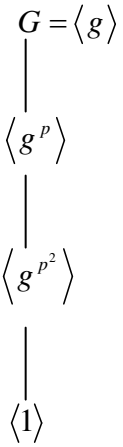
d. Στην ομάδα S_3, η εξίσωση $x^2 = 1$ έχει 4 λύσεις.

25.

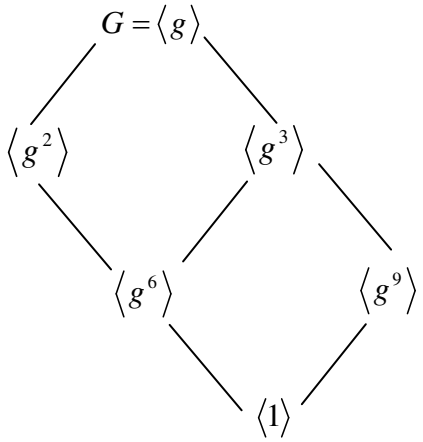
a.



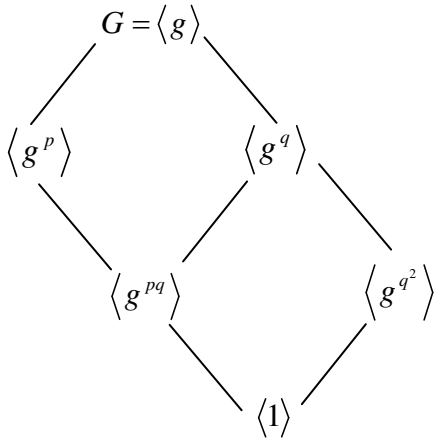
b.



c.



d.



26.

Αν το δοσμένο διάγραμμα ήταν το διάγραμμα υποομάδων μιας κυκλικής ομάδας G, τότε η G θα είχε ακριβώς 5 υποομάδες. Δηλαδή, η τάξη n της G θα είχε ακριβώς 5 θετικούς διαιρέτες (Θεώρημα 4.6.3 γ). Άρα $n = p^4$ για κάποιο πρώτο p. Τότε, όμως, για κάθε $H, K \leq G$ θα είχαμε $H \leq K$ ή $K \leq H$. Δηλαδή στο διάγραμμα υποομάδων της G κάθε δύο κορυφές συνδέονται με ανοδική διαδοχή ακμών. Αυτό δεν συμβαίνει στο δοσμένο διάγραμμα.

27.

Υπόδειξη:

a. Έστω $H=\left\{\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix}\in GL_2(\mathbb{R})\middle| m\in\mathbb{Z}\right\}$. Δείξτε ότι η απεικόνιση $\varphi:\mathbb{Z}\to H, m\mapsto\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix}$ είναι ισομορφισμός ομάδων. Επειδή οι υποομάδες της ομάδας $\mathbb{Z}$ είναι οι $d\mathbb{Z}$, $d\in\mathbb{N}$, παίρνουμε μέσω του ισομορφισμού φ ότι οι υποομάδες της H είναι οι $\varphi(d\mathbb{Z})=\left\{\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix}\in GL_2(\mathbb{R})\middle| m\in d\mathbb{Z}\right\}, d\in\mathbb{N}$.

b. Έστω $\left\{\begin{pmatrix}[1] & [m]\\ 0 & [1]\end{pmatrix}\in GL_2(\mathbb{Z}_{18})\middle| m\in\mathbb{Z}_{18}\right\}$. Δείξτε ότι η απεικόνιση $\varphi:\mathbb{Z}_{18}\to H, [m]\mapsto\begin{pmatrix}1 & [m]\\ 0 & 1\end{pmatrix}$ είναι ισομορφισμός ομάδων. Επειδή οι υποομάδες της ομάδας $\mathbb{Z}_{18}$ είναι οι $\langle[d]\rangle$, όπου $d\in\mathbb{N}$ και $d\,|\,18$, δηλαδή $d=1,2,3,6,9,18$, παίρνουμε μέσω του ισομορφισμού φ ότι οι υποομάδες της H είναι οι $\varphi(\langle[d]\rangle)=\left\{\begin{pmatrix}1 & [m]\\ 0 & 1\end{pmatrix}\in GL_2(\mathbb{Z}_{18})\middle|[m]\in\langle[d]\rangle\right\}, d\in\mathbb{N}, d\,|\,n$.

28.

Από το Θεώρημα του Lagrange έχουμε $7\,\|G|$ και $13\,\|G|$. Επειδή οι $7,13$ είναι σχετικά πρώτοι έχουμε $91\,\|G|$. Τότε από $|G|\le 180$ έπεται ότι $|G|=91$.

a. Επειδή $|G|=91$, κάθε γνήσια υποομάδα της G έχει τάξη 1,7, ή 13. Ξέρουμε ότι κάθε ομάδα με τάξη πρώτο αριθμό είναι κυκλική. Άρα κάθε γνήσια υποομάδα της G είναι κυκλική.

b. Έστω ότι η G είναι αβελιανή. Υπάρχει υποομάδα τάξης 7. Αυτή είναι κυκλική αφού το 7 είναι πρώτος. Έστω a ένας γεννήτορας της υποομάδας αυτής. Τότε $|a|=7$. Με όμοιο τρόπο έχουμε την ύπαρξη $b\in G$ με $|b|=13$. Σύμφωνα με την άσκηση 7.11, έχουμε $|ab|=7\cdot 13=91$ και άρα $G=\langle ab\rangle$, κυκλική.

c. Η G δεν έχει στοιχείο τάξης 2, γιατί $|G|=91$, που δεν είναι άρτιος.

29.

Υπόδειξη: Έστω $n\in\mathbb{Z}_{>0}$, $n>1$, και G κυκλική ομάδα τάξης n^5-n. Ξέρουμε ότι για κάθε θετικό διαιρέτη d της τάξης της G υπάρχει (μοναδική) υποομάδα της G τάξης d. Όπως ακριβώς στο Παράδειγμα 1.4.9 3, αποδεικνύεται ότι $30\,|\,n^5-n$.

30.

Υπόδειξη: Έχουμε $n=ab$, όπου $a,b>2$ και $\mu\kappa\delta(a,b)=1$. Ξέρουμε ότι υπάρχει ισομορφισμός δακτυλίων $\mathbb{Z}_{ab}\simeq\mathbb{Z}_a\times\mathbb{Z}_b$. Εφαρμόστε την Άσκηση 10.

31.

Υπόδειξη: Αρκεί να δείξουμε ότι η $U(\mathbb{Z}_{2^m})$, $m\ge 3$, έχει τουλάχιστον 2 στοιχεία τάξης 2. Δείξτε ότι τα στοιχεία $[-1]$ και $[2^{m-1}+1]$ είναι διαφορετικά και έχουν τάξη 2.

32.

a. Έστω $[a]_p$ ένας γεννήτορας της κυκλικής ομάδας $U(\mathbb{Z}_p)$. Δείξτε ότι τουλάχιστον ένα από τα στοιχεία $[a]_{p^2}, [a+p]_{p^2}$ είναι γεννήτορας της $U(\mathbb{Z}_{p^2})$.

b. Δείξτε ότι αν το $[b]_{p^2}$ είναι γεννήτορας της $U(\mathbb{Z}_{p^2})$, τότε το $[b]_{p^m}$ είναι γεννήτορας της $U(\mathbb{Z}_{p^m})$, $m\ge 3$.

33.

34.

a. Υπόδειξη: Κάθε στοιχείο του R_n έχει μοναδική παράσταση της μορφής $f(x)+\langle (x+1)^n \rangle$, όπου $\deg f(x) < n$. Το $f(x)+\langle (x+1)^n \rangle$ είναι αντιστρέψιμο αν και μόνο αν $\mu\kappa\delta(f(x),(x+1)^n)=1$ (βλ. άσκηση 5.23), ισοδύναμα $f(1)\neq 0$.

c. Απάντηση: Η G_4 έχει περισσότερα του ενός στοιχείου τάξης 2 , για παράδειγμα τα $x^2+\langle x^4+1\rangle$ και $x^3+x+1+\langle x^4+1\rangle$. Άρα δεν είναι κυκλική.

35.

a. Δεν αληθεύει.

b. Δεν αληθεύει. Η ομάδα $U(R)$ είναι άπειρη και περιέχει στοιχείο με πεπερασμένη τάξη διάφορο του 1. Για παράδειγμα, το $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in U(R)$ έχει τάξη 2. Κάθε άπειρη κυκλική ομάδα δεν έχει στοιχείο πεπερασμένης τάξης διάφορου του 1 (γιατί;).

36.

Υπόδειξη: Αν ρ, τ είναι αντιμεταθέσεις, τότε είναι συζυγή στοιχεία και, επειδή η G είναι αβελιανή, έχουμε $\varphi(\rho)=\varphi(\tau)$. Συνεπώς $\varphi(\rho\tau)=1$.

37.

Απάντηση:

a. Λ.

b. Σ. Έχουμε $|A_{n+1}|=\frac{(n+1)!}{2}$ και $|S_n|=n!$. Άρα για κάθε $n\geq 2$ έχουμε $|A_{n+1}|>|S_n|$. Συνεπώς κάθε απεικόνιση $A_{n+1}\to S_n$, $n\geq 2$, δεν είναι 1-1.

c. Σ. Η G έχει υποομάδα τάξης 6. Αν ήταν κυκλική, θα είχε μοναδική υποομάδα τάξης 6. Αυτή η υποομάδα έχει $\varphi(6)=2$ στοιχεία τάξης 6, άτοπο από την υπόθεση. (Χρησιμοποιήσαμε ότι το πλήθος των γεννητόρων μιας κυκλικής ομάδα τάξης n είναι ίσο με την τιμή της συνάρτησης του Euler στο *n*).

d. Σ. Αν G είναι κυκλική ομάδα που περιέχει υποομάδα τάξης 20, τότε η G περιέχει υποομάδα τάξης d για κάθε θετικό διαιρέτη d του 20. Δηλαδή θα είχε υποομάδες με τάξεις 20,10,5,4,2 και 1. Άρα η G έχει τουλάχιστον 4 γνήσιες μη τετριμμένες υποομάδες, άτοπο από την υπόθεση.

e. Σ.

f. Σ.

g. Λ. Ένα αντιπαράδειγμα είναι η S_3.

Ασκήσεις9
Κανονικές υποομάδες, ομάδα πηλίκο

1. Σε καθεμιά από τις ακόλουθες περιπτώσεις, εξετάστε αν η υποομάδα H της ομάδας G είναι κανονική.

a. $H=\{1,(12)\}, G=S_3$.

b. $H=\{1,(123),(213)\}, G=S_3$.

c. $H=\{\sigma\in S_4 \,|\, \sigma(4)=4\}$, $G=S_4$.

d. $H=\langle\sigma\rangle$, $\sigma=(1234)$, $G=S_4$.

e. $H=\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a,b,c\in\mathbb{R}, ac\neq 0\right\}$, $G=GL_2(\mathbb{R})=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in M_2(\mathbb{R}) \middle| ad-bc\neq 0\right\}$.

f. $H=\left\{\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \middle| m\in\mathbb{Z}\right\}$, $G=\left\{\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \middle| r\in\mathbb{R}\right\}$.

2. Αληθεύει ότι υπάρχει ομομορφισμός ομάδων $\varphi: S_4\to G$ με $\ker\varphi=\langle\sigma\rangle$, όπου $\sigma=(1234)$;

3. Δείξτε ότι η υποομάδα $SL_n(\mathbb{R})=\{A\in M_n(\mathbb{R}) \,|\, \det A=1\}$ της $GL_n(\mathbb{R})=\{A\in M_n(\mathbb{R}) \,|\, \det A\neq 0\}$ είναι κανονική και ότι υπάρχει ισομορφισμός ομάδων $GL_n(\mathbb{R})/SL_n(\mathbb{R})\simeq\mathbb{R}-\{0\}$.

4.

a. Δείξτε ότι οι κανονικές υποομάδες της S_3 είναι οι $S_3, A_3, \{1\}$.

b. Αν $\varphi: S_3\to H$ είναι ομομορφισμός ομάδων που δεν είναι μονομορφισμός, τότε $\varphi((123))=1_H$.

5. Υπάρχει ισομορφισμός ομάδων $\mathbb{R}/\mathbb{Z}\simeq E$, όπου $E=\{z\in\mathbb{C} \,|\, |z|=1\}$.

6. Δείξτε ότι η ομάδα $\mathbb{Q}/\mathbb{Z}$ είναι άπειρη και κάθε στοιχείο της έχει πεπερασμένη τάξη.

7. Αν $\varphi: G\to H$ είναι ομομορφισμός ομάδων και N είναι κανονική υποομάδα της G, τότε η $\varphi(N)$ είναι κανονική υποομάδα της $\varphi(G)$.

8. Έστω G μια ομάδα και $Z(G)=\{a\in G \,|\, ag=ga\ \forall g\in G\}$ (το *κέντρο* της G). Δείξτε ότι κάθε υποομάδα της $Z(G)$ είναι κανονική υποομάδα της G.

9. Έστω G μια ομάδα και H μια υποομάδα της $Z(G)$. Αν η ομάδα G/H είναι κυκλική, τότε η G είναι αβελιανή.

10. Έστω G μια ομάδα. Με $Aut(G)$ συμβολίζουμε το σύνολο των ισομορφισμών $G\to G$. Αν $a\in G$, ορίζουμε την απεικόνιση $\varphi_a: G\to G, \varphi_a(g)=a^{-1}ga$.

a. Δείξτε ότι το $Aut(G)$ με πράξη τη σύνθεση απεικονίσεων είναι μια ομάδα.

b. Δείξτε ότι $\varphi_a\in Aut(G)$ για κάθε $a\in G$.

c. Έστω $Inn(G)=\{\varphi_a \,|\, a\in G\}$. Δείξτε ότι η $InnG$ είναι κανονική υποομάδα της $Aut(G)$ και υπάρχει ισομορφισμός ομάδων $G/Z(G)\simeq Inn(G)$.

11. Έστω G μια ομάδα και $m\in\mathbb{Z}_{>0}$. Αν υπάρχει μοναδική υποομάδα $H\leq G$ με $|H|=m$, τότε η H είναι κανονική στη G.

12. Έστω G μια ομάδα με $|G|=210$ και N μια κανονική υποομάδα της G με $|N|=7$.

a. Δείξτε ότι $g^{30}\in N$ για κάθε $g\in G$.

b. Δείξτε ότι αν $g^7\in N$, όπου $g\in G$, τότε $g\in N$.

c. Έστω $g\in G$. Δείξτε την ισοδυναμία $g\in N\Leftrightarrow g^{37}\in N$.

13. Αν G είναι ομάδα και $H\leq G$ με $[G:H]=2$, τότε η H είναι κανονική υποομάδα της G.

14. Έστω G μια ομάδα, $H\leq G, K\leq G$, $[G:H]=[G:K]=2$ και $H\neq K$.

a. Δείξτε ότι η $H \cap K$ είναι κανονική υποομάδα της G.

b. Δείξτε ότι η $\frac{G}{H \cap K}$ δεν είναι κυκλική.

15. Έστω G μια ομάδα και H μια κυκλική κανονική υποομάδα της G. Δείξτε ότι κάθε υποομάδα της H είναι κανονική υποομάδα της G.

16. Αν H, K είναι κανονικές υποομάδες της ομάδας G και $H \cap K = \{1\}$, τότε $hk = kh$ για κάθε $h \in H$ και $k \in K$.

17. Έστω G_1, G_2 ομάδες. Δείξτε ότι η ομάδα $G = G_1 \times G_2$ έχει κανονική υποομάδα ισόμορφη με τη G_i, $i = 1, 2$.

18. Έστω $\varphi : G \to H$ ομομορφισμός ομάδων.

a. Δείξτε ότι αν N είναι κανονική υποομάδα της H, τότε το σύνολο $\varphi^{-1}(N) = \{ g \in G \,|\, \varphi(g) \in H \}$ είναι κανονική υποομάδα της G.

b. Έστω ότι $H = \mathbb{Z}_n$, $n > 0$, και η φ είναι επί. Δείξτε ότι για κάθε θετικό διαιρέτη d του n υπάρχει κανονική υποομάδα K της G με $[G : K] = d$

19. Έστω G μια ομάδα και N μια κανονική υποομάδα της G. Δείξτε ότι αν η N είναι άπειρη κυκλική ομάδα $N = \langle a \rangle$, τότε $g^2 a = a g^2$ για κάθε $g \in G$.

20. Εξετάστε ποιες από τις ακόλουθες προτάσεις είναι σωστές. Δικαιολογήστε την απάντησή σας.

a. Αν $\varphi : G \to H$ είναι επιμορφισμός ομάδων που δεν είναι ισομορφισμός και $|G| = 77$, τότε η H είναι αβελιανή.

b. Αν $\varphi : G \to H$ είναι ομομορφισμός ομάδων, $|G| = 20$ και $|H| = 26$, τότε $|\mathrm{Im}\,\varphi| = 1, 2$.

Υποδείξεις/Απαντήσεις
Ασκήσεις9

1.

a. Η H δεν είναι κανονική υποομάδα της S_3, αφού, για παράδειγμα, $(13)^{-1}(12)(13) = (13(12)(13) = (23) \notin H$.
b. Η H είναι κανονική υποομάδα της S_3. Εδώ $H = A_3$.
c. Η H δεν είναι κανονική υποομάδα της S_4. Πράγματι, έστω $h \in H, h(1) \neq 1$. Τότε αν $\tau = (14)^{-1}h(14)$, παρατηρούμε ότι $\tau(4) \neq 4$, δηλαδή $\tau \notin H$. Πράγματι, αν $\tau(4) = 4$, τότε $4 = \left((14)^{-1}h(14)\right)(4) \Rightarrow 1 = \left(h(14)\right)(4) \Rightarrow 1 = h(1).$
d. Η H δεν είναι κανονική υποομάδα της S_4. Για παράδειγμα, $(12)^{-1}(1234)(12) = (2134) \notin H$, αφού $H = \left\{1, \sigma, \sigma^2, \sigma^3\right\} = \left\{1, (1234), (12)(34), (4321)\right\}$.
e. Η H δεν είναι κανονική υποομάδα της $GL_2(\mathbb{R})$. Για παράδειγμα, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} \notin H$.
f. Η H είναι κανονική υποομάδα της G, αφού η G είναι αβελιανή.

2.

Δεν υπάρχει ομομορφισμός ομάδων $\varphi : S_4 \to G$ με $\ker\varphi = \langle\sigma\rangle$, όπου $\sigma = (1234)$, γιατί η υποομάδα $\ker\varphi$ της S_4 είναι κανονική, ενώ, όπως είδαμε στην προηγούμενη άσκηση, η $\langle\sigma\rangle$ δεν είναι κανονική υποομάδα της S_4.

3.

Η απεικόνιση $\det : GL_n(\mathbb{R}) \to \mathbb{R} - \{0\}, A \mapsto \det(A)$, όπου $\det(A)$ είναι η ορίζουσα του A, είναι επιμορφισμός ομάδων με πυρήνα το $SL_n(\mathbb{R})$. Άρα η $SL_n(\mathbb{R})$ είναι κανονική υποομάδα της $GL_n(\mathbb{R})$ και από το 1ο Θεώρημα Ισομορφισμών Ομάδων έχουμε $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R} - \{0\}$.

4.

a. Υπόδειξη: Οι υποομάδες της S_3 είναι οι $\{1\}, \{1,(12)\}, \{1,(23)\}, \{1,(13)\}, \{1,(123),(321)\} = A_3, S_3$.
b. Λύση: Αν $\varphi : S_3 \to H$ είναι ομομορφισμός ομάδων που δεν είναι μονομορφισμός, τότε $\ker\varphi \neq \{1\}$. Επειδή $\ker\varphi$ είναι κανονική υποομάδα της S_3, θα είναι η S_3 ή η A_3 σύμφωνα με το προηγούμενο υποερώτημα. Σε κάθε περίπτωση, $(123) \in Ker\varphi$.

5.

Υπόδειξη: Εφαρμόστε το το 1ο Θεώρημα Ισομορφισμών Ομάδων στον ομομορφισμό της άσκησης 3 από τις Ασκήσεις8.

6.

Υπενθυμίζουμε ότι αν $a, b \in \mathbb{Q}$, τότε έχουμε $a + \mathbb{Z} = b + \mathbb{Z} \Leftrightarrow a - b \in \mathbb{Z}$. Συνεπώς τα ακόλουθα στοιχεία του $\mathbb{Q}/\mathbb{Z}$

$$\frac{1}{2} + \mathbb{Z},\ \frac{1}{2^2} + \mathbb{Z},\ \frac{1}{2^3} + \mathbb{Z},\ \ldots$$

είναι ανά δύο διαφορετικά. Άρα η ομάδα $\mathbb{Q}/\mathbb{Z}$ είναι άπειρη.

Έστω $\frac{m}{n}+\mathbb{Z}\in\mathbb{Q}/\mathbb{Z}$, όπου $m,n\in\mathbb{Z}$, $n\neq 0$. Τότε $n(\frac{m}{n}+\mathbb{Z})=m+\mathbb{Z}=\mathbb{Z}=0_{\mathbb{Q}/\mathbb{Z}}$. Άρα το στοιχείο $\frac{m}{n}+\mathbb{Z}\in\mathbb{Q}/\mathbb{Z}$ έχει πεπερασμένη τάξη.

7.

Ξέρουμε ότι $\varphi(N)\leq\varphi(G)$ (αφού $N\leq G$ και φ ομομορφισμός ομάδων). Επειδή η N είναι κανονική υποομάδα της G έχουμε

$$g^{-1}ng\in N$$

για κάθε $g\in G$ και κάθε $n\in N$. Έστω $a\in\varphi(G)$ και $b\in\varphi(N)$. Τότε υπάρχουν $g\in G,n\in N$ με $a=\varphi(g),b=\varphi(n)$. Έχουμε

$$a^{-1}ba=\varphi(g)^{-1}\varphi(n)\varphi(g)=\varphi(g^{-1})\varphi(n)\varphi(g)=\varphi(g^{-1}ng)\in\varphi(N).$$

Άρα η $\varphi(N)$ είναι κανονική υποομάδα της $\varphi(G)$.

8.

Έστω $H\leq Z(G)$. Επειδή $Z(G)\leq G$ (βλ. άσκηση 4 από τις Ασκήσεις7) έχουμε $H\leq G$. Έστω $g\in G$ και $h\in H$. Επειδή $H\subseteq Z(G)$ έχουμε $hg=gh$. Άρα $g^{-1}hg=g^{-1}gh=h\in H$. Συνεπώς η H είναι κανονική στη G.

9.

Έστω ότι η G/H είναι κυκλική, $G/H=\langle aH\rangle$, και $g_1,g_2\in G$. Τότε υπάρχουν ακέραιοι m,n με $g_1H=(aH)^m=a^mH$ και $g_2H=(aH)^n=a^nH$. Έχουμε $g_1=g_11_G\in g_1H=a^mH\Rightarrow g_1=a^mh_1$ για κάποιο $h_1\in H$. Όμοια $g_2=a^mh_2$ για κάποιο $h_2\in H$. Άρα

$$g_1g_2=a^mh_1a^nh_2=a^ma^nh_1h_2=a^{m+n}h_1h_2,$$

γιατί $h_1a^n=a^nh_1$ αφού $h_1\in Z(G)$. Όμοια $g_2g_1=a^{m+n}h_1h_2$ και άρα $g_1g_2=g_2g_1$.

10.

Υπόδειξη: c.

- Δείξτε ότι $Inn(G)\leq Aut(G)$
- Αν $\psi\in Aut(G)$ και $\varphi_a\in Inn(G)$, δείξτε ότι $\psi^{-1}\circ\varphi_a\circ\psi=\varphi_{\psi^{-1}(a)}$. Η σχέση αυτή λέει ότι η υποομάδα $Inn(G)$ της $Aut(G)$ είναι κανονική.
- Θεωρήστε την απεικόνιση $G\to Inn(G),a\mapsto\varphi_{a^{-1}}$. Δείξτε ότι είναι επιμορφισμός ομάδων και έχει πυρήνα το $Z(G)$. Άρα $G/Z(G)\simeq Inn(G)$ από το $1^{\text{ο}}$ Θεώρημα Ισομορφισμών Ομάδων.

11.

Υπόδειξη: Για κάθε $g\in G$, το σύνολο $g^{-1}Hg$ είναι μια υποομάδα της G (αυτό έπεται εύκολα χρησιμοποιώντας το Λήμμα 4.3.3 ή άμεσα από το υποερώτημα b της προηγούμενης άσκησης) και $|g^{-1}Hg|=|H|$. Από τη μοναδικότητα της υπόθεσης έπεται ότι $g^{-1}Hg=H$ για κάθε $g\in G$.

12.

a. Επειδή η υποομάδα N της G είναι κανονική, το σύνολο G/N είναι ομάδα με πράξη που ορίζεται από $(aN)(bN) = abN$. Έχουμε $|G/N| = \frac{|G|}{|N|} = \frac{210}{7} = 30.$ Άρα για κάθε $g \in G$ έχουμε, σύμφωνα με το Πόρισμα 4.4.23, $(gN)^{30} = 1_{G/N} = N \Rightarrow g^{30}N = N \Rightarrow g^{30} \in N$.

b. Αν $g^7 \in N$, όπου $g \in G$, τότε στην ομάδα G/N έχουμε

$$(gN)^7 = g^7 N = N = 1_{G/N} \Rightarrow |gN| \mid 7,$$

σύμφωνα με την Πρόταση 4.3.11. Από το Πόρισμα 4.4.23 έχουμε

$$|gN| \mid |G/N| \Rightarrow |gN| \mid 30.$$

Άρα $|gN| \mid \mu\kappa\delta(30,7) \Rightarrow |gN| = 1 \Rightarrow gN = N \Rightarrow g \in N$.

c. Η συνεπαγωγή $g \in N \Rightarrow g^{37} \in N$ είναι σαφής. Αντίστροφα, έστω $g^{37} \in N$. Από το υποερώτημα a έχουμε $g^{30} \in N$. Επειδή οι $37, 30$ είναι σχετικά πρώτοι, υπάρχουν ακέραιοι x, y με $1 = 37x + 30y$. Άρα $g = g^{37x+30y} = (g^{37})^x (g^{30})^y \in N$ αφού $N \leq G$.

13.

Βλ. Λήμμα 4.7.9.

14.

b. Υπόδειξη: Δείξτε ότι οι $\frac{H}{H \cap K}, \frac{K}{H \cap K}$ είναι διαφορετικές υποομάδες της $\frac{G}{H \cap K}$ και $\left|\frac{H}{H \cap K}\right| = \left|\frac{K}{H \cap K}\right| = 2$. Άρα η G δεν είναι κυκλική σύμφωνα με το Θεώρημα 4.6.3 γ).

15.

Έστω $H = \langle a \rangle$ και $K \leq H$. Τότε $K = \langle a^m \rangle$ για κάποιο ακέραιο m σύμφωνα με το Θεώρημα 4.6.3 α). Επειδή η $H = \langle a \rangle$ είναι κανονική στη G, για κάθε $g \in G$ υπάρχει ακέραιος r με $g^{-1}ag = a^r$. Τότε $(g^{-1}ag)^m = a^{rm}$, δηλαδή

$$g^{-1}a^m g = a^{rm}.$$

Έστω $k \in K = \langle a^m \rangle$. Τότε $k = (a^m)^n$ για κάποιο ακέραιο n. Άρα

$$g^{-1}kg = g^{-1}(a^m)^n g = \left(g^{-1}a^m g\right)^n = (a^{rm})^n = (a^m)^{rn} \in \langle a^m \rangle = K.$$

Συνεπώς η K είναι κανονική υποομάδα της G.

16.

Για κάθε $h \in H$ και $k \in K$ έχουμε $k^{-1}hk \in H$ γιατί η H είναι κανονική υποομάδα της G. Άρα $h^{-1}k^{-1}hk \in H$ γιατί η H είναι υποομάδα. Όμοια παίρνουμε $h^{-1}k^{-1}hk \in K$. Άρα $h^{-1}k^{-1}hk \in H \cap K = \{1\} \Rightarrow h^{-1}k^{-1}hk = 1 \Rightarrow hk = kh$.

17.

Υπόδειξη: Δείξτε ότι το σύνολο $\{(g_1, 1_{G_2}) \in G_1 \times G_2 \mid g_1 \in G_1\}$ είναι υποομάδα της $G_1 \times G_2$ και ότι είναι ισόμορφη με τη G_1.

18.

19.

Επειδή η $N = \langle a \rangle$ είναι κανονική υποομάδα της G, υπάρχουν ακέραιοι r, s με

$$gag^{-1} = a^r,$$
$$g^{-1}ag = a^s.$$

Άρα $a^{rs} = (a^r)^s = (gag^{-1})^s = ga^s g^{-1} = g(g^{-1}ag)g^{-1} = a.$ Από $a^{rs} = a$ και το γεγονός ότι το a έχει άπειρη τάξη παίρνουμε $rs = 1$. Άρα $r = s = 1$ ή $r = s = -1$. Σε κάθε περίπτωση εύκολα επαληθεύεται ότι $g^2 a = ag^2$ για κάθε $g \in G$.

20.

a. Σ. Έχουμε $\ker\varphi \neq \{1\}$. Άρα $|G/\ker\varphi| = 1, 7, 11$. Συνεπώς η ομάδα $G/\ker\varphi$ είναι κυκλική (έχει τάξη 1 ή πρώτο αριθμό) και άρα αβελιανή. Από το 1ο Θεώρημα Ισομορφισμών Ομάδων, $H \simeq G/\ker\varphi$. Άρα H αβελιανή.

b. Σ. Από το Θεώρημα του Lagrange έχουμε $|\mathrm{Im}\,\varphi| \mid 26$. Από το 1ο Θεώρημα Ισομορφισμών Ομάδων έχουμε $|\mathrm{Im}\,\varphi| = |G/\ker\varphi| = \dfrac{|G|}{|\ker\varphi|}$ και άρα $|\mathrm{Im}\,\varphi| \mid 20$. Άρα $|\mathrm{Im}\,\varphi| \mid \mu\kappa\delta(26, 20)$, δηλαδή $|\mathrm{Im}\,\varphi| = 1, 2$.