IOAN PURDEA COSMIN PELEA

PROBLEME DE ALGEBRĂ

colecția
UNIVERSITAS
seria
MATEMATICĂ

EIKON

IOAN PURDEA **COSMIN PELEA**

PROBLEME DE ALGEBRĂ

Ediţia a II-a revăzută şi completată

2007

Cuprins

Prefaţă

Această culegere de probleme urmează structura cursului ,,*Algebră*" de Ioan Purdea şi Ioana Pop ([34]), apărut în 2003 la Editura GIL, Zalău, şi are la bază activitatea şi experienţa celor doi autori, a unuia de peste 45 de ani, iar a celuilalt de aproape 10 ani, în predarea algebrei la Facultatea de Matematică şi Informatică a Universităţii ,,Babeş-Bolyai" din Cluj Napoca, precum şi lecţiile ţinute de aceştia pentru profesorii de matematică din gimnaziu şi liceu la cursurile de perfecţionare în specialitate.

Lucrarea de faţă se adresează studenţilor de la secţiile de matematică, informatică, matematică şi informatică. matematică şi fizică, fizică, precum şi studenţilor din învăţământul tehnic şi economic. De asemenea, se adresează profesorilor de matematică pentru pregătirea examenului de definitivat în învăţământ, a examenului de gradul II şi a concursului de ocupare a catedrelor vacante. În bogatul material din această carte se găsesc probleme care pot fi abordate cu succes şi de către elevii de liceu.

Lucrarea are două părţi: prima cuprinde enunţurile problemelor şi, acolo unde este necesar, unele precizări de natură teoretică, iar partea a doua cuprinde soluţii, indicaţii şi răspunsuri. Cele peste 830 de probleme sunt distribuite în 7 capitole, aceleaşi capitole ca cele din cursul menţionat, şi este urmărită succesiunea paragrafelor din fiecare capitol al cursului. Pentru toate problemele cu grad mediu sau sporit de dificultate am prezentat în cea de a doua parte fie soluţia completă, fie am furnizat indicaţii amănunţite pentru rezolvarea lor.

Mulţumim colegilor Rodica Covaci, Septimiu Crivei şi Simion Breaz pentru ajutorul acordat la pregătirea manuscrisului pentru tipar.

Autorii

Partea I

ENUNŢURI

Capitolul 1

Relaţii. Funcţii

1.1. Fie A o mulţime cu m elemente şi B o mulţime cu n elemente. Să se determine numărul:
a) elementelor lui $A \times B$;
b) submulţimilor lui $A \times B$;
c) relaţiilor între elementele lui A şi B.

1.2. Fie mulţimile $A = \{1, 2\}$, $B = \{1, 2, 3\}$, $C = \{1, 2, 3, 4\}$ şi relaţiile binare (A, B, R_1), (B, C, R_2), (B, C, R_3) cu graficele $R_1 = \{(1, 3), (2, 3), (1, 2)\}$, $R_2 = \{(3, 1), (1, 4), (3, 4)\}$ şi $R_3 = \{(1, 2), (1, 4), (2, 2), (2, 3)\}$. Să se determine:
a) relaţia universală între elementele mulţimilor A şi B, complementara ei şi complementara relaţiei (A, B, R_1);
b) reuniunea si intersecţia relaţiilor (B, C, R_2) şi (B, C, R_3);
c) relaţiile $(A, C, R_2 \circ R_1)$ şi $(B, B, R_1 \circ R_2)$;
d) relaţiile $(B, A, \overset{-1}{R_1})$, $(C, B, \overset{-1}{R_2})$, $(C, A, \overset{-1}{\overline{R_2 \circ R_1}})$.

1.3. Fie $\leq$ relaţia de inegalitate în $\mathbb{R}$ şi $\geq$ inversa sa. Să se reprezinte într-un sistem de coordonate ortogonal graficul:
a) relaţiei $\leq$;
b) relaţiei $\geq$;
c) intersecţiei relaţiilor $\leq$ şi $\geq$;
d) reuniunii relaţiilor $\leq$ şi $\geq$;
e) complementarei relaţiei $\leq$.

1.4. Fie $<$ relaţia de inegalitate strictă în $\mathbb{N}$. Să se determine relaţiile $<^2$, $<^3$ şi produsele (compusele) $< \circ >$, $> \circ <$.

Dacă A şi B sunt mulţimi fixate atunci, adesea, o relaţie (binară) $\rho = (A, B, R)$ între elementele mulţimilor A şi B se identifică cu graficul său R.

1.5. Fie ρ graficul unei relaţii între numere reale. Să se indice transformarea geometrică ce ne conduce de la ρ la $\overset{-1}{\rho}$. Să se construiască $\overset{-1}{\rho_0}$ în cazul în care

$$\rho_0 = \{(x, y) \in \mathbb{R}^2 \mid y = \sqrt{3}\, x\}.$$

1.6. Fie $R_1, R_2 \subseteq A \times B$. Să se arate că

$$R_1 = R_2 \;\Leftrightarrow\; \overset{-1}{R_1} = \overset{-1}{R_2}.$$

1.7. Fie $\rho_{ij} \subseteq \mathbb{R}^n \times \mathbb{R}^n$ $(i, j = 1, \ldots, n)$ relaţiile definite astfel:

$$(a_1, \ldots, a_n)\rho_{ij}(b_1, \ldots, b_n) \;\Leftrightarrow\; a_1 + \cdots + a_i = b_1 + \cdots + b_j.$$

Să se determine relaţiile $\rho_i = \bigcap\limits_{j=1}^{n} \rho_{ij}$ $(i = 1, \ldots, n)$, $\rho = \bigcap\limits_{i=1}^{n} \rho_{ii}$ şi $\rho' = \bigcap\limits_{i,j=1}^{n} \rho_{ij}$.

1.8. Fie R, S, T şi R_k $(k \in \mathbb{N}^*)$ relaţiile definite în $\mathbb{N}$ astfel:

$$mRn \;\Leftrightarrow\; m|n \text{ (m divide pe n)};$$

$$mSn \;\Leftrightarrow\; m < n;$$

$$mR_kn \;\Leftrightarrow\; |m - n| = k.$$

Să se determine R^2, $S \circ R$, T^2, $R \circ R_k$, $R_k \circ R$, $R_k \circ S$, $S \circ R_k$, $R_k \circ R_1$.

1.9. Fie $C[a, b] = \{f : [a, b] \to \mathbb{R} \mid f \text{ este continuă}\}$ şi ρ_1, ρ_2, ρ_3 relaţiile definite pe $C[a, b]$ prin:

$$f\rho_1 g \;\Leftrightarrow\; \forall x \in [a, b],\; f(x) \leq g(x);$$

$$f\rho_2 g \;\Leftrightarrow\; f(a) = g(a),\; f(b) = g(b);$$

$$f\rho_3 g \;\Leftrightarrow\; \forall x \in [a, b],\; f(x) \neq g(x).$$

Să se determine ρ_1^2, ρ_2^2, ρ_3^2, $\rho_2 \circ \rho_1$, $\rho_3 \circ \rho_2$, $\rho_2 \circ \rho_3$.

1.10. Fie $A = \{1, 2, 3, 4\}$ şi fie pe A relaţiile $R = \{(1, 2), (1, 4), (2, 3), (4, 4), (4, 3)\}$, $S = \{(2, 4), (3, 4), (1, 1)\}$, $S' = \{(4, 4), (1, 4)\}$. Să se determine relaţiile $(S \cap S') \circ R$, $(S \circ R) \cap (S' \circ R)$, $R \circ (S \cap S')$, $(R \circ S) \cap (R \circ S')$.

1.11. Fie mulţimile $A = \{a_1, a_2, a_3, a_4\}$, $B = \{b_1, b_2, b_3, b_4, b_5\}$, $X = \{a_2, a_4\}$, $Y = \{b_1, b_2, b_4, b_5\}$ şi $R = \{(a_1, b_2), (a_3, b_5), (a_1, b_3), (a_2, b_4)\} \subseteq A \times B$. Să se determine $R(X)$, $R\langle a_2 \rangle$, $\overset{-1}{R}(Y)$, $\overset{-1}{R}\langle b_5 \rangle$, pr_1R, pr_2R.

1.12. Fie ρ relaţia binară definită în $\mathbb{N}$ astfel:

$$m\rho n \;\Leftrightarrow\; m \text{ divide pe } n.$$

Să se determine $\rho\langle 1 \rangle$, $\overset{-1}{\rho}(\{4, 9\})$, $pr_1\rho$, $pr_2\rho$.

1.13. Fie $\rho = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 \leq 1\}$. Să se determine $\rho\langle -1 \rangle$, $\rho\langle 0 \rangle$, $\rho\langle 1 \rangle$, $\rho\langle 2 \rangle$, $\rho([0, 1])$, $pr_1\rho$, $pr_2\rho$.

1.14. Fie $A, B \subseteq \mathbb{R}$, $X \subseteq A$, $Y \subseteq B$, $\rho \subseteq A \times B$. Să se dea interpretarea geometrică pentru fiecare dintre mulţimile $\rho(X)$, $\overset{-1}{\rho}(Y)$, $pr_1\rho$, $pr_2\rho$. Să se analizeze cazurile particulare $X = \{x\}$, $Y = \{y\}$.

1.15. Fie A, B două mulţimi, $R \subseteq A \times B$ şi $X \subseteq A$. Să se arate că

$$R(X) = \bigcup_{x \in X} R\langle x \rangle.$$

1.16. Fie A, B mulţimi, $R_1, R_2 \subseteq A \times B$. Să se arate că

$$R_1 = R_2 \Leftrightarrow \forall x \in A,\ R_1\langle x\rangle = R_2\langle x\rangle \Leftrightarrow \forall y \in B,\ \overset{-1}{R_1}\langle y\rangle = \overset{-1}{R_2}\langle y\rangle.$$

1.17. Fie A, B mulţimi, $R \subseteq A \times B$, $a \in A$ şi $X \subseteq A$. Să se arate că:
a) $R\langle a\rangle \neq \emptyset \ \Leftrightarrow\ a \in pr_1 R$;
b) $R(X) = R(X \cap pr_1 R)$;
c) $R(X) = \emptyset \ \Leftrightarrow\ X \cap pr_1 R = \emptyset$.

1.18. Fie $\rho = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 1\}$, $X = \left[-2, \frac{1}{2}\right]$ şi $Y = \left[-\frac{1}{2}, 1\right]$. Să se determine $\rho(X \cap Y)$ şi $\rho(X) \cap \rho(Y)$.

1.19. Fie $\rho = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 1\}$, $\rho' = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x > 2\}$ şi $X = [0, 3]$. Să se determine $(\rho \cap \rho')(X)$ şi $\rho(X) \cap \rho'(X)$.

1.20. Fie $X = \{z \in \mathbb{C} \mid |z| = 1\}$ şi ρ_1, ρ_2, ρ_3 relaţiile binare definite în $\mathbb{C}$ astfel:

$$z_1 \rho_1 z_2 \ \Leftrightarrow\ |z_1| = |z_2|;$$

$$z_1 \rho_2 z_2 \ \Leftrightarrow\ \arg z_1 = \arg z_2 \text{ sau } z_1 = 0 = z_2;$$

$$z_1 \rho_3 z_2 \ \Leftrightarrow\ \overline{z_1} = z_2,$$

(unde $\arg z_i$ şi $\overline{z_i}$ sunt argumentul redus, respectiv, conjugatul numărului complex z_i $(i = 1, 2)$). Să se determine $\rho_k(\mathbb{R})$, $\rho_k(X)$ şi $\rho_k\langle i\rangle$ $(k = 1, 2, 3)$.

1.21. Fie A, B două mulţimi, $X, X' \subseteq A$ şi $Y \subseteq B$. Să se arate că:
a) $\overset{-1}{\overline{X \times Y}} = Y \times X$;
b) $Y \neq \emptyset \ \Rightarrow\ pr_1(X \times Y) = X$;
c) $X \neq \emptyset \ \Rightarrow\ pr_2(X \times Y) = Y$;
d) $x \in X \ \Rightarrow\ (X \times Y)\langle x\rangle = Y$;
e) $x \notin X \ \Rightarrow\ (X \times Y)\langle x\rangle = \emptyset$;
f) $X \cap X' \neq \emptyset \ \Rightarrow\ (X \times Y)(X') = Y$;
g) $X \cap X' = \emptyset \ \Rightarrow\ (X \times Y)(X') = \emptyset$.

1.22. Fie A, B, C trei mulţimi, $R \subseteq A \times B$, $S \subseteq B \times C$, $X \subseteq A$, $Y, Y' \subseteq B$ şi $Z \subseteq C$. Să se arate că:
a) $S \circ (X \times Y) = X \times S(Y)$;
b) $(Y \times Z) \circ R = \overset{-1}{R}(Y) \times Z$;
c) $Y \cap Y' \neq \emptyset \ \Rightarrow\ (Y' \times Z) \circ (X \times Y) = X \times Z$;
d) $Y \cap Y' = \emptyset \ \Rightarrow\ (Y' \times Z) \circ (X \times Y) = \emptyset$.

1.23. Fie A o mulţime. Să se determine o relaţie omogenă ρ pe A astfel încât să fie îndeplinită condiţia:
a) $\rho \circ (A \times A) = A \times A$;
b) $(A \times A) \circ \rho = A \times A$;
c) $\rho \circ (A \times A) \circ \rho = A \times A$;
d) $(A \times A) \circ \rho \circ (A \times A) = A \times A$;
e) $\overset{-1}{\rho} \circ \rho = A \times A$.

1.24. Fie A, B, C trei mulţimi, $R \subseteq A \times B$ şi $S \subseteq B \times C$. Să se arate că:
a) $S \circ R = \{(a, c) \in A \times C \mid R\langle a\rangle \cap \overset{-1}{S}\langle c\rangle \neq \emptyset\}$;
b) $S \circ R = \bigcup\limits_{b \in B} \overset{-1}{R}\langle b\rangle \times S\langle b\rangle$.

1.25. Fie A, B, C mulţimi, $R \subseteq A \times B$ şi $S \subseteq B \times C$. Să se arate că:
a) $pr_1(S \circ R) = \overset{-1}{R}(pr_1 S) \subseteq pr_1 R$;
b) $pr_2(S \circ R) = S(pr_2 R) \subseteq pr_2 S$;
c) $S \circ R = \emptyset \ \Leftrightarrow\ pr_2 R \cap pr_1 S = \emptyset$;
d) $S \circ R \subseteq pr_1 R \times pr_2 S$.

1.26. Fie A, B mulţimi şi $R \subseteq A \times B$. Să se arate că următoarele condiţii sunt echivalente:
a) pentru orice $x \in A$, $R\langle x\rangle \neq \emptyset$;
b) $\Delta_A \subseteq \overset{-1}{R} \circ R$;
c) $pr_1 R = A$;
d) dacă A' este o mulţime şi $P_1, P_2 \subseteq A' \times A$ atunci

$$(R \circ P_1) \cap (R \circ P_2) = \emptyset \ \Leftrightarrow\ P_1 \cap P_2 = \emptyset;$$

e) dacă A' este o mulţime şi $P \subseteq A' \times A$ atunci

$$R \circ P = \emptyset \ \Leftrightarrow\ P = \emptyset;$$

f) dacă $X_1, X_2 \subseteq A$ atunci

$$R(X_1) \cap R(X_2) = \emptyset \ \Leftrightarrow\ X_1 \cap X_2 = \emptyset;$$

g) dacă $X \subseteq A$ atunci

$$R(X) = \emptyset \ \Leftrightarrow\ X = \emptyset;$$

h) dacă $Y_1, Y_2 \subseteq B$ atunci

$$Y_1 \cup Y_2 = B \ \Leftrightarrow\ \overset{-1}{R}(Y_1) \cup \overset{-1}{R}(Y_2) = A;$$

i) dacă $Y \subseteq B$ atunci

$$\overset{-1}{R}(Y) \cup \overset{-1}{R}(C_B(Y)) = A.$$

1.27. Fie A, B mulţimi şi $R \subseteq A \times B$. Să se arate că următoarele condiţii sunt echivalente:
a) pentru orice $x \in A$, $R\langle x\rangle$ conţine cel mult un element;
b) $R \circ \overset{-1}{R} \subseteq \Delta_B$;
c) dacă B' este o mulţime şi $S_1, S_2 \subseteq B \times B'$ atunci

$$(S_1 \cap S_2) \circ R = (S_1 \circ R) \cap (S_2 \circ R);$$

d) dacă B' este o mulţime şi $S_1, S_2 \subseteq B \times B'$ atunci

$$S_1 \cap S_2 = \emptyset \ \Rightarrow\ (S_1 \circ R) \cap (S_2 \circ R) = \emptyset;$$

e) dacă B' este o mulţime şi $S \subseteq B \times B'$ atunci

$$(S \circ R) \cap (C_{B\times B'}(S) \circ R) = \emptyset;$$

f) dacă $Y_1, Y_2 \subseteq B$ atunci

$$Y_1 \cap Y_2 = \emptyset \;\Rightarrow\; \overset{-1}{R}(Y_1) \cap \overset{-1}{R}(Y_2) = \emptyset;$$

g) dacă $Y \subseteq B$ atunci

$$\overset{-1}{R}(Y) \cap \overset{-1}{R}(C_B(Y)) = \emptyset;$$

h) dacă $Y \subseteq B$ atunci

$$\overset{-1}{R}(Y) \cap C_A(\overset{-1}{R}(Y)) = \overset{-1}{R}(C_B(Y)).$$

1.28. Fie A, B mulţimi, $R \subseteq A \times B$ şi $X, X' \subseteq A$. Să se arate că dacă pentru orice $y \in B$ secţiunea $\overset{-1}{R}\langle y\rangle$ are cel mult un element atunci

$$R(C_A(X)) = pr_2R \setminus R(X) \;\text{ şi }\; R(X \cap X') = R(X) \cap R(X').$$

1.29. Fie A, B, C mulţimi, $R_1, R_2 \subseteq A \times B$ şi $S \subseteq B \times C$. Să se arate că dacă pentru orice $z \in C$ secţiunea $\overset{-1}{S}\langle z\rangle$ are cel mult un element atunci

$$S \circ (R_1 \cap R_2) = (S \circ R_1) \cap (S \circ R_2).$$

1.30. Fie $R \subseteq B \times C$. Să se arate că următoarele afirmaţii sunt echivalente:
a) $X_1, X_2 \subseteq B,\ X_1 \neq X_2 \;\Rightarrow\; R(X_1) \neq R(X_2)$;
b) pentru orice mulţime A şi orice relaţii binare $R_1,\ R_2 \subseteq A \times B$ avem

$$R \circ R_1 = R \circ R_2 \;\Rightarrow\; R_1 = R_2.$$

1.31. Fie $R \subseteq A \times B$. Să se arate că următoarele afirmaţii sunt echivalente:
a) $Y_1, Y_2 \subseteq B,\ Y_1 \neq Y_2 \;\Rightarrow\; \overset{-1}{R}(Y_1) \neq \overset{-1}{R}(Y_2)$;
b) pentru orice mulţime C şi orice relaţii binare $R_1, R_2 \subseteq B \times C$ avem

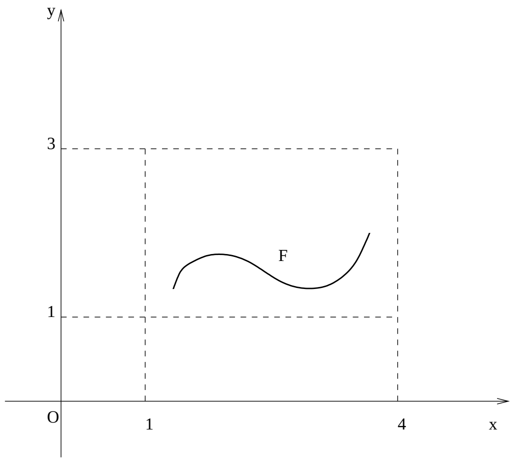
$$R_1 \circ R = R_2 \circ R \;\Rightarrow\; R_1 = R_2.$$

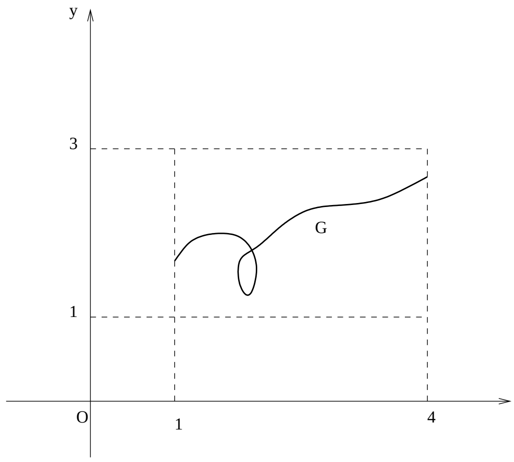
1.32. Să se arate că dacă $f = (A, B, F)$ este o funcţie atunci $pr_1F = A$.

1.33. Să se precizeze dacă sunt sau nu egale funcţiile:
a) $f : \mathbb{R} \to \mathbb{R},\ f(x) = x^2$ şi $g : \mathbb{R} \to (0, \infty),\ g(x) = x^2$;
b) $f : \mathbb{R} \to \mathbb{R},\ f(x) = x^2$ şi $g : (-\infty, 0] \to \mathbb{R},\ g(x) = x^2$;
c) $f : \mathbb{R} \to \mathbb{R},\ f(x) = x^2$ şi $g : \mathbb{R} \to \mathbb{R},\ g(t) = t^2$.

1.34. Fie $f : \mathbb{R} \to \mathbb{R},\ f(x) = x^2$ şi $X_1 = (-1, 0],\ X_2 = [0, 1]$. Să se determine $f(X_1 \cap X_2)$ şi $f(X_1) \cap f(X_2)$.

1.35. a) Fie $A, B \subseteq \mathbb{R}$ şi F o mulţime de puncte din plan. Ce condiţii trebuie să îndeplinească F pentru a fi graficul unei funcţii cu domeniul A şi codomeniul B?
b) Fie $A = [1, 4],\ B = [1, 3]$. Sunt mulţimile F şi G indicate în figurile următoare graficele unor funcţii cu domeniul A şi codomeniul B?





1.36. Fie $F, G \subseteq A \times B$ graficul unor funcţii definite pe A cu valori în B. Sunt $F \cup G$, $F \cap G$, $C_{A\times B}(F)$ grafice de funcţii definite pe A cu valori în B? Dar $\overset{-1}{F}$ este graficul unei funcţii cu domeniul B şi codomeniul A?

1.37. Fie F şi G cu semnificaţia din problema precedentă. Să se dea condiţii necesare şi suficiente pentru ca $F \cup G$ ($F \cap G$, respectiv $C_{A\times B}(F)$) să fie grafice de funcţii cu domeniul A şi codomeniul B, iar $\overset{-1}{F}$ să fie graficul unei funcţii cu domeniul B şi codomeniul A.

1.38. Fie $f : A \to B$ o funcţie şi F graficul său. Să se arate că următoarele afirmaţii sunt echivalente:
a) f este injectivă;
b) pentru orice $y \in B$, $\overset{-1}{F}\langle y\rangle$ conţine cel mult un element;
c) pentru orice $y \in B$, ecuaţia $f(x) = y$ (cu necunoscuta x) are cel mult o soluţie în mulţimea A.

1.39. Fie $A, B \subseteq \mathbb{R}$, $f : A \to B$ o funcţie şi F graficul său.
a) Să se arate că f este injectivă dacă şi numai dacă orice paralelă la Ox, dusă printr-un punct din B, conţine cel mult un punct din F.
b) Să se arate că dacă f este strict monotonă atunci f este injectivă. Este adevărată reciproca acestei afirmaţii?

1.40. Fie $f : A \to B$ o funcţie şi F graficul său. Să se arate că următoarele afirmaţii sunt echivalente:
a) f este surjectivă;
b) $pr_2 F = B$;
c) pentru orice $y \in B$, $\overset{-1}{F}\langle y\rangle$ conţine cel puţin un element, adică $\overset{-1}{F}\langle y\rangle \neq \emptyset$;
d) pentru orice $y \in B$, ecuaţia $f(x) = y$ (cu necunoscuta x) are cel puţin o soluţie în A.

1.41. Fie $A, B \subseteq \mathbb{R}$, $f : A \to B$ o funcţie şi F graficul său. Să se arate că f este surjectivă dacă şi numai dacă orice paralelă la Ox, dusă printr-un punct din B, conţine cel puţin un punct din F.

1.42. Să se dea câte un exemplu de funcţie care are:
a) exact două retracte (diferite) ;
b) o infinitate de retracte (diferite).

1.43. Să se dea câte un exemplu de funcţie care are :
a) exact două secţiuni (diferite) ;
b) o infinitate de secţiuni (diferite).

1.44. Să se dea un exemplu de funcţie injectivă a cărei inversă (considerată ca şi relaţie) nu este o funcţie.

1.45. Să se dea un exemplu de funcţie surjectivă a cărei inversă (considerată ca şi relaţie) nu este o funcţie.

1.46. Fie A şi B mulţimi finite cu m, respectiv n elemente. Cum trebuie să fie m şi n pentru ca să existe cel puţin
a) o funcţie injectivă $f : A \to B$;
b) o funcţie surjectivă $f : A \to B$;
c) o funcţie bijectivă $f : A \to B$?

1.47. Fie A o mulţime finită şi $f : A \to A$. Să se arate că următoarele afirmaţii sunt echivalente:
a) f este injectivă ;
b) f este surjectivă ;
c) f este bijectivă.

1.48. Fie $n \in \mathbb{N}$, $n \geq 2$ şi $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^n$. Este f bijectivă? În caz afirmativ să se determine f^{-1}.

1.49. Pentru o funcţie $f : A \to B$ se consideră funcţiile

$$f_* : \mathcal{P}(A) \to \mathcal{P}(B),\ f_*(X) = f(X) \text{ şi } f^* : \mathcal{P}(B) \to \mathcal{P}(A),\ f^*(Y) = \overset{-1}{f}(Y)$$

(unde $\mathcal{P}(A)$ este mulţimea submulţimilor lui A). Să se arate că sunt echivalente afirmaţiile:
a) f este injectivă;
b) f_* este injectivă;
c) $f^* \circ f_* = 1_{\mathcal{P}(A)}$;
d) f^* este surjectivă;
e) $f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$, pentru orice $X_1, X_2 \subseteq A$;
f) $f(C(X)) \subseteq C(f(X))$, pentru orice $X \subseteq A$.

1.50. Cu notaţiile din problema anterioară, să se arate că următoarele afirmaţii sunt echivalente:
a) f este surjectivă;
b) f_* este surjectivă;
c) $f_* \circ f^* = 1_{\mathcal{P}(B)}$;
d) f^* este injectivă;
e) $C(f(X)) \subseteq f(C(X))$, pentru orice $X \subseteq A$.

1.51. Fie $f : A \to \mathbb{N}$. Cu ajutorul lui f, definim funcţia $\overline{f}$ de la mulţimea submulţimilor finite X ale mulţimii A la $\mathbb{N}$ astfel:

$$\overline{f}(X) = \begin{cases} \sum\limits_{x \in X} f(x) & , \text{ dacă } X \neq \emptyset \\ 0 & , \text{ dacă } X = \emptyset. \end{cases}$$

a) Să se arate că dacă X_i $(i = 1, \dots, n)$ sunt mulţimi finite atunci

$$\overline{f}\left(\bigcup_{i=1}^{n} X_i\right) = \sum_{i=1}^{n} \overline{f}(X_i) - \sum_{1 \leq i < j \leq n} \overline{f}(X_i \cap X_j) + \sum_{1 \leq i < j < k \leq n} \overline{f}(X_i \cap X_j \cap X_k) - \cdots + (-1)^{n+1} \overline{f}\left(\bigcap_{i=1}^{n} X_i\right).$$

b) Notăm cu $|X|$ numărul de elemente ale unei mulţimi finite X. Să se arate, folosind pe a), că dacă X_i $(i = 1, \dots, n)$ sunt mulţimi finite atunci

$$\left|\bigcup_{i=1}^{n} X_i\right| = \sum_{i=1}^{n} |X_i| - \sum_{1 \leq i < j \leq n} |X_i \cap X_j| + \sum_{1 \leq i < j < k \leq n} |X_i \cap X_j \cap X_k| - \cdots + (-1)^{n+1} \left|\bigcap_{i=1}^{n} X_i\right|.$$

1.52. Fie A şi B două mulţimi finite cu m, respectiv n elemente. Să se determine numărul :
a) funcţiilor care au domeniul A şi codomeniul B;
b) funcţiilor injective care au domeniul A şi codomeniul B;
c) funcţiilor bijective care au domeniul A şi codomeniul B;
d) funcţiilor surjective care au domeniul A şi codomeniul B.

1.53. Fie n un întreg pozitiv. Există o funcţie $f : \mathbb{R} \to \mathbb{R}$ care verifică una dintre condiţiile:
a) $f(x^n) = x$ pentru orice $x \in \mathbb{R}$?
b) $[f(x)]^n = x$ pentru orice $x \in \mathbb{R}$?

1.54. Fie $g : \mathbb{R} \to \mathbb{R}$ o funcţie pară sau periodică. Există o funcţie $f : \mathbb{R} \to \mathbb{R}$ astfel ca $f(g(x)) = x$ pentru orice $x \in \mathbb{R}$?

1.55. Să se arate că o funcţie $f : A \to B$ are o secţiune (inversă la dreapta) unică dacă şi numai dacă f este bijectivă.

1.56. a) Să se dea un exemplu de funcţie injectivă care nu are nici o retractă (inversă la stânga).
b) Să se dea un exemplu de funcţie injectivă care deşi are o retractă unică, totuşi nu este bijectivă.
c) Fie $f : A \to B$ şi $|A| > 1$. Să se arate că f are o retractă unică dacă şi numai dacă f este bijectivă.

1.57. Să se arate că pentru orice funcţie $f : A \to B$ cu $A \neq \emptyset$ există o funcţie $g : B \to A$ astfel încât $f \circ g \circ f = f$. Esta g unică?

1.58. Fie A şi B două mulţimi. Să se arate că există o bijecţie între mulţimea relaţiilor cu domeniul A şi codomeniul B şi mulţimea funcţiilor cu domeniul A şi codomeniul $\mathcal{P}(B)$.

1.59. Fie A şi B două mulţimi. Să se arate că există o funcţie bijectivă între mulţimea $\mathcal{R}$ a relaţiilor binare cu domeniul A şi codomeniul B şi mulţimea $\mathcal{F}$ a funcţiilor $F : \mathcal{P}(A) \to \mathcal{P}(B)$ care au proprietatea că pentru orice familie $(X_i)_{i\in I}$ de submulţimi ale mulţimii A, $F\left(\bigcup_{i\in I} X_i\right) = \bigcup_{i\in I} F(X_i)$.

1.60. Fie $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \cos x$ şi $g : \mathbb{R} \to \mathbb{R}_+ = [0, +\infty)$, $g(x) = x^2$. Să se determine o funcţie $h : \mathbb{R}_+ \to \mathbb{R}$ astfel încât $f = h \circ g$. Este funcţia h unică?

1.61. Fie $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \sin x$ şi $g : \mathbb{R} \to \mathbb{R}_+$, $g(x) = x^2$. Există o funcţie $h : \mathbb{R}_+ \to \mathbb{R}$ astfel încât $f = h \circ g$?

1.62. Fie $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \cos x$, $A = [-2, +\infty)$ şi $g : A \to \mathbb{R}$, $g(x) = 2x + 1$. Să se determine o funcţie $h : \mathbb{R} \to A$ astfel încât $f = g \circ h$. Este funcţia h unică?

1.63. Fie $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \sin x$, $A = [0, +\infty)$ şi $g : A \to \mathbb{R}$, $g(x) = 2x+1$. Există o funcţie $h : \mathbb{R} \to A$ astfel încât $f = g \circ h$?

1.64. Să se arate că pentru orice două mulţimi A şi B există o funcţie bijectivă $\varphi_{A,B} : A \times B \to B \times A$ cu proprietatea că oricare ar fi funcţiile $f : A \to A'$ şi $g : B \to B'$ următoarea diagramă este comutativă

$$\begin{tikzcd} A \times B \arrow[r, "\varphi_{A,B}"] \arrow[d, "f\times g"'] & B \times A \arrow[d, "g\times f"] \\ A' \times B' \arrow[r, "\varphi_{A',B'}"] & B' \times A' \end{tikzcd} .$$

1.65. Să se arate că pentru orice mulţimi A, B şi C există o funcţie bijectivă $\varphi_{A,B,C} : (A \times B) \times C \to A \times (B \times C)$ cu proprietate că oricare ar fi funcţiile $f : A \to A'$, $g : B \to B'$ şi $h : C \to C'$ următoarea diagramă este comutativă

$$\begin{tikzcd} (A \times B) \times C \arrow[r, "\varphi_{A,B,C}"] \arrow[d, "(f\times g)\times h"'] & A \times (B \times C) \arrow[d, "f\times(g\times h)"] \\ (A' \times B') \times C' \arrow[r, "\varphi_{A',B',C'}"] & A' \times (B' \times C') \end{tikzcd} .$$

1.66. Fie $f : A \to B,\ g : A' \to B',\ X \subseteq A,\ X' \subseteq A',\ Y \subseteq B,\ Y' \subseteq B'$. Să se arate că:

$$(f \times g)(X \times X') = f(X) \times g(X') \text{ şi } \overset{-1}{\overline{f \times g}}(Y \times Y') = \overset{-1}{f}(Y) \times \overset{-1}{g}(Y').$$

Să se generalizeze aceste rezultate, luând în locul perechilor $(f, g), (X, X')$ şi (Y, Y') familii indexate cu aceeaşi mulţime de indici.

1.67. Fie $f : A \to B$, $g : A \to B'$, $Y \subseteq B$, $Y' \subseteq B'$. Se consideră funcţia $h : A \to B \times B'$, $h(x) = (f(x), g(x))$. Să se arate că

$$\overset{-1}{h}(Y \times Y') = \overset{-1}{f}(Y) \cap \overset{-1}{g}(Y').$$

Să se generalizeze acest rezultat, luând în locul perechilor (f, g) şi (Y, Y') familii indexate cu aceeaşi mulţime de indici.

1.68. Fie $f : A \to B$ şi $g : A' \to B'$ cu $A \neq \emptyset \neq A'$. Să se arate că:
a) $f \times g$ este injectivă dacă şi numai dacă f şi g sunt injective;
b) $f \times g$ este surjectivă dacă şi numai dacă f şi g sunt surjective.

1.69. Să se arate că există funcţii $F : A \times B \to A' \times B'$ care nu sunt de forma $F = f \times g$, unde $f : A \to A'$ şi $g : B \to B'$.

1.70. Fie A_1 şi A_2 două mulţimi. Reuniunea a două mulţimi disjuncte de acelaşi cardinal cu A_1 şi A_2 se numeşte *reuniune disjunctă* a lui A_1 cu A_2. De exemplu

$$A_1 \mathring{\cup} A_2 = (\{1\} \times A_1) \cup (\{2\} \times A_2)$$

este o reuniune disjunctă a lui A_1 cu A_2. Funcţiile

$$q_1 : A_1 \to A_1 \mathring{\cup} A_2,\ q_1(a_1) = (1, a_1) \text{ şi } q_2 : A_2 \to A_1 \mathring{\cup} A_2,\ q_2(a_2) = (2, a_2)$$

se numesc *injecţiile canonice*. Să se arate că:
a) $A_1 \mathring{\cup} A_2$ împreună cu injecţiile sale canonice are următoarea proprietate de universalitate: pentru orice mulţime B şi orice funcţii $u_1 : A_1 \to B$, $u_2 : A_2 \to B$ există o singură funcţie $u : A_1 \mathring{\cup} A_2 \to B$ astfel încât diagrama

$$\begin{tikzcd}
 & B & \\
A_1 \arrow[ur, "u_1"] \arrow[r, "q_1"] & A_1 \mathring{\cup} A_2 \arrow[u, dotted, "u"'] & A_2 \arrow[ul, "u_2"'] \arrow[l, "q_2"']
\end{tikzcd}$$

să fie comutativă, adică $u \circ q_1 = u_1$ şi $u \circ q_2 = u_2$.
b) Pentru orice mulţime B şi orice funcţii $u', u'' : A_1 \mathring{\cup} A_2 \to B$ avem

$$u' \circ q_1 = u'' \circ q_1 \text{ şi } u' \circ q_2 = u'' \circ q_2 \ \Rightarrow\ u' = u''.$$

c) Proprietatea de universalitate a reuniunii disjuncte determină reuniunea disjunctă până la o bijecţie.

1.71. Fie mulţimile $A = \{1, 2\}$, $B = \{1, 2, 3\}$ şi fie $f : A \to B$, $g : B \to A$ funcţiile definite prin

x	1	2
$f(x)$	2	3

x	1	2	3
$g(x)$	1	1	2

Să se determine funcţia $f^g : A^A \to B^B$.

1.72. Să se arate că funcţia $f : A_1 \to A_2$ este injectivă dacă şi numai dacă pentru orice mulţime B funcţia $f^{1_B} : A_1^B \to A_2^B$ este injectivă.

1.73. Să se arate că funcţia $g : B_2 \to B_1$ este surjectivă dacă şi numai dacă pentru orice mulţime A funcţia $1_A^g : A^{B_1} \to A^{B_2}$ este injectivă.

1.74. Fie $f : A_1 \to A_2$ şi $g : B_2 \to B_1$ două funcţii. Să se arate că:
a) dacă f este injectivă şi g este surjectivă atunci f^g este injectivă ;
b) dacă f este surjectivă şi g este injectivă, iar $B_2 \neq \emptyset$ atunci f^g este surjectivă.

1.75. Să se arate că pentru orice mulţimi A_1, A_2, B funcţia

$$\varphi : (A_1 \times A_2)^B \to A_1^B \times A_2^B,\ \varphi(u) = (p_1 \circ u, p_2 \circ u)$$

(unde p_1, p_2 sunt proiecţiile canonice ale produsului) este bijectivă, iar dacă

$$f_1 : A_1 \to A_1',\ f_2 : A_2 \to A_2' \text{ şi } g : B' \to B$$

sunt funcţii atunci diagrama

$$\begin{tikzcd}
(A_1 \times A_2)^B \arrow[r, "\varphi"] \arrow[d, "(f_1\times f_2)^g"'] & A_1^B \times A_2^B \arrow[d, "f_1^g\times f_2^g"] \\
(A_1' \times A_2')^{B'} \arrow[r, "\varphi'"] & {A_1'}^{B'} \times {A_2'}^{B'}
\end{tikzcd}$$

(unde φ' se defineşte analog cu φ) este comutativă.

1.76. Fie A, B_1, B_2 trei mulţimi. Dacă $f : B_1 \times B_2 \to A$ şi $y \in B_2$ atunci fie $f_y : B_1 \to A$ funcţia definită prin $f_y(x) = f(x, y)$, iar $F : B_2 \to A^{B_1}$ funcţia definită prin $F(y) = f_y$. Să se arate că funcţia

$$\varphi : A^{B_1 \times B_2} \to (A^{B_1})^{B_2},\ \varphi(f) = F$$

este bijectivă, iar dacă $h : A \to A'$, $g_1 : B_1' \to B_1$, $g_2 : B_2' \to B_2$ sunt funcţii atunci diagrama

$$\begin{tikzcd}
A^{B_1\times B_2} \arrow[r, "\varphi"] \arrow[d, "h^{g_1\times g_2}"'] & (A^{B_1})^{B_2} \arrow[d, "(h^{g_1})^{g_2}"] \\
{A'}^{B_1'\times B_2'} \arrow[r, "\varphi'"] & ({A'}^{B_1'})^{B_2'}
\end{tikzcd}$$

(unde φ' se defineşte analog cu φ) este comutativă.

1.77. Fie $R \subseteq A \times A$. Să se arate că :
a) R este reflexivă dacă şi numai dacă pentru orice $x \in A$, $x \in R\langle x\rangle$;
b) dacă R este simetrică atunci $pr_1R = pr_2R$;
c) dacă R este simetrică şi tranzitivă atunci pentru $x \in pr_1R$ avem xRx;
d) R este o relaţie de echivalenţă dacă şi numai dacă R este simetrică, tranzitivă şi $pr_1R = A$.

1.78. Să se găsească greşeala în următoarea ,,demonstraţie" a afirmaţiei: *o relaţie simetrică şi tranzitivă este o relaţie reflexivă (adică este o relaţie de echivalenţă)*: ,,Dacă $R \subseteq A \times A$ este simetrică atunci xRy implică yRx, iar din xRy şi yRx (întrucât R este tranzitivă) urmează xRx".

1.79. Să se arate că axiomele care definesc noţiunea de relaţie de echivalenţă sunt independente, adică nici una dintre ele nu este o consecinţă a celorlalte două.

1.80. Să se arate că dacă relaţiile $R, S \subseteq A \times A$ sunt reflexive atunci $R \circ S$ şi $S \circ R$ sunt reflexive.

1.81. Fie $R, S \subseteq A \times A$ două relaţii simetrice. Să se arate că $R \circ S$ este simetrică dacă şi numai dacă $R \circ S = S \circ R$.

1.82. Fie $R, S \subseteq A \times A$ două relaţii binare omogene tranzitive. Să se arate că dacă $R \circ S = S \circ R$ atunci $R \circ S$ este tranzitivă.

1.83. O *relaţie* $R \subseteq A \times A$ se numeşte *circulară* dacă

$$xRy \text{ şi } yRz \ \Rightarrow\ zRx.$$

Să se arate că R este o relaţie de echivalenţă dacă şi numai dacă R este reflexivă şi circulară.

1.84. Fie $R \subseteq A \times A$, $A' \subseteq A$ şi R' restricţia lui R la A', adică $R' = R \cap (A' \times A')$. Să se arate că dacă R este o relaţie de echivalenţă atunci $R' \subseteq A' \times A'$ este o relaţie de echivalenţă.

1.85. Fie $A = \{1, 2, 3, 4\}$, $\rho_1 = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 1), (2, 3), (1, 3), (3, 2), (3, 1)\}$, $\rho_2 = \{(1, 1), (2, 2), (3, 3), (4, 4), (2, 4)\}$, $\pi_1 = \{\{1, 2\}, \{3\}, \{4\}\}$ şi $\pi_2 = \{\{1, 2\}, \{1, 3, 4\}\}$.
a) Sunt ρ_1 şi ρ_2 relaţii de echivalenţă pe A? În caz afirmativ, să se determine mulţimea cât corespunzătoare.
b) Sunt π_1 şi π_2 partiţii ale lui A? În caz afirmativ, să se determine relaţia de echivalenţă corespunzătoare.

1.86. Să se determine partiţiile şi relaţiile de echivalenţă ale mulţimii $A = \{1, 2, 3\}$.

1.87. Fie A o mulţime. Să se arate că diagonala Δ_A (relaţia de egalitate pe A) şi relaţia universală $A \times A$ sunt relaţii de echivalenţă pe A şi să se determine mulţimile cât corespunzătoare.

1.88. Fie ρ_1, ρ_2 relaţiile definite pe $\mathbb{C}$ astfel:

$$z_1 \rho_1 z_2 \ \Leftrightarrow\ |z_1| = |z_2|;$$
$$z_1 \rho_2 z_2 \ \Leftrightarrow\ arg\, z_1 = arg\, z_2 \text{ sau } z_1 = 0 = z_2.$$

Să se arate că ρ_1 şi ρ_2 sunt relaţii de echivalenţă şi să se determine mulţimile cât $\mathbb{C}/\rho_i$ $(i = 1, 2)$. Să se reprezinte geometric clasele de echivalenţă determinate de relaţiile ρ_i.

1.89. Fie ρ_1, ρ_2 relaţiile definite pe $\mathbb{C}$ prin

$$z\rho_1 t \ \Leftrightarrow\ z \text{ şi } t \text{ au aceeaşi parte reală;}$$
$$z\rho_2 t \ \Leftrightarrow\ z \text{ şi } t \text{ au aceeaşi parte imaginară.}$$

Să se arate că ρ_1 şi ρ_2 sunt relaţii de echivalenţă şi să se determine mulţimile cât $\mathbb{C}/\rho_i$ $(i = 1, 2)$. Să se reprezinte geometric clasele de echivalenţă.

1.90. Fie ρ_1, ρ_2 relaţiile definite pe $\mathbb{R}$ prin

$$\begin{aligned} x\rho_1 y &\Leftrightarrow [x] = [y] \text{ (x şi y au aceeaşi parte întreagă);} \\ x\rho_2 y &\Leftrightarrow \{x\} = \{y\} \text{ (x şi y au aceeaşi parte fracţionară).} \end{aligned}$$

Să se arate că ρ_1 şi ρ_2 sunt relaţii de echivalenţă şi că există o bijecţie între $\mathbb{R}/\rho_1$ şi $\mathbb{Z}$, precum şi între $\mathbb{R}/\rho_2$ şi $[0, 1)$.

1.91. Fie $n \in \mathbb{N}^*$ şi $M_n(\mathbb{R})$ mulţimea matricelor pătrate de ordinul n cu elemente din $\mathbb{R}$. Să se arate că relaţia definită în $M_n(\mathbb{R})$ prin

$$A\rho B \Leftrightarrow \det A = \det B$$

este o relaţie de echivalenţă şi că există o bijecţie între $M_n(\mathbb{R})/\rho$ şi $\mathbb{R}$.

1.92. Fie $A \neq \emptyset$ şi $R \subseteq A \times A$. Să se arate că R este o relaţie de echivalenţă pe A dacă şi numai dacă $pr_1 R = A$ şi există o familie $(A_i)_{i\in I}$ de submulţimi nevide disjuncte ale mulţimii A astfel încât

$$R = \bigcup_{i\in I} A_i \times A_i.$$

1.93. În raport cu care dintre operaţiile de: reuniune, intersecţie, inversare şi complementare este închisă mulţimea $E(A)$ a relaţiilor de echivalenţă pe o mulţime A?

1.94. Fie $R_i \subseteq A_i \times A_i$ $(i = 1, 2)$ relaţii de echivalenţă. Să se arate că relaţia $R \subseteq A_1 \times A_2$, definită prin

$$(a_1, a_2)R(a_1', a_2') \Leftrightarrow a_1 R_1 a_1' \text{ şi } a_2 R_2 a_2'$$

este o relaţie de echivalenţă şi că există o bijecţie între mulţimile $(A_1 \times A_2)/R$ şi $(A_1/R_1) \times (A_2/R_2)$.

1.95. Fie $f, g : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, $g(x) = x^4$. Să se arate că $\ker f = \ker g$ şi să se stabilească o bijecţie între $\mathbb{R}/\ker f$ şi $\mathbb{R}_+ = [0, +\infty)$.

1.96. Fie $f, g : \mathbb{C} \to \mathbb{C}$, $f(z) = z^2$, $g(z) = z^4$. Să se arate că $\ker f \neq \ker g$ şi că există bijecţii între mulţimile $\mathbb{C}/\ker f$, $\mathbb{C}/\ker g$ şi $\mathbb{C}$.

1.97. Fie A o mulţime finită cu m elemente $(m \in \mathbb{N}^*)$ şi $E(A)$ mulţimea relaţiilor de echivalenţă între elementele mulţimii A. Să se determine numărul elementelor mulţimii $E(A)$.

1.98. O *relaţie* $R \subseteq A \times B$ se numeşte *difuncţională* dacă $R \circ \overset{-1}{R} \circ R = R$. Să se arate că inversa unei relaţii difuncţionale este o relaţie difuncţională.

1.99. Fie D mulţimea dreptelor din plan şi

$$R = \{(d_1, d_2) \in D \times D \mid d_1 \text{ este perpendiculară pe } d_2\}.$$

Să se arate că relaţia (D, D, R) este difuncţională.

1.100. Fie $f : A \to B$ o funcţie şi F graficul său. Să se arate că relaţia $f = (A, B, F)$ şi inversa sa $\overset{-1}{f} = (B, A, \overset{-1}{F})$ sunt relaţii difuncţionale.

1.101. Fie $R \subseteq A \times B$. Să se arate că următoarele afirmaţii sunt echivalente:
a) relaţia (A, B, R) este difuncţională;
b) dacă $a_1, a_2 \in A$ şi $R\langle a_1\rangle \cap R\langle a_2\rangle \neq \emptyset$ atunci $R\langle a_1\rangle = R\langle a_2\rangle$;
c) dacă $b_1, b_2 \in A$ şi $\overset{-1}{R}\langle b_1\rangle \cap \overset{-1}{R}\langle b_2\rangle \neq \emptyset$ atunci $\overset{-1}{R}\langle b_1\rangle = \overset{-1}{R}\langle b_2\rangle$;
d) există familiile $(A_i)_{i\in I}$, $(B_i)_{i\in I}$ de submulţimi disjuncte ale mulţimii A, respectiv ale mulţimii B, astfel încât

$$R = \bigcup_{i\in I} A_i \times B_i.$$

1.102. Fie $R \subseteq A \times A$. Să se arate că R este o relaţie de echivalenţă dacă şi numai dacă R este o relaţie difuncţională reflexivă.

1.103. Să se arate că dacă $R \subseteq A \times B$ este o relaţie difuncţională atunci:
a) $\overset{-1}{R} \circ R$ este o relaţie de echivalenţă pe $pr_1 R$;
b) $R \circ \overset{-1}{R}$ este o relaţie de echivalenţă pe $pr_2 R$;
c) există o bijecţie între mulţimile cât $pr_1 R/\overset{-1}{R} \circ R$ şi $pr_2 R/R \circ \overset{-1}{R}$.
Să se deducă de aici că pentru orice funcţie $f : A \to B$ există o bijecţie între mulţimile $A/\ker f$ şi $f(A)$.

1.104. Fie A, B două mulţimi, $A' \subseteq A$, $B' \subseteq B$, ρ_1 o relaţie de echivalenţă pe A' şi ρ_2 o relaţie de echivalenţă pe B'. Să se arate că dacă F este graficul unei bijecţii $f : A'/\rho_1 \to B'/\rho_2$ atunci $R = \overset{-1}{F_2} \circ F \circ F_1 \subseteq A \times B$ (unde F_1, F_2 sunt graficele funcţiilor canonice $p_{\rho_1} : A' \to A'/\rho_1$, respectiv $p_{\rho_2} : B' \to B'/\rho_2$) este o relaţie difuncţională pentru care $pr_1 R = A'$ şi $pr_2 R = B'$.

1.105. Să se arate că axiomele ce definesc noţiunea de relaţie de ordine (parţială) sunt independente, adică nici una dintre ele nu este o consecinţă a celorlalte două.

1.106. Fie A o mulţime. Să se arate că intersecţia dintre mulţimea relaţiilor de echivalenţă pe A şi mulţimea relaţiilor de ordine pe A este formată numai din relaţia de egalitate.

1.107. Să se dea câte un exemplu de mulţime:
a) ordonată care nu este total ordonată;
b) total ordonată care nu este bine ordonată;
c) bine ordonată;
d) ordonată care nu este dirijată;
e) dirijată care nu este total ordonată.

1.108. Fie A o mulţime, $A' \subseteq A$ şi $\rho \subseteq A \times A$. Să se arate că:
a) dacă ρ este o relaţie de ordine pe A atunci restricţia ρ' a lui ρ la A', adică $\rho' = \rho \cap (A' \times A')$, este o relaţie de ordine pe A';
b) ρ este o relaţie de ordine (totală) pe A dacă şi numai dacă $\overset{-1}{\rho}$ este o relaţie de ordine (totală) pe A.

1.109. Să se arate că relaţia de divizibilitate în $\mathbb{Z}$ este o relaţie de preordine, dar nu este nici relaţie de ordine şi nici relaţie de echivalenţă. Să se determine relaţia de echivalenţă indusă de această preordine şi relaţia de ordine în mulţimea cât. Să se găsească o bijecţie între mulţimea cât şi $\mathbb{N}$.

1.110. a) Să se determine toate relaţiile de ordine pe mulţimile $A = \{a\}$, $B = \{a, b\}$ şi $C = \{a, b, c\}$.
b) Câte mulţimi ordonate neizomorfe cu 1, 2 şi 3 elemente există?
c) Să se determine relaţiile de ordine totală de la punctul a).
d) În fiecare mulţime ordonată de la punctul a) să se determine elementele minimale, elementele maximale, cel mai mic element şi cel mai mare element.

1.111. Fie $(A, \leq)$ o mulţime ordonată. Să se arate că $(A, \leq)$ este izomorfă cu o submulţime a mulţimii ordonate $(\mathcal{P}(A), \subseteq)$.

1.112. Fie A şi B două mulţimi. Să se arate că funcţia

$$f : \mathcal{P}(A \times B) \to \mathcal{P}(B \times A),\ f(\rho) = \overset{-1}{\rho}$$

este un izomorfism de ordine pentru relaţia de incluziune.

1.113. Să se arate că :
a) dacă într-o mulţime ordonată există cel mai mic (cel mai mare) element atunci acesta este singurul element minimal (maximal);
b) unicitatea elementului minimal (maximal) nu implică faptul că acesta este cel mai mic (cel mai mare) element.

1.114. Fie $\mathcal{R}$ mulţimea relaţiilor de ordine pe o mulţime A. Să se arate că relaţiile de ordine totală pe A coincid cu elementele maximale din $(\mathcal{R}, \subseteq)$.

1.115. Să se arate că dacă ρ este o relaţie de ordine pe A atunci există o relaţie de ordine totală ρ' pe A astfel încât $\rho \subseteq \rho'$, adică orice ordonare poate fi extinsă la o ordonare totală.

1.116. Să se arate că orice mulţime ordonată finită verifică condiţia minimalităţii şi condiţia maximalităţii.

1.117. Să se arate că orice mulţime total ordonată finită este bine ordonată.

1.118. Să se arate că orice mulţime total ordonată $(A, \leq)$ care verifică condiţia minimalităţii şi condiţia maximalităţii este finită.

1.119. Să se arate că dacă $(A, \leq)$ este o mulţime bine ordonată şi $f : A \to A$ este o funcţie injectivă crescătoare atunci nu există nici un $a \in A$ astfel încât $a > f(a)$.

1.120. Să se arate că între două mulţimi bine ordonate există cel mult un izomorfism.

1.121. Să se demonstreze că o mulţime total ordonată A este bine ordonată dacă şi numai dacă A nu are nici o submulţime izomorfă cu mulţimea întregilor negativi ordonată de relaţia $\leq$ obişnuită.

1.122. Să se arate că orice două mulţimi finite total ordonate care au acelaşi număr de elemente sunt izomorfe.

1.123. Fie (A_i, ρ_i) $(i = 1, 2)$ două mulţimi ordonate. Să se arate că :
a) $A_1 \times A_2$ este ordonată de relaţia ρ definită astfel:

$$(a_1, a_2)\rho(a_1', a_2') \Leftrightarrow a_1\rho_1 a_1' \text{ şi } a_2\rho_2 a_2'.$$

Din faptul că ρ_1, ρ_2 sunt ordonări totale rezultă că ρ este o ordonare totală?
b) ρ este cea mai mare relaţie de ordine pe $A_1 \times A_2$ pentru care proiecţiile canonice sunt crescătoare.
c) $(A_1 \times A_2, \rho)$ are următoarea proprietate de universalitate: pentru orice mulţime ordonată (A, R) şi orice funcţii crescătoare $u_1 : A \to A_1$, $u_2 : A \to A_2$ există o singură funcţie crescătoare $u : A \to A_1 \times A_2$ astfel încât triunghiurile următoarei diagrame să fie comutative

$$\begin{tikzcd} & A \arrow[dl, "u_2"'] \arrow[d, dotted, "u"'] \arrow[dr, "u_1"] & \\ A_1 & A_1 \times A_2 \arrow[l, "p_1"'] \arrow[r, "p_2"] & A_2 \end{tikzcd} .$$

d) Proprietatea de universalitate a lui $(A_1 \times A_2, \rho)$ determină pe $(A_1 \times A_2, \rho)$ până la un izomorfism (de ordine).

1.124. Să se generalizeze problema precedentă pentru o familie oarecare de mulţimi ordonate. Să se deducă din generalizarea punctului a) al problemei anterioare că dacă $(A, \leq)$ este o mulţime ordonată şi I este o mulţime oarecare atunci relaţia $\leq$ definită prin

$$f \leq g \Leftrightarrow \forall i \in I,\ f(i) \leq g(i)$$

este o relaţie de ordine pe mulţimea de funcţii A^I. Să se examineze cazul particular când $I = \mathbb{R} = A$.

1.125. Fie (A, ρ_1), (B, ρ_2), (C, ρ_3) mulţimi ordonate, $f : A \to B$ şi $g : B \to C$. Să se arate că:
a) dacă f şi g sunt crescătoare atunci $g \circ f$ este crescătoare;
b) dacă f şi g sunt descrescătoare atunci $g \circ f$ este crescătoare;
c) dacă una dintre funcţiile f şi g este crescătoare şi cealaltă descrescătoare atunci $g \circ f$ este descrescătoare.

1.126. Să se dea un exemplu de funcţie bijectivă şi crescătoare care nu este un izomorfism de ordine. Să se arate că orice funcţie bijectivă şi crescătoare al cărei domeniu este o mulţime total ordonată este un izomorfism de ordine.

1.127. Fie $(A, \leq)$ o mulţime ordonată şi $a, b \in B$. Vom spune că b este un *succesor imediat* sau un *element imediat următor* al lui a dacă $a < b$ şi nu există nici un $x \in A$ astfel încât $a < x < b$. Dual se defineşte noţiunea de *predecesor imediat* sau *element imediat anterior* al lui a. Să se arate că într-o mulţime bine ordonată orice element, diferit de cel mai mare element (dacă acesta există), are un succesor imediat. Este adevărată afirmaţia duală?

1.128. Fie $(A, \leq)$ o mulţime ordonată şi $X \subseteq B \subseteq A$. Să se arate că:
a) dacă există $\inf_A X$ şi $\inf_B X$ atunci $\inf_B X \leq \inf_A X$;
b) dacă există $\sup_A X$ şi $\sup_B X$ atunci $\sup_B X \geq \sup_A X$.

1.129. Câte latici se pot defini pe o mulţime formată dintr-un element, din două elemente, din trei elemente?

1.130. Să se arate că:
a) o mulţime ordonată $(L, \leq)$ este o latice dacă şi numai dacă pentru orice submulţime finită nevidă $X \subseteq L$, există $\inf X$ şi $\sup X$.
b) orice latice finită $(L, \leq)$ este o latice completă şi să se determine $\inf \emptyset$ şi $\sup \emptyset$.

1.131. Să se arate, folosind teorema de caracterizare a laticilor complete ([34, Teorema 1.6.8]), că $(\mathbb{N}, \leq)$ nu este o latice completă.

1.132. Să se arate că:
a) orice lanţ (mulţime total ordonată) $(A, \leq)$ este o latice şi orice submulţime a lui A este o sublatice. Este $(A, \leq)$ o latice completă?
b) o latice $(A, \leq)$ este un lanţ dacă şi numai dacă orice submulţime a lui A este o sublatice.

1.133. Să se dea câte un exemplu de latice:
a) care are cel mai mic element, dar nu are cel mai mare element;
b) care are cel mai mare element, dar nu are cel mai mic element;
c) care nu are nici cel mai mic element şi nici cel mai mare element;
d) care are cel mai mic şi cel mai mare element.

1.134. Să se arate că $(\mathbb{N}, |)$ (mulţimea $\mathbb{N}$ ordonată de relaţia de divizibilitate) este o latice şi că $\mathbb{N}^*$ şi submulţimea $\{2k \mid k \in \mathbb{N}\}$ sunt sublatici. Este $(\mathbb{N}, |)$ o latice completă? Dar $(\mathbb{N}^*, |)$?

1.135. Să se arate că orice sublatice completă L' a unei latici complete $(L, \leq)$ conţine pe cel mai mic element al lui L şi pe cel mai mare element al lui L.

1.136. Fie A o mulţime şi $B \subseteq A$. Să se arate că $(\mathcal{P}(A), \subseteq)$ este o latice completă şi că $\mathcal{P}(B)$ este o sublatice a laticii $(\mathcal{P}(A), \subseteq)$ care este sublatice completă dacă şi numai dacă $A = B$.

1.137. Să se arate că $(\mathbb{R}^{\mathbb{R}}, \leq)$, unde $\leq$ este relaţia definită astfel:

$$f \leq g \ \Leftrightarrow \ \forall x \in \mathbb{R},\ f(x) \leq g(x),$$

este o latice, iar submulţimea $D(\mathbb{R}, \mathbb{R}) \subseteq \mathbb{R}^{\mathbb{R}}$ formată din funcţiile derivabile pe $\mathbb{R}$ este o mulţime dirijată, dar nu este o sublatice a lui $\mathbb{R}^{\mathbb{R}}$. Este $D(\mathbb{R}, \mathbb{R})$ o latice?

1.138. a) Fie (A_1, ρ_1) şi (A_2, ρ_2) două mulţimi ordonate. Să se arate că dacă (A_1, ρ_1) şi (A_2, ρ_2) sunt latici (complete) atunci $A_1 \times A_2$ este latice (completă) în raport cu relaţia ρ definită prin

$$(a_1, a_2)\rho(a_1', a_2') \ \Leftrightarrow \ a_1 \rho_1 a_1' \text{ şi } a_2 \rho_2 a_2'.$$

b) Examinaţi cazul particular $(A_1, \rho_1) = (\mathbb{N}, \leq)$, $(A_2, \rho_2) = (\mathbb{N}, |)$.
c) Să se generalizeze punctul a) pentru o familie oarecare de latici şi să se deducă din această generalizare că dacă $(L, \leq)$ este o latice (completă) atunci pentru orice mulţime I, mulţimea L^I este o latice (completă) în raport cu relaţia $\leq$ definită prin

$$f \leq g \ \Leftrightarrow \ \forall i \in I,\ f(i) \leq g(i).$$

d) Să se deducă din c) prima parte a problemei anterioare.

1.139. Să se arate că există funcţii crescătoare între latici, care nu sunt omomorfisme de latici.

1.140. Fie $f : A \to B$ o funcţie. Să se arate că:
a) funcţia $f^* : \mathcal{P}(B) \to \mathcal{P}(A),\ f^*(Y) = \overset{-1}{f}(Y)$ este un omomorfism de latici;
b) funcţia $f_* : \mathcal{P}(A) \to \mathcal{P}(B),\ f_*(X) = f(X)$ este un omomorfism de latici dacă şi numai dacă f este injectivă.

1.141. Fie $A = \{1, 2, 3\}$ şi $B = \{n \in \mathbb{N} \mid n|30\}$. Să se găsească:
a) un izomorfism între mulţimile ordonate $(\mathcal{P}(A), \subseteq)$ şi $(B, |)$;
b) toate izomorfismele lui $(\mathcal{P}(A), \subseteq)$ pe $(B, |)$.

1.142. Să se arate că în orice latice $(L, \leq)$ sunt verificate următoarele proprietăţi:

$$(a \vee b) \wedge c \geq (a \wedge c) \vee (b \wedge c),\ \forall a, b, c \in L\ (\textit{subdistributivitate});$$
$$a, b, c \in L,\ a \leq c\ \Rightarrow\ a \vee (b \wedge c) \leq (a \vee b) \wedge c\ (\textit{submodularitate}).$$

1.143. O *latice* $(L, \leq)$ se numeşte *modulară* dacă pentru orice $a, b, c \in L$

$$a \leq c \Rightarrow a \vee (b \wedge c) = (a \vee b) \wedge c.$$

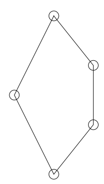
Să se arate că pentru o latice $(L, \leq)$ următoarele afirmaţii sunt echivalente:
a) L este modulară;
b) pentru orice $a, b, c \in L$ avem

$$a \vee [b \wedge (a \vee c)] = (a \wedge b) \vee (a \wedge c);$$

c) pentru orice $a, b, c \in L$,

$$a \leq b,\ a \vee c = b \vee c,\ a \wedge c = b \wedge c \Rightarrow a = b;$$

d) L nu conţine nici o sublatice izomorfă cu laticea



numită (laticea) *pentagon*.

1.144. Fie L o latice modulară şi $a, b \in L$. Să se arate că funcţiile:

$$\varphi_a : [b, a \vee b] \to [a \wedge b, a],\ \varphi_a(x) = a \wedge x\,,$$
$$\varphi_b : [a \wedge b, a] \to [b, a \vee b],\ \varphi_b(y) = y \vee b$$

sunt izomorfisme de latici şi $\varphi_a^{-1} = \varphi_b$.

1.145. O *latice* $(L, \leq)$ se numeşte *distributivă* dacă pentru orice $a, b, c \in L$ avem

$$(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c).$$

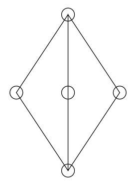
Să se arate că pentru o latice $(L, \leq)$ următoarele afirmaţii sunt echivalente:
a) L este distributivă;
b) pentru orice $a, b, c \in L$ avem

$$(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c);$$

c) pentru orice $a, b, c \in L$

$$a \vee c = b \vee c,\ \ a \wedge c = b \wedge c \Rightarrow a = b;$$

d) L este modulară şi nu conţine nici o sublatice izomorfă cu laticea



numită (laticea) *diamant*.

1.146. Să se arate că orice lanţ este o latice distributivă.

1.147. Să se arate că laticea $(\mathbb{N}, |)$ este distributivă.

1.148. Să se arate că orice sublatice a unei latici modulare (respectiv distributive) este o latice modulară (respectiv distributivă) şi că orice imagine omomorfă a unei latici modulare (respectiv distributive) este o latice modulară (respectiv distributivă).

1.149. Să se determine toate laticile neizomorfe cu cel mult 5 elemente. Care dintre acestea sunt modulare? Dar distributive?

1.150. O latice $(L, \leq)$ se numeşte *latice (algebră) Boole* dacă este distributivă, are cel mai mic şi cel mai mare element (notate cu 0, respectiv 1) şi pentru orice $x \in L$ există $x' \in L$ astfel încât $x \wedge x' = 0$ şi $x \vee x' = 1$ (numit *complement al lui* x). Să se arate că într-o latice Boole fiecare element are complement unic.

1.151. Fie M o mulţime. Să se arate că mulţimea $\mathcal{P}(M)$ a submulţimilor mulţimii M, ordonată cu incluziunea, formează o latice Boole.

1.152. Fie $\mathcal{P}$ mulţimea formulelor (expresiilor) calculului propoziţional şi $p, q \in \mathcal{P}$. Să se arate că relaţia ρ definită în $\mathcal{P}$ prin $p\,\rho\,q$ *dacă şi numai dacă* $p \to q$ *este identic adevărată* (*tautologie*) este o relaţie de preordine. Fie $\equiv$ echivalenţa determinată de ρ şi $\leq$ relaţia de ordine indusă de ρ pe mulţimea cât $\mathcal{P}/\equiv$ (vezi [34, Teorema 1.8.16]). Să se arate că $(\mathcal{P}/\equiv, \leq)$ este o latice Boole.

1.153. Fie B o latice (algebră) Boole, $a_i \in B$ $(i \in I)$ şi a_i' complementul lui a_i. Să se arate că:
a) dacă unul dintre elementele $\bigvee_{i\in I} a_i$, $\bigwedge_{i\in I} a_i'$ există atunci există şi celălalt şi

$$\left(\bigvee_{i\in I} a_i\right)' = \bigwedge_{i\in I} a_i';$$

b) dacă unul dintre elementele $\bigwedge_{i\in I} a_i$, $\bigvee_{i\in I} a_i'$ există atunci există şi celălalt şi

$$\left(\bigwedge_{i\in I} a_i\right)' = \bigvee_{i\in I} a_i'.$$

1.154. Fie A o mulţime şi $\mathcal{P}(A)$ mulţimea părţilor sale. O submulţime $\mathcal{C} \subseteq \mathcal{P}(A)$ se numeşte *sistem de închidere* pe A dacă pentru orice submulţime $\mathcal{D} \subseteq \mathcal{C}$ avem

$$\bigcap_{X\in\mathcal{D}} X \in \mathcal{C}.$$

Să se arate că:
a) orice sistem de închidere pe A conţine pe A;
b) dacă $\mathcal{C}$ este sistem de închidere pe A atunci $(\mathcal{C}, \subseteq)$ este latice completă.

1.155. Fie A o mulţime infinită, $\mathcal{P}_f(A)$ mulţimea submulţimilor finite şi $\mathcal{P}_i(A)$ mulţimea submulţimilor infinite ale lui A. Sunt $\mathcal{P}_f(A)$ şi $\mathcal{P}_i(A)$ sisteme de închidere pe A?

1.156. Fie A o mulţime. O funcţie $J : \mathcal{P}(A) \to \mathcal{P}(A)$ se numeşte *operator de închidere* pe A dacă verifică următoarele condiţii:
i) pentru orice $X \subseteq A$ avem $X \subseteq J(X)$, adică J este extensiv;
ii) pentru orice $X, Y \subseteq A$ cu $X \subseteq Y$ avem $J(X) \subseteq J(Y)$, adică J este crescător;
iii) pentru orice $X \subseteq A$ avem $J(J(X)) = J(X)$ (ceea ce este echivalent cu faptul că $J \circ J = J$), adică J este idempotent.
O *submulţime* $X \subseteq A$ se numeşte *închisă relativ la* J dacă $J(X) = X$, iar $J(X)$ se numeşte *închiderea lui* X *relativ la* J. Să se arate că:
a) $X \subseteq A$ este închisă dacă şi numai dacă există $X' \subseteq A$ astfel încât $X = J(X')$;
b) condiţia iii) din definiţia operatorului de închidere poate fi înlocuită cu

iii') $J(J(X)) \subseteq J(X),\ \forall X \subseteq A.$

1.157. Fie A mulţime şi $R \subseteq A \times A$ o relaţie de preordine. Să se arate că funcţia

$$J : \mathcal{P}(A) \to \mathcal{P}(A),\ J(X) = R(X)$$

este un operator de închidere pe A.

1.158. Fie A o mulţime şi J, J' doi operatori de închidere pe A. Să se arate că:
a) $J' \circ J$ este un operator de închidere dacă şi numai dacă

$$J \circ J' \circ J = J' \circ J;$$

b) dacă $J' \circ J = J \circ J'$ atunci $J' \circ J$ este un operator de închidere.

Fie A o mulţime. Spunem că un *operator de închidere* J este *algebric* dacă pentru orice $X \subseteq A$ şi orice $a \in J(X)$ există o submulţime finită $X' \subseteq X$ astfel încât $a \in J(X')$. Au loc următoarele afirmaţii:
i) Dacă $\mathcal{C}$ este un sistem de închidere pe A atunci

$$J_{\mathcal{C}} : \mathcal{P}(A) \to \mathcal{P}(A),\ J_{\mathcal{C}}(X) = \bigcap\{Y \in \mathcal{C} \mid X \subseteq Y\}$$

este un operator de închidere pe A (vezi [33, Teorema 1.5.6]).
ii) Dacă J este un operator de închidere pe A atunci

$$\mathcal{C}_J = \{X \subseteq A \mid J(X) = X\}$$

este un sistem de închidere pe A(vezi [33, Teorema 1.5.7]).
iii) Corespondenţa $\mathcal{C} \mapsto J_{\mathcal{C}}$ realizează o bijecţie între mulţimea sistemelor de închidere pe A şi mulţimea operatorilor de închidere pe A şi inversa sa este dată de corespondenţa $J \mapsto \mathcal{C}_J$ (vezi [33, Teorema 1.5.8]).

Spunem că un *sistem de închidere* $\mathcal{C}$ este *algebric* dacă operatorul de închidere $J_{\mathcal{C}}$ este algebric. Un sistem de închidere $\mathcal{C}$ este algebric dacă şi numai dacă pentru orice $\mathcal{D} \subseteq \mathcal{C}$ nevidă şi dirijată superior avem $\bigcap\limits_{X \in \mathcal{D}} X \in \mathcal{C}$ (vezi [33, Teorema 1.5.13]).

1.159. Fie $\mathcal{R}_r$ mulţimea relaţiilor reflexive între elementele unei mulţimi nevide A. Să se arate că:
a) $\mathcal{R}_r$ este un sistem de închidere algebric pe $A \times A$;
b) $\mathcal{R}_r$ este o sublatice a laticii $(\mathcal{P}(A \times A), \subseteq)$, dar nu este o sublatice completă;
c) dacă F_r este operatorul de închidere definit de $\mathcal{R}_r$ şi $\rho \subseteq A \times A$ atunci

$$F_r(\rho) = \rho \cup \Delta_A.$$

1.160. Fie $\mathcal{R}_t$ mulţimea relaţiilor tranzitive între elementele unei mulţimi A. Să se arate că :
a) $\mathcal{R}_t$ este un sistem de închidere algebric pe $A \times A$;
b) $\mathcal{R}_t$ nu este, în general, o sublatice a laticii $(\mathcal{P}(A \times A), \subseteq)$;
c) dacă F_t este operatorul de închidere definit de $\mathcal{R}_t$ şi $\rho \subseteq A \times A$ atunci

$$F_t(\rho) = \bigcup_{n \in \mathbb{N}^*} \rho^n.$$

1.161. Fie $\mathcal{R}_s$ mulţimea relaţiilor simetrice între elementele unei mulţimi A. Să se arate că:
a) $\mathcal{R}_s$ este o sublatice completă a laticii complete $(\mathcal{P}(A \times A), \subseteq)$;
b) dacă F_s este operatorul de închidere definit de $\mathcal{R}_s$ şi $\rho \subseteq A \times A$ atunci

$$F_s(\rho) = \rho \cup \overset{-1}{\rho}.$$

1.162. Fie $\mathcal{R}_a$ mulţimea relaţiilor antisimetrice între elementele unei mulţimi A. Să se arate că dacă $\rho_i \in \mathcal{R}_a$, $i \in I$ şi $I \neq \emptyset$ atunci $\bigcap\limits_{i \in I} \rho_i \in \mathcal{R}_a$, dar (în general) $\mathcal{R}_a$ nu este un sistem de închidere şi $\bigcup\limits_{i \in I} \rho_i \notin \mathcal{R}_a$.

1.163. Fie $\mathcal{R}_p$ mulţimea relaţiilor de preordine între elementele unei mulţimi A. Să se arate că:
a) $\mathcal{R}_p$ este un sistem de închidere algebric pe $A \times A$, dar (în general) nu este o sublatice a laticii $(\mathcal{P}(A \times A), \subseteq)$;
b) dacă F_p este operatorul de închidere definit de $\mathcal{R}_p$ şi $\rho \subseteq A \times A$ atunci

$$F_p(\rho) = \left(\bigcup_{n \in \mathbb{N}^*} \rho^n \right) \cup \Delta_A.$$

1.164. Fie A o mulţime şi $E(A)$ mulţimea relaţiilor de echivalenţă pe A. Să se arate că:
a) $E(A)$ este un sistem de închidere algebric pe $A \times A$, dar (în general) nu este o sublatice a laticii $(\mathcal{P}(A \times A), \subseteq)$;
b) dacă F_e este operatorul de închidere definit de $E(A)$ şi $\rho \subseteq A \times A$ atunci

$$F_e(\rho) = \left[\bigcup_{n \in \mathbb{N}^*} \left(\rho \cup \overset{-1}{\rho} \right)^n \right] \cup \Delta_A.$$

1.165. Fie F_r, F_s, F_t, F_p şi F_e operatorii de închidere din problemele **1.159, 1.160, 1.161, 1.163** şi **1.164**. Să se arate că:
a) $F_r \circ F_t$, $F_t \circ F_s$, $F_r \circ F_s$ şi $F_r \circ (F_t \circ F_s)$ sunt operatori de închidere;
b) $F_r \circ F_t = F_p$ şi $F_r \circ (F_t \circ F_s) = F_e$.

1.166. Să se arate că mulţimea sistemelor de închidere pe o mulţime A este un sistem de închidere pe $\mathcal{P}(A)$. Este acest sistem de închidere algebric?

1.167. Fie A o mulţime, $\mathcal{O}(A)$ mulţimea operatorilor de închidere pe mulţimea A şi $J, J' \in \mathcal{O}(A)$. Să se arate că:
a) mulţimea $\mathcal{O}(A)$ este ordonată de relaţia $\leq$ definită prin

$$J' \leq J \;\Leftrightarrow\; \forall X \subseteq A,\; J'(X) \subseteq J(X);$$

b) $(\mathcal{O}(A)), \leq)$ este o latice completă;
c) dacă $J' \circ J$ este un operator de închidere atunci

$$\sup(J', J) = J' \circ J.$$

1.168. Fie $\mathcal{O}(A)$, respectiv $\mathcal{S}(A)$ mulţimea operatorilor, respectiv sistemelor de închidere pe o mulţime A. Să se arate că funcţia

$$\varphi : \mathcal{O}(A) \to \mathcal{S}(A),\; \varphi(J) = J(\mathcal{P}(A))$$

este un antiizomorfism între $(\mathcal{O}(A), \leq)$ şi $(\mathcal{S}(A), \subseteq)$.

1.169. Fie $(A, \leq)$ şi $(B \leq)$ două mulţimi ordonate. Se spune că o pereche de funcţii $\varphi : A \to B$, $\psi : B \to A$ este o *corespondenţă Galois* dacă verifică următoarele condiţii: pentru $x, x_1, x_2 \in A$ şi $y, y_1, y_2 \in B$

$$x_1 \leq x_2 \;\Rightarrow\; \varphi(x_1) \geq \varphi(x_2);$$
$$y_1 \leq y_2 \;\Rightarrow\; \psi(y_1) \geq \psi(y_2);$$
$$x \leq \psi(\varphi(x)),\; y \leq \varphi(\psi(y)).$$

Să se arate că dacă (φ, ψ) este o corespondenţă Galois atunci

$$\varphi \circ \psi \circ \varphi = \varphi \text{ şi } \psi \circ \varphi \circ \psi = \psi.$$

1.170. Fie A şi B două mulţimi, iar $\varphi : \mathcal{P}(A) \to \mathcal{P}(B)$, $\psi : \mathcal{P}(B) \to \mathcal{P}(A)$ o corespondenţă Galois între $(\mathcal{P}(A), \subseteq)$ şi $(\mathcal{P}(B), \subseteq)$. Să se arate că:
a) funcţia $J : \mathcal{P}(A) \to \mathcal{P}(A),\ J(X) = \psi(\varphi(X))$ este operator de închidere pe A;
b) funcţia $J' : \mathcal{P}(B) \to \mathcal{P}(B),\ J'(Y) = \varphi(\psi(Y))$ este operator de închidere pe B;
c) egalitatea $f(X) = \varphi(X)$ defineşte o funcţie

$$f : \{X \subseteq A \mid J(X) = X\} \to \{Y \subseteq B \mid J'(Y) = Y\}$$

care este un antiizomorfism de ordine şi $f^{-1}(Y) = \psi(Y)$.

1.171. Fie $R \subseteq A \times B$ o relaţie binară, $\varphi : \mathcal{P}(A) \to \mathcal{P}(B)$, $\psi : \mathcal{P}(B) \to \mathcal{P}(A)$ funcţiile definite prin

$$\varphi(X) = \{y \in B \mid \forall x \in X,\ xRy\} \text{ şi } \psi(Y) = \{x \in A \mid \forall y \in Y,\ xRy\},$$

pentru orice $X \subseteq A$ şi $Y \subseteq B$. Să se arate că:

$$\varphi(X) = \bigcap_{x \in X} R\langle x\rangle \text{ şi } \psi(Y) = \bigcap_{y \in Y} \overset{-1}{R}\langle y\rangle,$$

iar φ şi ψ formează o corespondenţă Galois între $(\mathcal{P}(A), \subseteq)$ şi $(\mathcal{P}(B), \subseteq)$.

1.172. Dacă în problema anterioară se ia $A = \mathbb{R} = B$ şi în locul lui R relaţia $\leq$, să se găsească sistemele de închidere definite de operatorii de închidere $\varphi \circ \psi$ şi $\psi \circ \varphi$ (vezi problema **1.170**).

1.173. Spunem că două *mulţimi* X şi Y sunt *echivalente* (şi scriem $X \sim Y$) dacă există o funcţie bijectivă $f : X \to Y$. O mulţime echivalentă cu $\mathbb{N}$ se numeşte *mulţime numărabilă.* Să se arate că mulţimile $\mathbb{N}^*$, $\mathbb{Z}$, $\mathbb{N} \times \mathbb{N}$, $\mathbb{Q}_+ = \{x \in \mathbb{Q} \mid x > 0\}$ şi $\mathbb{Q}$ sunt numărabile.

1.174. Să se arate că dacă X este o mulţime infinită şi $x_0 \in X$ atunci

$$X \sim X \setminus \{x_0\}.$$

1.175. Să se arate că mulţimile $\mathbb{R}$, $[a, b]$, $(a, b]$, $[a, b)$, (a, b) $(a, b \in \mathbb{R},\ a < b)$, $[0, 1]$ sunt echivalente.

1.176. Fie $f : I \to J$ o funcţie bijectivă şi fie $(A_i)_{i \in I}$, $(B_j)_{j \in J}$ două familii de mulţimi astfel încât $A_i \sim B_{f(i)}$ pentru orice $i \in I$. Să se arate că: a) $\overset{\circ}{\bigcup_{i \in I}} A_i \sim \overset{\circ}{\bigcup_{j \in J}} B_j$,
b) $\prod_{i \in I} A_i \sim \prod_{j \in J} B_j$.

1.177. Fie mulţimile A_1, A_2, B_1, B_2 astfel încât $A_1 \sim A_2$ şi $B_1 \sim B_2$. Să se arate că $A_1^{B_1} \sim A_2^{B_2}$.

1.178. Fie $(X_i)_{i \in \mathbb{N}}$ o familie de mulţimi numărabile indexată după mulţimea numerelor naturale. Să se arate că mulţimea $\overset{\circ}{\bigcup_{i \in \mathbb{N}}} X_i$ este numărabilă.

Relaţia $\sim$ este reflexivă, simetrică şi tranzitivă. Asociem fiecărei mulţimi X un simbol $|X|$ numit *cardinalul* mulţimii X, caracterizat prin proprietatea

$$|X| = |Y| \Leftrightarrow X \sim Y.$$

Cardinalul mulţimii $\emptyset$ se notează cu 0, cardinalul submulţimii $\{0, 1, \ldots, n-1\}$ a mulţimii $\mathbb{N}$ se notează cu n, iar cardinalul mulţimii $\mathbb{N}$ se notează cu $\aleph_0$. Din problemele anterioare rezultă că egalităţile

$$\sum_{i \in I} |A_i| = \left|\overset{\circ}{\bigcup_{i \in I}} A_i\right|, \ \prod_{i \in I} |A_i| = \left|\prod_{i \in I} A_i\right|, \ |B|^{|A|} = \left|B^A\right|$$

nu depind de alegerea reprezentanţilor A_i, A, B ai cardinalelor $|A_i|, |A|, |B|$ $(i \in I)$, fapt care permite definirea ca mai sus a sumei, produsului, respectiv, ridicării la putere a cardinalelor. Amintim aici faptul că adunarea şi înmulţirea cardinalelor sunt asociative, comutative, înmulţirea este distributivă faţă de adunare (vezi [7, Cap.3]) şi produsul a două cardinale poate fi exprimat cu ajutorul sumei astfel:

$$\mathfrak{m} \cdot \mathfrak{n} = \underbrace{\mathfrak{m} + \mathfrak{m} + \cdots}_{\mathfrak{n}} = \underbrace{\mathfrak{n} + \mathfrak{n} + \cdots}_{\mathfrak{m}}.$$

De asemenea, amintim că ridicarea la putere a cardinalelor satisface următoarele proprietăţi: dacă $\mathfrak{m}, \mathfrak{n}, \mathfrak{p}, (\mathfrak{m}_i)_{i \in I}, (\mathfrak{m}_i)_{i \in I}$ sunt cardinale atunci

$$\left(\prod_{i \in I} \mathfrak{m}_i\right)^{\mathfrak{n}} = \prod_{i \in I} (\mathfrak{m}_i^{\mathfrak{n}}), \ \prod_{i \in I} (\mathfrak{m}^{\mathfrak{n}_i}) = \mathfrak{m}^{\left(\sum_{i \in I} \mathfrak{n}_i\right)}, \ (\mathfrak{m}^{\mathfrak{n}})^{\mathfrak{p}} = \mathfrak{m}^{\mathfrak{n} \cdot \mathfrak{p}}.$$

1.179. Fie $\mathfrak{m} = |X|$, $\mathfrak{n} = |Y|$ două numere cardinale. Scriem $\mathfrak{m} \leq \mathfrak{n}$ dacă există o funcţie injectivă $f : X \to Y$. Să se arate că:
a) relaţia $\leq$ nu depinde de alegerea reprezentanţilor;
b) dacă pentru cardinalele $\mathfrak{m}_1, \mathfrak{m}_2, \mathfrak{n}_1, \mathfrak{n}_2$ avem $\mathfrak{m}_1 \leq \mathfrak{n}_1$ şi $\mathfrak{m}_2 \leq \mathfrak{n}_2$ atunci

$$\mathfrak{m}_1 + \mathfrak{m}_2 \leq \mathfrak{n}_1 + \mathfrak{n}_2.$$

1.180. Fie $\mathfrak{m}$ şi $\mathfrak{n}$ două cardinale. Scriem $\mathfrak{m} < \mathfrak{n}$ dacă $\mathfrak{m} \leq \mathfrak{n}$ şi $\mathfrak{m} \neq \mathfrak{n}$. Să se arate că:
a) dacă $\mathfrak{m} < \mathfrak{n}$ atunci există un cardinal $\mathfrak{p} > 0$ astfel încât $\mathfrak{n} = \mathfrak{m} + \mathfrak{p}$;
b) $\mathfrak{m} \leq \mathfrak{n}$ dacă şi numai dacă există un cardinal $\mathfrak{p}$ astfel încât $\mathfrak{n} = \mathfrak{m} + \mathfrak{p}$.

1.181. Dacă $\mathfrak{m}$ şi $\mathfrak{n}$ sunt două cardinale cu $1 < \mathfrak{m}$, $1 < \mathfrak{n}$ atunci

$$\mathfrak{m} + \mathfrak{n} \leq \mathfrak{m} \cdot \mathfrak{n}.$$

1.182. Cardinalul $2^{\aleph_0}$ se notează cu $\mathfrak{c}$ şi se numeşte *puterea continuului.* Să se arate că au loc următoarele egalităţi: 1) $\aleph_0 + \aleph_0 = \aleph_0$; 2) $\underbrace{\aleph_0 + \aleph_0 + \cdots}_{\aleph_0} = \aleph_0 \ \cdot \ \aleph_0 = \aleph_0$; 3) $\mathfrak{c}^2 = \mathfrak{c}$; 4) $\mathfrak{c}^{\aleph_0} = \mathfrak{c}$; 5) $\mathfrak{c} + \mathfrak{c} = \mathfrak{c}$; 6) $\aleph_0^{\aleph_0} = \mathfrak{c}$; 7) $\aleph_0 \cdot \mathfrak{c} = \mathfrak{c}$.

1.183. Să se arate că mulţimile $\mathbb{R}$, $\mathbb{R}^2$, $\ldots$, $\mathbb{R}^n$ $(n \in \mathbb{N}^*)$ şi $\mathbb{C}$ sunt de puterea continuului.

1.184. Cardinalul unei mulţimi infinite se numeşte *cardinal infinit.* Să se arate că dacă $\mathfrak{m}$ este un cardinal infinit atunci:
a) $\mathfrak{m}^2 = \mathfrak{m}$;
b) $\mathfrak{m} + \mathfrak{m} = \mathfrak{m}$;
c) pentru orice cardinal $\mathfrak{n}$ cu proprietatea că $1 \leq \mathfrak{n} \leq \mathfrak{m}$ avem

$$\mathfrak{m} + \mathfrak{n} = \mathfrak{m} \text{ şi } \mathfrak{m} \cdot \mathfrak{n} = \mathfrak{m}.$$

Reamintim că două *mulţimi bine ordonate* $(X, \leq)$ şi $(Y, \leq)$ sunt *izomorfe* dacă există $f : X \to Y$ o funcţie bijectivă pentru care f şi f^{-1} sunt crescătoare. În acest caz scriem $(X, \leq) \approx (Y, \leq)$. Relaţia $\approx$ astfel obţinută este reflexivă, simetrică şi tranzitivă. Asociem fiecărei mulţimi bine ordonate $(X, \leq)$ un simbol $o(X, \leq)$, numit *ordinalul mulţimii bineordonate* $(X, \leq)$, caracterizat de proprietatea

$$o(X, \leq) = o(Y, \leq) \Leftrightarrow (X, \leq) \approx (Y, \leq)\,.$$

Cardinalul unei mulţimi bine ordonate de ordinal α se notează cu $\overline{\alpha}$ şi se numeşte *cardinalul ordinalului* α. Elementele mulţimii $\{\alpha \mid \overline{\alpha} = \mathfrak{m}\}$ se numesc ordinale corespunzătoare cardinalului $\mathfrak{m}$.

1.185. a) Să se arate că toate ordinalele corespunzătoare unui cardinal finit sunt egale.
b) Să se arate că (pentru cardinale infinite) există mai multe ordinale corespunzătoare aceluiaşi cardinal.

Ordinalul mulţimii vide se notează cu 0, ordinalul mulţimii $\{1, 2, \ldots, n\}$ $(n \in \mathbb{N}^*)$ se notează cu n, iar ordinalul lui $(\mathbb{N}, \leq)$ se notează cu ω.

1.186. Fie $(A, \leq)$, $(B, \leq)$ două mulţimi bine ordonate de ordinale α, respectiv β şi fie relaţia $\leq$ definită pe produsul cartezian $A \times B$ prin

$$(a_1, b_1) \leq (a_2, b_2) \;\Leftrightarrow\; a_1 < a_2 \text{ sau } (a_1 = a_2 \text{ şi } b_1 \leq b_2)$$

(numită *ordonare lexicografică*). Să se arate că:
a) mulţimea $(A \times B, \leq)$ este bine ordonată;
b) dacă mulţimile bine ordonate $(A', \leq)$ şi $(B', \leq)$ sunt izomorfe cu $(A, \leq)$, respectiv $(B, \leq)$ atunci mulţimile bine ordonate $(A \times B, \leq)$ şi $(A' \times B', \leq)$ sunt izomorfe — ceea ce permite definirea *produsului* $\beta \cdot \alpha$ al *ordinalelor* β şi α astfel: $\beta \cdot \alpha$ *este ordinalul mulţimii bine ordonate* $(A \times B, \leq)$.

1.187. Fie $(I, \leq)$ o mulţime bine ordonată, pentru fiecare $i \in I$, $(A_i, \leq)$ o mulţime bineordonată de ordinal α_i şi relaţia $\leq$ definită pe $\overset{\circ}{\bigcup\limits_{i \in I}} A_i$ prin

$$(i_1, a') \leq (i_2, a'') \;\Leftrightarrow\; (i_1 = i_2 \text{ şi } a' \leq a'' \text{ în } A_{i_1}) \text{ sau } i_1 \leq i_2.$$

Să se arate că:
a) mulţimea $\left(\overset{\circ}{\bigcup\limits_{i \in I}} A_i\,,\ \leq\right)$ este bine ordonată;
b) dacă f este un izomorfism de ordine între mulţimile bine ordonate $(J, \leq)$ şi $(I, \leq)$ şi pentru fiecare $i \in I$ mulţimile bine ordonate $(A_i, \leq)$ şi $(B_{f(i)}, \leq)$ sunt izomorfe

atunci mulţimile bine ordonate $\left(\overset{\circ}{\bigcup_{i\in I}} A_i\,,\ \leq\right)$ şi $\left(\overset{\circ}{\bigcup_{j\in I}} B_j\,,\ \leq\right)$ au acelaşi ordinal — ceea ce permite definirea *sumei* $\sum_{i\in I}\alpha_i$ a *familiei de ordinale* $(\alpha_i)_{i\in I}$ astfel: $\sum_{i\in I}\alpha_i$ *este ordinalul mulţimii bine ordonate* $\left(\overset{\circ}{\bigcup_{i\in I}} A_i\,,\ \leq\right)$;

c) dacă α şi β sunt două ordinale atunci ordinalul $\alpha+\beta$ nu este întotdeauna egal cu ordinalul $\beta+\alpha$.

Capitolul 2

Grupoizi. Semigrupuri. Grupuri

2.1. Să se dea două exemple de grupoizi care nu sunt semigrupuri şi să se cerceteze dacă au elemente neutre.

2.2. Să se dea un exemplu de grupoid care are două elemente neutre la stânga (dreapta). Există grupoizi care au două elemente neutre la stânga diferite şi un element neutru la dreapta? Există grupoizi care au două elemente neutre?

2.3. Să se dea exemplu de grupoid cu element neutru în care există un element cu două simetrice diferite. Există semigrupuri cu această proprietate?

2.4. Să se dea un exemplu de grupoid cu element neutru în care există un element simetrizabil cu care nu se poate simplifica. Există semigrupuri cu această proprietate?

2.5. Fie $*$ operaţia definită pe $\mathbb{R}$ prin

$$x * y = x + y + xy.$$

Să se arate că $(\mathbb{R}, *)$ este un monoid comutativ şi că intervalul $[-1, +\infty)$ este o parte stabilă a lui $(\mathbb{R}, *)$.

2.6. Fie $\lambda \in \mathbb{R}$ şi $*$ operaţia definită pe $\mathbb{R}$ prin

$$x * y = xy - 2x - 2y + \lambda.$$

Să se determine valorile parametrului real λ pentru care intervalul $(2, +\infty)$ este o parte stabilă în $(\mathbb{R}, *)$.

2.7. Pe $\mathbb{R}$ se defineşte operaţia $*$ astfel

$$x * y = xy + 2ax + by, \ \forall x, y \in \mathbb{R}.$$

Să se determine $a, b \in \mathbb{R}$ astfel încât $(\mathbb{R}, *)$ să fie un semigrup comutativ.

2.8. Fie m, n, p trei numere întregi şi $*$ operaţia definită în $\mathbb{Z}$ prin

$$x * y = mxy + n(x + y) + p.$$

i) Să se determine o condiţie necesară şi suficientă pentru ca operaţia $*$ să fie asociativă.
ii) Să se determine condiţii necesare şi suficiente pentru existenţa elementului neutru în $(\mathbb{Z}, *)$.
iii) Să se determine m, n şi p astfel încât $(\mathbb{Z}, *)$ să fie grup.

2.9. Fie M o mulţime şi $\circ$ compunerea funcţiilor.
i) Să se determine în $(M^M, \circ)$ elementele inversabile la stânga (dreapta), elementele inversabile, elementele cu care se poate simplifica la stânga (dreapta) şi elementele cu care se poate simplifica.
ii) Cum trebuie să fie M pentru ca elementele inversabile la stânga să coincidă cu cele inversabile la dreapta şi cu cele inversabile?
iii) Să se întocmească tabla operaţiei $\circ$ în cazul $M = \{0, 1\}$ şi să se găsească în acest caz elementele cerute la punctul i).

2.10. Fie A o mulţime finită cu n elemente. Să se determine:
i) numărul operaţiilor (binare) pe A;
ii) numărul operaţiilor (binare) comutative pe A;
iii) numărul operaţiilor (binare) pe A care admit element neutru;
iv) numărul operaţiilor comutative şi cu element neutru ce se pot defini pe A.

2.11. Fie φ o operaţie pe mulţimea A şi $B \subseteq A$ o parte stabilă în (A, φ). Operaţia $\varphi' : B \times B \to B$ definită prin

$$(*) \qquad \varphi'(b_1, b_2) = \varphi(b_1, b_2),\ \forall b_1, b_2 \in B$$

se numeşte *operaţia indusă de φ pe B*. Să se arate că:
i) dacă φ este asociativă, respectiv comutativă, atunci φ' este asociativă, respectiv comutativă;
ii) dacă B nu este stabilă atunci formula $(*)$ nu defineşte o operaţie în B.

2.12. Să se dea un exemplu de submulţime a lui $\mathbb{Z}$ care nu este stabilă relativ la $+$ şi să se arate că $+$ nu induce o operaţie pe această mulţime. Să se determine părţile stabile finite ale lui $(Z, +)$.

2.13. Să se determine părţile stabile finite ale semigrupului $(\mathbb{Z}, \cdot)$.

2.14. Fie $(A, \cdot)$ un grupoid. Să se arate că mulţimile

$$B_1 = \{a \in A \mid (ax)y = a(xy),\ \forall x, y \in A\},$$
$$B_2 = \{a \in A \mid (xa)y = x(ay),\ \forall x, y \in A\},$$
$$B_3 = \{a \in A \mid (xy)a = x(ya),\ \forall x, y \in A\}$$

sunt părţi stabile în $(A, \cdot)$ şi că $(A, \cdot)$ este un semigrup dacă şi numai dacă A coincide cu una dintre mulţimile $B_1,\ B_2,\ B_3$.

2.15. Să se arate, folosind problema anterioară, că operaţia $\cdot$ definită pe mulţimea $A = \{a, b, c, d, f\}$ prin tabla

$\cdot$	a	b	c	d	f
a	a	a	a	d	d
b	a	b	c	d	d
c	a	c	b	d	d
d	d	d	d	a	a
f	a	f	f	a	a

este asociativă.

2.16. Fie M o mulţime şi $\mathcal{P}(M)$ mulţimea părţilor sale. Să se determine un izomorfism între grupoizii $(\mathcal{P}(M), \cup)$ şi $(\mathcal{P}(M), \cap)$. Sunt $(\mathcal{P}(M), \cup)$ şi $(\mathcal{P}(M), \cap)$ grupuri?

2.17. Fie $(A, \cdot)$ un grupoid şi $X, Y \subseteq A$. Definim $X \cdot Y = \{x \cdot y \mid x \in X,\ y \in Y\}$. Să se arate că:
i) $(\mathcal{P}(A), \cdot)$ are un subgrupoid izomorf cu $(A, \cdot)$;
ii) $X \cdot Y = Y \cdot X$ dacă şi numai dacă pentru orice $x \in X$ şi $y \in Y$ există $x', x'' \in X$ şi $y', y'' \in Y$ astfel încât $xy = y'x'$ şi $yx = x''y''$. Deduceţi de aici că $(A, \cdot)$ comutativ implică $(\mathcal{P}(A), \cdot)$ comutativ.
iii) B este un subgrupoid în $(A, \cdot)$ dacă şi numai dacă $B \cdot B \subseteq B$;
iv) dacă $B_1, B_2 \subseteq A$ sunt părţi stabile şi $B_1 \cdot B_2 = B_2 \cdot B_1$ atunci $B_1 \cdot B_2$ este parte stabilă;
v) dacă $Y_1, Y_2 \subseteq A$ atunci

$$X \cdot (Y_1 \cup Y_2) = (X \cdot Y_1) \cup (X \cdot Y_2),\ (Y_1 \cup Y_2) \cdot X = (Y_1 \cdot X) \cup (Y_2 \cdot X),$$
$$X \cdot (Y_1 \cap Y_2) \subseteq (X \cdot Y_1) \cap (X \cdot Y_2),\ (Y_1 \cap Y_2) \cdot X \subseteq (Y_1 \cdot X) \cap (Y_2 \cdot X),$$

iar dacă $x \in A$ este un element cu care se poate simplifica şi $X = \{x\}$ atunci ultimele două incluziuni devin egalităţi;
vi) dacă $(A, \cdot)$ este un semigrup, respectiv un monoid, atunci $(\mathcal{P}(A), \cdot)$ este un semigrup, respectiv un monoid;
vii) dacă $A \neq \emptyset$ atunci $(\mathcal{P}(A), \cdot)$ nu este grup, chiar dacă $(A, \cdot)$ este un grup.

2.18. Să se arate că mulţimea $S(\mathbb{N}, +)$ a subgrupoizilor lui $(\mathbb{N}, +)$ formează, în raport cu incluziunea mulţimilor, o latice completă. Să se verifice că pentru orice $n \in \mathbb{N}$, $n\mathbb{N} = \{nk \mid k \in \mathbb{N}\}$ este parte stabilă în $(\mathbb{N}, +)$ şi să se determine $2\mathbb{N} \wedge 3\mathbb{N}$ şi $2\mathbb{N} \vee 3\mathbb{N}$ în laticea $(S(\mathbb{N}, +), \subseteq)$. Este $S(\mathbb{N}, +)$ sublatice în $(\mathcal{P}(\mathbb{N}), \subseteq)$?

2.19. Fie $(A, \cdot)$ un grupoid. Un *element* $x \in A$ se numeşte *idempotent* dacă $x^2 = x$. Să se arate că dacă $(A, \cdot)$ este un semigrup comutativ şi orice element din A este idempotent atunci funcţia $f : A \to \mathcal{P}(A)$, $f(x) = xA$ (unde $xA = \{x\} \cdot A$) este un omomorfism al lui $(A, \cdot)$ în $(\mathcal{P}(A), \cap)$ şi în $(\mathcal{P}(A), \cdot)$.

2.20. O mulţime ordonată $(L, \leq)$ se numeşte *semilatice* în raport cu $\vee$ dacă pentru orice $a, b \in L$ există $a \vee b = \sup(a, b)$.
a) Dacă $(L, \leq)$ este o semilatice în raport cu $\vee$ atunci $(L, \vee)$ este un semigrup comutativ în care toate elementele sunt idempotente.
b) Dacă $(L, \vee)$ este un semigrup comutativ în care toate elementele sunt idempotente atunci relaţia $\leq$ definită pe L prin

$$a \leq b \Leftrightarrow a \vee b = b$$

este o relaţie de ordine şi $(L, \leq)$ este o semilatice în care

$$\sup(a, b) = a \vee b,\ \forall a, b \in L.$$

c) Corespondenţa $(A, \cdot) \mapsto (A, \leq)$ (unde $x \leq y \Leftrightarrow xy = y$) realizează o bijecţie între clasa semigrupurilor comutative cu toate elementele idempotente şi clasa semilaticilor în raport cu $\vee$.

2.21. O mulţime ordonată $(L, \leq)$ se numeşte *semilatice* în raport cu $\wedge$ dacă pentru orice $a, b \in L$ există $a \wedge b = \inf(a, b)$.
a) Dacă $(L, \leq)$ este o semilatice în raport cu $\wedge$ atunci $(L, \wedge)$ este un semigrup comutativ în care toate elementele sunt idempotente.
b) Dacă $(L, \wedge)$ este un semigrup comutativ în care toate elementele sunt idempotente atunci relaţia $\leq$ definită pe L prin

$$a \leq b \Leftrightarrow a \wedge b = a$$

este o relaţie de ordine şi $(L, \leq)$ este o semilatice în care

$$\inf(a, b) = a \wedge b,\ \forall a, b \in L.$$

c) Corespondenţa $(A, \cdot) \mapsto (A, \leq)$ (unde $x \leq y \Leftrightarrow xy = x$) realizează o bijecţie între clasa semigrupurilor comutative cu toate elementele idempotente şi clasa semilaticilor în raport cu $\wedge$.

2.22. a) Dacă $(L, \leq)$ este o latice atunci egalităţile

$$a \vee b = \sup(a, b),\ a \wedge b = \inf(a, b)$$

definesc pe L două operaţii (binare) $\vee$, $\wedge$ care sunt asociative, comutative şi verifică legile de absorbţie, adică

$$a \vee (a \wedge b) = a,\ a \wedge (a \vee b) = a.$$

b) Dacă $(L, \vee, \wedge)$ este o structură algebrică cu două operaţii (binare) asociative, comutative care verifică legile de absorbţie atunci

$$a \vee b = b \Leftrightarrow a \wedge b = a$$

pentru orice $a, b \in L$, relaţia $\leq$ definită prin

$$a \leq b \Leftrightarrow a \vee b = b \Leftrightarrow a \wedge b = a$$

este o relaţie de ordine şi $(L, \leq)$ este o latice în care

$$\sup(a, b) = a \vee b,\ \inf(a, b) = a \wedge b,\ \forall a, b \in L.$$

c) Corespondenţa $(L, \vee, \wedge) \mapsto (L, \leq)$ (unde $x \leq y \Leftrightarrow x \vee y = y$) realizează o bijecţie între clasa structurilor algebrice cu două operaţii (binare) asociative, comutative care verifică legile de absorbţie şi clasa laticilor.

2.23. Fie $a, b \in \mathbb{R}$ şi $f : \mathbb{C} \to \mathbb{R}$, $f(z) = a|z| + b$. Să se determine a şi b astfel încât f să fie un omomorfism al lui $(\mathbb{C}, \cdot)$ în $(\mathbb{R}, \cdot)$.

2.24. Fie $(A, \cdot)$, $(B, \cdot)$ grupoizi şi $y_0 \in B$.
i) Ce proprietate trebuie să aibă y_0 pentru ca funcţia constantă $f : A \to B$, $f(x) = y_0$ să fie un omomorfism?
ii) Ce condiţii trebuie să verifice B pentru ca oricare ar fi grupoidul $(A, \cdot)$ să existe un omomorfism de la $(A, \cdot)$ la $(B, \cdot)$?

2.25. Fie $(A,\cdot)$, $(B,\cdot)$ grupoizi, $1 \in A$ element neutru în $(A,\cdot)$ şi $f : A \to B$ un omomorfism. Să se arate că:
i) $f(1)$ este un element neutru în $(f(A),\cdot)$;
ii) dacă $(B,\cdot)$ are un element neutru şi acesta aparţine lui $f(A)$ atunci f este unital (adică $f(1)$ este unitatea lui $(B,\cdot)$);
iii) dacă f este surjectiv atunci $(B,\cdot)$ are element neutru şi f este unital.

2.26. Fie $(A,\cdot)$, $(B,*)$ grupoizi şi $f : A \to B$ omomorfism. Să se arate că:
i) dacă A' este un subgrupoid al lui $(A,\cdot)$ atunci $f(A')$ este un subgrupoid al lui $(B,\cdot)$, iar dacă grupoidul $(A,\cdot)$ este comutativ, respectiv semigrup, monoid, grup atunci grupoidul $(f(A'),\cdot)$ este comutativ, respectiv semigrup, monoid, grup;
ii) dacă B' este un subgrupoid al lui $(B,\cdot)$ atunci $\overset{-1}{f}(B')$ este un subgrupoid al lui $(A,\cdot)$.

2.27. Să se arate că există grupoizi care nu sunt semigrupuri, dar se aplică omomorf pe semigrupuri şi chiar pe grupuri.

2.28. Fie $(A,\cdot)$, $(B,\cdot)$ grupoizi şi $f : A \to B$ un omomorfism.
i) Dacă un *element* $x \in A$ este *regulat* (adică cu x se poate simplifica) rezultă oare că $f(x)$ este regulat?
ii) Dacă cei doi grupoizi au unitate şi $x \in A$ este inversabil atunci cum trebuie să fie f pentru ca $f(x^{-1}) = [f(x)]^{-1}$?

2.29. Fie $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, $C = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$, $D = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$. Să se determine subsemigrupurile $\langle A\rangle$, $\langle A, D\rangle$, $\langle B, C\rangle$ şi $\langle B, D\rangle$ ale semigrupului $(M_2(\mathbb{Z}),\cdot)$.

2.30. a) Fie $(A,\cdot)$ un grupoid şi $X \subseteq A$. Să se arate că subgrupoidul lui $(A,\cdot)$ generat de X este reuniunea tuturor submulţimilor $X_k \subseteq A$ $(k \in \mathbb{N})$ obţinute astfel

$$X_0 = X,\ X_{k+1} = X_k \cup \{x_1 \cdot x_2 \mid x_1, x_2 \in X_k\}.$$

b) Fie $(A,\cdot),(B,\cdot)$ doi grupoizi şi $X \subseteq A$. Să se arate că dacă $f : A \to B$ este un omomorfism atunci $f(\langle X\rangle) = \langle f(X)\rangle$.

2.31. Fie $(A,\cdot)$, $(B,\cdot)$ grupoizi şi fie X un sistem de generatori pentru $(A,\cdot)$. Să se arate că o funcţie a lui X în B se extinde cel mult într-un mod la un omomorfism al lui $(A,\cdot)$ în $(B,\cdot)$.

2.32. a) Fie $(A,\cdot)$ un semigrup, respectiv un monoid. Să se arate că orice funcţie $f : \{1\} \to A$ se poate prelungi în mod unic la un omomorfism, respectiv omomorfism unital al lui $(\mathbb{N}^*,+)$, respectiv $(\mathbb{N},+)$ în $(A,\cdot)$.
b) Se poate prelungi funcţia $g : \{1,2\} \to \mathbb{N}$, $g(1) = 1 = g(2)$ la un endomorfism al lui $(\mathbb{N}^*,+)$?
c) Să se determine subsemigrupul $\langle 2\rangle$ generat de 2 în $(\mathbb{N},\cdot)$ şi să se găsească toate omomorfismele lui $(\mathbb{N}^*,+)$ în $\langle 2\rangle$.

2.33. Fie $m, n \in \mathbb{Z}$, $m < -1$, $n > 1$. Să se determine endomorfismele $f : \mathbb{Q} \to \mathbb{Q}$ ale lui $(\mathbb{Q},\cdot)$ pentru care avem $f(\mathbb{Q}) \subseteq \{m, m+1, \ldots, n\}$.

2.34. Fie $n \in \mathbb{N}^*$, $M_n(\mathbb{C})$ mulţimea matricelor pătrate de ordinul n cu elemente din $\mathbb{C}$ şi $A = (a_{ij}) \in M_n(\mathbb{C})$. Care dintre funcţiile $f_k : M_n(\mathbb{C}) \to \mathbb{C}$ $(k = 1, 2, 3)$ definite prin $f_1(A) = \det A$, $f_2(A) = \sum_{i=1}^{n} a_{ii}$ şi $f_3(A) = 1$ sunt omomorfisme ale lui $(M_n(\mathbb{C}), \cdot)$ în $(\mathbb{C}, \cdot)$? Dar ale lui $(M_n(\mathbb{C}), +)$ în $(\mathbb{C}, +)$?

2.35. Fie $f, g : \mathbb{C} \to \mathbb{C}$, $f(z) = |z|$, iar $g(0) = 0$ şi $g(z) = arg\, z$ pentru $z \neq 0$. Sunt f şi g endomorfisme ale lui $(\mathbb{C}, +)$? Dar ale lui $(\mathbb{C}, \cdot)$?

2.36. a) Fie $(A_i\,, \cdot\,)_{i\in I}$ o familie de grupoizi. Să se arate că pe produsul cartezian $P = \prod_{i\in I} A_i$ există o singură structură de grupoid $(P, \cdot)$ pentru care proiecţiile canonice $p_j : P \to A_j$, $p_j((a_i)_{i\in I}) = a_j$ sunt omomorfisme. Mai mult, dacă fiecare $(A_i, \cdot)$ este semigrup, respectiv grupoid comutativ, monoid, grup, atunci $(P, \cdot)$ este, de asemenea, semigrup, respectiv grupoid comutativ, monoid, grup.
b) Să se arate că grupoidul $(P, \cdot)$ de mai sus are următoarea proprietate de universalitate: pentru orice grupoid $(B, \cdot)$ şi orice familie de omomorfisme $u_i : B \to A_i$, $i \in I$ există un singur omomorfism $u : B \to P$ astfel încât diagrama

$$\begin{tikzcd} B \arrow[d, dotted, "u"'] \arrow[dr, "u_j"] & \\ P \arrow[r, "p_j"] & A_j \end{tikzcd}$$

să fie comutativă pentru orice $j \in I$.
c) Dacă grupoidul $(P', \cdot)$ şi omomorfismele $p'_i : P' \to A'_i$, $i \in I$ au aceeaşi proprietate de universalitate ca şi $(P, \cdot)$ şi omomorfismele $p_i, i \in I$ atunci grupoizii $(P, \cdot)$ şi $(P', \cdot)$ sunt izomorfi, adică proprietatea de universalitate a lui $(P, \cdot)$ determină pe $(P, \cdot)$ până la un izomorfism.
d) Fie $(A, \cdot)$ un grupoid şi $(A_i, \cdot) = (A, \cdot)$ pentru orice $i \in I$. Să se arate că grupoidul $(P, \cdot) = (A^I, \cdot)$ are un subgrupoid izomorf cu $(A, \cdot)$.

2.37. Fie A_1, A_2, A trei grupoizi, respectiv grupuri şi $f_1 : A_1 \to A$, $f_2 : A_2 \to A$ două omomorfisme. Să se arate că:
a) submulţimea $S = \{(a_1, a_2) \in A_1 \times A_2 \mid f_1(a_1) = f_2(a_2)\}$ este un subgrupoid, respectiv subgrup al produsului $(A_1 \times A_2, \cdot)$, funcţiile $g_1 : S \to A_1$, $g_1(a_1, a_2) = a_1$, $g_2 : S \to A_2$, $g_2(a_1, a_2) = a_2$ sunt omomorfisme şi diagrama

$$\begin{tikzcd} S \arrow[r, "g_1"] \arrow[d, "g_2"'] & A_1 \arrow[d, "f_1"] \\ A_2 \arrow[r, "f_2"] & A \end{tikzcd}$$

este comutativă;
b) tripletul (S, g_1, g_2) are următoarea proprietate de universalitate: pentru orice grupoid S' şi orice omomorfisme $g'_1 : S' \to A_1$, $g'_2 : S' \to A_2$ care fac comutativ

pătratul diagramei

$$\begin{tikzcd}
S' \arrow[rr, "g_1'"] \arrow[dd, "g_2'"'] \arrow[dr, dotted, "g"] & & A_1 \arrow[dd, "f_1"] \\
& S \arrow[ur, "g_1"'] \arrow[dl, "g_2"] & \\
A_2 \arrow[rr, "f_2"] & & A
\end{tikzcd}$$

există un omomorfism unic $g : S' \to S$ astfel încât $g_1' = g_1 \circ g$ şi $g_2' = g_2 \circ g$;
c) proprietatea de universalitate a tripletului (S, g_1, g_2) determină pe S până la un izomorfism.

2.38. Fie $(A, \cdot)$, $(B, \cdot)$ grupoizi, respectiv grupuri şi $f, g : A \to B$ omomorfisme. Să se arate că:
a) submulţimea $E = \{a \in A \mid f(a) = g(a)\}$ este un subgrupoid, respectiv subgrup al lui $(A, \cdot)$ şi $f \circ i = g \circ i$, unde $i : E \to A$ este omomorfismul de incluziune;
b) perechea (E, i) are următoarea proprietate de universalitate: pentru orice grupoid $(C, \cdot)$ şi orice omomorfism $h : C \to A$ care verifică egalitatea $f \circ h = g \circ h$ există un omomorfism unic $\gamma : C \to E$ astfel încât $h = i \circ \gamma$;
c) proprietatea de universalitate a perechii (E, i) determină pe E până la un izomorfism.

2.39. Fie $(A, \cdot)$ un grupoid. Să se arate că Δ_A şi $A \times A$ sunt congruenţe pe $(A, \cdot)$ şi grupoidul cât $(A/\Delta_A, \cdot)$ este izomorf cu $(A, \cdot)$. Câte elemente are mulţimea suport a grupoidului cât $(A/A \times A, \cdot)$?

2.40. Fie ρ_1 şi ρ_2 relaţiile binare definite în $\mathbb{C}$ astfel:

$$z_1 \rho_1 z_2 \Leftrightarrow \arg z_1 = \arg z_2 \text{ sau } z_1 = 0 = z_2 \, ;$$
$$z_1 \rho_2 z_2 \Leftrightarrow |z_1| = |z_2|.$$

Sunt ρ_1 şi ρ_2 congruenţe pe $(\mathbb{C}, +)$? Dar pe $(\mathbb{C}, \cdot)$? În caz afirmativ să se determine grupoidul cât.

2.41. a) Fie $(G, \cdot)$, $(G', \cdot)$ doi grupoizi şi $f : G \to G'$ un omomorfism. Să se arate că nucleul $\ker f$ al funcţiei f este o congruenţă pe $(G, \cdot)$ şi că grupoizii $(G/\ker f, \cdot)$ şi $(f(G), \cdot)$ sunt izomorfi.
b) Să se arate că funcţia $f : \mathbb{C} \to \mathbb{R}$, $f(z) = |z|$ este un omomorfism de la $(\mathbb{C}, \cdot)$ la $(\mathbb{R}, \cdot)$ şi să se aplice punctul a) acestui omomorfism.
c) Să se arate că $f : M_n(\mathbb{C}) \to \mathbb{C}$, $f(A) = \det A$ este un omomorfism de la $(M_n(\mathbb{C}), \cdot)$ la $(\mathbb{C}, \cdot)$ şi să se aplice punctul a) acestui omomorfism.

2.42. a) Fie $(A, \cdot)$ un grupoid, B un subgrupoid în $(A, \cdot)$ şi ρ o congruenţă pe $(A, \cdot)$. Să se arate că $\rho(B)$ este subgrupoid în $(A, \cdot)$, că relaţiile $\rho' = \rho \cap (B \times B)$ şi $\rho'' = \rho \cap (\rho(B) \times \rho(B))$ sunt congruenţe pe B, respectiv pe $\rho(B)$ şi că grupoizii cât B/ρ' şi $\rho(B)/\rho''$ sunt izomorfi.
b) Să se arate că $B = \{x \in \mathbb{R} \mid |x| > 1\}$ este un subgrupoid al lui $(\mathbb{C}, \cdot)$ şi să se aplice punctul a) lui A şi congruenţei ρ_2 din problema **2.40**.

2.43. Fie $n \in \mathbb{N}$ şi ρ_n relaţia binară definită în $\mathbb{Z}$ prin

$$x\rho_n y \Leftrightarrow \exists k \in \mathbb{Z} : x - y = kn.$$

Menţionăm că în locul notaţiei $x\rho_n y$ se foloseşte, în general, notaţia $x \equiv y (\bmod n)$, iar ρ_n se numeşte *congruenţa modulo n*. Să se arate că:
a) ρ_n este o congruenţă pe $(\mathbb{Z}, +)$ şi să se determine grupoidul cât $(\mathbb{Z}/\rho_n, +)$;
b) $m|n \Leftrightarrow \rho_n \subseteq \rho_m$.

2.44. Este congruenţa modulo n ($n \in \mathbb{N}$) o congruenţă pe $(\mathbb{Z}, \cdot)$? În caz afirmativ să se determine grupoidul cât.

2.45. Fie $(A, \cdot)$ un grupoid şi ρ o congruenţă pe $(A, \cdot)$. Să se arate că grupoidul cât $(A/\rho, \cdot)$ nu este, în general, un subgrupoid al grupoidului $(\mathcal{P}(A), \cdot)$ introdus în problema **2.17.**

2.46. a) Fie $(A, \cdot)$ un grupoid şi $\rho_1 \subseteq \rho_2$ două congruenţe pe $(A, \cdot)$. Să se arate că există un unic omomorfism de grupoizi $f : A/\rho_1 \to A/\rho_2$ astfel încât $p_{\rho_2} = f \circ p_{\rho_1}$, iar dacă notăm nucleul lui f cu ρ_2/ρ_1 atunci grupoizii cât $(A/\rho_1)/(\rho_2/\rho_1)$ şi A/ρ_2 sunt izomorfi.
b) Să se aplice punctul a) lui $(\mathbb{Z}, +)$ şi congruenţelor modulo 2 şi modulo 6.

2.47. Fie $(A, \cdot)$ un grupoid. Un element $a \in A$ se numeşte *nongenerator* al lui A dacă pentru orice $X \subseteq A$,

$$\langle X \cup \{a\} \rangle = A \Rightarrow \langle X \rangle = A.$$

Un *subgrupoid* $M \neq A$ al lui $(A, \cdot)$ se numeşte *maximal* dacă pentru orice subgrupoid B al lui $(A, \cdot)$,

$$M \subseteq B \Rightarrow B = M \text{ sau } B = A.$$

Să se arate că:
a) mulţimea $F(A)$ a nongeneratorilor lui A formează un subgrupoid al lui $(A, \cdot)$, numit *subgrupoidul lui Frattini*;
b) pentru orice automorfism $f : A \to A$ avem $f(F(A)) \subseteq F(A)$;
c) $F(A)$ coincide cu intersecţia subgrupoizilor maximali ai lui $(A, \cdot)$ (dacă nu există subgrupoizi maximali atunci această intersecţie este A).

2.48. Fie $(A, \cdot)$ un *semigrup ciclic* (adică un semigrup generat de un element al lui A). Dacă există $k_1, k_2 \in \mathbb{N}^*$ diferite astfel încât $a^{k_1} = a^{k_2}$ şi n este cel mai mic întreg pozitiv pentru care există un $m \in \mathbb{N}^*$, $m < n$ astfel încât $a^m = a^n$, atunci perechea (m, n) se numeşte *tipul* lui $(A, \cdot)$. Să se arate că dacă $(A, \cdot)$ este de tipul (m, n) atunci:
i) $a^{m+q(n-m)} = a^m$ pentru orice $q \in \mathbb{N}$;
ii) $a^k \in K_{n-m} = \{a^m, a^{m+1}, \ldots, a^{n-1}\}$ pentru $k \geq n$; K_{n-m} se numeşte *partea periodică* a lui A;
iii) $A = \{a, a^2, \ldots, a^m, a^{m+1}, \ldots, a^{n-1}\}$;
iv) K_{n-m} este parte stabilă în $(A, \cdot)$ şi $(K_{n-m}, \cdot)$ este grup.

2.49. Să se arate că
i) pentru orice $m, n \in \mathbb{N}^*$, $m < n$, există un semigrup ciclic de tipul (m, n);
ii) toate semigrupurile ciclice de tipul (m, n) sunt izomorfe;
iii) orice semigrup ciclic infinit este izomorf cu $(\mathbb{N}^*, +)$.

2.50. Să se întocmească tabla de operaţie a semigrupului ciclic de tipul $(3, 7)$ şi să se arate că partea sa periodică este un grup.

2.51. Fie $(A, \cdot)$ un semigrup. Un *element* $x \in A$ se numeşte *regular* dacă există $x' \in A$ astfel încât $xx'x = x$. Dacă orice $x \in A$ este regular atunci $(A, \cdot)$ se numeşte *semigrup regular*. Să se arate că:
i) dacă x este regular atunci există $\overline{x} \in A$ astfel încât $x\overline{x}x = x$ şi $\overline{x}x\overline{x} = \overline{x}$;
ii) un semigrup regular cu mulţimea suport nevidă are elemente idempotente;
iii) dacă M este o mulţime atunci semigrupul $(M^M, \circ)$ al transformărilor lui M (adică al funcţiilor $f : M \to M$) este regular.

2.52. Fie $(A, \cdot)$ un semigrup. Să se arate că:
i) dacă $(A, \cdot)$ este grup atunci există în A un singur element idempotent;
ii) dacă $(A, \cdot)$ este regular şi $A \neq \emptyset$ atunci A are un singur element idempotent dacă şi numai dacă $(A, \cdot)$ este grup.

2.53. Fie $G = (-1, 1)$, $x, y \in G$ şi

$$x * y = \frac{x + y}{1 + xy}. \tag{1}$$

Să se arate că:
i) egalitatea (1) defineşte o operaţie $*$ pe G şi $(G, *)$ este un grup abelian;
ii) între grupul multiplicativ al numerelor reale pozitive $(\mathbb{R}_+^*, \cdot)$ şi $(G, *)$ există un izomorfism $f : \mathbb{R}_+^* \to G$ de forma $f(x) = \dfrac{\alpha x - 1}{x + 1}$.

2.54. Fie $x, y \in \mathbb{R}$ şi $x * y = xy - 5x - 5y + 30$. Este $(\mathbb{R}, *)$ grup? Dar $(\mathbb{R} \setminus \{5\}, *)$?

2.55. Fie X o mulţime nevidă şi $(G, \cdot)$ un grup. Dacă $f, g \in G^X$ atunci definim funcţia $f \cdot g : X \to G$ prin $(f \cdot g)(x) = f(x) \cdot g(x)$. Să se arate că $(G^X, \cdot)$ este grup şi că $(G^X, \cdot)$ are un subgrup izomorf cu $(G, \cdot)$.

2.56. Să se arate că un grupoid $(G, +)$ este grup abelian dacă şi numai dacă verifică condiţiile:
i) $(x + y) + z = x + (z + y),\ \forall x, y, z \in G$;
ii) $\exists 0 \in G :\ \forall x \in G,\ 0 + x = x$;
iii) $\forall x \in G,\ \exists x' \in G :\ x' + x = 0$.

2.57. Să se arate că un semigrup $(G, \cdot)$ este grup dacă şi numai dacă $G \neq \emptyset$ şi $a \cdot G = G = G \cdot a$ pentru orice $a \in G$.

2.58. Fie $(G, \cdot)$ un grup şi $x, y \in G$. Să se arate că:
a) $(x \cdot y)^{-1} = x^{-1} \cdot y^{-1} \Leftrightarrow x \cdot y = y \cdot x \Leftrightarrow (x \cdot y)^2 = x^2 \cdot y^2$;
b) $x \cdot y = y \cdot x \Rightarrow (x \cdot y)^n = x^n \cdot y^n,\ \forall n \in \mathbb{Z}$;
c) $x \cdot y = y \cdot x \Rightarrow x^m \cdot y^n = y^n \cdot x^m,\ \forall m, n \in \mathbb{Z}$.

2.59. Fie $(G, \cdot)$ un grup şi $f, g : G \to G$, $f(x) = x^{-1}$, $g(x) = x^2$. Să se arate că:
i) f este o bijecţie;
ii) f este automorfism dacă şi numai dacă $(G, \cdot)$ este abelian;
iii) g este omomorfism dacă şi numai dacă $(G, \cdot)$ este abelian.

2.60. Să se arate că un semigrup finit este grup dacă şi numai dacă mulţimea suport este nevidă şi toate elementele sale sunt regulate. Grupurile infinite se pot caracteriza analog?

2.61. Fie $\mathbb{R}_+^* = \{x \in \mathbb{R} \mid x > 0\}$. Să se arate că grupurile $(\mathbb{R}_+^*, \cdot)$ şi $(\mathbb{R}, +)$ sunt izomorfe.

2.62. Fie $n > 1$ întreg impar şi fie $*$ operaţia definită pe $\mathbb{R}$ prin

$$x * y = \sqrt[n]{x^n + y^n}.$$

Să se arate că $(\mathbb{R}, *)$ este un grup izomorf cu $(\mathbb{R}, +)$.

2.63. Să se arate că grupul $(\mathbb{C}, +)$ este izomorf cu $(\mathbb{R} \times \mathbb{R}, +)$, dar $(\mathbb{C}^*, \cdot)$ nu este izomorf cu $(\mathbb{R}^* \times \mathbb{R}^*, \cdot)$.

2.64. Fie $(G, \cdot)$, $(G', \cdot)$ şi $(G'', \cdot)$ trei grupuri. Să se arate că au loc următoarele izomorfisme de grupuri:
i) $(G \times G', \cdot) \simeq (G' \times G, \cdot)$;
ii) $((G \times G') \times G'', \cdot) \simeq (G \times (G' \times G''), \cdot) \simeq (G \times G' \times G'', \cdot)$.

2.65. Fie $(G, \cdot)$ un semigrup cu $G \neq \emptyset$ şi fie $t_a, t'_a : G \to G$, $t_a(x) = ax$, $t'_a(x) = xa$ $(a \in G)$. Să se arate că:
i) dacă $(G, \cdot)$ este grup atunci pentru orice $a \in G$ funcţiile t_a, t'_a sunt bijecţii;
ii) dacă pentru orice $a \in G$, t_a şi t'_a sunt surjecţii atunci $(G, \cdot)$ este grup.

2.66. Fie $(G, \cdot)$ un semigrup, $G \neq \emptyset$, $g \in G$ şi $t_g, t'_g : G \to G$ funcţiile definite prin $t_g(x) = gx$, $t'_g(x) = xg$, iar

$$T(G) = \{t_g \mid g \in G\},\ T'(G) = \{t'_g \mid g \in G\}.$$

Să se arate că:
i) $T(G)$ şi $T'(G)$ sunt subsemigrupuri ale lui $(G^G, \circ)$;
ii) dacă $(G, \cdot)$ este un monoid atunci $(G, \cdot)$ este izomorf cu $(T(G), \circ)$, iar funcţia $f : G \to T'(G)$, $f(g) = t'_g$ este o bijecţie şi $f(g_1 \cdot g_2) = f(g_2) \circ f(g_1)$, adică f este antiizomorfism;
iii) dacă $(G, \cdot)$ este un grup atunci $T(G)$ şi $T'(G)$ sunt subgrupuri ale lui $(S_G, \circ)$ izomorfe cu $(G, \cdot)$.

2.67. Fie $(G, \cdot)$ un grupoid, $End(G, \cdot)$ mulţimea endomorfismelor grupoidului $(G, \cdot)$ şi $Aut(G, \cdot)$ mulţimea automorfismelor lui $(G, \cdot)$. Să se arate că:
a) $End(G, \cdot)$ este un subsemigrup al semigrupului $(G^G, \circ)$;
b) $Aut(G, \cdot)$ este un subgrup al grupului simetric $(S_G, \circ)$.

2.68. Fie $(G,+)$ şi $(G',+)$ doi grupoizi şi $f,g:G\to G'$ omomorfisme. Să se arate că:
a) funcţia $f+g:G\to G'$, $(f+g)(x)=f(x)+g(x)$ este un omomorfism dacă şi numai dacă $f(x)+g(x)=g(x)+f(x)$ pentru orice $x\in G$;
b) dacă $(G',+)$ este grup abelian atunci mulţimea $Hom(G,G')$ a omomorfismelor lui $(G,+)$ în $(G',+)$ este un grup abelian în raport cu operaţia definită mai sus.

2.69. Pe $Q=\{a_1+a_2i+a_3j+a_4k \mid a_1,a_2,a_3,a_4\in\mathbb{R}\}$ se defineşte înmulţirea astfel: dacă $q=a_1+a_2i+a_3j+a_4k$ şi $q'=b_1+b_2i+b_3j+b_4k$ atunci

$$\begin{aligned}qq'&=(a_1b_1-a_2b_2-a_3b_3-a_4b_4)+(a_1b_2+a_2b_1+a_3b_4-a_4b_3)i\\&\quad+(a_1b_3-a_2b_4+a_3b_1+a_4b_2)j+(a_1b_4+a_2b_3-a_3b_2+a_4b_1)k.\end{aligned}$$

Să se arate că:
i) $(Q,\cdot)$ este un monoid necomutativ;
ii) grupul elementelor inversabile din $(Q,\cdot)$ coincide cu $Q^*=Q\setminus\{0\}$;
iii) $H=\{-1,1,-i,i,-j,j,-k,k\}$ este un subgrup al lui $(Q^*,\cdot)$ (numit *grupul cuaternionilor*);
iv) $(Q^*,\cdot)$ are un subgrup izomorf cu $(\mathbb{C}^*,\cdot)$.

2.70. Să se arate că $H=\{z\in\mathbb{C}\mid |z|=1\}$ este un subgrup al lui $(\mathbb{C}^*,\cdot)$, dar nu este subgrup al lui $(\mathbb{C},+)$ şi să se dea un exemplu de alt subgrup H' al lui $(\mathbb{C}^*,\cdot)$ astfel încât $H\cup H'$ să nu fie subgrup al lui $(\mathbb{C}^*,\cdot)$.

2.71. Fie $(G,\cdot)$ un grup, fie $X\subseteq G$ şi $X^{-1}=\{x^{-1}\mid x\in X\}$. Să se arate că $\mathcal{I}=\{X\subseteq G\mid X^{-1}\subseteq X\}$ este o sublatice completă a laticii $(\mathcal{P}(G),\subseteq)$ şi că mulţimea $\mathcal{S}$ a subgrupurilor lui G este inclusă în $\mathcal{I}$, dar $\mathcal{I}\neq\mathcal{S}$.

2.72. Fie $(G,\cdot)$ un grup. Să se arate că:
i) laticea subgrupurilor lui $(G,\cdot)$ este o sublatice a laticii subsemigrupurilor lui $(G,\cdot)$ dar nu este sublatice completă;
ii) pentru orice subgrup H al lui $(G,\cdot)$ există o familie de subgrupuri ciclice H_i, $i\in I$, ale lui G astfel încât $H=\sup(H_i)_{i\in I}$.

2.73. Fie $(G,\cdot)$ un grup. Să se arate că reuniunea a două subgrupuri ale lui $(G,\cdot)$ este un subgrup al lui $(G,\cdot)$ dacă şi numai dacă unul dintre ele este inclus în celălalt. Să se deducă de aici că G nu poate fi scris $G=H_1\cup H_2$ unde H_1 şi H_2 sunt subgrupuri ale lui G diferite de G.

2.74. Fie $(G,\cdot)$ un grup şi H_1,H_2,H_3 subgrupuri ale lui $(G,\cdot)$. Să se arate că $H_3\subseteq H_1\cup H_2$ dacă şi numai dacă $H_3\subseteq H_1$ sau $H_3\subseteq H_2$.

2.75. Fie $(G,\cdot)$ un grup şi H, K subgrupuri ale lui G. Să se arate că are loc egalitatea $|H|\cdot|K|=|H\cdot K|\cdot|H\cap K|$.

2.76. a) Să se dea câte un exemplu de ciclu (permutare circulară) de lungime 4, de transpoziţie şi de permutare care nu e ciclu.
b) Fie $\sigma_1=(1,2,3)\circ(4,5,6,7)$, $\sigma_2=(3,4)\circ(5,2,6,1,8)$, $\sigma_3=(1,3,4)\circ(2,3,5,7)\circ(1,8,4,6)$, $\sigma_4=(8,2,1,4,3)\circ(1,2)\circ(1,5)$ şi $\sigma_5=(8,7,4,3,1,2)\circ(5,6)$ permutări din S_8. Să se găsească σ_1^3, $\sigma_2^2\circ\sigma_1$, $\sigma_3\circ\sigma_4\circ\sigma_5$, $\sigma_3^4\circ\sigma_4^2$ şi $\sigma_5\circ\sigma_4\circ\sigma_3$.

2.77. Fie M o mulţime. Să se arate că dacă $|M| \geq 3$ atunci centrul grupului $(S_M, \circ)$ este format doar din funcţia identică.

2.78. Spunem că două *permutări* $f, g \in S_M$ ale unei mulţimi M sunt *disjuncte* dacă pentru orice $x \in M$ are loc cel puţin una dintre egalităţile $f(x) = x$, $g(x) = x$. Să se arată că dacă $f, g \in S_M$ sunt permutări disjuncte atunci $f \circ g = g \circ f$.

2.79. Să se arate că două cicluri $(i_1, i_2, \ldots, i_l)$, $(j_1, j_2, \ldots, j_k)$ din S_n sunt disjuncte dacă şi numai dacă mulţimile $\{i_1, i_2, \ldots, i_l\}$, $\{j_1, j_2, \ldots, j_k\}$ sunt disjuncte.

2.80. a) Să se descompună în produs de cicluri disjuncte permutarea

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 9 & 12 & 8 & 11 & 6 & 7 & 5 & 3 & 2 & 4 & 10 & 1 \end{pmatrix}.$$

b) Să se scrie în două moduri ca produs de transpoziţii permutarea

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

2.81. Fie $n, l \in \mathbb{N}$, $n \geq l \geq 2$. Să se determine:
i) numărul transpoziţiilor din S_n;
ii) numărul ciclurilor de lungime n din S_n;
iii) numărul ciclurilor de lungime l din S_n;
iv) numărul tuturor ciclurilor (de lungime cel puţin 2) din S_n.

2.82. Fie $n \in \mathbb{N}$, $n \geq 2$, $2 \leq l \leq n$ şi $\sigma = (i_1, i_2, \ldots, i_l) \in S_n$. Să se arate că:
a) $\sigma^{-1} = (i_l, i_{l-1}, \ldots, i_1) = \sigma^{l-1}$;
b) l este cel mai mic număr natural nenul pentru care σ^l este permutarea identică (adică ordinul lui σ este l);
c) $\sigma^m(i_j) = \begin{cases} i_{j+m} & , \text{ dacă } j+m < l \\ i_{j+m-l} & , \text{ dacă } j+m > l \end{cases}$ $(m \in \mathbb{N}^*)$.

2.83. a) Fie $\gamma = (i_1, i_2, \ldots, i_k) \in S_n$. Să se arate că pentru orice $\sigma \in S_n$ avem $\sigma \circ \gamma \circ \sigma^{-1} = (\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_k))$.
b) Fie $\sigma_1 = (1,2,3) \circ (4,5,6,7)$, $\sigma_2 = (3,4) \circ (5,2,6,1,8)$, $\sigma_3 = (1,3,4) \circ (2,3,5,7) \circ (1,8,4,6)$, $\sigma_4 = (8,2,1,4,3) \circ (1,2) \circ (1,5)$ şi $\sigma_5 = (8,7,4,3,1,2) \circ (5,6)$ permutări din S_8. Să se determine $\sigma_1 \circ \sigma_4 \circ \sigma_1^{-1}$, $\sigma_5^{-2} \circ \sigma_3 \circ \sigma_5^2$, $\sigma_2^{-5} \circ \sigma_4 \circ \sigma_2^5$.
c) Fie $\sigma_1 = (1,2,3) \circ (4,5,6) \circ (7,8,9)$, $\sigma_2 = (1,4,7) \circ (2,5,8) \circ (3,6,9)$, $\sigma_3 = (4,5,6) \circ (7,8,9)$. Să se arate că $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$ şi $\sigma_1 \circ \sigma_3 = \sigma_3 \circ \sigma_1$.

2.84. Să se găsească elementele din grupul simetric $(S_n, \circ)$ permutabile cu ciclul $(i_1, i_2, \ldots, i_n) \in S_n$.

2.85. Să se arate că fiecare din următoarele mulţimi constituie un sistem de generatori pentru grupul simetric $(S_n, \circ)$:
a) $\{(i,j) \mid i,j \in \{1, \ldots, n\},\ i \neq j\}$ (mulţimea transpoziţiilor din S_n);
b) $\{(1,2), (1,3), \ldots, (1,n)\}$;
c) $\{(1,2), (2,3), \ldots, (n-1,n)\}$;
d) $\{(i_1,i_2), (i_1,i_2,\ldots,i_n)\}$, unde $\{i_1,i_2,\ldots,i_n\} = \{1,2,\ldots,n\}$;
e) $\{(i_1,i_2), (j_1,j_2,\ldots,j_n)\}$, unde $\{j_1,j_2,\ldots,j_n\} = \{1,2,\ldots,n\}$.

2.86. Să se arate că fiecare din următoarele mulţimi constituie un sistem de generatori pentru *grupul altern* A_n (grupul permutărilor pare de grad n):
a) mulţimea tuturor ciclurilor de lungime 3;
b) $\{(1,2,3),(1,2,4),\ldots,(1,2,n)\}$.

2.87. Fie $K \in \{\mathbb{Q},\mathbb{R},\mathbb{C}\}$ şi $M_n(K)$ mulţimea matricelor pătrate de ordinul n cu elemente din K, iar

$$GL_n(K) = \{A \in M_n(K) \mid \det A \neq 0\},\ SL_n(K) = \{A \in M_n(K) \mid \det A = 1\}.$$

Să se arate că:
i) $(M_n(K),\cdot)$ este un monoid necomutativ pentru $n > 1$ şi că acest monoid are un submonoid izomorf cu $(K,\cdot)$ — reamintim că o parte stabilă a unui monoid se numeşte *submonoid* atunci când conţine elementul neutru al monoidului. Este $(M_n(K),\cdot)$ grup?
ii) $GL_n(K)$ este o parte stabilă a lui $(M_n(K),\cdot)$ şi $(GL_n(K),\cdot)$ este un grup numit *grupul general liniar* de gradul n peste K.
iii) $(GL_n(K),\cdot)$ are (pentru $n \geq 1$) un subgrup izomorf cu $(K^*,\cdot)$.
iv) $(GL_2(\mathbb{R}),\cdot)$ are un subgrup izomorf cu $(\mathbb{C}^*,\cdot)$.
v) $SL_n(K)$ este un subgrup al lui $GL_n(K)$.

2.88. Fie $n \in \mathbb{N},\ n \geq 2,\ K \in \{\mathbb{Q},\mathbb{R},\mathbb{C}\}$ şi $GL_n(K)$ grupul general liniar de gradul n peste K. Să se arate că $Z(GL_n(K)) = \{aI_n \mid a \in K^*\}$, unde $Z(GL_n(K))$ este centrul grupului $GL_n(K)$, iar I_n este matricea unitate.

2.89. Fie $GL_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det A \text{ este inversabil în } (\mathbb{Z},\cdot)\} = \{A \in M_n(\mathbb{Z}) \mid \det A \in \{-1,1\}\}$ şi $SL_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Q}) \mid \det A = 1\}$. Să se arate că:
i) $GL_n(\mathbb{Z})$ este un subgrup al lui $(GL_n(\mathbb{Q}),\cdot)$;
ii) grupul $(GL_n(\mathbb{Z}),\cdot)$ este infinit dacă $n > 1$;
iii) subgrupul lui $(GL_2(\mathbb{Z}),\cdot)$ generat de $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ este izomorf cu $(\mathbb{Z},+)$;
iv) $SL_n(\mathbb{Z})$ este un subgrup al lui $GL_n(\mathbb{Z})$.

2.90. Fie

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Să se arate că în $(GL_2(\mathbb{Z}),\cdot)$ avem $\mathrm{ord}A = 4$, $\mathrm{ord}B = 3$ şi $\mathrm{ord}(AB) = \infty$.

2.91. Fie $n \in \mathbb{N}^*$. Să se arate că grupul $(GL_n(\mathbb{Z}),\cdot)$ are un subgrup izomorf cu grupul $(S_n,\circ)$ al permutărilor unei mulţimi cu n elemente, adică $(S_n,\circ)$ se scufundă izomorf în $(GL_n(\mathbb{Z}),\cdot)$.

2.92. Să se arate că orice grup finit de ordin n se scufundă izomorf în $(GL_n(\mathbb{Z}),\cdot)$.

2.93. Să se determine ordinele elementelor

$$x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ y = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix},\ z = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

$$u = \begin{pmatrix} -2+3i & -2+2i \\ 1-i & 3-2i \end{pmatrix},\ v = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

în $(GL_n(\mathbb{C}),\cdot)$ şi grupurile ciclice generate de acestea.

2.94. Fie M o mulţime, $\mathcal{P}(M)$ mulţimea submulţimilor sale şi $\triangle$ *diferenţa simetrică*, adică pentru $X, Y \subseteq M$ avem $X \triangle Y = (X \setminus Y) \cup (Y \setminus X)$. Să se arate că $(\mathcal{P}(M), \triangle)$ este un grup în care orice element diferit de $\emptyset$ are ordinul 2.

2.95. Fie $(L, \vee, \wedge, ')$ o latice Boole. Definim în L operaţia $+$ prin

$$x + y = (x \wedge y') \vee (x' \wedge x).$$

Să se arate că $(L, +)$ este un grup în care orice element diferit de elementul neutru are ordinul 2.

2.96. Să se arate că dacă $(G, \cdot)$ este un grup finit de ordin par atunci există cel puţin un element $x \in G \setminus \{1\}$ astfel încât $x^{-1} = x$ (adică x are ordinul 2).

2.97. Fie $(G, \cdot)$ un grup şi $x, y \in G$. Să se arate că $\mathrm{ord}(xy) = \mathrm{ord}(yx)$.

2.98. Fie $(G, \cdot)$, $(G', \cdot)$ două grupuri, $x \in G$ şi $f : G \to G'$ un omomorfism. Să se arate că:
i) dacă $x \in G$ şi ordinul lui x este finit atunci ordinul lui $f(x)$ este finit şi $\mathrm{ord} f(x)$ divide $\mathrm{ord}(x)$;
ii) dacă f este injectiv şi $x \in G$ atunci $\mathrm{ord} f(x) = \mathrm{ord}\, x$;
iii) dacă $\mathrm{ord} f(x) = \mathrm{ord}\, x$ pentru orice $x \in G$ atunci omomorfismul f este injectiv.

2.99. Fie $(G, \cdot)$ un grup. Să se arate că:
i) G are un singur element de ordin 1;
ii) pentru orice $x \in G$ avem $\mathrm{ord} x = \mathrm{ord}\, x^{-1}$;
iii) dacă $x \in G$, $n = \mathrm{ord}\, x$ şi $k \in \mathbb{N}^*$ atunci $\mathrm{ord}(x^k) = \dfrac{n}{(k, n)}$, unde (k, n) este c.m.m.d.c. al lui k şi n;
iv) dacă $n = \mathrm{ord} x$ şi $n = km$ atunci $\mathrm{ord}(x^k) = m$;
v) dacă $(G, \cdot)$ este un grup ciclic de ordin $n \in \mathbb{N}^*$, generat de x, atunci x^k este un generator pentru G dacă şi numai dacă $(k, n) = 1$;
vi) dacă $(G, \cdot)$ este un grup ciclic de ordinul n şi $D_n = \{d \in \mathbb{N}^* \mid d|n\}$ atunci laticea subgrupurilor lui $(G, \cdot)$ este izomorfă cu $(D_n, |)$.

2.100. Fie $(G, \cdot)$ un grup şi $x, y \in G$ *elemente permutabile*, adică $xy = yx$. Fie $m = \mathrm{ord}\, x$, $n = \mathrm{ord}\, y$, $m, n \in \mathbb{N}^*$. Să se arate că:
i) $\mathrm{ord}(xy)$ este finit şi $\mathrm{ord}(xy)$ divide pe $[m, n]$ (unde $[m, n]$ este c.m.m.m.c. al lui m şi n);
ii) dacă $\langle x \rangle \cap \langle y \rangle = \{1\}$ atunci $\mathrm{ord}(xy) = [m, n]$;
iii) dacă $(m, n) = 1$ atunci $\mathrm{ord}(xy) = mn$ şi $\langle x, y \rangle = \langle xy \rangle$;
iv) există în G (chiar şi numai în ipoteza iniţială) un element de ordinul $[m, n]$.

2.101. Fie $\sigma \in S_n$. Să se arate că dacă $\sigma = \gamma_1 \circ \cdots \circ \gamma_k$ este descompunerea lui σ în cicluri disjuncte şi lungimea lui γ_i este l_i $(i = 1, \ldots, k)$ atunci ordinul lui σ este c.m.m.m.c. al numerelor $l_1, \ldots, l_k$.

2.102. Să se arate că dacă $(G, \cdot)$ este un grup, $x, y \in G$, $\mathrm{ord}\, x < \infty$, $\mathrm{ord}\, y < \infty$ şi $xy \neq yx$ atunci este posibil ca $\mathrm{ord}(xy) = \infty$.

2.103. Fie $(G,\cdot)$ un grup şi $t(G) = \{x \in G \mid \mathrm{ord}x < \infty\}$. Să se arate că:
i) dacă $(G,\cdot)$ este abelian atunci $t(G)$ este un subgrup al lui G (numit *partea de torsiune* a lui G);
ii) dacă $(G,\cdot)$ este necomutativ atunci $t(G)$ nu este, în general, un subgrup în G;
iii) $(G \setminus t(G)) \cup \{1\}$ nu este, în general, subgrup (nici chiar în caz abelian);
iv) dacă $\emptyset \neq H \subseteq t(G)$ atunci H este un subgrup în G dacă şi numai dacă

$$(*) \qquad h_1, h_2 \in H \Rightarrow h_1h_2 \in H;$$

v) dacă $(G,\cdot)$ este finit şi $\emptyset \neq H \subseteq G$ atunci H este un subgrup în G dacă şi numai dacă verifică pe $(*)$.

2.104. Fie $(G,\cdot)$ şi $(G',\cdot)$ două grupuri abeliene. Să se arate că:
i) dacă G şi G' sunt izomorfe atunci $t(G)$ şi $t(G')$ sunt izomorfe;
ii) este posibil ca $t(G)$ şi $t(G')$ să fie izomorfe fără ca G şi G' să fie izomorfe.

2.105. Să se arate că grupurile : i) $(\mathbb{Q}, +)$ şi $(\mathbb{Q}^*, \cdot)$; ii) $(\mathbb{R}, +)$ şi $(\mathbb{R}^*, \cdot)$; iii) $(\mathbb{C}, +)$ şi $(\mathbb{C}^*, \cdot)$; iv) $(\mathbb{R}^*, \cdot)$ şi $(\mathbb{C}^*, \cdot)$ nu sunt izomorfe.

2.106. Un grup G în care fiecare element are ordin finit, adică $G = t(G)$, se numeşte *grup cu torsiune*. Să se dea exemplu de grup cu torsiune infinit.

2.107. Să se arate că $(\mathbb{Z}, +)$ este un grup ciclic şi că a orice grup ciclic infinit este izomorf cu $(\mathbb{Z}, +)$.

2.108. Fie $n \in \mathbb{Z}$ şi $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$. Să se arate că:
i) $n\mathbb{Z}$ este subgrup al lui $(\mathbb{Z}, +)$;
ii) $n\mathbb{Z} \subseteq m\mathbb{Z}$ dacă şi numai dacă $m|n$ (m divide pe n);
iii) pentru orice subgrup H al lui $(\mathbb{Z}, +)$ există un unic $n \in \mathbb{N}$ astfel încât $H = n\mathbb{Z}$;
iv) laticea subgrupurilor lui $(\mathbb{Z}, +)$ este antiizomorfă cu laticea $(\mathbb{N}, |)$;
v) $m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z}$ şi $m\mathbb{Z} + n\mathbb{Z} = (m, n)\mathbb{Z}$ (unde (m, n) şi $[m, n]$ sunt c.m.m.d.c., respectiv c.m.m.m.c. al lui m şi n);
vi) laticea congruenţelor lui $(\mathbb{Z}, +)$ este antiizomorfă cu laticea $(\mathbb{N}, |)$;
vii) laticea subgrupurilor şi laticea congruenţelor lui $(\mathbb{Z}, +)$ sunt latici distributive.

2.109. Să se arate că fiecare dintre grupurile $Hom(\mathbb{Q}, \mathbb{Z})$ şi $Hom(\mathbb{Z}_n, \mathbb{Z})$ ($n \in \mathbb{N}$, $n \geq 2$) este format dintr-un singur omomorfism.

2.110. Să se arate că grupul $(\mathbb{Z}, +)$ este izomorf cu orice subgrup al său diferit de $\{0\}$ şi că $(\mathbb{Z}, +)$ nu este izomorf cu $(\mathbb{Q}, +)$.

2.111. Fie $n \in \mathbb{N}^*$ şi $U_n = \{\varepsilon \mid \varepsilon^n = 1\}$. Să se arate că U_n este un subgrup ciclic al lui $(\mathbb{C}^*, \cdot)$ (numit *grupul rădăcinilor de ordinul* n *ale unităţii*) şi că orice grup ciclic de ordinul n este izomorf cu $(U_n, \cdot)$.

2.112. Să se arate că laticea subgrupurilor unui grup ciclic este distributivă.

2.113. Să se arate că mulţimea subgrupurilor unui grup infinit este infinită.

2.114. Să se determine grupurile care au: i) un singur subgrup; ii) două subgrupuri.

2.115. Care sunt grupurile în care pentru orice submulţime nevidă X subsemigrupul generat de X coincide cu subgrupul generat de X?

2.116. a) Să se determine grupurile cât ale lui $(\mathbb{Z},+)$ şi să se arate că acestea sunt ciclice.
b) Să se arate că orice grup ciclic este izomorf cu $(\mathbb{Z},+)$ sau cu un grup cât al lui $(\mathbb{Z},+)$.

2.117. Să se arate că produsul direct a două grupuri ciclice, fiecare de ordin cel puţin 2, este un grup ciclic dacă şi numai dacă grupurile sunt finite şi ordinele lor sunt relativ prime.

2.118. Fie $n \in \mathbb{N},\ n \geq 2$. Să se arate că produsul direct a n grupuri ciclice, fiecare de ordin cel puţin 2, este un grup ciclic dacă şi numai dacă grupurile sunt finite şi ordinele lor sunt două câte două relativ prime.

2.119. Să se arate că grupurile $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ şi $\mathbb{Z}_{n_1 n_2 \cdots n_k}$ sunt izomorfe dacă şi numai dacă numerele $n_1, n_2, \ldots, n_k$ sunt două câte două relativ prime.

2.120. Să se arate că produsul direct al unei familii infinite de grupuri ciclice, fiecare de ordin cel puţin 2, nu este un grup ciclic.

2.121. Să se arate că, abstracţie făcând de un izomorfism, există un singur grup neciclic de ordinul 4 (numit *grupul lui Klein).*

2.122. Să se determine toate grupurile neizomorfe de ordinele $1, 2, 3, 4$ şi 5.

2.123. Să se arate că dacă $f : \mathbb{Z} \to \mathbb{Z}$ este un endomorfism al grupului $(\mathbb{Z},+)$ atunci $f(x) = f(1) \cdot x$ pentru orice $x \in \mathbb{Z}$ (adică f este o translaţie a lui $(\mathbb{Z},\cdot)$) şi că orice translaţie a lui $(\mathbb{Z},\cdot)$ este un endomorfism al lui $(\mathbb{Z},+)$.

2.124. Să se arate că endomorfismele grupului $(\mathbb{Q},+)$ coincid cu translaţiile lui $(\mathbb{Q},\cdot)$.

2.125. Fie $(G,+)$ un grup abelian. Să se arate că grupul $(Hom(\mathbb{Z},G),+)$ este izomorf cu $(G,+)$.

2.126. Să se determine omomorfismele lui $(\mathbb{Z}_6,+)$ în $(\mathbb{Z}_3,+)$ şi ale lui $(\mathbb{Z}_3,+)$ în $(\mathbb{Z}_9,+)$.

2.127. Să se arate că grupurile $(Hom(\mathbb{Z}_m,\mathbb{Z}_n),+)$ şi $(\mathbb{Z}_{(m,n)},+)$ (unde (m,n) este c.m.m.d.c. al lui m şi n) sunt izomorfe.

2.128. Fie $(G,\cdot)$ un grup ciclic şi $G = \langle a \rangle$. Să se arate că un endomorfism $f : G \to G$ este automorfism dacă şi numai dacă $G = \langle f(a) \rangle$.

2.129. Să se arate că următoarele grupuri sunt izomorfe: i) $(Aut(\mathbb{Z},+),\circ)$ şi $(\mathbb{Z}_2,+)$; ii) $(Aut(\mathbb{Z}_5,+),\circ)$ şi $(\mathbb{Z}_4,+)$; iii) $(Aut(\mathbb{Z}_6,+),\circ)$ şi $(\mathbb{Z}_2,+)$.

2.130. Fie $(G,\cdot)$ un grup, H un subgrup, ρ_H relaţia de echivalenţă la stânga determinată de subgrupul H, fie S un sistem de reprezentanţi pentru mulţimea cât G/ρ_H, iar $f : G \to G$ funcţia definită prin $f(sh) = s$ (unde $s \in S,\ h \in H$). Să se arate că pentru orice $x \in G$ şi orice $h \in H$ au loc următoarele: i) $f(f(x)) = f(x)$; ii) $x^{-1}f(x) \in H$; iii) $f(xh) = f(x)$.

2.131. Fie $(G, \cdot)$ un grup, H un subgrup şi $f : G \to G$ o funcţie care verifică pentru orice $x \in G$ şi orice $h \in H$ condiţiile următoare: i) $f(f(x)) = f(x)$; ii) $x^{-1}f(x) \in H$; iii) $f(xh) = f(x)$. Să se arate că $f(G)$ este un sistem de reprezentanţi pentru mulţimea cât G/ρ_H.

2.132. Fie $(G, \cdot)$ un grup şi $\emptyset \neq A \subseteq G$. Să se arate că există un subgrup H al lui G astfel încât A să fie o clasă la stânga sau la dreapta a lui G în raport cu H dacă şi numai dacă $xy^{-1}z \in A$ pentru orice $x, y, z \in A$.

2.133. Fie $(G, \cdot)$ un grup şi H_1, H_2 subgrupuri ale lui G. Să se arate că:
i) $H_1 \cdot H_2$ este un subgrup dacă şi numai dacă $H_1 \cdot H_2 = H_2 \cdot H_1$;
ii) dacă $H_1 \cdot H_2$ este un subgrup atunci $\sup(H_1, H_2)$ în laticea subgrupurilor lui G este $H_1 \cdot H_2$;
iii) dacă $H_1 \trianglelefteq G$ şi $H_2 \trianglelefteq G$ atunci $H_1 \cdot H_2 \trianglelefteq G$.

2.134. Fie $(G, \cdot)$ un grup şi $X \subseteq G$. Să se arate că:
i) subgrupul $\langle X \rangle$ generat de X este comutativ dacă şi numai dacă pentru orice $x, y \in X$ avem $xy = yx$;
ii) dacă pentru orice $x \in X$ şi orice $g \in G$ avem $g^{-1}xg \in X$ atunci $\langle X \rangle \trianglelefteq G$;
iii) dacă $X = X_1 \cup X_2$ şi pentru orice $x_1 \in X_1$ şi $x_2 \in X_2$ avem $x_1x_2 = x_2x_1$ atunci $\langle X \rangle = \langle X_1 \rangle \cdot \langle X_2 \rangle$;
iv) dacă $X = X_1 \cup X_2$ şi $X_1X_2 = X_2X_1$ atunci $\langle X \rangle = \langle X_1 \rangle \cdot \langle X_2 \rangle$.

2.135. Fie $G = \mathbb{Z} \times \mathbb{Z} \times \{-1, 1\}$ şi $\cdot$ operaţia definită în G astfel:

$$(m_1, m_2, m_3) \cdot (n_1, n_2, n_3) = \begin{cases} (m_1 + n_1, m_2 + n_2, n_3), & \text{dacă } m_3 = 1\,; \\ (m_1 + n_1, m_2 + n_2, -n_3), & \text{dacă } m_3 = -1\,. \end{cases}$$

Să se arate că:
i) $(G, \cdot)$ este un grup;
ii) subgrupul $H_1 = \langle (1, 0, 1), (0, 1, 1) \rangle$ este normal în G;
iii) subgrupul $H_2 = \langle (1, 0, 1) \rangle$ este normal în H_1, dar nu este normal în G.

2.136. Să se determine:
i) ordinul fiecărui element din S_3;
ii) subgrupurile lui S_3 şi să se arate că laticea subgrupurilor lui S_3 este modulară, dar nu este distributivă;
iii) subgrupurile normale ale lui S_3;
iv) grupurile cât ale lui S_3.

2.137. Să se arate că laticea subgrupurilor grupului altern A_4 nu este modulară.

2.138. Fie $(G, \cdot)$ un grup, H, N subgrupuri în G şi $\rho_{H,N} \subseteq G \times G$ relaţia

$$x \rho_{H,N} y \Leftrightarrow \exists h \in H,\ \exists n \in N :\ y = hxn.$$

Să se arate că:
i) $\rho_{H,N}$ este o relaţie de echivalenţă pe G şi $G/\rho_{H,N} = \{HxN \mid x \in G\}$ (HxN se numeşte *clasa lui x după perechea de subgrupuri* (H, N));
ii) dacă $N \trianglelefteq G$ atunci $\rho_{H,N}$ coincide cu echivalenţa la stânga definită de HN.

2.139. Să se determine descompunerea lui S_3 în clase după perechea de subgrupuri (H, N), unde $H = N = \langle(1,2)\rangle$.

2.140. Un grup necomutativ care are toate subgrupurile normale se numeşte *grup hamiltonian.* Fie $(H, \cdot)$ grupul cuaternionilor (vezi problema **2.69**). Să se arate că:
i) $(H, \cdot)$ este grup hamiltonian;
ii) laticea subgrupurilor lui $(H, \cdot)$ este modulară, dar nu este distributivă;
iii) pentru orice $x, y \in H$ avem $x^2y^2 = y^2x^2$, deşi $(H, \cdot)$ nu este comutativ;
iv) dacă $a, b \in \{i, j, k\}$, $a \neq b$ atunci $H = \langle a, b\rangle$ şi $a^4 = 1 = b^4$, $a^2 = b^2$, $aba = a$ iar din aceste egalităţi să se deducă egalităţile: $aba = a$, $a^3b = ba$ şi $b^3a = ab$.

2.141. Să se arate că laticea subgrupurilor normale ale unui grup este modulară.

2.142. Fie $(G, \cdot)$ un grup necomutativ şi $Z(G)$ centrul său. Să se arate că grupul cât $(G/Z(G), \cdot)$ nu este ciclic.

2.143. Să se determine subgrupurile şi grupurile cât ale lui: a) $(\mathbb{Z}_{12}, +)$; b) $(\mathbb{Z}_{15}, +)$.

2.144. Fie U_6 muţimea rădăcinilor de ordinul 6 ale unităţii. Să se determine subgrupurile şi grupurile cât ale lui $(U_6, \cdot)$.

2.145. Fie $(G, \cdot)$ un grup. Să se arate că:
i) dacă toate elementele din $G \setminus \{1\}$ au ordinul 2 atunci G este abelian;
ii) dacă G este finit şi orice element din $G \setminus \{1\}$ are ordinul 2 atunci ordinul lui G este de forma 2^k, cu $k \in \mathbb{N}$.

2.146. Să se arate că orice grup de ordinul 6 este izomorf cu $(\mathbb{Z}_6, +)$ sau cu grupul simetric $(S_3, \circ)$.

2.147. Să se arate că rotaţiile şi simetriile unui triunghi echilateral formează un grup $(\Delta_3, \circ)$ izomorf cu grupul simetric $(S_3, \circ)$.

2.148. Fie P_n un poligon regulat cu n laturi ($n \in \mathbb{N}$, $n \geq 3$). Să se arate că izometriile f ale planului care au proprietatea că $f(P_n) = P_n$ formează un grup $(\Delta_n, \circ)$ (numit *grupul diedral de grad* n) şi că ordinul acestui grup este $2n$. (Amintim că o transformare geometrică f a planului se numeşte *izometrie* dacă păstrează distanţa dintre orice două puncte, adică pentru orice puncte M, N din plan avem $MN = f(M)f(N)$.)

2.149. Fie p un număr prim impar. Să se arate că orice grup de ordinul $2p$ este izomorf cu $(\mathbb{Z}_{2p}, +)$ sau cu grupul diedral $(\Delta_p, \circ)$.

2.150. Să se determine toate grupurile neizomorfe de ordinul 10.

2.151. Să se determine toate grupurile neizomorfe de ordinul 8.

2.152. Fie $(G_1, \cdot)$, $(G_2, *)$ două grupuri şi e_1, respectiv e_2 elementele lor neutre. Să se arate că grupurile cât $(G_1/G_1, \cdot)$ şi $(G_2/G_2, *)$ sunt izomorfe. Când sunt izomorfe grupurile $(G_1/\{e_1\}, \cdot)$ şi $(G_2/\{e_2\}, *)$?

2.153. Fie $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. Să se arate că $SL_n(K)$ este un subgrup normal al lui $(GL_n(K), \cdot)$ şi că grupul cât $(GL_n(K)/SL_n(K), \cdot)$ este izomorf cu $(K^*, \cdot)$. Ce se întâmplă pentru $K = \mathbb{Z}$?

2.154. Fie $U_2 = \{-1, 1\}$ grupul rădăcinilor de ordinul 2 ale unităţii. Să se arate că au loc următoarele izomorfisme de grupuri: a) $(\mathbb{C}/\mathbb{R}, +) \simeq (\mathbb{R}, +)$; b) $(\mathbb{Q}^*/U_2, \cdot) \simeq (\mathbb{Q}^*_+, \cdot)$; c) $(\mathbb{R}^*/U_2, \cdot) \simeq (\mathbb{R}^*_+, \cdot)$.

2.155. Fie $H = \{z \in \mathbb{C} \mid |z| = 1\}$. Să se arate că $H \trianglelefteq (\mathbb{C}^*, \cdot)$ şi că au loc izomorfismele: i) $(\mathbb{R}/\mathbb{Z}, +) \simeq (H, \cdot)$; ii) $(\mathbb{C}^*/H, \cdot) \simeq (\mathbb{R}^*_+, \cdot)$; iii) $(\mathbb{C}^*/\mathbb{R}^*_+, \cdot) \simeq (H, \cdot)$.

2.156. Să se arate că:
i) există o funcţie bijectivă între mulţimea suport a grupului cât $(\mathbb{Q}/\mathbb{Z}, +)$ şi mulţimea $A = \{x \in \mathbb{Q} \mid 0 \leq x < 1\}$;
ii) grupul $(\mathbb{Q}/\mathbb{Z}, +)$ este cu torsiune şi $t(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$;
iii) pentru orice $n \in \mathbb{N}^*$ grupul $(\mathbb{Q}/\mathbb{Z}, +)$ are un singur subgrup de ordin n, iar acest subgrup este ciclic.

2.157. Fie $U = \{z \in \mathbb{C} \mid \exists n \in \mathbb{N}^* :\ z^n = 1\}$. Să se arate că U este subgrup în $(\mathbb{C}^*, \cdot)$ şi că $(\mathbb{Q}/\mathbb{Z}, +) \simeq (U, \cdot)$.

2.158. Fie funcţiile

$$f_{a,b} : \mathbb{R} \to \mathbb{R},\ f_{a,b}(x) = ax + b\ (a, b \in \mathbb{R}),$$

$S_{\mathbb{R}}$ mulţimea permutărilor lui $\mathbb{R}$ şi

$$G = \{f_{a,b} \mid a \in \mathbb{R}^*,\ b \in \mathbb{R}\},\ H = \{f_{a,0} \mid a \in \mathbb{R}^*\},\ N = \{f_{1,b} \mid b \in \mathbb{R}\}.$$

i) Să se arate că $G \leq (S_{\mathbb{R}}, \circ)$. Este G subgrup normal în $S_{\mathbb{R}}$?
ii) Să se arate că $H \leq (G, \circ)$. Este H subgrup normal în G?
iii) Să se arate că $N \trianglelefteq (G, \circ)$ şi $(G/N, \circ) \simeq (\mathbb{R}^*, \cdot)$.
iv) Este N subgrup normal şi în $(S_{\mathbb{R}}, \circ)$?

2.159. Fie $(G, \cdot)$ un grup şi N un subgrup al său. Să se arate că dacă descompunerea lui G în raport cu N la stânga are un sistem de reprezentanţi H care este subgrup atunci:
i) H este un sistem de reprezentanţi şi pentru descompunerea la dreapta;
ii) $H \cap N = \{1\},\ HN = G = NH$;
iii) orice $g \in G$ are o reprezentare unică de forma $g = hn$ cu $h \in H$, $n \in N$;
iv) N este normal în G şi grupul $(G/N, \cdot)$ este izomorf cu $(H, \cdot)$.

2.160. Fie $K = \{e, (1, 2) \circ (3, 4), (1, 3) \circ (2, 4), (1, 4) \circ (2, 3)\}$, unde e este permutarea identică din S_4. Să se arate că:
a) submulţimea K formează un subgrup comutativ al lui S_4 izomorf cu grupul lui Klein;
b) K este un subgrup normal al lui S_4 şi $(S_4/K, \circ) \simeq (S_3, \circ)$;
c) $(A_4/K, \circ) \simeq (\mathbb{Z}_3, +)$.

2.161. Fie $(G, \cdot)$ un grup, H un subgrup al său, ρ_H relaţia de echivalenţă la stânga definită de H. Să se arate că:
i) pentru orice $a \in G$ funcţia $t_a : G/\rho_H \to G/\rho_H$, $t_a(xH) = axH$ este o permutate a lui G/ρ_H;
ii) funcţia $f : G \to S_{G/\rho_H}$, $f(a) = t_a$ este un omomorfism al lui G în grupul permutărilor mulţimii cât G/ρ_H;

iii) $\operatorname{Ker} f = \bigcap_{x \in G} xHx^{-1}$;
iv) dacă $H \trianglelefteq G$ atunci grupul translaţiilor stângi ale lui $(G/H, \cdot)$ este izomorf cu grupul $(G/H, \cdot)$.

2.162. Să se descompună grupurile S_3 şi S_4 în clase de elemente conjugate.

2.163. Fie $(G, \cdot)$ un grup, $x, y \in G$ şi $X, Y \subseteq G$. Să se arate că:
i) dacă x şi y sunt conjugate atunci x şi y au acelaşi ordin;
ii) dacă X şi Y sunt conjugate atunci X şi Y au acelaşi cardinal.

2.164. Să se arate că permutările

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 3 & 6 & 1 & 4 \end{pmatrix} \text{ şi } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 4 & 2 & 1 & 6 \end{pmatrix}$$

sunt conjugate în S_6 şi să se determine numărul permutărilor $\sigma \in S_6$ pentru care are loc egalitatea $\sigma^{-1} \circ \alpha \circ \sigma = \beta$.

2.165. Să se descompună grupul cuaternionilor în clase de elemente conjugate.

2.166. Fie matricele

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \ B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Să se determine normalizatorii acestor matrice în grupul $GL_2(\mathbb{R})$.

2.167. Fie $(G, \cdot)$ un grup. Se numeşte *acţiune a grupului* G *pe mulţimea* X o funcţie $G \times X \to X$, $(g, x) \mapsto gx$ pentru care avem

$$1x = x \text{ şi } (g_1 g_2)x = g_1(g_2 x), \ \forall x \in X, \ \forall g_1, g_2 \in G.$$

Să se arate că:
i) dacă H este un subgrup al grupului S_X al permutărilor lui X şi $f : G \to H$ este un omomorfism atunci funcţia $G \times X \to X$, $(g, x) \mapsto [f(g)](x)$ este o acţiune a lui G pe X. Să se deducă de aici că orice subgrup al lui S_X acţionează pe X;
ii) conjugarea în G determină o acţiune $G \times G \to G$ a lui G pe G definită prin $(g, x) \mapsto g^{-1}xg$.

2.168. Să se arate că dacă grupul $(G, \cdot)$ acţionează pe mulţimea X atunci relaţia $\sim$ definită pe X prin

$$x \sim x' \Leftrightarrow \exists g \in G : \ gx = x'$$

este o relaţie de echivalenţă pe mulţimea X. Clasa de echivalenţă O_x a lui x se numeşte *orbita* lui x.

2.169. Fie $(G, \cdot)$ un grup şi $x \in G$. Să se arate că orbita lui x în raport cu acţiunea lui G pe G definită de conjugarea în G coincide cu clasa de conjugare a lui x.

2.170. O *acţiune* a grupului G pe mulţimea X se numeşte *tranzitivă* dacă pentru orice $x, x' \in X$ există $g \in G$ astfel încât $gx = x'$. Să se arate că o acţiune este tranzitivă dacă şi numai dacă are o singură orbită.

2.171. Fie $(G, \cdot)$ un grup şi X o mulţime. Să se arate că:
i) dacă $G \times X \to X$, $(g, x) \mapsto gx$ este o acţiune a lui G pe X atunci, fixând pe g, funcţia $t_g : X \to X$, $t_g(x) = gx$ este bijectivă, iar $t : G \to S_X$, $t(g) = t_g$ este un omomorfism de grupuri;
ii) dacă $t : G \to S_X$ este un omomorfism de grupuri atunci $\alpha : G \times X \to X$, $\alpha(g, x) = [t(g)](x)$ este o acţiune a lui G pe X;
iii) corespondenţa $t \mapsto \alpha$ este o bijecţie între mulţimea omomorfismelor lui $(G, \cdot)$ în $(S_X, \circ)$ şi mulţimea acţiunilor lui G pe X.

2.172. Fie $G \times X \to X$, $(g, x) \mapsto gx$ o acţiune a grupului $(G, \cdot)$ pe mulţimea X, fie $x \in X$ şi $F_x = \{g \in G \mid gx = x\}$. Să se arate că:
i) F_x este un subgrup al lui G numit *stabilizatorul* lui x;
ii) cardinalul orbitei lui x coincide cu indicele lui F_x în G;
iii) dacă $X = G$ şi acţiunea este definită de conjugare atunci F_x coincide cu normalizatorul lui x;
iv) cardinalul clasei de conjugare a unui element $g \in G$ coincide cu indicele normalizatorului lui g în G.

2.173. Dacă grupul $(G, \cdot)$ acţionează pe X atunci orice subgrup al lui G acţionează pe X. Să se arate că dacă G acţionează tranzitiv pe X şi F este stabilizatorul unui $x_0 \in X$ atunci există o bijecţie între mulţimea orbitelor acţiunii lui F pe X şi mulţimea $\{FgF \mid g \in G\}$ a claselor lui G după (F, F).

2.174. Fie $(G, \cdot)$ un grup, $G \times X \to X$, $(g, x) \mapsto gx$ o acţiune a lui G pe mulţimea X şi $F = \{g \in G \mid gx = g,\ \forall x \in X\}$. Să se arate că $F \trianglelefteq G$ şi că:
i) există o singură acţiune a grupului $(G/F, \cdot)$ pe X astfel încât $(gF)x = gx$;
ii) funcţia $t_{gF} : X \to X$, $t_{gF}(x) = (gF)x$ este o permutare a lui X şi funcţia $\varphi : G/F \to S_X$, $\varphi(gF) = t_{gF}$ este un omomorfism injectiv de grupuri.

2.175. Fie $(G, \cdot)$ un grup finit de ordinul n şi $x \in G$. Să se arate că:
i) numărul elementelor conjugate cu x este un divizor al lui n;
ii) dacă m este ordinul lui x atunci numărul elementelor conjugate cu x este un divizor al lui $\dfrac{n}{m}$;
iii) dacă m' este ordinul centrului lui G atunci numărul elementelor conjugate cu x este un divizor al lui $\dfrac{n}{m'}$;
iv) dacă $l \in \mathbb{N}$ atunci numărul elementelor conjugate cu x^l este un divizor al numărului elementelor conjugate cu x.

2.176. În $G = \mathbb{Z} \times \mathbb{Z}$ se defineşte operaţia $\cdot$ prin

$$(m_1, n_1) \cdot (m_2, n_2) = (m_1 + m_2, (-1)^{m_2} n_1 + n_2).$$

Să se arate că $(G, \cdot)$ este un grup şi să se determine pentru fiecare element (m, n) numărul elementelor conjugate cu (m, n).

2.177. Să se determine toate grupurile neizomorfe care au numai două clase de elemente conjugate.

2.178. Fie K_1, K_2, K_3 clase de elemente conjugate în grupul $(G, \cdot)$. Să se arate că:
i) $K_1 \cap K_2K_3 \neq \emptyset \Rightarrow K_1 \subseteq K_2K_3$:
ii) dacă G este finit, $K_1 = K_2K_3$ şi k_i este numărul elementelor din K_i $(i = 1, 2, 3)$ atunci k_1 divide pe k_2k_3.

2.179. Fie $(G, \cdot)$ un grup finit, H_1, H_2 subgrupuri ale lui G şi $x \in G$. Dacă $n_1 = |H_1|$, $n_2 = |H_2|$ şi $m = |H_2 \cap x^{-1}H_1x|$ atunci numărul elementelor clasei H_1xH_2 a lui x în raport cu (H_1, H_2) este $\dfrac{n_1n_2}{m}$.

2.180. Să se arate că centrul unui grup $(G, \cdot)$ al cărui ordin este de forma p^k, cu p prim şi $k \in \mathbb{N}^*$, este diferit de $\{1\}$.

2.181. Să se arate că pentru orice număr prim p există numai două grupuri neizomorfe de ordinul p^2.

2.182. Să se determine toate grupurile neizomorfe de ordinul 9.

2.183. Să se determine grupurile care au trei subgrupuri.

2.184. Fie $(G, \cdot)$ un grup necomutativ de ordinul p^3 cu p număr prim. Să se arate că $|Z(G)| = p$ şi că grupul cât $G/Z(G)$ este izomorf cu $\mathbb{Z}_p \times \mathbb{Z}_p$.

2.185. Fie $(G, \cdot)$ un grup abelian, p un număr prim şi

$$G_p = \{g \in G \mid \operatorname{ord} g = p^k,\ k \in \mathbb{N}\}.$$

Să se arate că G_p este un subgrup deplin invariant al lui G.

2.186. Fie $(A, +)$ un grup abelian, B un subgrup al său, $n \in \mathbb{N}^*$ şi

$$nB = \{nb \mid b \in B\},\ B[n] = \{b \in B \mid nb = 0\}.$$

Să se arate că:
i) nB şi $B[n]$ sunt subgrupuri ale lui A;
ii) dacă B este un subgrup caracteristic atunci nB şi $B[n]$ sunt subgrupuri caracteristice;
iii) dacă B este un subgrup deplin invariant atunci nB şi $B[n]$ sunt subgrupuri deplin invariante.

2.187. Fie $(G, \cdot)$ un grup şi H un subgrup al său. Să se arate că:
i) dacă H este deplin invariant în G şi f este un endomorfism al lui G atunci funcţia $\overline{f} : G/H \to G/H$, $\overline{f}(gH) = f(g)H$ este un endomorfism al lui G/H;
ii) dacă H este deplin invariant în G şi H' este un subgrup al lui G astfel încât $H \subseteq H'$ şi H'/H să fie deplin invariant în G/H atunci H' este subgrup deplin invariant în G.

2.188. Fie $(G, \cdot)$ un grup. Să se arate că:
i) mulţimea subgrupurilor caracteristice ale lui G formează o sublatice completă a laticii subgrupurilor normale ale lui G;
ii) mulţimea subgrupurilor deplin invariante ale lui G formează o sublatice completă a laticii subgrupurilor caracteristice ale lui G.

2.189. Fie $(G, \cdot)$ un grup şi $X \subseteq G$. Să se arate că:
i) subgrupul lui G generat de $\bigcup\{f(X) \mid f \in Aut(G, \cdot)\}$ este cel mai mic subgrup caracteristic al lui lui G ce include pe X;
i) subgrupul lui G generat de $\bigcup\{f(X) \mid f \in End(G, \cdot)\}$ este cel mai mic subgrup deplin invariant al lui lui G ce include pe X.

2.190. Fie $(G, \cdot)$ un grup, $X \subseteq G$ şi H un subgrup caracteristic (deplin invariant) al lui G astfel încât $X \cap H = \emptyset$. Să se arate că există un subgrup caracteristic (deplin invariant) H' al lui G astfel ca:
i) $H \subseteq H'$;
ii) $X \cap H' = \emptyset$;
iii) dacă H'' este un subgrup caracteristic (deplin invariant) al lui G astfel încât $H' \subseteq H''$ atunci $X \cap H'' \neq \emptyset$.

2.191. Fie $(G, \cdot)$ un grup. Un element $a \in A$ se numeşte *nongenerator* al lui G dacă pentru orice $X \subseteq G$, $\langle X \cup \{a\}\rangle = G$ implică $\langle X\rangle = G$. Un *subgrup* M al lui G se numeşte *maximal* dacă $M \neq G$ şi pentru orice subgrup H, din $M \subseteq H$ deducem $H = M$ sau $H = G$. Să se arate că:
a) mulţimea $F(G)$ a nongeneratorilor lui G formează un subgrup caracteristic al lui G, numit *subgrupul lui Frattini*;
b) $F(G)$ coincide cu intersecţia tuturor subgrupurilor maximale ale lui G (dacă nu există subgrupuri maximale atunci această intersecţie este G).

2.192. Să se arate că subgrupoidul Frattini al unui grup nu coincide, în general, cu subgrupul Frattini al acestuia.

2.193. Fie matricele

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},\ B = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix},\ C = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$$

din grupul $GL_n(\mathbb{Z})$. Să se determine comutatorii $[A, B]$, $[B, C]$, $[C, A]$.

2.194. Fie $(G, \cdot)$ un grup, $Z(G)$ centrul său şi G' subgrupul său derivat. Să se arate că:
i) pentru orice $x, y \in G$ au loc egalităţile:

$$xy = yx[x, y],\ [x, y]^{-1} = [y, x],\ [x, y^{-1}] = y[y, x]y^{-1},\ [x^{-1}, y] = x[y, x]x^{-1},$$
$$[xy, z] = y^{-1}[x, z]y[y, z],\ [x, yz] = [x, z]z^{-1}[x, y]z;$$

ii) dacă $x, y \in G$ atunci $[x, y] = 1$ dacă şi numai dacă $xy = yx$;
iii) $x \in Z(G) \Leftrightarrow \forall y \in G,\ [x, y] = 1$;
iv) G este abelian dacă şi numai dacă $G' = \{1\}$.

2.195. Fie $(G, \cdot)$ un grup. Să se arate că dacă $G' \subseteq Z(G)$ atunci pentru orice $x, y, z \in G$ şi orice $n \in \mathbb{Z}$ avem

$$[x, [y, z]] = [[x, y], z],\ [xy, z] = [x, z] \cdot [y, z],\ [x, yz] = [x, y] \cdot [x, z],$$
$$[x^n, y] = [x, y^n] = [x, y]^n,\ (x \cdot y)^n = x^n y^n [y, x]^{\frac{n(n-1)}{2}},$$
$$[x, [y, z]] \cdot [y, [z, x]] \cdot [z, [x, y]] = 1.$$

2.196. Să se demonstreze că

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \ a, b, c \in \mathbb{Z} \right\}$$

este un subgrup al lui $GL_3(\mathbb{Z})$ şi că subgrupul comutator al lui G coincide cu centrul lui G.

2.197. Fie $(G, \cdot)$ un grup şi N un subgrup al lui G. Să se arate că N este normal în G dacă şi numai dacă $[N, G] \subseteq N$.

2.198. Fie $(G, \cdot)$ un grup şi N_1, N_2 subgrupuri normale ale lui G. Să se arate că

$$[N_1, N_2] \subseteq N_1 \cap N_2.$$

2.199. Fie G un grup, X un sistem de generatori al lui G şi $N \trianglelefteq G$. Să se arate că dacă $[x, y] \in N$ pentru orice $x, y \in X$ atunci $G' \subseteq N$.

2.200. Să se determine subgrupul derivat al grupului cuaternionilor.

2.201. Să se determine subgrupul derivat al grupului simetric $(S_3, \circ)$.

2.202. Să se determine subgrupul derivat al grupului simetric $(S_n, \circ)$.

2.203. Fie $(G, \cdot)$ un grup finit şi H un p-subgrup al său. Să se arate că dacă H nu este un p-subgrup Sylow atunci H este un subgrup propriu al normalizatorului său în G.

2.204. Fie G un grup finit, P un p-subgrup Sylow al lui G şi $N_G(P)$ normalizatorul lui P în G. Să se arate că dacă H şi H' sunt subgrupuri ale lui G astfel încât $N_G(P) \subseteq H \subseteq H'$ atunci $N_G(H) = H$ şi $|H' : H| \equiv 1 \pmod{p}$.

2.205. Să se determine subgrupurile Sylow ale grupului simetric $(S_4, \circ)$.

2.206. Să se determine toate grupurile neizomorfe de ordinul 15.

2.207. Fie p, q numere prime. Să se arate dacă $(G, \cdot)$ este un grup de ordinul pq atunci G nu este simplu. Mai mult, dacă $p \neq q$, $p - 1$ nu se divide prin q şi $q - 1$ nu se divide prin p atunci $(G, \cdot)$ este izomorf cu $(\mathbb{Z}_{pq}, +)$.

2.208. Fie p, q numere prime, $p \neq q$. Să se arate dacă $(G, \cdot)$ este un grup de ordinul p^2q atunci G nu este simplu. Mai mult, dacă $p^2 - 1$ nu se divide prin q şi $q - 1$ nu se divide prin p atunci G este abelian.

2.209. Arătaţi că orice grup de ordinul 255 este ciclic.

2.210. Fie $(G, \cdot)$ un grup şi H, H' subgrupuri ale lui $(G, \cdot)$ cu proprietatea că

$$hh' = h'h, \ \forall h \in H, \ \forall h' \in H'.$$

Să se arate că:
i) există un unic omomorfism $f : H \times H' \to G$ astfel încât

$$f(h, 1) = h \text{ şi } f(1, h') = h', \ \forall h \in H, \ \forall h' \in H';$$

ii) f este injectiv dacă şi numai dacă $H \cap H' = \{1\}$;
iii) f este surjectiv dacă şi numai dacă $\langle H \cup H' \rangle = G$.

2.211. Fie $(G, \cdot)$ un grup, X o mulţime şi $(G^X, \cdot)$ grupul din problema **2.55**. Să se arate că G^X este produsul direct al familiei de grupuri $(G_x, \cdot) = (G, \cdot)$, $x \in X$.

2.212. Fie $(G_i, \cdot)$, $i \in I$ o familie de grupuri, $(P, \cdot)$ produsul direct al acestei familii, $(p_i)_{i \in I}$ familia proiecţiilor canonice şi $(P', \cdot)$ produsul restrâns al familiei $(G_i, \cdot)$, $i \in I$. Să se arate că dacă X_i este un sistem de generatori pentru $(G_i, \cdot)$, $i \in I$, atunci $X = \bigcup \{p_i(X_i) \mid i \in I\}$ este un sistem de generatori pentru $(P', \cdot)$. În ce caz X este un sistem de generatori şi pentru $(P, \cdot)$?

2.213. a) Să se determine un sistem de generatori X pentru grupul $(\mathbb{Z} \times \mathbb{Z}, +)$ cu următoarele proprietăţi:
i) cardinalul lui X este 2;
ii) pentru orice grup abelian $(A, +)$ şi orice funcţie $f : X \to A$ există un omomorfism unic $\overline{f} : \mathbb{Z} \times \mathbb{Z} \to A$ care extinde pe f (adică $f = \overline{f} \circ i$, unde $i : X \to \mathbb{Z} \times \mathbb{Z}$ este funcţia de incluziune).
b) Să se generalizeze punctul a).

2.214. Pentru un grup abelian cu torsiune $(A, +)$ şi un număr prim p, subgrupul $A_p = \{a \in A \mid \exists k \in \mathbb{N} : \ p^k a = 0\}$ se numeşte *p-componenta primară* a lui A. Să se arate că A este izomorf cu suma directă a componentelor sale primare, adică

$$A \simeq \bigoplus_{p \in \mathbb{P}} A_p$$

(unde cu $\mathbb{P}$ am notat mulţimea numerelor prime).

2.215. Fie p un număr prim şi $\mathbb{Z}_{p^\infty} = \{z \in \mathbb{C} \mid \exists k \in \mathbb{N} : \ z^{p^k} = 1\}$. Să se arate că $\mathbb{Z}_{p^\infty}$ este un subgrup al lui $(\mathbb{C}^*, \cdot)$ şi că are loc izomorfismul

$$(\mathbb{Q}/\mathbb{Z}, +) \simeq \bigoplus_{p \in \mathbb{P}} (\mathbb{Z}_{p^\infty}, \cdot).$$

2.216. Să se determine toate grupurile abeliene neizomorfe de ordinul 32.

2.217. Să se determine toate grupurile abeliene neizomorfe de ordinul 64.

2.218. Să se determine toate grupurile abeliene neizomorfe de ordinul 96.

2.219. Să se arate că grupul $(\mathbb{Z}, +)$ nu are şiruri de compoziţie.

2.220. Să se arate că un grup abelian $(A, +)$ are şiruri de compoziţie dacă şi numai dacă A este finit.

2.221. Să se determine toate şirurile de compoziţie ale grupului $(\mathbb{Z}_6 \times \mathbb{Z}_5, +)$.

2.222. Fie $(A, +)$ un grup abelian finit de ordinul $n = p_1 \cdots p_k$, cu $p_1, \ldots, p_k$ numere prime diferite. Să se determine toate şirurile de compoziţie ale lui A.

2.223. Să se arate că un grup $(G, \cdot)$ este nilpotent de clasă 1 dacă şi numai dacă G este abelian şi $G \neq \{1\}$.

2.224. Să se arate că dacă $(G, \cdot)$ este un grup nilpotent de clasă cel mult 2 atunci, pentru orice $x, y, z \in G$ avem $[xy, z] = [x, z] \cdot [y, z]$ şi $[x, yz] = [x, y] \cdot [x, z]$.

2.225. Să se arate că grupul cuaternionilor este nilpotent de clasă 2.

2.226. Să se determine $n \in \mathbb{N}^*$ pentru care grupul simetric $(S_n, \circ)$ este nilpotent.

2.227. Să se arate că grupul simetric $(S_n, \circ)$ este resolubil pentru $n \leq 4$.

2.228. Să se arate că orice grup de ordinul $2p$, cu p prim, este resolubil.

2.229. Fie p şi q două numere prime, nu neapărat diferite. Să se arate că orice grup de ordinul pq este resolubil.

Capitolul 3

Inele şi corpuri

3.1. Fie $\perp$ şi $\top$ operaţiile definite pe $\mathbb{Z}$ astfel:

$$x \perp y = x + y + 3; \; x \top y = xy + 3x + 3y + 6.$$

Să se arate că $(\mathbb{Z}, \perp, \top)$ este domeniu de integritate şi să se determine elementele inversabile din acest domeniu.

3.2. Fie $*$ operaţia definită pe $\mathbb{C}$ astfel:

$$(a_1 + b_1 i) * (a_2 + b_2 i) = a_1 a_2 + (a_1 b_2 + a_2 b_1) i \quad (a_1, a_2, b_1, b_2 \in \mathbb{R}).$$

Să se arate că $(\mathbb{C}, +, *)$ este un inel asociativ, comutativ, cu unitate care are divizori ai lui zero.

3.3. Fie $+$ şi $\top$ operaţiile definite pe $\mathbb{Q} \times \mathbb{Q}$ astfel:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$
$$(a_1, b_1) \top (a_2, b_2) = (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1 + b_1 b_2).$$

Să se arate că $(\mathbb{Q} \times \mathbb{Q}, +, \top)$ este un corp comutativ.

3.4. Fie M o mulţime şi $\mathcal{P}(M)$ mulţimea submulţimilor lui M. Definim pe $\mathcal{P}(M)$ două operaţii $+$ şi $\cdot$ astfel:

$$X + Y = (X \setminus Y) \cup (Y \setminus X) \text{ şi } X \cdot Y = X \cap Y.$$

Să se arate că:
i) $(\mathcal{P}(M), +, \cdot)$ este inel asociativ, comutativ, cu unitate;
ii) dacă $|M| \geq 2$ atunci orice $X \in \mathcal{P}(M) \setminus \{\emptyset, M\}$ este divizor al lui zero;
iii) $(\mathcal{P}(M), +, \cdot)$ este corp dacă şi numai dacă $|M| = 1$.

3.5. Să se arate că într-un inel cu unitate, comutativitatea adunării este o consecinţă a celorlalte axiome.

3.6. Să se dea exemplu de inel finit necomutativ.

3.7. Fie $(R,+,\cdot)$ un inel asociativ şi $a,b\in R$. Să se arate că:
a) $(a+b)^2=a^2+2ab+b^2 \Leftrightarrow ab=ba \Leftrightarrow a^2-b^2=(a-b)(a+b)$;
b) dacă $ab=ba$ atunci pentru orice $n\in\mathbb{N}^*$ avem

$$\begin{aligned}(a+b)^n =&C_n^0a^n+C_n^1a^{n-1}b+\cdots+C_n^{n-1}ab^{n-1}+C_n^nb^n;\\ a^n-b^n =&(a-b)\left(a^{n-1}+a^{n-2}b+\cdots+ab^{n-2}+b^{n-1}\right);\\ a^{2n+1}+b^{2n+1} =& (a+b)\left(a^{2n}-a^{2n-1}b+\cdots-ab^{2n-1}+b^{2n}\right).\end{aligned}$$

3.8. Fie $(R,+,\cdot)$ un inel asociativ cu unitate şi $n\in\mathbb{N}$. Dacă $(xy)^k=x^ky^k$ pentru orice $x,y\in R$ şi $k\in\{n,n+1,n+2\}$ atunci inelul R este comutativ.

3.9. Să se arate că dacă într-un inel asociativ cu unitate $(R,+,\cdot)$ avem $x^3=x$ pentru orice $x\in\mathbb{R}$ atunci inelul R este comutativ.

3.10. Să se arate că dacă într-un inel asociativ $(R,+,\cdot)$ avem $x^6=x$ pentru orice $x\in\mathbb{R}$ atunci $x^2=x$ pentru orice $x\in\mathbb{R}$.

3.11. Fie $(R,+,\cdot)$ un inel asociativ. Să se arate că următoarele condiţii sunt echivalente:
i) $a\in R,\ a^2=0\ \Rightarrow\ a=0$;
ii) $a\in R,\ n\in\mathbb{N}^*,\ a^n=0\ \Rightarrow\ a=0$.

3.12. Să se arate că într-un inel cu unitate $(R,+,\cdot)$ orice element idempotent diferit de 0 şi 1 este un divizor al lui zero.

3.13. Fie $(R,+,\cdot)$ un inel asociativ, comutativ, cu unitate, cu $R\neq\{0\}$. Să se calculeze produsul tuturor elementelor idempotente nenule ale lui R.

3.14. Fie $(R,+,\cdot)$ un inel. Un element $a\in R$ se numeşte *central* dacă $ax=xa$ pentru orice $x\in R$ (adică a aparţine centrului inelului R). Să se arate că dacă R nu are elemente nilpotente nenule atunci orice element idempotent este central.

3.15. Fie $n\in\mathbb{N}^*\setminus\{1\}$ şi $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ (cu $p_1,\ldots,p_k$ numere prime distincte şi $\alpha_1,\ldots,\alpha_k\in\mathbb{N}^*$) descompunerea lui n în factori primi. Să se arate că:
a) $\widehat{a}$ este nilpotent în $(\mathbb{Z}_n,+,\cdot)$ dacă şi numai dacă $p_1\cdots p_k|a$;
b) inelul $(\mathbb{Z}_n,+,\cdot)$ are elemente nilpotente nenule dacă şi numai dacă există un număr prim p astfel încât $p^2|n$.

3.16. Fie $n\in\mathbb{N}^*\setminus\{1\}$. Să se determine elementele idempotente ale lui $(\mathbb{Z}_n,+,\cdot)$.

3.17. Fie $R=\{0,1,a,b\}$ un inel asociativ în care 0 este elementul nul şi 1 elementul unitate. Să se arate că:
i) funcţia $f:R\to R,\ f(x)=1+x$ este bijectivă;
ii) $\displaystyle\sum_{x\in R}f(x)=1+a+b$ şi $1+1+1+1=0$;
iii) dacă R este corp atunci $1+1=0$;
iv) R este corp dacă şi numai dacă există $x\in R$ astfel încât $1+x=x^2$.

3.18. Un inel asociativ $(R,+,\cdot)$ se numeşte *inel Boole* dacă orice element din R este idempotent (adică $x^2=x$ pentru orice $x\in R$). Fie $(R,+,\cdot)$ un inel Boole. Să se arate că:
i) $x+x=0$ pentru orice $x\in R$;
ii) $(R,+,\cdot)$ este un inel comutativ;
iii) R nu conţine divizori ai lui zero dacă şi numai dacă $R=\{0\}$ sau $|R|=2$;
iv) $(R,+,\cdot)$ este corp dacă şi numai dacă este cu unitate şi $|R|=2$.

3.19. i) Fie $(R,\vee,\wedge)$ o latice Boole (adică o latice distributivă, cu cel mai mic element 0, cel mai mare element 1, în care fiecare element x are un complement x'). Să se arate că operaţiile $+$ şi $\cdot$ definite pe R astfel:

$$x+y=(x\wedge y')\vee(x'\wedge y),\ xy=x\wedge y$$

înzestrează pe R cu o structură de inel Boole cu unitate în care 0 este elementul nul şi 1 este elementul unitate.
ii) Fie $(R,+,\cdot)$ un inel Boole cu unitate. Să se arate că operaţiile $\vee$ şi $\wedge$ definite pe R astfel:

$$x\vee y=x+y-xy,\ x\wedge y=xy$$

înzestrează pe R cu o structură de latice Boole în care 0 este cel mai mic element, 1 este cel mai mare element şi $x'=1-x$.
iii) Notând cu $f(R,\vee,\wedge)$, respectiv $g(R,+,\cdot)$, inelul introdus la i), respectiv laticea introdusă la ii), avem

$$g(f(R,\vee,\wedge))=(R,\vee,\wedge)\text{ şi }f(g(R,+,\cdot))=(R,+,\cdot),$$

adică f realizează o bijecţie între clasa laticelor Boole şi clasa inelelor Boole, iar $f^{-1}=g$.

3.20. Fie $(R,+,\cdot)$ un inel asociativ finit, cu unitate şi $a\in R$, $a\neq 0$. Să se arate că a este inversabil dacă şi numai dacă a nu este divizor al lui zero.

3.21. Să se arate că orice domeniu de integritate finit este corp.

3.22. Fie $(R,+,\cdot)$ un inel asociativ, cu unitate. Dacă un element $a\in R$ are mai mult decât un invers la stânga atunci inelul R este infinit şi a are o infinitate de inverse la stânga.

3.23. Să se rezolve în $\mathbb{Z}_{12}$ ecuaţiile $\widehat{4}x+\widehat{5}=\widehat{9}$ şi $\widehat{5}x+\widehat{5}=\widehat{9}$ şi în $M_2(\mathbb{C})$ ecuaţia $\begin{pmatrix}1&2\\1&2\end{pmatrix}X=\begin{pmatrix}1&2\\1&2\end{pmatrix}$.

3.24. În $\mathbb{Z}_{12}$, să se determine divizorii lui zero şi să se rezolve sistemul:

$$\begin{cases}\widehat{3}x+\widehat{4}y=\widehat{11}\\ \widehat{4}x+\widehat{9}y=\widehat{10}\end{cases}.$$

3.25. Să se dea exemple de părţi stabile ale mulţimii $\mathbb{R}$ în raport cu $+$ şi $\cdot$ care nu sunt inele în raport cu operaţiile induse de $+$ şi $\cdot$, respectiv de părţi stabile ale mulţimii $\mathbb{C}$ în raport cu $+$ şi $\cdot$ care sunt corpuri sau inele în raport cu operaţiile induse de $+$ şi $\cdot$. Folosind definiţia subinelului şi a subcorpului, să se precizeze care din exemplele date sunt subinele sau subcorpuri ale lui $(\mathbb{C},+,\cdot)$.

3.26. Să se dea exemplu de subinel al unui inel cu unitate care nu conţine unitatea şi de subinel al unui corp care nu este subcorp.

3.27. Să se dea exemplu de subinel S al unui inel cu unitate $(R, +, \cdot)$ care este, în raport cu operaţiile induse, un inel cu unitate, dar unitatea sa este diferită de unitatea lui R.

3.28. Fie $(K, +, \cdot)$ un corp comutativ. Să se arate că orice subinel al lui K care conţine unitatea este domeniu de integritate.

3.29. Să se arate că

$$R = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$$

este o parte stabilă a lui $M_2(\mathbb{Z})$ în raport cu adunarea şi înmulţirea matricelor şi că R este un domeniu de integritate în raport cu operaţiile induse.

3.30. Să se arate că mulţimea

$$K = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$$

este stabilă în raport cu adunarea şi înmulţirea din $M_2(\mathbb{Q})$ şi că formează corp comutativ în raport cu operaţiile induse.

3.31. Fie $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ şi $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, adică

$$\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z} \cdot \sqrt{2} \text{ şi } \mathbb{Q}(\sqrt{2}) = \mathbb{Q} + \mathbb{Q} \cdot \sqrt{2}.$$

Să se arate că:
i) $\mathbb{Z}[\sqrt{2}]$ este un subinel al lui $(\mathbb{R}, +, \cdot)$ care conţine pe 1 şi acest subinel este generat de $\{1, \sqrt{2}\}$;
ii) $\mathbb{Q}(\sqrt{2})$ este un subcorp al lui $(\mathbb{R}, +, \cdot)$ şi acest subcorp este generat de $\sqrt{2}$;
iii) $S_1 = \{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Z}\}$ nu este subinel al lui $(\mathbb{R}, +, \cdot)$;
iv) $S_2 = \{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\}$ nu este subcorp al lui $(\mathbb{R}, +, \cdot)$.

3.32. Un număr $d \in \mathbb{Z}$ se numeşte *întreg liber de pătrate* dacă $d \neq 1$ şi d nu se divide prin pătratul nici unui număr prim. Fie d un întreg liber de pătrate. Să se arate că:
i) $\sqrt{d} \notin \mathbb{Q}$;
ii) $a, b \in \mathbb{Q}$ şi $a + b\sqrt{d} = 0$ implică $a = b = 0$;
iii) $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ este un subinel în $(\mathbb{C}, +, \cdot)$ care conţine pe 1 şi acest subinel este generat de $\{1, \sqrt{d}\}$;
iv) $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ este un subcorp al lui $(\mathbb{R}, +, \cdot)$ şi acest subcorp este generat de $\sqrt{d}$.

3.33. Fie $d \in \mathbb{Z}$ un întreg liber de pătrate şi funcţia

$$\delta : \mathbb{Z}[\sqrt{d}] \to \mathbb{N}, \ \delta(z) = |z \cdot \overline{z}|,$$

unde cu $\overline{z} = a - b\sqrt{d}$ s-a notat conjugatul lui $z = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{2}]$. Să se arate că z este inversabil în $\mathbb{Z}[\sqrt{d}]$ dacă şi numai dacă $\delta(z) = 1$.

3.34. Să se determine elementele inversabile ale inelului întregilor lui Gauss

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

3.35. Să se arate că inelul $\mathbb{Z}[\sqrt{2}]$ are o infinitate de elemente inversabile.

3.36. Fie $p, q \in \mathbb{Z}$ şi $\theta \in \mathbb{C}$ o soluţie a ecuaţiei

$$(*) \qquad x^2 + px + q = 0.$$

Să se arate că:
a) $\mathbb{Z}[\theta] = \{a + b\theta \mid a, b \in \mathbb{Z}\}$ este subinelul lui $\mathbb{C}$ generat de $\{1, \theta\}$;
b) $\mathbb{Q}(\theta) = \{a + b\theta \mid a, b \in \mathbb{Q}\}$ este subcorpul lui $\mathbb{C}$ generat de θ;
c) dacă $\theta' \in \mathbb{C}$ e cealaltă soluţie a ecuaţiei $(*)$ atunci $\mathbb{Z}[\theta] = \mathbb{Z}[\theta']$ şi $\mathbb{Q}(\theta) = \mathbb{Q}(\theta')$;
d) dacă $z = a + b\theta \in \mathbb{Q}(\theta)$ $\left(a, b \in \mathbb{Q},\ \theta = \dfrac{-p + \sqrt{p^2 - 4q}}{2}\right)$ atunci

$$z = \left(a - \frac{p}{2}b\right) + \sqrt{p^2 - 4q}\,\frac{b}{2},$$

iar dacă $\overline{z} = \left(a - \dfrac{p}{2}b\right) - \sqrt{p^2 - 4q}\,\dfrac{b}{2}$ este conjugatul lui z atunci $\overline{z} = a + b\theta'$;
e) funcţia $\delta : \mathbb{Z}[\theta] \to \mathbb{N}$, $\delta(z) = |z \cdot \overline{z}|$ are următoarele proprietăţi:
i) $\delta(z_1 z_2) = \delta(z_1)\delta(z_2)$ pentru orice $z_1, z_2 \in \mathbb{Z}[\theta]$;
ii) $\delta(z) = 0$ $(z \in \mathbb{Z}[\theta])$ dacă şi numai dacă $z = 0$;
iii) dacă $p^2 - 4q$ nu este pătrat perfect atunci

$$\delta(a + b\theta) = 0 \ (a, b \in \mathbb{Z}) \Leftrightarrow a = b = 0;$$

iv) $z \in \mathbb{Z}[\theta]$ este inversabil în $\mathbb{Z}[\theta]$ dacă şi numai dacă $\delta(z) = 1$;
f) afirmaţiile i), ii) şi iii) de la e) sunt adevărate şi pentru funcţia

$$\delta_0 : \mathbb{Q}(\theta) \to \mathbb{Q},\ \delta_0(z) = |z \cdot \overline{z}|.$$

3.37. Determinaţi subinelele lui $(\mathbb{Q}, +, \cdot)$ ce conţin pe 1.

3.38. Să se determine subinelul şi subcorpul lui $(\mathbb{R}, +, \cdot)$ generat de $\{1, \sqrt[3]{2}\}$.

3.39. Să se determine:
i) cea mai mică submulţime a lui $\mathbb{R}$ stabilă în raport cu $+$ şi $\cdot$ ce conţine pe 1;
ii) cel mai mic subinel al lui $(\mathbb{R}, +, \cdot)$ care conţine pe 1;
iii) cel mai mic subcorp al lui $(\mathbb{R}, +, \cdot)$.

3.40. Fie $a, b, c \in \mathbb{R}$ şi

$$x \perp y = ax + by - 2;\ x \top y = xy - 2x - 2y + c,\ \forall x, y \in \mathbb{R}.$$

i) Să se determine a, b, c astfel încât $(\mathbb{R}, \perp, \top)$ să fie corp;
ii) Să se determine apoi $\alpha, \beta \in \mathbb{R}$ astfel în cât funcţia $f : \mathbb{R} \to \mathbb{R},\ f(x) = \alpha x + \beta$ să stabilească un izomorfism de la $(\mathbb{R}, +, \cdot)$ la $(\mathbb{R}, \perp, \top)$.

3.41. Să se arate că inelul $\mathbb{Z}[\sqrt{2}]$ este izomorf cu inelul R din problema **3.29**.

3.42. Să se arate că corpul $\mathbb{Q}(\sqrt{2})$ este izomorf cu corpul K din problema **3.30**.

3.43. Fie $d \in \mathbb{Z}$ un întreg liber de pătrate şi

$$R = \left\{ \begin{pmatrix} a & b \\ bd & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}.$$

Să se arate că R este subinel în $(M_2(\mathbb{Z}), +, \cdot)$ şi că inelele $(\mathbb{Z}[\sqrt{d}], +, \cdot)$ şi $(R, +, \cdot)$ sunt izomorfe.

3.44. Fie $d \in \mathbb{Z}$ un întreg liber de pătrate şi

$$K = \left\{ \begin{pmatrix} a & b \\ bd & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}.$$

Să se arate că:
i) K este parte stabilă în $M_2(\mathbb{Q})$ în raport cu adunarea şi înmulţirea şi formează corp în raport cu operaţiile induse;
ii) corpurile $(\mathbb{Q}(\sqrt{d}), +, \cdot)$ şi $(K, +, \cdot)$ sunt izomorfe.

3.45. Să se arate că inelul $(\mathbb{Z}, +, \cdot)$ şi inelul $(\mathbb{Z}, \perp, \top)$ din problema **3.1** sunt izomorfe.

3.46. Fie $(R, +, \cdot)$ un inel (asociativ, comutativ, cu unitate) şi $(R', \perp, \top)$ o structură algebrică cu două operaţii (binare). Să se arate că dacă există un omomorfism surjectiv $f : R \to R'$ atunci $(R', \perp, \top)$ este inel (asociativ, comutativ, cu unitate). Cu alte cuvinte, orice imagine omomorfă a unui inel este un inel.

3.47. Să se arate că există structuri algebrice cu două operaţii (binare) care nu sunt inele, dar au imagini omomorfe inele.

3.48. Să se arate că dacă $(R, +, \cdot)$ din problema **3.46** este domeniu de integritate nu rezultă, în general, că $(R', \perp, \top)$ este domeniu de integritate.

3.49. Fie $(R, +, \cdot)$ şi $(R', +, \cdot)$ două inele şi $f : R \to R'$ un omomorfism de inele.
a) Să se arate că a idempotent în R implică $f(a)$ idempotent în R'.
b) Dacă R şi R' sunt inele asociative, să se arate că a nilpotent în R implică $f(a)$ nilpotent în R'.
c) Dacă f este surjectiv, să se arate că a central în R implică $f(a)$ central în R'.
d) Dacă R, R' sunt inele asociative cu unitate şi f este unital, să se arate că a inversabil în R implică $f(a)$ inversabil în R'.
e) Sunt reciprocele implicaţiilor de mai sus adevărate? Justificaţi răspunsul.

3.50. Fie $(R, +, \cdot)$ un inel (corp), R' o mulţime pentru care există o bijecţie $f : R \to R'$. Să se arate că se pot defini în mod unic două operaţii $\perp$ şi $\top$ pe R' astfel încât $(R', \perp, \top)$ să fie inel (corp) şi f să fie izomorfism între $(R, +, \cdot)$ şi $(R', \perp, \top)$.

3.51. Fie $(R, +, \cdot)$ un inel şi $n \in \mathbb{N}^*$. Să se arate că:
i) inelul $(M_n(R), +, \cdot)$ are $n + 1$ subinele izomorfe cu $(R, +, \cdot)$;
ii) inelul $(M_n(R), +, \cdot)$, cu $n \geq 2$, este comutativ dacă şi numai dacă $R \cdot R = \{0\}$;
iii) dacă $n \geq 2$ şi $R \neq \{0\}$ atunci inelul $(M_n(R), +, \cdot)$ are divizori ai lui zero şi elemente nilpotente nenule;

iv) inelul $(M_n(R), +, \cdot)$ este cu unitate dacă şi numai dacă inelul $(R, +, \cdot)$ este cu unitate;
v) dacă $n \geq 2$ şi $(R, +, \cdot)$ este un inel nenul cu unitate, atunci inelul $(M_n(R), +, \cdot)$ are elemente idempotente diferite de elementul nul şi elementul unitate;
vi) inelul $(M_n(R), +, \cdot)$ este corp (domeniu de integritate) dacă şi numai dacă $n = 1$ şi $(R, +, \cdot)$ este corp (domeniu de integritate).

3.52. Fie $(R, +, \cdot)$ un inel asociativ cu unitate şi $n \in \mathbb{N}^*$. Să se determine centrul inelului $(M_n(R), +, \cdot)$.

3.53. Pe mulţimea $Q = \{a_1 + a_2 i + a_3 j + a_4 k \mid a_1, a_2, a_3, a_4 \in \mathbb{R}\}$ se defineşte înmulţirea ca în problema **2.69** şi adunarea astfel: dacă $q = a_1 + a_2 i + a_3 j + a_4 k$ şi $q' = b_1 + b_2 i + b_3 j + b_4 k$ atunci

$$q + q' = (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k.$$

Să se arate că $(Q, +, \cdot)$ este un corp (numit *corpul cuaternionilor*) şi să se determine centrul său.

3.54. Fie $(R, +, \cdot)$ un inel asociativ cu unitate şi $(U(R, +, \cdot), \cdot)$ grupul (multiplicativ) al elementelor inversabile ale inelului R. Să se arate că:
i) $0 \in U(R, +, \cdot)$ dacă şi numai dacă $|R| = 1$;
ii) $(R, +, \cdot)$ este corp dacă şi numai dacă $R \neq 0$ şi $U(R, +, \cdot) = R^* = R \setminus \{0\}$;
iii) dacă $(R, +, \cdot)$ şi $(R', +, \cdot)$ sunt inele izomorfe atunci grupurile $(U(R, +, \cdot), \cdot)$ şi $(U(R', +, \cdot), \cdot)$ sunt izomorfe;
iv) există inele $(R, +, \cdot)$ şi $(R', +, \cdot)$ neizomorfe pentru care grupurile $(U(R, +, \cdot), \cdot)$ şi $(U(R', +, \cdot), \cdot)$ sunt izomorfe.

3.55. Fie $n \in \mathbb{N}^*$, $A, B \in M_n(\mathbb{C})$. Să se arate că:
i) următoarele afirmaţii sunt echivalente:
   a) A este inversabilă la stânga;
   b) A este inversabilă la dreapta;
   c) A este inversabilă;
ii) dacă $A + B = AB$ atunci $AB = BA$ şi să se dea un exemplu de astfel de matrice.

3.56. a) Să se determine $U(\mathbb{Z}, +, \cdot)$, $U(M_n(K), +, \cdot)$, cu $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ şi $n \in \mathbb{N}^*$, şi $U(M_n(\mathbb{Z}), +, \cdot)$, cu $n \in \mathbb{N}^*$.
b) Fie $n \in \mathbb{N}^*$, $(R, +, \cdot)$ un inel asociativ, comutativ, cu unitate şi $(K, +, \cdot)$ un corp. Să se determine $U(M_n(R), +, \cdot)$ şi $U(M_n(K), +, \cdot)$.
c) Să se arate că dacă $n \in \mathbb{N}$, $n \geq 2$ atunci grupul $(U(M_n(\mathbb{Z}), +, \cdot), \cdot)$ este infinit.

3.57. Fie $(R, +, \cdot)$ un inel asociativ, comutativ, cu unitate, $m, n \in \mathbb{N}^*$ şi $M_{m,n}(R)$ mulţimea matricelor de tipul (m, n) cu elemente din R. Să se arate că $(M_{m,n}(R), +)$ este un grup izomorf cu $(R^{mn}, +)$. Sunt izomorfe grupurile $(U(M_n(R), +, \cdot), \cdot)$ şi $((U(R, +, \cdot))^{n^2}, \cdot)$?

3.58. Fie M o mulţime, $(R, +, \cdot)$ un inel şi $R^M = \{f \mid f : M \to R\}$. Pe R^M se definesc două operaţii (binare) astfel: dacă $f, g \in R^M$ atunci $f + g,\ fg : R \to M$ sunt funcţiile definite prin

$$(f + g)(x) = f(x) + g(x) \text{ şi } (fg)(x) = f(x) \cdot g(x),\ \forall x \in M.$$

1) Să se arate că:
a) $(R^M, +, \cdot)$ este un inel care este asociativ, comutativ, respectiv cu unitate dacă $(R, +, \cdot)$ este asociativ, comutativ, respectiv cu unitate;
b) dacă $|M| \geq 2$ şi $|R| \geq 2$ atunci $(R^M, +, \cdot)$ are divizori ai lui zero;
c) dacă $M \neq \emptyset$ atunci inelul $(R^M, +, \cdot)$ are un subinel izomorf cu $(R, +, \cdot)$;
d) dacă $|M| = 1$ atunci inelul $(R^M, +, \cdot)$ este izomorf cu $(R, +, \cdot)$;
e) inelul $(R^M, +, \cdot)$ este corp dacă şi numai dacă $|M| = 1$ şi $(R, +, \cdot)$ este corp.
2) Dacă $(R, +, \cdot)$ este un inel asociativ cu unitate, să se determine $U(R^M, +, \cdot)$. Să se analizeze cazurile $R = \mathbb{R}$ şi $R = \mathbb{Z}$.

3.59. Fie $(R, +, \cdot)$ un inel asociativ cu unitate şi $(End(R, +), +, \circ)$ inelul endomorfismelor grupului său aditiv. Să se arate că:
i) dacă pentru orice $f \in End(R, +)$ şi orice $x \in R$, $f(x) = f(1) \cdot x$ atunci inelele $(R, +, \cdot)$ şi $(End(R, +), +, \circ)$ sunt izomorfe;
ii) dacă inelul $(R, +, \cdot)$ este comutativ atunci inelul $(End(R, +), +, \circ)$ este comutativ dacă şi numai dacă $(R, +, \cdot) \simeq (End(R, +), +, \circ)$.

3.60. Să se determine endomorfismele şi automorfismele grupurilor $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ şi $(\mathbb{Z}_n, +)$ $(n \in \mathbb{N},\ n \geq 2)$. Care dintre acestea sunt endomorfisme, respectiv automorfisme pentru inelele $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ şi $(\mathbb{Z}_n, +, \cdot)$?

3.61. Să se descrie toate structurile de inel, respectiv inel cu unitate, ce se pot defini pe grupul abelian $(\mathbb{Z}, +)$.

3.62. Fie $n \in \mathbb{N}$, $n \geq 2$. Să se arate că toate structurile de inel cu unitate pe grupul abelian $(\mathbb{Z}_n, +)$ sunt izomorfe cu inelul $(\mathbb{Z}_n, +, \cdot)$.

3.63. Fie p un număr prim. Să se arate că, abstracţie făcând de un izomorfism, există doar două inele asociative cu p elemente.

3.64. Să se arate că singurul omomorfism nenul de corpuri de la $(\mathbb{Q}, +, \cdot)$ la $(\mathbb{C}, +, \cdot)$ este omomorfismul de incluziune.

3.65. Să se determine automorfismele corpului $\mathbb{Q}(\sqrt{2})$.

3.66. Să se arate că singurul endomorfism nenul al corpului $(\mathbb{R}, +, \cdot)$ este $1_{\mathbb{R}}$.

3.67. Fie $m, n \in \mathbb{N},\ m \geq 2,\ n \geq 2$. Să se determine omomorfismele de inele de la $(\mathbb{Z}_m, +, \cdot)$ la $(\mathbb{Z}_n, +, \cdot)$.

3.68. Să se arate că dacă $(R, +, \cdot)$ este un inel şi restricţiile la $\mathbb{Z}$ a două omomorfisme $g, h : \mathbb{Q} \to R$ sunt egale atunci $g = h$.

3.69. Să se determine idealele subinelelor lui $(\mathbb{Z}, +, \cdot)$.

3.70. Fie $(R, +, \cdot)$ un inel asociativ. Pentru două ideale U, V ale lui R considerăm $U : V = \{r \in R \mid rx \in U,\ \forall x \in V\}$. Să se arate că:
i) $U : V$ este ideal în R;
ii) dacă U_1, U_2, V_1, V_2 sunt ideale în R atunci au loc egalităţile: $U : U = R$, $(U_1 \cap U_2) : V = (U_1 : V) \cap (U_2 : V)$, $U : (V_1 + V_2) = (U : V_1) \cap (U : V_2)$;
iii) dacă inelul R este comutativ şi T este, de asemenea, ideal al lui R atunci $U : (U + V) = U : V$ şi $(U : V) : T = U : (V : T)$;
iv) dacă R este comutativ, cu unitate, $U : V = R$ dacă şi numai dacă $V \subseteq U$;
v) în inelul numerelor întregi avem $n\mathbb{Z} : m\mathbb{Z} = \dfrac{[m, n]}{m}\mathbb{Z}$ $(m, n \in \mathbb{N},\ m \neq 0)$.

3.71. Fie $(R,+,\cdot)$ un inel asociativ şi comutativ şi U, V ideale în R. Să se arate că $\sqrt{U} = \{r \in R \mid \exists n \in \mathbb{N}: \ r^n \in U\}$ este, de asemenea, ideal în R şi să se verifice egalităţile $\sqrt{\sqrt{U}} = \sqrt{U}$, $\sqrt{U \cap V} = \sqrt{U} \cap \sqrt{V}$ şi $\sqrt{U+V} = \sqrt{\sqrt{U}+\sqrt{V}}$.

3.72. Este intersecţia dintre un ideal stâng şi un ideal drept un ideal (bilateral)? Justificaţi răspunsul.

3.73. Să se arate că laticea idealelor unui inel este modulară.

3.74. Să se arate că într-un inel asociativ şi comutativ elementele nilpotente formează un ideal.

3.75. Să se arate că într-un inel asociativ, comutativ, cu unitate suma unui element inversabil cu un element nilpotent este un element inversabil.

3.76. Fie $(R,+,\cdot)$ un inel Boole nenul. Să se arate că:
i) R este inel simplu dacă şi numai dacă R este izomorf cu inelul $(\mathbb{Z}_2,+,\cdot)$;
ii) orice ideal al lui R generat de o submulţime finită este principal.

3.77. a) Fie $(R_1,+,\cdot)$ şi $(R_2,+,\cdot)$ două inele cu unitate. Să se determine idealele produsului direct $(R_1 \times R_2,+,\cdot)$ al celor două inele.
b) Să se determine idealele inelului $(\mathbb{Z} \times \mathbb{Z},+,\cdot)$ şi al inelului $(K \times K,+,\cdot)$ (unde $(K,+,\cdot)$ este un corp).

3.78. Fie $(R,+,\cdot)$ un inel cu unitate şi $(M_n(R),+,\cdot)$ inelul matricelor pătrate cu elemente din R. Să se arate că dacă $\mathcal{U}$ este un ideal al lui $(M_n(R),+,\cdot)$ şi $A \in \mathcal{U}$ atunci permutând două linii (coloane) ale lui A, înmulţind o linie (coloană) a lui A cu un element din R sau adunând la o linie (coloană) a lui A o altă linie (coloană) a lui A înmulţită cu un element din R obţinem tot o matrice din $\mathcal{U}$.

3.79. Fie $(R,+,\cdot)$ un inel şi $(M_n(R),+,\cdot)$ inelul matricelor pătrate cu elemente din R. Să se arate că:
a) matricele triunghiulare (adică matricele $A = (a_{ij})$, cu $a_{ij} = 0$ pentru orice $i,j \in \{1,\ldots,n\}$, $i > j$) formează un subinel necomutativ T al lui $(M_n(R),+,\cdot)$;
b) $U = \{A = (a_{ij}) \mid a_{ij} = 0, \ \forall i,j \in \{1,\ldots,n\}, \ i \geq j\}$ este un ideal al lui T;
c) inelul cât T/U este comutativ.

3.80. Fie $(R,+,\cdot)$ un inel cu unitate şi $(M_n(R),+,\cdot)$ inelul matricelor pătrate cu elemente din R. Să se arate că:
i) orice ideal al lui $M_n(R)$ este de forma $M_n(U)$, unde U este un ideal al lui R;
ii) dacă U este ideal în R, inelele $M_n(R)/M_n(U)$ şi $M_n(R/U)$ sunt izomorfe;
iii) dacă R este un inel simplu atunci $M_n(R)$ este un inel simplu;
iv) dacă R este un corp atunci $M_n(R)$ este un inel simplu;
v) dacă R nu are unitate, proprietatea i) nu rămâne, în general, adevărată;
vi) proprietatea de la i) nu se menţine pentru ideale stângi (drepte).

3.81. Fie M o mulţime, $(\mathcal{P}(M),+,\cdot)$ inelul introdus în problema **3.4** şi $N \subseteq M$. Să se arate că:
i) inelele $(\mathcal{P}(M \setminus N),+,\cdot)$ şi $(\mathcal{P}(M)/\mathcal{P}(N),+,\cdot)$ sunt izomorfe;
ii) dacă M este finită, orice ideal al lui $\mathcal{P}(M)$ este de forma $\mathcal{P}(N)$ cu $N \subseteq M$;
iii) dacă M este infinită atunci ii) nu are loc.

3.82. Să se arate că dacă $f : R \to R'$ este un omomorfism surjectiv de inele şi U este un ideal al lui R care include pe $\operatorname{Ker} f$ atunci inelele cât R/U şi $R'/f(U)$ sunt izomorfe.

3.83. Fie $(R, +, \cdot)$ un inel. Să se arate că:
i) toţi nondivizorii lui zero din R au acelaşi ordin în grupul $(R, +)$;
ii) dacă $a \in R^*$ nu este divizor al lui zero atunci ordinul lui a în $(R, +)$ este infinit sau un număr prim;
iii) dacă $|R| = 4$ şi R nu are divizori ai lui zero atunci grupul $(R, +)$ este izomorf cu grupul lui Klein;
iv) dacă $|R| = 6$ atunci R are divizori ai lui zero.

3.84. Să se arate că într-un corp $(K, +, \cdot)$ nu există elemente nenule a, b astfel încât $2a = 3b = 0$.

3.85. Să se determine caracteristica unui inel Boole.

3.86. Fie $m, n \in \mathbb{N}^* \setminus \{1\}$. Să se determine caracteristica inelului $(\mathbb{Z}_m \times \mathbb{Z}_n, +, \cdot)$.

3.87. Să se determine caracteristica inelelor $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z}_2 \times \mathbb{Z}$, $\mathbb{Q} \times \mathbb{Z}_4$, $End(\mathbb{Z}, +)$ şi $End(\mathbb{Z}_3, +)$.

3.88. Să se dea exemple de inele infinite de caracteristică finită.

3.89. Să se dea exemple de inele asociative, comutative, cu unitate care nu sunt corpuri, dar au caracteristica număr prim.

3.90. Să se determine corpurile K pentru care $\{0, 1\}$ formează un subcorp al lui K.

3.91. Fie K un corp comutativ de caracteristică infinită, $n \in \mathbb{N}^*$ şi $A, B \in M_n(K)$. Este posibil ca $AB - BA = I_n$?

3.92. Fie R un inel asociativ cu unitate, fără divizori ai lui zero, cu $|R| \geq 2$. Să se arate că grupurile $(R, +)$ şi $(U(R, +, \cdot), \cdot)$ nu sunt izomorfe.

3.93. Fie K un corp. Să se arate că grupurile $(K, +)$ şi $(K^*, \cdot)$ nu sunt izomorfe.

3.94. Fie $(R, +, \cdot)$ un inel asociativ, comutativ, cu unitate şi $(R[X], +, \cdot)$ inelul polinoamelor într-o nedeterminată peste R. Se consideră familia de grupuri $(R_n, +) = (R, +)$, $n \in \mathbb{N}$. Să se arate că grupul $(R[X], +)$ este izomorf cu suma directă a (produsul restrâns al) familiei de grupuri $(R_n, +)$, $n \in \mathbb{N}$.

3.95. Fie R un inel asociativ, comutativ, cu unitate. Să se arate că o serie formală $f = a_0 + a_1X + \cdots + a_nX^n + \cdots$ cu coeficienţi în R este inversabilă în $R[[X]]$ dacă şi numai dacă a_0 este inversabil în R.

3.96. Să se determine elementele inversabile ale următoarelor inele de polinoame: i) $(\mathbb{Z}[X], +, \cdot)$; ii) $(\mathbb{Q}[X], +, \cdot)$; iii) $(\mathbb{R}[X], +, \cdot)$; iv) $(\mathbb{C}[X], +, \cdot)$; v) $(\mathbb{Z}_p[X], +, \cdot)$ (cu p număr prim).

3.97. Există polinoame inversabile ca serii formale care nu sunt inversabile ca polinoame? Justificaţi răspunsul.

3.98. Să se determine toate polinoamele $h \in \mathbb{Z}_4[X]$ care verifică egalitatea

$$(\widehat{2}X^2 + \widehat{2}X + \widehat{3})h = \widehat{1}.$$

3.99. Fie $(R, +, \cdot)$ un inel asociativ, comutativ, cu unitate, $a_0, \ldots, a_n \in R$ şi $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$. Să se arate că:
a) f este inversabil în $R[X]$ dacă şi numai dacă a_0 este inversabil în R şi $a_1, \ldots, a_n$ sunt elemente nilpotente ale lui R;
b) f este nilpotent în $R[X]$ dacă şi numai dacă $a_0, a_1, \ldots, a_n$ sunt elemente nilpotente ale lui R

3.100. Fie $n \in \mathbb{N}$, $n \geq 2$. Să se determine elementele inversabile din $(\mathbb{Z}_n[X], +, \cdot)$.

3.101. Fie $(R, +, \cdot)$ un inel asociativ, comutativ, cu unitate. Să se arate că un polinom nenul f este un divizor al lui zero în $R[X]$ dacă şi numai dacă există $a \in R$, $a \neq 0$ astfel încât $af = 0$.

3.102. Să se arate că ecuaţia $x^2 + 1 = 0$ are o infinitate de soluţii în corpul cuaternionilor.

3.103. Există polinoame nenule cu coeficienţi într-un inel asociativ, comutativ, cu unitate pentru care numărul rădăcinilor depăşeşte gradul? Justificaţi răspunsul.

3.104. Să se determine rădăcinile polinomului $aX^2 + bX + c$ $(a, b, c \in \mathbb{C},\ a \neq 0)$.

3.105. Să se rezolve în $\mathbb{C}$ ecuaţiile: a) $x^2 + (2 - i)x - i = 0$; b) $y^2 + i\sqrt{6}y - 3 = 0$; c) $x^2 + \sqrt{3}x + i = 0$.

3.106. a) Fie $p, q \in \mathbb{C}$. Să se găsească două numere $\alpha, \beta \in \mathbb{C}$ astfel încât $\alpha + \beta$ să fie o soluţie a ecuaţiei $y^3 + py + q = 0$.
b) Să se determine rădăcinile polinomului $aX^3 + bX^2 + cX + d \in \mathbb{C}[X]$, $a \neq 0$.

3.107. Să se rezolve în $\mathbb{C}$ ecuaţiile: a) $x^3 - 3x - 4 = 0$; b) $x^3 + 6x^2 + 18x + 27 = 0$.

3.108. a) Fie $p, q, r \in \mathbb{C}$ şi $h = X^4 + pX^2 + qX + r$. Să se determine $m \in \mathbb{C}$ astfel încât $h = f^2 - g^2$ unde $f = X^2 + \dfrac{p}{2} + m$ şi $g \in \mathbb{C}[X]$.
b) Să se deducă, folosind a), o metodă de rezolvare a ecuaţiei

$$ax^4 + bx^3 + cx^2 + dx + e = 0,\ a, b, c, d, e \in \mathbb{C},\ a \neq 0.$$

3.109. Să se determine rădăcinile polinomului $X^4 + 6X^2 + 6i\sqrt{6}X - 9 \in \mathbb{C}[X]$.

3.110. Să se dea exemple de inele asociative, comutative, cu unitate R pentru care omomorfismul $\varphi : R[X] \to R^R$, $\varphi(f) = \widetilde{f}$ (unde $\widetilde{f}$ este funcţia polinomială deteminată de f) nu este: a) injectiv; b) surjectiv.

3.111. a) Fie $(R, +, \cdot)$ un domeniu de integritate infinit şi $f, g \in R[X]$. Să se arate că $\widetilde{f} = \widetilde{g}$ dacă şi numai dacă $f = g$ (ceea ce permite aplicarea metodei coeficienţilor nedeterminaţi în cazul funcţiilor polinomiale definite pe domenii de integritate infinite, de exemplu pe $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$).
b) Fie $(R, +, \cdot)$ un domeniu de integritate finit cu n elemente, $R = \{a_1, \ldots, a_n\}$ şi $f, g \in R[X]$. Să se arate că $\widetilde{f} = \widetilde{g}$ dacă şi numai dacă $(X - a_1) \cdots (X - a_n) \mid (f - g)$.

3.112. Fie $f = X^3 + \widehat{2}X^2 + X + \widehat{1} \in \mathbb{Z}_3[X]$. Care sunt polinoamele de grad cel mult 3 din $\mathbb{Z}_3[X]$ care definesc aceeaşi funcţie polinomială ca şi f? Dar cele de grad cel mult 4?

3.113. Fie $(R, +, \cdot)$ un inel asociativ, comutativ, cu unitate. Să se arate că omomorfismul φ din problema **3.110** este surjectiv dacă şi numai dacă $R = \{0\}$ sau R este un corp finit.

3.114. Fie $(R, +, \cdot)$ un domeniu de integritate. Să se arate că:
a) dacă φ este un endomorfism surjectiv al lui $R[X]$ cu proprietatea că

$$\varphi(r) = r,\ \forall r \in R$$

atunci există $a, b \in R$ astfel încât $\varphi = E_{aX+b}$ (amintim că $E_{aX+b}(f) = f(aX + b)$);
b) dacă $a, b \in R$ atunci E_{aX+b} este automorfism al lui $R[X]$ dacă şi numai dacă a este inversabil.

3.115. Să se determine automorfismele inelelelor $\mathbb{Z}[X]$, $\mathbb{Q}[X]$ şi $\mathbb{Z}_p[X]$ (cu p număr prim).

3.116. Este inelul cât $\mathbb{C}[X]/(X^2 + 1)$ un domeniu de integritate?

3.117. Este inelul cât $\mathbb{Q}[X, Y]/(X, Y)$ un corp?

3.118. Să se demonstreze că au loc următoarele izomorfisme de inele: a) $\mathbb{C} \simeq \mathbb{R}[X]/(X^2 + 1)$; b) $\mathbb{Z}[X]/(n, X) \simeq \mathbb{Z}_n$; c) $\mathbb{Z}[X]/(n) \simeq \mathbb{Z}_n[X]$ ($n \in \mathbb{N}$, $n \geq 2$).

3.119. Fie $(K, +, \cdot)$ un corp comutativ. Să se arate că au loc următoarele izomorfisme: a) $K[X]/(X + 1) \simeq K$; b) $K[X, Y]/(X - Y) \simeq K[X] \simeq K[X, Y]/(X + Y)$.

3.120. Să se arate că următoarele inele cât sunt izomorfe: a) $\mathbb{Q}[X]/(X^2 - 1)$ şi $\mathbb{Q}[X]/(X^2 - 4)$; b) $\mathbb{Z}_2[X]/(X^2 - \widehat{1})$ şi $\mathbb{Z}_2[X]/(X^2)$; c) $\mathbb{Z}_5[X]/(X^2 + \widehat{1})$ şi $\mathbb{Z}_5[X]/(X^2 + \widehat{2}X + \widehat{2})$; d) $\mathbb{R}[X]/(X^2 + 1)$ şi $\mathbb{R}[X]/(X^2 + 2X + 2)$.

3.121. Să se scrie cu ajutorul polinoamelor simetrice fundamentale următoarele polinoame şi fracţii raţionale simetrice cu coeficienţi reali:
a) $(X_1^2 + X_2^2)(X_2^2 + X_3^2)(X_3^2 + X_1^2)$;
b) $X_1^3X_2 + \cdots + X_1^3X_n + X_2^3X_1 + X_2^3X_3 + \cdots + X_2^3X_n + \cdots + X_n^3X_1 + \cdots + X_n^3X_{n-1}$;
c) $(X_1^2 + X_1^3 + X_1^4) + (X_2^2 + X_2^3 + X_2^4) + (X_3^2 + X_3^3 + X_3^4) + (X_4^2 + X_4^3 + X_4^4)$;
d) $\dfrac{X_1}{X_2} + \dfrac{X_2}{X_1} + \dfrac{X_2}{X_3} + \dfrac{X_3}{X_2} + \dfrac{X_3}{X_1} + \dfrac{X_1}{X_3}$.

3.122. Ştiind că $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ sunt rădăcinile polinomului $X^3 - 3X - 4$, să se determine numărul $(\alpha_1^2 + \alpha_2^2)(\alpha_2^2 + \alpha_3^2)(\alpha_3^2 + \alpha_1^2)$.

3.123. Fie $(K, +, \cdot)$ un corp comutativ şi $f = a_0 + a_1X + \cdots + a_nX^n \in K[X]$. Polinomul $f' = a_1 + 2a_2X + \cdots + na_nX^{n-1}$ se numeşte *derivata formală a polinomului* f. Să se arate că pentru orice $f, g \in K[X]$, $k \in \mathbb{N}^*$ şi $\alpha \in K$ avem

$$(f + g)' = f' + g',\ (\alpha f)' = \alpha f',\ (fg)' = f'g + fg' \text{ şi } (f^k)' = kf^{k-1}f'.$$

3.124. Fie $(K,+,\cdot)$ un corp comutativ de caracteristică ∞ şi $f \in K[X]$. Să se arate că $a \in K$ este rădăcină multiplă de ordinul m a lui f dacă şi numai dacă

$$f(a) = f'(a) = \cdots = f^{(m-1)}(a) = 0 \text{ şi } f^{(m)}(a) \neq 0.$$

3.125. Fie $f = X^n - s_1X^{n-1} + s_2X^{n-2} + \cdots + (-1)^{n-1}s_{n-1}X + (-1)^n s_n \in \mathbb{C}[X]$, $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ rădăcinile lui f, $S_0 = n$ şi $S_k = \alpha_1^k + \cdots + \alpha_n^k$ $(k \in \mathbb{N}^*)$. Să se demonstreze egalităţile de mai jos (numite *formulele lui Newton*):

$$S_k - s_1S_{k-1} + \cdots + (-1)^{k-2}s_{k-2}S_2 + (-1)^{k-1}s_{k-1}S_1 + (-1)^k k s_k = 0,\ \forall k < n,$$
$$S_k - s_1S_{k-1} + \cdots + (-1)^{n-1}s_{n-1}S_{k-n+1} + (-1)^n s_n S_{k-n} = 0,\ \forall k \geq n.$$

3.126. Să se scrie formulele lui Newton în cazul: a) $n = 2$; b) $n = 3$.

3.127. Să se arate că formulele lui Newton rămân adevărate în cazul în care R este un domeniu de integritate, $s_1, \ldots, s_n$ sunt polinomamele simetrice fundamentale din $R[X_1, \ldots, X_n]$ şi $S_k = X_1^k + \cdots + X_n^k$ $(k \in \mathbb{N}^*)$.

3.128. Fie $f = a_0 + a_1X + \cdots + a_nX^n$, $g = b_0 + b_1X + \cdots + b_mX^m$, cu $a_n \neq 0$, $b_m \neq 0$, două polinoame din $\mathbb{C}[X]$, $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ rădăcinile lui f, $\beta_1, \ldots, \beta_m \in \mathbb{C}$ rădăcinile lui g. Numărul complex

$$\mathbf{R}_{f,g} = a_n^m b_m^n \prod_{(i,j)\in\{1,\ldots,n\}\times\{1,\ldots,m\}} (\alpha_i - \beta_j)$$

se numeşte *rezultanta polinoamelor* f şi g. Să se arate că:
a) $\mathbf{R}_{f,g} = 0$ dacă şi numai dacă f şi g au cel puţin o rădăcină comună;
b) $\mathbf{R}_{f,g} = (-1)^{mn}\mathbf{R}_{g,f}$;
c) $\mathbf{R}_{f,g} = a_n^m g(\alpha_1)\cdots g(\alpha_n) = (-1)^{mn} b_m^n f(\beta_1)\cdots f(\beta_m)$;
d) $\mathbf{R}_{f,g_1g_2} = \mathbf{R}_{f,g_1} \cdot \mathbf{R}_{f,g_2}$;
e) dacă f, g sunt polinoame din $\mathbb{R}[X]$ ($\mathbb{Q}[X]$, respectiv $\mathbb{Z}[X]$) atunci $\mathbf{R}_{f,g}$ este un număr real (raţional, respectiv întreg).

3.129. Fie $f = a_0 + a_1X + \cdots + a_nX^n$, $g = b_0 + b_1X + \cdots + b_mX^m$, cu $a_n \neq 0$, $b_m \neq 0$, două polinoame din $\mathbb{C}[X]$. Să se arate că rezultanta $\mathbf{R}_{f,g}$ a polinoamelor f şi g este egală cu determinantul

$$\left.\begin{vmatrix}
a_n & a_{n-1} & a_{n-2} & \ldots & a_0 & 0 & 0 & \ldots & 0 \\
0 & a_n & a_{n-1} & \ldots & a_1 & a_0 & 0 & \ldots & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & 0 & \ldots & & & & \ldots & a_0 \\
b_m & b_{m-1} & b_{m-2} & \ldots & & & & \ldots & 0 \\
0 & b_m & b_{m-1} & \ldots & & & & \ldots & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & 0 & \ldots & & & & \ldots & b_0
\end{vmatrix}\right.
\begin{array}{l}
\left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} m \text{ linii} \\
\left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} n \text{ linii}
\end{array}$$

3.130. Să se scrie sub formă de determinant rezultanta polinoamelor $a_0+a_1X+a_2X^2$ şi $b_0 + b_1X + b_2X^2 + b_3X^3$ $(a_2 \neq 0 \neq b_3)$.

3.131. Să se arate că următoarele polinoame au o rădăcină comună:
a) $X^5 - X^4 - X^2 + 1$ şi $X^3 + 2X^2 - 3$;
b) $2X^3 + X^2 + X - 1$ şi $3X^3 + 2X^2 + 2X - 1$.

3.132. Să se determine $\lambda \in \mathbb{C}$ astfel încât următoarele polinoame cu coeficienţi complecşi să aibă o rădăcină comună:
a) $2X^3 + X^2 + X - 1$ şi $2X^3 + \lambda X^2 - 3X - (\lambda + 1)$;
b) $X^3 + 3X^2 + 2X + \lambda$ şi $X^2 - 3X + 2$.

3.133. Fie $f = a_0 + a_1X + \cdots + a_nX^n$, cu $a_n \neq 0$, un polinom din $\mathbb{C}[X]$ şi f' derivata formală a lui f. Numărul complex $\mathbf{D}_f = (-1)^{\frac{n(n-1)}{2}} \dfrac{1}{a_n} \mathbf{R}_{f,f'}$ se numeşte *discriminantul polinomului* f. Să se arate că polinomul f are rădăcini multiple dacă şi numai dacă $\mathbf{D}_f = 0$.

3.134. Fie $f = a_0 + a_1X + \cdots + a_nX^n$, cu $a_n \neq 0$, un polinom din $\mathbb{C}[X]$, $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ rădăcinile sale şi $S_k = \alpha_1^k + \cdots + \alpha_n^k$ $(k \in \mathbb{N}^*)$. Să se arate că

$$\mathbf{D}_f = a_n^{2n-2} \begin{vmatrix} n & S_1 & S_2 & \ldots & S_{n-1} \\ S_1 & S_2 & S_3 & \ldots & S_n \\ S_2 & S_3 & S_4 & \ldots & S_{n+1} \\ \vdots & \vdots & \vdots & & \vdots \\ S_{n-1} & S_n & S_{n+1} & \ldots & S_{2n-2} \end{vmatrix}.$$

3.135. Să se calculeze discriminantul următoarelor polinoame: a) $aX^2 + bX + c$ $(a, b, c \in \mathbb{C},\ a \neq 0)$; b) $X^3 + pX + q$ $(p, q \in \mathbb{C})$; c) $3X^3 + 3X^2 + 5X + 2 \in \mathbb{R}[X]$; d) $2X^4 - X^3 - 4X^2 + X + 1 \in \mathbb{R}[X]$.

3.136. Să se determine $\lambda \in \mathbb{C}$ pentru care următoarele polinoame din $\mathbb{C}[X]$ au rădăcini multiple: a) $X^3 - 3X + \lambda$; b) $X^4 - 4X^3 + (2 - \lambda)X^2 + 2X - 2$.

Capitolul 4

Semigrupuri şi inele de fracţii

4.1. Să se dea exemple de semigrupuri comutative care nu pot fi scufundate izomorf într-un grup.

4.2. Fie $(G, \cdot)$ un grup, A un subsemigrup comutativ al lui G şi $\emptyset \neq S \subseteq A$ o parte stabilă a lui G. Să se arate că subsemigrupul lui G generat de $A \cup S^{-1}$ este

$$\{as^{-1} \mid a \in A,\ s \in S\}$$

şi că acesta este izomorf cu semigrupul de fracţii A_S. Să se deducă de aici că A are un grup de fracţii izomorf cu subgrupul lui G generat de A.

4.3. Să se determine următoarele semigrupuri de fracţii (sau diferenţe): a) $(\mathbb{Z}_{\mathbb{Z}^*}, \cdot)$; b) $(\mathbb{Z}^*_{\mathbb{Z}^*}, \cdot)$; c) $(\mathbb{Z}_{2\mathbb{Z}^*}, \cdot)$; d) $(\mathbb{N}_{2\mathbb{N}}, +)$; e) $(2\mathbb{N}_{2\mathbb{N}}, +)$; f) $(2\mathbb{Z}_{2\mathbb{Z}^*}, \cdot)$; g) $(2\mathbb{Z}_{2\mathbb{Z}}, +)$.

4.4. Fie $(A, \cdot)$ un semigrup comutativ, $S \neq \emptyset$ o parte stabilă în A cu elementele căreia se poate simplifica şi $f : A \to A_S$ omomorfismul canonic. Să se arate că dacă $q_1, \ldots, q_n \in A_S$ atunci există $s \in S$ astfel încât $f(s)q_1, \ldots, f(s)q_n \in f(A)$.

4.5. Un triplet $(A, +, \cdot)$, unde A este mulţime şi $+, \cdot$ sunt operaţii pe A se numeşte *semiinel*, respectiv *semiinel comutativ* dacă verifică următoarele condiţii:
i) $(A, +)$ este monoid comutativ;
ii) $(A, \cdot)$ este semigrup, respectiv semigrup comutativ;
iii) $a(b + c) = ab + ac$ şi $(b + c)a = ba + ca$, $\forall a, b, c \in A$.
Să se arate că orice semiinel comutativ $(A, +, \cdot)$ cu proprietatea

$$a, b, c \in A,\ a + b = a + c \Rightarrow b = c$$

se scufundă izomorf într-un inel minimal, numit *inelul diferenţelor semiinelului* $(A, +, \cdot)$.

4.6. Să se construiască inelul diferenţelor semiinelului $(\mathbb{N}, +, \cdot)$ şi să se arate că se poate identifica cu inelul $(\mathbb{Z}, +, \cdot)$ acceptat intuitiv.

4.7. Să se dea exemple de inele comutative care nu pot fi scufundate izomorf într-un corp.

4.8. Fie $(K, +, \cdot)$ un corp, R un subinel comutativ nenul al lui K şi $\emptyset \neq S \subseteq R$ un sistem multiplicativ ce nu conţine pe 0. Să se arate că subinelul lui K generat de $R \cup S^{-1}$ este

$$\{as^{-1} \mid a \in R,\ s \in S\}$$

şi că acesta este izomorf cu inelul R_S. Să se deducă de aici că inelul R are un corp de fracţii izomorf cu subcorpul lui K generat de R.

4.9. Să se determine inelul total de fracţii în cazul următoarelor inele: a) $(\mathbb{Z}, +, \cdot)$; b) $(2\mathbb{Z}, +, \cdot)$; c) $(\mathbb{Z}_3, +, \cdot)$; d) $(\mathbb{Q}, +, \cdot)$.

4.10. Să se determine inelul fracţiilor cu numărători în inelul $(\mathbb{Z}, +, \cdot)$ şi numitori în $2\mathbb{Z}^* \cup \{1\}$.

4.11. Să se determine inelul total de fracţii al inelului întregilor lui Gauss. Generalizare pentru $(\mathbb{Z}[\sqrt{d}], +, \cdot)$ cu $d \in \mathbb{Z} \setminus \{1\}$ liber de pătrate.

4.12. Fie p un număr prim şi

$$\mathbb{Q}^{(p)} = \left\{ \frac{m}{n} \in \mathbb{Q} \mid (n, p) = 1 \right\}.$$

Să se arate că:
a) $\mathbb{Q}^{(p)}$ este parte stabilă a lui $\mathbb{Q}$ în raport cu adunarea şi înmulţirea;
b) $(\mathbb{Q}^{(p)}, +, \cdot)$ este un domeniu de integritate;
c) corpul de fracţii al lui $(\mathbb{Q}^{(p)}, +, \cdot)$ este $(\mathbb{Q}, +, \cdot)$.

4.13. Să se arate că pentru orice subinel nenul cu unitate R al lui $(\mathbb{Q}, +, \cdot)$ există un sistem multiplicativ $\emptyset \neq S \subseteq \mathbb{Z}$ (ce nu conţine pe 0) astfel încât $R = \mathbb{Z}_S$.

4.14. Fie $(R, +, \cdot)$ un domeniu de integritate şi $a \in R \setminus \{0\}$. Să se arate că dacă S este semigrupul generat de a atunci inelul R_S este izomorf cu inelul cât $R[X]/(aX - 1)$.

4.15. Fie $(R, +, \cdot)$ un inel nenul asociativ şi comutativ, $\emptyset \neq S \subseteq A$ un sistem multiplicativ ce nu conţine pe 0 şi divizori ai lui zero, iar $f : R \to R_S$ omomorfismul canonic. Să se arate că:
a) dacă $(R', +, \cdot)$ este un inel şi $g, h : R_S \to R'$ sunt omomorfisme de inele atunci

$$g \circ f = h \circ f \Rightarrow g = h;$$

b) dacă R are unitate atunci f este izomorfism dacă şi numai dacă $S \subseteq U(R, +, \cdot)$.

4.16. Fie $(R, +, \cdot)$ un domeniu de inegritate, $\emptyset \neq S \subseteq R$ un sistem multiplicativ ce nu conţine pe 0 şi $f : R \to R_S$ omomorfismul canonic. Să se arate că f este un izomorfism dacă şi numai dacă orice element din R_S este rădăcină a unui polinom de forma $X - a$ cu $a \in R$.

4.17. Fie $n \in \mathbb{N}$, $n \geq 2$ şi $S \neq \emptyset$ un sistem multiplicativ al lui $\mathbb{Z}_n$ ce nu conţine pe $\widehat{0}$ şi divizori ai lui zero. Să se arate că omomorfismul canonic $f : \mathbb{Z}_n \to (\mathbb{Z}_n)_S$ este surjectiv.

4.18. Pe $(\mathbb{R}^{\mathbb{R}}, +, \cdot)$ inelul definit pe $\mathbb{R}^{\mathbb{R}} = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$ ca în problema **3.58**. Să se arate că:
a) o funcţie nenulă $g : \mathbb{R} \to \mathbb{R}$ este nondivizor al lui zero în $(\mathbb{R}^{\mathbb{R}}, +, \cdot)$ dacă şi numai dacă pentru orice $x \in \mathbb{R}$ avem $g(x) \neq 0$;
b) o funcţie nenulă $g : \mathbb{R} \to \mathbb{R}$ este element inversabil în $(\mathbb{R}^{\mathbb{R}}, +, \cdot)$ dacă şi numai dacă g nu este divizor al lui zero în $(\mathbb{R}^{\mathbb{R}}, +, \cdot)$;
c) inelul total de fracţii al inelului $(\mathbb{R}^{\mathbb{R}}, +, \cdot)$ este izomorf cu $(\mathbb{R}^{\mathbb{R}}, +, \cdot)$.

4.19. Să se arate că funcţia $g : \left(\mathbb{Z}^{\mathbb{N}}\right)_{\mathbb{Z}^*} \to \left(\mathbb{Z}_{\mathbb{Z}^*}\right)^{\mathbb{N}}$ definită prin

$$g\left(\frac{(x_n)_{n\in\mathbb{N}}}{y}\right) = \left(\frac{x_n}{y}\right)_{n\in\mathbb{N}}$$

este un omomorfism. Este g izomorfism?

4.20. Să se arate că orice omomorfism injectiv (surjectiv, bijectiv) între două domenii de integritate induce un omomorfism injectiv (surjectiv, respectiv bijectiv) între corpurile lor de fracţii.

4.21. Fie $(R, +, \cdot)$ un inel nenul asociativ, comutativ şi cu unitate, iar $\emptyset \neq S \subseteq A$ un sistem multiplicativ ce nu conţine pe 0 şi divizori ai lui zero. Să se arate că dacă toate idealele lui R sunt principale atunci toate idealele lui R_S sunt principale.

Capitolul 5

Divizibilitatea în monoizi comutativi cu simplificare şi în domenii de integritate

5.1. Să se determine relaţia de asociere în divizibilitate şi mulţimea cât în raport cu aceasta în cazul monoizilor sau domeniilor de integritate următoare: a) $(\mathbb{N}^*, \cdot)$; b) $(\mathbb{Q}^*, \cdot)$; c) $(\mathbb{Z}, +, \cdot)$; d) $(\mathbb{R}, +, \cdot)$; e) $(\mathbb{Z}_2, +, \cdot)$; f) $(\mathbb{Z}[i], +, \cdot)$.

5.2. Fie $K \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\} \cup \{\mathbb{Z}_p \mid p \text{ număr prim}\}$ şi $f \in K[X]$. Să se determine polinoamele asociate în divizibilitate cu f.

5.3. Să se arate că:
i) relaţia de divizibilitate din $\mathbb{Z}_2[X_1, \ldots, X_n]$ este relaţie de ordine;
ii) dacă R este domeniu de integritate în care relaţia de divizibilitate este relaţie de ordine atunci caracteristica lui R este 2;
iii) există domenii de integritate de caracteristică 2 în care relaţia de divizibilitate nu este relaţie de ordine.

5.4. Fie R un domeniu de integritate în care orice elemente nenule sunt asociate în divizibilitate. Să se arate că R este un corp.

5.5. Fie R un domeniu de integritate în care orice element nenul este inversabil sau ireductibil. Să se arate că R este un corp.

5.6. Fie R, R' domenii de integritate şi $\varphi : R \to R'$ un izomorfism de inele. Să se arate că $a \in R$ este element ireductibil (prim) în R dacă şi numai dacă $\varphi(a)$ este element ireductibil (prim) în R'.

5.7. Fie K' un corp comutativ, K un subcorp al lui K' şi $f \in K[X]$. Să se arate că dacă un polinom f este ireductibil în $K'[X]$ atunci este ireductibil şi în $K[X]$. Este reciproca adevărată?

5.8. Fie $p, q \in \mathbb{Z}$, $(p, q) = 1$ şi $f \in \mathbb{Z}[X]$. Să se arate că dacă $f\left(\dfrac{p}{q}\right) = 0$ atunci

$$(p - q) | f(1) \text{ şi } (p + q) | f(-1).$$

În particular, să se arate că dacă $a \in \mathbb{Z}$ şi $f(a) = 0$ atunci

$$(1 - a) | f(1) \text{ şi } (1 + a) | f(-1).$$

5.9. Să se descompună în produs de polinoame ireductibile toate polinoamele din $\mathbb{Z}_2[X] \setminus \mathbb{Z}_2$ de grad cel mult 3.

5.10. Fie K un corp comutativ şi $f \in K[X]$. Să se arate că:
a) dacă $\operatorname{grad} f = 1$ atunci f este ireductibil;
b) dacă $\operatorname{grad} f \in \{2, 3\}$ atunci f este ireductibil dacă şi numai dacă f nu are nici o rădăcină în K;
c) polinoamele ireductibile din $K[X]$ de grad 4 (sau mai mare) nu pot fi, în general, caracterizate ca la b);
d) polinomul X^2+1 este ireductibil în $\mathbb{Q}[X]$, dar polinomul $X^2+\widehat{1}$ nu este ireductibil în $\mathbb{Z}_5[X]$;
e) polinomul $X^3 + X + 1$ este ireductibil în $\mathbb{Z}_5[X]$.
Sunt adevărate afirmaţiile de la a) şi b) când K este doar domeniu de integritate?

5.11. i) Este $f = 6X + 12$ ireductibil în $\mathbb{Z}[X]$? Dar în $\mathbb{Q}[X]$?
ii) Fie $g \in \mathbb{Z}[X]$. Să se arate că g este ireductibil în $\mathbb{Z}[X]$ dacă şi numai dacă g este ireductibil în $\mathbb{Q}[X]$ şi primitiv în $\mathbb{Z}[X]$.
iii) Fie R un domeniu factorial şi K corpul fracţiilor lui R. Să se generalizeze punctul ii) la R şi la K.

5.12. Fie R un domeniu factorial. Să se arate că R este corp dacă şi numai dacă orice polinom de grad 1 din $R[X]$ este ireductibil în $R[X]$.

5.13. Să se determine elementele prime şi elementele ireductibile în: i) $(\mathbb{N}^*, \cdot)$; ii) $(\mathbb{Z}, +, \cdot)$; iii) $(\mathbb{C}[X], +, \cdot)$; iv) $(\mathbb{R}[X], +, \cdot)$.

5.14. Fie $f = 7X^4+2X^3+9X^2+5X-5$. Să se determine câtul şi restul împărţirii în $\mathbb{Z}[X]$ a polinomului f la polinomul: a) $X-1$; b) $X-2$; c) X^2+2X; d) X^2-3X+2; e) $X^3 + X + 1$; f) X^4.

5.15. Fie (R, δ) un domeniu euclidian ($\delta : R^* \to \mathbb{N}$) şi $a, b \in R$, $b \neq 0$. Să se arate că existenţa a două elemente $q, r \in R$ pentru care

$$a = bq + r, \text{ cu } r = 0 \text{ sau } \delta(r) < \delta(b)$$

nu implică, în general, unicitatea lor.

5.16. Să se arate că pentru orice $a, b \in \mathbb{Z}$, $b \neq 0$ există $q', r' \in \mathbb{Z}$ astfel încât

$$a = bq' + r' \text{ şi } |r'| \leq \frac{|b|}{2}.$$

Sunt q' şi r' unic determinaţi de condiţiile de mai sus?

5.17. Folosind algoritmul lui Euclid, să se determine:
a) $(4148, 7684)$ în $\mathbb{Z}$;
b) $(X^{18} - 1,\ X^{33} - 1)$ şi $(X^3 - 1,\ X^4 + X^3 + 2X^2 + X + 1)$ în $\mathbb{Q}[X]$.

5.18. Fie R un domeniu cu ideale principale şi $a, b, c \in R$. Să se arate că:

$$(a, b, c) = d \Rightarrow \exists u, v, t \in R:\ d = au + bv + ct;$$
$$(a, b, c) = 1 \Leftrightarrow \exists u, v, t \in R:\ 1 = au + bv + ct.$$

Să se generalizeze pentru n elemente.

5.19. Fie R un domeniu cu ideale principale şi $a, b, c \in R$, $a \neq 0 \neq b$. Să se arate că:
i) ecuaţia $ax + by = c$ are soluţii în $R \times R$ dacă şi numai dacă $(a, b)|c$;
ii) dacă (x_0, y_0) este o soluţie a ecuaţiei de mai sus atunci orice soluţie este de forma $\left(x_0 + \frac{b}{(a,b)}t, y_0 - \frac{a}{(a,b)}t\right)$ cu $t \in R$.

5.20. Să se determine:
i) $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ astfel încât $31x - 17y = 1$;
ii) $(x, y) \in \mathbb{N}^* \times \mathbb{N}^*$ astfel încât $31x - 17y = 1$.

5.21. Să se rezolve în $\mathbb{Z}$ următoarele sisteme de congruenţe:

$$a) \quad \begin{cases} x \equiv 2 (\operatorname{mod} 7) \\ x \equiv 3 (\operatorname{mod} 6) \end{cases} ; \qquad b) \quad \begin{cases} 3x \equiv 2 (\operatorname{mod} 5) \\ x \equiv 6 (\operatorname{mod} 7) \\ x \equiv 1 (\operatorname{mod} 6) \end{cases} .$$

5.22. Fie $a, b, c, d, m, n \in \mathbb{Z}$. Să se arate că dacă sunt verificate condiţiile

$$(a, b) = 1, \ (m, a) = 1, \ (n, b) = 1$$

atunci congruenţele $mx \equiv c (\operatorname{mod} a)$ şi $ny \equiv d (\operatorname{mod} b)$ au o soluţie comună în $\mathbb{Z}$.

5.23. (*Teorema chineză a resturilor pentru k congruenţe*) Fie numerele întregi a_1, a_2, $\ldots$, a_k două câte două prime între ele. Să se arate că oricare ar fi $c_1, c_2, \ldots, c_k \in \mathbb{Z}$ congruenţele $x \equiv c_i (\operatorname{mod} a_i)$ $(i = 1, \ldots, k)$ au o soluţie comună, unică modulo $a_1 a_2 \cdots a_k$.

5.24. Să se arate că congruenţa $mx \equiv c(\operatorname{mod} a)$ are soluţii în $\mathbb{Z}$ dacă şi numai dacă $(m, a)|c$, iar în acest caz are exact (m, a) soluţii necongruente modulo a.

5.25. 1) Să se arate că rezolvarea ecuaţiei $x^2 + y^2 = z^2$ în $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ se poate reduce la cazul când numerele x şi y sunt prime între ele.
2) Fie $x, y, z \in \mathbb{Z}$ astfel încât $x^2 + y^2 = z^2$ şi $(x, y) = 1$. Să se arate că x şi y nu pot fi ambele impare, iar dacă y este par atunci există $m, n \in \mathbb{Z}$ astfel încât

$$x = m^2 - n^2, \ y = 2mn \text{ şi } z = m^2 + n^2.$$

5.26. Fie $d \in \mathbb{Z} \setminus \{1\}$ liber de pătrate, $\delta : \mathbb{Z}[\sqrt{d}] \to \mathbb{N}$, $\delta(z) = |z \cdot \overline{z}|$. Să se arate că pentru orice $z_1, z_2, z \in \mathbb{Z}[\sqrt{d}]$ avem:
i) dacă $z_1|z_2$ atunci $\delta(z_1)|\delta(z_2)$;
ii) $z_1 \sim z_2$ dacă şi numai dacă $\delta(z_1) = \delta(z_2)$ şi $z_1|z_2$;
iii) $\delta(z_1) = \delta(z_2)$ nu implică, în general, $z_1 \sim z_2$;
iv) dacă $\delta(z)$ este un număr prim atunci z este element ireductibil în $\mathbb{Z}[\sqrt{d}]$.

5.27. Să se arate că inelul întregilor lui Gauss $(\mathbb{Z}[i], +, \cdot)$ este un domeniu euclidian şi să se determine:
a) c.m.m.d.c. şi c.m.m.m.c. al numerelor $z_1 = 12 - 3i$ şi $z_2 = 3 + 6i$ în $\mathbb{Z}[i]$;
b) câte un generator pentru fiecare dintre idealele $(z_1) \cap (z_2)$ şi (z_1, z_2).

5.28. Fie $p, q \in \mathbb{Z}$ cu $|p| + |q| < 3$, $\theta \in \mathbb{C}$ o soluţie a ecuaţiei $x^2 + px + q = 0$, subinelul

$$\mathbb{Z}[\theta] = \{a + b\theta \mid a, b \in \mathbb{Z}\}$$

al lui $\mathbb{C}$ şi funcţia $\delta : \mathbb{Z}[\theta] \to \mathbb{N}$, $\delta(z) = |z \cdot \overline{z}|$. Să se arate că $(\mathbb{Z}[\theta], \delta)$ este un domeniu euclidian.

5.29. Scrieţi toate domeniile euclidiene care se obţin din problema anterioară.

5.30. Să se arate că inelele $\mathbb{Z}\left[\dfrac{1+i\sqrt{7}}{2}\right]$ şi $\mathbb{Z}\left[\dfrac{1+i\sqrt{11}}{2}\right]$ sunt euclidiene.

5.31. Fie U un ideal nenul al inelului întregilor lui Gauss. Să se arate că inelul cât $\mathbb{Z}[i]/U$ este finit.

5.32. 1) Să se arate că în $(\mathbb{Z}[i], +, \cdot)$ au loc următoarele:
a) 2, 5 şi 17 nu sunt elemente ireductibile;
b) 3 şi 7 sunt elemente ireductibile;
c) $1 + i$ şi $1 + 2i$ sunt elemente ireductibile.
2) Să se scrie numerele 4 şi $18 + 36i$ ca produs de elemente ireductibile din $\mathbb{Z}[i]$.

5.33. Să se arate că:
a) orice element prim din $\mathbb{Z}[i]$ este un divizor al unui număr prim din $\mathbb{Z}$;
b) dacă p este un număr prim şi $p \equiv 3 (\text{mod } 4)$ atunci p este ireductibil în $\mathbb{Z}[i]$;
c) dacă p este un număr prim şi $p \equiv 1 (\text{mod } 4)$ atunci p este produsul a două elemente conjugate ireductibile în $\mathbb{Z}[i]$ care nu sunt asociate în divizibilitate;
d) orice element ireductibil din $\mathbb{Z}[i]$ este asociat în divizibilitate cu $1 + i$ sau cu un număr (natural) prim de forma $4k + 3$ sau cu un element ireductibil în $\mathbb{Z}[i]$ care divide un număr (natural) prim de forma $4k + 1$.

5.34. Să se arate că în $(\mathbb{Z}[i\sqrt{5}], +, \cdot)$ au loc următoarele:
a) 3 este element ireductibil, dar nu este element prim;
b) 6 şi $2(1 + i\sqrt{5})$ nu au un c.m.m.d.c.;
c) 3 şi $1 + i\sqrt{5}$ au un c.m.m.d.c.

5.35. Fie R domeniu euclidian, $a, b \in R$ relativ prime şi $m, n \in \mathbb{N}$. Să se arate că

$$(a^m - b^m, a^n - b^n) = a^{(m,n)} - b^{(m,n)}.$$

5.36. (*Criteriul lui Eisenstein*) Fie $n \in \mathbb{N}^*$ şi $f = a_0 + \cdots + a_{n-1}X^{n-1} + a_nX^n$ un polinom primitiv din $\mathbb{Z}[X]$. Să se arate că dacă există un număr prim p cu proprietatea că $p \,|\, a_0, \ldots, p \,|\, a_{n-1}$ şi p^2 nu divide pe a_0 atunci polinomul f este ireductibil peste $\mathbb{Z}$.

5.37. Să se arate că în $\mathbb{Z}[X]$ există polinoame ireductibile de orice grad $n \geq 0$, iar în $\mathbb{Q}[X]$ există polinoame ireductibile de orice grad $n \geq 1$.

5.38. Fie R un domeniu de integritate, $a, b \in R$, a inversabil şi $f \in R[X]$. Să se arate că f este ireductibil dacă şi numai dacă $f(aX + b)$ este ireductibil.

5.39. Fie p un număr prim. Să se arate că polinomul

$$f = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Z}[X]$$

este ireductibil peste $\mathbb{Q}$.

5.40. Să se arate că următoarele polinoame cu coeficienţi întregi sunt ireductibile în $\mathbb{Q}[X]$: a) $X^5 + 5X^4 + 10X^3 - 15X^2 + 15X - 20$; b) $X^{2^n} + 1$ ($n \in \mathbb{N}^*$); c) $X^{p^n} + p - 1$ (p prim, $n \in \mathbb{N}$).

5.41. Să se descompună în factori ireductibili în $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ şi în $\mathbb{C}[X]$ următoarele polinoame: i) $40X^2 - 20X$; ii) $10X^2 + 5X - 5$; iii) $X^3 - 8$; iv) $X^3 + 8$; v) $X^4 - 1$; vi) $x^4 + 1$; vii) $X^6 - 1$; viii) $X^6 + 1$; ix) $X^8 - 1$; x) $X^8 + 1$.

5.42. Să se descompună polinomul $X^4 - 5X^2 + 6$ în factori ireductibili peste $\mathbb{Q}$, peste $\mathbb{Q}(\sqrt{2})$ şi peste $\mathbb{R}$.

5.43. Fie p un număr prim şi $f = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n$ un polinom cu coeficienti întregi. Polinomul $\widehat{a_0} + \widehat{a_1}X + \cdots + \widehat{a_{n-1}}X^{n-1} + X^n$ se numeşte *redusul modulo p al lui f*. Să se arate că:
a) dacă f este reductibil peste $\mathbb{Z}$ atunci fiecare factor al lui f se reduce modulo p la un polinom de acelaşi grad din $\mathbb{Z}_p[X]$;
b) dacă redusul modulo p al lui f este ireductibil peste $\mathbb{Z}_p$ atunci f este ireductibil peste $\mathbb{Q}$.

5.44. Folosind problema anterioară, să se studieze care din următoarele polinoame sunt ireductibile peste $\mathbb{Q}$:

$$f = X^3 + 6X^2 + 5X + 25,\ g = X^3 + 6X^2 + 11X + 8,\ h = X^4 + 8X^3 + X^2 + 2X + 5.$$

5.45. Fie K un corp comutativ, $f = a_0 + a_1X + \cdots + a_nX^n \in K[X]$ şi

$$g = a_n + a_{n-1}X + \cdots + a_0X^n.$$

Să se arate că dacă f este ireductibil în $K[X]$ atunci şi g este ireductibil.

5.46. Să se arate că $\mathbb{Z}[X]$ este un domeniu factorial, dar are ideale care nu sunt principale.

5.47. Să se arate că $\mathbb{R}[X]$ este un domeniu cu ideale principale, dar $\mathbb{R}[X, Y]$ are ideale care nu sunt principale.

5.48. Fie K un corp comutativ. Să se arate că idealul (X^2, XY, Y^2) nu este principal în $K[X, Y]$ şi că inelul cât $K[X, Y]/\,(X^2, XY, Y^2)$ are ideale care nu sunt principale. Poate fi generat idealul (X^2, XY, Y^2) al lui $K[X, Y]$ cu două elemente?

5.49. Să se descompună în factori irductibili în $\mathbb{Q}[X, Y]$ polinoamele: i) $X^3 - Y^3$; ii) $Y^4 - X^2$; iii) $X^2 - Y^6$; iv) $X^7 + 2X^3Y + 3X^2 + 9Y$ şi să se demonstreze ireductibilitatea fiecărui factor.

5.50. Fie K un corp comutativ.
i) Să se arate că un polinom omogen $f = aX^2+bXY+cY^2 \in K[X,Y]$ este ireductibil în $K[X,Y]$ dacă şi numai dacă $a \neq 0$ şi $g = aX^2 + bX + c$ este ireductibil în $K[X]$.
ii) Să se generalizeze i) pentru polinoamele omogene de grad $n \geq 2$ din $K[X,Y]$.
iii) Să se arate că factorii ireductibili ai unui polinom omogen din $K[X,Y]$ sunt polinoame omogene.

5.51. Să se arate că în $\mathbb{Z}[i]$:
a) există o infinitate de ideale prime;
b) idealele (3) şi $(1+i)$ sunt prime;
c) idealul (2) nu este prim.

5.52. În inelul $4\mathbb{Z}$ idealul generat de 8 este maximal, dar inelul cât corespunzător nu este un corp.

5.53. Să se arate că într-un inel Boole nenul un ideal este maximal dacă şi numai dacă este prim.

5.54. Să se arate că idealul generat de X este ideal prim în $\mathbb{Z}[X]$ dar nu este ideal maximal.

5.55. Să se arate că idealul generat de X este ideal maximal în $\mathbb{Q}[X]$.

5.56. Fie $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Să se arate că idealul (n, X) al lui $\mathbb{Z}[X]$ este prim dacă şi numai dacă n este număr prim.

5.57. Să se arate că idealele (X, Y) şi $(X-2, Y-3)$ sunt maximale în $\mathbb{C}[X,Y]$.

5.58. Să se arate că idealele $(Y-3)$ şi (X^2+1) sunt prime în $\mathbb{Q}[X,Y]$. Sunt ele maximale?

5.59. Sunt idealele (X^2) şi (X^2-1) prime în $\mathbb{Q}[X]$? Dar maximale?

5.60. Fie R un inel nenul, asociativ, comutativ, cu unitate. Să se arate că un ideal $M \neq R$ al său este maximal dacă şi numai dacă pentru orice $x \in R \setminus M$ există $r \in R$ astfel încât $1 - rx \in M$.

5.61. Un *inel* R se numeşte *local* dacă are un singur ideal maximal. Fie R un inel asociativ, comutativ cu unitate. Să se arate că:
1) R este corp dacă şi numai dacă $R^2 \neq \{0\}$ şi $\{0\}$ este (singurul) ideal maximal al lui R;
2) următoarele condiţii sunt echivalente:
  i) R este inel local;
  ii) elementele neinversabile din R formează un ideal;
  iii) suma a două elemente neinversabile din R este un element neinversabil.

5.62. Fie R un domeniu de integritate, $P \neq R$ un ideal prim al lui R, $S = R \setminus P$ şi K corpul fracţiilor lui R. Să se arate că:
i) $\{ab^{-1} \mid a \in R,\, b \in S\}$ este subinel al lui K şi că acest subinel coincide cu inelul de fracţii R_S;
ii) inelul R_S este local;
iii) $A = \left\{\dfrac{a}{b} \mid a, b \in \mathbb{Z},\, b \text{ impar}\right\}$ este subinel al lui $\mathbb{Q}$ şi inelul A este local.

5.63. Să se arate dacă R este un inel comutativ local atunci inelul seriilor formale $R[[X]]$ este local.

Capitolul 6

Spaţii vectoriale

6.1. Fie V un K-spaţiu vectorial, $V \neq \{0\}$, $\alpha, \beta \in K$ şi $u, v \in V$. Care din următoarele afirmaţii:
a) $\alpha u = \alpha v \Rightarrow u = v$,
b) $\alpha u = \beta u \Rightarrow \alpha = \beta$,
c) $\alpha \neq 0$ şi $\alpha u = \alpha v \Rightarrow u = v$,
d) $u \neq 0$ şi $\alpha u = \beta u \Rightarrow \alpha = \beta$,
e) $\alpha u = 0 \Rightarrow \alpha = 0$ sau $u = 0$
sunt adevărate?

6.2. Arătaţi că grupul abelian $(\mathbb{R}_+^*, \cdot)$ este $\mathbb{R}$-spaţiu vectorial în raport cu operaţia externă $*$ definită prin

$$\alpha * x = x^\alpha,\ \alpha \in \mathbb{R},\ x \in \mathbb{R}_+^*$$

şi că acest spaţiu vectorial este izomorf cu $\mathbb{R}$-spaţiul vectorial definit pe $\mathbb{R}$ de operaţiile uzuale de adunare şi înmulţire.

6.3. Fie K un corp comutativ, $V = K \times K$, fie $(x, y), (x', y') \in V$ şi $\alpha \in K$. Este V un K-spaţiu vectorial în raport cu operaţiile definite astfel:
i) $(x, y) + (x', y') = (x + x', y + y'),\ \alpha(x, y) = \begin{cases} (0,0) & , \text{ dacă } \alpha = 0; \\ (\alpha x, \alpha^{-1} y) & , \text{ dacă } \alpha \neq 0? \end{cases}$
ii) $(x, y) + (x', y') = (x + 2x', y + 3y'),\ \alpha(x, y) = (\alpha x, \alpha y)$?
iii) $(x, y) + (x', y') = (x + x', y + y'),\ \alpha(x, y) = (x, 0)$?
Justificaţi răspunsul.

6.4. Fie V un K-spaţiu vectorial şi M o mulţime. Să se arate că V^M este K-spaţiu vectorial în raport cu operaţiile definite punctual în V^M, adică

$$(f + g)(x) = f(x) + g(x),\ (\alpha f)(x) = \alpha f(x),\ \forall f, g \in V^M,\ \forall \alpha \in K.$$

6.5. Fie $(V, +)$ un grup abelian, $V \neq \{0\}$, K un corp şi $\alpha \in K$. Să se arate că:
i) dacă $(V, +)$ este un K-spaţiu vectorial şi $t_\alpha : V \to V$, $t_\alpha(x) = \alpha x$ atunci $t_\alpha \in End(V, +)$ şi aplicaţia $\varphi : K \to End(V, +)$, $\varphi(\alpha) = t_\alpha$ este omomorfism injectiv de inele;
ii) dacă $\varphi : K \to End(V, +)$ este omomorfism injectiv de inele atunci grupul $(V, +)$ este K-spaţiu vectorial în raport cu operaţia externă definită prin $\alpha x = (\varphi(\alpha))(x)$;
iii) există o bijecţie între operaţiile externe pe V cu domeniul de operatori K cu proprietatea că înzestrează grupul $(V, +)$ cu o structură de K-spaţiu vectorial şi omomorfismele injective de inele între K şi $End(V, +)$.

6.6. Fie $(V, +)$ un grup abelian şi K un corp. Să se arate că există o structură de K-spaţiu vectorial pe $(V, +)$ dacă şi numai dacă inelul $(End(V, +)+, \circ)$ are un subinel care este corp izomorf cu K.

6.7. Să se arate că oricare ar fi K un corp nu există nici o structură de K-spaţiu vectorial pe grupul $(\mathbb{Z}, +)$.

6.8. Fie K un corp. Să se arate că există pe grupul $(\mathbb{Q}, +)$ o structură de K-spaţiu vectorial dacă şi numai dacă corpurile K şi $\mathbb{Q}$ sunt izomorfe.

6.9. Fie K un corp şi $V \neq \{0\}$ un K-spaţiu vectorial. Să se arate că ordinul fiecărui element $v \in V \setminus \{0\}$ în grupul $(V, +)$ coincide cu caracteristica lui K.

6.10. Poate fi organizată o mulţime finită ca un spaţiu vectorial peste un corp infinit?

6.11. Să se arate că grupul $(\mathbb{Q}, +)$ nu poate fi organizat ca un spaţiu vectorial peste corpul numerelor reale.

6.12. Să se definească o structură de $\mathbb{Z}_2$-spaţiu vectorial pe grupul lui Klein.

6.13. a) Fie p un număr prim şi $n \in \mathbb{N}^*$. Să se dea câte un exemplu de spaţiu vectorial cu câte: i) 2 vectori; ii) 4 vectori; iii) 2^n vectori; iv) p^n vectori.
b) Fie m un număr natural care nu este de forma p^n cu $n \in \mathbb{N}$ şi p număr prim. Există spaţii vectoriale cu m elemente?

6.14. Fie K un corp comutativ şi $n \in \mathbb{N}$. Să se arate că

$$P_n(K) = \{f \in K[X] \mid \operatorname{grad} f \leq n\}$$

este un subspaţiu al K-spaţiului vectorial $K[X]$, iar $\{f \in K[X] \mid \operatorname{grad} f = n\}$ şi $\{f \in K[X] \mid \operatorname{grad} f \geq n\}$ nu sunt subspaţii.

6.15. Fie V un K-spaţiu vectorial şi S un subspaţiu al lui V. Este $C_V S = V \setminus S$ un subspaţiu al lui V? Dar $C_V S \cup \{0\}$?

6.16. Fie V un K-spaţiu vectorial şi $S \subseteq V$. Să se arate că S este un subspaţiu al lui V dacă şi numai dacă $S \neq \emptyset$ şi $\alpha \in K$, $x, y \in S$ implică $\alpha x + y \in S$.

6.17. Fie V un K-spaţiu vectorial, S un subspaţiu al lui V şi $x, y \in V$. Notăm $\langle S, x\rangle = \langle S \cup \{x\}\rangle$. Să se arate că dacă $x \in V \setminus S$ şi $x \in \langle S, y\rangle$ atunci $y \in \langle S, x\rangle$.

6.18. Fie V un K-spaţiu vectorial, $\alpha, \beta, \gamma \in K$ şi $x, y, z \in V$ astfel încât $\alpha\gamma \neq 0$ şi $\alpha x + \beta y + \gamma z = 0$. Să se arate că $\langle x, y\rangle = \langle y, z\rangle$.

6.19. Fie K un corp comutativ, $n \in \mathbb{N}$ şi S un subspaţiu al K-spaţiului vectorial $K[X]$ care conţine câte un polinom de grad i pentru orice $i \in \{0, 1, \ldots, n\}$ dar nu conţine nici un polinom de grad mai mare ca n. Să se arate că $S = P_n(K)$.

6.20. Formează polinoamele $f_1 = 3X + 2$, $f_2 = 4X^2 - X + 1$, $f_3 = X^3 - X^2 + 3$ un sistem de generatori pentru $\mathbb{R}$-spaţiul vectorial $P_3(\mathbb{R}) = \{f \in \mathbb{R}[X] \mid \operatorname{grad} f \leq 3\}$? Justificaţi răspunsul.

6.21. Fie V_1, V_2 substaţii ale unui spaţiu vectorial V. Să se arate că următoarele afirmaţii sunt echivalente: a) $V_1 \cup V_2$ este subspaţiu al lui V; b) $V_1 + V_2 = V_1 \cup V_2$; c) $V_1 \subseteq V_2$ sau $V_2 \subseteq V_1$.

6.22. Să se arate că laticea subspaţiilor unui spaţiu vectorial este modulară, dar nu este, în general, distributivă.

6.23. Fie V un K-spaţiu vectorial şi $A_1, \dots, A_n$ ($n \in \mathbb{N}^*$) subspaţii ale lui V. Să se arate că $V = A_1 + \dots + A_n$ dacă şi numai dacă funcţia

$$f : A_1 \times \dots \times A_n \to V, \ f(a_1, \dots, a_n) = a_1 + \dots + a_n$$

este surjectivă. Ce condiţie trebuie să îndeplinească f pentru a avea loc egalitatea $V = A_1 \oplus \dots \oplus A_n$?

6.24. Să se arate că proprietatea unui subspaţiu de a fi sumand direct este tranzitivă.

6.25. Să se arate că un subspaţiu al unui spaţiu vectorial V poate avea doi complemenţi direcţi diferiţi în V.

6.26. În $\mathbb{R}$-spaţiul vectorial $\mathbb{R}^{\mathbb{R}} = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$ considerăm

$$(\mathbb{R}^{\mathbb{R}})_i = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ este impară}\}, \ (\mathbb{R}^{\mathbb{R}})_p = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ este pară}\}.$$

Să se arate că $(\mathbb{R}^{\mathbb{R}})_i$ şi $(\mathbb{R}^{\mathbb{R}})_p$ sunt subspaţii ale lui $\mathbb{R}^{\mathbb{R}}$ şi că $\mathbb{R}^{\mathbb{R}} = (\mathbb{R}^{\mathbb{R}})_i \oplus (\mathbb{R}^{\mathbb{R}})_p$.

6.27. Să se arate că subspaţiile lui $\mathbb{R}^2$ sunt $\{0\}$ şi

$$V_{a,b} = \{(x, y) \in \mathbb{R}^2 \mid ax + by = 0\}, \text{ cu } a, b \in \mathbb{R}.$$

Să se dea interpretarea geometrică. Când are loc egalitatea $V_{a,b} = V_{a',b'}$? Dar $\mathbb{R}^2 = V_{a,b} \oplus V_{a',b'}$?

6.28. Să se arate că subspaţiile $\mathbb{R}$-spaţiului vectorial $\mathbb{R}^3$ sunt

$$V_{a,b,c} = \{(at, bt, ct) \mid t \in \mathbb{R}\} \text{ şi } W_{a,b,c} = \{(x, y, z) \in \mathbb{R}^3 \mid ax + by + cz = 0\},$$

cu $a, b, c \in \mathbb{R}$. Să se dea interpretarea geometrică. Când are loc egalitatea $\mathbb{R}^3 = V_{a,b,c} \oplus V_{a',b',c'} \oplus V_{a'',b'',c''}$? Dar $\mathbb{R}^3 = V_{a,b,c} \oplus W_{a',b',c'}$?

6.29. Fie V, V' două K-spaţii vectoriale. Să se arate că o funcţie $f : V \to V'$ este o transformare liniară dacă şi numai dacă $f(\alpha x + y) = \alpha f(x) + f(y)$ pentru orice $\alpha \in K$ şi $x, y \in V$.

6.30. Fie V, V_1, V_2 K-spaţii vectoriale. Să se arate că pentru orice transformare liniară f de la produsul direct $V_1 \times V_2$ la V există două transformări liniare unic determinate $g : V_1 \to V$, $h : V_2 \to V$ astfel încât $f(x_1, x_2) = g(x_1) + h(x_2)$, pentru orice $x_1 \in V_1$, $x_2 \in V_2$.

6.31. Fie V, V_1, V_2 K-spaţii vectoriale, două funcţii $f : V \to V_1$, $g : V \to V_2$ şi $h : V \to V_1 \times V_2$, $h(x) = (f(x), g(x))$. Să se arate că h este o transformare liniară dacă şi numai dacă f şi g sunt transformări liniare. Generalizare.

6.32. a) Fie $m \in \mathbb{N}^*$ şi $f : \mathbb{R}^m \to \mathbb{R}$. Să se arate că f este o transformare liniară de $\mathbb{R}$-spaţii vectoriale dacă şi numai dacă există $a_1, \ldots, a_m \in \mathbb{R}$, unic determinate, astfel încât $f(x_1, \ldots, x_m) = a_1x_1 + \cdots + a_mx_m$, pentru orice $(x_1, \ldots, x_m) \in \mathbb{R}^m$.
b) Să se determine tranformările liniare $f : \mathbb{R}^m \to \mathbb{R}^n$ $(n \in \mathbb{N}^*)$.

6.33. Să se arate că există o transformare liniară $f : \mathbb{R}^2 \to \mathbb{R}^2$ astfel încât $f(1,1) = (2,5)$ şi $f(1,0) = (1,4)$. Să se determine $f(2,3)$. Este f izomorfism?

6.34. Există o transformare liniară $f : \mathbb{R}^3 \to \mathbb{R}^2$ astfel încât $f(1,0,3) = (1,1)$ şi $f(-2,0,-6) = (2,1)$?

6.35. Fie V un K-spaţiu vectorial şi S un sumand direct al lui V. Să se arate că toţi complemenţii direcţi ai lui S sunt izomorfi.

6.36. Fie V un K-spaţiu vectorial, $\mathcal{P}_l(V)$ şi $\mathcal{P}'_l(V)$, mulţimea submulţimilor libere, respectiv legate, ale lui V şi $X, Y \subseteq V$. Care din următoarele afirmaţii:
a) $X, Y \in \mathcal{P}_l(V) \Rightarrow X \cup Y \in \mathcal{P}_l(V)$,
b) $X, Y \in \mathcal{P}_l(V) \Rightarrow X \cap Y \in \mathcal{P}_l(V)$,
c) $X, Y \in \mathcal{P}'_l(V) \Rightarrow X \cup Y \in \mathcal{P}'_l(V)$,
d) $X, Y \in \mathcal{P}'_l(V) \Rightarrow X \cap Y \in \mathcal{P}'_l(V)$,
e) $\{0\} \in \mathcal{P}_l(V)$,
f) $\{0\} \in \mathcal{P}'_l(V)$,
g) $V \in \mathcal{P}_l(V)$,
h) $V \in \mathcal{P}'_l(V)$,
i) $x \in V,\ x \neq 0 \Rightarrow \{x\} \in \mathcal{P}_l(V)$,
j) $x \in V,\ x \neq 0 \Rightarrow \{x\} \in \mathcal{P}'_l(V)$,
k) $X, Y \in \mathcal{P}_l(V),\ X \subseteq Y \Rightarrow Y \in \mathcal{P}_l(V)$,
l) $X, Y \in \mathcal{P}'_l(V),\ X \subseteq Y \Rightarrow Y \in \mathcal{P}'_l(V)$,
m) $Y \in \mathcal{P}_l(V),\ X \subseteq Y \Rightarrow X \in \mathcal{P}_l(V)$,
n) $Y \in \mathcal{P}'_l(V),\ X \subseteq Y \Rightarrow X \in \mathcal{P}'_l(V)$,
o) $\emptyset \in \mathcal{P}_l(V)$
sunt adevărate?

6.37. Fie V un K-spaţiu vectorial şi $X, Y \subseteq V$. Să se arate că:
i) $\langle X \cup Y \rangle = \langle X \rangle + \langle Y \rangle$;
ii) $\langle X \cap Y \rangle \subseteq \langle X \rangle \cap \langle Y \rangle$ şi daţi un exemplu pentru care are loc egalitatea şi unul pentru care nu are loc egalitatea;
iii) dacă $X \cap Y = \emptyset$ şi $X \cup Y$ este liberă atunci $\langle X \cup Y \rangle = \langle X \rangle \oplus \langle Y \rangle$.

6.38. Fie K un corp comutativ, $V_1 = K[X^2]$ şi V_2 submulţimea lui $K[X]$ formată din polinomul nul şi polinoamele care au în scrierea algebrică coeficienţii puterilor pare ale lui X egali cu 0. Să se arate că V_1 şi V_2 sunt subspaţii ale lui $K[X]$ şi $K[X] = V_1 \oplus V_2$.

6.39. a) Fie $a, b, c \in \mathbb{R}$ şi polinoamele $f_1 = (X-b)(X-c)$, $f_2 = (X-c)(X-a)$, $f_3 = (X-a)(X-b)$. Să se arate că:
i) vectorii f_1, f_2, f_3 sunt liniar independenţi în $\mathbb{R}$-spaţiul vectorial $\mathbb{R}[X]$ dacă şi numai dacă $(a-b)(b-c)(c-a) \neq 0$;
ii) dacă $(a-b)(b-c)(c-a) \neq 0$ atunci pentru orice $f \in \mathbb{R}[X]$ cu grad $f \leq 2$ există $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$, unic determinate, astfel încât $f = \lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3$.
b) Să se determine $\lambda_1, \lambda_2, \lambda_3$ când $f = 1 + 2X - X^2$, $a = 1$, $b = 2$ şi $c = 3$.

6.40. Fie V un $\mathbb{R}$-spaţiu vectorial şi $v_1, v_2, v_3 \in V$. Să se arate că $\langle v_1, v_2, v_3 \rangle = \langle v_2 + v_3, v_3 + v_1, v_1 + v_2 \rangle$ şi că vectorii v_1, v_2, v_3 sunt liniar independenţi dacă şi numai dacă vectorii $v_2 + v_3, v_3 + v_1, v_1 + v_2$ sunt liniar independenţi. Este această proprietate adevărată într-un spaţiu vectorial peste un corp oarecare K?

6.41. Fie $n \in \mathbb{N}$ şi $f_n : \mathbb{R} \to \mathbb{R}$, $f_n(x) = \sin^n x$. Să se arate că $L = \{f_n \mid n \in \mathbb{N}\}$ este o submulţime liberă a $\mathbb{R}$-spaţiului vectorial $\mathbb{R}^{\mathbb{R}}$.

6.42. Fie $\lambda_1, \ldots, \lambda_n \in \mathbb{R}^*$ ($n \in \mathbb{N}^*$) cu $|\lambda_i| \neq |\lambda_j|$ pentru orice $i, j \in \{1, \ldots, n\}$, $i \neq j$ şi funcţiile $f_i : \mathbb{R} \to \mathbb{R}$, $f_i(x) = \sin(\lambda_i x)$, $i \in \{1, \ldots, n\}$. Să se arate că $f_1, \ldots, f_n$ sunt vectori liniar independenţi ai $\mathbb{R}$-spaţiului vectorial $\mathbb{R}^{\mathbb{R}}$.

6.43. Să se dea o condiţie necesară şi suficientă pentru ca vectorii $v_1 = (a_1, b_1)$, $v_2 = (a_2, b_2)$ să formeze o bază a lui $\mathbb{R}^2$. Să se interpreteze geometric această condiţie. Folosind condiţia stabilită, găsiţi o infinitate de baze ale lui $\mathbb{R}^2$. Există o bază a lui $\mathbb{R}^2$ în care coordonatele unui vector $v = (x, y)$ să coincidă cu x şi y? Să se arate că $v_1 = (1, 0)$ şi $v_2 = (1, 1)$ formează o bază a lui $\mathbb{R}^2$ şi să se găsească coordonatele lui $v = (x, y)$ în această bază.

6.44. Să se arate că vectorii $(1, 2, -1)$, $(3, 2, 4)$, $(-1, 2, -6)$ din $\mathbb{R}^3$ sunt liniar dependenţi şi să se găsească o relaţie de dependenţă între ei.

6.45. Să se determine $a \in \mathbb{R}$ astfel încât vectorii $v_1 = (a, 1, 1)$, $v_2 = (1, a, 1)$, $v_3 = (1, 1, a)$ să formeze o bază a lui $\mathbb{R}^3$.

6.46. Formulaţi şi rezolvaţi în cazul lui $\mathbb{R}^3$ o problemă analogă cu problema **6.43**.

6.47. Care dintre următoarele submulţimi ale lui $\mathbb{R}^3$:
a) $\{(1, 0, -1), (2, 5, 1), (0, -4, 3)\}$;
b) $\{(2, -4, 1), (0, 3, -1), (6, 0, 1)\}$;
c) $\{(1, 2, -1), (1, 0, 3), (2, 1, 1)\}$;
d) $\{(-1, 3, 1), (2, -4, -3), (-3, 8, 2)\}$;
e) $\{(1, -3, -2), (-3, 1, 3), (-2, -10, -2)\}$
sunt baze ale $\mathbb{R}$-spaţiului vectorial $\mathbb{R}^3$?

6.48. Fie $n \in \mathbb{N}^*$. Să se arate că vectorii

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

formează o bază a $\mathbb{R}$-spaţiului vectorial $\mathbb{R}^n$ şi să se scrie coordonatele vectorului $(x_1, \ldots, x_n)$ în această bază.

6.49. Să se arate că în $\mathbb{R}$-spaţiul vectorial $M_2(\mathbb{R})$ matricele

$$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ E_2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix},\ E_3 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},\ E_4 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

formează o bază şi să se determine coordonatele matricei $A = \begin{pmatrix} -2 & 3 \\ 4 & -2 \end{pmatrix}$ în această bază.

6.50. Fie $m, n \in \mathbb{N}^*$. Există o bază a lui $M_{m,n}(\mathbb{R})$ în care coordonatele unei matrice coincid cu elementele sale?

6.51. Fie K un corp comutativ şi $n \in \mathbb{N}^*$. Să se arate că pentru orice matrice $A \in M_n(K)$ există $m \in \mathbb{N}^*$, $m \leq n^2$ şi $a_0, a_1, \ldots, a_{m-1} \in K$ astfel încât

$$a_0 I_n + a_1 A + \cdots + a_{m-1} A^{m-1} + A^m = O_n.$$

6.52. a) Există o bază a lui $\mathbb{R}[X]$ în care coordonatele unui polinom să coincidă cu coeficienţii săi?
b) Să se arate că polinoamele $(X-a)^n \in \mathbb{R}[X]$, cu $n \in \mathbb{N}$, formează o bază a lui $\mathbb{R}[X]$ şi să se determine coordonatele unui polinom $f \in \mathbb{R}[X]$ în această bază.

6.53. a) Exisă o bază a $\mathbb{R}$-spaţiului vectorial $\mathbb{C}$ în care coordonatele lui $z = a + bi$ $(a, b \in \mathbb{R})$ să fie a, b?
b) Să se găsească o condiţie necesară şi suficientă pentru ca numerele complexe $z_1 = a_1 + b_1 i$, $z_2 = a_2 + b_2 i$ $(a_1, a_2, b_1, b_2 \in \mathbb{R})$ să formeze o bază a lui $\mathbb{C}$ peste $\mathbb{R}$.

6.54. Fie $p \in \mathbb{N}$ un număr prim. Să se arate că operaţiile uzuale de adunare şi înmulţire înzestrează pe $V = \{a + b\sqrt[3]{p} + c\sqrt[3]{p^2} \mid a, b, c \in \mathbb{Q}\}$ cu o structură de $\mathbb{Q}$-spaţiu vectorial şi să se determine o bază şi dimensiunea acestui spaţiu vectorial.

6.55. Fie V un K-spaţiu vectorial, X o mulţime. Să se arate că:
i) V^X este un K-spaţiu vectorial în raport cu operaţiile definite punctual;
ii) $V^{(X)} = \{f \in V^X \mid \operatorname{supp} f \text{ finit}\}$ este un subspaţiu al lui V^X;
iii) Dacă X este infinită şi $V \neq \{0\}$ atunci V^X şi $V^{(X)}$ sunt de dimensiune infinită.

6.56. Fie V un spaţiu vectorial, V_1, V_2 subspaţii ale lui V şi $X_1 \subseteq V_1$, $X_2 \subseteq V_2$. Să se arate că:
i) dacă $V = V_1 \oplus V_2$ şi X_i este bază a lui V_i $(i = 1, 2)$ atunci $X_1 \cap X_2 = \emptyset$ şi $X_1 \cup X_2$ este o bază a lui V;
ii) dacă $X_1 \cap X_2 = \emptyset$, X_i generează pe V_i $(i = 1, 2)$ şi $X_1 \cup X_2$ este o bază a lui V atunci X_i este bază a lui V_i $(i = 1, 2)$ şi $V = V_1 \oplus V_2$.

6.57. Fie K un corp, K' un subcorp al lui K şi V un K-spaţiu vectorial de dimensiune $n \in \mathbb{N}$. Să se arate că, folosind operaţiile din corpul K şi faptul că K' este subcorp în K, grupul $(K, +)$ poate fi organizat ca un spaţiu vectorial peste K' şi că dacă $\dim_{K'} K = m$ $(m \in \mathbb{N}^*)$ atunci $\dim_{K'} V = mn$.

6.58. Să se determine numărul bazelor ordonate ale următoarelor spaţii vectoriale: a) ${}_{Z_2}(Z_2)^2$; b) ${}_{Z_2}(Z_2)^3$; c) ${}_{Z_3}(Z_3)^2$; d) ${}_{Z_3}(Z_3)^3$.

6.59. Fie K un corp finit cu q elemente şi V un K-spaţiu vectorial de dimensiune $n \in \mathbb{N}^*$. Să se determine numărul bazelor ordonate ale lui V.

6.60. Fie K un corp finit cu q elemente şi $n \in \mathbb{N}^*$. Să se determine ordinul grupului $GL_n(K)$.

6.61. Fie K un corp finit cu q elemente, V un K-spaţiu vectorial de dimensiune $n \in \mathbb{N}^*$, $k \in \{0, 1, \ldots, n\}$ şi $G_n^k(q)$ numărul subspaţiilor lui V care au dimensiunea k. Numerele $G_n^k(q)$ se numesc *numerele lui Gauss* asociate lui V. Să se arate că:
i) $G_n^0(q) = 1 = G_n^n(q)$;
ii) $G_n^k(q) = \dfrac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}$, pentru $k \in \{1, \ldots, n-1\}$;
iii) $G_n^k(q) = G_n^{n-k}(q)$, pentru $k \in \{0, 1, \ldots, n\}$;
iv) $G_n^k(q) = q^k G_{n-1}^k(q) + G_{n-1}^{k-1}(q)$, pentru $k \in \{1, \ldots, n-1\}$.

6.62. Daţi un exemplu de subspaţiu propriu S al unui K-spaţiu vectorial V care are aceeaşi dimensiune cu spaţiul V. Poate fi dimensiunea lui V finită?

6.63. Fie V un K-spaţiu vectorial de dimensiune 3 şi V_1, V_2 două subspaţii diferite de dimensiune 2. Să se arate că $V_1 \cap V_2$ are dimensiunea 1. Care este semnificaţia geometrică în cazul $K = \mathbb{R}$, $V = \mathbb{R}^2$?

6.64. Fie V un K-spaţiu vectorial de dimensiune $n \in \mathbb{N}^*$ şi V_1, V_2 subspaţii ale lui V. Să se arate că dacă $\dim V_1 = n-1$ şi $V_2 \nsubseteq V_1$ atunci $\dim(V_1 \cap V_2) = \dim V_2 - 1$ şi $V_1 + V_2 = V$.

6.65. Fie V un K-spaţiu vectorial de dimensiune finită şi V_1, V_2 subspaţii ale lui V care verifică egalitatea $\dim(V_1 + V_2) = \dim(V_1 \cap V_2) + 1$. Să se arate că $V_1 \subseteq V_2$ sau $V_2 \subseteq V_1$.

6.66. Fie V un K-spaţiu vectorial de dimensiune finită şi V_1, V_2, S_1, S_2 subspaţii ale lui V astfel încât $V = V_1 \oplus V_2 = S_1 \oplus S_2$. Să se arate că

$$\dim(V/(V_1 \cap S_1)) \leq \dim V_2 + \dim S_2.$$

6.67. Fie f şi g endomorfisme ale unui K-spaţiu vectorial V de dimensiune finită. Dacă $f + g$ este un automorfism al lui V şi $f \circ g$ este endomorfismul nul atunci $\dim V = \dim f(V) + \dim g(V)$.

6.68. Fie K un corp comutativ, $V = M_2(K)$,

$$V_1 = \left\{ \begin{pmatrix} a & b \\ c & a \end{pmatrix} \mid a, b, c \in K \right\},\ V_2 = \left\{ \begin{pmatrix} 0 & a \\ -a & b \end{pmatrix} \mid a, b \in K \right\}.$$

Să se arate că V_1 şi V_2 sunt subspaţii ale lui V şi să se găsească dimensiunile lui V_1, V_2, $V_1 + V_2$ şi $V_1 \cap V_2$.

6.69. În $\mathbb{Q}$-spaţiul vectorial $\mathbb{Q}^3$ considerăm vectorii

$$a = (-2, 1, 3),\ b = (3, -2, -1),\ c = (1, -1, 2),\ d = (-5, 3, 4),\ e = (-9, 5, 10).$$

Să se arate că $\langle a, b \rangle = \langle c, d, e \rangle$.

6.70. În $\mathbb{R}$-spaţiul vecorial $\mathbb{R}^4$ se consideră subspaţiile generate astfel:
a) $S = \langle u_1, u_2 \rangle$, cu $u_1 = (1, 2, 1, 0)$, $u_2 = (-1, 1, 1, 1)$,
$T = \langle v_1, v_2 \rangle$, cu $v_1 = (2, -1, 0, 1)$, $v_2 = (1, -1, 3, 7)$;
b) $S = \langle u_1, u_2 \rangle$, cu $u_1 = (1, 1, 0, 0)$, $u_2 = (1, 0, 1, 1)$,

$T = \langle v_1, v_2 \rangle$, cu $v_1 = (0, 0, 1, 1)$, $v_2 = (0, 1, 1, 0)$;
c) $S = \langle u_1, u_2, u_3 \rangle$, cu $u_1 = (1, 2, -1, -2)$, $u_2 = (3, 1, 1, 1)$, $u_3 = (-1, 0, 1, -1)$,
$T = \langle v_1, v_2 \rangle$, cu $v_1 = (-1, 2, -7, -3)$, $v_2 = (2, 5, -6, -5)$;
d) $S = \langle u_1, u_2, u_3 \rangle$, cu $u_1 = (1, 2, 1, -2)$, $u_2 = (2, 3, 1, 0)$, $u_3 = (1, 2, 2, -3)$,
$T = \langle v_1, v_2, v_3 \rangle$, cu $v_1 = (1, 1, 1, 1)$, $v_2 = (1, 0, 1, -1)$, $v_3 = (1, 3, 0, -3)$.
Să se determine câte o bază şi dimensiunea subspaţiilor S, T, $S + T$ şi $S \cap T$.

6.71. Fie V_1, V_2 două K-spaţii vectoriale de dimensiune finită cu $\dim V_1 = \dim V_2$ şi $f : V_1 \to V_2$ o transformare liniară. Să se arate că următoarele afirmaţii sunt echivalente: i) f este injectivă; ii) f este surjectivă; iii) f este izomorfism.

6.72. Să se arate că, în cazul spaţiilor vectoriale de dimensiune infinită, condiţiile din problema anterioară nu sunt echivalente.

6.73. Fie $P_2(\mathbb{R}) = \{f \in \mathbb{R}[X] \mid \operatorname{grad} f \leq 2\}$ şi $\varphi : P_2(\mathbb{R}) \to M_2(\mathbb{R})$,

$$\varphi(f) = \begin{pmatrix} f(1) - f(2) & 0 \\ 0 & f(0) \end{pmatrix}.$$

Să se arate că φ este liniară şi să se determine dimensiunile lui $\mathrm{Im}\varphi$ şi $\mathrm{Ker}\varphi$.

6.74. Fie $\varphi \in \mathbb{R}$. Să se arate că rotaţia în plan de unghi φ, adică funcţia $f : \mathbb{R}^2 \to \mathbb{R}^2$, $f(x, y) = (x \cos\varphi - y \sin\varphi, x \sin\varphi + y \cos\varphi)$, este automorfism al lui $\mathbb{R}^2$. Să se scrie matricea lui f în baza canonică a lui $\mathbb{R}^2$ (adică în baza (e_1, e_2), cu $e_1 = (1, 0)$, $e_2 = (0, 1)$).

6.75. Să se arate că funcţiile $f : \mathbb{R}^2 \to \mathbb{R}^2$, $f(x, y) = (x, -y)$ (simetria în raport cu axa Ox) şi $g : \mathbb{R}^2 \to \mathbb{R}^2$, $f(x, y) = (-x, y)$ (simetria în raport cu axa Oy) sunt automorfisme ale lui $\mathbb{R}^2$. Să se scrie matricele lui f, g, $f - g$, $f + 2g$ şi $g \circ f$ în baza canonică.

6.76. Fie $f : \mathbb{R}^2 \to \mathbb{R}^3$, $f(x, y) = (x + y, 2x - y, 3x + 2y)$, $v = ((1, 2), (-2, 1))$ şi $v' = ((1, -1, 0), (-1, 0, 1), (1, 1, 1))$, Să se arate că v, respectiv v' este bază în $\mathbb{R}^2$, respectiv $\mathbb{R}^3$ şi să se scrie matricea lui f în perechea de baze (v, v').

6.77. Fie $f : \mathbb{R}^3 \to \mathbb{R}^4$ aplicaţia liniară definită pe baza canonică astfel:

$$f(e_1) = (1, 2, 3, 4),\ f(e_2) = (4, 3, 2, 1),\ f(e_3) = (-2, 1, 4, 1).$$

Să se determine:
i) $f(v)$ pentru orice $v \in \mathbb{R}^3$;
ii) matricea lui f în bazele canonice;
iii) câte o bază în $\mathrm{Im}\, f$ şi $\mathrm{Ker}\, f$.

6.78. Să se arate că fiecare dintre mulţimile de vectori $\{v_1, v_2, v_3\}$ şi $\{v'_1, v'_2, v'_3\}$ cu $v_1 = (1, 2, 1)$, $v_2 = (2, 3, 3)$, $v_3 = (3, 7, 1)$ şi $v'_1 = (3, 1, 4)$, $v'_2 = (5, 2, 1)$, $v'_3 = (1, 1, -6)$ formează câte o bază a lui $\mathbb{R}^3$ şi să se găsească legătura dintre coordonatele unui vector scris în cele două baze.

6.79. Fie $v = (v_1, v_2, v_3, v_4)$ o bază a $\mathbb{R}$-spaţiului vectorial $\mathbb{R}^4$, vectorii $u_1 = v_1$, $u_2 = v_1 + v_2$, $u_3 = v_1 + v_2 + v_3$, $u_4 = v_1 + v_2 + v_3 + v_4$ şi $f \in End_{\mathbb{R}}(\mathbb{R}^4)$ cu

$$[f]_v = \begin{pmatrix} 1 & 2 & 0 & 1 \\ 3 & 0 & -1 & 2 \\ 2 & 5 & 3 & 1 \\ 1 & 2 & 1 & 3 \end{pmatrix}.$$

Să se arate că $u = (u_1, u_2, u_3, u_4)$ este o bază a lui $\mathbb{R}^4$ şi să se scrie matricea $[f]_u$.

6.80. Fie V un spaţiu vectorial real, $v = (v_1, v_2, v_3)$ o bază a lui V, vectorii $u_1 = v_1 + 2v_2 + v_3$, $u_2 = v_1 + v_2 + 2v_3$, $u_3 = v_1 + v_2$ şi $f \in End_{\mathbb{R}}(V)$. Să se arate că $u = (u_1, u_2, u_3)$ este o bază a lui V şi să se scrie matricea lui $[f]_v$ ştiind că

$$[f]_u = \begin{pmatrix} 1 & 1 & 3 \\ 0 & 5 & -1 \\ 2 & 7 & -3 \end{pmatrix}.$$

6.81. Fie $P_2(\mathbb{R}) = \{f \in \mathbb{R}[X] \mid \operatorname{grad} f \leq 2\}$. Să se arate că $\varphi : P_2(\mathbb{R}) \to P_2(\mathbb{R})$, $\varphi(a_0 + a_1X + a_2X^2) = a_0 + a_1 + (a_1 + a_2)X + (a_0 + a_2)X^2$ este o transformare liniară şi să se determine $[f]_b$ şi $[f]_{b'}$ unde $b = (1, X, X^2)$ şi $b' = (1, X - 1, X^2 + 1)$.

6.82. Fie V, V' două $\mathbb{R}$-spaţii vectoriale, $a = (a_1, a_2, a_3)$, $b = (b_1, b_2, b_3)$ câte o bază în V, respectiv V' şi $f : V \to V'$ o transformare liniară a cărei matrice în perechea de baze (a, b) este

$$[f]_{a,b} = \begin{pmatrix} -1 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Să se determine:
i) $f(v)$ pentru orice $v \in V$;
ii) dimensiunea spaţiilor vectoriale $\operatorname{Im} f$ şi $\operatorname{Ker} f$;
iii) matricea $[f]_{a',b'}$, unde $a' = (a_1, a_1 + a_2, a_1 + a_2 + a_3)$ şi $b' = (b_1, b_1 + b_2, b_1 + b_2 + b_3)$.

6.83. Fie $S = \{(x, 2x) \mid x \in \mathbb{R}\}$.
i) Să se arate că S este subspaţiu al $\mathbb{R}$-spaţiului vectorial $\mathbb{R}^2$ şi să se reprezinte geometric elementele sale.
ii) Să se determine spaţiul cât $\mathbb{R}^2/S$ şi să se reprezinte geometric elementele sale.
iii) Să se determine câte o bază în S şi în $\mathbb{R}^2/S$.

6.84. Să se determine spaţiile cât ale lui $\mathbb{R}^2$ şi să se interpreteze geometric.

6.85. Fie $S = \{(t, 2t, 3t) \mid t \in \mathbb{R}\}$ şi $T = \{(x, y, z) \mid x + y + z = 1\}$.
i) Să se arate că S şi T sunt subspaţii ale lui $\mathbb{R}^3$ şi să se reprezinte geometric elementele lor.
ii) Să se determine $S \cap T$ şi $S + T$.
iii) Să se determine spaţiile cât $\mathbb{R}^3/S$ şi $\mathbb{R}^3/T$. Interpretare geometrică.
iv) Să se determine câte o bază în S, T, $\mathbb{R}^3/S$ şi $\mathbb{R}^3/T$.

6.86. Să se determine spaţiile cât ale lui $\mathbb{R}^3$ şi să se interpreteze geometric.

6.87. Fie V, V' $\mathbb{R}$-spaţii vectoriale, $v = (v_1, v_2, v_3)$ o bază în V, $v' = (v_1', v_2', v_3')$ o bază în V' şi $f : V \to V'$ transformarea liniară cu

$$[f]_{v,v'} = \begin{pmatrix} 0 & -1 & 5 \\ 1 & 0 & 0 \\ 0 & 1 & -5 \end{pmatrix}.$$

Să se determine:
i) dimensiunea şi câte o bază pentru $\operatorname{Im} f$ şi $\operatorname{Ker} f$;
ii) dimensiunea şi câte o bază pentru $V/\operatorname{Ker} f$ şi $V'/\operatorname{Im} f$;
iii) $[f]_{v,e'}$ în cazul în care $V' = \mathbb{R}^3$, $v_1' = (1,0,0)$, $v_2' = (0,1,1)$, $v_3' = (0,0,1)$ şi e' este baza canonică a lui $\mathbb{R}^3$;
iv) $f(x)$ pentru $x = 2v_1 - v_2 + 3v_3$, în condiţiile de la iii).

6.88. Fie $f \in End_{\mathbb{Q}}(\mathbb{Q}^4)$ pentru care matricea în baza canonică este

$$a) \begin{pmatrix} 1 & 2 & 1 & 2 \\ 3 & 2 & 3 & 2 \\ -1 & -3 & 0 & 4 \\ 0 & 4 & -1 & -3 \end{pmatrix}; \quad b) \begin{pmatrix} 0 & 1 & 2 & 3 \\ -1 & 2 & 1 & 0 \\ 3 & 0 & -1 & -2 \\ 5 & -3 & -1 & 1 \end{pmatrix}.$$

Să se determine câte o bază în $\operatorname{Ker} f$, $\operatorname{Im} f$, $\operatorname{Ker} f + \operatorname{Im} f$ şi $\operatorname{Ker} f \cap \operatorname{Im} f$.

6.89. Fie K un corp comutativ, $m, n \in \mathbb{N}^*$, $AX = B$ un sistem liniar de m ecuaţii cu n necunoscute scris sub formă matriceală, $AX = O_{m,1}$ sistemul liniar şi omogen asociat şi $r = \operatorname{rang} A$. Să se arate că mulţimea S_0 a soluţiilor sistemului omogen formează un subspaţiu de dimensiune $n - r$ al lui K^n, iar mulţiea S_B a soluţiilor sistemului $AX = B$ se obţine din S_0 astfel: $S_B = s + S_0$, unde $s \in K^n$ este o soluţie a lui $AX = B$. O bază a lui S_0 se numeşte *sistem fundamental de soluţii* al sistemului liniar şi omogen $AX = O_{m,1}$.

6.90. Fie $K = \mathbb{R}$. Să se verifice egalitatea $S_B = s + S_0$ din problema precdentă în cazul sistemului de ecuaţii:

$$\begin{cases} 2x_1 + x_2 - x_3 - x_4 + x_5 = 1 \\ x_1 - x_2 + x_3 + x_4 - 2x_5 = 0 \\ 3x_1 + 3x_2 - 3x_3 - 3x_4 + 4x_5 = 2 \end{cases}$$

şi să se determine un sistem fundamental de soluţii pentru sistemul liniar omogen asociat.

6.91. Să se determine câte un sistem fundamental de soluţii pentru sistemele:

$$a) \begin{cases} 2x_1 + x_2 - 4x_3 = 0 \\ 3x_1 + 5x_2 - 7x_3 = 0 \\ 4x_1 - 5x_2 - 6x_3 = 0 \end{cases}; \quad b) \begin{cases} 2x_1 - 4x_2 + 5x_3 + 3x_4 = 0 \\ 3x_1 - 6x_2 + 4x_3 + 2x_4 = 0 \\ 4x_1 - 8x_2 + 17x_3 + 11x_4 = 0 \end{cases}$$

şi să se completeze până la o bază a lui $\mathbb{R}^3$, respectiv $\mathbb{R}^4$.

6.92. Fie p un număr prim şi V un $\mathbb{Z}_p$-spaţiu vectorial cu $\dim_{\mathbb{Z}_p} V = 1$. Să se determine cardinalul mulţimii $End_{\mathbb{Z}_p}(V)$.

6.93. a) Să se arate că dacă V, V' sunt $\mathbb{Q}$-spaţii vectoriale atunci o *funcţie* $f : V \to V'$ este liniară dacă şi numai dacă este *aditivă*, adică $f(x + y) = f(x) + f(y)$ pentru orice $x, y \in V$.
b) Să se arate că există o funcţie aditivă $f : \mathbb{R} \to \mathbb{R}$ care nu este $\mathbb{R}$-liniară.

6.94. Fie V_1, V_2 K-spaţii vectoriale şi $f : V_1 \to V_2$ o transformare liniară. Să se arate că următoarele afirmaţii sunt echivalente:
a) f este surjectivă;
b) există o transformare liniară $s : V_2 \to V_1$ astfel încât $f \circ s = 1_{V_2}$;
c) dacă V este un K-spaţiu vectorial şi $\alpha, \beta : V \to V_1$ sunt transformări liniare atunci $\alpha \circ \beta = h \circ f$ implică $\alpha = \beta$.

6.95. a) Fie V_1, V_2, V_3 K-spaţii vectoriale, $f : V_2 \to V_3$, $g : V_1 \to V_3$ transformări liniare şi f surjectivă. Să se arate că există o transformare liniară $h : V_1 \to V_2$ astfel încât diagrama

$$\begin{tikzcd} V_3 & V_1 \arrow[l, "g"'] \arrow[dl, dotted, "h"] \\ V_2 \arrow[u, "f"] & \end{tikzcd}$$

să fie comutativă, adică $g = f \circ h$.
b) Fie $f : \mathbb{R}^3 \to \mathbb{R}^2$, $f(x, y, z) = (2x - y, z)$. Să se arate că f este o transformare liniară surjectivă şi să se găsească o transformare liniară $h : \mathbb{R}^2 \to \mathbb{R}^3$ astfel încât

$$f \circ h = 1_{\mathbb{R}^2}.$$

Să se scrie matricele lui f şi h în bazele canonice.

6.96. Fie V_1, V_2 K-spaţii vectoriale şi $f : V_1 \to V_2$ o transformare liniară. Să se arate că următoarele afirmaţii sunt echivalente:
a) f este injectivă;
b) există o transformare liniară $r : V_2 \to V_1$ astfel încât $r \circ f = 1_{V_1}$;
c) dacă V este un K-spaţiu vectorial şi $\alpha, \beta : V \to V_1$ sunt transformări liniare atunci $f \circ \alpha = f \circ \beta$ implică $\alpha = \beta$.

6.97. a) Fie V_1, V_2, V_3 K-spaţii vectoriale, $f : V_1 \to V_2$, $g : V_1 \to V_3$ transformări liniare şi f injectivă. Să se arate că există o transformare liniară $h : V_2 \to V_3$ astfel încât diagrama

$$\begin{tikzcd} V_1 \arrow[r, "f"] \arrow[d, "g"'] & V_2 \arrow[dl, dotted, "h"] \\ V_3 & \end{tikzcd}$$

să fie comutativă, adică $g = h \circ f$.
b) Fie $f : \mathbb{R}^2 \to \mathbb{R}^3$, $f(x, y) = (x - y, x + y, 2x)$. Să se arate că f este o transformare liniară injectivă şi să se găsească o transformare liniară $h : \mathbb{R}^3 \to \mathbb{R}^2$ astfel încât

$$h \circ f = 1_{\mathbb{R}^2}.$$

Să se scrie matricele lui f şi h în bazele canonice.

6.98. Fie V un K-spaţiu vectorial şi $f \in End_K(V)$.
a) Să se arate că f este element inversabil în inelul $(End_K(V), +, \circ)$ dacă şi numai dacă f nu este divizor al lui zero în $(End_K(V), +, \circ)$.
b) Să se demonstreze că dacă $\dim V < \infty$ atunci are loc echivalenţa condiţiilor: i) f nu este divizor al lui zero în inelul $(End_K(V), +, \circ)$; ii) f este inversabilă la stânga; iii) f este inversabilă la dreapta; iv) f este inversabilă.

6.99. Fie K un corp comutativ, $n \in \mathbb{N}^*$ şi $A \in M_n(K)$. Să se demonstreze echivalenţa condiţiilor: i) A nu este divizor al lui zero în inelul $M_n(K)$; ii) A este inversabilă la stânga; iii) A este inversabilă la dreapta; iv) A este inversabilă.

6.100. Fie K corp comutativ, $m, n \in \mathbb{N}^*$, $A \in M_{m,n}(K)$. Să se demonstreze că:
i) $\exists B \in M_{n,m}(K) : \ BA = I_m \Leftrightarrow \text{rang}A = n$;
ii) $\exists B \in M_{n,m}(K) : \ AB = I_n \Leftrightarrow \text{rang}A = m$.

6.101. Fie K un corp comutativ şi V, V' K-spaţii vectoriale. Să se arate că:
i) dacă unul dintre spaţiile V, V' este de dimensiune infinită, iar celălalt este nenul atunci spaţiul vectorial $Hom_K(V, V')$ are dimensiunea infinită;
ii) dacă $\dim V' = m$, $\dim V = n$ $(m, n \in \mathbb{N}^*)$ atunci $\dim Hom_K(V, V') = mn$;
iii) dacă $V' = K$ şi $\dim V = n$, $n \in \mathbb{N}^*$ atunci spaţiul vectorial $V^* = Hom_K(V, K)$ este izomorf cu V. Spaţiul V^* se numeşte *dualul* lui V, iar o transformare din V^* se numeşte *formă liniară*;
iv) dacă $e = (e_1, \dots, e_n)$ este o bază a lui V atunci formele liniare

$$e_i^* : V \to K, \ e_i^*(e_j) = \delta_{ij} = \begin{cases} 1, & \text{dacă } i = j \\ 0, & \text{dacă } i \neq j \end{cases} \ (i = 1, \dots, n)$$

formează o bază a lui V^*, numită *duala bazei* e.

6.102. Fie K un corp comutativ şi $n \in \mathbb{N}^*$. Să se arate că dacă $f : K^n \to K$ este o formă liniară atunci există $a_i \in K$ $(i = 1, \dots, n)$ astfel încât

$$f(x_1, \dots, x_n) = a_1 x_1 + \cdots + a_n x_n.$$

Să se determine coordonatele lui f în duala bazei canonice a lui K^n şi în duala bazei $e'_1 = (1, 0, \dots, 0)$, $e'_2 = (1, 1, 0, \dots, 0)$, $e'_n = (1, 1, \dots, 1)$.

6.103. Fie K un corp comutativ, V_1, V_2, V_3 spaţii vectoriale peste K şi $f : V_1 \to V_2$ o transformare liniară. Să se arate că:
i) funcţia $f^* : V_2^* = Hom_K(V_2, K) \to V_1^* = Hom_K(V_1, K)$, $f^*(h) = h \circ f$, numită *duala lui* f, este liniară;
ii) dacă şi $g : V_2 \to V_3$ este liniară atunci $(g \circ f)^* = f^* \circ g^*$;
iii) dacă f este injectivă (surjectivă) atunci f^* este surjectivă (injectivă);
iv) dacă f este izomorfism atunci f^* este izomorfism.

Fie K un corp comutativ, $n \in \mathbb{N}^*$ şi $V, V_1, \dots, V_n$ K-spaţii vectoriale. O *funcţie* $f : V_1 \times \cdots \times V_n \to V$ se numeşte *n-liniară* sau *(K-)multiliniară* dacă f este liniară în fiecare variabilă adică pentru orice $i \in \{1, \dots, n\}$ şi orice $v_1 \in V_1, \dots, v_{i-1} \in V_{i-1}$, $v_{i+1} \in V_{i+1}, \dots$, $v_n \in V_n$ fixaţi funcţia

$$f(v_1, \dots, v_{i-1}, -, v_{i+1}, \dots, v_n) : V_i \to V, \ x \mapsto f(v_1, \dots, v_{i-1}, x, v_{i+1}, \dots, v_n)$$

este liniară. Dacă $n = 2$ atunci f se numeşte *funcţie biliniară.* Dacă $V = K$ atunci f se numeşte *formă n-liniară.* Dacă $V = K$ şi $n = 2$ atunci f se numeşte *formă biliniară.* O *funcţie (formă) n-liniară* $f : V \times \cdots \times V \to V'$ ($f : V \times \cdots \times V \to K$) care satisface condiţia

$$v_i = v_j,\ i \neq j \Rightarrow f(v_1, \ldots, v_n) = 0$$

se numeşte *alternă.* Din proprietăţile determinantului rezultă că determinantul de ordinul n este o formă n-liniară alternă atât de liniile cât şi de coloanele sale.

6.104. Fie K corp comutativ şi $n \in \mathbb{N}^*$. Să se arate că:
i) $f : K^n \to K,\ f(x_1, \ldots, x_n) = x_1 \cdots x_n$ este o formă n-liniară;
ii) $f : K^n \times K^n \to K,\ f((x_1, \ldots, x_n), (y_1, \ldots, y_n)) = x_1y_1 + \cdots + x_ny_n$ este o formă biliniară.

6.105. Fie K corp comutativ. Să se arate că:
i) dacă $a_{11}, a_{12}, a_{21}, a_{22} \in K$ atunci $f : K^2 \times K^2 \to K$ definită prin

$$(*) \qquad f((x_1, x_2), (y_1, y_2)) = a_{11}x_1y_1 + a_{12}x_1y_2 + a_{21}x_2y_1 + a_{22}x_2y_2$$

este o formă biliniară;
ii) dacă $f : K^2 \times K^2 \to K$este o formă biliniară atunci există $a_{11}, a_{12}, a_{21}, a_{22} \in K$ astfel încât f să fie definită prin $(*)$. Generalizare.

6.106. Fie K un corp comutativ, $n \in \mathbb{N}^*$, V, V' K-spaţii vectoriale şi fie $f : V \times \cdots \times V \to V'$ o funcţie n-multiliniară. Să se arate că dacă

$$v_i = v_{i+1}\ (i \in \{1, \ldots, n-1\}) \Rightarrow f(v_1, \ldots, v_n) = 0$$

atunci f este alternă.

6.107. 1) Fie K un corp comutativ de caracteristică diferită de 2 şi fie $f : V \times \cdots \times V \to V'$ o funcţie K-multiliniară. Să se arate că sunt echivalente afirmaţiile:
i) f este alternă;
ii) f este *antisimetrică*, adică $1 \leq i < j \leq n$ implică

$$f(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) = -f(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_n);$$

iii) pentru orice $\sigma \in S_n$, $f(v_1, \ldots, v_n) = (-1)^{\operatorname{inv}\sigma} f(v_{\sigma(1)}, \ldots, v_{\sigma(n)})$.
2) Rămân echivalente condiţiile de mai sus dacă corpul K are caracteristica 2?

6.108. Fie K un corp comutativ şi $n \in \mathbb{N}^*$. Privim coloanele unei matrice $A \in M_n(K)$ ca elemente din K^n şi identificăm pe $M_n(K)$ cu $(K^n)^n$. Să se arate întâi în cazul $n = 2$ şi pe urmă în cazul general că:
i) dacă $f : (K^n)^n \to K$ este o formă n-liniară alternă cu proprietatea că $f(I_n) = 1$ atunci $f(A) = \det A$ (am notat cu I_n matricea unitate, adică $I_n = (e_1, \ldots, e_n)$ unde $e_1, \ldots, e_n$ este baza canonică);
ii) pentru orice scalar $a \in K$ există o formă n-liniară alternă unică $f : (K^n)^n \to K$ astfel încât $f(I_n) = a$; această formă este definită prin $f(A) = a \det A$, adică

$$f(A) = f(I_n) \det A.$$

6.109. Fie K un corp comutativ, $m, n \in \mathbb{N}^*$, $A \in M_m(K)$, $B \in M_{m,n}(K)$, $C \in M_n(K)$ şi $O_{n,m}$ matricea nulă din $M_{n,m}(K)$. Folosind problema anterioară, să se arate că

$$\begin{vmatrix} A & B \\ O_{n,m} & C \end{vmatrix} = |A| \cdot |C|.$$

6.110. Fie K un corp comutativ, V un K-spaţiu vectorial şi $\mathcal{B}(V)$ mulţimea formelor biliniare $f : V \times V \to K$. Dacă $\dim V = n$ şi $v = (v_1, \ldots, v_n)$ este o bază ordonată a lui V, iar $f \in \mathcal{B}(V)$ atunci matricea $M_v(f) = (a_{ij}) \in M_n(K)$, unde $a_{ij} = f(v_i, v_j)$, se numeşte *matricea formei biliniare f în baza v*. Să se arate că:

i) $\mathcal{B}(V)$ este K-spaţiu vectorial în raport cu operaţiile definite punctual;

ii) dacă $A = M_v(f)$, $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, unde $x_1, \ldots, x_n$ sunt coordonatele lui $x \in V$ în baza v şi $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ este matricea analogă pentru $y \in V$ atunci

$$f(x, y) = {}^tX \cdot A \cdot Y,$$

unde ${}^tX$ este transpusa lui X;

iii) funcţia $\varphi_v : \mathcal{B}(V) \to M_n(K)$, $\varphi_v(f) = M_v(f)$ este izomorfism de spaţii vectoriale;

iv) $\dim \mathcal{B}(V) = n^2$;

v) dacă v şi w sunt baze ordonate ale lui V, S este matricea de trecere de la v la w, $A = M_v(f)$ şi $B = M_w(f)$ atunci $B = {}^tS \cdot A \cdot S$.

6.111. Să se arate că

$$f : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R},\ f((x_1, x_2), (y_1, y_2)) = 2x_1y_1 + 3x_1y_2 + 4x_2y_1 - x_2y_2$$

este o formă biliniară şi să se determine matricea lui f în baza canonică şi în baza $((1, 1), (1, -1))$.

6.112. Ştiind că $f : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ este forma biliniară care are în baza canonică matricea $A = \begin{pmatrix} 1 & 2 \\ -1 & 3 \end{pmatrix}$ să se determine $f((x_1, x_2), (y_1, y_2))$.

6.113. Să se arate că

$$f : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R},\ f((x_1, x_2, x_3), (y_1, y_2, y_3)) = x_1y_1 - 2x_1y_2 + x_2y_1 - x_3y_3$$

este biliniară şi să se determine matricea lui f în baza $((1, 0, 1), (1, 0, -1), (0, 1, 0))$.

6.114. Fie K un corp comutativ şi V un spaţiu vectorial peste K. O *formă biliniară* $f : V \times V \to K$ se numeşte *simetrică*, respectiv *antisimetrică* dacă $f(x, y) = f(y, x)$, respectiv $f(x, y) = -f(y, x)$ pentru orice $x, y \in V$. Dacă $\dim V = n$ ($n \in \mathbb{N}^*$) să se arate că sunt echivalente următoarele condiţii:

i) forma biliniară $f : V \times V \to K$ este simetrică (antisimetrică);

ii) pentru orice bază $v = (v_1, \ldots, v_n)$ a lui V matricea lui f în baza v este simetrică (antisimetrică);

iii) există o bază $v = (v_1, \ldots, v_n)$ a lui V în care matricea lui f este simetrică (antisimetrică).

6.115. Fie K un corp comutativ de caracteristică diferită de 2 şi V un K-spaţiu vectorial cu $\dim V = n \in \mathbb{N}^*$. Să se arate că:
i) pentru orice formă biliniară $f : V \times V \to K$ există o formă biliniară simetrică $f_s : V \times V \to K$ şi o formă biliniară antisimetrică $f_a : V \times V \to K$ astfel încât

$$f = f_s + f_a;$$

ii) pentru orice matrice $A \in M_n(K)$ există o matrice simetrică $A_s \in M_n(K)$ şi o matrice antisimetrică $A_a \in M_n(K)$ astfel încât $A = A_s + A_a$.

6.116. Fie V un K-spaţiu vectorial. O funcţie $q : V \to K$ se numeşte *formă pătratică* dacă există o formă biliniară simetrică $f : V \times V \to K$ astfel încât

$$q(x) = f(x, x), \ \forall x \in V.$$

Să se arate că dacă corpul K are caracteristica diferită de 2 atunci:
i) pentru orice formă pătratică $q : V \to K$ există o singură formă biliniară simetrică $f : V \times V \to K$ astfel încât $q(x) = f(x, x)$ pentru orice $x \in V$; această formă este numită *forma polară a lui* q şi este definită prin

$$f(x, y) = \frac{1}{2}[q(x + y) - q(x) - q(y)]; \tag{1}$$

ii) dacă $f : V \times V \to K$ este o formă biliniară simetrică şi nenulă atunci forma pătratică q asociată lui f este nenulă.

6.117. *Matricea unei forme pătratice* este, prin definiţie, matricea formei sale polare. Să se afle matricele următoarelor forme pătratice în bazele canonice:
1) $q_1 : \mathbb{R}^2 \to \mathbb{R},\ q_1(x, y) = 2x^2 + 3xy + 6y^2$;
2) $q_2 : \mathbb{R}^2 \to \mathbb{R},\ q_2(x, y) = 8xy + 4y^2$;
3) $q_3 : \mathbb{R}^3 \to \mathbb{R},\ q_3(x, y, z) = x^2 + 2xy + 4xz + 3y^2 + yz + 7z^2$;
4) $q_4 : \mathbb{R}^2 \to \mathbb{R},\ q_4(x, y) = 4xy$;
5) $q_5 : \mathbb{R}^3 \to \mathbb{R},\ q_5(x, y, z) = x^2 + 4xy + 4y^2 + 2xz + z^2 + 2yz$.

6.118. Fie K un corp comutativ, V un K-spaţiu vectorial de dimensiune n şi $f : V \times V \to K$ o *formă biliniară*. Se spune că f este *diagonalizabilă* dacă există o bază a lui V în care matricea lui f are forma diagonală. Să se arate că:
i) dacă f este diagonalizabilă atunci f este simetrică;
ii) dacă corpul K are caracteristica diferită de 2 atunci este adevărată şi reciproca lui i), adică f este simetrică implică f este diagonalizabilă.

6.119. Fie $A = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$ şi $B = \begin{pmatrix} 0 & 1 & 2 \\ 1 & -1 & 3 \\ 2 & 3 & 4 \end{pmatrix}$. Să se diagonalizeze următoarele forme biliniare
i) $f : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = {}^t xAy$, unde $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ şi $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$;
ii) $f : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$, $f(x, y) = {}^t xBy$, unde $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ şi $y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$.

6.120. Să se diagonalizeze formele pătratice asociate transformărilor biliniare din problema anterioară.

6.121. Să se diagonalizeze formele pătratice din problema **6.117**, prin completare la pătrate.

6.122. Să se arate că forma biliniară simetrică

$$f : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2,\ f(x, y) = x_1y_2 + x_2y_1,$$

unde $x = (x_1, x_2)$ şi $y = (y_1, y_2)$, nu este diagonalizabilă.

6.123. Fie K un corp comutativ, $n \in \mathbb{N}^*$ şi $A, B \in M_n(K)$. Să se arate că:
a) ${}^tA\,A$ şi $A\,{}^tA$ sunt simetrice;
b) dacă A este antisimetrică atunci A^2 este simetrică;
c) dacă A şi B sunt simetrice atunci AB este simetrică dacă şi numai dacă $AB = BA$;
d) dacă A şi B sunt ambele simetrice ori antisimetrice atunci $AB - BA$ este antisimetrică;
e) dacă A este simetrică şi B este antisimetrică atunci $AB - BA$ este simetrică;
f) dacă n este impar, K are caracteristica diferită de 2 şi A este antisimetrică atunci $\det A = 0$.

6.124. Fie K un corp de caracteristică 2, $n \in \mathbb{N}^*$ şi $A \in M_n(K)$. Să se arate că:
i) A este simetrică dacă şi numai dacă A este antisimetrică;
ii) matricea $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ nu se poate scrie sub formă de sumă dintre o matrice simetrică şi una antisimetrică.

6.125. Să se afle o submulţime infinită a lui $M_2(\mathbb{R})$ formată din matrice care au acelaşi polinom caracteristic.

6.126. Fie K un corp comutativ, $n \in \mathbb{N}^*$, $A \in M_n(K)$. Să se arate că matricea A şi transpusa sa ${}^tA$ au acelaşi polinom caracteristic.

6.127. Fie K un corp comutativ, $m, n \in \mathbb{N}^*$, $A \in M_n(K)$, $B \in M_{n,m}(K)$, $C \in M_m(K)$. Să se arate că polinomul caracteristic al matricei

$$M = \begin{pmatrix} A & O_{m,n} \\ B & C \end{pmatrix}$$

coincide cu produsul polinoamelor caracteristice ale lui A şi C.

6.128. Fie K un corp comutativ, $n \in \mathbb{N}^*$, $A, B \in M_n(K)$. Să se arate că dacă A sau B este inversabilă atunci polinoamele caracteristice ale matricelor AB şi BA coincid.

6.129. Să se determine matricele din $M_2(\mathbb{R})$ care au valorile proprii 1 şi -1.

6.130. Fie K un corp comutativ, $n \in \mathbb{N}$, $n \geq 2$ şi $A \in M_n(K)$. Să se arate că:
i) 0 este valoare proprie a lui A dacă şi numai dacă A este singulară, adică $\det A = 0$;
ii) dacă suma elementelor de pe fiecare linie a lui A este 1 atunci 1 este valoare proprie a lui A.

6.131. Fie K un corp comutativ, $n \in \mathbb{N}^*$ şi $A \in M_n(K)$. Să se arate că:
i) A este inversabilă dacă şi numai dacă 0 nu este valoare proprie a lui A şi în acest caz $p_{A^{-1}}(\lambda) = (-1)^n \lambda^n [p_A(0)]^{-1} p_A(\lambda^{-1})$;
ii) dacă A este inversabilă şi $\lambda \in K^*$ este valoare proprie a lui A atunci λ^{-1} este valoare proprie a lui A^{-1}.

6.132. Fie V un K-spaţiu vectorial şi $f \in Aut_K(V)$. Să se arate că valorile proprii ale lui f sunt nenule, apoi să se determine relaţia dintre valorile proprii ale lui f şi valorile proprii ale lui f^{-1} şi dintre vectorii proprii ai lui f şi vectorii proprii ai lui f^{-1}. Există endomorfisme care au toate valorile proprii nenule, dar nu sunt automorfisme?

6.133. Fie K un corp comutativ, $m \in \mathbb{N}^*$, $A \in M_m(K)$ şi

$$p = a_0 + a_1 X + \cdots + a_n X^n \in K[X].$$

Să se arate că dacă $\lambda \in K$ este valoare proprie a lui A atunci $p(\lambda)$ este valoare proprie pentru $p(A) = a_0 I_n + a_1 A + \cdots + a_n A^n$. În particular, dacă λ este valoare proprie a lui A atunci λ^n este valoare proprie pentru A^n.

6.134. Fie V un K-spaţiu vectorial, $p = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$ şi $f \in End_K(V)$. Să se arate că $p(f) = a_0 1_V + a_1 f + \cdots + a_n f^n \in End_K(V)$, iar dacă $\lambda \in K$ şi $x \in V$ sunt valoare, respectiv vector propriu pentru f atunci $p(\lambda)$ şi x sunt valoare, respectiv vector propriu pentru $p(f)$.

6.135. Fie K un corp comutativ, $n \in \mathbb{N}^*$, $A = (a_{ij}) \in M_n(K)$, $p_A = a_0 + a_1 X + \cdots + a_n X^n$ polinomul caracteristic şi $\lambda_1, \ldots, \lambda_n \in K$ valorile proprii ale lui A. Să se arate că:
i) $p_A = (a_{11} - X)(a_{22} - X) \cdots (a_{nn} - X) + q$, unde $\operatorname{grad} q \leq n - 2$;
ii) $a_n = (-1)^n,\ a_{n-1} = -1^{n-1}\operatorname{Tr}(A),\ a_0 = \det A$;
iii) $\lambda_1 + \cdots + \lambda_n = \operatorname{Tr}(A),\ \lambda_1 \cdots \lambda_n = (-1)^n \det A$;
iv) $a_{n-2} = (-1)^n \sum\limits_{i<j} \begin{vmatrix} a_{ii} & a_{ij} \\ a_{ji} & a_{jj} \end{vmatrix}$.

6.136. Fie K un corp comutativ, $n \in \mathbb{N}^*$, $A \in M_n(K)$, $f \in K[X]$, $m = \operatorname{grad} f$ şi b_m coeficientul lui X^m din f. Să se arate că:
i) dacă $x_1, \ldots, x_m$ sunt rădăcinile lui f atunci $\det f(A) = b_m^n p_A(x_1) \cdots p_A(x_m)$;
ii) dacă $\lambda_1, \ldots, \lambda_n$ sunt valorile proprii ale lui A atunci $\det f(A) = f(\lambda_1) \cdots f(\lambda_n)$ şi să se deducă de aici că valorile proprii ale lui $f(A)$ sunt $f(\lambda_1), \ldots, f(\lambda_n)$.

6.137. Fie V un $\mathbb{R}$-spaţiu vectorial, $v = (v_1, v_2, v_3, v_4)$ o bază a lui V şi f un endomorfism al lui V cu

$$[f]_v = \begin{pmatrix} 1 & 1 & 0 & 2 \\ 0 & -1 & 1 & 2 \\ 0 & 0 & 2 & 3 \\ 0 & 0 & 0 & -2 \end{pmatrix}.$$

a) Să se determine valorile proprii şi vectorii proprii ai lui f.
b) Să se arate că există o bază a lui V formată din vectori proprii ai lui f şi să se determine o astfel de bază.
c) Să se scrie matricea lui f în baza determinată la b).

6.138. Fie $v = (v_1, v_2, v_3, v_4)$ o bază a lui $\mathbb{R}^4$ şi $f \in End_{\mathbb{R}}(R^4)$ cu

$$[f]_v = \begin{pmatrix} 1 & 0 & 2 & -1 \\ 0 & 1 & 4 & -2 \\ 2 & -1 & 0 & 1 \\ 2 & -1 & -1 & 2 \end{pmatrix}.$$

Să se determine valorile proprii şi vectorii proprii ai lui f şi să se arate că $S = \langle v_1 + 2v_2, v_2 + v_3 + 2v_4 \rangle$ este un subspaţiu f-invariant al lui $\mathbb{R}^4$.

6.139. Fie K un corp comutativ, $n \in \mathbb{N}^*$, $A \in M_n(K)$. Să se arate că matricea A este similară cu o matrice triunghiulară din $M_n(K)$ (adică este *triangulabilă* în $M_n(K)$) dacă şi numai dacă polinomul caracteristic al lui A are toate rădăcinile (n rădăcini) în K.

6.140. Fie $f, g : \mathbb{R}^2 \to \mathbb{R}^2$ şi $h : \mathbb{R}^3 \to \mathbb{R}^3$ transformările liniare definite prin

$$f(x, y) = (-3x + 4y, 2x - y),\ g(x, y) = (x + y, x - y),$$
$$h(x, y, z) = (-x + 2y + 2z, 2x + 2y + 2z, -3x - 6y - 6z).$$

1) Să se determine:
i) polinoamele caracteristice ale lui f, g şi h;
ii) valorile proprii ale lui f, g şi h;
iii) subspaţiile proprii ale lui f, g şi h corspunzătoare fiecărei valori proprii.
2) Sunt f, g, h diagonalizabile? În caz afirmativ, să se determine câte o bază a lui $\mathbb{R}^2$, respectiv $\mathbb{R}^3$ în care matricele lui f, g, respetiv h sunt diagonale şi să se stabilească legătura dintre aceste matrice şi matricele $[f]_e$, $[g]_e$, $[h]_{e'}$, unde e este baza canonică a lui $\mathbb{R}^2$ şi e' este baza canonică a lui $\mathbb{R}^3$, iar după aceea să se afle $([f]_e)^n$, $([g]_e)^n$ şi $([h]_{e'})^n$ pentru $n \in \mathbb{N}$.

6.141. Pentru aplicaţiile liniare $f, g : \mathbb{R}^3 \to \mathbb{R}^3$ definite prin

$$f(x_1, x_2, x_3) = (3x_1 + 2x_2 + 2x_3, x_1 + 4x_2 + x_3, -2x_1 - 4x_2 - x_3),$$
$$g(x_1, x_2, x_3) = (4x_1 + 9x_2, -2x_2 + 8x_3, 7x_3)$$

se menţin cerinţele din problema anterioară.

6.142. Să se arate că aplicaţia liniară

$$f : \mathbb{R}^2 \to \mathbb{R}^2,\ f(x, y) = (3x + 2y, -2x + 3y)$$

nu este diagonalizabilă.

6.143. Să se arate că rotaţia de unghi φ, adică

$$f : \mathbb{R}^2 \to \mathbb{R}^2,\ f(x, y) = (x \cos\varphi - y \sin\varphi, x \sin\varphi + y \cos\varphi)$$

nu este diagonalizabilă.

6.144. Fie $A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ şi $B = \begin{pmatrix} 3 & 2 \\ -2 & 3 \end{pmatrix}$. Să se arate că:
i) A nu este diagonalizabilă în $M_n(\mathbb{Q})$, dar este diagonalizabilă în $M_2(\mathbb{R})$;
ii) B nu este diagonalizabilă în $M_n(\mathbb{R})$, dar este diagonalizabilă în $M_2(\mathbb{C})$.

6.145. Să se studieze dacă matricea

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -2 \\ 1 & 0 & -2 & 5 \end{pmatrix} \in M_4(\mathbb{R})$$

este diagonalizabilă. În caz afirmativ să se determine matricea diagonalizatoare, adică $S \in GL_4(\mathbb{R})$ pentru care $S^{-1}AS$ coincide cu forma diagonală, şi să se calculeze A^n ($n \in \mathbb{N}^*$).

6.146. Fie K un corp comutativ şi $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(K)$. Se cer:
i) polinomul caracteristic al lui A;
ii) $\det A = 0 \Rightarrow A^n = (a+d)^{n-1} \det A$;
iii) $\det A \neq 0 \Rightarrow A^{-1} = \dfrac{1}{\det A}(A - \mathrm{Tr}(A) \cdot I_2)$;
iv) dacă $K = \mathbb{R}$ şi $\Delta = (\mathrm{Tr}(A))^2 - 4 \det A$ atunci

A este diagonalizabilă în $M_2(\mathbb{R}) \Leftrightarrow \Delta > 0$ sau $\Delta = 0$ şi $A = aI_2$ ($a \in \mathbb{R}$),
A este diagonalizabilă în $M_2(\mathbb{C}) \Leftrightarrow \Delta \neq 0$ sau $\Delta = 0$ şi $A = aI_2$ ($a \in \mathbb{R}$).

6.147. Fie K un corp comutativ, V un K-spaţiu vectorial, $\dim V = n \in \mathbb{N}^*$ şi $f : V \to V$ un endomorfism liniar. Să se arate că:
i) dacă f are o singură valoare proprie în K atunci f este diagonalizabil dacă şi numai dacă există $\lambda \in K$ astfel încât $f(v) = \lambda v$, adică $f = \lambda \cdot 1_V$;
ii) dacă $A = (a_{ij}) \in M_n(K)$ are o singură valoare proprie în K atunci A este diagonalizabilă dacă şi numai dacă $A = \lambda I_n$, unde $\lambda \in K$;
iii) matricele $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, cu $a \in K^*$ nu sunt diagonalizabile.

6.148. Să se arate că dacă $A \in M_n(\mathbb{C})$ şi $\det A \neq 0$ atunci există $g \in \mathbb{C}[X]$ cu $\mathrm{grad}\, g \leq n - 1$ astfel încât $A^{-1} = g(A)$.

6.149. Folosind teorema Cayley-Hamilton, calculaţi $A^4 - 11A^2 + 22A$, unde

$$A = \begin{pmatrix} 0 & 0 & 2 \\ 2 & 1 & 0 \\ -1 & -1 & 3 \end{pmatrix}.$$

6.150. Fie $V = \mathbb{R}^4$ şi $f : V \to V$ transformarea liniară care are în baza canonică $e = (e_1, e_2, e_3, e_4)$ matricea

$$\text{a)} \quad [f]_e = \begin{pmatrix} 2 & -1 & 0 & 1 \\ 0 & 3 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 0 & 3 \end{pmatrix} = A\,; \ \text{b)} \quad [f]_e = \begin{pmatrix} 2 & -4 & 2 & 2 \\ -2 & 0 & 1 & 3 \\ -2 & -2 & 3 & 3 \\ -2 & -6 & 3 & 7 \end{pmatrix} = A.$$

Să se determine:
i) forma canonică Jordan J a lui A;
ii) o bază canonică Jordan a lui f, adică o bază v în care avem $J = [f]_v$;
iii) $S \in GL_4(\mathbb{R})$ pentru care $J = S^{-1}AS$.

6.151. Fie $V = \mathbb{R}^6$ şi $f : V \to V$ transformarea liniară care are în baza canonică $e = (e_1, \ldots, e_6)$ matricea

$$[f]_e = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} = A.$$

Să se afle forma canonică Jordan J a lui A şi o bază canonică Jordan a lui f.

6.152. Să se găsească forma canonică Jordan a matricei

$$A = \begin{pmatrix} a & a & a & a \\ 0 & a & a & a \\ 0 & 0 & a & a \\ 0 & 0 & 0 & a \end{pmatrix} \quad (a \in \mathbb{R}^*).$$

6.153. Care dintre următoarele matrice

$$A = \begin{pmatrix} -3 & 3 & -2 \\ -7 & 6 & -3 \\ 1 & -1 & 2 \end{pmatrix},\ B = \begin{pmatrix} 0 & 1 & -1 \\ -4 & 4 & -2 \\ -2 & 1 & 1 \end{pmatrix},\ C = \begin{pmatrix} 0 & -1 & -1 \\ -3 & -1 & -2 \\ 7 & 5 & 6 \end{pmatrix},$$
$$D = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

sunt similare ?

6.154. Să se găsescă forma canonică Jordan a următoarelor matrice pătratice cu elemente din $\mathbb{R}$:

$$a)\ \begin{pmatrix} 1 & 2 & 0 \\ 0 & 2 & 0 \\ -2 & -2 & -1 \end{pmatrix},\ b)\ \begin{pmatrix} 3 & 0 & 8 \\ 3 & -1 & 6 \\ -2 & 0 & -5 \end{pmatrix},\ c)\ \begin{pmatrix} -4 & 2 & 10 \\ -4 & 3 & 7 \\ -3 & 1 & 7 \end{pmatrix},$$
$$d)\ \begin{pmatrix} 3 & 1 & 0 & 0 \\ -4 & -1 & 0 & 0 \\ 7 & 1 & 2 & 1 \\ -17 & -6 & -1 & 0 \end{pmatrix}.$$

Capitolul 7

Corpuri comutative. Teoria lui Galois

7.1. Să se dea exemple de numere reale algebrice şi de numere reale trancendente.

7.2. Să se dea exemple de numere algebrice şi de numere trancendente din $\mathbb{C} \setminus \mathbb{R}$.

7.3. Să se arate că nulţimea T a numerelor transcendente nu este stabilă nici relativ la adunare, nici relativ la înmulţire.

7.4. Fie $z = a + bi \in \mathbb{C}$, $a, b \in \mathbb{R}$. Să se arate că z este algebric dacă şi numai dacă a şi b sunt algebrice.

7.5. Fie $K \leq K'$ o extindere de corpuri comutative, $a \in K$, $u \in K'$ şi

$$A = \{x \in K' \mid x \text{ este element algebric peste } K\}.$$

Folosind numai definiţia elementelor algebrice, să se arate că

$$u \in A \Leftrightarrow u + a \in A \Leftrightarrow u^2 \in A,$$

iar dacă $f \in K[X]$ şi grad$f \geq 1$ atunci

$$u \in A \Leftrightarrow f(u) \in A.$$

7.6. Fie $f \in \mathbb{Q}[X]$, grad$f \geq 1$. Să se arate că numerele $f(\pi)$ şi $f(e)$ sunt transcendente.

7.7. Să se determine corpul $\mathbb{R}(\sqrt{2} + i\sqrt{3})$ şi subcorpul său prim.

7.8. Fie $K \leq K'$ o extindere de corpuri şi $a_i, b_j \in K'$, $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, n\}$. Să se arate că $K(a_1, \ldots, a_m) = K(b_1, \ldots, b_n)$ dacă şi numai dacă $\{a_1, \ldots, a_m\} \subseteq K(b_1, \ldots, b_n)$ şi $\{b_1, \ldots, b_n\} \subseteq K(a_1, \ldots, a_m)$.

7.9. Să se arate că numărul $1 + \sqrt{2}$ este algebric şi să se determine polinomul său minimal peste $\mathbb{Q}$.

7.10. Este numărul $\sqrt{2} + \sqrt{3}$ algebric? În caz afirmativ, să se determine polinomul său minimal (peste $\mathbb{Q}$).

7.11. Să se determine corpurile $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2})$ şi subcorpurile lor prime.

7.12. Fie $n \in \mathbb{N}$, $n \geq 2$. Să se determine corpurile $\mathbb{Q}(\sqrt[n]{2})$ şi $\mathbb{Q}(\sqrt[n]{3})$.

7.13. Să se arate că mulţimea subcorpurilor corpului $\mathbb{R}$ este infinită.

7.14. Să se arate că pentru orice $n \in \mathbb{N}^*$ există K astfel încât $\mathbb{Q} \leq K \leq \mathbb{R}$ şi $[K : Q] = n$. Folosind acest rezultat, să se arate că extinderile $Q \leq \mathbb{R}$ şi $\mathbb{Q} \leq \mathbb{C}$ sunt infinite.

7.15. Să se determine gradul extinderii $\mathbb{R} \leq \mathbb{C}$, să se arate că orice număr complex este algebric peste $\mathbb{R}$ şi $\mathbb{C} = \mathbb{R}(z)$ pentru orice $z \in \mathbb{C} \setminus \mathbb{R}$.

7.16. Să se determine subcorpurile lui $\mathbb{C}$ care includ pe $\mathbb{R}$.

7.17. Fie $a, b \in \mathbb{Q}$. Să se determine subcorpul K al lui $\mathbb{C}$ generat de $z = a + bi$.

7.18. Să se determine numerele $u \in \mathbb{Q}(\sqrt{2})$ care generează corpul $\mathbb{Q}(\sqrt{2})$.

7.19. Să se determine gradul extinderii $\mathbb{Q} \leq \mathbb{Q}(i, \sqrt{2})$ şi corpul $\mathbb{Q}(i, \sqrt{2})$.

7.20. Fie $K \leq K'$ o extindere de corpuri de grad prim. Să se arate că:
1) $K' = K(u)$ pentru orice $u \in K' \setminus K$;
2) dacă $K = \mathbb{Q}$ sau $K = \mathbb{Z}_p$ (cu p număr prim) atunci K' este generat de orice element $u \in K' \setminus K$.

7.21. Fie $K \in \{\mathbb{Q}\} \cup \{\mathbb{Z}_p \mid p \text{ număr prim}\}$ şi $K \leq K'$ o extindere de corpuri de grad prim. Să se determine subcorpurile lui K'.

7.22. Fie $u = 2 + \sqrt{3}$, $v = \sqrt[4]{5} + \sqrt{5}$, $w = \sqrt[3]{2} + \sqrt[3]{4}$. Să se arate că numerele u, v şi w sunt algebrice, să se găsească polinoamele minimale ale acestor numere şi să se determine corpurile $\mathbb{Q}(u)$, $\mathbb{Q}(v)$, $\mathbb{Q}(w)$.

7.23. Să se arate că $\mathbb{Q}\left(\sqrt{\dfrac{3}{2}}\right) = \mathbb{Q}(\sqrt{6})$.

7.24. Să se arate că dacă $u \in \mathbb{Q}$ şi $\sqrt{u} \notin \mathbb{Q}$ atunci există un întreg liber de pătrate d astfel încât $\mathbb{Q}(\sqrt{u}) = \mathbb{Q}(\sqrt{d})$.

7.25. Să se arate că o extindere K a lui $\mathbb{Q}$ are gradul 2 dacă şi numai dacă $K = \mathbb{Q}(\sqrt{d})$ unde d este un întreg liber de pătrate.

7.26. Fie K_1 şi K_2 corpuri care au acelaşi subcorp prim P. Să se arate că dacă $f : K_1 \to K_2$ este un omomorfism nenul atunci $f|_P = 1_P$. Folosind acest rezultat, să se arate că singurul endomorfism nenul al unui corp prim K este 1_K. În particular, să se determine automorfismele corpurilor $\mathbb{Q}$ şi $\mathbb{Z}_p$ (p număr prim).

7.27. Să se arate că nu sunt izomorfe corpurile $\mathbb{Q}(\sqrt{2})$ şi $\mathbb{Q}(\sqrt{3})$.

7.28. Fie $d, d' \in \mathbb{Z} \setminus \{1\}$ întregi liberi de pătrate. Să se demonstreze echivalenţa:

$$\mathbb{Q}(\sqrt{d}) \simeq \mathbb{Q}(\sqrt{d'}) \Leftrightarrow d = d'.$$

7.29. Să se determinele automorfismele corpului $\mathbb{Q}(\sqrt{d})$, unde $d \in \mathbb{Z} \setminus \{1\}$ este un întreg liber de pătrate.

7.30. Să se determine un subcorp K al lui $\mathbb{C}$, neinclus în $\mathbb{R}$, izomorf cu $\mathbb{Q}(\sqrt[4]{2})$.

7.31. Să se determine un subcorp K al lui $\mathbb{C}$, neinclus în $\mathbb{R}$, izomorf cu $\mathbb{Q}(\sqrt[3]{2})$.

7.32. Să se determine gradul şi câte o bază pentru fiecare dintre următoarele extinderi de corpuri: a) $\mathbb{Q} \leq \mathbb{Q}(\sqrt{3}\,,\, i)$; b) $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}\,,\, i\sqrt{2})$; c) $\mathbb{Q} \leq \mathbb{Q}(\sqrt{18}\,,\, \sqrt[4]{2})$; d) $\mathbb{Q} \leq \mathbb{Q}(\sqrt{3}, i\sqrt{5}, \sqrt{7})$; e) $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

7.33. Fie α o rădăcină a polinomului $f = X^3 - 6X^2 + 9X + 3 \in \mathbb{Q}[X]$. Să se determine:
a) gradul şi o bază a extinderii $\mathbb{Q} \leq \mathbb{Q}(\alpha)$;
b) coordonatele elementelor α^4, α^5, $3\alpha^5 - \alpha^4 + 2$, $\dfrac{1}{\alpha}$, $\dfrac{1}{\alpha+1}$, $\dfrac{1}{\alpha^2 - 6\alpha + 8}$ în baza găsită la punctul a).

7.34. a) Să se determine polinoamele de grad cel mult 3 din $\mathbb{Z}_2[X]$ ireductibile peste $\mathbb{Z}_2$.
b) Să se construiască un corp cu 4 elemente şi să se alcătuiască tablele de adunare şi înmulţire ale acestui corp.
c) Să se construiască un corp cu 8 elemente.

7.35. Să se determine:
a) polinoamele de gradul 2 din $\mathbb{Z}_3[X]$ ireductibile peste $\mathbb{Z}_3$;
b) un corp cu 9 elemente.

7.36. Fie K un corp finit cu q elemente. Spunem că un *polinom* din $K[X]$ este *unitar* dacă are coeficientul termenului de grad maxim egal cu 1. Să se arate că:
a) numărul polinoamelor unitare de gradul 2 din $K[X]$ ireductibile peste K este $\dfrac{q^2 - q}{2}$;
b) numărul polinoamelor unitare de gradul 3 din $K[X]$ ireductibile peste K este $\dfrac{q^3 - q}{3}$.

7.37. Să se determine corpurile de descompunere peste $\mathbb{Q}$ şi peste $\mathbb{R}$ ale următoarelor polinoame: a) $f = X^2 - 2$; b) $f = X^2 + 2$; c) $f = X^3 - 1$; d) $f = X^3 + 1$; e) $f = X^4 - 2$; f) $f = X^4 + 2$; g) $f = X^4 + X^2 + 1$.

7.38. Fie $n \in \mathbb{N}^*$, $f = X^n - 1 \in \mathbb{Q}[X]$ şi $g = X^n - a \in \mathbb{Q}[X]$, iar ε o rădăcină primitivă de ordinul n a unităţii şi u o rdăcină a lui g. Să se arate că:
a) $\mathbb{Q}(\varepsilon)$ este corpul de descompunere al lui f peste $\mathbb{Q}$;
b) $\mathbb{Q}(\varepsilon, u)$ este corpul de descompunere al lui g peste $\mathbb{Q}$.

7.39. Să se determine grupurile Galois ale extinderilor $\mathbb{Q} \leq \mathbb{R}$, $\mathbb{R} \leq \mathbb{C}$ şi $\mathbb{Q} \leq \mathbb{Q}(i)$.

7.40. Fie K subcorpul prim al corpului K'. Să se arate că $G(K, K') = Aut(K')$.

7.41. Fie $f = X^3 - 2 \in \mathbb{Q}[X]$. Să se determine:
1) grupul Galois $G_f(\mathbb{Q})$ al lui f peste $\mathbb{Q}$ şi permutarea rădăcinilor lui f indusă de fiecare automorfism din $G_f(\mathbb{Q})$;
2) diagrama laticei subgrupurilor lui $G_f(\mathbb{Q})$;
3) diagrama laticei subcorpurilor corpului $D_f(\mathbb{Q})$ de descompunere al lui f peste $\mathbb{Q}$.

7.42. Fie $f = X^4 - 2 \in \mathbb{Q}[X]$. Să se determine:
1) grupul Galois $G_f(\mathbb{Q})$ al lui f peste $\mathbb{Q}$ şi să se arate că $G_f(\mathbb{Q})$ nu este izomorf cu grupul simetric S_4;
2) diagrama laticei subgrupurilor lui $G_f(\mathbb{Q})$;
3) diagrama laticei subcorpurilor corpului $D_f(\mathbb{Q})$ de descompunere al lui f peste $\mathbb{Q}$.

7.43. Fie $K = \mathbb{Q}(\varepsilon)$, unde ε este o rădăcină de ordinul 3 a unităţii şi $f = X^3 - 2 \in K[X]$. Să se determine:
1) grupul Galois al lui f peste K;
2) diagrama laticei subgrupurilor grupului Galois $G_f(K)$ al lui f peste K;
3) diagrama laticei subcorpurilor corpului $D = D_f(K)$ de descompunere al lui f peste K, care includ pe K.

7.44. Fie $p \in \mathbb{N}^*$ un număr prim, $\varepsilon \neq 1$ o rădăcină de ordinul p a unităţii, $K = \mathbb{Q}(\varepsilon)$ şi $f = X^p - 2 \in K[X]$. Să se determine:
1) grupul Galois al lui f peste K;
2) diagrama laticei subgrupurilor grupului Galois $G_f(K)$ al lui f peste K;
3) diagrama laticei subcorpurilor corpului $D = D_f(K)$ de descompunere al lui f peste K, care includ pe K.

7.45. Să se arate că pentru orice $n \in \mathbb{N}^*$ şi orice număr prim $p \in \mathbb{N}$ există:
i) un polinom de gradul n ireductibil peste $\mathbb{Z}_p$;
ii) o extindere de corpuri $\mathbb{Z}_p \leq D$ de gradul n.

7.46. Să se arate că pentru orice $n \in \mathbb{N}^*$ şi orice corp prim P există:
i) un polinom de gradul n ireductibil peste P;
ii) o extindere de corpuri $P \leq K$ de gradul n.

7.47. Fie K un subcorp al lui $\mathbb{R}$, $f \in K[X]$ un polinom ireductibil peste K şi $p = \operatorname{grad} f > 2$. Să se arate că dacă p este prim şi f are exact $p-2$ rădăcini reale, atunci grupul Galois $G_f(K)$ al lui f peste K este izomorf cu S_p.

7.48. Să se arate că ecuaţia $x(x^2 - 4)(x^2 + 2) = 2$ nu este rezolvabilă prin radicali peste $\mathbb{Q}$.

Partea II

SOLUŢII, INDICAŢII şi RĂSPUNSURI

Capitolul 1

Relaţii. Funcţii

1.1. a) Dacă $m = 0$ sau $n = 0$ atunci A sau B fiind mulţimea vidă avem $A \times B = \emptyset$, deci numărul cerut este 0. Fie $m, n \in \mathbb{N}^*$, $A = \{1, \ldots, m\}$, $B = \{1, \ldots, n\}$ şi fie $f(m,n)$ numărul cerut (adică $f(m,n) = |A \times B|$). Demonstrăm prin inducţie după $m \in \mathbb{N}^*$ că $f(m,n) = mn$. Din

$$\{1\} \times \{1, 2, \ldots, n\} = \{(1,1), (1,2), \ldots, (1,n)\}$$

rezultă $f(1,n) = n = 1 \cdot n$. Presupunând că $f(m,n) = mn$ avem

$$\begin{aligned}\{1, \ldots, m, m+1\} \times \{1, \ldots, n\} = (&\{1, \ldots, m\} \times \{1, \ldots, n\}) \cup \\ &\cup \{(m+1, 1), (m+1, 2), \ldots, (m+1, n)\}\end{aligned}$$

de unde deducem că

$$f(m+1, n) = f(m,n) + f(1,n) = mn + n = (m+1)n.$$

b) Fie $\mathcal{P}(A \times B)$ mulţimea submulţimilor mulţimii $A \times B$. Întrucât $A \times B$ are C_{mn}^k submulţimi cu k elemente, numărul cerut este

$$C_{mn}^0 + C_{mn}^1 + \cdots + C_{mn}^{mn} = 2^{mn}.$$

c) Cum orice relaţie cu domeniul A şi codomeniul B este determinată de graficul său, numărul relaţiilor între elementele mulţimilor A şi B este egal cu numărul submulţimilor lui $A \times B$, adică este egal cu 2^{mn}.

1.2. a) Relaţia universală între elementele mulţimilor A şi B are domeniul A, codomeniul B şi graficul

$$A \times B = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)\}.$$

Complementara sa este relaţia vidă pentru că

$$C_{A \times B}(A \times B) = (A \times B) \setminus (A \times B) = \emptyset.$$

Complementara relaţiei (A, B, R_1) este relaţia $(A, B, C_{A \times B}(R_1))$ cu graficul

$$C_{A \times B}(R_1) = (A \times B) \setminus R_1 = \{(1,1), (2,1), (2,2)\}.$$

b) Reuniunea şi intersecţia relaţiilor binare (B, C, R_2) şi (B, C, R_3) sunt relaţiile $(B, C, R_2 \cup R_3)$, respectiv $(B, C, R_2 \cap R_3)$ cu

$$R_2 \cup R_3 = \{(1,2),(1,4),(2,2),(2,3),(3,1),(3,4)\} \text{ şi } R_2 \cap R_3 = \{(1,4)\}.$$

c) Avem

$$\begin{aligned} R_2 \circ R_1 &= \{(a,c) \in A \times C \mid \exists b \in B :\ (a,b) \in R_1,\ (b,c) \in R_2\} = \\ &= \{(1,1),(1,4),(2,1),(2,4)\}, \\ R_1 \circ R_2 &= \{(b_1,b_2) \in B \times B \mid \exists a \in A \cap C :\ (b_1,a) \in R_2,\ (a,b_2) \in R_1\} = \\ &= \{(3,2),(3,3)\}. \end{aligned}$$

d) Avem

$$\overset{-1}{R_1} = \{(b,a) \in B \times A \mid (a,b) \in R_1\} = \{(3,1),(3,2),(2,1)\},$$

$$\overset{-1}{R_2} = \{(1,3),(4,1),(4,3)\},$$

iar din c) rezultă

$$\overset{-1}{\overline{R_2 \circ R_1}} = \{(1,1),(4,1),(1,2),(4,2)\}.$$

Menţionăm că pentru determinarea acestui grafic putea fi folosită şi egalitatea

$$\overset{-1}{\overline{R_2 \circ R_1}} = \overset{-1}{R_1} \circ \overset{-1}{R_2}.$$

e) Complementara relaţiei $\leq$ este relaţia $>$ şi are ca grafic semiplanul deschis format din punctele situate sub prima bisectoare.

Observaţii:

i) Dacă domeniul A şi codomeniul B ale unei relaţii binare (A, B, R) sunt mulţimi finite, $A = \{a_1, \ldots, a_m\}$, $B = \{b_1, \ldots, b_n\}$, fixând o ordine pe aceste mulţimi (de exemplu cea dată de succesiunea indicilor în mulţimea numerelor naturale), putem identifica relaţia dată cu o matrice cu m coloane şi n linii, care are la intersecţia liniei i cu coloana j pe 1 dacă $(a_j, b_i) \in R$ şi pe 0 dacă $(a_j, b_i) \notin R$, adică 0, respectiv 1 reprezintă falsul, respectiv adevărul. Astfel, relaţiile R_1, R_2 şi R_3 vor fi reprezentate, respectiv, prin matricele:

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

ii) Din i) rezultă imediat că operaţia care asociază unei relaţii binare R complementara sa se va reprezenta prin matricea obţinută înlocuind în matricea lui R fiecare 0 cu 1 şi fiecare 1 cu 0. Conform cu cele de mai sus, relaţiile de la punctul a) se reprezintă, respectiv, prin matricele:

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

iii) Două relaţii care au acelaşi domeniu şi acelaşi codomeniu vor fi reprezentate prin matrice de acelaşi tip. Matricele care reprezintă reuniunea şi intersecţia acestora se obţin la fel ca suma a două matrice, luând disjuncţia, respectiv conjuncţia elementelor de pe aceeaşi poziţie din cele două matrice:

$$0 \vee 0 = 0,\ 1 \vee 0 = 0 \vee 1 = 1 \vee 1 = 1,$$
$$0 \wedge 0 = 0 \wedge 1 = 1 \wedge 0 = 0,\ 1 \wedge 1 = 1.$$

Astfel, relaţiile $R_2 \cup R_3$ şi $R_2 \cap R_3$ se reprezintă, respectiv, prin matricele:

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

iv) Unele proprietăţi ale reuniunii şi intersecţiei relaţiilor (de exemplu, asociativitatea şi comutativitatea) sunt determinate de proprietăţi similare ale disjuncţiei şi conjuncţiei.

v) Compusa $(C, B, R \circ S)$ a două relaţii (A, B, R) şi (C, D, S) este egală cu compusa relaţiilor $(A \cap D, B, R \cap ((A \cap D) \times D))$ şi $(C, A \cap D, S \cap (C \times (A \cap D)))$.

vi) Compusei $R \circ S$ a două relaţii (A, B, R) şi (C, D, S) îi va corespunde matricea obţinută astfel:

• din matricea corespunzătoare lui R reţinem coloanele şi din cea corespunzătoare lui S liniile corespunzătoare elementelor din intersecţia $D \cap A$, obţinând astfel restricţiile

$$(A \cap D, B, R \cap ((A \cap D) \times D)) \text{ şi } (C, A \cap D, S \cap (C \times (A \cap D)))$$

ale celor două relaţii (evident, această etapă poate fi omisă dacă $A = D$);

• dacă $A \cap D = \emptyset$ atunci $R \circ S = \emptyset$; dacă $A \cap D \neq \emptyset$ atunci matricea corespunzătoare compusei $R \circ S$ se obţine printr-un procedeu asemănător înmulţirii matricelor ,,înmulţirea" elementelor 0 şi 1 realizându-se după regulile conjuncţiei, iar ,,adunarea" produselor obţinute realizându-se după regulile disjuncţiei.

De exemplu, compusa $R_2 \circ R_1$ a relaţiilor din problema noastră are în linia 1 şi coloana 1 elementul

$$(0 \wedge 0) \vee (0 \wedge 1) \vee (1 \wedge 1) = 0 \vee 0 \vee 1 = 1,$$

şi matricea corespunzătoare compusei $R_2 \circ R_1$ este

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

Pentru calculul matricei compusei $R_1 \circ R_2$, să remarcăm că $A \cap C = A = \{1, 2\}$, deci din matricea asociată lui R_2 reţinem liniile corespunzătoare perechilor $(x, 1)$ şi $(x, 2)$ cu $x = 1, 2, 3$, adică primele două linii, deci compusa $R_2 \circ R_1$ se reprezintă prin matricea

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

vii) În ceea ce priveşte inversa unei relaţii, aceasta se reprezintă prin transpusa matricei corespunzătoare relaţiei date, deci matricele corespunzătoare relaţiilor

$$\overset{-1}{R_1},\ \overset{-1}{R_2} \text{ şi } \overset{-1}{\overline{R_2 \circ R_1}}$$

sunt, respectiv,

$$\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \text{ şi } \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

1.3. a) Graficul relaţiei $\leq$ este format de punctele din plan de coordonate (x, y) cu $x \leq y$, deci este mulţimea punctelor din plan situate deasupra sau pe prima bisectoare.
b) Graficul relaţiei $\geq$ este format de punctele din plan de coordonate (x, y) cu $x \leq y$, deci este mulţimea punctelor din plan situate sub sau pe prima bisectoare.
c) Intersecţia relaţiilor $\leq$ şi $\geq$ are graficul

$$\{(x, y) \in \mathbb{R}^2 \mid x \leq y \text{ şi } x \geq y\} = \{(x, y) \in \mathbb{R}^2 \mid x = y\},$$

deci este mulţimea punctelor de pe prima bisectoare.
d) Din faptul că pentru orice numere reale x şi y avem $x \leq y$ sau $x \geq y$ rezultă că reuniunea relaţiilor $\leq$ şi $\geq$ are graficul

$$\{(x, y) \in \mathbb{R}^2 \mid x \leq y \text{ sau } x \geq y\} = \mathbb{R}^2,$$

adică graficul este mulţimea tuturor punctelor din plan.

1.4. Pentru orice $x, y \in \mathbb{N}$ avem

$$x < y \Leftrightarrow y - x > 0 \Leftrightarrow y - x \geq 1$$

şi astfel,

$$\begin{aligned} x <^2 y &\Leftrightarrow \exists z \in \mathbb{N},\ x < z,\ z < y \Leftrightarrow\ \exists z \in \mathbb{N},\ z - x \geq 1,\ y - z \geq 1 \\ &\Leftrightarrow y - x \geq 2 \Leftrightarrow x + 2 \leq y \Leftrightarrow x + 1 < y. \end{aligned}$$

Analog,

$$x <^3 y \Leftrightarrow x + 3 \leq y \Leftrightarrow x + 2 < y.$$

De asemenea, avem

$$\begin{aligned} x(< \circ >)y &\Leftrightarrow \exists z \in \mathbb{N},\ x > z,\ z < y \Leftrightarrow \exists z \in \mathbb{N},\ z < \min(x, y) \\ &\Leftrightarrow (x, y) \in \mathbb{N}^* \times \mathbb{N}^*; \\ x(> \circ <)y &\Leftrightarrow \exists z \in \mathbb{N},\ x < z,\ z > y \Leftrightarrow \exists z \in \mathbb{N}, z > \max(x, y) \\ &\Leftrightarrow (x, y) \in \mathbb{N} \times \mathbb{N}. \end{aligned}$$

Observaţie: Relaţiile $<$ şi $>$ sunt una inversa celeilalte. Din cele de mai sus rezultă că inversa unei relaţii nu este simetrică a relaţiei date relativ la compunerea relaţiilor.

1.5. Transformarea geometrică ce duce pe $\rho \subseteq \mathbb{R} \times \mathbb{R}$ în $\overset{-1}{\rho}$ va duce fiecare punct $(x, y) \in \rho$ în punctul (y, x), deci este simetria în raport cu prima bisectoare. Cum ρ_0 se reprezintă în plan prin dreapta ce trece prin origine şi face un unghi de $60°$ cu axa Ox, deducem că $\overset{-1}{\rho_0}$ este dreapta care trece prin origine şi face un unghi de $30°$ cu Ox. Lăsăm cititorului trasarea graficului relaţiei $\overset{-1}{\rho_0}$.

1.6. Echivalenţa

$$(a,b) \in R_1 \Leftrightarrow (a,b) \in R_2$$

are loc dacă si numai dacă are loc echivalenţa

$$(b,a) \in \overset{-1}{R_1} \Leftrightarrow (b,a) \in \overset{-1}{R_2}.$$

1.7. Fie $a = (a_1, \ldots, a_n),\ b = (b_1, \ldots, b_n)$. Avem

$$\begin{aligned}
a\rho_i b &\Leftrightarrow\ a\rho_{i1}b,\ a\rho_{i2}b,\ \ldots,\ a\rho_{in}b \\
&\Leftrightarrow\ \sum_{k=1}^{i} a_k = b_1,\ \sum_{k=1}^{i} a_k = b_1 + b_2,\ \ldots,\ \sum_{k=1}^{i} a_k = \sum_{k=1}^{n} b_k \\
&\Leftrightarrow b_2 = b_3 = \cdots = b_n = 0 \text{ şi } \sum_{k=1}^{i} a_k = b_1, \\
a\rho b &\Leftrightarrow\ a\rho_{11}b,\ a\rho_{22}b,\ \ldots, a\rho_{nn}b \\
&\Leftrightarrow\ a_1 = b_1,\ a_1 + a_2 = b_1 + b_2,\ \ldots,\ \sum_{k=1}^{n} a_k = \sum_{k=1}^{n} b_k \\
&\Leftrightarrow\ a_1 = b_1,\ a_2 = b_2,\ \ldots,\ a_n = b_n \\
&\Leftrightarrow\ a = b,
\end{aligned}$$

deci ρ este relaţia de egalitate în $\mathbb{R}^n$ şi, cum din asociativitatea intersecţiei rezultă

$$\rho' = \bigcap_{i=1}^{n} \rho_i,$$

deducem

$$a\rho b\ \Leftrightarrow\ a = b = (a_1, 0, \ldots, 0).$$

1.8. Cum

$$mR^2 n \Leftrightarrow \exists p \in \mathbb{N}:\ m|p,\ p|n \Leftrightarrow m|n,$$

avem $R^2 = R$, iar din

$$m(S \circ R)n \Leftrightarrow \exists p \in \mathbb{N}:\ mRp,\ pSn \Leftrightarrow \exists p \in \mathbb{N}:\ m|p,\ p < n \Leftrightarrow m < n,$$

deducem $S \circ R = S$. Avem $T^2 = \mathbb{N} \times \mathbb{N}$ deoarece

$$mT^2 n \Leftrightarrow \exists p \in \mathbb{N}:\ (m,p) = 1,\ (p,n) = 1$$

şi $p = 1$ satisface condiţiile de mai sus pentru orice $m, n \in \mathbb{N}$.

Folosind faptul că $|a - b| = k \Leftrightarrow a = b + k$ sau $a = b - k$ avem

$$\begin{aligned}
m(R \circ R_k)n &\Leftrightarrow \exists p \in \mathbb{N}:\ |m - p| = k,\ p|n \Leftrightarrow (m-k)|n \text{ sau } (m+k)|n; \\
m(R_k \circ R)n &\Leftrightarrow \exists p \in \mathbb{N}:\ m|p,\ |p - n| = k \Leftrightarrow m|(n-k) \text{ sau } m|(n+k); \\
m(R_k \circ S)n &\Leftrightarrow \exists p \in \mathbb{N}:\ m < p,\ |p - n| = k \Leftrightarrow m < n + k; \\
m(S \circ R_k)n &\Leftrightarrow \exists p \in \mathbb{N}:\ |m - p| = k,\ p < n \Leftrightarrow m - k < n \Leftrightarrow m < n + k; \\
m(R_k \circ R_l)n &\Leftrightarrow \exists p \in \mathbb{N}:\ |m - p| = l,\ |p - n| = k \\
&\Leftrightarrow |m - n| = k + l \text{ sau } |m - n| = |k - l|.
\end{aligned}$$

1.9. Răspuns. $\rho_1^2 = \rho_1$, $\rho_2^2 = \rho_2$, $\rho_3^2 = C[a,b] \times C[a,b]$, $\rho_2 \circ \rho_3 = \rho_3 \circ \rho_2$,

$$f(\rho_2 \circ \rho_1)g \Leftrightarrow f(a) \leq g(a) \text{ şi } f(b) \leq g(b);$$
$$f(\rho_3 \circ \rho_2)g \Leftrightarrow f(a) \neq g(a) \text{ şi } f(b) \neq g(b).$$

1.10. Răspuns. $(S \cap S') \circ R = \emptyset = R \circ (S \cap S')$, $(S \circ R) \cap (S' \circ R) = \{(1,4),(4,4)\}$, $(R \circ S) \cap (R \circ S') = \{(1,4)\}$.

Observaţie: Din cele de mai sus rezultă că operaţia $\circ$ nu este, în general, distributivă faţă de operaţia $\cap$.

1.11. Avem:

$$R(X) = \{y \in B \mid \exists x \in X : \ xRy\} = \{b_4\},$$
$$R\langle a_2 \rangle = \{y \in B \mid a_2 R y\} = \{b_4\},$$
$$\overset{-1}{R}(Y) = \{x \in A \mid \exists y \in Y : \ xRy\} = \{a_1, a_2, a_3\},$$
$$\overset{-1}{R}\langle b_5 \rangle = \{x \in A \mid xRb_5\} = \{a_3\},$$
$$pr_1 R = \overset{-1}{R}(B) = \{x \in A \mid \exists y \in B : \ xRy\} = \{a_1, a_2, a_3\},$$
$$pr_2 R = R(A) = \{y \in B \mid \exists x \in X : \ xRy\} = \{b_2, b_3, b_4, b_5\}.$$

Observaţie: Şi calculul secţiunilor pentru relaţii binare care au domeniul şi codomeniul finite poate fi realizat cu ajutorul matricelor prezentate în Observaţiile de după soluţia problemei **1.2**. Ţinând cont de ordinea fixată în domeniul (codomeniul) unei relaţii binare (A, B, R), o submulţime $X \subseteq A$ (respectiv $X \subseteq B$) poate fi reprezentată ca o matrice coloană în care marcăm cu 1 poziţiile corespunzătoare elementelor din X şi prin 0 poziţiile corespunzătoare elementelor din $A \setminus X$ (respectiv $B \setminus X$). Astfel, submulţimilor $A, X, \{a_2\} \subseteq A$ şi $B, Y, \{b_5\} \subseteq B$ le corespund, respectiv, matricele:

$$\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Matricele corespunzătoare relaţiilor R şi $\overset{-1}{R}$ fiind

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ şi, respectiv, } \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

deducem că secţiunile $R(X)$, $R\langle a_2 \rangle$, $\overset{-1}{R}(Y)$, $\overset{-1}{R}\langle b_5 \rangle$, $pr_1 R$, $pr_2 R$ se reprezintă, respectiv, prin matricele (coloană):

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

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

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

1.12. Răspuns. $\rho\langle 1\rangle=\mathbb{N}$, $\overset{-1}{\rho}(\{4,9\})=\{1,2,3,4,9\}$, $pr_1\rho=\mathbb{N}$, $pr_2\rho=\mathbb{N}$.

1.13. Avem $\rho\langle -1\rangle=\{y\in\mathbb{R}\mid 1+y^2\leq 1\}=\{0\}=\rho\langle 1\rangle$,

$$\rho\langle 0\rangle=\{y\in\mathbb{R}\mid y^2\leq 1\}=[-1,1],\ \rho\langle 2\rangle=\{y\in\mathbb{R}\mid 4+y^2\leq 1\}=\emptyset,$$

$$\rho([0,1])=\{y\in\mathbb{R}\mid \exists x\in[0,1]: x^2+y^2\leq 1\}=[-1,1],$$

$$pr_1\rho=\{x\in\mathbb{R}\mid \exists y\in\mathbb{R}: x^2+y^2\leq 1\}=[-1,1]=pr_2\rho.$$

Interpretare geometrică: Graficul relaţiei ρ e discul unitate, prin urmare, pentru o submulţime $A\subseteq\mathbb{R}$, $\rho\langle a\rangle=\{y\in\mathbb{R}\mid \exists a\in A, a^2+y^2\leq 1\}$ este mulţimea ordonatelor tuturor punctelor din discul unitate care au abscisa în A. Ca urmare, pentru un $a\in\mathbb{R}$, $\rho\langle a\rangle=\{y\in\mathbb{R}\mid a^2+y^2\leq 1\}$ este mulţimea ordonatelor punctelor din plan ce se află în intersecţia discului unitate cu dreapta $x=a$.

1.14. Indicaţie. Vezi interpretarea geometrică din problema anterioară. Pentru determinarea contraimaginii se poate ţine seama de problema **1.5**.

1.15. Indicaţie. Se foloseşte definiţia secţiunii unei relaţii după o submulţime.

1.16. Indicaţie. Se foloseşte definiţia secţiunii unei relaţii după un element.

1.17. Indicaţie. Se folosesc definiţiile secţiunii şi a proiecţiei întâi.

1.18. Răspuns. $\rho(X\cap Y)=\left[-1,-\sqrt{\dfrac{3}{4}}\right]\cup\left[\sqrt{\dfrac{3}{4}},1\right]$, $\rho(X)\cap\rho(Y)=[-1,1]$.

1.19. Răspuns. $(\rho\cap\rho')(X)=\emptyset$, $\rho(X)\cap\rho'(X)=[-1,1]$.

Observaţie: Din cele de mai sus rezultă că incluziunile

$$\rho(X\cap Y)\subseteq\rho(X)\cap\rho(Y)\text{ şi }(\rho\cap\rho')(X)\subseteq\rho(X)\cap\rho'(X)$$

nu sunt, în general, egalităţi.

1.20. Răspuns. $\rho_1(\mathbb{R})=\mathbb{C}$, $\rho_1(X)=X$, $\rho_1\langle i\rangle=\{z\in\mathbb{C}\mid |z|=1\}$, $\rho_2(\mathbb{R})=\mathbb{R}$, $\rho_2(X)=\mathbb{C}\setminus\{0\}$, $\rho_2\langle i\rangle=\{bi\mid b\in\mathbb{R}, b>0\}$, $\rho_3(\mathbb{R})=\mathbb{R}$, $\rho_3(X)=X$, $\rho_3\langle i\rangle=\{-i\}$.

1.21. Indicaţie. Se folosesc definiţiile secţiunii şi ale celor două proiecţii.

1.22. a) Avem

$$\begin{aligned}(a,c)\in S\circ(X\times Y) &\Leftrightarrow \exists b\in B,(a,b)\in X\times Y \text{ şi } (b,c)\in S\\ &\Leftrightarrow a\in X \text{ şi } (\exists b\in Y,(b,c)\in S)\\ &\Leftrightarrow a\in X \text{ şi } c\in S(Y)\\ &\Leftrightarrow (a,c)\in X\times S(Y).\end{aligned}$$

b) Avem

$$\begin{aligned}(a,c)\in (Y\times Z)\circ R &\Leftrightarrow \exists b\in B,(a,b)\in R \text{ şi } (b,c)\in Y\times Z\\ &\Leftrightarrow c\in Z \text{ şi } (\exists b\in B, b\in Y \text{ şi } (a,b)\in R)\\ &\Leftrightarrow c\in Z \text{ şi } a\in \overset{-1}{R}(Y)\\ &\Leftrightarrow (a,c)\in \overset{-1}{R}(Y)\times Z.\end{aligned}$$

c) Dacă $y_0\in Y\cap Y'$ atunci pentru orice $(x,z)\in X\times Z$ avem $(x,y_0)\in X\times Y$ şi $(y_0,z)\in Y'\times Z$, de unde urmează $(x,z)\in(Y'\times Z)\circ(X\times Y)$. Deci

$$X\times Z\subseteq (Y'\times Z)\circ(X\times Y).$$

Invers, dacă $(a,c)\in(Y'\times Z)\circ(X\times Y)$ atunci $\exists b\in B$ astfel încât $(a,b)\in X\times Y$ şi $(b,c)\in Y'\times Z$, de unde rezultă $a\in X$ şi $c\in Z$, adică $(a,c)\in X\times Z$. Deci

$$(Y'\times Z)\circ(X\times Y)\subseteq X\times Z.$$

d) Presupunem că $(Y'\times Z)\circ(X\times Y)\neq\emptyset$, adică există $(a,c)\in(Y'\times Z)\circ(X\times Y)$, ceea ce implică $\exists b\in B$ astfel încât $(a,b)\in X\times Y$ şi $(b,c)\in Y'\times Z$, de unde deducem $b\in Y\cap Y'\neq\emptyset$, ceea ce contrazice ipoteza.

1.23. a) Avem

$$(a_1,a_2)\in\rho\circ(A\times A)\Leftrightarrow \exists a_3\in A,(a_3,a_2)\in\rho\Leftrightarrow a_2\in pr_2\rho.$$

Deci ρ verifică condiţia cerută dacă şi numai dacă $pr_2\rho=A$.
b) Analog se arată că această condiţie este verificată dacă şi numai dacă $pr_1\rho=A$.
c) Avem

$$\begin{aligned}(a_1,a_2)\in\rho\circ(A\times A)\circ\rho &\Leftrightarrow \exists a_3,a_4\in A:(a_1,a_3)\in\rho \text{ şi } (a_4,a_2)\in\rho\Leftrightarrow\\ &\Leftrightarrow a_1\in pr_1\rho \text{ şi } a_2\in pr_2\rho.\end{aligned}$$

Deci ρ verifică condiţia cerută dacă şi numai dacă $pr_1\rho=A=pr_2\rho$.
d) Avem

$$(a_1,a_2)\in(A\times A)\circ\rho\circ(A\times A)\Leftrightarrow\exists a_3,a_4\in A:(a_3,a_4)\in\rho\Leftrightarrow\rho\neq\emptyset.$$

Deci ρ verifică condiţia cerută dacă şi numai dacă $\rho\neq\emptyset$.
e) Avem

$$\begin{aligned}(a_1,a_2)\in\overset{-1}{\rho}\circ\rho &\Leftrightarrow \exists a_3\in A,(a_1,a_3)\in\rho \text{ şi } (a_3,a_2)\in\overset{-1}{\rho}\\ &\Leftrightarrow \exists a_3\in A, a_3\in\rho\langle a_1\rangle \text{ şi } a_3\in\rho\langle a_2\rangle\\ &\Leftrightarrow \rho\langle a_1\rangle\cap\rho\langle a_2\rangle\neq\emptyset.\end{aligned}$$

Deci ρ verifică condiţia cerută dacă şi numai dacă pentru orice $(a_1,a_2)\in A\times A$, avem $\rho\langle a_1\rangle\cap\rho\langle a_2\rangle\neq\emptyset$.

1.24. a) Avem

$$\begin{aligned}(a,c)\in S\circ R &\Leftrightarrow \exists b\in B, (a,b)\in R \text{ şi } (b,c)\in S\\ &\Leftrightarrow \exists b\in B, b\in R\langle a\rangle \text{ şi } b\in \overset{-1}{S}\langle c\rangle\\ &\Leftrightarrow R\langle a\rangle\cap \overset{-1}{S}\langle c\rangle\neq\emptyset.\end{aligned}$$

b) Avem

$$\begin{aligned}(a,c)\in S\circ R \Leftrightarrow \exists b\in B: (a,b)\in R, (b,c)\in S \Leftrightarrow \exists b\in B: a\in \overset{-1}{R}\langle b\rangle, c\in S\langle b\rangle\\ \Leftrightarrow \exists b\in B: (a,c)\in \overset{-1}{R}\langle b\rangle\times S\langle b\rangle \Leftrightarrow (a,c)\in\bigcup_{b\in B}\overset{-1}{R}\langle b\rangle\times S\langle b\rangle,\end{aligned}$$

de unde rezultă egalitatea cerută.

1.25. a) Folosind incluziunea $pr_1 S\subseteq B$, avem

$$\begin{aligned}pr_1(S\circ R) &= (\overset{-1}{\overline{S\circ R}})(C) = (\overset{-1}{R}\circ\overset{-1}{S})(C) = \overset{-1}{R}(\overset{-1}{S}(C))\\ &= \overset{-1}{R}(pr_1 S)\subseteq \overset{-1}{R}(B) = pr_1 R.\end{aligned}$$

b) Folosind incluziunea $pr_2 R\subseteq B$, avem

$$pr_2(S\circ R) = (S\circ R)(A) = S(R(A)) = S(pr_2 R)\subseteq S(B) = pr_2 S.$$

c) Avem

$$\begin{aligned}S\circ R\neq\emptyset &\Leftrightarrow \exists (a,c)\in S\circ R \Leftrightarrow \exists b\in B, (a,b)\in R \text{ şi } (b,c)\in S\\ &\Leftrightarrow \exists b\in B, b\in pr_2 R \text{ şi } b\in pr_1 S \Leftrightarrow pr_2 R\cap pr_1 S\neq\emptyset.\end{aligned}$$

d) Avem

$$\begin{aligned}(a,c)\in S\circ R \Rightarrow \exists b\in B, (a,b)\in R \text{ şi } (b,c)\in S \Rightarrow a\in pr_1 R \text{ şi } c\in pr_2 S \Rightarrow\\ \Rightarrow (a,c)\in pr_1 R\times pr_2 S.\end{aligned}$$

1.26. a)$\Rightarrow$b). Într-adevăr,

$$\begin{aligned}(x,x)\in\Delta_A \Rightarrow x\in A \Rightarrow R\langle x\rangle\neq\emptyset \Rightarrow \exists y\in B, y\in R\langle x\rangle \Rightarrow \exists y\in B, xRy\\ \Rightarrow \exists y\in B, xRy \text{ şi } y\overset{-1}{R}x \Rightarrow (x,x)\in\overset{-1}{R}\circ R.\end{aligned}$$

Deci $\Delta_A\subseteq \overset{-1}{R}\circ R$.
b)$\Rightarrow$c). Într-adevăr,

$$x\in A\Rightarrow (x,x)\in\Delta_A\Rightarrow (x,x)\in\overset{-1}{R}\circ R\Rightarrow \exists y\in B, xRy\Rightarrow x\in pr_1 R.$$

Deci $A\subseteq pr_1 R$, iar incluziunea inversă este adevărată pentru orice relaţie. Rezultă că $pr_1 R = A$.

c)⇒d). Implicaţia din d) este echivalentă cu implicaţia

$$P_1 \cap P_2 \neq \emptyset \Rightarrow (R \circ P_1) \cap (R \circ P_2) \neq \emptyset.$$

Demonstrăm această implicaţie. Din $P_1 \cap P_2 \neq \emptyset$ rezultă că există $(x_1, x_2) \in P_1 \cap P_2 \subseteq A' \times A$, iar din $x_2 \in A$, urmează conform lui c) că există $x \in B$ astfel încât $(x_2, x) \in R$. Din $(x_1, x_2) \in P_1$ şi $(x_2, x) \in R$ obţinem $(x_1, x) \in R \circ P_1$, iar din $(x_1, x_2) \in P_2$ şi $(x_2, x) \in R$ deducem $(x_1, x) \in R \circ P_2$. Deci $(x_1, x) \in (R \circ P_1) \cap (R \circ P_2)$, adică $(R \circ P_1) \cap (R \circ P_2) \neq \emptyset$.
d)⇒e). Dacă în d) luăm $P_1 = P_2 = P$ atunci obţinem

$$R \circ P = \emptyset \Rightarrow P = \emptyset,$$

iar implicaţia

$$P = \emptyset \Rightarrow R \circ P = \emptyset$$

este evidentă.
e)⇒f). Întrucât $R(X_1 \cap X_2) \subseteq R(X_1) \cap R(X_2)$, din $R(X_1) \cap R(X_2) = \emptyset$ rezultă $R(X_1 \cap X_2) = \emptyset$. Prin urmare, dacă $P = \{(x, x) \mid x \in X_1 \cap X_2\}$ atunci $R \circ P = \emptyset$, ceea ce (conform lui e)) implică $P = \emptyset$. Deci $X_1 \cap X_2 = \emptyset$.
f)⇒g). Dacă în f) luăm $X_1 = X_2 = X$ atunci obţinem

$$R(X) = \emptyset \Rightarrow X = \emptyset,$$

iar implicaţia

$$X = \emptyset \Rightarrow R(X) = \emptyset$$

este evidentă.
g)⇒h). Întrucât $\overset{-1}{R}(Y_1 \cup Y_2) = \overset{-1}{R}(Y_1) \cup \overset{-1}{R}(Y_2)$, din $Y_1 \cup Y_2 = B$ rezultă

$$\overset{-1}{R}(Y_1) \cup \overset{-1}{R}(Y_2) = \overset{-1}{R}(B) = pr_1 R \subseteq A. \tag{1}$$

Din g) urmează că pentru orice $x \in A$ avem $R\langle x \rangle \neq \emptyset$, adică există $y \in B$ astfel încât xRy, ceea ce ne arată că $x \in pr_1 R$. Astfel am arătat că $A \subseteq pr_1 R$. Rezultă $A = pr_1 R$, de unde (conform lui (1)) deducem

$$\overset{-1}{R}(Y_1) \cup \overset{-1}{R}(Y_2) = A.$$

h)⇒ i). Dacă în h) luăm $Y_1 = Y$ şi $Y_2 = C(Y)$ atunci obţinem pe i).
i)⇒a). Dacă în i) luăm $Y = \emptyset$ atunci obţinem $\overset{-1}{R}(B) = A$, de unde rezultă că pentru orice $x \in A$ există un $y \in B$ astfel ca xRy, adică $R\langle x \rangle \neq \emptyset$. Deci R verifică pe a).

1.27. a)⇒b). Într-adevăr, dacă $(y_1, y_2) \in R \circ \overset{-1}{R}$ atunci există $x \in A$ astfel încât $(y_1, x) \in \overset{-1}{R}$ şi $(x, y_2) \in R$, de unde rezultă $y_1, y_2 \in R\langle x \rangle$ ceea ce (conform lui a)) implică $y_1 = y_2$, adică $(y_1, y_2) \in \Delta_B$. Deci $R \circ \overset{-1}{R} \subseteq \Delta_B$.
b)⇒c). Incluziunea

$$(S_1 \cap S_2) \circ R \subseteq (S_1 \circ R) \cap (S_2 \circ R) \tag{1}$$

are loc pentru orice $R \subseteq A \times B$. Invers, dacă

$$(x, z) \in (S_1 \circ R) \cap (S_2 \circ R),$$

atunci $(x, z) \in S_1 \circ R$ şi $(x, z) \in S_2 \circ R$, de unde rezultă că

$$\exists y \in B, (x, y) \in R \text{ şi } (y, z) \in S_1 \tag{2}$$

şi

$$\exists y' \in B, (x, y') \in R \text{ şi } (y', z) \in S_2, \tag{3}$$

ceea ce ne arată că $y, y' \in R\langle x\rangle$. De aici, conform lui b), rezultă $y = y'$. Acum, din (2) şi (3) urmează $(x, y) \in R$ şi $(y, z) \in S_1 \cap S_3$, adică

$$(x, z) \in (S_1 \cap S_2) \circ R.$$

Deci am demonstrat incluziunea

$$(S_1 \circ R) \cap (S_2 \circ R) \subseteq (S_1 \cap S_2) \circ R,$$

care împreună cu (1), dă egalitatea cerută.
c)⇒d). Într-adevăr, dacă $S_1 \cap S_2 = \emptyset$ atunci, conform lui c), avem

$$(S_1 \circ R) \cap (S_2 \circ R) = (S_1 \cap S_2) \circ R = \emptyset \circ R = \emptyset.$$

d)⇒ e). Dacă în d) luăm $S_1 = S$ şi $S_2 = C(S)$ atunci obţinem pe e).
e)⇒f). Arătăm că negaţia lui f) implică negaţia lui e). Din negaţia lui f) rezultă că $\exists Y_1, Y_2 \subseteq B$ astfel încât

$$Y_1 \cap Y_2 = \emptyset \text{ şi } \overset{-1}{R}(Y_1) \cap \overset{-1}{R}(Y_2) \neq \emptyset.$$

Din $\overset{-1}{R}(Y_1) \cap \overset{-1}{R}(Y_2) \neq \emptyset$ urmează că există un $x \in \overset{-1}{R}(Y_1) \cap \overset{-1}{R}(Y_2)$, ceea ce implică existenţa unui $y_1 \in Y_1$ şi a unui $y_2 \in Y_2$ astfel încât xRy_1 şi xRy_2. Din $Y_1 \cap Y_2 = \emptyset$ rezultă $y_1 \neq y_2$. Deci luând $S = \{(y_1, y_2)\}$ avem $(y_2, y_2) \in C(S)$. Prin urmare $(x, y_2) \in S \circ R$ şi $(x, y_2) \in C(S) \circ R$, adică

$$(S \circ R) \cap (C(S) \circ R) \neq \emptyset,$$

ceea ce demonstrează negaţia lui e).
f)⇒g). Dacă în f) luăm $Y_1 = Y$ şi $Y_2 = C(Y)$ atunci obţinem pe g).
g)⇒h). Dacă $a \in \overset{-1}{R}(B) \cap C(\overset{-1}{R}(Y))$ atunci $a \in \overset{-1}{R}(B)$ şi $a \notin \overset{-1}{R}(Y)$. Deci există $b \in B$ astfel încât $(a, b) \in R$ şi pentru orice $y \in Y$ avem $(a, y) \notin R$, de unde urmează că $b \in C(Y)$ şi $(a, b) \in R$, ceea ce implică $a \in \overset{-1}{R}(C(Y))$. Astfel am arătat că incluziunea

$$\overset{-1}{R}(B) \cap C(\overset{-1}{R}(Y)) \subseteq \overset{-1}{R}(C(Y)) \tag{4}$$

are loc pentru orice relaţie $R \subseteq A \times B$. Dacă R verifică pe g) atunci

$$\overset{-1}{R}(C(Y)) \subseteq C(\overset{-1}{R}(Y)),$$

de unde, întrucât $C(Y) \subseteq B$ implică $\overset{-1}{R}(C(Y)) \subseteq \overset{-1}{R}(B)$, deducem

$$\overset{-1}{R}(C(Y)) \subseteq \overset{-1}{R}(B) \cap C(\overset{-1}{R}(Y)). \tag{5}$$

Din (4) şi (5) rezultă h).
h)⇒a). Arătăm că negaţia lui a) implică negaţia lui h). Din negaţia lui a) rezultă că există $x_0 \in A$ astfel încât $R\langle x_0\rangle$ să conţină două elemente diferite $y_1, y_2 \in B$. Dacă $Y = \{y_1\}$ atunci $x_0 \in \overset{-1}{R}(Y)$ şi $y_2 \in C(Y)$, de unde urmează $x_0 \notin C(\overset{-1}{R}(Y))$ şi $x_0 \in \overset{-1}{R}\langle y_2\rangle \subseteq \overset{-1}{R}(C(Y))$, ceea ce ne arată că

$$\overset{-1}{R}(B) \cap C(\overset{-1}{R}(Y)) \neq \overset{-1}{R}(C(Y)).$$

Deci negaţia lui h) este demonstrată.

Observaţie: $R \subseteq A \times B$ este graficul unei funcţii dacă şi numai dacă R verifică o condiţie din problema **1.26** şi o condiţie din problema **1.27**.

1.28. În ipoteza problemei avem

$$\begin{aligned} y \in R(C(X)) &\Leftrightarrow \exists a \in A, a \notin X, aRy \Leftrightarrow y \in pr_2 R, y \notin R(X) \\ &\Leftrightarrow y \in pr_2 R \setminus R(X), \end{aligned}$$

ceea ce demonstrează că

$$R(C_A(X)) = pr_2 R \setminus R(X).$$

Incluziunea $R(X \cap X') \subseteq R(X) \cap R(X')$ are loc pentru orice $R \subseteq A \times B$. Dacă R verifică ipoteza din enunţ atunci

$$\begin{aligned} y \in R(X) \cap R(X') &\Rightarrow (\exists x \in X, xRy) \text{ şi } (\exists x' \in X', x'Ry) \\ &\Rightarrow x = x' \in X \cap X', xRy \Rightarrow y \in R(X \cap X'). \end{aligned}$$

Rezultă că $R(X) \cap R(X') \subseteq R(X \cap X')$, deci

$$R(X \cap X') = R(X) \cap R(X').$$

Observaţii: a) Relaţia $R(X \cap X') = R(X) \cap R(X')$ se poate generaliza de la două submulţimi ale lui A la o familie oarecare de submulţimi ale lui A.
b) Dacă $f : A \to B$ este o funcţie şi $Y, Y' \subseteq B$ atunci egalităţile stabilite în problema de mai sus ne conduc la $\overset{-1}{f}(C(Y)) = C(\overset{-1}{f}(Y))$ şi $\overset{-1}{f}(Y_1 \cap Y_2) = \overset{-1}{f}(Y_1) \cap \overset{-1}{f}(Y_2)$.

1.29. Incluziunea

$$S \circ (R_1 \cap R_2) \subseteq (S \circ R_1) \cap (S \circ R_2) \tag{1}$$

are loc pentru orice relaţii. Din $(x, z) \in (S \circ R_1) \cap (S \circ R_2)$ rezultă că există $y \in B$ astfel încât $(x, y) \in R_1$ şi $(y, z) \in S$ şi există $y' \in B$ astfel încât $(x, y') \in R_2$ şi $(y', z) \in S$. Din ipoteza problemei deducem că $y = y' \in B$ aşadar, $(x, y) \in R_1$, $(x, y) \in R_2$ şi $(y, z) \in S$, adică $(x, y) \in R_1 \cap R_2$ şi $(y, z) \in S$, de unde obţinem că $(x, z) \in S \circ (R_1 \cap R_2)$. Aceasta arată că

$$(S \circ R_1) \cap (S \circ R_2) \subseteq S \circ (R_1 \cap R_2). \tag{2}$$

Conform (1) şi (2) avem $S \circ (R_1 \cap R_2) = (S \circ R_1) \cap (S \circ R_2)$.

1.30. Întâi menţionăm că implicaţia a) este echivalentă cu
a′) $X_1,\, X_2 \subseteq B,\, R(X_1) = R(X_2) \Rightarrow X_1 = X_2$.
a)⇒b). Dacă $R \circ R_1 = R \circ R_2$ atunci pentru orice $a \in A$ avem

$$R(R_1\langle a\rangle) = R(R_2\langle a\rangle),$$

de unde, conform lui a′), rezultă că $R_1\langle a\rangle = R_2\langle a\rangle$ pentru orice $a \in A$, ceea ce implică $R_1 = R_2$.
b)⇒a). Din negaţia lui a) rezultă că

$$\exists X_1,\, X_2 \subseteq B,\, X_1 \neq X_2 \text{ şi } R(X_1) = R(X_2).$$

Din $X_1 \neq X_2$ rezultă că una dintre submulţimile X_1, X_2 conţine un element care nu aparţine celeilalte, de exemplu există $x_1 \in X_1, x_1 \notin X_2$. Luând $A = \{x_1\}$ şi $R_1 = \{x_1\} \times X_1$, $R_2 = \{x_1\} \times X_2$, avem $R_1 \neq R_2$ şi

$$R \circ R_1 = \{x_1\} \times R(X_2) = \{x_1\} \times R(X_1) = R \circ R_2.$$

Astfel am arătat că negaţia lui a) implică negaţia lui b).

Observaţie: Din a) urmează că $pr_1R = B$, adică $R\langle b\rangle \neq \emptyset$ pentru orice $b \in B$. Într-adevăr, dacă $b \in B$ atunci din $\{b\} \neq \emptyset$ urmează $R\langle b\rangle \neq R(\emptyset) = \emptyset$.

1.31. a)⇒b). Dacă R verifică condiţia a) din enunţ atunci $\overset{-1}{R}$ verifică condiţia a) din problema de mai sus. Avem

$$R_1 \circ R = R_2 \circ R \Rightarrow \overset{-1}{R} \circ \overset{-1}{R_1} = \overset{-1}{R} \circ \overset{-1}{R_1}$$

şi, conform problemei anterioare, avem $\overset{-1}{R_1} = \overset{-1}{R_2}$, de unde rezultă $R_1 = R_2$.
b)⇒a). Dacă R verifică condiţia b) din enunţ atunci $\overset{-1}{R}$ verifică condiţia b) din problema anterioară. Deci $\overset{-1}{R}$ verifică condiţia a) din problema de mai sus, ceea ce ne arată că R verifică condiţia a) din enunţ.

Observaţie: Din condiţia a) rezultă că $pr_2R = B$.

1.32. Indicaţie. Se foloseşte definiţia funcţiei.

1.33. Răspuns. a) $f \neq g$; b) $f \neq g$; c) $f = g$.

1.34. Răspuns. $f(X_1 \cap X_2) = \{0\}$, $f(X_1) \cap f(X_2) = [0, 1)$.

Observaţie: Din cele de mai sus rezultă că în $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$ nu are loc, în general, egalitatea.

1.35. Răspuns. a) $F \subseteq A \times B$ şi orice paralelă la axa Oy dusă printr-un punct din A să intersecteze pe F exact într-un punct. b) Nu.

1.36. Răspuns. În general, nu.

1.37. Răspuns. $F \cup G$ este un grafic funcţional dacă şi numai dacă $F = G$; $F \cap G$ este graficul unei funcţii dacă şi numai dacă $F = G$; $C(F)$ este un grafic funcţional dacă şi numai dacă $A = \emptyset$ sau B este formată din două elemente; $\overset{-1}{F}$ este grafic al unei funcţii dacă şi numai dacă F este graficul unei bijecţii.

1.38. Indicaţie. Se foloseşte definiţia injectivităţii.

1.39. Indicaţii. a) Se foloseşte problema anterioară (punctul b)) şi interpretarea geometrică din soluţia probemei **1.13**.
b) Dacă luăm $A = B = \{1, 2, 3\}$ (ordonată de relaţia uzuală din $\mathbb{N}$) atunci funcţia $f : A \to A$, $f(1) = 2$, $f(2) = 1$, $f(3) = 3$ este injectivă şi nu este monotonă.

1.40. Indicaţie. Se foloseşte definiţia surjectivităţii.

1.41. Indicaţie. Se foloseşte problema anterioară (punctul c)) şi interpretarea geometrică din soluţia probemei **1.13**.

1.42. Întrucât orice funcţie care are o retractă este injectivă, rezultă că funcţiile cerute trebuie să fie injective. Funcţiile cerute nu sunt bijective, deoarece o bijecţie are numai o retractă.
a) Fie $A = \{1, 2\}, B = \{1, 2, 3\}$ şi $f : A \to B$ funcţia dată în tabelul

x	1	2
$f(x)$	2	3

Dacă $r : B \to A$ este o retractă a lui f atunci $r \circ f = 1_A$, de unde urmează $r(2) = 1$ şi $r(3) = 2$, iar $r(1)$ trebuie să verifice doar condiţia $r(1) \in A$. Rezultă că $r(1)$ poate fi ales în două şi numai două feluri. Deci f are cel mult două retracte diferite $r_1, r_2 : B \to A$ definite astfel:

x	1	2	3
$r_1(x)$	1	1	2

x	1	2	3
$r_2(x)$	2	1	2

Din $r_1(1) \neq r_2(1)$ rezultă că $r_1 \neq r_2$. Se verifică uşor că $r_1 \circ f = 1_A$ şi $r_2 \circ f = 1_A$. Deci r_1 şi r_2 sunt retracte ale lui f. Prin urmare f are exact două retracte.
b) Fie $f : A \to B$ o funcţie injectivă, care nu este surjectivă. Pentru ca f să aibă o infinitate de retracte este necesar ca B să fie infinită. Fie $A = B = \mathbb{N}$ şi $f : \mathbb{N} \to \mathbb{N}$, $f(n) = 2n$. Dacă $r_k : \mathbb{N} \to \mathbb{N}$, $k \in \mathbb{N}$ sunt funcţiile definite astfel:

$$r_k(n) = \begin{cases} \dfrac{n}{2}, & \text{dacă } n \text{ este par} \\ k, & \text{dacă } n \text{ este impar} \end{cases}$$

atunci $r_k \circ f = 1_{\mathbb{N}}$. Deci r_k, $k \in \mathbb{N}$ sunt retracte diferite ale lui f.

1.43. Întrucât orice funcţie care are o secţiune este surjectivă, rezultă că funcţiile cerute sunt surjective. Funcţiile cerute nu sunt bijective, deoarece o bijecţie are numai o secţiune.
a) Fie $A = \{1, 2, 3\}, B = \{1, 2\}$ şi $f : A \to B$ funcţia definită astfel:

x	1	2	3
$f(x)$	2	1	2

Dacă $s : B \to A$ este o secţiune a lui f atunci $f \circ s = 1_B$, de unde urmează $s(1) = 2$ şi $s(2) \in \{1, 3\}$, adică $s(2)$ poate fi ales în două feluri. Deci f are cel mult două secţiuni diferite $s_1, s_2 : B \to A$ definite astfel:

$$\begin{array}{c|cc} x & 1 & 2 \\ \hline s_1(x) & 2 & 1 \end{array} \qquad \begin{array}{c|cc} x & 1 & 2 \\ \hline s_2(x) & 2 & 3 \end{array}$$

Din $s_1(2) \neq s_2(2)$ rezultă că $s_1 \neq s_2$. Se verifică uşor că $f \circ s_1 = 1_B$ şi $f \circ s_2 = 1_B$. Deci f are exact două secţiuni diferite.
b) Fie $f : \mathbb{R} \to [0, \infty[$, $f(x) = x^2$. Dacă $s_k : [0, \infty) \to \mathbb{R}$ $(k = 0, 1, 2, \dots)$ sunt funcţiile definite astfel:

$$s_k(x) = \begin{cases} \sqrt{x}, & \text{dacă } x \neq k \\ -\sqrt{x}, & \text{dacă } x = k \end{cases}$$

atunci $(f \circ s_k)(x) = x$ pentru orice $x \in [0, \infty)$. Deci s_k $(k = 0, 1, 2, \dots)$ sunt secţiuni diferite ale lui f.

1.44. Indicaţie. Orice funcţie injectivă care nu este surjectivă.

1.45. Indicaţie. Orice funcţie surjectivă care nu este injectivă.

1.46. Răspuns. a) $m \leq n$; b) $m \geq n$; c) $m = n$.

1.47. Indicaţie. Cum $f(A) \subseteq A$, condiţia f nu este surjectivă (adică $f(A) \neq A$) este echivalentă cu faptul că numărul elementelor mulţimii $f(A)$ este strict mai mic decât numărul elementelor din A ceea ce are loc dacă şi numai dacă există cel puţin două elemente din A care au aceeaşi imagine prin f, adică dacă f nu este injectivă.

1.48. Răspuns. Deosebim două cazuri:
a) Dacă n este impar atunci f este bijectivă şi $f^{-1} : \mathbb{R} \to \mathbb{R}$, $f^{-1}(x) = \sqrt[n]{x}$.
b) Dacă n este par atunci f nu este nici injectivă şi nici surjectivă, dar $g : \mathbb{R}_+ \to \mathbb{R}_+$, $g(x) = x^n$ (unde $\mathbb{R}_+ = [0, \infty)$) este bijectivă şi $g^{-1} : \mathbb{R}_+ \to \mathbb{R}_+$, $g^{-1}(x) = \sqrt[n]{x}$.

1.49. a)$\Rightarrow$b). Dacă $f_*(X_1) = f_*(X_2)$ atunci $f(X_1) = f(X_2)$. Rezultă că pentru orice $x_1 \in X_1$ există un $x_2 \in X_2$ astfel încât $f(x_1) = f(x_2)$, de unde, conform lui a), urmează $x_1 = x_2$, adică $x_1 \in X_2$. Astfel am arătat că $X_1 \subseteq X_2$. Analog se arată că $X_2 \subseteq X_1$. Deci $f_*(X_1) = f_*(X_2)$ implică $X_1 = X_2$, adică f_* este injectivă.
b)$\Rightarrow$c). Pentru orice funcţie $f : A \to B$ şi orice $X \subseteq A$ are loc incluziunea

$$X \subseteq \overset{-1}{f}(f(X)) = (f^* \circ f_*)(X). \tag{1}$$

Dacă $x \in \overset{-1}{f}(f(X))$ atunci $f(x) \in f(X)$, adică există un element $x' \in X$ astfel încât $f(x) = f(x')$. Rezultă că $f_*(\{x\}) = f(\{x'\})$, ceea ce, conform lui b), implică $\{x\} = \{x'\}$, adică $x = x' \in X$. Astfel, am arătat că

$$(f^* \circ f_*)(X) \subseteq X. \tag{2}$$

Din (1) şi (2) umează c).
c)$\Rightarrow$d). Din c) urmează că f_* este o secţiune a lui f^*. Deci f^* are o secţiune, ceea ce ne arată că f^* este surjectivă.

d)$\Rightarrow$e). Incluziunea $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$ are loc pentru orice funcţie. Fie

$$y \in f(X_1) \cap f(X_2) \tag{3}$$

Din d) rezultă că există $Y_1, Y_2 \subseteq B$ astfel încât $f^*(Y_i) = X_i$ $(i = 1, 2)$, adică

$$\overset{-1}{f}(Y_i) = X_i. \tag{4}$$

Întrucât $f(\overset{-1}{f}(Y_i)) \subseteq Y_i$, din (3) şi (4) urmează că $y \in Y_1 \cap Y_2$. Aşadar,

$$\overset{-1}{f}\langle y\rangle \subseteq \overset{-1}{f}(Y_1 \cap Y_2) = \overset{-1}{f}(Y_1) \cap \overset{-1}{f}(Y_2) = X_1 \cap X_2,$$

deci există $x \in X_1 \cap X_2$ cu $f(x) = y$. Rezultă $y \in f(X_1 \cap X_2)$ şi astfel am demonstrat

$$f(X_1) \cap f(X_2) \subseteq f(X_1 \cap X_2).$$

Deci f verifică pe e).
e)$\Rightarrow$f). Dacă în e) luăm $X_1 = X$ şi $X_2 = C(X)$ atunci obţinem

$$\emptyset = f(X) \cap f(C(X)),$$

de unde rezultă că $f(C(X)) \subseteq C(f(X))$.
f)$\Rightarrow$a). Dacă $x, x' \in A$ şi $x \neq x'$ atunci $x' \in C(\{x\})$, prin urmare $f(x') \in f(C(\{x\}))$, ceea ce, conform lui f), implică $f(x') \in C(\{f(x)\})$, adică $f(x) \neq f(x')$. Deci f este injectivă.

1.50. Indicaţie. Rezolvarea este similară cu a problemei precedente.

1.51. Notăm cu (1) egalitatea ce trebuie demonstrată la a) şi cu (2) cea de la b).
a) Demonstrăm pe (1) prin inducţie după numărul natural nenul n. Pentru $n = 1$, egalitatea (1) devine

$$\overline{f}(X_1) = \overline{f}(X_1)$$

şi este, evident, adevărată. Examinăm şi cazul $n = 2$, care va fi folosit în partea deductivă a inducţiei. Pentru $n = 2$ egalitatea (1) devine

$$\overline{f}(X_1 \cup X_2) = \overline{f}(X_1) + \overline{f}(X_2) - \overline{f}(X_1 \cap X_2), \tag{3}$$

iar din definiţia lui $\overline{f}$ rezultă că această egalitate este adevărată.

Presupunem că egalitatea (1) este adevărată pentru $n = m - 1$ şi o demonstrăm pentru $n = m$. Într-adevăr, din asociativitatea reuniunii şi din (3) rezultă

$$\overline{f}\left(\bigcup_{i=1}^{m} X_i\right) = \overline{f}\left(\bigcup_{i=1}^{m-1} X_i\right) + \overline{f}(X_m) - \overline{f}((X_1 \cup \dots \cup X_{m-1}) \cap X_m).$$

Întrucât

$$(X_1 \cup \dots \cup X_{m-1}) \cap X_m = \bigcup_{i=1}^{m-1} (X_i \cap X_m),$$

aplicând ipoteza inducţiei, obţinem

$$\overline{f}\left(\bigcup_{i=1}^{m} X_i\right) = \sum_{i=1}^{m} \overline{f}(X_i) - \sum_{1\le i<j\le m-1} \overline{f}(X_i \cap X_j) + \cdots + (-1)^m \overline{f}\left(\bigcap_{i=1}^{m-1} X_i\right)$$
$$- \left[\sum_{i=1}^{m-1} \overline{f}(X_i \cap X_m) - \sum_{1\le i<j\le m-1} \overline{f}(X_i \cap X_j \cap X_m) + \cdots + (-1)^m \overline{f}\left(\bigcap_{i=1}^{m} X_i\right)\right].$$

Printr-o regrupare convenabilă a termenilor, primim egalitatea

$$\overline{f}\left(\bigcup_{i=1}^{m} X_i\right) = \sum_{i=1}^{m} \overline{f}(X_i) - \sum_{1\le i<j\le m} \overline{f}(X_i \cap X_j) + \cdots + (-1)^{m+1} \overline{f}\left(\bigcap_{i=1}^{m} X_i\right),$$

care trebuia demonstrată.

b) Dacă aplicăm pe (1) în cazul $A = \bigcup_{i=1}^{n} X_i$ şi $f : A \to \mathbb{N}$, $f(x) = 1$, obţinem (2).

1.52. a) Notăm cu $|M|$ numărul elementelor unei mulţimi finite M. Dacă $m > 0$ şi $n = 0$ atunci $\left|B^A\right| = 0$, iar dacă $m = n = 0$ atunci $\left|B^A\right| = 1$. Demonstrăm prin inducţie după $m \in \mathbb{N}^*$ că

(1) $$\left|B^A\right| = n^m.$$

Dacă $m = 1$ atunci evident $\left|B^A\right| = n = n^1$.

Presupunem că (1) este adevărată pentru $m = k$ şi demonstrăm că este adevărată pentru $m = k+1$. Dacă A este formată din $k+1$ elemente, iar A' este o submulţime a lui A formată din k elemente şi $x_0 \in A$, $x_0 \notin A'$ atunci $A = A' \cup \{x_0\}$. Cu ajutorul unei funcţii $g : A' \to B$, definim n funcţii diferite f_g^y, $y \in B$ astfel:

$$f_g^y = \begin{cases} g(x) & , \text{ dacă } x \in A' \\ y & , \text{ dacă } x = x_0. \end{cases}$$

Dacă $f \in B^A$, $y = f(x_0)$ şi g este restricţia lui f la A' atunci $f = f_g^y$. Deci

$$B^A = \bigcup \{f_g^y \mid y \in B, g \in B^{A'}\},$$

iar funcţia $F : B \times B^{A'} \to B^A$, $F(y, g) = f_g^y$ este bijectivă. Rezultă că

$$\left|B^A\right| = \left|B \times B^{A'}\right| = n \cdot n^k = n^{k+1}.$$

b) Dacă $m > n$ atunci numărul cerut este egal cu zero. Fie $m \le n$. Demonstrăm (în acest caz) prin inducţie după m că numărul cerut este

$$A_n^m = n(n-1)\ldots(n-m+1).$$

Dacă $m = 1 \le n$ atunci există n funcţii de la A la B şi fiecare este injectivă. Deci, în acest caz, afirmaţia este adevărată.

Presupunem afirmaţia adevărată pentru $m = k < n$ şi o demonstrăm pentru $m = k + 1$. Dacă $|A| = k + 1$, iar $A' \subseteq A$, $|A'| = k$ şi $x_0 \in A$, $x_0 \notin A'$ atunci

$A = A' \cup \{x_0\}$. O funcţie $f : A \to B$ este determinată în mod unic de $f(x_0)$ şi de restricţia f' a lui f la A'. Dacă f este injectivă atunci f' este injectivă, iar dacă f' este injectivă atunci f este injectivă dacă şi numai dacă $f(x_0) \notin f(A')$. Deci, f' fiind fixat, există $n-k$ posibilităţi de alegere pentru $f(x_0)$. Conform ipotezei inducţiei, f' se poate alege în

$$A_n^k = n(n-1)\dots(n-k+1).$$

Deci există

$$(n-k)A_n^k = A_n^{k+1}$$

posibilităţi de a defini pe f.
c) Dacă $m \neq n$ atunci numărul cerut este 0. Dacă $m = n$ atunci funcţia $f : A \to B$ este bijectivă dacă şi numai dacă este injectivă. Deci, în acest caz, rezultă din b) că numărul cerut este

$$A_n^n = n! = P_n.$$

d) Dacă $m < n$ atunci numărul cerut este zero. Presupunem că $m \geq n$. Fie $A = \{x_1, \dots, x_m\}$ şi $B = \{y_1, \dots, y_n\}$. Dacă S este mulţimea funcţiilor surjective de la A la B, iar

$$S_i = \{f \in B^A \mid y_i \notin f(A)\} \ (i = 1, \dots, n)$$

atunci $S = B^A \setminus \bigcup_{i=1}^n S_i$, de unde rezultă că $|S| = \left|B^A\right| - \left|\bigcup_{i=1}^n S_i\right|$. Acum, din a) şi din problema precedentă deducem

$$|S| = n^m - \sum_{i=1}^n |S_i| + \sum_{1 \leq i < j \leq n} |S_i \cap S_j| - \dots + (-1)^n \left|\bigcap_{i=1}^n S_i\right|. \tag{2}$$

Pe de altă parte, din definiţia lui S_i rezultă că numărul funcţiilor din S_i coincide cu numărul funcţiilor definite pe A şi cu valori în $B \setminus \{y_i\}$. Deci acest număr este $(n-1)^m$, adică

$$|S_i| = (n-1)^m. \tag{3}$$

Numărul funcţiilor din $S_i \cap S_j$ coincide cu numărul funcţiilor definite pe A şi cu valori în $B \setminus \{y_i, y_j\}$, adică

$$|S_i \cap S_j| = (n-2)^m.$$

Analog se obţin egalităţile

$$|S_i \cap S_j \cap S_k| = (n-3)^m, \dots, \left|\bigcap_{i=1}^n S_i\right| = 0. \tag{4}$$

Din (2), (3) şi (4) rezultă

$$|S| = n^m - C_n^1(n-1)^m + C_n^2(n-2)^m - C_n^3(n-3)^m + \dots + (-1)^{n-1}C_n^{n-1}.$$

1.53. Fie $g : \mathbb{R} \to \mathbb{R}$, $g(x) = x^n$.
a) Avem
$$f(x^n) = x, \forall x \in \mathbb{R} \Leftrightarrow f \circ g = 1_{\mathbb{R}}.$$
Deci există f (cu proprietatea cerută) dacă şi numai dacă funcţia g este injectivă, iar g este injectivă dacă şi numai dacă n este impar. Prin urmare, există f dacă şi numai dacă n este impar. Dacă n este impar atunci g este chiar bijectivă, de unde rezultă că f este unică şi $f(x) = \sqrt[n]{x}$, dacă $n \geq 3$, iar dacă dacă $n = 1$ atunci $f(x) = x$.
b) Avem
$$[f(x)]^n = x, \forall x \in \mathbb{R} \Leftrightarrow g \circ f = 1_{\mathbb{R}}.$$
Deci există f (cu proprietatea cerută) dacă şi numai dacă g este surjectivă, iar g este surjectivă dacă şi numai dacă n este impar. Prin urmare, există f dacă şi numai dacă n este impar. Dacă n este impar atunci g este chiar bijectivă, de unde rezultă că f este unică şi $f(x) = \sqrt[n]{x}$, dacă $n \geq 3$, iar dacă dacă $n = 1$ atunci $f(x) = x$.

1.54. Indicaţie. Condiţia din enunţ exprimă faptul că g admite o retractă, ceea ce nu e cazul, deoarece o funcţie pară sau periodică nu e injectivă.

1.55. Dacă f este bijectivă şi $s_1, s_2 : B \to A$ sunt secţiuni ale lui f, adică
$$f \circ s_1 = 1_B = f \circ s_2,$$
atunci (compunând din stânga cu f^{-1}) rezultă $s_1 = f^{-1} = s_2$. Deci f are o singură secţiune şi anume pe f^{-1}.

Invers, presupunem că f are o secţiune unică. Rezultă că f este surjectivă. Dacă f nu ar fi injectivă atunci ar exista două elemente $x_1, x_2 \in A$, $x_1 \neq x_2$ astfel încât $f(x_1) = f(x_2) = y_0$ şi am putea construi două secţiuni diferite $s_1, s_2 : B \to A$ astfel:
$$s_i(y) = \begin{cases} x_i & , \text{ dacă } y = y_0 \\ x_y & , \text{ dacă } y \neq y_0 \end{cases}$$
unde $i = 1, 2$ şi x_y este o soluţie a ecuaţiei $f(x) = y$. Astfel am ajuns la o contradicţie. Deci f este şi injectivă. Rezultă că f este bijectivă.

1.56. a) Dacă $A = \emptyset$ şi B este o mulţime oarecare atunci există o singură funcţie cu domeniul A şi codomeniul B, graficul acestei funcţii fiind $\emptyset$. Această funcţie este injectivă, iar dacă $B \neq \emptyset$, atunci nu are nici o retractă, deoarece nu există nici o funcţie cu domeniul $B \neq \emptyset$ şi codomeniul $A = \emptyset$.
b) Dacă $|A| = 1$, $|B| > 1$ şi $f : A \to B$ atunci f este injectivă, dar nu este surjectivă, iar din B în A există o singură funcţie, care este retractă a lui f.
c) Dacă f este bijectivă şi $r_1, r_2 : B \to A$ sunt retracte ale lui f, adică
$$r_1 \circ f = 1_A = r_2 \circ f$$
atunci (compunând la dreapta cu f^{-1}) rezultă $r_1 = f^{-1} = r_2$. Deci f are o singură retractă şi anume pe f^{-1}.

Invers, presupunem că $|A| > 1$ şi că f are o retractă unică. Rezultă că f este injectivă. Fie $x_1, x_2 \in A$, $x_1 \neq x_2$. Dacă f nu ar fi surjectivă atunci ar exista $y_0 \in B \setminus f(A)$ şi am putea construi două retracte diferite $r_1, r_2 : B \to A$ astfel: dacă $y \in B \setminus f(A)$, atunci $r_i(y) = x_i$, iar dacă $y \in f(A)$, atunci $r_i(y) = x$, unde x este unicul element din A pentru care avem $f(x) = y$. Astfel am ajuns la o contradicţie. Deci f este şi surjectivă. Rezultă că f este bijectivă.

1.57. Indicaţii. Descompunem pe f în produsul (compusa) unei injecţii cu o surjecţie astfel: $f = i \circ f'$, unde $f' : A \to f(A)$, $f'(x) = f(x)$ şi $i : f(A) \to B$, $i(y) = y$. Întrucât f' este o surjecţie şi $f(A) \neq \emptyset$, deoarece $A \neq \emptyset$, iar i este o injecţie, urmează că f' are o secţiune $s : f(A) \to A$ şi i are o retractă $r : B \to f(A)$. Definind pe $g : B \to A$ prin $g = s \circ r$ avem

$$\begin{aligned} f \circ g \circ f &= (i \circ f') \circ (s \circ r) \circ (i \circ f') = i \circ (f' \circ s) \circ (r \circ i) \circ f' \\ &= i \circ 1_{f(A)} \circ 1_{f(A)} \circ f' = i \circ f' = f. \end{aligned}$$

Deci $g = s \circ r$ verifică condiţia cerută. Întrucât o funcţie injectivă care nu este surjectivă poate avea mai multe retracte, iar o funcţie surjectivă care nu este injectivă poate avea mai multe secţiuni, propunem cititorului să construiască un exemplu care să arate că, în general, g nu este unic determinată.

1.58. Indicaţie. Dacă $R \subseteq A \times B$ atunci definim funcţia $\overline{R} : A \to \mathcal{P}(B)$, $\overline{R}(x) = R\langle x \rangle$. Funcţia $f : \{R \mid R \subseteq A \times B\} \to [\mathcal{P}(B)]^A$, $f(R) = \overline{R}$ este bijectivă.

1.59. Indicaţie. Dacă $R \subseteq A \times B$ atunci definim funcţia $\overline{R} : \mathcal{P}(A) \to \mathcal{P}(B)$ prin $\overline{R}(X) = R(X)$. Funcţia $f : \mathcal{R} \to \mathcal{F}$, $f(R) = \overline{R}$ este bijectivă.

1.60. Egalitatea $f = h \circ g$ ne arată că diagrama

$$\begin{tikzcd} \mathbb{R} \arrow[r, "f"] \arrow[d, "g"'] & \mathbb{R} \\ \mathbb{R}_+ \arrow[ur, dotted, "h"'] & \end{tikzcd}$$

este comutativă. Întrucât funcţia g este surjectivă şi

$$g(x_1) = g(x_2) \Rightarrow x_1^2 = x_2^2 \Rightarrow x_1 = \pm x_2 \Rightarrow \cos x_1 = \cos x_2 \Rightarrow f(x_1) = f(x_2),$$

(din teorema de factorizare a unei funcţii printr-o surjecţie) rezultă existenţa şi unicitatea funcţiei h cu proprietatea cerută. Din aceeaşi teoremă urmează că dacă $s : \mathbb{R}_+ \to \mathbb{R}$ este o secţiune a lui g atunci $h = f \circ s$. Întrucât funcţia $s : \mathbb{R}_+ \to \mathbb{R}$, $s(x) = \sqrt{x}$ este o secţiune a lui g rezultă că funcţia $h : \mathbb{R}_+ \to \mathbb{R}$ este definită prin

$$h(x) = (f \circ s)(x) = \cos \sqrt{x}.$$

1.61. Răspuns. Nu.

1.62. Egalitatea $f = g \circ h$ ne arată că diagrama

$$\begin{tikzcd} \mathbb{R} & \mathbb{R} \arrow[l, "f"'] \arrow[dl, dotted, "h"] \\ A \arrow[u, "g"] & \end{tikzcd}$$

este comutativă. Întrucât funcţia g este injectivă şi

$$f(\mathbb{R}) = [-1, 1] \subseteq [-3, +\infty) = g(A),$$

(din teorema de factorizare a unei funcţii printr-o injecţie) rezultă existenţa şi unicitatea lui h cu proprietatea cerută. Din aceeaşi teoremă urmează că dacă $r : \mathbb{R} \to A$ este o retractă a lui g atunci $h = r \circ f$. Funcţia $r : \mathbb{R} \to A$,

$$r(x) = \begin{cases} \dfrac{x-1}{2} & , \text{ dacă } x \in [-3, +\infty) \\ 0 & , \text{ dacă } x \in (-\infty, -3) \end{cases}$$

fiind o retractă a lui g, deducem că funcţia $h : \mathbb{R} \to A$ este definită prin

$$h(x) = (r \circ f)(x) = \frac{\cos x - 1}{2}.$$

1.63. Răspuns. Nu.

1.64. Răspuns. $\varphi_{A,B}((a,b)) = (b,a)$.

1.65. Răspuns. $\varphi_{A,B,C}(((a,b),c)) = (a,(b,c))$.

1.66. Indicaţie. Fie funcţiile $f_i : A_i \to B_i$, $i \in I$ şi pentru fiecare i din I fie $X_i \subseteq A_i$, $Y_i \subseteq B_i$. Folosind definiţia produsului cartezian al unei familii de funcţii

$$\prod_{i\in I} f_i : \prod_{i\in I} A_i \to \prod_{i\in I} B_i, \ \left(\prod_{i\in I} f_i\right)((a_i)_{i\in I}) = (f_i(a_i))_{i\in I}$$

se demostrează că

$$\left(\prod_{i\in I} f_i\right)\left(\prod_{i\in I} X_i\right) = \prod_{i\in I}(f_i(X_i)) \text{ şi } \overset{-1}{\overline{\prod_{i\in I} f_i}}\left(\prod_{i\in I} Y_i\right) = \prod_{i\in I}\left(\overset{-1}{f_i}(Y_i)\right).$$

1.67. Indicaţie. Fie funcţiile $f_i : A \to B_i$, $i \in I$ şi pentru fiecare $i \in I$ fie $Y_i \subseteq B_i$. Se arată că funcţia $h : A \to \prod\limits_{i\in I} B_i$, $h(a) = (f_i(a))_{i\in I}$ verifică egalitatea

$$\overset{-1}{h}\left(\prod_{i\in I} Y_i\right) = \bigcap_{i\in I} \overset{-1}{h}(Y_i).$$

1.68. Indicaţie. Se folosesc definiţiile injectivităţii, surjectivităţii şi a produsului cartezian a două funcţii.

1.69. Dacă $f : A \to A'$ şi $g : B \to B'$ sunt funcţii date atunci $f \times g$ este singura funcţie pentru care pătratele diagramei sunt comutative:

$$\begin{tikzcd} A \arrow[d, "f"'] & A \times B \arrow[l, "p_1"'] \arrow[r, "p_2"] \arrow[d, "f\times g"'] & B \arrow[d, "g"] \\ A' & A' \times B' \arrow[l, "p_1'"'] \arrow[r, "p_2'"] & B' \end{tikzcd}$$

unde p_i, p_i' $(i = 1, 2)$ sunt proiecţiile canonice. Rezultă că F este de forma cerută dacă şi numai dacă există $f : A \to A'$ şi $g : B \to B'$ astfel încât diagrama

$$\begin{tikzcd} A \arrow[d, dotted, "f"'] & A \times B \arrow[l, "p_1"'] \arrow[r, "p_2"] \arrow[d, "F"'] & B \arrow[d, dotted, "g"] \\ A' & A' \times B' \arrow[l, "p_1'"'] \arrow[r, "p_2'"] & B' \end{tikzcd}$$

să fie comutativă. Întrucât p_i $(i = 1, 2)$ sunt surjecţii, din teorema de factorizare a unei funcţii printr-o surjecţie rezultă că existenţa lui f şi g este echivalentă cu implicaţiile

$$p_i(a_1, b_1) = p_i(a_2, b_2) \Rightarrow (p'_i \circ F)(a_1, b_1) = (p'_i \circ F)(a_2, b_2)$$

pentru $i = 1, 2$, care exprimă faptul că au loc egalităţile:

$$p'_1(F(a, b_1)) = p'_1(F(a, b_2)) \text{ şi } p'_2(F(a_1, b)) = p'_2(F(a_2, b))$$

pentru orice a, a_1, $a_2 \in A$ şi orice b, b_1, $b_2 \in B$. Prin urmare, dacă F nu verifică una din egalităţile de mai sus, atunci F nu se poate scrie sub forma cerută. De exemplu, dacă $A = B = A' = B' = \{1, 2\}$ şi $F : A \times B \to A \times B$ este funcţia definită prin tabelul

(x, y)	(1,1)	(1,2)	(2,1)	(2,2)
$F(x, y)$	(2,1)	(1,2)	(1,1)	(2,2)

atunci F nu se poate scrie sub forma cerută.

1.70. Indicaţie. a) Funcţia $u : A_1 \overset{\circ}{\cup} A_2 \to B$ este definită astfel:

$$u(i, a_i) = \begin{cases} u_1(a_1) & , \text{ dacă } i = 1 \\ u_2(a_2) & , \text{ dacă } i = 2. \end{cases}$$

b) Se aplică unicitatea lui u.
c) Dacă tripletul (A, q'_1, q'_2) are aceeaşi proprietate de universalitate ca şi $(A_1 \overset{\circ}{\cup} A_2, q_1, q_2)$ atunci din proprietatea de universalitate a lui $A_1 \overset{\circ}{\cup} A_2$ rezultă că există $v : A_1 \overset{\circ}{\cup} A_2 \to A$ astfel încât

$$(1) \qquad v \circ q_1 = q'_1 \text{ şi } v \circ q_2 = q'_2,$$

iar din proprietatea de universalitate a lui A urmează că există o funcţie $v' : A \to A_1 \overset{\circ}{\cup} A_2$ astfel încât

$$(2) \qquad v' \circ q'_1 = q_1 \text{ şi } v' \circ q'_2 = q_2.$$

Din (1), (2) şi b) se deduce că $v' \circ v = 1_{A_1 \overset{\circ}{\cup} A_2}$ si $v \circ v' = 1_A$, ceea ce ne arată că v este o bijecţie şi $v^{-1} = v'$.

Observaţii: i) Proprietatea de universalitate a reuniunii disjuncte este duala proprietăţii de universalitate a produsului cartezian.
ii) Reuniunea disjunctă se poate generaliza pentru o familie arbitrară $(A_i)_{i \in I}$ de mulţimi. Se obţine mulţimea

$$\overset{\circ}{\bigcup_{i \in I}} A_i = \bigcup_{i \in I} (\{i\} \times A_i),$$

care împreună cu injecţiile canonice corespunzătoare

$$q_j : A_j \to \overset{\circ}{\bigcup_{i \in I}} A_i, \ q_j(a_j) = (j, a_j), \forall a_j \in A_j \ (j \in I)$$

verifică o proprietate de universalitate analogă celei din problema **1.70** (fiind, astfel, unic determinată până la o bijecţie).

1.71. Indicaţie. Se determină cele patru elemente ξ_i $(i = 1, 2, 3, 4)$ din A^A şi pentru orice $b \in B$ avem $f^g(\xi_i)(b) = (f \circ \xi_i \circ g)(b) = f(\xi_i(g(b)))$.

1.72. Indicaţie. Se foloseşte caracterizarea funcţiilor injective cu ajutorul proprietăţii de simplificare.

1.73. Indicaţie. Se foloseşte caracterizarea funcţiilor surjective cu ajutorul proprietăţii de simplificare.

1.74. Avem $f^g : A_1^{B_1} \to A_2^{B_2}$. Fie $\xi, \xi' \in A_1^{B_1}$ şi $\eta \in A_2^{B_2}$.
a) Dacă f este injectivă şi g este surjectivă atunci:

$$f^g(\xi) = f^g(\xi') \Rightarrow f \circ \xi \circ g = f \circ \xi' \circ g \Rightarrow \xi = \xi',$$

adică f^g este injectivă.
b) Dacă f este surjectivă şi g este injectivă, atunci f are o secţiune s şi g are o retractă r, de unde urmează că ecuaţia

$$f^g(\xi) = \eta$$

are soluţia $\xi = s \circ \eta \circ r$, adică f^g este surjectivă.

1.75. Indicaţie. Bijectivitatea lui φ este o consecinţă a proprietăţii de universalitate a produsului cartezian. Comutativitatea diagramei din enunţ se stabileşte punctual.

1.76. Indicaţie. Dacă $\varphi(f) = \varphi(f') = F$ atunci $f_y = f'_y$ pentru orice $y \in B_2$, adică $f(x, y) = f'(x, y)$, pentru orice $x \in B_1,\ y \in B_2$, aşadar $f = f'$. Dacă $F \in (A^{B_1})^{B_2}$ atunci pentru orice $y \in B_2$, $F(y) \in A^{B_1}$. Definind funcţia $f \in A^{B_1 \times B_2}$ prin $f(x, y) = (F(y))(x)$, avem $f_y = F(y)$, deci $\varphi(f) = F$. Comutativitatea diagramei din enunţ se stabileşte punctual.

1.77. Indicaţii. c) $x \in pr_1 R \Rightarrow \exists y \in A :\ xRy \Rightarrow xRy$ şi $\ yRx \Rightarrow xRx.$
d) Este o consecinţă imediată a punctului c).

1.78. *Greşeala este următoarea*: poate să existe $x \in A$ pentru care nu există nici un $y \in A$ astfel încât xRy.

1.79. Arătăm că nici una din axiome nu este o consecinţă a celorlalte:
• *Simetria* nu rezultă din reflexivitate şi tranzitivitate deoarece relaţia $\leq$ în $\mathbb{R}$ este reflexivă şi tranzitivă, dar nu este simetrică.
• *Reflexivitatea* nu este o consecinţă a simetriei şi a tranzitivităţii deoarece relaţia de paralelism între dreptele din plan este simetrică şi tranzitivă, dar nu este reflexivă.
• Fie $A = \{1, 2, 3\}$ şi $\rho = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3), (3, 2)\} \subseteq A \times A$. Relaţia ρ este reflexivă şi simetrică, dar nu este tranzitivă. Deci *tranzitivitatea* este independentă de reflexivitate şi simetrie.

Observaţii: Relaţiile reflexive, simetrice sau tranzitive pe o mulţime finită A pot fi caracterizate folosind identificarea relaţiilor binare cu matrice (bivalente) pe care am descris-o în observaţiile ce succed problema **1.2**. Astfel:
• cum o relaţie este reflexivă dacă şi numai dacă conţine pe Δ_A, toate elementele de pe diagonala matricei asociate acestei relaţii vor fi egale cu 1;

• cum o relaţie este simetrică dacă şi numai dacă coincide cu inversa sa, deducem că o relaţie este simetrică dacă şi numai dacă se va reprezenta printr-o matrice simetrică faţă de diagonala principală;
• verificarea tranzitivităţii unei relaţii se face ţinând seama de faptul că o relaţie R este tranzitivă dacă şi numai dacă $R \circ R \subseteq R$ şi de observaţiile anterioare.

Propunem cititorului să ilustreze independenţa axiomelor ce definesc o relaţie de echivalenţă folosind observaţiile de mai sus.

1.80. $\Delta_A \subseteq \Delta_A \circ \Delta_A \subseteq R \circ S$. Analog $\Delta_A \subseteq S \circ R$.

1.81. Dacă $R \circ S$ este simetrică atunci $R \circ S = \overset{-1}{\overline{R \circ S}} = \overset{-1}{S} \circ \overset{-1}{R} = S \circ R$. Reciproc, dacă $R \circ S = S \circ R$ atunci $\overset{-1}{\overline{R \circ S}} = \overset{-1}{S} \circ \overset{-1}{R} = S \circ R = R \circ S$.

1.82. $(R \circ S) \circ (R \circ S) = R \circ (S \circ R) \circ S = R \circ (R \circ S) \circ S = (R \circ R) \circ (S \circ S) \subseteq R \circ S$

1.83. Dacă R este o relaţie de echivalenţă atunci R este reflexivă, simetrică şi tranzitivă. Folosind tranzitivitatea şi simetria avem

$$xRy \text{ şi } yRz \Rightarrow xRz \Rightarrow zRx,$$

adică R este circulară. Invers, dacă R este reflexivă şi circulară atunci

$$xRy \Rightarrow xRy \text{ şi } yRy \Rightarrow yRx,$$

adică R este simetrică. Folosind faptul că R este circulară şi simetrică, avem

$$xRy \text{ şi } yRz \Rightarrow zRx \Rightarrow xRz,$$

adică R este tranzitivă. Deci R este o relaţie de echivalenţă.

1.84. Indicaţie. Se folosesc definiţiile reflexivităţii, simetriei şi tranzitivităţii.

1.85. Răspuns. a) ρ_1 este o relaţie de echivalenţă pe A, dar ρ_2 nu este echivalenţă. Partiţia corespunzătoare echivalenţei ρ_1 este $A/\rho_1 = \{\{1,2,3\},\{4\}\}$.
b) π_1 este o partiţie a lui A, iar π_2 nu este o partiţie. Relaţia de echivalenţă corespunzătoare partiţiei π_1 este

$$\begin{aligned}\rho &= \{(1,1),(2,2),(1,2),(2,1),(3,3),(4,4)\}\\ &= (\{1,2\}\times\{1,2\}) \cup (\{3\}\times\{3\}) \cup (\{4\}\times\{4\}).\end{aligned}$$

1.86. Cum fiecare relaţie de echivalenţă pe A este determinată de o partiţie a lui A prezentăm mai jos partiţiile lui A şi alături echivalenţele corespunzătoare:

$$\pi_1 = \{\{1\},\{2\},\{3\}\},\ \rho_1 = \Delta_A;$$

$$\pi_2 = \{A\},\ \rho_2 = A \times A;$$

$$\pi_3 = \{\{1\},\{2,3\}\},\ \rho_3 = \{(1,1),(2,2),(3,3),(2,3),(3,2)\};$$

$$\pi_4 = \{\{2\},\{1,3\}\},\ \rho_4 = \{(1,1),(2,2),(3,3),(1,3),(3,1)\};$$

$$\pi_5 = \{\{3\},\{1,2\}\},\ \rho_5 = \{(1,1),(2,2),(3,3),(1,2),(2,1)\}.$$

1.87. Răspuns. $A/\Delta_A = \{\{a\} \mid a \in A\}$, $A/A \times A = \{A\}$.

1.88. Răspuns. Clasele de echivalenţă ale unui $z \in \mathbb{C}^*$ modulo ρ_1 şi ρ_2 sunt

$$\rho_1\langle z\rangle = \{z' \in \mathbb{C} \mid |z| = |z'|\}, \text{ respectiv } \rho_2\langle z\rangle = \{z' \in \mathbb{C} \mid \arg z = \arg z'\},$$

adică $\rho_1\langle z\rangle$ este mulţimea punctelor de pe cercul cu centrul în origine şi de rază $|z|$, iar $\rho_2\langle z\rangle$ este mulţimea punctelor de pe semidreapta deschisă care pleacă din origine şi trece prin z. Menţionăm că $\rho_i\langle 0\rangle = \{0\}$ $(i = 1, 2)$, iar mulţimile cât sunt

$$\mathbb{C}/\rho_i = \{\rho_i\langle z\rangle \mid z \in \mathbb{C}\} \ (i = 1, 2).$$

1.89. Indicaţie. Clasele de echivalenţă modulo ρ_1 au ca reprezintare geometrică drepte paralele cu Oy, iar clasele modulo ρ_2, drepte paralele cu Ox.

1.90. Indicaţie. Se aplică [34, Teorema 1.8.15] funcţiilor $f : \mathbb{R} \to \mathbb{Z}$, $f(x) = [x]$ şi $g : \mathbb{R} \to [0, 1)$, $g(x) = \{x\}$.

1.91. Indicaţie. Se arată că egalitatea $f(\rho\langle A\rangle) = \det A$ este independentă de alegerea reprezentantului $A \in \rho\langle A\rangle$, adică defineşte o funcţie $f : M_n(\mathbb{R})/\rho \to \mathbb{R}$, iar după aceea se stabileşte că f este o bijecţie.

1.92. Indicaţie. Dacă R este o relaţie de echivalenţă atunci familia $R\langle x\rangle$, $x \in A$ verifică condiţiile de mai sus.

1.93. Răspuns. $E(A)$ este închisă în raport cu intersecţia şi cu inversarea.

1.94. Indicaţii. Dacă $p_i : A_i \to A_i/R_i$ $(i = 1, 2)$ sunt funcţiile canonice atunci funcţia $p_1 \times p_2 : A_1 \times A_2 \to (A_1/R_1) \times (A_2/R_2)$ este surjectivă şi $\ker(p_1 \times p_2) = R$, deci R este o echivalenţă şi există o bijecţie între $(A_1/R_1) \times (A_2/R_2)$ şi $(A_1 \times A_2)/R$..
Altfel: Se poate proceda şi arătând că egalitatea

$$f((R_1\langle a_1\rangle, R_2\langle a_2\rangle)) = R\langle(a_1, a_2)\rangle$$

defineşte o funcţie $f : (A_1/R_1) \times (A_2/R_2) \to (A_1 \times A_2)/R$, adică nu depinde de alegerea reprezentanţilor, iar după aceea stabilind că f este o bijecţie.

1.95. Dacă $x_1, x_2 \in \mathbb{R}$ atunci

$$(x_1, x_2) \in \ker f \Leftrightarrow x_1^2 = x_2^2 \Leftrightarrow x_1 = \pm x_2 \Leftrightarrow x_1^4 = x_2^4 \Leftrightarrow (x_1, x_2) \in \ker g,$$

ceea ce ne arată că $\ker f = \ker g$ şi $\mathbb{R}/\ker f = \{\{-x, x\} \mid x \in \mathbb{R}\}$.

Întrucât $f(\mathbb{R}) = \mathbb{R}_+$, din [34, Teorema 1.8.15] urmează că există o funcţie bijectivă $\overline{f} : \mathbb{R}/\ker f \to \mathbb{R}_+$ astfel încât diagrama

$$\begin{tikzcd}
\mathbb{R} \arrow[r, "f"] \arrow[d, "p_{\ker f}"'] & \mathbb{R} \\
\mathbb{R}/\ker f \arrow[r, dotted, "\overline{f}"] & \mathbb{R}_+ \arrow[u, "i"']
\end{tikzcd}$$

să fie comutativă, unde i este funcţia de incluziune şi $p_{\ker f}$ este funcţia canonică. Din comutativitatea diagramei de mai sus urmează că

$$\overline{f}(\{-x, x\}) = x^2.$$

1.96. Indicaţie. Avem $(1, i) \in \ker g$ şi $(1, i) \notin \ker f$, iar bijecţiile $\mathbb{C}/\ker f \to \mathbb{C}$ şi $\mathbb{C}/\ker f \to \mathbb{C}$ se pot obţine aplicând [34, Teorema 1.8.15] funcţiilor f, respectiv g.

1.97. Fie $0 < k \leq m$ şi

$$n_k = |\{\rho \in E(A) \mid |A/\rho| = k\}|,$$

adică n_k este numărul acelor relaţii de echivalenţă pe A ale căror mulţimi cât sunt formate din k clase. Avem

$$|E(A)| = n_1 + n_2 + \cdots + n_m.$$

Reducem determinarea lui n_k la determinarea numărului de surjecţii ale lui A pe o mulţime K formată din k elemente. Dacă $f : A \to K$ este o funcţie surjectivă, atunci, conform teoremei de factorizare a unei funcţii printr-o surjecţie, există o funcţie bijectivă unică $\overline{f} : A/\ker f \to K$ astfel încât diagrama următoare să fie comutativă

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "p_{\ker f}"'] & K . \\ A/\ker f \arrow[ur, dotted, "\overline{f}"'] & \end{tikzcd}$$

Deci $|A/\ker f| = k$. Fie S mulţimea surjecţiilor de la A la K şi

$$E_k(A) = \{\rho \in E(A) \mid |A/\rho| = k\}.$$

Rezultatele obţinute ne permit să definim funcţia

$$\varphi : S \to E_k(A),\ \varphi(f) = \ker f.$$

Dacă $\rho \in E_k(A)$ şi $h : A/\rho \to K$ este o bijecţie atunci $\varphi(h \circ p_\rho) = \rho$. Deci funcţia φ este surjectivă. Avem

$$(f, f') \in \ker \varphi \Leftrightarrow \ker f = \ker f' \Leftrightarrow f = h \circ f',$$

unde $h : K \to K$ este o bijecţie. Rezultă că

$$f \neq f' \Leftrightarrow h \neq 1_S,$$

aşadar fiecare clasă din $S/\ker f$ are $k!$ elemente şi astfel

(1) $$|S/\ker \varphi| = \frac{|S|}{k!}.$$

Din [34, Teorema 1.8.15] deducem că există o bijecţie între $S/\ker \varphi$ şi $E_k(A)$, ceea ce, împreună cu (1) şi problema **1.52**, ne conduce la

$$n_k = |E_k(A)| = \frac{1}{k!}\left[k^m - C_k^1(k-1)^m + \cdots + (-1)^{k-1}C_k^{k-1}\right].$$

1.98. $\overset{-1}{R} \circ \overset{-1}{\overline{\overset{-1}{R}}} \circ \overset{-1}{R} = \overset{-1}{R} \circ R \circ \overset{-1}{R} = \overset{-1}{\overline{R \circ \overset{-1}{R} \circ R}} = \overset{-1}{R}.$

1.99. $d_1 \perp d_2,\ d_2 \perp d_3$ şi $d_3 \perp d_4 \Rightarrow (d_1 \| d_3$ sau $d_1 = d_3)$ şi $d_3 \perp d_4 \Rightarrow d_1 \perp d_4$.

1.100. $F \circ \overset{-1}{F} \circ F \subseteq \Delta_B \circ F = F$ şi $F \circ \overset{-1}{F} \circ F \supseteq F \circ \Delta_A = F$.

Observaţie: Din problemele **1.99** şi **1.100** rezultă că funcţiile formează o subclasă a clasei relaţiilor difuncţionale şi că incluziunea aceasta este strictă.

1.101. a)$\Rightarrow$b). Din $R\langle a_1\rangle \cap R\langle a_2\rangle \neq \emptyset$ rezultă că există $b_0 \in R\langle a_1\rangle \cap R\langle a_2\rangle$, adică $a_1 R b_0$ şi $a_2 R b_0$, ceea ce implică

$$a_2 R b_0 \text{ şi } b_0 \overset{-1}{R} a_1. \tag{1}$$

Dacă $b \in R\langle a_1\rangle$ atunci $a_1 R b$, care împreună cu (1) ne dă $(a_2, b) \in R \circ \overset{-1}{R} \circ R$. Deci, conform lui a), avem $(a_2, b) \in R$, adică $b \in R\langle a_2\rangle$. Astfel s-a arătat că $R\langle a_1\rangle \subseteq R\langle a_2\rangle$. Analog se arată că $R\langle a_2\rangle \subseteq R\langle a_1\rangle$. Deci $R\langle a_1\rangle = R\langle a_2\rangle$.
b)$\Rightarrow$c). Din $\overset{-1}{R}\langle b_1\rangle \cap \overset{-1}{R}\langle b_2\rangle \neq \emptyset$ rezultă că există $a_0 \in \overset{-1}{R}\langle b_1\rangle \cap \overset{-1}{R}\langle b_2\rangle$, adică $a_0 R b_1$ şi $a_0 R b_2$, ceea ce implică

$$b_1, b_2 \in R\langle a_0\rangle. \tag{2}$$

Dacă $a \in \overset{-1}{R}\langle b_1\rangle$ atunci $a R b_1$, adică $b_1 \in R\langle a\rangle$, ceea ce împreună cu (2) implică $R\langle a\rangle \cap R\langle a_0\rangle \neq \emptyset$. Deci, conform lui b), urmează că $R\langle a\rangle = R\langle a_0\rangle$. Acum, din (2) deducem că $b_2 \in R\langle a\rangle$, de unde obţinem $a \in \overset{-1}{R}\langle b_2\rangle$. Astfel am arătat că $\overset{-1}{R}\langle b_1\rangle \subseteq \overset{-1}{R}\langle b_2\rangle$. Incluziunea inversă se demonstrează analog. Deci $\overset{-1}{R}\langle b_1\rangle = \overset{-1}{R}\langle b_2\rangle$.
c)$\Rightarrow$b). Demonstraţia acestei implicaţii este similară cu cea a implicaţiei precedente.
c)$\Rightarrow$d). Fie $B_i, i \in I$ o indexare bijectivă a mulţimii

$$\{R\langle x\rangle \mid x \in A \text{ şi } R\langle x\rangle \neq \emptyset\}.$$

Pentru fiecare $i \in I$ alegem câte un $y_i \in B_i$ şi fie $A_i = \overset{-1}{R}\langle y_i\rangle$. Din c) rezultă că $A_i, i \in I$ verifică următoarea condiţie

$$i_1, i_2 \in I \text{ şi } A_{i_1} \cap A_{i_2} \neq \emptyset \ \Rightarrow\ A_{i_1} = A_{i_2}. \tag{3}$$

Întrucât c)$\Rightarrow$ b), urmează că $B_i, i \in I$ verifică următoarea condiţie

$$i_1, i_2 \in I \text{ şi } B_{i_1} \cap B_{i_2} \neq \emptyset \ \Rightarrow\ B_{i_1} = B_{i_2}. \tag{4}$$

Să demonstrăm că

$$R = \bigcup_{i \in I} A_i \times B_i. \tag{5}$$

Dacă $(a, b) \in R$ atunci $b \in R\langle a\rangle$ şi $a \in \overset{-1}{R}\langle b\rangle$, iar din (4) rezultă că pentru orice $b' \in R\langle a\rangle$ avem $\overset{-1}{R}\langle b'\rangle = \overset{-1}{R}\langle b\rangle$. Deci există $i \in I$ astfel încât $a \in A_i = \overset{-1}{R}\langle b\rangle$ şi $b \in B_i = R\langle a\rangle$. Prin urmare, am arătat că

$$R \subseteq \bigcup_{i \in I} A_i \times B_i. \tag{6}$$

Dacă $(a,b) \in \bigcup_{i\in I} A_i \times B_i$ atunci există $i \in I$ astfel încât $(a,b) \in A_i \times B_i$, de unde rezultă că $b \in B_i = R\langle a\rangle$, ceea ce implică $(a,b) \in R$. Deci am demonstrat şi incluziunea

$$\bigcup_{i\in I} A_i \times B_i \subseteq R. \tag{7}$$

Din (6) şi (7) urmează (5).
d)$\Rightarrow$a). Avem

$$(a,b) \in R \Rightarrow (a,b) \in R \text{ şi } (b,a) \in \overset{-1}{R} \text{ şi } (a,b) \in R \Rightarrow (a,b) \in R \circ \overset{-1}{R} \circ R,$$

ceea ce ne arată că incluziunea $R \subseteq R \circ \overset{-1}{R} \circ R$ are loc pentru orice relaţie. Din $(a,b) \in R \circ \overset{-1}{R} \circ R$ urmează că există $b_1 \in B$ şi $a_1 \in A$ astfel încât aRb_1, $b_1 \overset{-1}{R} a_1$, $a_1 R b$, adică $b_1 \in R\langle a\rangle \cap R\langle a_1\rangle$ şi $b \in R\langle a_1\rangle$, de unde (conform lui (4)) rezultă că $b \in R\langle a_1\rangle = R\langle a\rangle$, adică aRb. Deci am demonstrat şi incluziunea $R \circ \overset{-1}{R} \circ R \subseteq R$. Rezultă că relaţia R este difuncţională.

1.102. Soluţia 1: Dacă R este o echivalenţă atunci R este reflexivă,

$$\overset{-1}{R} = R \text{ şi } R \circ R = R,$$

de unde difuncţionalitatea relaţiei R urmează astfel:

$$R \circ \overset{-1}{R} \circ R = R \circ R \circ R = R \circ R = R.$$

Invers, dacă R este o difuncţională reflexivă atunci

$$R \circ \overset{-1}{R} \circ R = R \text{ şi } \Delta_A \subseteq R.$$

Deci

$$\overset{-1}{R} = \Delta_A \circ \overset{-1}{R} \circ \Delta_A \subseteq R \circ \overset{-1}{R} \circ R = R,$$

adică R este simetrică şi $\overset{-1}{R} = R$. Tranzitivitatea relaţiei R rezultă astfel:

$$R \circ R = R \circ \overset{-1}{R} \circ \Delta_A \subseteq R \circ \overset{-1}{R} \circ R = R.$$

Soluţia 2: O altă soluţie se poate obţine din problemele **1.92** şi **1.101**.

1.103. a) Avem

$$x \in pr_1 R \Rightarrow \exists y \in B, xRy \Rightarrow \exists y \in B, xRy, xRy \text{ şi } y\overset{-1}{R}x \Rightarrow x\overset{-1}{R} \circ Rx,$$

ceea ce ne arată că $\overset{-1}{R} \circ R \subseteq pr_1 R \times pr_2 R$ este reflexivă pentru orice relaţie $R \subseteq A \times B$ (nu numai pentru relaţii difuncţionale). Folosind ipoteza că R este difuncţională, simetria şi tranzitivitatea relaţiei $\overset{-1}{R} \circ R$ rezultă astfel:

$$\overset{-1}{\overline{\overset{-1}{R} \circ R}} = \overset{-1}{R} \circ R;$$

$$\left(\overset{-1}{R} \circ R\right) \circ \left(\overset{-1}{R} \circ R\right) = \overset{-1}{R} \circ \left(R \circ \overset{-1}{R} \circ R\right) = \overset{-1}{R} \circ R.$$

b) Analog cu a).
c) Dacă $x \in pr_1 R$ atunci

$$y \in R\langle x\rangle \Rightarrow \overset{-1}{R}(R\langle x\rangle) = \overset{-1}{R}\langle y\rangle. \tag{1}$$

Într-adevăr, dacă $y \in R\langle x\rangle$ şi $x' \in \overset{-1}{R}(R\langle x\rangle)$, atunci xRy şi există $y' \in R\langle x\rangle$, $x'Ry'$, de unde urmează $x'Ry'$, $y'\overset{-1}{R}x$, xRy, ceea ce implică

$$(x', y) \in R \circ \overset{-1}{R} \circ R = R,$$

adică $x' \in \overset{-1}{R}\langle y\rangle$. Deci $\overset{-1}{R}(R\langle x\rangle) \subseteq \overset{-1}{R}\langle y\rangle$. Invers, dacă $x' \in \overset{-1}{R}\langle y\rangle$ şi $y \in R\langle x\rangle$ atunci $y\overset{-1}{R}x$ şi $y \in R\langle x\rangle$, de unde urmează că $x' \in \overset{-1}{R}(R\langle x\rangle)$. Deci $\overset{-1}{R}\langle y\rangle \subseteq \overset{-1}{R}(R\langle x\rangle)$. Astfel am demonstrat pe (1). Analog se arată că dacă $y \in pr_2 R$ atunci

$$x \in \overset{-1}{R}\langle y\rangle \Rightarrow R\left(\overset{-1}{R}\langle y\rangle\right) = R\langle x\rangle. \tag{2}$$

Din (1) şi (2) rezultă că

$$pr_1 R/\overset{-1}{R} \circ R = \{\overset{-1}{R}\langle y\rangle \mid y \in pr_2 R\} \text{ şi } pr_2 R/R \circ \overset{-1}{R} = \{R\langle x\rangle \mid x \in pr_1 R\}.$$

Acum arătăm că

$$x, x' \in \overset{-1}{R}\langle y\rangle \Rightarrow R\langle x\rangle = R\langle x'\rangle. \tag{3}$$

Într-adevăr, dacă $x, x' \in \overset{-1}{R}\langle y\rangle$ şi $y' \in R\langle x\rangle$ atunci $x'Ry$, $y\overset{-1}{R}x$, xRy', de unde urmează

$$(x', y') \in R \circ \overset{-1}{R} \circ R = R,$$

ceea ce ne arată că $y' \in R\langle x'\rangle$. Deci $R\langle x\rangle \subseteq R\langle x'\rangle$. Analog se arată că $R\langle x'\rangle \subseteq R\langle x\rangle$. Rezultă că $R\langle x\rangle = R\langle x'\rangle$.

Din (3) deducem că formula $\varphi\left(\overset{-1}{R}\langle y\rangle\right) = R\langle x\rangle$, unde $x \in \overset{-1}{R}\langle y\rangle$, defineşte o funcţie

$$\varphi : pr_1 R/\overset{-1}{R} \circ R \to pr_2 R/R \circ \overset{-1}{R}.$$

Propunem cititorului să arate că φ este o bijecţie.

Dacă $R \subseteq A \times B$ este graficul unei funcţii $f : A \to B$ atunci

$$R \circ \overset{-1}{R} = \Delta_{pr_1 R} \text{ şi } \overset{-1}{R} \circ R = \ker f.$$

Deci, în acest caz, φ este bijecţia căutată.

1.104. Indicaţie. Avem

$$\begin{aligned} R \circ \overset{-1}{R} \circ R &= \overset{-1}{F_2} \circ F \circ F_1 \circ \overset{-1}{F_1} \circ \overset{-1}{F} \circ F_2 \circ \overset{-1}{F_2} \circ F \circ F_1 \\ &= \overset{-1}{F_2} \circ F \circ \Delta_{A'/\rho_1} \circ \overset{-1}{F} \circ \Delta_{B'/\rho_2} \circ F \circ F_1 \\ &= \overset{-1}{F_2} \circ F \circ \overset{-1}{F} \circ F \circ F_1 \\ &= \overset{-1}{F_2} \circ \Delta_{B'/\rho_2} \circ F \circ F_1 \\ &= \overset{-1}{F_2} \circ F \circ F_1 = R. \end{aligned}$$

Verificarea egalităţilor $pr_1 R = A'$ şi $pr_2 R = B'$ o lăsăm cititorului.

1.105. Indicaţie. Se procedează la fel ca în rezolvarea problemei **1.79**.

Observaţii: O relaţie (A, A, R) este antisimetrică dacă şi numai dacă $R \cap \overset{-1}{R} \subseteq \Delta_A$. Rezultă că o relaţie binară omogenă pe o mulţime finită A este antisimetrică dacă şi numai dacă, în matricea asociată, orice element egal cu 1 care nu este pe diagonala principală are ca simetric faţă de diagonala principală pe 0. Matricele

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

sunt exemple de matrice asociate unei relaţii antisimetrice, respectiv unei relaţii care nu este antisimetrică (definite pe o mulţime cu 3 elemente).

Propunem şi aici cititorului să ilustreze independenţa axiomelor ce definesc o relaţie de ordine folosind matrice bivalente.

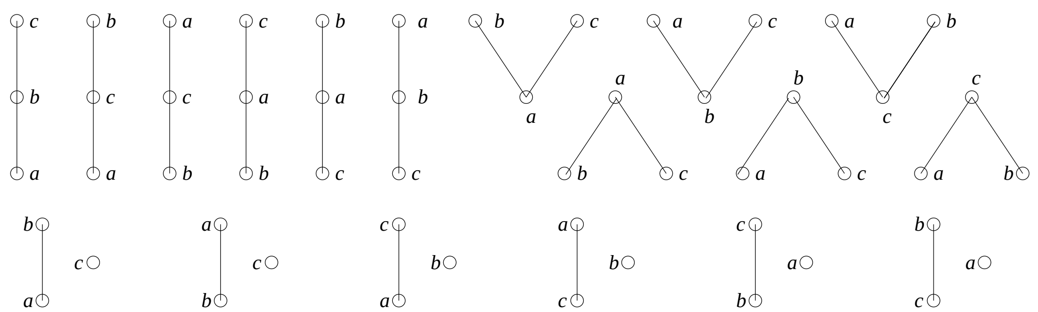
1.106. Dacă R este atât o relaţie de ordine cât şi de echivalenţă pe A atunci $\Delta_A \subseteq R$, iar dacă $a_1 R a_2$ atunci şi $a_2 R a_1$, ceea ce implică $a_1 = a_2$.

1.107. Răspuns. a) $\mathbb{N}$ împreună cu relaţia de divizibilitate (pe $\mathbb{N}$) ; b) $(\mathbb{Z}, \leq)$; c) $(\mathbb{N}, \leq)$; d) $(\mathbb{N}, =)$; e) $(\mathcal{P}(M), \subseteq)$ unde M este o mulţime formată din cel puţin două elemente.

1.108. Indicaţie. Se folosesc definiţiile reflexivităţii, antisimetriei, tranzitivităţii şi a relaţiei de ordine totală.

1.109. Indicaţie. Se aplică [34, Teorema 1.8.16] .

1.110. a) Pe A există o singură relaţie de ordine şi anume Δ_A. Pe B avem următoarele relaţii de ordine: $\rho_1 = \Delta_B$, $\rho_2 = \{(a,a), (b,b), (a,b)\}$ şi $\rho_3 = \overset{-1}{\rho_2}$. Relaţiile de ordine pe C sunt Δ_C şi cele redate în diagramele:



b) Din a) rezultă că numărul mulţimilor ordonate neizomorfe cu un element este 1, cu 2 elemente este 3 şi cu 3 elemente este 5.
Propunem cititorului să răspundă la c) şi d), folosind diagramele de la a).

1.111. Indicaţie. Dacă $a \in A$ atunci corespondenţa care asociază lui a pe

$$f(a) = \{x \in A \mid x \leq a\}$$

realizează un izomorfism $f : A \to \{f(a) \mid a \in A\}$.

1.112. Indicaţie. Rezultă din proprietăţile inversei unei relaţii binare.

1.113. Indicaţie. b) Relaţia $\rho \subseteq \mathbb{R} \times \mathbb{R}$ definită prin

$$x\rho y \Leftrightarrow (x \neq 0 \neq y \text{ şi } x \leq y) \text{ sau } x = 0 = y$$

este o relaţie de ordine. În $(\mathbb{R}, \rho)$ zero este unicul element minimal (maximal), dar nu există cel mai mic (cel mai mare) element.

1.114. Fie ρ_0 o ordonare totală pe A, $\rho \in \mathcal{R}$ şi $\rho_0 \subseteq \rho$. Dacă $x\rho y$ atunci întrucât ρ_0 este o relaţie de ordine totală, urmează că $x\rho_0 y$ sau $y\rho_0 x$. Dacă $y\rho_0 x$ atunci din $\rho_0 \subseteq \rho$ rezultă $y\rho x$, care împreună cu $x\rho y$ ne dă $x = y$. Deci $x\rho y$ implică $x\rho_0 y$, adică $\rho_0 = \rho$. Astfel am arătat că ρ_0 este un element maximal în $(\mathcal{R}, \subseteq)$.

Invers, arătăm că dacă $\rho_0 \in \mathcal{R}$ nu este o ordonare totală atunci ρ_0 nu este un element maximal în $(\mathcal{R}, \subseteq)$. Într-adevăr, dacă ordonarea ρ_0 nu este totală atunci există $x, y \in A$ astfel încât $(x, y) \notin \rho_0$ şi $(y, x) \notin \rho_0$. Relaţia

$$\rho = \rho_0 \cup \{(a, b) \mid a\rho_0 x \text{ şi } y\rho_0 b\}$$

este o ordonare pe A şi $\rho_0 \subseteq \rho$ pentru că $a\rho b$. Deci ρ_0 nu este un element maximal în $(\mathcal{R}, \subseteq)$.

1.115. Indicaţie. Se aplică lema lui Zorn mulţimii $(\mathcal{R}, \subseteq)$ din problema **1.114**.

1.116. Indicaţie. Se foloseşte echivalenţa dintre condiţia minimalităţii (maximalităţii) şi condiţia lanţurilor descrescătoare (crescătoare).
Altfel: Se aplică o inducţie în raport cu numărul elementelor mulţimii.

1.117. Indicaţie. Se arată prin inducţie în raport cu numărul de elemente ale mulţimii că orice şir strict descrescător este finit.

1.118. Din faptul că $(A, \leq)$ este total ordonată şi din condiţia minimalităţii urmează că $(A, \leq)$ este bine ordonată. Rezultă că putem forma cu elementele lui A un şir crescător

$$a_0 < a_1 < a_2 < \ldots .$$

Cum condiţia maximalităţii este echivalentă cu cerinţa ca orice şir crescător din A să fie finit, deducem că acest şir este finit. Deci A este finită.

1.119. Indicaţie. Dacă ar exista un $a \in A$ astfel încât $a > f(a)$ atunci

$$a > f(a) > f(f(a)) > \ldots .$$

1.120. Indicaţie. Fie A şi B două mulţimi bine ordonate. Dacă ar exista două izomorfisme diferite $f, g : A \to B$ atunci ar exista un $a \in A$ astfel încât $f(a) < g(a)$ sau $g(a) < f(a)$ de unde ar urma $g^{-1}(f(a)) < a$ sau $f^{-1}(g(a)) < a$. În continuare se aplică problema anterioară.

1.121. Indicaţie. O mulţime total ordonată este bine ordonată dacă şi numai dacă verifică condiţia lanţurilor descrescătoare.

1.122. Indicaţii. Dacă $(A = \{a_1, \ldots, a_n\}, \rho_1)$ şi $(B = \{b_1, \ldots, b_n\}, \rho_2)$ sunt cele două lanţuri finite atunci putem scrie, fără a restrânge generalitatea,

$$a_1\rho_1 a_2 \rho_1 \ldots \rho_1 a_n \text{ şi } b_1 \rho_2 b_2 \rho_2 \ldots \rho_2 b_n,$$

iar izomorfismul dorit este dat de corespondenţa $a_i \mapsto b_i$ $(i = \{1, \ldots, n\})$.

O altă soluţie poate fi obţinută prin inducţie în raport cu numărul (comun) de elemente ale mulţimilor A şi B.

1.123. Indicaţie. a) Faptul că ρ_1 şi ρ_2 sunt ordonări totale nu implică, în general, că ρ este o ordonare totală. c) $u(a) = (u_1(a), u_2(a))$.

1.124. Indicaţie. $A^I = \prod_{i \in I} A_i$, unde $A_i = A$ pentru orice $i \in I$.

1.125. Indicaţie. Se folosesc definiţiile compusei şi a funcţiei (des)crescătoare.

1.126. Dacă ρ_1, ρ_2 sunt relaţii de ordine pe A şi ρ_1 este strict inclusă în ρ_2 atunci funcţia 1_A din (A, ρ_1) în (A, ρ_2) este bijectivă şi crescătoare, dar $1_A^{-1} = 1_A$ din (A, ρ_2) în (A, ρ_1) nu este crescătoare.

Fie acum $f : A \to B$ o bijecţie crescătoare de la mulţimea total ordonată $(A, \leq)$ la mulţimea ordonată $(B, \leq)$ — am notat la fel relaţiile de ordine din cele două mulţimi deoarece nu există pericol de confuzie. Să arătăm că şi f^{-1} este crescătoare. Fie $b_1, b_2 \in B$ cu $b_1 \leq b_2$. Cum f e bijectivă, există $a_1, a_2 \in A$, unic determinate, astfel încât $f(a_1) = b_1$, $f(a_2) = b_2$ şi astfel avem $a_1 = f^{-1}(b_1)$ şi $a_2 = f^{-1}(b_2)$. Cum $(A, \leq)$ este total ordonată, avem $a_1 \geq a_2$ sau $a_1 \leq a_2$. Dacă $a_1 \geq a_2$ atunci, cum f este crescătoare, avem $b_1 = f(a_1) \geq f(a_2) = b_2 (\geq b_1)$. Deducem $b_1 = b_2$ şi, în consecinţă, $a_1 = a_2$. Reflexivitatea relaţiei $\leq$ din A ne permite să scriem $f^{-1}(b_1) \leq f^{-1}(b_2)$. Dacă $a_1 \leq a_2$ atunci concluzia $f^{-1}(b_1) \leq f^{-1}(b_2)$ survine imediat.

1.127. Indicaţie. Dacă $(A, \leq)$ este bine ordonată şi $a \in A$ nu este cel mai mare element al lui A atunci cel mai mic element din $\{x \in A \mid x > a\}$ este succesorul imediat al lui a. Mulţimea

$$\{1\} \cup \left\{1 - \frac{1}{n} \mid n = 1, 2 \ldots \right\}$$

este bine ordonată de relaţia $\leq$ şi zero este cel mai mic element. În această mulţime 1 nu are predecesor imediat.

1.128. Indicaţie. Avem

$$\inf{}_B X \in \{a \in A \mid \forall x \in X,\ a \leq x\} \text{ şi } \sup{}_B X \in \{a \in A \mid \forall x \in X,\ a \geq x\}.$$

1.129. Indicaţie. Se foloseşte problema **1.110**.

1.130. Indicaţie. a) Se face inducţie după numărul de elemente ale lui X. b) Se foloseşte punctul a) şi $\inf\emptyset = \sup L$, $\sup\emptyset = \inf L$.

1.131. Indicaţie. Nu există $\inf_{\mathbb{N}}\emptyset$.

1.132. Indicaţie. Se foloseşte faptul că $a \le b \Leftrightarrow a \vee b = b \Leftrightarrow a \wedge b = a$.

1.133. Răspuns. a) $(\mathbb{N}, \le)$, b) $(\{n \in \mathbb{Z} \mid n \le 0\}, \le)$, c) $(\mathbb{Z}, \le)$, d) $(\{0,1\}, \le)$.

1.134. Indicaţie. Dacă $X \subseteq \mathbb{N}$ atunci $\sup X$ este cel mai mic multiplu comun al numerelor din X dacă X este finită şi este 0 dacă X este infinită, iar $\inf X$ este cel mai mare divizor comun al numerelor din X.

1.135. Indicaţie. $\inf\emptyset = 1 \in L'$ şi $\sup\emptyset = 0 \in L'$.

1.136. Indicaţie. Se folosesc definiţia sublaticii, problema anterioară şi faptul că $\inf_{\mathcal{P}(A)}\emptyset = A$.

1.137. Pentru orice $f, g \in \mathbb{R}^{\mathbb{R}}$ avem $\sup(f,g) = \alpha$ şi $\inf(f,g) = \beta$, unde $\alpha, \beta \in \mathbb{R}^{\mathbb{R}}$ sunt funcţiile definite prin $\alpha(x) = \max(f(x), g(x))$ şi $\beta(x) = \min(f(x), g(x))$. Fie $f, g \in D(\mathbb{R}, \mathbb{R})$. Se arată uşor că pentru orice $x \in \mathbb{R}$ avem

$$f(x) \le f^2(x) + g^2(x) + 1 \text{ şi } g(x) \le f^2(x) + g^2(x) + 1.$$

Prin urmare $f^2 + g^2 + 1 \in D(\mathbb{R}, \mathbb{R})$ este o majorantă comună pentru f şi g însă luând, de exemplu, $f, g : \mathbb{R} \to \mathbb{R}$, $f(x) = x$, $g(x) = -x$ avem $f, g \in D(\mathbb{R}, \mathbb{R})$ şi $\alpha = \sup(f,g) \notin D(\mathbb{R}, \mathbb{R})$ deoarece $\alpha(x) = |x|$ şi α nu este derivabilă în $x = 0$. Deci $D(\mathbb{R}, \mathbb{R})$ nu este sublatice în $(\mathbb{R}^{\mathbb{R}}, \le)$.

Pentru a arăta că $D(\mathbb{R}, \mathbb{R})$ nu este latice considerăm funcţiile $f, g \in \mathbb{R}^{\mathbb{R}}$, $f(x) = x$, $g(x) = -x$ şi presupunem că ar exista $h = \sup_{D(\mathbb{R},\mathbb{R})}(f,g)$. Atunci, pentru orice $x \in \mathbb{R}$, avem $x \le h(x)$ şi $-x \le h(x)$. Dacă

$$h_n : \mathbb{R} \to \mathbb{R},\ h_n(x) = \begin{cases} -x & , \text{ dacă } x \in \left(-\infty, -\dfrac{1}{n}\right) \\ \dfrac{2}{n} - \sqrt{\dfrac{2}{n^2} - x^2} & , \text{ dacă } x \in \left[-\dfrac{1}{n}, \dfrac{1}{n}\right] \\ x & , \text{ dacă } x \in \left(\dfrac{1}{n}, \infty\right) \end{cases} \quad , \ n \in \mathbb{N}^*,$$

atunci $f(x) \le h_n(x)$ şi $g(x) \le h_n(x)$ pentru orice $n \in \mathbb{N}^*$ şi orice $x \in \mathbb{R}$ şi deducem că $h(x) \le h_n(x)$ pentru orice $n \in \mathbb{N}^*$ şi orice $x \in \mathbb{R}$. Rezultă că

$$-x \le h(x) \le -x,\ \forall x \in \left(-\infty, -\frac{1}{n}\right) \text{ şi } x \le h(x) \le x,\ \forall x \in \left(\frac{1}{n}, \infty\right)$$

şi, în consecinţă, pentru orice $n \in \mathbb{N}^*$, avem

$$h(x) = -x,\ \forall x \in \left(-\infty, -\frac{1}{n}\right) \text{ şi } h(x) = x,\ \forall x \in \left(\frac{1}{n}, \infty\right).$$

Urmează că

$$h(x) = -x,\ \forall x \in (-\infty, 0) \text{ şi } h(x) = x,\ \forall x \in (0, \infty),$$

de unde continuitatea lui h ne conduce la faptul că $h(x) = |x|$, ceea ce contrazice derivabilitatea (în origine, a) lui h.

1.138. Indicaţie. Dacă $(A_i,\rho_i)_{i\in I}$ este o familie de mulţimi ordonate atunci

$$(a_i)_{i\in I}\rho(b_i)_{i\in I} \;\Leftrightarrow\; a_i\rho_i b_i,\ \forall i\in I$$

defineşte o relaţie de ordine ρ pe $\prod\limits_{i\in I} A_i$.

Dacă mulţimile ordonate $(A_i,\rho_i)_{i\in I}$ sunt latici şi $(a_i)_{i\in I},(b_i)_{i\in I}\in\prod\limits_{i\in I} A_i$ atunci

$$(a_i)_{i\in I}\wedge(b_i)_{i\in I}=(a_i\wedge b_i)_{i\in I},\ (a_i)_{i\in I}\vee(b_i)_{i\in I}=(a_i\vee b_i)_{i\in I},$$

iar dacă laticile A_i sunt complete şi $(a_i^j)_{i\in I},\ j\in J$ atunci

$$\bigwedge_{j\in J}(a_i^j)_{i\in I}=\left(\bigwedge_{j\in J}a_i^j\right)_{i\in I},\ \ \bigvee_{j\in J}(a_i^j)_{i\in I}=\left(\bigvee_{j\in J}a_i^j\right)_{i\in I}.$$

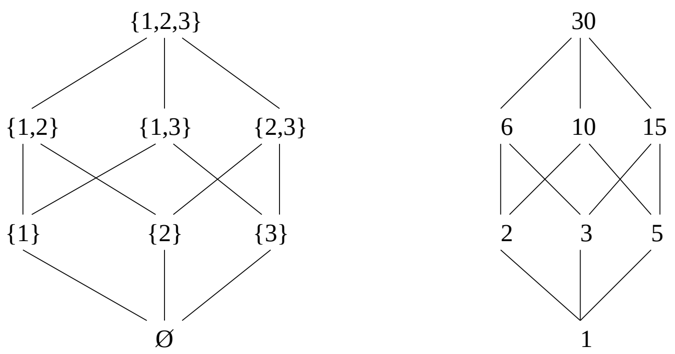
1.139. Răspuns. Dacă A şi B sunt două mulţimi şi $R\subseteq A\times B$ atunci funcţia

$$\mathcal{P}(A)\to\mathcal{P}(B),\ X\mapsto R(X)$$

este crescătoare (în raport cu $\subseteq$) dar nu este, în general, un omomorfism de latici.

1.140. Indicaţie. b) Vezi problema **1.49**.

1.141. a) Diagramele mulţimilor ordonate $(\mathcal{P}(A),\subseteq)$ şi $(B,|)$ sunt:



Funcţia $f:\mathcal{P}(A)\to B$ definită prin $f(\emptyset)=1,\ f(\{1\})=2,\ f(\{2\})=3,\ f(\{3\})=5,$ $f(\{1,2\})=6,\ f(\{1,3\})=10,\ f(\{2,3\})=15,\ f(\{1,2,3\})=30$ este un izomorfism de ordine.

b) Orice izomorfism de ordine $g:\mathcal{P}(A)\to B$ conservă nivelele diagramelor, adică, pe lânga egalităţile $g(\emptyset)=1,\ g(\{1,2,3\})=30$ avem

(1) $\quad g(\{\{1\},\{2\},\{3\}\})=\{2,3,5\},\ g(\{\{1,2\},\{1,3\},\{2,3\}\})=\{6,10,15\}.$

Mulţimile ordonate $(\mathcal{P}(A),\subseteq)$ şi $(B,|)$ sunt latici, iar

$$\{1,2\}=\{1\}\cup\{2\},\ \{1,3\}=\{1\}\cup\{3\},\ \{2,3\}=\{2\}\cup\{3\}.$$

De aici, întrucât izomorfismele de ordine între latici coincid cu izomorfismele de latici, urmează că restricţia lui g la mulţimea $\{\{1,2\},\{1,3\},\{2,3\}\}$ este determinată de restricţia lui g la $\{\{1\},\{2\},\{3\}\}$. De aici şi din (1) deducem că izomorfismele lui $(\mathcal{P}(A),\subseteq)$ pe $(B,|)$ sunt determinate de bijecţiile lui $\{\{1\},\{2\},\{3\}\}$ pe $\{2,3,5\}$. Deci există 6 izomorfisme.

1.142. Din $a \wedge c \leq a$ şi $a \leq a \vee b$ rezultă $a \wedge c \leq a \vee b$, iar cum avem şi $a \wedge c \leq c$, urmează că $a \wedge c \leq (a \vee b) \wedge c$. Analog se obţine $b \wedge c \leq (a \vee b) \wedge c$ şi astfel se obţine proprietatea de subdistributivitate. Proprietatea de submodularitate rezultă din proprietatea de subdistributivitate ţinând seama de faptul că $a \leq c$ implică $a \wedge c = a$.

1.143. Din problema **1.142** avem:

$$(1) \qquad a, b, c \in L,\ a \leq c \ \Rightarrow\ a \vee (b \wedge c) \leq (a \vee b) \wedge c.$$

a)⇒b) L modulară şi $a \leq a \vee c$ implică $a \vee [b \wedge (a \vee c)] = (a \wedge b) \vee (a \wedge c)$.
b)⇒a) Din $a \leq c$ avem $a \vee c = c$, ceea ce, înlocuit în

$$a \vee [b \wedge (a \vee c)] = (a \wedge b) \vee (a \wedge c)$$

conduce la $a \vee (b \wedge c) = (a \wedge b) \vee c$.
a)⇒c) Dacă L este modulară şi $a \leq b$ atunci $a \vee (b \wedge c) = (a \vee c) \wedge b$ şi, conform ipotezei de la c), avem

$$a = a \vee (a \wedge c) = a \vee (b \wedge c) = (a \vee c) \wedge b = (b \vee c) \wedge b = b.$$

c)⇒a) Fie $a, b, c \in L$ cu proprietatea că $a \leq c$. Notăm

$$a_1 = a \vee (b \wedge c),\ c_1 = (a \vee b) \wedge c.$$

Din (1) deducem $a_1 \vee b \leq c_1 \vee b$. Evident $a \leq a_1$, de unde obţinem $a \vee b \leq a_1 \vee b$. Cum $a \vee b \geq (a \vee b) \wedge c = c_1$ avem $a_1 \vee b \geq c_1$, de unde rezultă

$$a_1 \vee b = (a_1 \vee b) \vee b \geq c_1 \vee b.$$

Aşadar $a_1 \vee b = c_1 \vee b$. Prin dualitate (folosind $c_1 \leq c$) se arată că $a_1 \wedge b = c_1 \wedge b$. Inegalitatea $a_1 \leq c_1$ şi c) ne conduc la $a_1 = c_1$, adică $a \vee (b \wedge c) = (a \vee b) \wedge c$.
c)⇒d) Pentagonul nu verifică proprietatea de la c).
d)⇒c) Dacă c) nu are loc în laticea L atunci există $a, b, c \in L$ cu

$$a \leq b,\ a \vee c = b \vee c,\ a \wedge c = b \wedge c \text{ şi } a \neq b.$$

Deducem că $\{a, b, c, a \vee c = b \vee c, a \wedge c = b \wedge c\}$ este o sublatice a lui L izomorfă cu pentagonul.

1.144. Indicaţie. Se arată că φ_a şi φ_b sunt funcţii crescătoare pentru care

$$\varphi_a \circ \varphi_b = 1_{[a \wedge b, a]} \text{ şi } \varphi_b \circ \varphi_a = 1_{[b, a \vee b]}.$$

1.145. Din problema **1.142** avem:

$$(1) \qquad (a \vee b) \wedge c \geq (a \wedge c) \vee (b \wedge c),\ \forall a, b, c \in L.$$

a)⇒ b) $(a \vee c) \wedge (b \vee c) = [a \wedge (b \vee c)] \vee [c \wedge (b \vee c)] = [a \wedge (b \vee c)] \vee c = [(a \wedge b) \vee (a \wedge c)] \vee c = (a \wedge b) \vee [(a \wedge c) \vee c] = (a \wedge b) \vee c$.
b)⇒ a) Se demonstrează analog.

a)$\Rightarrow$ c) $a = a \wedge (a \vee c) = a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) = (a \wedge b) \vee (b \wedge c) = b \wedge (a \vee c) = b \wedge (b \vee c) = b$.
c)$\Rightarrow$ a) Din c) rezultă că laticea L este modulară. Fie $a, b, c \in L$. Notăm

$$u = (a \wedge b) \vee [(a \vee b) \wedge c] \text{ şi } v = (b \wedge c) \vee [(b \vee c) \wedge a].$$

Conform modularităţii laticii L avem

$$a \wedge b \leq a \vee b \Rightarrow u = (a \wedge b) \vee [(a \vee b) \wedge c] = (a \vee b) \wedge [(a \wedge b) \vee c],$$
$$b \wedge c \leq b \vee c \Rightarrow v = (b \wedge c) \vee [(b \vee c) \wedge a] = (b \vee c) \wedge [(b \wedge c) \vee a].$$

Dar

$$u \wedge b = (a \vee b) \wedge [(a \wedge b) \vee c] \wedge b = b \wedge [(a \wedge b) \vee c] = (a \wedge b) \vee (b \wedge c),$$
$$v \wedge b = (b \vee c) \wedge [(b \wedge c) \vee a] \wedge b = b \wedge [(b \wedge c) \vee a] = (b \wedge c) \vee (a \wedge b)$$

şi

$$u \vee b = (a \wedge b) \vee [(a \vee b) \wedge c] \vee b = b \vee [(a \vee b) \wedge c] = (a \vee b) \wedge (b \vee c),$$
$$v \vee b = (b \wedge c) \vee [(b \vee c) \wedge a] \vee b = b \vee [(b \vee c) \wedge a] = (a \vee b) \wedge (b \vee c).$$

În concluzie, $u \wedge b = v \wedge b$ şi $u \vee b = v \vee b$. Rezultă că $u = v$ şi astfel,

$$u \vee c = v \vee c.$$

Dar

$$u \vee c = (a \vee b) \wedge [(a \wedge b) \vee c] \vee c = (a \vee b) \wedge c,$$
$$v \vee c = (b \vee c) \wedge [(b \wedge c) \vee a] \vee c = c \wedge [(b \wedge c) \vee a] = (b \wedge c) \vee (a \wedge c),$$

deci $(a \vee b) \wedge c = (b \wedge c) \vee (a \wedge c)$.
c)$\Rightarrow$ d) Din c) rezultă că că L este modulară, iar pentru diamant avem $a \neq b$ chiar dacă $a \vee c = b \vee c$, $a \wedge c = b \wedge c$.
d)$\Rightarrow$ c) Demonstrăm că dacă L este modulară şi satisface c), atunci L conţine o sublatice izomorfă cu diamantul. Într-adevăr, cum L nu verifică c), există $a, b, c \in L$ astfel încât $a \vee c = b \vee c$, $a \wedge c = b \wedge c$ şi $a \neq b$. Cum L este modulară deducem că a şi b nu sunt comparabile. Dacă am avea $a \leq c$ atunci $c = a \vee c = b \vee c$ implică $b \leq c$, aşadar $a = a \wedge c = b \wedge c = b$, ceea ce este fals. Analog se arată că $c \leq a$ nu convine. Deci submulţimea $\{a, b, c, a \vee c = b \vee c, a \wedge c = b \wedge c\}$ formează o sublatice a lui L izomorfă cu diamantul.

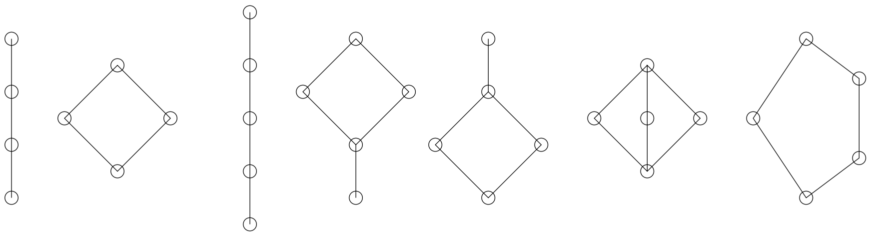
1.146. Indicaţie. Nu conţine sublatici izomorfe cu pentagonul sau diamantul.

1.147. Indicaţie. Se arată, folosind legătura dintre cel mai mic multiplu comun şi cel mai mare divizor comun, că dacă $a, b, c \in \mathbb{N}$ şi $c \neq 0$ atunci

$$a \vee c = b \vee c \text{ şi } a \wedge c = b \wedge c \Rightarrow a = b.$$

1.148. Indicaţii. Pentru latici modulare se foloseşte caracterizarea de la punctul b) al problemei **1.143**, iar pentru latici distributive se foloseşte definiţia.

1.149. Indicaţie. Pentru laticile neizomorfe cu cel mult 3 elemente, vezi problema **1.129**. Laticile neizomorfe cu 4 şi 5 elemente sunt cele din diagramele:



Pentru partea a doua a problemei se folosesc problemele **1.143.** d) şi **1.145.** d).

1.150. Indicaţie. Se foloseşte distributivitatea unei latici Boole şi punctul c) din problema **1.145**.

1.151. Indicaţie. Reuniunea este distributivă faţă de intersecţie, $\emptyset$ este cel mai mic element, M este cel mai mare element şi pentru o submulţime $X \subseteq M$ complementul este $C_M X = M \setminus X$.

1.152. Indicaţie. Cel mai mic element din $(\mathcal{P}/\equiv, \leq)$ este clasa formulelor identic false (contradicţiilor), cel mai mare element este clasa formulelor identic adevărate (tautologiilor), iar complementul clasei unei propoziţii p este clasa negaţiei propoziţiei p.

1.153. a) Presupunem că există $x = \bigvee_{i\in I} a_i$. Rezultă că $a_i \leq x$ pentru orice $i \in I$, de unde urmează $x' \leq a_i'$ pentru orice $i \in I$. Deci x' este o minorantă a familiei a_i', $i \in I$. Dacă $b \in B$ este o altă minorantă a acestei familii (adică $b \leq a_i'$ pentru orice $i \in I$) atunci $b' \geq (a_i')' = a_i$ $(i \in I)$, adică b' este o majorantă a familiei a_i, $i \in I$. Acum, din $x = \bigvee_{i\in I} a_i$ rezultă $x \leq b'$, adică $x' \geq b$. Deci x' este cea mai mare minorantă a familiei a_i', $i \in I$, adică $x' = \bigwedge_{i\in I} a_i'$. Astfel am arătat că egalitatea din enunţul punctului a) are loc.

Se arată prin dualitate că dacă există $y = \bigwedge_{i\in I} a_i'$ atunci $y' = \bigvee_{i\in I} a_i$.

b) Afirmaţia de la b) este duala celei de la a).

1.154. Indicaţii. a) Se ia $\mathcal{D} = \emptyset$. b) Dacă $\mathcal{D} \subseteq \mathcal{C}$ atunci

$$\inf{}_{(\mathcal{C},\subseteq)}\mathcal{D} = \bigcap_{X\in\mathcal{D}} X \text{ şi } \sup{}_{(\mathcal{C},\subseteq)}\mathcal{D} = \bigcap\left\{Y \in \mathcal{C} \mid \bigcup_{X\in\mathcal{D}} X \subseteq Y\right\}.$$

1.155. Răspuns. Nu.

1.156. Indicaţii. a) Se foloseşte iii) din definiţia operatorului de închidere.
b) Din i) rezultă că $J(X) \subseteq J(J(X))$ are loc pentru orice $X \subseteq A$.

1.157. Indicaţie. Pentru funcţia din enunţ, condiţia i) din definiţia operatorului de închidere rezultă din reflexivitate, ii) din proprietăţile relaţiilor binare, iar iii') din tranzitivitatea relaţiei R.

1.158. a) Presupunem că J, J' şi $J' \circ J$ sunt operatori de închidere. Dacă $X \subseteq A$ atunci din proprietatea de extensivitate a lui J rezultă

$$(J' \circ J)(X) \subseteq (J \circ J' \circ J)(X), \tag{1}$$

iar din extensivitatea lui J' şi independenţa lui $J' \circ J$ urmează

$$(J \circ J' \circ J)(X) \subseteq (J' \circ J \circ J' \circ J)(X) = (J' \circ J)(X). \tag{2}$$

Din (1) şi (2) rezultă egalitatea din enunţul lui a).

Invers, presupunem că operatorii de închidere J şi J' verifică egalitatea din enunţul lui a). Din extensivitatea lui J şi J' rezultă că

$$X \subseteq J(X) \subseteq (J' \circ J)(X)$$

pentru orice $X \subseteq A$, adică $J' \circ J$ este extensiv. Din monotonia lui J şi J' obţinem

$$X \subseteq Y \Rightarrow J(X) \subseteq J(Y) \Rightarrow (J' \circ J)(X) \subseteq (J' \circ J)(Y),$$

unde $X, Y \subseteq A$, ceea ce ne arată că $J' \circ J$ este monoton. Din ipoteză şi din idempotenţa lui lui J rezultă că

$$(J' \circ J \circ J' \circ J)(X) = (J' \circ J' \circ J)(X) = (J' \circ J)(X)$$

pentru orice $X \subseteq A$. Prin urmare $J' \circ J$ este idempotent. Deci $J' \circ J$ este un operator de închidere.
b) Este suficient să arătăm că egalitatea de la b) implică egalitatea de la a). Dacă J şi J' comută atunci $J \circ J' \circ J = J' \circ J \circ J = J' \circ J$.

1.159. Indicaţie. a) Dacă $\rho_i \in \mathcal{R}_r$, $i \in I$, atunci $\bigcap\limits_{i \in I} \rho_i \in \mathcal{R}_r$, iar dacă $I \neq \emptyset$ şi $\{\rho_i \mid i \in I\}$ este dirijată superior atunci şi $\bigcup\limits_{i \in I} \rho_i \in \mathcal{R}_r$.
b) Cu notaţiile de la a), pentru $I = \emptyset$ avem $\bigcup\limits_{i \in I} \rho_i = \emptyset \notin \mathcal{R}_r$.
c) $\rho \cup \Delta_A$ este cea mai mică relaţie reflexivă care include pe ρ.

1.160. Indicaţie. b) Se arată, printr-un contraexemplu, că reuniunea a două relaţii tranzitive poate să nu fie tranzitivă. În rest, se procedează ca la problema anterioară.

1.161. Indicaţie. Se procedează ca la problema **1.159** .

1.162. Indicaţie. Dacă $|A| > 1$ atunci $A \times A \notin \mathcal{R}_a$, deci $\mathcal{R}_a$ nu e sistem de închidere.

1.163. Indicaţie. Se procedează ca la problema **1.159** .

1.164. Indicaţie. Se procedează ca la problema **1.159** .

1.165. Indicaţie. a) Se foloseşte definiţia operatorului de închidere. Pentru prima şi ultima funcţie se poate aplica punctul b) şi problema **1.158**.

1.166. Indicaţie. Se folosesc definiţia sistemului de închidere şi caracterizarea sistemului de închidere algebric din remarcile ce preced enunţul problemei **1.159**.

1.167. Indicaţie. b) Dacă $(J_i)_{i\in I}$ este o familie de operatori de închidere pe A şi $J : \mathcal{P}(A) \to \mathcal{P}(A)$ este funcţia definită prin $J(X) = \bigcap\limits_{i\in I} J_i(X)$ atunci J este un operator de închidere şi $\inf(J_i)_{i\in I} = J$.

1.168. Indicaţie. Bijectivitatea lui φ se deduce din remarcile ce preced enunţul problemei **1.159**.

1.169. Fie $x \in A$ şi $y = \varphi(x)$. Avem

$$\begin{aligned} x \le \psi(\varphi(x)) &\Rightarrow \varphi(x) \ge \varphi(\psi(\varphi(x))), \\ y \le \varphi(\psi(y)) &\Leftrightarrow \varphi(x) \le \varphi(\psi(\varphi(x))), \end{aligned}$$

deci $\varphi \circ \psi \circ \varphi = \varphi$. Analog $\psi \circ \varphi \circ \psi = \psi$.

1.170. Indicaţii. La a) şi b) se folosesc definiţia operatorului de închidere, definiţia corespondenţei Galois şi problema anterioară, iar la c) se arată că φ şi ψ dau prin compunere funcţiile identice ale mulţimilor $\mathcal{P}(A)$ şi $\mathcal{P}(B)$.

1.171. Indicaţie. Egalităţile dorite se obţin folosind proprietăţile relaţiilor binare şi definiţia corespondenţei Galois.

1.172. Răspuns. Sistemul de închidere definit de $\varphi \circ \psi$, respectiv $\psi \circ \varphi$ este

$$\{[a, +\infty) \mid a \in \mathbb{R}\} \cup \{\emptyset, \mathbb{R}\}, \text{ respectiv } \{(-\infty, a] \mid a \in \mathbb{R}\} \cup \{\emptyset, \mathbb{R}\}.$$

1.173. Indicaţii. Numărabilitatea mulţimii $\mathbb{N}^*$ rezultă din bijectivitatea funcţiei $\mathbb{N} \to \mathbb{N}^*$, $n \mapsto n + 1$ iar a mulţimii $\mathbb{Z}$ din bijectivitatea funcţiei

$$\varphi : \mathbb{N} \to \mathbb{Z},\ \varphi(n) = \begin{cases} \dfrac{n}{2} & \text{, dacă } n \text{ este par;} \\ -\dfrac{n+1}{2} & \text{, dacă } n \text{ este impar.} \end{cases}$$

Cum pentru orice număr natural n există $m, k \in \mathbb{N}$, unic determinate, cu proprietatea că $n = 2^m(2k + 1)$ deducem că funcţia $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(m, k) \mapsto 2^m(2k + 1)$ este bijectivă, deci mulţimea $\mathbb{N} \times \mathbb{N}$ este numărabilă. Aceasta rezultă şi din faptul ca elementele mulţimii $\mathbb{N} \times \mathbb{N}$ pot fi ,,numărate” aşa cum indică săgeţile din figura de mai jos

$$\begin{tikzcd}
(0,0) \arrow[r] & (0,1) \arrow[dl] & (0,2) \arrow[r] & (0,3) \arrow[dl] & \cdots \\
(1,0) \arrow[d] & (1,1) \arrow[ur] & (1,2) \arrow[dl] & (1,3) & \cdots \\
(2,0) \arrow[ur] & (2,1) \arrow[dl] & (2,2) & (2,3) & \cdots \\
(3,0) & (3,1) & (3,2) & (3,3) & \cdots \\
\vdots & \vdots & \vdots & \vdots &
\end{tikzcd}$$

Similar, se poate stabili o bijecţie între $\mathbb{N}^*$ şi $\mathbb{Q}_+$ aranjând numerele raţionale într-un şir după cum urmează: considerăm fracţiile ireductibile $\dfrac{p}{q}$ cu $p, q \in \mathbb{N}^*$ care sunt reprezentanţi pentru numerele raţionale pozitive şi le grupăm în clase determinate de suma $p+q$. Astfel, o k-clasă este formată din fracţiile ireductibile pentru care suma numărătorului cu numitorul este k. În interiorul unei k-clase aşezarea elementelor se face în ordinea descrescătoare a numitorilor, obţinându-se astfel şirul

$$\frac{1}{k-1}, \frac{2}{k-2}, \ldots, \frac{k-2}{2}, \frac{k-1}{1}$$

(din care, evident, lipsesc fracţiile reductibile). Acum putem realiza succesiunea elementelor din $\mathbb{Q}_+$ punând elementele 1-clasei, apoi ale 2-clasei ş. a. m. d.
Din cele de mai sus se deduce existenţa unei bijecţii $\psi : \mathbb{N}^* \to \mathbb{Q}_+$. Funcţiile

$$f : \mathbb{N} \to \mathbb{Q}_+ \cup \{0\},\ f(n) = \begin{cases} 0 & , \text{ dacă } n = 0; \\ \psi(n) & , \text{ dacă } n \in \mathbb{N}^*, \end{cases}$$
$$g : \mathbb{N}^* \to \mathbb{Q}_-,\ g(n) = -\psi(n),$$

sunt, de asemenea, bijective. Echivalenţa mulţimilor $\mathbb{N}$ şi $\mathbb{Q}$ se obţine arătând că

$$\chi : \mathbb{N} \to \mathbb{Q},\ \chi(n) = \begin{cases} f\left(\dfrac{n}{2}\right) & , \text{ dacă } n \text{ este par;} \\ g\left(\dfrac{n+1}{2}\right) & , \text{ dacă } n \text{ este impar} \end{cases}$$

este o funcţie bijectivă.

Observaţie: Printr-un procedeu analog cu cel din ultima parte a soluţiei acestei probleme se poate arăta că reununea disjunctă a două mulţimi numărabilă este o mulţime numărabilă.

1.174. Reamintim că o *mulţime* X se numeşte *finită* dacă există $n \in \mathbb{N}$ astfel încât $X \sim \{1, 2, \ldots, n\}$, în caz contrar, se numeşte *infinită*. Notăm, de asemenea, că o mulţime X este infinită dacă şi numai dacă există $X' \subseteq X$, $X' \neq X$ pentru care $X' \sim X$ (Dedekind) sau, echivalent, dacă X are o submulţime numărabilă (Cantor).

Aşadar, din X infinită deducem că există $A \subseteq X$ şi există o funcţie bijectivă $f_0 : \mathbb{N}^* \to A$. Funcţia

$$f : \mathbb{N} \to A \cup \{x_0\},\ f(n) = \begin{cases} f_0(n) & , \text{ dacă } n \in \mathbb{N}^*; \\ x_0 & , \text{ dacă } n = 0 \end{cases}$$

este, de asemenea, bijectivă. Concluzia dorită se obţine arătând că

$$\varphi : X \to X \setminus \{x_0\},\ \varphi(x) = \begin{cases} x & , \text{ dacă } x \notin A \cup \{x_0\}; \\ f(n+1) & , \text{ dacă } x = f(n) \end{cases}$$

este o funcţie bijectivă. Evident, φ este bine definită.

Fie $x, x' \in X$ astfel încât $\varphi(x) = \varphi(x')$. Rezultă că fie $x, x' \notin A \cup \{x_0\}$ ceea ce ne conduce imediat la $x = x'$, fie $x, x' \in A \cup \{x_0\}$ ceea ce înseamnă că există $k, l \in \mathbb{N}$ astfel încât $x = f(k)$ şi $x' = f(l)$ şi

$$f(k+1) = \varphi(x) = \varphi(x') = f(l+1).$$

Bijectivitatea funţiei f ne conduce la $k+1 = l+1$. Astfel, avem $k = l$ şi $x = f(k) = f(l) = x'$, ceea ce completează demonstaţia injectivităţii lui φ.

Fie $y \in X \setminus \{x_0\}$ arbitrar. Dacă $y \notin A \cup \{x_0\}$ atunci $y = \varphi(y) \in \varphi(X)$. Dacă $y \in A(\subseteq A \cup \{x_0\})$ atunci există $n \in \mathbb{N}$ astfel încât $y = f(n)$. Dar $y \neq x_0$ implică $n \neq \emptyset$. Rezultă $y = f(n) = f(n-1+1) = \varphi(f(n-1)) \in \varphi(X)$. Deci φ este şi surjectivă.

1.175. Indicaţii. Funcţiile $\varphi : \mathbb{R} \to (-1,1)$, $\varphi(x) = \dfrac{x}{x+1}$ şi $\psi : [0,1] \to [a,b]$, $\psi(x) = (b-a)x + a$ sunt bijective. Problema anterioară şi faptul că $\sim$ este tranzitivă completează soluţia.

1.176. Indicaţii. Se folosesc proprietăţile de universalitate ale reuniunii disjuncte şi produsului cartezian, mai exact, unicitatea pâna la o bijecţie a acestora.

1.177. Indicaţie. Se foloseşte problema **1.74**.

1.178. Vom începe prin a demonstra că pentru orice $n \in \mathbb{N}^*$ există şi sunt unic determinate numerele naturale k, j cu proprietatea că $1 \leq j \leq k+1$ şi $n = \dfrac{k(k+1)}{2} + j$. Demonstrăm prin inducţie după n existenţa numerelor k, j. Dacă $n = 1$ atunci $k = 0$ şi $j = 1$, iar dacă $n = 2$ atunci $k = j = 1$. Presupunem afirmaţia adevărată pentru n. Avem $n+1 = \dfrac{k(k+1)}{2} + j + 1$. Dacă $j < k+1$ atunci $j+1 \leq k+1$ şi $n+1 = \dfrac{k'(k'+1)}{2} + j'$, unde $k' = k$ şi $j' = j+1$. Dacă $j = k+1$ atunci

$$n+1 = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2} + 1 = \frac{k'(k'+1)}{2} + j',$$

unde $k' = k+1$ şi $j' = 1$. Dacă $n = \dfrac{k(k+1)}{2} + j = \dfrac{k'(k'+1)}{2} + j'$ cu $j, j', k, k' \in \mathbb{N}$, $1 \leq j \leq k+1$ şi $1 \leq j' \leq k'+1$ atunci $2(j'-j) = (k-k')(k+k'+1)$. Dacă $k' < k$ atunci $(k-k')(k+k'+1) > k+k'+1 \geq 2(k'+1) > 2(j'-j)$, contradicţie. Similar $k < k'$ ne conduce la o contradicţie. Deci $k = k'$ şi $j = j'$, ceea ce demonstrează unicitatea numerelor j, k. Pentru un număr natural nenul n notăm k şi j de mai sus cu $\alpha(n)$, respectiv cu $\beta(n)$.

Revenind la problema noastră, putem considera că mulţimile X_i sunt disjuncte. Mulţimile X_i fiind numărabile, rezultă că pentru orice $i \in I$ există $f_i : \mathbb{N}^* \to X_i$ bijecţie. Fie $f : \mathbb{N}^* \to \bigcup\limits_{i\in I} X_i$, $f(n) = f_{\alpha(n)-\beta(n)+2}(\beta(n))$.

Dacă $n, n' \in \mathbb{N}^*$ şi $f(n) = f(n')$ atunci (în $X_{\alpha(n)-\beta(n)+2} \cap X_{\alpha(n')-\beta(n')+2}$) avem $f_{\alpha(n)-\beta(n)+2}(\beta(n)) = f_{\alpha(n')-\beta(n')+2}(\beta(n'))$. Mulţimile X_i fiind disjuncte, aceasta are loc doar dacă $\alpha(n) - \beta(n) + 2 = \alpha(n') - \beta(n') + 2$, iar cum $f_{\alpha(n)-\beta(n)+2}$ este bijectivă avem $\beta(n) = \beta(n')$ şi, implicit, $\alpha(n) = \alpha(n')$. Rezultă $n = n'$, aşadar funcţia f este injectivă.

Funcţia f este surjectivă deoarece pentru orice $x \in \bigcup\limits_{i\in I} X_i$ există $n \in \mathbb{N}^*$ astfel încât $f(n) = x$. Într-adevăr, dacă $x \in \bigcup\limits_{i\in I} X_i$ atunci există un unic $i \in I$ pentru care $x \in X_i$. Cum f_i este surjectivă, deducem că există $m \in \mathbb{N}^*$ astfel încât $x = f_i(m)$. Căutăm pe n astfel încât $m = \beta(n)$ şi $i = \alpha(n) - \beta(n) + 2$ şi obţinem $n = \dfrac{(i+m-2)(i+m-1)}{2} + m (\in \mathbb{N}^*)$.

Deci f este o bijecţie şi $\bigcup\limits_{i\in I} X_i$ este numărabilă.

1.179. a) Fie X, Y astfel încât $|X| \leq |Y|$ şi fie $f : X \to Y$ o injecţie. Dacă pentru X', Y' avem $X \sim X'$, $Y \sim Y'$ şi $\varphi : X \to X'$, $\psi : Y \to Y'$ sunt două bijecţii atunci $\psi \circ f \circ \varphi^{-1}$ este o injecţie şi astfel avem $|X'| \leq |Y'|$.

b) Fie X_1, X_2, Y_1, Y_2 mulţimi de cardinale, respectiv, $\mathfrak{m}_1, \mathfrak{m}_2, \mathfrak{n}_1, \mathfrak{n}_2$ astfel încât $X_1 \cap X_2 = \emptyset = Y_1 \cap Y_2$. Din $\mathfrak{m}_1 \leq \mathfrak{n}_1$ şi $\mathfrak{m}_2 \leq \mathfrak{n}_2$ rezultă că există două injecţii $f_1 : X_1 \to Y_1$, $f_2 : X_2 \to Y_2$. Este imediat faptul că

$$f : X_1 \cup X_2 \to Y_1 \cup Y_2,\ f(x) = \begin{cases} f_1(x) & \text{, dacă } x \in X_1; \\ f_2(x) & \text{, dacă } x \in X_2 \end{cases}$$

este o funcţie injectivă. Deci $|X_1 \cup X_2| \leq |Y_1 \cup Y_2|$ şi $\mathfrak{m}_1 + \mathfrak{m}_2 \leq \mathfrak{n}_1 + \mathfrak{n}_2$.

Observaţii: i) ,,Relaţia" $\leq$ este reflexivă, antisimetrică şi tranzitivă.
ii) $|X| \leq |Y|$ dacă şi numai dacă există $Z \subseteq Y$ astfel încât $X \sim Z$.
iii) Proprietăţi similare cu cea pe care am demonstrat-o la b) au loc şi pentru înmulţire şi ridicare la putere. Astfel, dacă pentru cardinalele $\mathfrak{m}_1, \mathfrak{m}_2, \mathfrak{n}_1, \mathfrak{n}_2$ avem $\mathfrak{m}_1 \leq \mathfrak{n}_1$ şi $\mathfrak{m}_2 \leq \mathfrak{n}_2$ atunci $\mathfrak{m}_1 \cdot \mathfrak{m}_2 \leq \mathfrak{n}_1 \cdot \mathfrak{n}_2$ şi $\mathfrak{m}_1^{\mathfrak{m}_2} \leq \mathfrak{n}_1^{\mathfrak{n}_2}$.

1.180. a) Fie X şi Y două mulţimi cu $|X| = \mathfrak{m}$ şi $|Y| = \mathfrak{n}$. Din $\mathfrak{m} < \mathfrak{n}$ rezultă că există $Y' \subseteq Y$ astfel încât $X \sim Y'$. Fie $Y'' = Y \setminus Y'$ şi $\mathfrak{p} = |Y''|$. Din $|Y'| = \mathfrak{m} < \mathfrak{n}$ deducem $Y' \subseteq Y$ şi $Y' \neq Y$. Astfel, $Y'' \neq \emptyset$ şi $\mathfrak{p} > 0$. Cum $Y = Y' \cup Y''$ şi $Y' \cap Y'' = \emptyset$, avem $|Y| = |Y'| + |Y''|$, deci $\mathfrak{n} = \mathfrak{m} + \mathfrak{p}$.
b) Pentru $\mathfrak{m} \neq \mathfrak{n}$, necesitatea condiţiei din enunţ urmează din a), iar pentru $\mathfrak{m} = \mathfrak{n}$, urmează considerând $\mathfrak{p} = 0$. Pe de altă parte, orice cardinal $\mathfrak{p}$ are proprietatea $\mathfrak{p} \geq 0$, de unde conform problemei **1.179.** b) avem $\mathfrak{m} + \mathfrak{p} \geq \mathfrak{m} + 0 = \mathfrak{m}$, deci, dacă $\mathfrak{n} = \mathfrak{m} + \mathfrak{p}$ atunci $\mathfrak{m} \leq \mathfrak{n}$.

Observaţie: i) Să remarcăm că proprietăţile pe care le întâlnim la cardinalele finite sunt chiar cele pe care le cunoaştem din $\mathbb{N}$.
ii) Reciproca afirmaţiei de la a) din problema de mai sus nu este valabilă. Ca exemplu, să luăm egalitatea $\aleph_0 = \aleph_0 + 1$ care derivă din $\mathbb{N} \sim \mathbb{N}^*$.

1.181. Din $\mathfrak{m} > 1$, $\mathfrak{n} > 1$ deducem că există cardinalele $\mathfrak{m}' > 0$ şi $\mathfrak{n}' > 0$ astfel încât $\mathfrak{m} = \mathfrak{m}' + 1$, $\mathfrak{n} = \mathfrak{n}' + 1$. Avem $\mathfrak{m}\mathfrak{n} = (\mathfrak{m}' + 1)(\mathfrak{n}' + 1) = \mathfrak{m}'\mathfrak{n}' + \mathfrak{m}' + \mathfrak{n}' + 1$. Din $\mathfrak{m}' > 0$ şi $\mathfrak{n}' > 0$ deducem $\mathfrak{m}'\mathfrak{n}' \geq 1$, deci $\mathfrak{m}\mathfrak{n} \geq 1 + \mathfrak{m}' + \mathfrak{n}' + 1 = \mathfrak{m} + \mathfrak{n}$.

1.182. 1) se obţine din observaţia ce succede soluţia problemei **1.173**.
2) rezultă din problema **1.178**.
3) $\mathfrak{c}^2 = \mathfrak{c} \cdot \mathfrak{c} = 2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0} = \mathfrak{c}$.
4) $\mathfrak{c}^{\aleph_0} = \left(2^{\aleph_0}\right)^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} = \mathfrak{c}$.
5) Din $2 < \mathfrak{c}$ avem, conform problemei **1.181**, $\mathfrak{c} + \mathfrak{c} \leq \mathfrak{c}^2 = \mathfrak{c}$, iar cum $\mathfrak{c} \leq \mathfrak{c} + \mathfrak{c}$ obţinem $\mathfrak{c} + \mathfrak{c} = \mathfrak{c}$.
6) Din $2 < \aleph_0 \leq \mathfrak{c}$ avem, conform observaţiei iii) de după soluţia problemei **1.179**,

$$\mathfrak{c} = 2^{\aleph_0} \leq \aleph_0^{\aleph_0} \leq \mathfrak{c}^{\aleph_0} = \mathfrak{c},$$

deci $\aleph_0^{\aleph_0} = \mathfrak{c}$.
7) Observaţia menţionată mai sus (la 6)) ne conduce de la $2 < \aleph_0 \leq \mathfrak{c}$ la

$$\mathfrak{c} = 2 \cdot \mathfrak{c} \leq \aleph_0 \cdot \mathfrak{c} \leq \mathfrak{c}^2 = \mathfrak{c},$$

aşadar $\aleph_0 \cdot \mathfrak{c} = \mathfrak{c}$.

Observaţii: a) Dacă X este o mulţime atunci corespondenţa $f \mapsto \overset{-1}{f}\langle 1\rangle$ realizează o bijecţie între mulţimea $\{0,1\}^X$ a funcţiilor de la X la $\{0,1\}$ şi mulţimea $\mathcal{P}(X)$ a submulţimilor mulţimii X.
b) $\aleph_0 < \mathfrak{c}$ deoarece $\mathfrak{c} = 2^{\aleph_0} = |\mathcal{P}(\mathbb{N})| \geq |\mathbb{N}|$ şi, conform teoremei lui Cantor — dacă X este o mulţime atunci $X \nsim \mathcal{P}(X)$ — avem $|\mathcal{P}(\mathbb{N})| \neq |\mathbb{N}|$.

1.183. Indicaţie. Funcţiile $\varphi : \mathbb{R} \to \mathcal{P}(\mathbb{Q}),\ \varphi(x) = \{a \in \mathbb{Q} \mid a \leq x\}$ şi

$$\psi : \{0,1\}^{\mathbb{N}} \to [0,1),\ \psi((a_i)_{i\in\mathbb{N}}) = 0, a_0a_1a_2\ldots a_i\ldots$$

sunt injective şi astfel avem

$$|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})| = 2^{\aleph_0} = \mathfrak{c} \text{ şi } \mathfrak{c} = 2^{\aleph_0} = \left|\{0,1\}^{\mathbb{N}}\right| \leq |[0,1)| = |\mathbb{R}|,$$

deci $|\mathbb{R}| = \mathfrak{c}$.

Observaţie: Mulţimea $\mathbb{R}$ nu este numărabilă deoarece $\mathbb{R} \sim \mathcal{P}(\mathbb{N})$ (având acelaşi cardinal) şi $\mathcal{P}(\mathbb{N}) \nsim \mathbb{N}$.

1.184. a) Fie X o mulţime cu $|X| = \mathfrak{m}$ şi fie

$$R = \{(A,f) \mid A \subseteq X,\ A \text{ infinită},\ f : A \to A \times A \text{ bijecţie}\}.$$

Cum X este infinită, rezultă că există $B \subseteq X$ astfel încât $B \sim \mathbb{N}$. Din faptul că $B \times B \sim \mathbb{N} \times \mathbb{N} \sim \mathbb{N}$ obţinem existenţa unei bijecţii $g : B \to B \times B$ şi deducem că $R \neq \emptyset$ deoarece $(B,g) \in R$.

Relaţia $\leq$ definită prin

$$(A,f) \leq (A',f') \ \Leftrightarrow\ A \subseteq A' \text{ şi } f'|_A = f$$

este o relaţie de ordine pe R. Fie $L \subseteq R$ un lanţ, $A_0 = \bigcup\limits_{(A,f)\in L} A$ şi funcţia

$$f_0 : A_0 \to A_0 \times A_0$$

definită prin $f_0(x) = f(x)$ dacă $x \in A$ şi $(A,f) \in R$. Atunci $(A_0, f_0) \in R$ şi $(R, \leq)$ verifică ipoteza lemei lui Zorn. Rezultă că în $(R, \leq)$ există un element maximal (E,f). Dacă notăm $|E| = \mathfrak{a}$ atunci $\mathfrak{a}$ este un cardinal transfinit şi $\mathfrak{a}^2 = \mathfrak{a}$.

Dacă $\mathfrak{a} < \mathfrak{m}$ atunci $\mathfrak{a} \leq \mathfrak{a} + \mathfrak{a} \leq \mathfrak{a}^2 = \mathfrak{a}$ de unde deducem că $2\mathfrak{a} = \mathfrak{a} + \mathfrak{a} = \mathfrak{a}$ şi $3\mathfrak{a} = 2\mathfrak{a} + \mathfrak{a} = \mathfrak{a} + \mathfrak{a} = \mathfrak{a}$. Dacă $|X \setminus E| \leq \mathfrak{a}$ atunci $X = (X \setminus E) \cup E$ ne conduce la $\mathfrak{m} = |X \setminus E| + \mathfrak{a} \leq \mathfrak{a} + \mathfrak{a} = \mathfrak{a}$, ceea ce contrazice faptul că $\mathfrak{a} < \mathfrak{m}$. Aşadar, $|X \setminus E| > \mathfrak{a}$ de unde rezultă că există $F \subseteq X \setminus E$ astfel încât $|F| = \mathfrak{a}$. Pentru $M = E \cup F$ avem

$$M \times M = (E \cup F) \times (E \cup F) = (E \times E) \cup (E \times F) \cup (F \times E) \cup (F \times F) = (E \times E) \cup Z,$$

unde $Z = (E \times F) \cup (F \times E) \cup (F \times F)$. Dar

$$|Z| = |E \times F| + |F \times E| + |F \times F| = \mathfrak{a}^2 + \mathfrak{a}^2 + \mathfrak{a}^2 = \mathfrak{a} + \mathfrak{a} + \mathfrak{a} = 3\mathfrak{a} = \mathfrak{a}$$

de unde urmează că $Z \sim F$. Dacă $g : Z \to F$ este o bijecţie atunci şi

$$h : E \cup F \to (E \times E) \cup Z = (E \cup F) \times (E \cup F),\ h(x) = \begin{cases} f(x) & , x \in E; \\ g(x) & , x \in F \end{cases}$$

este o bijecţie. Deducem că $(E \cup F, h) \in R$, iar cum $(E, f) \leq (E \cup F, h)$, se contrazice maximalitatea lui (E, f).

În concluzie $\mathfrak{a} = \mathfrak{m}$, deci $\mathfrak{m}^2 = \mathfrak{m}$.

b) Cum $\mathfrak{m} \leq \mathfrak{m} + \mathfrak{m} \leq \mathfrak{m}^2 = \mathfrak{m}$, rezultă că $\mathfrak{m} + \mathfrak{m} = \mathfrak{m}$.

c) Din $0 \leq \mathfrak{n} \leq \mathfrak{m}$ deducem $\mathfrak{m} = \mathfrak{m} + 0 \leq \mathfrak{m} + \mathfrak{n} = \mathfrak{m}$, deci $\mathfrak{m} + \mathfrak{n} = \mathfrak{m}$, iar din $1 \leq \mathfrak{n} \leq \mathfrak{m}$ deducem $\mathfrak{m} = \mathfrak{m} \cdot 1 \leq \mathfrak{m} \cdot \mathfrak{m} \leq \mathfrak{m} \cdot \mathfrak{m} = \mathfrak{m}^2 = \mathfrak{m}$, de unde rezultă $\mathfrak{m} \cdot \mathfrak{n} = \mathfrak{m}$.

1.185. a) Este o consecinţă imediată a problemei **1.122**.

b) Fie $R = \{(m, n) \in \mathbb{N} \times \mathbb{N} \mid 0 < m \leq n\} \cup \{(m, 0) \mid m \in \mathbb{N}\}$. Evident, $(\mathbb{N}, R)$ este o mulţime bine ordonată, dar $(\mathbb{N}, R)$ şi $(\mathbb{N}, \leq)$ nu sunt izomorfe, deci nu au acelaşi ordinal (0 este cel mai mare element din $(\mathbb{N}, R)$, iar în $(\mathbb{N}, \leq)$ nu există cel mai mare element).

1.186. Indicaţii. a) Se foloseşte definiţia mulţimii bine ordonate.

b) Dacă $f : A \to A'$ şi $g : B \to B'$ sunt izomorfisme de ordine atunci $f \times g$ este un izomorfism de ordine.

1.187. Indicaţii. a) Se foloseşte definiţia mulţimii bine ordonate.

b) Dacă $\varphi_i : A_i \to B_{f(i)}$ $(i \in I)$ sunt izomorfisme de ordine atunci corespondenţa

$$\overset{\circ}{\bigcup_{i \in I}} A_i \to \overset{\circ}{\bigcup_{j \in J}} B_j\,,\ \ (i, a_i) \mapsto (f(i), \varphi_i(a_i))$$

este un izomorfism de ordine.

c) Evident, lanţul numerelor naturale nenule are ordinalul ω (fiind izomorf cu lanţul numerelor naturale), iar din soluţia de la punctul b) al problemei **1.185** deducem că $1 + \omega = \omega \neq \omega + 1$.

Capitolul 2

Grupoizi. Semigrupuri. Grupuri

2.1. Răspuns. Grupoizii $(A, *)$ cu $A = (0, +\infty)$ şi $a * b = a^b$ pentru orice $a, b \in A$ şi $(V, \times)$ cu V mulţimea vectorilor (segmentelor orientate) din spaţiu şi $x \times y$ produsul vectorial al lui x cu y, pentru orice $x, y \in V$ nu sunt semigrupuri. Cei doi grupozi nu au elemente neutre.

2.2. Răspuns. Grupoidul definit de tabla

$*$	a	b
a	a	b
b	a	b

are două elemente neutre la stânga diferite. Răspunsul la cele două întrebări este negativ.

2.3. Răspuns. Un exemplu ar fi grupoidul definit prin

$*$	e	a	b
e	e	a	b
a	a	e	e
b	b	e	a

Într-un semigrup cu element neutru (monoid) orice element are cel mult un simetric.

2.4. Răspuns. În grupoidul din problema anterioară, elementul a este simetrizabil şi $a * a = a * b$. Într-un semigrup cu element neutru se poate simplifica cu orice element simetrizabil.

2.5. Evident, $x * y = y * x$ pentru orice $x, y \in \mathbb{R}$, iar dacă $x, y, z \in \mathbb{R}$ atunci

$$(x * y) * z = (x + y + xy) * z = x + y + xy + z + xz + yz + xyz,$$
$$x * (y * z) = x * (y + z + yz) = x + y + z + yz + xy + xz + xyz.$$

Deci $(\mathbb{R}, *)$ este semigrup comutativ. Dacă $e \in \mathbb{R}$ este element neutru atunci

$$e * x = x,\ \forall x \in \mathbb{R} \Leftrightarrow e + x + ex = x,\ \forall x \in \mathbb{R} \Leftrightarrow e(1 + x) = 0,\ \forall x \in \mathbb{R},$$

de unde deducem că $e = 0$. Arătăm că $e = 0$ este element neutru. Într-adevăr,

$$0 * x = 0 + x + 0x = x,\ \forall x \in \mathbb{R}.$$

Aşadar, $(\mathbb{R}, *)$ este monoid comutativ, iar cum

$$x * y = x + y + xy = -1 + (1 + x)(1 + y),$$

avem

$$x, y \in [-1, +\infty) \Rightarrow x \geq -1, y \geq -1 \Rightarrow (1 + x)(1 + y) \geq 0 \Rightarrow x * y \in [-1, +\infty).$$

2.6. Cum $x * y = 2 - 2 + xy - 2x - 2y + \lambda = 2 + (x - 2)(y - 2) + \lambda - 6$, rezultă că

$$x, y \in (2, +\infty) \Rightarrow x * y \in (2, +\infty)$$

dacă şi numai dacă $\lambda \geq 6$, pentru că $(x - 2)(y - 2) > 0$ şi $(x - 2)(y - 2)$ tinde la 0 când $x \to 2,\ y \to 2\ (x, y \geq 2)$.

2.7. Răspuns. $a = b = 0$ sau $a = \dfrac{1}{2},\ b = 1.$

2.8. i) Pentru orice $x, y, z \in \mathbb{Z}$ avem:

$$\begin{aligned} x * (y * z) &= m^2xyz + mnxz + mnyz + mpz + mnxy + n^2x + n^2y + np + nz + p,\\ (x * y) * z &= m^2xyz + mnxy + mnxz + mpx + mnyz + nx + n^2y + n^2z + np + p. \end{aligned}$$

Aşadar, $*$ este asociativă dacă şi numai dacă

$$mpz + n^2x + nz = mpx + nx + n^2z,\ \forall x, y, z \in \mathbb{Z},$$

adică

$$(z - x)(mp - n^2 + n) = 0,\ \forall x, y, z \in \mathbb{Z},$$

iar aceasta are loc dacă şi numai dacă

$$mp - n^2 + n = 0. \tag{1}$$

Deci (1) este o condiţie necesară şi suficientă pentru ca operaţia $*$ să fie asociativă.
ii) Evident, operaţia $*$ este comutativă. Un număr $e \in \mathbb{Z}$ este element neutru dacă şi numai dacă

$$x * e = x,\ \forall x \in \mathbb{Z} \Leftrightarrow (me + n - 1)x + (ne + p) = 0,\ \forall x \in \mathbb{Z}.$$

Dar un polinom din $\mathbb{Z}[X]$ are o infinitate de rădăcini dacă şi numai dacă este polinomul nul, prin urmare,

$$\begin{cases} me + n - 1 = 0 \\ ne + p = 0 \end{cases}. \tag{2}$$

Astfel, am redus problema la determinarea unor condiţii necesare şi suficiente pentru existenţa unui $e \in \mathbb{Z}$ care verifică condiţiile (2). Deosebim cazurile:
1) Dacă $m = 0$ atunci $n = 1$, $e = -p$ şi $x * y = x + y + p$.
2) Dacă $n = 0$ atunci $p = 0$ şi $me = 1$. Deducem că $e = \dfrac{1}{m}$ care este un număr întreg dacă şi numai dacă $m \in \{-1, 1\}$. În acest caz $x * y = xy$ sau $x * y = -xy$.

3) Dacă $m \neq 0 \neq n$ atunci $e = -\dfrac{p}{n} = \dfrac{1-n}{m} \in \mathbb{Z}$. Aşadar, $n|p$ şi $mp - n^2 + n = 0$.
iii) Din ii) rezultă că existenţa elementului neutru implică (1). Deci $(\mathbb{Z}, *)$ este un monoid comutativ. În cazul 1) acest monoid este grup deoarece pentru orice $x \in \mathbb{Z}$, $x' = -2p - x \in \mathbb{Z}$ este simetricul lui x. În cazul 2) monoidul $(\mathbb{Z}, *)$ nu este grup pentru că numai -1 şi 1 sunt simetrizabile. În cazul 3), dacă $x \in \mathbb{Z}$ şi x' este simetricul lui x atunci

$$x' = \frac{-p - np - n^2 x}{mnx + n^2} = \frac{-p - np - (n + mp)x}{n + mp + mnx} \in \mathbb{Z}.$$

Trecând la limită când $x \to \infty$ rezultă $\dfrac{n + mp}{mn} = \dfrac{1}{m} + \dfrac{p}{n} \in \mathbb{Z}$, care împreună cu $n|p$ implică $\dfrac{1}{m} \in \mathbb{Z}$ adică $m \in \{-1, 1\}$. Prin urmare, pentru $m \notin \{-1, 1\}$, monoidul $(\mathbb{Z}, *)$ nu este grup.

• Dacă $m = 1$ atunci $e = 1 - n$, $p = n^2 - n$ şi $x' = \dfrac{1 - n^2 - nx}{x + n}$. Luând $x = 0$ primim $0' = \dfrac{1}{n} - n \in \mathbb{Z}$, adică $n \in \{-1, 1\}$. Dacă $n = 1$ atunci $p = 0$, $e = 0$ şi $x * y = xy + x + y$, iar în $(\mathbb{Z}, *)$ singurele elemente simetrizabile sunt 0 şi -2. Dacă $n = -1$ atunci $p = 2$, $e = 2$ şi $x * y = xy - x - y + 2$, iar în $(\mathbb{Z}, *)$ sunt simetrizabile numai 0 şi 2.
• Dacă $m = -1$ se veifică analog cu cazul anterior că monoidul $(\mathbb{Z}, *)$ nu este grup.
În concluzie, $(\mathbb{Z}, *)$ este grup dacă şi numai dacă $m = 0$, $n = 1$ şi $p \in \mathbb{Z}$.

2.9. Răspuns. i) Elementele inversabile la stânga (dreapta) coincid cu funcţiile injective (surjective) şi cu elementele cu care se poate simplifica la stânga (dreapta) — vezi [34, Teoremele 1.3.14, 1.3.15]. Elementele inversabile coincid cu funcţiile bijective.
ii) M trebuie să fie finită.
iii) În acest caz, M^M este formtă din patru funcţii, definite prin tabelele:

x	0	1
$f_1(x)$	0	1

x	0	1
$f_2(x)$	1	0

x	0	1
$f_3(x)$	0	0

x	0	1
$f_4(x)$	1	1

,

tabla de operaţie este

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_3	f_3	f_3
f_4	f_4	f_4	f_4	f_4

iar elementele cerute la punctul i) sunt f_1 şi f_2.

2.10. i) Din soluţia problemei **1.52** punctul a) deducem că numărul operaţiilor (binare) pe A este $n^{(n^2)}$.
ii) Tabla unei operaţii binare comutative $\varphi : A \times A \to A$ este simetrică în raport cu diagonala principală deoarece $\varphi(a, b) = \varphi(b, a)$. Rezultă că φ este determinată de valorile sale pe $D = \{(a, a) \mid a \in A\} \cup D'$, unde D' este o submulţime a lui $A \times A$ obţinută alegând pentru orice $a, b \in A$, $a \neq b$, doar una dintre perechile (a, b) şi (b, a). Aşadar, D' are atâtea elemente câte submulţimi cu câte două elemente are A şi, prin urmare, $|D| = n + C_n^2 = \dfrac{n(n+1)}{2}$. Cum orice operaţie comutativă pe A

este determinată de restricţia sa la D, urmează că numărul operaţiilor comutative pe A coincide cu numărul funcţiilor cu domeniul D şi codomeniul A, deci este egal cu $\left|A^D\right| = n^{\frac{n(n+1)}{2}}$.
iii) Dacă $a \in A$ este element neutru pentru $\varphi : A \times A \to A$ atunci linia şi coloana elementului a din tabla lui φ sunt determinate întrucât $\varphi(a,b) = b = \varphi(b,a)$. Deci operaţia binară φ va fi determinată de restricţia sa la

$$D = \{(x,y) \in A^2 \mid x \neq a \neq y\} = (A \setminus \{a\}) \times (A \setminus \{a\}).$$

Cum $|D| = (n-1)^2$, numărul operaţiilor care au ca element neutru pe a este $\left|A^D\right| = n^{(n-1)^2}$, deci numărul operaţiilor pe A care admit element neutru este

$$n \cdot \left|A^D\right| = n^{(n-1)^2+1}.$$

iv) Din cele de mai sus deducem că numărul operaţiilor comutative care au element neutru pe $a \in A$ este egal cu numărul funcţiilor de la $D = (A \setminus \{a\}) \times (A \setminus \{a\}) \cap D'$ la A, adică $\left|A^D\right| = n^{\frac{n(n-1)}{2}}$. Deci numărul operaţiilor comutative pe A care admit element neutru este $n \cdot \left|A^D\right| = n^{\frac{n(n-1)}{2}+1}$.

2.11. Indicaţie. Se folosesc definiţia asociativităţii, a comutativităţii şi a stabilităţii.

2.12. Indicaţie. Mulţimea termenilor şirului $x,\ 2x = x + x, \dots,\ nx = (n-1)x + x, \dots$ este finită dacă şi numai dacă $x = 0$. Submulţimile lui $\mathbb{Z}$ finite şi stabile în $(\mathbb{Z}, +)$ sunt $\emptyset$ şi $\{0\}$.

2.13. Indicaţie. Cum mulţimea puterilor cu exponent din $\mathbb{N}^*$ ale unui număr întreg x este finită numai dacă $|x| \leq 1$, părţile stabile finite ale lui $(\mathbb{Z}, \cdot)$ se caută printre submulţimile mulţimii $A = \{-1, 0, 1\}$. Dintre cele $2^3 = 8$ submulţimi ale lui A sunt stabile numai $\emptyset$, $\{0\}$, $\{1\}$, $\{-1,1\}$, $\{0,1\}$, $\{-1,0,1\}$.

2.14. Indicaţie. Pentru orice $i \in \{1,2,3\}$ incluziunea $A \subseteq B_i$ exprimă chiar asociativitatea operaţiei $\cdot$.

2.15. Indicaţie. Se arată că $A = B_1$ (vezi problema anterioară), stabilind că operaţiile

$$\varphi_c : A \times A \to A,\ \varphi_c(x,y) = (cx)y \text{ şi } \varphi'_c : A \times A \to A,\ \varphi'_c(x,y) = c(xy)$$

coincid, ceea ce se constată alcătuind tablele lor. Analog se arată că $f \in B_1$, după care, aplicând problema anterioară deducem că elementele $a = f \cdot f$, $b = c \cdot c$, $d = c \cdot f$ aparţin lui B_1. Deci $A = B_1$ şi, conform cu problema anterioară, operaţia $\cdot$ este asociativă.

2.16. Indicaţie. $f : \mathcal{P}(M) \to \mathcal{P}(M),\ f(X) = C_M(X)(= M \setminus X)$ este un izomorfism.

2.17. Indicaţii. i) $\{\{a\} \mid a \in A\}$ este un subgrupoid al lui $(\mathcal{P}(A), \cdot)$ izomorf cu $(A, \cdot)$.
iv) $(B_1 \cdot B_2)(B_1 \cdot B_2) = B_1(B_2 \cdot B_1)B_2 = B_1(B_1 \cdot B_2)B_2 = (B_1 \cdot B_1)(B_2 \cdot B_2) \subseteq B_1 \cdot B_2$.
vii) Dacă în $\mathcal{P}(A) \neq \emptyset$ există element neutru, fie acesta M, atunci $M \neq \emptyset$ şi totuşi $\emptyset \cdot M = \emptyset \cdot \emptyset$.

2.18. Indicaţie. $2\mathbb{N} \wedge 3\mathbb{N} = 2\mathbb{N} \cap 3\mathbb{N} = 6\mathbb{N}$, $2\mathbb{N} \vee 3\mathbb{N} = \langle 2\mathbb{N} \cup 3\mathbb{N} \rangle = 2\mathbb{N} + 3\mathbb{N}$.

2.19. Indicaţie. $z \in xA \cap yA \Rightarrow \exists a \in A :\ z = xa = x^2a = xz \in x(yA) = xyA$.

2.20. Indicaţie. b) Pentru orice $a, b \in L$, $a \vee b$ este o majorantă pentru a şi b deoarece $a \vee (a \vee b) = (a \vee a) \vee b = a \vee b = a \vee (b \vee b) = (a \vee b) \vee b = b \vee (a \vee b)$ iar dacă $c \in L$ este o majorantă pentru a şi b atunci $a \vee c = c = b \vee c$ şi astfel, $(a \vee b) \vee c = a \vee (b \vee c) = a \vee c = c$, aşadar $a \vee b \leq c$.

2.21. Indicaţie. Această problemă este duala problemei anterioare.

2.22. Indicaţie. Această problemă este o consecinţă a problemelor anterioare. Pentru detalii se poate consulta şi [34, Teorema 1.6.5].

2.23. Răspuns. $a_1 = 0 = b_1;\ a_2 = 1,\ b_2 = 0;\ a_3 = 0,\ b_3 = 1$.

2.24. Răspuns. i) $y_0^2 = y_0$, adică y_0 trebuie să fie idempotent.
ii) $(B, \cdot)$ trebuie să conţină un element idempotent.

2.25. Indicaţie. ii) Se calculează produsul în $(f(A), \cdot)$ al lui $f(1)$ cu elementul neutru al lui $(B, \cdot)$. iii) Se aplică ii).

2.26. Indicaţie. Se folosesc definiţia subgrupoidului şi definiţia omomorfismului.

2.27. Indicaţie. Orice grupoid se aplică omomorf pe grupul cu un element.

2.28. Răspuns. i) În general, nu. De exemplu, $f : \mathbb{N}^* \to \{0, 1\}$, $f(1) = 1$ şi $f(n) = 0$ pentru $n > 1$ este un omomorfism al lui $(\mathbb{N}^*, \cdot)$ în $(\{0, 1\}, \cdot)$, în $(\mathbb{N}^*, \cdot)$ orice element este regulat, dar 0 nu este regulat în $(\{0, 1\}, \cdot)$. ii) f trebuie să fie unital.

2.29. Răspuns. $\langle A \rangle = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{N}^* \right\}$,

$$\langle A, D \rangle = \langle A \rangle \cup \left\{ \begin{pmatrix} 2^k & 0 \\ 0 & 0 \end{pmatrix} \mid k \in \mathbb{N}^* \right\} \cup \left\{ \begin{pmatrix} 2^k & 2^k n \\ 0 & 0 \end{pmatrix} \mid k, n \in \mathbb{N}^* \right\},$$

$$\langle B, C \rangle = \left\{ \begin{pmatrix} 2^k & 0 \\ 0 & 1 \end{pmatrix} \mid k \in \mathbb{N}^* \right\} \cup \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 2^n \end{pmatrix} \mid n \in \mathbb{N}^* \right\} \cup \left\{ \begin{pmatrix} 2^k & 0 \\ 0 & 2^n \end{pmatrix} \mid k, n \in \mathbb{N}^* \right\},$$

$$\langle B, D \rangle = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 2^n \end{pmatrix} \mid n \in \mathbb{N}^* \right\} \cup \left\{ \begin{pmatrix} 2^n & 0 \\ 0 & 0 \end{pmatrix} \mid n \in \mathbb{N}^* \right\}.$$

2.30. Indicaţii. a) Se arată că $\bigcup_{k \in \mathbb{N}} X_k$ este cel mai mic între subgrupoizii lui $(A, \cdot)$ ce include pe X. b) Dacă $Y_0 = f(X)$ şi $Y_{k+1} = Y_k \cup \{y_1 \cdot y_2 \mid y_1, y_2 \in Y_k\}$, se arată prin inducţie că $f(X_k) = Y_k$ pentru orice $k \in \mathbb{N}$.

2.31. Indicaţie. Se arată că dacă $f, g : A \to B$ sunt omomorfisme ale căror restricţii la X coincid, atunci $f = g$. Se procedează astfel: faptul că X generează pe $(A, \cdot)$ înseamnă că $\langle X \rangle = A$ şi se arată prin inducţie după n că $f|_{X_n} = g|_{X_n}$.

2.32. Răspuns. a) Dacă $f(1) = a$ atunci un omomorfism $\overline{f}$ care prelungeşte pe f este definit prin $\overline{f}(n) = a^n$. b) Nu, deoarece $g(1) = 1$ implică $g(2) = g(1+1) = g(1) + g(1) = 2$. c) Subsemigrupul lui $(\mathbb{N}, \cdot)$ generat de 2 este $\langle 2 \rangle = \{2^k \mid k \in \mathbb{N}^*\}$, iar omomorfismele cerute sunt $f_n : \mathbb{N}^* \to \langle 2 \rangle$, $f_n(k) = 2^{nk}$ $(n \in \mathbb{N}^*)$.

2.33. Cum $f(\mathbb{Q})$ este parte stabilă în $(\mathbb{Q}, \cdot)$ şi trebuie să fie şi o submulţime finită a lui $\mathbb{Z}$ deducem că există următoarele posibilităţi: 1) $f(\mathbb{Q}) = \{0\}$, 2) $f(\mathbb{Q}) = \{1\}$, 3) $f(\mathbb{Q}) = \{-1, 1\}$, 4) $f(\mathbb{Q}) = \{0, 1\}$, 5) $f(\mathbb{Q}) = \{-1, 0, 1\}$ (vezi soluţia problemei

2.13). În primele două cazuri obţinem endomorfismele f_1, f_2 definite respectiv prin $f_1(x) = 0$ şi $f_2(x) = 1$. Din $0x = 0$ rezultă că pentru orice endomorfism f avem $f(0)f(x) = f(0)$, ceea ce implică $f(0) = 0$ sau $f(x) = 1$ pentru orice $x \in \mathbb{Q}$. Deducem că în cazul 3) nu există nici un endomorfism, iar în cazurile 4) şi 5) avem $f(0) = 0$. Egalitatea $1x = x$ conduce la faptul că orice endomorfism f verifică egalitatea $f(1)f(x) = f(x)$, ceea ce arată că

$$f(1) = 0 \Rightarrow f(x) = 0,\ \forall x \in \mathbb{Q}.$$

Astfel, în cazul 4), $f(1) = 1$. În consecinţă $f(x^{-1}) = [f(x)]^{-1}$ pentru orice $x \neq 0$ şi se obţine un singur endomorfism f_4 definit prin

$$f_4(x) = \begin{cases} 0 & ,\ x = 0; \\ 1 & ,\ x \neq 0. \end{cases}$$

În cazul 5) este imposibil ca $f(1) = -1$ deoarece, în caz contrar, am avea

$$1 = (-1)(-1) = f(1)f(1) = f(1 \cdot 1) = f(1) = -1.$$

Urmează că $f(0) = 0$, $f(1) = 1$ şi $f(x) \in \{-1, 1\}$ pentru orice $x \neq 0$. Fie

$$A = \{p \in \mathbb{N}^* \mid p \text{ prim}\} \cup \{-1\} \text{ şi } B = \{p^{-1} \mid p \in A\}.$$

Cum mulţimea $A \cup B$ este un sistem de generatori pentru $(\mathbb{Q}, \cdot)$ şi $f(x^{-1}) = [f(x)]^{-1}$, f este determinat de restricţia sa la A. La fiecare submulţime nevidă P a lui A asociem un endomorfism f_P definit prin $f_P(0) = 0$, iar dacă $x \in \mathbb{Q}^*$ se scrie sub forma $x = p_1^{k_1} \cdots p_i^{k_i} q_{i+1}^{k_{i+1}} \cdots q_n^{k_n}$, cu $k_j \in \mathbb{Z}$ $(j = 1, \ldots, n)$, $p_j \in P$ $(j = 1, \ldots, i)$, $q_j \in A \setminus P$ $(j \in i, \ldots, n)$, atunci $f_P(x) = (-1)^{k_1 + \cdots + k_i}$. Când P parcurge mulţimea submulţimilor nevide ale lui A atunci f_P parcurge mulţimea endomorfismelor din cazul 5). Deci endomorfismele cerute sunt f_1, f_2, f_4 şi f_P cu $\emptyset \neq P \subseteq A$.

2.34. Răspuns. f_1 este omomorfism al lui $(M_n(\mathbb{C}), \cdot)$ în $(\mathbb{C}, \cdot)$, dar nu este omomorfism al lui $(M_n(\mathbb{C}), +)$ în $(\mathbb{C}, +)$, f_2 nu este omomorfism al lui $(M_n(\mathbb{C}), \cdot)$ în $(\mathbb{C}, \cdot)$, dar este omomorfism al lui $(M_n(\mathbb{C}), +)$ în $(\mathbb{C}, +)$, iar f_3 este omomorfism al lui $(M_n(\mathbb{C}), \cdot)$ în $(\mathbb{C}, \cdot)$, dar nu este omomorfism al lui $(M_n(\mathbb{C}), +)$ în $(\mathbb{C}, +)$.

2.35. Răspuns. f nu este endomorfism al lui $(\mathbb{C}, +)$, dar este endomorfism al lui $(\mathbb{C}, \cdot)$, iar g nu este endomorfism nici pentru $(\mathbb{C}, +)$, nici pentru $(\mathbb{C}, \cdot)$.

2.36. a) *Unicitatea:* Presupunem că există o operaţie $\cdot$ în P astfel ca fiecare p_j să fie omomorfism. Atunci

$$(a_i^1)_{i\in I} \cdot (a_i^2)_{i\in I} = (p_j((a_i^1)_{i\in I}) \cdot p_j((a_i^2)_{i\in I}))_{j\in I} = (p_j((a_i^1 \cdot a_i^2)_{i\in I}))_{i\in I} = (a_j^1 \cdot a_j^2)_{i\in I},$$

ceea ce arată unicitatea modului de a defini această operaţie.
Existenţa: Putem introduce o structură de grupoid pe P definind

$$(1) \qquad (a_i^1)_{i\in I} \cdot (a_i^2)_{i\in I} = (a_i^1 \cdot a_i^2)_{i\in I},$$

pentru orice $(a_i^1)_{i\in I}, (a_i^2)_{i\in I} \in P$. Dacă $j \in I$ atunci din (1) urmează

$$p_j((a_i^1 \cdot a_i^2)_{i\in I})) = a_j^1 \cdot a_j^2 = p_j((a_i^1)_{i\in I}) \cdot p_j((a_i^2)_{i\in I}),$$

ceea ce ne arată că p_j, $j \in I$ sunt omomorfisme.
b) *Unicitatea lui u:* Presupunem că există un omomorfism $u : B \to P$ este pentru care diagrama

$$\begin{tikzcd} B \arrow[d, "u"'] \arrow[dr, "u_j"] & \\ P \arrow[r, "p_j"] & A_j \end{tikzcd}$$

este comutativă pentru orice $j \in I$. Atunci $p_j(u(b)) = u_j(b)$ pentru orice $b \in B$, adică componenta de indice j ale familiei $u(b)$ este $u_j(b)$. Deci $u(b) = (u_i(b))_{i\in I}$ pentru orice $b \in B$, de unde rezultă unicitatea modului de a defini pe u.
Existenţa lui u: Definim funcţia $u : B \to P$ prin $u(b) = (u_i(b))_{i\in I}$. Pentru orice $b_1, b_2 \in B$, folosind definiţia lui u şi (1), avem

$$\begin{aligned} u(b_1 \cdot b_2) = (u_i(b_1 \cdot b_2))_{i\in I} &= (u_i(b_1) \cdot u_i(b_2))_{i\in I} = (u_i(b_1))_{i\in I} \cdot (u_i(b_2))_{i\in I} \\ &= u(b_1) \cdot u(b_2). \end{aligned}$$

Deci u este un omomorfism. Pentru orice $b \in B$ şi orice $j \in I$ avem

$$(p_j \circ u)(b) = p_j((u_i(b))_{i\in I}) = u_j(b), \tag{2}$$

de unde urmează $p_j \circ u = u_j$, adică diagrama din enunţ este comutativă.
c) Din proprietatea de universalitate a lui P rezultă că există un singur omomorfism $f : P' \to P$ astfel încât

$$\begin{tikzcd} P' \arrow[d, dotted, shift right, "f"'] \arrow[dr, "p'_j"] & \\ P \arrow[u, dotted, shift right, "f'"'] \arrow[r, "p_j"] & A_j \end{tikzcd} \qquad p'_j = p_j \circ f, \forall j \in I,$$

iar din proprietatea de universalitate a lui P' urmează că există un singur omomorfism $f' : P \to P'$ astfel ca $p_j = p'_j \circ f'$ pentru orice $j \in I$. Deci $p_j = p_j \circ (f \circ f')$ pentru orice $j \in I$, iar pe de altă parte $p_j = p_j \circ 1_P$ pentru orice $j \in I$. Acum, din unicitatea lui u deducem că $f \circ f' = 1_P$. Analog se arată că $f' \circ f = 1_{P'}$. Deci f este un izomorfism şi $f^{-1} = f'$.
d) Dacă $f_1, f_2 \in A^I$ atunci $f_1 \cdot f_2 : I \to A$ este definită prin $(f_1 \cdot f_2)(i) = f_1(i) \cdot f_2(i)$, pentru orice $i \in I$. Submulţimea $\{f_a \in A^I \mid f_a(i) = a, \forall i \in I\}$ este un subgrupoid al lui $(A^I, \cdot)$ izomorf cu $(A, \cdot)$ deoarece corespondenţa $a \mapsto f_a$ este un omomorfism injectiv de la A la A^I.

2.37. Indicaţie. b) Din $f_1 \circ g'_1 = f_2 \circ g'_2$ rezultă că $(g'_1(x), g'_2(x)) \in S$ pentru $x \in S'$, ceea ce ne permite să definim pe g prin $g(x) = (g'_1(x), g'_2(x))$.

Observaţii: a) Tripletul (S, g_1, g_2) se numeşte *produsul fibrat al omomorfismelor* f_1, f_2.
b) Se constată cu uşurinţă că enunţul problemei de mai sus rămâne adevărat dacă înlocuim „*grupoid*" cu „*mulţime*" şi „*omomorfism*" cu „*funcţie*". Atunci (S, g_1, g_2) este *produsul fibrat al funcţiilor* f_1 şi f_2.

2.38. Indicaţie. b) Din $f \circ h = g \circ h$ rezultă că $h(C) \subseteq E$, ceea ce ne permite să definim pe γ prin $\gamma(c) = h(c)$.

Observaţii: a) Perechea (E, i) se numeşte *nucleul perechii de omomorfisme* (f, g).
b) Se constată cu uşurinţă că enunţul problemei de mai sus rămâne adevărat dacă înlocuim ,,*grupoid*” cu ,,*mulţime*” şi ,,*omomorfism*” cu ,,*funcţie*”. Atunci perechea (E, i) este *nucleul perechii de funcţii* (f, g).

2.39. Răspuns. $|A/A \times A| = 1$.

2.40. Răspuns. ρ_1 nu este congruenţă nici pe $(\mathbb{C}, +)$ şi nici pe $(\mathbb{C}, \cdot)$; ρ_2 nu este congruenţă pe $(\mathbb{C}, +)$, dar este congruenţă pe $(\mathbb{C}, \cdot)$, iar dacă $z \in \mathbb{C}$ atunci clasa de echivalenţă $\rho_2\langle z\rangle$ a lui z în raport cu ρ_2 este formată din numerele complexe situate pe cercul cu centrul în origine şi de rază $|z|$. În grupoidul cât $(\mathbb{C}/\rho_2, \cdot)$ produsul a două clase este definit prin $\rho_2\langle z\rangle \cdot \rho_2\langle z'\rangle = \rho_2\langle zz'\rangle$.

2.41. Indicaţii. a) Din [34, Teorema 1.8.15] rezultă că funcţia $\overline{f} : A/\ker f \to f(A)$, $\overline{f}((\ker f)\langle x\rangle) = f(x)$ este bijectivă, iar faptul că $\overline{f}$ este omomorfism se verifică imediat.
b) Nucleul lui f este congruenţa ρ_2 din problema anterioară $f(\mathbb{C}) = [0, +\infty)$, iar izomorfismul $\mathbb{C}/\rho_2 \to [0, +\infty)$ dat de a) asociază cercului cu centrul în origine şi de rază $|z|$ lungimea razei sale.
c) Izomorfismul $M_n(\mathbb{C})/\ker f \to \mathbb{C}$ dat de a) asociază clasei matricelor cu acelaşi determinant valoarea acestui determinant.

Observaţie: Afirmaţia de la a) din problema de mai sus se numeşte *teorema întâi de izomorfism pentru grupoizi.*

2.42. Indicaţii. a) Avem $\rho(B) = \{y \in A \mid \exists b \in B : \ b\rho y\}$. Dacă $x \in B$ atunci $\rho'\langle x\rangle = \{b \in B \mid x\rho b\}$, iar dacă $y \in \rho(B)$ atunci clasa $\rho''\langle y\rangle = \{a \in A \mid y\rho a\}$ are un reprezentant din B. Izomorfismul dintre grupoizii cât $B/\rho' = \{\rho'\langle x\rangle \subseteq B \mid x \in B\}$ şi $\rho(B)/\rho'' = \{\rho\langle y\rangle \subseteq A \mid y \in \rho(B)\}$ este dat de corespondenţa $\rho'\langle x\rangle \mapsto \rho''\langle x\rangle$. Acelaşi rezultat se poate obţine aplicând **2.41** a) restricţiei la B a omomrfismului $p_\rho : A \to A/\rho$.
b) Dacă ρ_2', respectiv ρ_2'' sunt restricţiile lui ρ_2 la B, respectiv la $\rho_2(B) = \{z \in \mathbb{C} \mid |z| > 1\}$ atunci ρ_2' şi ρ_2'' sunt congruenţe pe B, respectiv $\rho_2(B)$ şi

$$B/\rho_2' = \{\{-x, x\} \mid x > 1\},\ \rho_2(B)/\rho_2'' = \{\rho_2\langle z\rangle \mid |z| > 1\},$$

adică $\rho_2(B)/\rho_2''$ este formată din cercurile cu centrul în origine şi de rază (strict) mai mare decât 1. Izomorfismul dat de a) este $B/\rho_2' \to \rho_2(B)/\rho_2'',\ \{-x, x\} \mapsto \rho_2\langle x\rangle$.

Observaţie: Afirmaţia de la a) din problema de mai sus se numeşte *teorema a doua de izomorfism pentru grupoizi.*

2.43. Indicaţie. $\mathbb{Z}/\rho_n = \mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, unde $\overline{i} = \{kn + i \mid k \in \mathbb{Z}\}$, iar operaţia $+$ este definită pe $\mathbb{Z}_n$ prin $\overline{i} + \overline{j} = \overline{i + j}$.

2.44. Răspuns. Da, pentru că $n|x_1 - y_1$ şi $n|x_2 - y_2$ implică

$$n|x_1(x_2 - y_2) + y_2(x_1 - y_1) = x_1x_2 - y_1y_2.$$

Operaţia din $(\mathbb{Z}_n, \cdot)$ este definită prin $\overline{i} \cdot \overline{j} = \overline{ij}$.

2.45. Indicaţie. $(\mathbb{Z}_2, \cdot)$ nu este o subalgebră a algebrei $(\mathcal{P}(\mathbb{Z}), \cdot)$.

2.46. Indicaţii. a) Din teorema de factorizare a unei funcţii printr-o funcţie surjectivă rezultă existenţa unei singure funcţii $f : A/\rho_1 \to A/\rho_2$ astfel încât $p_{\rho_2} = f \circ p_{\rho_1}$. Aceasta este surjectivă şi e definită prin $f(\rho_1\langle x\rangle) = \rho_2\langle x\rangle$. Se arată că f este un omomorfism de grupoizi. Tot din teorema de factorizare a unei funcţii printr-o surjecţie deducem existenţa unei bijecţii $\overline{f}$ care face comutativ triunghiul din dreapta al diagramei

$$\begin{tikzcd}
A \arrow[r, "p_{\rho_1}"] \arrow[dr, "p_{\rho_2}"'] & A/\rho_1 \arrow[r, "p_{\rho_2/\rho_1}"] \arrow[d, dotted, "f"] & (A/\rho_1)/(\rho_2/\rho_1) \arrow[dl, dotted, "\overline{f}"] \\
 & A/\rho_2 &
\end{tikzcd}$$

Se arată uşor că $\overline{f}$ este un omomorfism de grupoizi.
b) Cu notaţiile de la **2.43** avem $\rho_6 \subseteq \rho_2$, $\mathbb{Z}/\rho_2 = \mathbb{Z}_2 = \{\widehat{0}, \widehat{1}\}$, $\mathbb{Z}/\rho_6 = \mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$, $\mathbb{Z}_6/(\rho_6/\rho_2) = \{\{\overline{0}, \overline{2}, \overline{4}\}, \{\overline{1}, \overline{3}, \overline{5}\}\}$. Izomorfismul dintre $\mathbb{Z}_2$ şi $\mathbb{Z}_6/(\rho_6/\rho_2)$ dat de a) asociază lui $\widehat{0}$ pe $\{\overline{0}, \overline{2}, \overline{4}\}$, iar lui $\widehat{1}$ pe $\{\overline{1}, \overline{3}, \overline{5}\}$.

Observaţie: Afirmaţia de la a) din problema de mai sus se numeşte *teorema a treia de izomorfism pentru grupoizi.*

2.47. a) Fie $a_1, a_2 \in F(A)$. Ştiind că $\langle X \cup \{a_1 \cdot a_n\}\rangle \subsetneq \langle X \cup \{a_1, a_2\}\rangle$ din egalitatea $\langle X \cup \{a_1 \cdot a_2)\}\rangle = A$ deducem $\langle X \cup \{a_1, a_2\}\rangle = A$. Întrucât $a_2 \in F(A)$, urmează $\langle X \cup \{a_1\}\rangle = A$, iar din $a_1 \in F(A)$ avem $\langle X\rangle = A$. Aşadar $a_1 \cdot a_2 \in F(A)$, adică $F(A)$ este un subgrupoid.
b) Fie $a \in F(A)$ şi $f : A \to A$ un automorfism. Dacă $\langle X \cup \{f(a)\}\rangle = A$ atunci aplicăm pe f^{-1} şi, conform problemei anterioare, avem $\langle f^{-1}(X) \cup \{a\}\rangle = A$ de unde, întrucât $a \in F(A)$, urmează $\langle f^{-1}(X)\rangle = A$. Aplicând pe f, obţinem $\langle X\rangle = A$. Deci $f(a) \in F(A)$ şi astfel, $f(F(A)) \subseteq F(A)$.
c) Fie $\{M_i \mid i \in I\}$ mulţimea subgrupoizilor maximali ai lui $(A, \cdot)$ şi $M = \bigcap_{i\in I} M_i$. Avem:

$$a \notin M \Rightarrow \exists i_0 \in I, a \notin M_{i_0} \Rightarrow \langle M_{i_0} \cup \{a\}\rangle = A \text{ şi } \langle M_{i_0}\rangle = M_{i_0} \neq A \Rightarrow a \notin F(A)\,,$$

ceea ce ne arată că $F(A) \subseteq M$.

Dacă $a \notin F(A)$, atunci există $X \subseteq A$ astfel încât $\langle X \cup \{a\}\rangle = A$ şi $\langle X\rangle \neq A$. Fie $\mathcal{S}$ mulţimea acelor subgrupoizi B ai lui A pentru care avem $X \subseteq B$ şi $a \notin B$. Evident că $\langle X\rangle \in \mathcal{S}$, adică $\mathcal{S} \neq \emptyset$. Mulţimea ordonată $(\mathcal{S}, \subseteq)$ verifică ipoteza lemei lui Zorn, deci există un subgrupoid M' maximal în $(\mathcal{S}, \subseteq)$. Acesta este un subgrupoid maximal al lui A, iar din $M' \in \mathcal{S}$ urmează $a \notin M'$. Rezultă $a \notin M$ şi astfel am arătat că $a \notin F(A)$ implică $a \notin M$, adică $M \subseteq F(A)$.

2.48. i) Demonstrăm egalitatea cerută prin inducţie după $q \in \mathbb{N}$. Egalitatea este, evident, adevărată pentru $q = 0$. Dacă $q > 0$ şi $a^{m+(q-1)(n-m)} = a^m$ atunci

$$a^{m+q(n-m)} = a^{m+(q-1)(n-m)+n-m} = a^{m+(q-1)(n-m)}a^{n-m} = a^m a^{n-m} = a^n = a^m.$$

ii) Dacă $k \geq n$ atunci $k - m \geq n - m$. Împărţind pe $k - m$ la $n - m$ obţinem

$$k - m = q(n - m) + r, \text{ cu } 0 \leq r < n - m,$$

de unde, folosind i), deducem

$$a^k = a^{m+q(n-m)+r} = a^{m+q(n-m)} \cdot a^r = a^m \cdot a^r = a^m \cdot a^{n-m} = a^n = a^m.$$

iii) Egalitatea cerută rezultă din ii).
iv) Stabilitatea submulţimii K_{n-m} în $(A, \cdot)$ este o consecinţă imediată a lui ii). Vom demonstra că $(K_{n-m}, \cdot)$ este grup arătând că este izomorf cu grupul aditiv $(\mathbb{Z}_{n-m}, +)$ al claselor de resturi modulo $n-m$. Numerele $m, m+1, \ldots, n-1$ formează un sistem complet de reprezentanţi al lui $\mathbb{Z}_{n-m} = \{\overline{0}, \overline{1}, \ldots, \overline{n-m-1}\}$. Aşadar, pentru fiecare $\overline{i} \in \mathbb{Z}_{n-m}$ există un singur $k_i \in \{m, m+1, \ldots, n-1\}$ astfel încât $\overline{i} = \overline{k_i}$, de unde urmează că funcţia $f : \mathbb{Z}_{n-m} \to K_{n-m}$, $f(\overline{i}) = a^{k_i}$ este bijectivă. Dacă $\overline{i}, \overline{j} \in \mathbb{Z}_{n-m}$ şi $k_i + k_j - m = q(n-m) + r$, cu $0 \leq r < n-m$, atunci $i + j \equiv k_i + k + j \equiv m + r (\operatorname{mod} n - m)$ şi $m \leq m + r < n$. Rezultă că $k_{i+j} = m + r$, adică $f(\overline{i+j}) = a^{m+r}$, iar cum

$$f(\overline{i}) \cdot f(\overline{j}) = a^{k_i} \cdot a^{k_j} = a^{k_i + k_j} = a^{m+q(n-m)+r} = a^{m+r},$$

deducem că f este un izomorfism.

2.49. Indicaţie. i) Notăm cu r_k restul împărţirii lui k la $n-m$ şi considerăm funcţia

$$f : \mathbb{N}^* \to \{1, \ldots, n-1\},\ f(k) = \begin{cases} k & , \text{ dacă } k < n; \\ m + r_{k-m} & , \text{ dacă } k \geq n. \end{cases}$$

Se arată că pentru orice $k, j \in \mathbb{N}^*$ avem $f(k) + f(j) = f(k+j)$ şi că egalitatea

$$k \circ j = f(k+j)$$

defineşte o operaţie (binară) asociativă pe $A = \{1, \ldots, n-1\}$. Semigrupul $(A, \circ)$ este generat de 1, iar tipul său este (m, n).
ii) Dacă $\langle a \rangle$ şi $\langle b \rangle$ sunt semigrupuri ciclice de tip (m, n) atunci $\varphi : \langle a \rangle \to \langle b \rangle$, $\varphi(a^k) = b^k$ $(k = 1, \ldots, n-1)$ este un izomorfism.
iii) Dacă $\langle a \rangle$ este un semigrup ciclic infinit atunci $\psi : \mathbb{N} \to \langle a \rangle$, $\psi(k) = a^k$ este un izomorfism.

2.50. Indicaţie. Se foloseşte problema **2.48**.

2.51. Indicaţii. i) $\overline{x} = x'xx'$; ii) $x'x$ este idempotent; iii) Vezi problema **1.57**.

2.52. Indicaţie. ii) Presupunem că $(A, \cdot)$ este regular şi are un singur element idempotent. Fie ecuaţia $ax = b$, cu $a, b \in A$. Cum $a\overline{a}$ şi $b\overline{b}$ sunt idempotente, rezultă că $a\overline{a} = b\overline{b}$, de unde, înmulţind cu b, obţinem $a(\overline{a}b) = b$. Deci $\overline{a}b$ este o soluţie a ecuaţiei $ax = b$. Analog se arată că $b\overline{a}$ este o soluţie a ecuaţiei $ya = b$.

2.53. i) Dacă $x, y \in G$ atunci $x * y \in G$ deoarece

$$x * y = -1 + \frac{(x+1)(y+1)}{1+xy} \quad \text{şi} \quad x * y = 1 - \frac{(x-1)(y-1)}{1+xy}.$$

Aşadar, $*$ este o operaţie pe G. Din (1) rezultă că $*$ este comutativă. Asociativitatea sa se obţine astfel:

$$(x * y) * z = \frac{x+y}{1+xy} * z = \frac{x+y+z+xyz}{xy+xz+yz+1},$$
$$x * (y * z) = x * \frac{y+z}{1+yz} = \frac{x+y+z+xyz}{xy+xz+yz+1}.$$

Presupunem că e este elementul neutru. Atunci $x * e = x$ pentru orice $x \in G$, adică $\dfrac{x+e}{1+xe} = x$ pentru orice $x \in G$. Rezultă că $e = 0$. Prin urmare, dacă elementul neutru există, acesta este 0. Întrucât $x * 0 = x$ pentru orice $x \in G$, rezultă că 0 este elementul neutru. Dacă x' este simetricul lui $x \in G$ atunci $x * x' = 0$ de unde deducem $x' = -x \in G$. Deci, dacă simetricul lui x există, acesta este $-x$. Se verifică uşor că $-x$ este simetricul lui x pentru orice $x \in G$. Astfel am arătat că $(G, *)$ este un grup abelian.
ii) Cum imaginea elementului neutru printr-un omomorfism de grupuri este elementul neutru, rezultă că $f(1) = 0$, ceea ce implică $\alpha = 1$. Deci

$$f(x) = \frac{x-1}{x+1}\,. \tag{2}$$

Întrucât,

$$\frac{x-1}{x+1} > -1 \Leftrightarrow \frac{2x}{x+1} > 0\,,$$
$$\frac{x-1}{x+1} < +1 \Leftrightarrow \frac{-2}{x+1} < 0\,,$$

avem $f(x) \in G$ pentru orice $x \in \mathbb{R}_+^*$, ceea ce arată că egalitatea (2) defineşte o funcţie $f : \mathbb{R}_+^* \to G$. Funcţia f este bijectivă deoarece ecuaţia $f(x) = y$ are o soluţie unică $x = \dfrac{1+y}{1-y} \in \mathbb{R}_+^*$. Prin calcul se arată că f este un omomorfism, adică

$$f(x_1x_2) = \frac{x_1x_2 - 1}{x_1x_2 + 1} = f(x_1) * f(x_2)\,.$$

Deci f este izomorfism.

2.54. Indicaţie. $(\mathbb{R}, *)$ este monoid comutativ şi $e = 6$ este elementul neutru. $(\mathbb{R}, *)$ nu este grup deoarece 5 nu are simetric. $(\mathbb{R} \setminus \{5\}, *)$ este grup comutativ. În acest grup elementul neutru este $e = 6$ şi simetricul lui $x \neq 5$ este $x' = \dfrac{5x-24}{x-5} \neq 5$.

2.55. Indicaţie. Fie $a \in G$ şi $f_a : X \to G$, $f_a(x) = a$. Funcţia $\varphi : G \to G^X$, $\varphi(a) = f_a$ este un omomorfism injectiv.

2.56. Indicaţie. Se ia în i) $x = 0$.

2.57. Indicaţie. Faptul că $aG = G = Ga$ pentru orice $a \in G$ este echivalent cu faptul că pentru orice $a, b \in G$ ecuaţiile $ax = b$ şi $ya = b$ au soluţii în G.

2.58. Indicaţii. b) Se consideră cazurile i) $n = 0$, ii) $n \in \mathbb{N}^*$, iii) $-n \in \mathbb{N}^*$. Cazul ii) se demonstrează prin inducţie după n, iar soluţia pentru cazul iii) rezultă din ii), a) şi din definiţia puterilor cu exponent negativ.
c) Dacă $m = 0$ sau $n = 0$, egalitatea are loc. Prin inducţie se arată că

$$xy = yx \Rightarrow x^m y = yx^m,\ \forall m \in \mathbb{N}^*.$$

Folosind acest rezultat avem

$$xy = yx \Rightarrow yx^{-1} = x^{-1}y \Rightarrow x^{-1}y = yx^{-1} \Rightarrow x^{-m}y = yx^{-m},\ \forall m \in \mathbb{N}^*.$$

Aşadar, $xy = yx$ implică $x^m y = yx^m$ pentru orice $m \in \mathbb{Z}$. Folosind acest fapt deducem:

$$x^m y = yx^m \Rightarrow x^m y^n = y^n x^m,\ \forall n \in \mathbb{Z}.$$

2.59. Indicaţie. Se foloseşte punctul i) al problemei anterioare.

2.60. Indicaţii. Dacă $a \in G$ este regulat atunci funcţiile $t_a, t'_a : G \to G$, $t_a(x) = ax$, $t'_a(x) = xa$ fiind injective, sunt şi surjective (deoarece G este finit), deci pentru orice $a, b \in G$ ecuaţiile $ax = b$ şi $ya = b$ au soluţii în G şi astfel G este grup. Grupurile infinite nu pot fi caracterizate analog: de exemplu, $(\mathbb{Z}^*, \cdot)$ este un semigrup în care orice element este regulat, dar nu e grup.

2.61. Indicaţie. Fie $a \in \mathbb{R}$, $a > 0$, $a \neq 1$. Funcţia $f : \mathbb{R}_+^* \to \mathbb{R}$, $f(x) = \log_a x$ este un izomorfism.

2.62. Indicaţie. $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \sqrt[n]{x}$ este un izomorfism al lui $(\mathbb{R}, +)$ pe $(\mathbb{R}, *)$.

2.63. Indicaţie. Funcţia $f : \mathbb{C} \to \mathbb{R} \times \mathbb{R}$, $f(a + bi) = (a, b)$ este un izomorfism al lui $(\mathbb{C}, +)$ în $(\mathbb{R} \times \mathbb{R}, +)$. În $(\mathbb{R}^* \times \mathbb{R}^*, \cdot)$ avem $[(a, b)]^n = (1, 1)$ $(n \in \mathbb{N}^*)$ dacă şi numai dacă $a, b \in \{-1, 1\}$. Dacă ar exista un izomorfism g al lui $(\mathbb{C}^*, \cdot)$ în $(\mathbb{R}^* \times \mathbb{R}^*, \cdot)$ atunci toate rădăcinile complexe z ale unităţii (care formează o mulţime infinită) ar verifica o egalitate de forma $[g(z)]^n = (1, 1)$ deci bijecţia g ar duce o submulţime infinită a domeniului într-o submulţime finită a codomeniului, ceea ce e imposibil.

2.64. Indicaţii. i) Corespondenţa $(g, g') \mapsto (g', g)$ realizează un izomorfism.
ii) Corespondenţele $(g, g', g'') \mapsto ((g, g'), g'')$ şi $(g, g', g'') \mapsto (g, (g', g''))$ realizează izomorfisme. Aceste izomorfisme pot fi obţinute şi aplicând proprietatea de universalitate a produsului direct de grupuri.

2.65. Indicaţie. Surjectivitatea lui t_a (respectiv t'_a) este echivalentă cu faptul că pentru orice $b \in G$ ecuaţia $ax = b$ (respectiv $ya = b$) are soluţie în G.

2.66. Indicaţie. ii) Dacă $(G, \cdot)$ este un monoid atunci corepondenţa $g \mapsto t_g$ realizează izomorfismul cerut. iii) Funcţia $\varphi : G \to T'(G)$, $\varphi(g) = t_{g^{-1}}$ este izomorfism.

2.67. Indicaţie. i) Compusa a două omomorfisme de grupoizi este, de asemenea, un omomorfism. ii) $Aut(G, \cdot) = U(End(G, \cdot), \circ)$.

2.68. Indicaţie. ii) Dacă $0'$ este elementul neutru din $(G', +)$ atunci $\theta : G \to G'$, $\theta(x) = 0'$ este elementul neutru din $(Hom(G, G'), +)$, iar dacă $f : G \to G'$ este un omomorfism atunci $-f : G \to G'$, $(-f)(x) = -f(x)$ este, de asemenea, un omomorfism.

2.69. Indicaţii. Să remarcăm că înmulţirea definită este determinată de (distributivitatea sa faţă de adunare şi) de produsele din tabla

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

i) $1 = 1 + 0i + 0j + 0k$ este elementul neutru. ii) Pentru $q = a_1 + a_2 i + a_3 j + a_4 k$ luăm $\overline{q} = a_1 - a_2 i - a_3 j - a_4 k$ şi $N(q) = q\overline{q}$. Avem $N(q) = a_1^2 + a_2^2 + a_3^2 + a_4^2$, iar dacă $q \neq 0$ atunci $q^{-1} = \dfrac{1}{N(q)} \cdot \overline{q}$.

2.70. Evident, $H \neq \emptyset$ (de exemplu, $1 \in H$). Întrucât $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$ şi $|z|^{-1} = |z^{-1}|$, avem

$$z_1, z_2 \in H \Rightarrow |z_1| = 1 = |z_2^{-1}| \Rightarrow |z_1 \cdot z_2^{-1}| = |z_1| \cdot |z_2^{-1}| = 1 \Rightarrow z_1 \cdot z_2^{-1} \in H.$$

Deci H este subgrup al lui $(\mathbb{C}^*, \cdot)$. Cum $1 \in H$, dar $1 + 1 \notin H$, H nu este parte stabilă, deci nici subgrup, în $(\mathbb{C}, +)$. Luând $H' = \mathbb{R}^*$, H' este subgrup al lui $(\mathbb{C}^*, \cdot)$, dar $H \cup H'$ nu este subgrup deoarece nu este parte stabilă (de exemplu, $2, i \in H \cup H'$ şi $2i \notin H \cup H'$).

2.71. Indicaţie. $\emptyset \in \mathcal{I} \setminus \mathcal{S}$.

2.72. Indicaţii. i) Supremumul mulţimii vide în laticea subsemigrupurilor lui G este $\emptyset$, care nu este un subgrup al lui G. ii) $H = \sup(\langle x \rangle)_{x \in H}$.

2.73. Indicaţie. Dacă $H_1, H_2 \leq G$ şi există $h_1 \in H_1 \setminus H_2$, $h_2 \in H_2 \setminus H_1$ atunci $h_1 h_2 \notin H_1 \cup H_2$ pentru că $h_1 h_2 \in H_1$ implică $h_2 \in H_1$, iar $h_1 h_2 \in H_2$ implică $h_1 \in H_2$.

2.74. Indicaţie. $H_3 \subseteq H_1 \cup H_2$ dacă şi numai dacă $H_3 = (H_1 \cap H_3) \cup (H_2 \cap H_3)$ şi se poate folosi ultima parte din problema anterioară.

2.75. Indicaţie. Fie $f : H \times K \to H \cdot K$, $f(h, k) = hk$ şi $\rho = \ker f$. Cum f este o funcţie surjectivă avem $|(H \times K)/\rho| = |H \cdot K|$ (vezi [34, Teorema 1.8.15]). În plus, $\left|\overline{(h, k)}\right| = |H \cap K|$, deoarece clasa de echivalenţă $\overline{(h, k)}$ a lui (h, k) este

$$\overline{(h, k)} = \{(hkg^{-1}, g) \mid g \in (H \cap K)k\}.$$

Toate clasele din $(H \times K)/\rho$ având cardinalul $|H \cap K|$ şi cardinalul mulţimii claselor fiind $|H \cdot K|$ avem $|H| \cdot |K| = |H \times K| = |H \cdot K| \cdot |H \cap K|$.

2.76. Răspuns.
a) În S_7, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 3 & 5 & 7 & 6 & 2 \end{pmatrix} = (2, 4, 5, 7)$, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = (1, 2)$ şi $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 2 & 6 & 7 & 4 & 5 \end{pmatrix}$ nu este un ciclu. b) $\sigma_1^3 = (4, 8, 6, 5)$, $\sigma_2^2 \circ \sigma_1 = (2, 3, 5, 8, 4, 6)$, $\sigma_3 \circ \sigma_4 \circ \sigma_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 7 & 1 & 3 & 8 & 5 & 2 \end{pmatrix}$, $\sigma_3^4 \circ \sigma_4^2 = (2, 4, 8, 7, 3, 5, 6)$, $\sigma_5 \circ \sigma_4 \circ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 2 & 5 & 4 & 7 & 3 & 6 \end{pmatrix}$.

2.77. Dacă $f \in S_M \setminus \{1_M\}$ atunci există $a \in M$ astfel încât $b = f(a) \neq a$. Din $|M| \geq 3$ rezultă că există $c \in M \setminus \{a, b\}$. Luând funcţia $g : M \to M$ definită prin $g(b) = c$, $g(c) = b$ şi $g(x) = x$ pentru orice $x \in M \setminus \{b, c\}$ avem $(f \circ g)(a) = b$ şi $(g \circ f)(a) = c$ ceea ce implică $f \circ g \neq g \circ f$.

2.78. Dacă $f, g \in S_M$ sunt permutări disjuncte şi $x \in M$ atunci avem una din următoarele posibilităţi: i) $f(x) = x = g(x)$, ii) $f(x) \neq x$ (şi atunci $x = g(x)$) sau iii) $g(x) \neq x$ (şi atunci $x = f(x)$). În primul caz avem $(f \circ g)(x) = x = (g \circ f)(x)$. În cazul ii) avem $(f \circ g)(x) = f(g(x)) = f(x)$, iar cum $f(x) \neq x$ şi f este injectivă avem $f(f(x)) \neq f(x)$, deci $f(x) = g(f(x)) = (g \circ f)(x)$. Analog se tratează şi cazul iii). Aşadar, $f \circ g = g \circ f$.

2.79. Indicaţie. Fie $\alpha = (i_1, i_2, \ldots, i_l)$ şi $\beta = (j_1, j_2, \ldots, j_k)$. Dacă $\{i_1, i_2, \ldots, i_l\}$, $\{j_1, j_2, \ldots, j_k\}$ sunt mulţimi disjuncte, faptul că $\alpha, \beta \in S_n$ sunt disjuncte rezultă din definiţie. Reciproc, se arată că dacă $\{i_1, i_2, \ldots, i_l\} \cap \{j_1, j_2, \ldots, j_k\} \neq \emptyset$ atunci α şi β nu sunt disjuncte. Într-adevăr, fără a restrânge generalitatea putem presupune că $i_1 = j_1$ şi atunci $\alpha(i_1) = i_2 \neq i_1$ şi $\beta(i_1) = \beta(j_1) = j_2 \neq j_1 = i_1$.

2.80. Răspuns. a) $\tau = (1, 9, 2, 12) \circ (3, 8) \circ (4, 11, 10) \circ (5, 6, 7)$; b) $\sigma = (1, 2, 3) \circ (4, 5, 6, 8) = (1, 3) \circ (1, 2) \circ (4, 8) \circ (4, 6) \circ (4, 5) = (1, 2) \circ (2, 3) \circ (4, 5) \circ (5, 6) \circ (6, 8)$.

2.81. Răspuns. i) C_n^2; ii) $(n-1)!$; iii) $(l-1)! \cdot C_n^l$; iv) $\sum_{l=2}^{n} (l-1)! \cdot C_n^l$.

2.82. Indicaţie. iii) se arată prin inducţie după m.

2.83. Indicaţii. a) Avem $(\sigma \circ \gamma \circ \sigma^{-1})(\sigma(i_k)) = \sigma(i_1)$. Dacă $j \in \{1, \ldots, k-1\}$ avem $(\sigma \circ \gamma \circ \sigma^{-1})(\sigma(i_j)) = \sigma(i_{j+1})$, iar dacă $i \notin \{\sigma(i_1), \ldots, \sigma(i_k)\}$, adică $\sigma^{-1}(i) \notin \{i_1, \ldots, i_k\}$, atunci $\gamma(\sigma^{-1}(i)) = \sigma^{-1}(i)$, ceea ce implică $(\sigma \circ \gamma \circ \sigma^{-1})(i) = i$.
b) Folosind a) se arată că $\sigma_1 \circ \sigma_4 \circ \sigma_1^{-1} = (4, 3, 2, 5, 1) \circ (2, 3) \circ (2, 6)$, $\sigma_5^{-2} \circ \sigma_3 \circ \sigma_5^2 = (8, 4, 7) \circ (7, 5, 2, 3) \circ (8, 6, 4, 1)$, $\sigma_2^{-5} \circ \sigma_4 \circ \sigma_2^5 = (8, 2, 1, 3, 4) \circ (1, 2) \circ (1, 5)$.
c) Se verifică egalităţile $\sigma_1 \circ \sigma_2 \circ \sigma_1^{-1} = \sigma_2$ şi $\sigma_1 \circ \sigma_3 \circ \sigma_1^{-1} = \sigma_3$.

2.84. Fie $\sigma \in S_n$ şi $\gamma = (i_1, i_2, \ldots, i_n)$. Presupunem că $\gamma \circ \sigma = \sigma \circ \gamma$. Aceasta înseamnaă că $(\gamma \circ \sigma)(i_l) = (\sigma \circ \gamma)(i_l)$ pentru orice $l \in \{1, \ldots, n\}$. Aşadar, notând $i_k = \sigma(i_1)$ şi înlocuind pe l cu 1 obţinem $i_{k+1} = \sigma(i_2)$, dacă $k \leq n-1$ şi $i_1 = \sigma(i_2)$. Luând $l = 2$ primim $i_{k+2} = \sigma(i_3)$ dacă $k+1 \leq n-1$ şi $i_2 = \sigma(i_3)$. Contimuând raţionamentul, conform problemei **2.82**, se obţine $\sigma = \gamma^{k-1}$. Deci σ comută cu γ numai dacă σ este o putere a lui γ. Întrucât puterile lui γ comută cu γ, urmează că elementele din S_n permutabile cu γ coincid cu puterile lui γ.

2.85. Indicaţii. a) Orice permutate (diferită de permutarea identică) se scrie ca un produs de cicluri disjuncte şi orice ciclu se scrie ca un produs de transpoziţii astfel

$$(i_1, i_2, \ldots, i_k) = (i_1, i_k) \circ (i_1, i_{k-1}) \circ \cdots \circ (i_1, i_2).$$

b) Pentru orice $i, j \in \{1, \ldots, n\}$, $i \neq j$ avem $(i, j) = (1, i) \circ (1, j) \circ (1, i)$ (vezi **2.83**).
c) $(1, 2) \circ (2, 3) \circ (1, 2) = (1, 3)$, $(1, 3) \circ (3, 4) \circ (1, 3) = (1, 4)$ ş. a. m. d. (vezi **2.83**).
d) Conform problemei **2.83** avem $(i_1, i_2, \ldots, i_n) \circ (i_1, i_2) \circ (i_n, i_{n-1}, \ldots, i_1) = (i_2, i_3)$, $(i_1, i_2, \ldots, i_n) \circ (i_2, i_3) \circ (i_n, i_{n-1}, \ldots, i_1) = (i_3, i_4)$ ş. a. m. d.
e) Cum $(j_1, j_2, \ldots, j_n) = (j_n, j_1, j_2, \ldots, j_{n-1})$ putem face ca i_1 să apară pe prima poziţie în scrierea ciclului $(j_1, j_2, \ldots, j_n)$, apoi, folosind problema **2.82**, găsim între puterile lui $(j_1, j_2, \ldots, j_n) = (i_1, i_2', \ldots, i_n')$ (cu $\{i_1, i_2', \ldots, i_n'\} = \{1, 2, \ldots, n\}$) un ciclu de forma $(i_1, i_2, i_3'', \ldots, i_n'')$ (cu $\{i_1, i_2, i_3'', \ldots, i_n''\} = \{1, 2, \ldots, n\}$) şi folosim punctul anterior.

2.86. Indicaţii. a) Din punctul a) al problemei anterioare se deduce că toate produsele de câte două transpoziţii generează pe A_n, iar dacă $i, j, k, l \in \{1, \ldots, n\}$ sunt distincte,

$$(i, l) \circ (i, j) = (i, j, l) \text{ şi } (i, j) \circ (k, l) = (i, j) \circ (i, k) \circ (k, i) \circ (k, l) = (i, j, k) \circ (k, l, i).$$

b) Se foloseşte punctul b) al problemei anterioare şi

$$(1, 3) \circ (1, 2) = (1, 2, 3),\ (1, 4) \circ (1, 2) = (1, 2, 4), \ldots, (1, n) \circ (1, 2) = (1, 2, n).$$

2.87. Indicaţii. Matricea unitate I_n are $\det I_n = 1$, iar dacă $A, B \in M_n(K)$ atunci $\det(AB) = \det A \cdot \det B$. Rezultă că dacă $\det A \neq 0$ atunci $\det A^{-1} = (\det A)^{-1}$.
i) Funcţia $f : K \to M_n(K),\ f(x) = xI_n$ este un omomorfism injectiv. $(M_n(K), \cdot)$ nu este grup deoarece matricele cu determinantul nul nu sunt inversabile.
ii) $GL_n(K)$ este parte stabilă în $M_n(K)$ deoarece

$$A, B \in GL_n(K) \Rightarrow \det A \neq 0 \neq \det B \Rightarrow \det(AB) = \det A \cdot \det B \neq 0 \Rightarrow AB \in GL_n(K).$$

Din asociativitatea înmulţirii matricelor rezultă că operaţia indusă de aceasta în $GL_n(K)$ este asociativă, iar din $\det I_n = 1$ rezultă $I_n \in GL_n(K)$. În plus, dacă $A \in GL_n(K)$ atunci $\det A \neq 0$, de unde rezultă că există $A^{-1} \in M_n(K)$ astfel încât $AA^{-1} = I_n = A^{-1}A$. Avem $\det A^{-1} \neq 0$, adică $A^{-1} \in GL_n(K)$ şi astfel $(GL_n(K), \cdot)$ este grup. Acesta este grupul elementelor inversabile ale monoidului $(M_n(K), \cdot)$.
iii) Funcţia $\varphi : K^* \to GL_n(K),\ \varphi(x) = xI_n$ este un omomorfism injectiv.
iv) Funcţia $\psi : \mathbb{C}^* \to GL_n(\mathbb{R}),\ \psi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ este un omomorfism injectiv.
v) Cum $I_n \in SL_n(K)$, avem $SL_n(K) \neq \emptyset$. Dacă $A, B \in SL_n(K)$ atunci $AB \in SL_n(K)$ deoarece $\det(AB) = \det A \cdot \det B = 1$, iar dacă $A \in SL_n(K)$, din $AA^{-1} = I_n$ deducem $\det A^{-1} = \det A^{-1} \cdot \det A = 1$, aşadar $A^{-1} \in SL_n(K)$.

2.88. Evident $\{aI_n \mid a \in K^*\} \subseteq Z(GL_n(K))$. Invers, dacă $A = (a_{ij}) \in Z(GL_n(K))$ atunci, pentru orice $i, j \in \{1, \ldots, n\}$, A comută cu matricea E_{ij} obţinută din I_n prin permutarea liniilor i şi j, iar din $E_{ij} \cdot A = A \cdot E_{ij}$ rezultă $a_{ii} = a_{jj}$ şi $a_{ij} = a_{ji}$. Urmează că A este simetrică şi $a_{11} = a_{22} = \cdots = a_{nn} = a$. Fie $x \in K^* \setminus \{1\}$ şi

$$E_{11}^x = \begin{pmatrix} x & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix},$$

adică matricea obţinută din I_n înlocuind elementul din linia 1 şi coloana 1 cu x. Din $E_{11}^x \in GL_n(K)$ rezultă că $E_{11}^x \cdot A = A \cdot E_{11}^x$, ceea ce implică $a_{1j}x = a_{1j}$ pentru orice $j \in \{2, 3, \ldots, n\}$, de unde rezultă că $a_{12} = a_{13} = \cdots = a_{1n} = 0$. Analog se obţine $a_{21} = a_{23} = \cdots = a_{2n} = 0,\ \ldots,\ a_{n1} = a_{n2} = \cdots = a_{n,n-1} = 0$, deci $A = aI_n$.

2.89. Indicaţie. iii) Dacă $n \in \mathbb{Z}$ atunci $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

2.90. Indicaţie. $AB = -\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

2.91. Fie I_n matricea unitate de tipul (n, n), $E_1, \ldots, E_n$ liniile sale şi $E^1, \ldots, E^n$ coloanele sale. Pentru $\sigma \in S_n$ notăm $\overline{\sigma}(I_n) = \left(E^{\sigma(1)}, E^{\sigma(2)}, \ldots, E^{\sigma(n)}\right)$. Avem

$$\overline{\sigma}(I_n) \in GL_n(\mathbb{Z}) \text{ şi } \overline{\sigma}(I_n) = \begin{pmatrix} E_{\sigma^{-1}(1)} \\ \cdots \\ E_{\sigma^{-1}(n)} \end{pmatrix},$$

iar dacă $\sigma, \tau \in S_n$ atunci

$$\begin{aligned}\overline{\sigma}(I_n)\overline{\tau}(I_n) &= \begin{pmatrix} E_{\sigma^{-1}(1)} \\ \cdots \\ E_{\sigma^{-1}(n)} \end{pmatrix} \left(E^{\tau(1)}, E^{\tau(2)}, \ldots, E^{\tau(n)}\right) \\ &= \begin{pmatrix} E_{\sigma^{-1}(1)}E^{\tau(1)} & \ldots & E_{\sigma^{-1}(1)}E^{\tau(n)} \\ \vdots & & \vdots \\ E_{\sigma^{-1}(n)}E^{\tau(1)} & \ldots & E_{\sigma^{-1}(n)}E^{\tau(n)} \end{pmatrix} = \left(E^{\sigma(\tau(1))}, \ldots, E^{\sigma(\tau(n))}\right) \\ &= \overline{\sigma \circ \tau}(I_n).\end{aligned}$$

Rezultă că funcţia $f : S_n \to GL_n(\mathbb{Z}),\ f(\sigma) = \overline{\sigma}(I_n)$ este un omomorfism injectiv.

2.92. Indicaţie. Se aplică Teorema lui Cayley şi problema anterioară.

2.93. Răspuns. $\operatorname{ord} x = 2$, $\operatorname{ord} y = \infty$, $\operatorname{ord} z = 4$, $\operatorname{ord} u = \operatorname{ord} v = \infty$ şi $\langle x\rangle = \{x, x^2\}$, $\langle y\rangle = \{y^k \mid k \in \mathbb{Z}\}$, $\langle z\rangle = \{z, z^2, z^3, z^4\}$, $\langle u\rangle = \{u^k \mid k \in \mathbb{Z}\}$, $\langle v\rangle = \{v^k \mid k \in \mathbb{Z}\}$.

2.94. Fie $C(X) = C_M X = M \setminus X$ complementara submulţimii $X \subseteq M$. Avem

$$X \triangle Y = [X \cap C(Y)] \cup [Y \cap C(X)]. \tag{1}$$

În stabilirea asociativităţii operaţiei $\triangle$ avem nevoie de egalitatea

$$C(X \triangle Y) = (X \cap Y) \cup [C(X) \cap C(Y)] \tag{2}$$

care se deduce din (1), din formulele lui de Morgan şi din distributivitatea intersecţiei faţă de reuniune astfel:

$$\begin{aligned}C(X \triangle Y) &= C(X \cap C(Y)) \cap C(Y \cap C(X)) = [C(X) \cup Y] \cup [C(Y) \cup X] \\ &= \{[C(X) \cup Y] \cap C(Y)\} \cup \{[C(X) \cup Y] \cap X\} \\ &= [C(X) \cap C(Y)] \cup [Y \cap C(Y)] \cup [C(X) \cup X] \cup [Y \cap X] \\ &= [C(X) \cap C(Y)] \cup \emptyset \cup \emptyset \cup (X \cap Y) = (X \cap Y) \cup [C(X) \cap C(Y)].\end{aligned}$$

Folosind (1) şi (2) avem

$$\begin{aligned}&(X \triangle Y) \triangle Z = [(X + Y) \cap C(Z)] \cup [C(X + Y) \cap Z] \\ &=\{[(X \cap C(Y)) \cup (Y \cap C(X))] \cap C(Z)\} \cup \{[(X \cap Y) \cup (C(X) \cap C(Y))] \cap Z\} \\ &=[X \cap C(Y) \cap C(Z)] \cup [Y \cap C(X) \cap C(Z)] \cup [X \cap Y \cap Z] \cup [C(X) \cap C(Y) \cap Z] \\ &=(X \cap Y \cap Z) \cup [X \cap C(Y) \cap C(Z)] \cup [C(X) \cap Y \cap C(Z)] \cup [C(X) \cap C(Y) \cap Z].\end{aligned}$$

La acelaşi rezultat se ajunge şi calculând pe $X \triangle (Y \triangle Z)$. Deci $\triangle$ este asociativă.

Din definiţia operaţiei $\triangle$ rezultă că $\triangle$ este comutativă, are element neutru submulţimea vidă şi $X \triangle X = \emptyset$, adică opusa lui X este X. Deci $(\mathcal{P}(M), \triangle)$ este grup abelian în care orice element diferit de $\emptyset$ are ordinul 2.

2.95. Indicaţie. Problema **2.95** este o generalizare a problemei **2.94** şi, pentru a o rezolva, se procedează în mod analog: se arată că $(x + y)' = (x \wedge y) \vee (x' \wedge y')$, se stabileşte asocitivitatea lui $+$ demonstrând că

$$(x + y) + z = (x \wedge y' \wedge z') \vee (x' \wedge y \wedge z') \vee (x' \wedge y' \wedge z) \vee (x \wedge y \wedge z) = x + (y + z),$$

se verifică faptul că cel mai mic element 0 este element neutru şi că $x + x = 0$.

2.96. Indicaţie. $\{\{x,-x\} \mid x \in G\}$ este o partiţie a lui G.

2.97. Dacă $\mathrm{ord}(xy) = n \in \mathbb{N}^*$ atunci înmulţind cu y la stânga şi cu y^{-1} la dreapta în egalitatea $x(yx)^{n-1}y = (xy)^n = 1$ avem $(yx)^n = 1$, de unde rezultă că $\mathrm{ord}(yx)$ este finit şi $\mathrm{ord}(yx)$ divide pe $\mathrm{ord}(xy)$. Analog se obţine $\mathrm{ord}(xy) \mid \mathrm{ord}(yx)$, deci $\mathrm{ord}(xy) = \mathrm{ord}(yx)$. Dacă $\mathrm{ord}(xy)$ este infinit şi $\mathrm{ord}(yx)$ ar fi finit, conform celor de mai sus, s-ar obţine o contradicţie.

2.98. Reamintim că pentru orice $k \in \mathbb{Z}$ avem $[f(x)]^k = f(x^k)$. Notăm cu 1 şi $1'$ elementele neutre din G, respectiv din G'.
i) Dacă $\mathrm{ord}\, x = n \in \mathbb{N}^*$ atunci $[f(x)]^n = f(x^n) = f(1) = 1'$, ceea ce implică $\mathrm{ord} f(x) | n$.
ii) Dacă $\mathrm{ord}\, x$ este finit, egal cu $n \in \mathbb{N}^*$, atunci, conform a), $\mathrm{ord} f(x) = m \in \mathbb{N}^*$ şi $m|n$. Avem, de asemenea, $f(1) = 1' = [f(x)]^m = f(x^m)$ de unde, pe baza injectivităţii lui f, deducem $x^m = 1$, adică $n|m$. Deci $m = n$. Dacă $\mathrm{ord}\, x = \infty$ şi $\mathrm{ord} f(x)$ ar fi finit, egal cu $m \in \mathbb{N}^*$ atunci ca mai sus se obţine $x^m = 1$, contradicţie.
iii) dacă $\mathrm{ord} f(x) = \mathrm{ord}\, x$ pentru orice $x \in G$ atunci $f(x) = 1'$ implică $\mathrm{ord}\, x = 1$, adică $x = 1$. Urmează că nucleul lui f este $\{1\}$, deci f este injectiv.

2.99. i) Elementul neutru este singurul element de ordinul 1.
ii) Pentru orice $k \in \mathbb{Z}$ avem $(x^{-1})^k = (x^k)^{-1}$, deci $x^k = 1$ dacă şi numai dacă $(x^{-1})^k = 1$, de unde urmează că $\mathrm{ord}\, x = \mathrm{ord}\, x^{-1}$.
iii) Fie $d = (k,n)$ şi $m = \mathrm{ord}(x^k)$. Avem $n = n'd$ şi $k = k'd$, unde $(k',n') = 1$. Să arătăm că $m = n'$. Din $m = \mathrm{ord}(x^k)$ rezultă că $x^{km} = 1$, iar cum $n = \mathrm{ord}\, x$ deducem că $n|km$, de unde urmează $n'|k'm$. De aici şi din $(k',n') = 1$ avem $n'|m$. Din $k = k'd$, $n = n'd$ şi $n = \mathrm{ord}\, x$ obţinem

$$(x^k)^{n'} = x^{kn'} = x^{k'dn'} = x^{k'n} = (x^n)^{k'} = 1,$$

aşadar $m = \mathrm{ord}(x^k)$ divide pe n'. Cum $m, n' \in \mathbb{N}^*$, $m|n'$ şi $n'|m$ avem $m = n'$.
iv) $\mathrm{ord}(x^k) = \dfrac{n}{(k,n)} = \dfrac{n}{(k,km)} = \dfrac{n}{k} = m.$
v) $G = \langle x^k \rangle \Leftrightarrow \mathrm{ord}(x^k) = n \Leftrightarrow (k,n) = 1.$
vi) Corespondenţa $d \mapsto \left\langle x^{\frac{n}{d}} \right\rangle$ realizează un izomorfism de ordine între laticea $(D_n, |)$ şi laticea subgrupurilor lui $(G, \cdot)$.

Observaţie: Cu notaţiile de mai sus, considerând că c.m.m.d.c. a două numere întregi este număr natural, din ii) şi iii) rezultă că $\mathrm{ord}(x^k) = \dfrac{n}{(k,n)}$ pentru orice $k \in \mathbb{Z}$.

2.100. Fie $a = [m,n]$ şi $d = (m,n)$. Dacă $m = m'd$, $n = n'd$ $(m'n' \in \mathbb{N}^*)$ atunci $a = m'n'd = mn' = m'n$.
i) Din $(xy)^a = x^a \cdot y^a = (x^m)^{n'} \cdot (y^n)^{m'} = 1 \cdot 1 = 1$ rezultă că $\mathrm{ord}(xy)$ este finit şi divide pe a.
ii) Dacă $b = \mathrm{ord}(xy)$ atunci $x^b \cdot y^b = (xy)^b = 1$ implică $x^b = y^{-b}$. Dar $x^b \in \langle x \rangle$ şi $y^{-b} \in \langle y \rangle$, ceea ce arată că $x^b = y^{-b} = 1$. Cum $\mathrm{ord}\, x = m$ şi $\mathrm{ord}\, y = n$ avem $m|b$ şi $n|b$, deci $a|b$, ceea ce împreună cu i) conduce la $\mathrm{ord}(xy) = [m,n]$.
iii) Din Teorema lui Lagrange avem că $|\langle x \rangle \cap \langle y \rangle|$ divide pe $m = |\langle x \rangle|$ şi pe $n = |\langle y \rangle|$, iar cum $(m,n) = 1$, avem $|\langle x \rangle \cap \langle y \rangle| = 1$. În consecinţă, $\langle x \rangle \cap \langle y \rangle = \{1\}$, aşadar

$\mathrm{ord}(xy) = [m,n] = mn$. Evident, $\langle xy\rangle \subseteq \langle x,y\rangle$. Cum $(m,n) = 1$, există $u,v \in \mathbb{Z}$ astfel încât $um + vn = 1$. Deducem că

$$x = x^{um+vn} = (x^m)^u x^{vn} = x^{vn} = x^{vn}(y^n)^v = (xy)^{vn}$$

şi, analog, $y = (xy)^{um}$. Deci $x,y \in \langle xy\rangle$, ceea ce implică $\langle x,y\rangle \subseteq \langle xy\rangle$.
iv) Fie $\{p_1,p_2,\ldots,p_l\}$ mulţimea obţinută reunind mulţimea divizorilor primi ai lui m cu mulţimea divizorilor primi ai lui n. Avem

$$m = p_1^{\alpha_1}\cdots p_l^{\alpha_l},\ n = p_1^{\beta_1}\cdots p_l^{\beta_l},$$

unde $\alpha_i,\beta_i \in \mathbb{N}$ $(i = 1,\ldots,l)$. Putem presupune, fără a restrânge generalitatea, că $\alpha_1 \leq \beta_1,\ \ldots,\ \alpha_k \leq \beta_k,\ \alpha_{k+1} \geq \beta_{k+1},\ \ldots,\ \alpha_l \geq \beta_l$, unde $1 \leq k \leq l$. Atunci

$$a = [m,n] = p_1^{\beta_1}\cdots p_k^{\beta_k}p_{k+1}^{\alpha_{k+1}}\cdots p_l^{\alpha_l},$$

unde numerele $p = p_1^{\beta_1}\cdots p_k^{\beta_k}$, $q = p_{k+1}^{\alpha_{k+1}}\cdots p_l^{\alpha_l}$ sunt relativ prime, iar dacă

$$p' = p_{k+1}^{\beta_{k+1}}\cdots p_l^{\beta_l},\ q' = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$$

atunci $\mathrm{ord}(x^{q'}) = q$ şi $\mathrm{ord}(y^{p'}) = p$ (vezi problema anterioară). Conform punctului ii), elementul $x^{q'}y^{p'} \in G$ are ordinul $pq = a$.

2.101. Indicaţie. Dacă $i,j = 1,\ldots,k$, $i \neq j$ atunci $\langle\gamma_i\rangle \cap \langle\gamma_j\rangle = \{e\}$ şi se aplică ii) din problema anterioară.

2.102. Indicaţie. Vezi problema **2.90** sau dacă $(S_P,\circ)$ este grupul permutărilor planului P şi s_A, s_B sunt simetriile lui P în raport cu două puncte diferite A, respectiv B din P atunci $\mathrm{ord}\, s_A = 2 = \mathrm{ord}\, s_B$ şi $\mathrm{ord}(s_A \circ s_B) = \infty$.

2.103. i) Din problema **2.117** rezultă că $t(G) \neq \emptyset$ $(1 \in t(G))$ şi că $xy \in t(G)$ pentru orice $x,y \in t(G)$. Cum $\mathrm{ord}\, x = \mathrm{ord}\, x^{-1}$ avem şi $x^{-1} \in t(G)$ pentru orice $x \in t(G)$, deci $t(G)$ este subgrup.
ii) Vezi problema **2.102**.
iii) De exemplu, în $(\mathbb{R}^*,\cdot)$ avem $\mathrm{ord}\, 2 = \infty = \mathrm{ord}\left(-\dfrac{1}{2}\right)$, dar $\mathrm{ord}\left(-\dfrac{1}{2}\cdot 2\right) = 2$. Aşadar, $(\mathbb{R}^* \setminus t(\mathbb{R}^*)) \cup \{1\} = \mathbb{R}^* \setminus \{-1\}$ nu este subgrup.
iv) Dacă $h \in H$ atunci, cum $H \subseteq t(G)$, urmează că $n = \mathrm{ord}\, h < \infty$ şi $h^n = 1$. Deci $h^{-1} = h^{n-1} \in H$.
v) Dacă G este finit atunci $t(G) = G$ şi se aplică iii).

2.104. Indicaţii. i) Un izomorfism $f : G \to G'$ induce între părţile de torsiune un izomorfism $f' : t(G) \to t(G')$, $f'(x) = f(x)$; ii) $t(\mathbb{Q}^*,\cdot) = \{-1,1\} = t(\mathbb{R}^*,\cdot)$.

2.105. Indicaţie. Părţile de torsiune nu sunt izomorfe.

2.106. Răspuns. $t(\mathbb{C}^*,\cdot)$.

2.107. Indicaţie. $\mathbb{Z} = \langle 1\rangle$.

2.108. Indicaţii. iii) Se foloseşte faptul că orice subgrup al unui grup ciclic este ciclic sau se poate proceda astfel: dacă $H = \{0\}$ atunci $n = 0$, iar dacă $H \neq \{0\}$ atunci $H \cap \mathbb{N}^* \neq \emptyset$ şi $n = \min(H \cap \mathbb{N}^*)$. Într-adevăr, $n\mathbb{Z} \subseteq H$, iar dacă $h \in H$ atunci, conform teoremei împărţirii cu rest în $\mathbb{Z}$, există $q, r \in \mathbb{Z}$ astfel încât $h = nq + r$ şi $0 \leq r \leq n - 1$. Rezultă că $r \in H \cap \mathbb{N}$ şi pentru a nu contrazice minimalitatea lui n trebuie ca $r = 0$, deci $h \in n\mathbb{Z}$. Unicitatea lui n rezultă din ii) şi antisimetria divizibilităţii în $\mathbb{N}$.
iv) Corespondenţa $n \mapsto n\mathbb{Z}$ realizează un antiizomorfism de ordine (deci şi un antiizomorfism laticial) între laticea $(\mathbb{N}, |)$ şi laticea subgrupurilor lui $(\mathbb{Z}, +)$.
v) Este o consecinţă imediată a lui iv). Se poate proceda şi astfel: dacă $x \in m\mathbb{Z} \cap n\mathbb{Z}$ atunci $m|x$, $n|x$ şi avem $[m,n]|x$, iar dacă $[m,n]|x$ atunci $m|x$ şi $n|x$, şi deducem că $m\mathbb{Z} \cap n\mathbb{Z} = [m,n]\mathbb{Z}$; se verifică $m\mathbb{Z} + n\mathbb{Z} \leq \mathbb{Z}$, prin urmare există $d \in \mathbb{N}$ astfel încât $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ şi $d = (m,n)$ deoarece $d|m$, $d|n$, iar dacă $d' \in \mathbb{N}$ cu $d'|m$ şi $d'|n$ atunci $d' \in m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, deci $d'|d$.
vi) Se foloseşte iii), iv) şi [34, Teorema 2.8.13].
vii) $(\mathbb{N}, |)$ este latice distributivă (vezi problema **1.147**).

2.109. Fie $f : \mathbb{Q} \to \mathbb{Z}$ un omomorfism, $x \in \mathbb{Q}$ arbitrar şi $f(x) = a \in \mathbb{Z}$. Atunci, pentru orice $n \in \mathbb{N}^*$ avem $a = f(x) = f\left(n \cdot \dfrac{x}{n}\right) = n \cdot f\left(\dfrac{x}{n}\right)$, iar cum $f\left(\dfrac{x}{n}\right) \in \mathbb{Z}$, deducem că $a = 0$ (fiind multiplu pentru orice $n \in \mathbb{N}^*$), aşadar $f(x) = 0$ pentru orice $x \in \mathbb{Q}$.

Fie $n \in \mathbb{N}$, $n \geq 2$ şi $g : \mathbb{Z}_n \to \mathbb{Z}$ un omomorfism. Dacă $\widehat{x} \in \mathbb{Z}_n$ şi $g(\widehat{x}) = a \in \mathbb{Z}$ atunci $na = ng(\widehat{x}) = g\left(n\widehat{x}\right) = g\left(\widehat{nx}\right) = g(\widehat{0}) = 0$, iar cum $n \neq 0$, deducem că $a = 0$, deci $g(\widehat{x}) = 0$ pentru orice $\widehat{x} \in \mathbb{Z}_n$.

2.110. Indicaţii. Dacă $n \in \mathbb{N}^*$ atunci corepondenţa $k \mapsto nk$ realizează un izomorfism de la $(\mathbb{Z}, +)$ la $(n\mathbb{Z}, +)$. Cum singurul omomorfism de la $(\mathbb{Q}, +)$ la $(\mathbb{Z}, +)$ este omomorfismul nul, aceste grupuri nu sunt izomorfe.

2.111. Indicaţii. $U_n = \langle \varepsilon_1 \rangle$, unde $\varepsilon_1 = \cos \dfrac{2\pi}{n} + i \sin \dfrac{2\pi}{n}$, iar dacă G este un grup ciclic de ordinul n generat de x atunci funcţia $f : G \to U_n$, $f(x^k) = \varepsilon_1^k$ este un izomorfism.

2.112. Indicaţii. Vezi problema **2.99**, vi) şi problema **2.108**, vii).

2.113. Indicaţie. Fie $(G, \cdot)$ un grup infinit. Dacă G are un element de ordin infinit atunci $\langle x \rangle \simeq (\mathbb{Z}, +)$ şi din problema **2.108** rezultă că G are o infinitate de subgrupuri. Dacă toate elementele lui G au ordinele finite şi mulţimea subgrupurilor ciclice ale lui G ar fi formată numai din $H_1, \ldots, H_n$ atunci $G = H_1 \cup H_2 \cup \cdots \cup H_n$, de unde ar urma că G este finit.

2.114. Răspuns. i) Grupurile cu câte un singur element. ii) Grupurile de ordinul p, cu p număr prim.

2.115. Răspuns. Grupurile cu torsiune.

2.116. Indicaţii. i) Grupurile cât ale lui $(\mathbb{Z}, +)$ sunt $(\mathbb{Z}/n\mathbb{Z}, +)$, cu $n \in \mathbb{N}$. Dacă $n = 0$ atunci $\mathbb{Z}/\{0\} = \{\{k\} \mid k \in \mathbb{Z}\} \simeq \mathbb{Z}$. Dacă $n \in \mathbb{N}^*$ atunci $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, unde $\overline{i} = i + n\mathbb{Z}$. Operaţia din grupul cât este definită de egalitatea $\overline{i} + \overline{j} = \overline{i+j}$ şi avem $\mathbb{Z}_n = \langle \overline{1} \rangle$. ii) $(\mathbb{Z}_n, +) \simeq (U_n, \cdot)$ pentru orice $n \in \mathbb{N}^*$.

2.117. Indicaţie. Cum orice grup ciclic este izomorf cu $(\mathbb{Z},+)$ sau cu $(\mathbb{Z}_n,+)$, $n\in\mathbb{N}^*$, este suficient să demonsrăm următoarele:
a) $(\mathbb{Z}\times\mathbb{Z},+)$ *nu este ciclic.* Într-adevăr, dacă $(a,b)\in\mathbb{Z}$ şi $a\neq b$ atunci subgrupul $\langle(a,b)\rangle$ nu conţine perechile (m,m), cu $m\in\mathbb{Z}$, iar dacă $a=b$ atunci subgrupul $\langle(a,b)\rangle$ nu conţine perechile $(m,n)\in\mathbb{Z}\times\mathbb{Z}$, cu $m\neq n$. Deci pentru orice $a,b\in\mathbb{Z}$, subgrupul $\langle(a,b)\rangle$ este diferit de $\mathbb{Z}\times\mathbb{Z}$.
b) $(\mathbb{Z}\times\mathbb{Z}_n,+)$, *cu* $n\in\mathbb{N}^*$, *nu este ciclic* deoarece este infinit şi are elemente nenule de ordin finit.
b') $(\mathbb{Z}_n\times\mathbb{Z},+)$, *cu* $n\in\mathbb{N}^*$, *nu este ciclic.*
c) $(\mathbb{Z}_m\times\mathbb{Z}_n,+)$, *cu* $(m,n)=d>1$, *nu este ciclic* deoarece ordinul fiecărui element din acest grup nu depăşeşte pe $\dfrac{mn}{d}$ (vezi problema **2.100**) şi $\dfrac{mn}{d}<mn$.
d) $(\mathbb{Z}_m\times\mathbb{Z}_n,+)$, *cu* $(m,n)=1$, *este ciclic* deoarece elementul $(\overline{1},\widehat{1})=(\overline{1},\widehat{0})+(\overline{0},\widehat{1})$ are ordinul mn.

2.118. Indicaţie. Se foloseşte problema anterioară şi se face o inducţie după n.

2.119. Indicaţie. Se foloseşte problema anterioară.

2.120. Cum produsul direct este un grup infinit, ca să fie ciclic ar trebui să fie izomorf cu $(\mathbb{Z},+)$. Atunci orice subgrup nenul al său ar fi ciclic infinit, deci şi grupurile din familia dată ar fi infinite, ele fiind izomorfe cu subgrupuri ale produsului direct. Urmează că produsul direct are un subgrup ciclic izomorf cu $(\mathbb{Z}\times\mathbb{Z},+)$ contradicţie cu a) din soluţia problemei **2.117**.

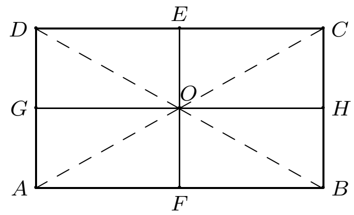
2.121. Presupunem că există un grup de ordinul 4 neciclic $(G,\cdot)$. Fie $G=\{e,a,b,c\}$ şi e elementul neutru. Din ipoteza că G nu este ciclic urmează că nici un element din G nu are ordinul 4. Întrucât e este singurul element de ordinul 1 şi ordinul fiecărui element divide ordinul grupului, rezultă $\operatorname{ord} a=\operatorname{ord} b=\operatorname{ord} c=2$. Deci $a^2=b^2=c^2=e$ şi putem completa în tabla de operaţie a lui $(G,\cdot)$ linia şi coloana lui e, precum şi diagonala care conţine pătratele elementelor din G.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Întrucât translaţiile unui grup sunt bijecţii, rezultă că în tabla de operaţie, atât pe fiecare linie cât şi pe fiecare coloană figurează toate elementel lui G, fără repetiţii. Această constatare ne permite să completăm toate locurile din tabla de operaţie într-un singur mod, ca mai sus. Astfel, s-a demonstrat că există cel mult un grup de ordinul 4 neciclic. Pentru a demonstra existenţa acestui grup putem proceda astfel:
i) Arătăm că G este un grup în raport cu operaţia definită în tabelul de mai sus.
ii) Găsim un exemplu de grup neciclic de ordinul 4.

Prima cale duce la complicaţii când se demonstrează asociativitatea operaţiei. De aceea vom urma calea a doua. În acest scop considerăm un dreptunghi $ABCD$, care nu este pătrat, E mijlocul laturii $[CD]$, F mijlocul lui $[AB]$, G mijlocul lui

$[AD]$ şi H mijlocul lui $[BC]$.



Fie următoarele funcţii bijective ale acestui dreptunghi pe el însuşi: σ_1 = funcţia identică, σ_2 = simetria în raport cu EF, σ_3 = simetria în raport cu GH, σ_4 = simetria în raport cu $O = AC \cap BD$. Fiecare dintre aceste funcţii este determinată de imaginile vârfurilor A, B, C, D prin ea. Dea aceea putem face următoarele identificări:

$$\sigma_1 = \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}, \sigma_2 = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}, \sigma_3 = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix},$$
$$\sigma_4 = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}.$$

Arătăm că mulţimea $K = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ formează un grup împreună cu compunerea funcţiilor. În acest scop întocmim tabelul

$\circ$	σ_1	σ_2	σ_3	σ_4
σ_1	σ_1	σ_2	σ_3	σ_4
σ_2	σ_2	σ_1	σ_4	σ_3
σ_3	σ_3	σ_4	σ_1	σ_2
σ_4	σ_4	σ_3	σ_2	σ_1

Din tabel deducem că mulţimea K este o parte stabilă în monoidul funcţiilor dreptunghiului în el însuşi şi că unitatea acestui monoid aparţine lui K. Deci $(K, \circ)$ este un monoid. Din tabel rezultă că $\sigma_1^{-1} = \sigma_1$, $\sigma_2^{-1} = \sigma_2$, $\sigma_3^{-1} = \sigma_3$, $\sigma_4^{-1} = \sigma_4$. Astfel s-a arătat că $(K, \circ)$ este un grup. Tot din tabel deducem că $\operatorname{ord} \sigma_1 = 1$ şi $\operatorname{ord} \sigma_2 = \operatorname{ord} \sigma_3 = \operatorname{ord} \sigma_4 = 2$. Deci grupul $(K, \circ)$ nu este ciclic, dar din tabel se vede că este comutativ.

2.122. Dacă $G = \{e\}$ este o mulţime cu un singur element atunci pe G se poate defini o singură operaţie binară $*$ dată de egalitatea $e * e = e$ şi $(G, *)$ este un grup. Rezultă că, abstracţie făcând de un izomorfism, există un singur grup de ordinul 1. Dacă G este un grup de ordinul 2, respectiv 3,5, rezultă din [34, Teorema 2.7.10] că G este izomorf cu U_2, respectiv cu U_3, U_5. Dacă G este un grup de ordinul 4 atunci distingem două cazuri: a) G este ciclic şi atunci $G \simeq U_4$; b) G nu este ciclic şi atunci G este izomorf cu grupul $(K, \circ)$ din problema anterioară. Prin urmare, abstracţie făcând de un izomorfism, există două grupuri de ordinul 4: grupul rădăcinilor de ordinul 4 ale unităţii şi grupul lui Klein.

2.123. Indicaţie. Dacă $x \in \mathbb{N}^*$, $f(x) = f(\underbrace{1 + 1 + \cdots + 1}_{x \text{ termeni}}) = xf(1)$ şi $f(-x) = -f(x)$.

2.124. Indicaţie. Dacă f este un endomorfism al grupului $(\mathbb{Q},+)$ şi $m,n \in \mathbb{N}^*$ atunci $f\left(\dfrac{m}{n}\right) = f\Bigg(\underbrace{\dfrac{1}{n}+\cdots+\dfrac{1}{n}}_{m \text{ termeni}}\Bigg) = mf\left(\dfrac{1}{n}\right)$. Rezultă că $f(1) = f\left(\dfrac{n}{n}\right) = nf\left(\dfrac{1}{n}\right)$, deci $f\left(\dfrac{1}{n}\right) = \dfrac{1}{n}f(1)$, $f\left(\dfrac{m}{n}\right) = \dfrac{m}{n}f(1)$, iar $f\left(-\dfrac{m}{n}\right) = -f\left(\dfrac{m}{n}\right)$.

2.125. Indicaţie. Un omomorfism f de la $(\mathbb{Z},+)$ la $(G,+)$ este determinat de $f(1)$. Funcţia $\varphi : Hom(\mathbb{Z},G) \to G$, $\varphi(f) = f(1)$ este un izomorfism de grupuri.

2.126. Indicaţie. Un omomorfism $f : \mathbb{Z}_6 \to \mathbb{Z}_3$ este determinat de $f(\overline{1})$ şi $f(\overline{1}) = \widehat{a}$ dacă şi numai daxcă $6\widehat{a} = \widehat{0}$. Deci $\widehat{a}$ poate fi orice element din $\mathbb{Z}_3$. Rezultă că există 3 omomorfisme de la $\mathbb{Z}_6$ în $\mathbb{Z}_3$. Analog se deduce că există 3 omomorfisme ale lui $\mathbb{Z}_3$ în $\mathbb{Z}_9$.

2.127. Indicaţie. Fie $x \in \mathbb{Z}$. Notăm cu $\overline{x}$, respectiv $\widehat{x}$ clasa lui x în $\mathbb{Z}_m$, respectiv $\mathbb{Z}_n$. Dacă $f : \mathbb{Z}_m \to \mathbb{Z}_n$ este un omomorfism atunci f este determinat de $f(\overline{1}) \in \mathbb{Z}_n$ şi $mf(\overline{1}) = f(\overline{m}) = f(\overline{0}) = \widehat{0}$ şi $nf(\overline{1}) = \widehat{0}$. Prin urmare, dacă $d = (m,n)$ şi $n = kd$ atunci $d\,f(\overline{1}) = \widehat{0}$ deoarece există $u,v \in \mathbb{Z}$ astfel încât $um + vn = d$. Rezultă că reprezentanţii lui $f(\overline{1})$ sunt multipli de k, adică $f(\overline{1}) \in k\mathbb{Z}_n$. Dacă $\widehat{a} \in k\mathbb{Z}_n$ atunci funcţia $f : \mathbb{Z}_m \to \mathbb{Z}_n$, $f(\overline{x}) = \widehat{xa}$ este un omomorfism. Funcţia $\varphi : Hom(\mathbb{Z}_m,\mathbb{Z}_n) \to k\mathbb{Z}_n$, $\varphi(f) = f(\overline{1})$ este un izomorfism, iar $k\mathbb{Z}_n = \left\langle \widehat{k} \right\rangle$ şi ordinul lui $\widehat{k}$ este d. Deci $k\mathbb{Z}_n \simeq \mathbb{Z}_d$.

2.128. Indicaţie. Cum $f(G) = f(\langle a\rangle) = \langle f(a)\rangle$, omomorfismul f este surjectiv dacă şi numai dacă $G = \langle f(a)\rangle$.

2.129. Indicaţii. i) Singurele automorfisme ale lui $(\mathbb{Z},+)$ sunt $1_{\mathbb{Z}}$ şi $-1_{\mathbb{Z}}$ (vezi problema **2.123**).
ii) $(\mathbb{Z}_5,+)$ este generat de orice $\overline{x} \in \mathbb{Z}_5^* = \mathbb{Z}_5 \setminus \{\overline{0}\}$. Din problema anterioară rezultă că automorfismele lui $\mathbb{Z}_5$ sunt date de următoarele egalităţi:

$$f_1(\overline{x}) = \overline{x},\ f_2(\overline{x}) = 2\overline{x},\ f_3(\overline{x}) = 3\overline{x},\ f_4(\overline{x}) = 4\overline{x},$$

şi că $Aut(\mathbb{Z}_5,+) = \langle f_2\rangle \simeq \mathbb{Z}_4$.
iii) $(\mathbb{Z}_6,+)$ are numai doi generatori: pe $\overline{1}$ şi pe $\overline{5}$. Automorfismele lui $\mathbb{Z}_6$ sunt date de egalităţile $f_1(\overline{x}) = \overline{x}$ şi $f_2(\overline{x}) = 5\overline{x}$.

2.130. Indicaţii. Dacă $s \in S$, $h,h' \in H$ atunci avem: i) $f(f(sh)) = f(s) = s = f(sh)$; ii) $(sh)^{-1}f(sh) = h^{-1}s^{-1}s = h^{-1} \in H$; iii) $f((sh')h) = f(s(h'h)) = s = f(sh)$.

2.131. Indicaţie. Din ii) rezultă că o clasă $xH \in G/\rho_H$ are ca reprezentant pe $f(x)$, deci $\bigcup\limits_{x\in G} f(x)H = G$, iar din i) şi iii) se deduce că elemente diferite din $f(G)$ determină clase diferite în G/ρ_H.

2.132. Fie H subgrup în G, $A = aH$ şi $x,y,z \in A$. Atunci există $h_1,h_2,h_3 \in H$ astfel încât $x = ah_1$, $y = ah_2$, $z = ah_3$, deci $xy^{-1}z = ah_1h_2^{-1}h_3 \in aH = A$. Invers, dacă A verifică condiţia din enunţ şi fixăm un element $a \in A$, iar H este mulţimea soluţiilor ecuaţiilor $ax = b$, cu $b \in A$, atunci H este subgrup al lui G. Într-adevăr, $1 \in H$, iar dacă $ax_1 = b_1$ şi $ax_2 = b_2$, cu $b_1,b_2 \in A$, atunci $x_2 = a^{-1}b_2$, $a(x_1x_2^{-1}) = b_1(a^{-1}b_2)^{-1} = b_1b_2^{-1}a$ şi $b_1b_2^{-1}a \in A$, deci $x_1x_2^{-1} \in H$. Este evident că $A = aH$. Analog se procedează în cazul claselor la dreapta.

2.133. Indicaţii. Din teorema de caracterizare a subgrupului se deduce uşor că

$$H \leq G \Leftrightarrow H \neq \emptyset,\ H \cdot H = H,\ H^{-1} = H.$$

i) Dacă $H_1H_2 \leq G$ atunci $H_1H_2 = (H_1H_2)^{-1} = (H_2)^{-1}(H_1)^{-1} = H_2H_1$, iar dacă are loc egalitatea $H_1H_2 = H_2H_1$ atunci $(H_1H_2)(H_1H_2) = (H_1H_1)(H_2H_2) = H_1H_2$ şi $(H_1H_2)^{-1} = (H_2)^{-1}(H_1)^{-1} = H_2H_1 = H_1H_2$.
ii) $H_1, H_2 \subseteq H_1H_2$, iar dacă $H \leq G$ cu $H_1, H_2 \subseteq H$ atunci $H_1H_2 \subseteq H \cdot H = H$.
iii) Dacă $g \in G$, $h_1 \in H_1$ şi $h_2 \in H_2$ atunci $g^{-1}(h_1h_2)g = (g^{-1}h_1g)(g^{-1}h_2g) \in H_1H_2$.

2.134. Indicaţii. i) Din condiţia din enunţ se deduce că orice două produse finite de elemente din $X \cup X^{-1}$ comută.
ii) Se foloseşte i) şi faptul că pentru orice $n \in \mathbb{N}^*$ şi $x_1, \ldots, x_n \in X$ avem

$$g^{-1}(x_1x_2 \cdots x_n)g = (g^{-1}x_1g)(g^{-1}x_2g) \cdots (g^{-1}x_ng).$$

iii) Condiţia din enunţ conduce la faptul că orice element din subgrupul $\langle X_1 \rangle$ comută cu orice element din subgrupul $\langle X_2 \rangle$, de unde urmează $\langle X_1 \rangle \langle X_2 \rangle = \langle X_2 \rangle \langle X_1 \rangle$, deci, conform problemei anterioare, punctul ii), avem $\langle X_1 \rangle \langle X_2 \rangle = \langle \langle X_1 \rangle \cup \langle X_2 \rangle \rangle = \langle X_1 \cup X_2 \rangle$.
iv) Dacă $X_1X_2 = X_2X_1$ atunci $\langle X_1 \rangle \langle X_2 \rangle = \langle X_2 \rangle \langle X_1 \rangle$ şi se continuă ca la punctul iii).

2.135. Indicaţie. i) Elementul neutru al lui G este $(0,0,1)$, inversul lui $(m_1, m_2, 1)$ este $(-m_1, -m_2, 1)$, iar inversul lui $(m_1, m_2, -1)$ este $(-m_1, -m_2, -1)$.
ii) Conform punctului ii) al problemei anterioare, $H_1 \trianglelefteq G$.
iii) Din $(1,0,1) \cdot (0,1,1) = (0,1,1) \cdot (1,0,1)$ rezultă că grupul H_1 este comutativ, aşadar $H_2 \trianglelefteq H_1$. Însă H_2 nu este normal în G, deoarece $H_2 = \mathbb{Z} \times \{0\} \times \{1\}$ şi

$$(1,0,1)^{-1} \cdot (1,0,1) \cdot (1,0,-1) = (0,1,-1) \notin H_2.$$

Observaţie: Din punctul iii) al problemei anterioare se deduce că relaţia $\trianglelefteq$ (pe mulţimea subgrupurilor normale ale unui grup) nu este, în general, tranzitivă.

2.136. i) $S_3 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$, unde σ_1 este permutarea identică, $\sigma_2 = (2,3)$, $\sigma_3 = (1,2)$, $\sigma_4 = (1,3)$, $\sigma_5 = (1,2,3)$, $\sigma_6 = (1,3,2)$. Tabla compunerii în S_3 este

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_6	σ_5	σ_4	σ_3
σ_3	σ_3	σ_5	σ_1	σ_6	σ_2	σ_4
σ_4	σ_4	σ_6	σ_5	σ_1	σ_3	σ_2
σ_5	σ_5	σ_3	σ_4	σ_2	σ_6	σ_1
σ_6	σ_6	σ_4	σ_2	σ_3	σ_1	σ_5

Rezultă că σ_1 este elementul neutru,

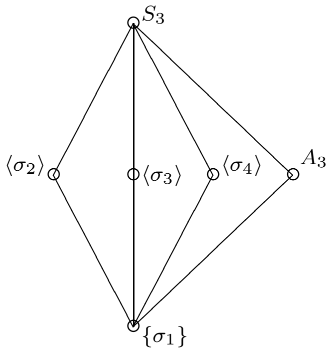
$$\sigma_2^2 = \sigma_3^2 = \sigma_4^2 = \sigma_1,\ \sigma_5^2 = \sigma_6,\ \sigma_5^3 = \sigma_6 \circ \sigma_5 = \sigma_1,\ \sigma_6^2 = \sigma_5,\ \sigma_6^3 = \sigma_5 \circ \sigma_6 = \sigma_1.$$

Aşadar, σ_1 are ordinul 1, $\sigma_2, \sigma_3, \sigma_4$ au ordinul 2, iar σ_5, σ_6 au ordinul 3. Menţionăm că acest fapt rezultă şi din punctul b) al problemei **2.82**.
ii) Subgrupurile improprii ale lui S_3 sunt $\{\sigma_1\}$ şi S_3. Din teorema lui Lagrange urmează că ordinul unui subgrup divide ordinul grupului. Întrucât $|S_3| = 3! = 6$, rezultă că un subgrup propriu poate avea ordinul 2 sau 3. Deducem că subgrupurile

proprii sunt ciclice şi că subgrupurile de ordinul 2 sunt generate de elementele de ordinul 2, iar cele de ordinul 3 sunt generate elemente de ordinul 3. Deci S_3 are următoarele subgrupuri proprii:

$$\langle\sigma_2\rangle = \{\sigma_1, \sigma_2\},\ \langle\sigma_3\rangle = \{\sigma_1, \sigma_3\},\ \langle\sigma_4\rangle = \{\sigma_1, \sigma_4\},\ \langle\sigma_5\rangle = \{\sigma_1, \sigma_5, \sigma_6\} = \langle\sigma_6\rangle = A_3.$$

Diagrama laticii subgrupurilor lui S_3 este



deci această latice este modulară deoarece nu conţine nici o sublatice izomorfă cu pentagonul, dar nu este distributivă deoarece are sublatici izomorfe cu diamantul.
iii) Subgrupurile improprii ale oricărui grup sunt normale. Subgrupul altern este un subgrup de indice 2, deci este normal. Notăm $H_1 = \langle\sigma_2\rangle$, $H_2 = \langle\sigma_3\rangle$, $H_3 = \langle\sigma_4\rangle$ şi cu ρ_i, respectiv ρ_i' echivalenţa la stânga, respectiv la dreapta definită de H_i $(i = 1, 2, 3)$. Avem

$$S_3/\rho_1 = \{\{\sigma_1, \sigma_2\}, \{\sigma_3, \sigma_5\}, \{\sigma_4, \sigma_6\}\},\ S_3/\rho_1' = \{\{\sigma_1, \sigma_2\}, \{\sigma_3, \sigma_6\}, \{\sigma_4, \sigma_5\}\},$$

deoarece

$$\begin{aligned} &\sigma_3 \circ \{\sigma_1, \sigma_2\} = \{\sigma_3, \sigma_5\},\ \sigma_4 \circ \{\sigma_1, \sigma_2\} = \{\sigma_4, \sigma_6\},\\ &\{\sigma_1, \sigma_2\} \circ \sigma_3 = \{\sigma_3, \sigma_6\},\ \{\sigma_1, \sigma_2\} \circ \sigma_4 = \{\sigma_4, \sigma_5\}. \end{aligned}$$

Rezultă că subgrupul H_1 nu este normal. Analog se obţine

$$\begin{aligned} S_3/\rho_2 &= \{\{\sigma_1, \sigma_3\}, \{\sigma_2, \sigma_6\}, \{\sigma_4, \sigma_5\}\},\ S_3/\rho_2' = \{\{\sigma_1, \sigma_3\}, \{\sigma_2, \sigma_5\}, \{\sigma_4, \sigma_6\}\},\\ S_3/\rho_3 &= \{\{\sigma_1, \sigma_4\}, \{\sigma_2, \sigma_5\}, \{\sigma_3, \sigma_6\}\},\ S_3/\rho_3' = \{\{\sigma_1, \sigma_4\}, \{\sigma_2, \sigma_6\}, \{\sigma_3, \sigma_5\}\}, \end{aligned}$$

deci nici subgrupurile H_2 şi H_3 nu sunt normale. În concluzie, subgrupurile normale sunt $\{\sigma_1\}$, A_3 şi S_3.
iv) Din iii) rezultă că S_3 are trei grupuri cât. Acestea au ca mulţimi suport pe

$$S_3/\{\sigma_1\} = \{\{\sigma_1\}, \{\sigma_2\}, \{\sigma_3\}, \{\sigma_4\}, \{\sigma_5\}, \{\sigma_6\}\},\ S_3/S_3 = \{S_3\},\ S_3/A_3 = \{A_3, \sigma_2 \circ A_3\},$$

iar operaţiile sunt definite astfel:

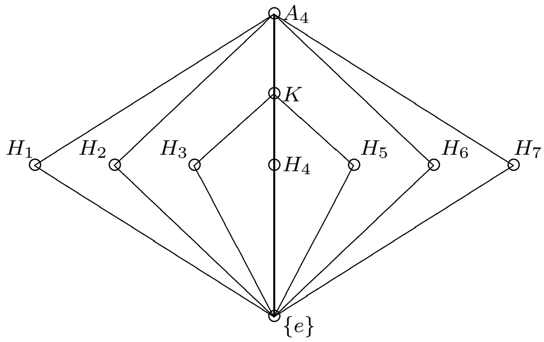
$\circ$	$\{\sigma_1\}$	$\{\sigma_2\}$	$\{\sigma_3\}$	$\{\sigma_4\}$	$\{\sigma_5\}$	$\{\sigma_6\}$
$\{\sigma_1\}$	$\{\sigma_1\}$	$\{\sigma_2\}$	$\{\sigma_3\}$	$\{\sigma_4\}$	$\{\sigma_5\}$	$\{\sigma_6\}$
$\{\sigma_2\}$	$\{\sigma_2\}$	$\{\sigma_1\}$	$\{\sigma_6\}$	$\{\sigma_5\}$	$\{\sigma_4\}$	$\{\sigma_3\}$
$\{\sigma_3\}$	$\{\sigma_3\}$	$\{\sigma_5\}$	$\{\sigma_1\}$	$\{\sigma_6\}$	$\{\sigma_2\}$	$\{\sigma_4\}$
$\{\sigma_4\}$	$\{\sigma_4\}$	$\{\sigma_6\}$	$\{\sigma_5\}$	$\{\sigma_1\}$	$\{\sigma_3\}$	$\{\sigma_2\}$
$\{\sigma_5\}$	$\{\sigma_5\}$	$\{\sigma_3\}$	$\{\sigma_4\}$	$\{\sigma_2\}$	$\{\sigma_6\}$	$\{\sigma_1\}$
$\{\sigma_6\}$	$\{\sigma_6\}$	$\{\sigma_4\}$	$\{\sigma_2\}$	$\{\sigma_3\}$	$\{\sigma_1\}$	$\{\sigma_5\}$

$\circ$	S_3
S_3	S_3

$\circ$	A_3	$\sigma_2 \circ A_3$
A_3	A_3	$\sigma_2 \circ A_3$
$\sigma_2 \circ A_3$	$\sigma_2 \circ A_3$	A_3

Deci grupul $S_3/\{\sigma_1\}$ este izomorf cu S_3 şi grupul S_3/A_3 este izomorf cu $\mathbb{Z}_2$.

2.137. Indicaţii. $A_4 = \{e, (1,2,3), (1,3,2), (1,2,4), (1,4,2), (1,3,4), (1,4,3), (2,3,4), (2,4,3), (1,2) \circ (3,4), (1,3) \circ (2,4), (1,4) \circ (2,3)\}$, iar laticea subgrupurilor lui A_4 este



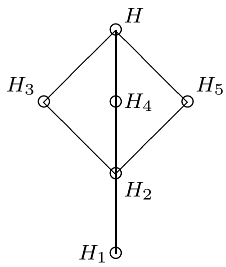
unde $H_1 = \{e, (1,2,3), (1,3,2)\}$, $H_2 = \{e, (1,2,4), (1,4,2)\}$, $H_3 = \{e, (1,2) \circ (3,4)\}$, $H_4 = \{e, (1,3) \circ (2,4)\}$, $H_5 = \{e, (1,4) \circ (2,3)\}$, $H_6 = \{e, (1,3,4), (1,4,3)\}$, $H_7 = \{e, (2,3,4), (2,4,3)\}$ şi $K = \{e, (1,2) \circ (3,4), (1,3) \circ (2,4), (1,4) \circ (2,3)\}$. Laticea aceasta nu este modulară deoarece $\{e, H_3, H_6, K, A_4\}$ este o sublatice a sa izomorfă cu pentagonul.

2.138. Indicaţie. ii) Dacă $N \trianglelefteq G$ atunci partiţia determinată pe G de $\rho_{H,N}$ coincide cu partiţia determinată pe G de relaţia de echivalenţă la stânga definită de HN.

2.139. Răspuns. $S_3/\rho_{H,N} = \{\{\sigma_1, (1,2)\}, \{(1,3), (2,3), (1,3,2), (1,2,3)\}\}$.

2.140. i) Avem $H = \{-1, 1, -i, i, -j, j, -k, k\}$, $\text{ord}(1) = 1$, $\text{ord}(-1) = 2$ şi $\text{ord}(i) = \text{ord}(-i) = \text{ord}(j) = \text{ord}(-j) = \text{ord}(k) = \text{ord}(-k) = 4$. Aşadar, subgrupurile ciclice ale grupului H sunt $H_1 = \langle 1 \rangle = \{1\}$, $H_2 = \langle -1 \rangle = \{-1, 1\}$, $H_3 = \langle i \rangle = \{-1, 1, -i, i\} = \langle -i \rangle$, $H_4 = \langle j \rangle = \{-1, 1, -j, j\} = \langle -j \rangle$ şi $H_5 = \langle k \rangle = \{-1, 1, -k, k\} = \langle -k \rangle$. Din teorema lui Lagrange rezultă că ordinul unui subgrup al lui H poate fi 1, 2, 4 sau 8. Orice subgrup conţine elementul neutru, deci singurul subgrup de ordinul 1 este H_1. Întrucât orice subgrup de ordinul 2 este ciclic, urmează că singurul subgrup de ordinul 2 este H_2. Cum grupul H nu are trei elemente de ordinul 2, rezultă că nu are subgrupuri de ordinu 4 neciclice (vezi soluţia problemei **2.122**). Deci subgrupurile de ordinul 4 sunt H_3, H_4 şi H_5. Astfel am arătat că mulţimea subgrupurilor lui H este $\{H_1, H_2, H_3, H_4, H_5, H\}$. Subgrupurile H_1 şi H sunt normale, deoarece subgrupurile improprii ale oricărui grup sunt normale. Elementele lui H_2 comută cu toate elementele lui H (H_2 coincide cu centrul lui H), de unde deducem că H_2 este normal. Conform teoremei lui Lagrange avem $|H : H_3| = |H : H_4| = |H : H_5| = 2$, iar cum orice subgrup de indice 2 este normal, urmează că H_3, H_4 şi H_5 sunt normale. Aşadar, grupul $(H, \cdot)$ este hamiltonian.

ii) Laticea subgrupurilor (normale ale) lui H este



Această latice este modulară deoarece nu are sublatici izomorfe cu pentagonul şi nu este distributivă doarece are o sublatice izomorfă cu diamantul.
iii) Cum $x^2, y^2 \in \{-1, 1\}$ avem $x^2y^2 = y^2x^2$.
iv) Subgrupurile lui H fiind normale, avem

$$\langle a, b\rangle = \langle a\rangle \cdot \langle b\rangle = \{1, a, a^2, a^3\} \cdot \{1, b, b^2, b^3\}.$$

Întrucât $a^2 = -1 = b^2$ şi $ab \in \{-c, c\}$ unde $c \in \{i, j, k\}\setminus\{a, b\}$, rezultă că $\langle a, b\rangle = H$. Am văzut la punctul i) că $\operatorname{ord} a = \operatorname{ord} b = 4$. Deci $a^4 = 1 = b^4$. Celelalte egalităţi se verifică prin calcul.

2.141. Reamintim că în laticea subgrupurilor normale ale unui grup $(G, \cdot)$ avem $N_1 \wedge N_2 = N_1 \cap N_2$ şi $N_1 \vee N_2 = N_1 \cdot N_2$ pentru orice subgrupuri normale N_1, N_2. Modularitatea acestei latici revine la a arăta că

$$N_1, N_2, N_3 \trianglelefteq G,\ N_1 \subseteq N_3 \Rightarrow N_1 \cdot (N_2 \cap N_3) = (N_1 \cdot N_2) \cap N_3.$$

Cum $N_1 \subseteq N_1 \cdot N_2$ şi $N_1 \subseteq N_3$ avem $N_1 \subseteq (N_1 \cdot N_2) \cap N_3$, iar din incluziunile $N_2 \cap N_3 \subseteq N_2 \subseteq N_1 \cdot N_2$ şi $N_2 \cap N_3 \subseteq N_3$ deducem $N_2 \cap N_3 \subseteq (N_1 \cdot N_2) \cap N_3$. Astfel se obţine implicaţia

$$(*) \qquad N_1 \subseteq N_3 \Rightarrow N_1 \cdot (N_2 \cap N_3) \subseteq (N_1 \cdot N_2) \cap N_3,$$

adevărată în orice latice şi numită proprietatea de submodularitate. Incluziunea inversă din concluzia lui $(*)$ se obţine astfel: dacă $n_3 \in (N_1 \cdot N_2) \cap N_3$ atunci $n_3 \in N_3$ şi există $n_1 \in N_1$, $n_2 \in N_2$ astfel încât $n_3 = n_1 \cdot n_2$. În ipoteza $N_1 \subseteq N_3$ se deduce că $n_2 = n_1^{-1} \cdot n_3 \in N_1^{-1} \cdot N_3 \subseteq N_3^{-1} \cdot N_3 \subseteq N_3$. Aşadar, $n_2 \in N_2 \cap N_3$ şi, prin urmare, $n_3 = n_1 \cdot n_2 \in N_1 \cdot (N_2 \cap N_3)$.

2.142. Indicaţie. Dacă $G/Z(G)$ ar fi ciclic atunci ar exista un element $a \in G$ astfel încât $G = \bigcup\limits_{k\in\mathbb{Z}} a^k Z(G)$, de unde ar urma că grupul $(G, \cdot)$ este comutativ.

2.143. Indicaţii. a) Pentru determinarea subgrupurilor lui $\mathbb{Z}_{12}$ se poate folosi fie faptul că subgrupurile unui grup ciclic sunt ciclice, fie din faptul că subgrupurile grupului cât $\mathbb{Z}_{12} = \mathbb{Z}/12\mathbb{Z}$ sunt de forma $H/12\mathbb{Z}$, unde $H \leq (\mathbb{Z}, +)$ cu $12\mathbb{Z} \subseteq H$. Conform problemei **2.108** rezultă că $H = n\mathbb{Z}$ cu $n \in \mathbb{N}$ şi $n|12$. Deducem că $n \in \{1, 2, 3, 4, 6, 12\}$, deci subgrupurile lui $\mathbb{Z}_{12}$ sunt:

$$H_1 = 1\mathbb{Z}/12\mathbb{Z} = \mathbb{Z}_{12},\ H_2 = 2\mathbb{Z}/12\mathbb{Z} = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\},\ H_3 = 3\mathbb{Z}/12\mathbb{Z} = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\},$$
$$H_4 = 4\mathbb{Z}/12\mathbb{Z} = \{\overline{0}, \overline{4}, \overline{8}\},\ H_5 = 6\mathbb{Z}/12\mathbb{Z} = \{\overline{0}, \overline{6}\},\ H_6 = 12\mathbb{Z}/12\mathbb{Z} = \{\overline{0}\}.$$

Mulţimile suport ale grupurilor cât sunt:

$$\mathbb{Z}_{12}/H_1 = \{\mathbb{Z}_{12}\},\ \mathbb{Z}_{12}/H_2 = \{H_2, \overline{1} + H_2\},\ \mathbb{Z}_{12}/H_3 = \{H_3, \overline{1} + H_3, \overline{2} + H_3\},$$

$$\mathbb{Z}_{12}/H_4 = \{H_4, \overline{1}+H_4, \overline{2}+H_4, \overline{3}+H_4\}, \mathbb{Z}_{12}/H_5 = \{H_5, \overline{1}+H_5, \overline{2}+H_5, \overline{3}+H_5, \overline{4}+H_5, \overline{5}+H_5\},$$

$$\mathbb{Z}_{12}/H_6 = \{\overline{i} + H_6 \mid \overline{i} \in \mathbb{Z}_{12}\} = \{\{\overline{i}\} \mid \overline{i} \in \mathbb{Z}_{12}\},$$

iar operaţiile din grupurile cât sunt definite prin egalităţile

$$(\overline{i} + H_k) + (\overline{j} + H_k) = \overline{i + j} + H_k,\ \overline{i}, \overline{j} \in \mathbb{Z}_{12},\ k \in \{1, 2, 3, 4, 5, 6\}.$$

Fie pe cale directă, fie folosind a treia teoremă de izomorfism pentru grupuri, rezultă că

$$\mathbb{Z}_{12}/H_2 \simeq \mathbb{Z}_2,\ \mathbb{Z}_{12}/H_3 \simeq \mathbb{Z}_3,\ \mathbb{Z}_{12}/H_4 \simeq \mathbb{Z}_4,\ \mathbb{Z}_{12}/H_5 \simeq \mathbb{Z}_6,\ \mathbb{Z}_{12}/H_6 \simeq \mathbb{Z}_{12}.$$

2.144. Indicaţie. Subgrupurile unui grup ciclic sunt ciclice.

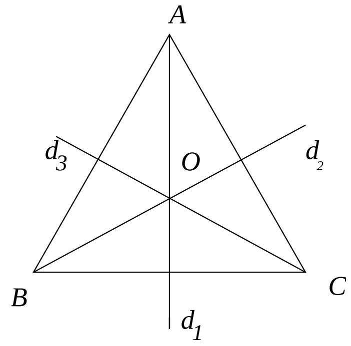
2.145. Indicaţii. i) Dacă $x, y \in G$, din $\text{ord}(xy) = 2$ rezultă $(xy)^{-1} = xy$, adică $y^{-1}x^{-1} = xy$, de unde urmează $yx = xy$.
ii) Se demonstrează prin inducţie după $n = |G|$. Dacă $n = 1$ atunci $|G| = 2^0$. Considerăm $n > 1$ şi presupunem proprietatea adevărată pentru grupurile de ordin cel mult $n - 1$. Dacă G este un grup de ordinul n care verifică ipoteza afirmaţiei din enunţ şi $x \in G \setminus \{1\}$ atunci $\langle x \rangle \trianglelefteq G$ şi grupul cât $G/\langle x \rangle$ verifică ipoteza afirmaţiei din enunţ şi $|G/\langle x \rangle| < n$. Conform ipotezei inducţiei avem $|G/\langle x \rangle| = 2^l$, deci $|G| = 2^l \cdot 2 = 2^{l+1}$.

2.146. Fie $(G, \cdot)$ un grup de ordinul 6. Distingem două cazuri:
i) Dacă $(G, \cdot)$ este ciclic atunci $(G, \cdot) \simeq (\mathbb{Z}_6, +)$.
ii) Dacă $(G, \cdot)$ nu este ciclic atunci orice $x \in G \setminus \{1\}$ are ordinul 2 sau 3, deoarece ordinul unui element divide ordinul grupului. Din problema **2.145** rezultă că G conţine un element a de ordinul 3 — această proprietate se deduce şi din faptul că dacă toate elementele din $G \setminus \{1\}$ ar avea ordinul 2 atunci G ar avea un subgrup izomorf cu grupul ui Klein. Subgrupul $N = \langle a \rangle = \{1, a, a^2\}$ are indicele 2, aşadar $N \trianglelefteq G$, iar dacă $b \in G \setminus N$ atunci $bN = Nb$, adică $\{b, ba, ba^2\} = \{b, ab, a^2b\}$. În grupul cât $G/N = \{N, Nb\}$ avem $Nb^{2k} = N$ şi $Nb^{2k+1} = Nb$. Deci pentru orice $c \in Nb = G \setminus N$ avem $Nc^3 = Nb$, adică $c^3 \notin N$. Rezultă că ordinul lui c nu este 3, de unde urmează că ordinul lui c este 2. Mai avem că $ba = a^2b$. Într-adevăr, din $bN = Nb$ rezultă că $ba = a^kb$ ($k \in \{0, 1, 2\}$), ceea ce implică

$$1 = (ba)(ba) = (a^kb)(ba) = a^{k+1},$$

de unde deducem $k = 2$. În concluzie, $G = \{1, a, a^2, b, ba, ba^2\}$ şi $a^3 = 1$, $b^2 = 1$, $ba = a^2b$, deci $G = \langle a, b \rangle$, iar a, b verifică relaţiile de mai sus. Deci există cel mult un un grup neciclic de ordin 6. Întrucât $(S_3, \circ)$ are ordinul 6 şi nu este ciclic, rezultă că orice grup de ordinul 6 neciclic este izomorf cu $(S_3, \circ)$.

2.147. Fie ABC un triunghi echilateral, d_1, d_2, d_3 axele sale de simetrie şi O centrul său de simetrie (adică $\{O\} = d_1 \cap d_2 \cap d_3$).



Notând cu r rotaţia în jurul lui O de $120°$ (în sensul acelor de ceasornic), cu s simetria în raport cu d_1 şi cu Δ_3 mulţimea rotaţiilor şi simetriilor care aplică triunghiul pe el însuşi avem

$$\Delta_3 = \{r^0, r, r^2, s, r \circ s, r^2 \circ s\},$$

deoarece $r^0 = 1$ este aplicaţia identică, r^2 este rotaţia de $240°$, $r \circ s$ este simetria în raport cu d_2 şi $r^2 \circ s$ este simetria în raport cu d_3. Prin urmare,

$$r^3 = 1,\ s^2 = 1,\ r \circ s = s \circ r^2,$$

iar tabla operaţiei $\circ$ este

$\circ$	1	r	r^2	s	$r \circ s$	$r^2 \circ s$
1	1	r	r^2	s	$r \circ s$	$r^2 \circ s$
r	r	r^2	1	$r \circ s$	$r^2 \circ s$	s
r^2	r^2	1	r	$r^2 \circ s$	s	$r \circ s$
s	s	$r^2 \circ s$	$r \circ s$	1	r^2	r
$r \circ s$	$r \circ s$	s	$r^2 \circ s$	r	1	r^2
$r^2 \circ s$	$r^2 \circ s$	$r \circ s$	s	r^2	r	1

Deci $(\Delta_3, \circ)$ nu este ciclic. Din problema anterioară rezultă $(\Delta_3, \circ) \simeq (S_3, \circ)$.

2.148. Indicaţii. Se verifică cu uşurinţă faptul că Δ_n este o parte stabilă (în raport cu compunerea) a grupului izometriilor planului, că funcţia identică a planului (pe care o notăm cu 1) este în Δ_n şi că inversa oricărei izometrii f pentru care $f(P_n) = P_n$ are aceeaşi proprietate. Fie $A_1, A_2, \ldots, A_n$ vârfurile poligonului P_n, despre care presupunem că se succed în ordinea scrisă, în sensul acelor de ceasornic şi fie O centrul cercului circumscris lui. Cum izometriile planului păstrează distanţele, măsurile unghiurilor şi transformă orice segment de dreaptă într-un segment de dreaptă, rezultă că imaginea prin $f \in \Delta_n$ a oricărei laturi a poligonului regulat P_n va fi o latură a poligonului $f(P_n) = P_n$, ceea ce înseamnă că imaginile prin f ale vârfurilor $A_1, A_2, \ldots, A_n$ sunt determinate, în mod unic, de $f(A_1)$ şi $f(A_2)$. Aceasta ne permite să caracterizăm toate elementele din Δ_n cu ajutorul rotaţiei r de centru O şi unghi $2\pi/n$ în sensul acelor de ceasornic şi cu ajutorul simetriei s a planului faţă de axa OA_1. Într-adevăr, deoarece imaginea laturii $[A_1A_2]$ este o latură a lui P_n, dacă $f(A_1) = A_k$ ($k \in \{1, \ldots, n\}$) atunci $f(A_2) = A_{k+1}$ sau $f(A_2) = A_{k-1}$. Dacă $f(A_1) = A_k$ şi $f(A_2) = A_{k+1}$ atunci $f = r^{k-1}$, iar dacă $f(A_1) = A_k$ şi $f(A_2) = A_{k-1}$ atunci $f = r^{k-1} \circ s$. Dar $r^n = s^2 = 1$, de unde urmează că $\Delta_n = \{1, r, \ldots, r^{n-1}, s, r \circ s, \ldots, r^{n-1} \circ s\}$. Aşadar $|\Delta_n| = 2n$.

Observaţii: Păstrând notaţiile de mai sus, se pot stabili următoarele:
a) Δ_n este subgrupul grupului izometriilor planului generat de r şi s.
b) Avem $r^{n-1} \circ s = s \circ r$ deoarece $(r^{n-1} \circ s)(A_1) = (s \circ r)(A_1)$, $(r^{n-1} \circ s)(A_2) = (s \circ r)(A_2)$.
c) Grupul Δ_n este determinat de generatorii r, s şi relaţiile $r^n = 1$, $s^2 = 1$, $r^{n-1} \circ s = s \circ r$.
d) Avem $(r^k)^{-1} = r^{n-k}$ pentru orice $k \in \{1, \ldots, n-1\}$.
e) Prin inducţie după k, se poate demonstra că $r^{n-k} \circ s = s \circ r^k$ şi $(r^k \circ s)^{-1} = r^k \circ s$ pentru orice $k \in \{0, \ldots, n-1\}$.
f) Grupul diedral $(\Delta_n, \circ)$ este un grup neciclic de ordin $2n$.

2.149. Având în vedere problema anterioară, această problemă este o generalizare a problemei **2.146**. Fie $(G, \cdot)$ un grup de ordin $2p$. Distingem două cazuri:
i) Dacă $(G, \cdot)$ este ciclic atunci $(G, \cdot) \simeq (\mathbb{Z}_{2p}, +)$.
ii) Dacă $(G, \cdot)$ nu este ciclic atunci orice $x \in G \setminus \{1\}$ are ordinul 2 sau p, deoarece ordinul unui element divide ordinul grupului. Din problema **2.145** rezultă că G conţine un element a de ordinul p. Subgrupul $N = \langle a \rangle = \{1, a, \ldots, a^{p-1}\}$ are indicele 2, aşadar $N \trianglelefteq G$, iar dacă $b \in G \setminus N$ atunci $bN = Nb$, adică

$$\{b, ba, \ldots, ba^{p-1}\} = \{b, ab, \ldots, a^{p-1}b\}.$$

În grupul cât $G/N = \{N, Nb\}$ avem $Nb^{2k} = N$ şi $Nb^{2k+1} = Nb$. Deci pentru orice $c \in Nb = G \setminus N$ avem $Nc^3 = Nb$, adică $c^3 \notin N$. Rezultă că ordinul lui c nu este p, de unde urmează că ordinul lui c este 2. Mai avem că $ba = a^{p-1}b$. Într-adevăr, din $bN = Nb$ rezultă că $ba = a^k b$ $(k \in \{0, 1, \ldots, p-1\})$, ceea ce implică $1 = (ba)(ba) = (a^k b)(ba) = a^{k+1}$, de unde deducem $k = p - 1$. În concluzie, $G = \{1, a, \ldots, a^{p-1}, b, ba, \ldots, ba^{p-1}\}$ şi $a^p = 1$, $b^2 = 1$, $ba = a^{p-1}b$, deci $G = \langle a, b \rangle$, iar a şi b verifică relaţiile de mai sus. Deci există cel mult un un grup neciclic de ordin $2p$. Întrucât $(\Delta_p, \circ)$ are ordinul $2p$ şi nu este ciclic, rezultă că orice grup de ordinul $2p$ neciclic este izomorf cu $(\Delta_p, \circ)$.

2.150. Indicaţie. Se aplică problema anterioară pentru $p = 5$.

2.151. Indicaţie. Fie $(G, \cdot)$ un grup cu 8 elemente. Ordinul unui element din $G \setminus \{1\}$ poate fi 2,4 sau 8. Dacă G are un element de ordinul 8 atunci G este ciclic şi deci $(G, \cdot) \simeq (\mathbb{Z}_8, +)$. Presupunem că G nu are elemente de ordinul 8. Distingem următoarele cazuri:
a) Dacă fiecare element din G are ordinul 2 atunci G este abelian şi G este izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
b) G are un element x de ordinul 4. Rezultă că $N = \{1, x, x^2, x^3\}$ este un subgrup de indice 2 al lui G, deci $N \trianglelefteq G$. Urmează că $yN = Ny$ pentru orice $y \in G \setminus N$, adică

$$(*) \qquad \{y, yx, yx^2, yx^3\} = \{y, xy, x^2y, x^3y\}.$$

În grupul cât G/N avem $y^2N = N$, adică $y^2 \in N$. Dacă am avea $y^2 = x$ sau $y^2 = x^3$ ar rezulta că y are ordinul 8, ceea ce este exclus. Urmează că $y^2 = 1$ sau $y^2 = x^2$ ceea ce, împreună cu $(*)$, implică $yx = xy$ sau $yx = x^3y$. Avem, deci, următoarele subcazuri:
b$_1$) $y^2 = 1$ şi $yx = xy$. Rezultă că G este abelian şi $G = \langle x, y \rangle$. Grupul G este izomorf cu $\mathbb{Z}_4 \times \mathbb{Z}_2$.
b$_1'$) $y^2 = x^2$ şi $yx = xy$. Rezultă că $(xy)^2 = x^2y^2 = x^4 = 1$. Deci $z = xy$ are ordinul 2 şi $zN = yN$. Suntem, prin urmare, în subcazul b$_1$). adică $G \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$.
b$_2$) $y^2 = 1$ şi $yx = x^3y$. Grupul G este izomorf cu grupul diedral $(\Delta_4, \circ)$.
b$_3$) $y^2 = x^2$ şi $yx = x^3y$. Grupul G este izomorf cu grupul cuaternionilor.

În concluzie, grupurile neizomorfe de ordinul 8 sunt $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, grupul diedral de grad 4 şi grupul cuaternionilor. Primele trei sunt comutative, iar ultimele două sunt necomutative.

2.152. Indicaţii. $G_1/G_1 = \{G_1\} \simeq \{e_1\} \simeq \{e_2\} \simeq \{G_2\} = G_2/G_2$; $G_1/\{e_1\} \simeq G_2/\{e_2\}$ dacă şi numai dacă $G_1 \simeq G_2$.

2.153. Indicaţie. Se arată că $f : GL_n(K) \to K^*$, $f(A) = \det A$ şi $g : GL_n(\mathbb{Z}) \to U_2$, $g(A) = \det A$ sunt omomorfisme de grupuri şi se aplică prima teoremă de izomorfism.

2.154. Indicaţii. Se arată că funcţiile următoare sunt omomorfisme de grupuri şi se aplică prima teoremă de izomorfism: a) $f : \mathbb{C} \to \mathbb{R}$, $f(a + bi) = b$; b) $f : \mathbb{Q}^* \to \mathbb{Q}^*_+$, $f(x) = |x|$; c) $f : \mathbb{R}^* \to \mathbb{R}^*_+$, $f(x) = |x|$.

2.155. Indicaţii. Se arată că funcţiile: i) $f : \mathbb{R} \to H$, $f(x) = \cos(2\pi x) + i \sin(2\pi x)$; ii) $f : \mathbb{C}^* \to \mathbb{R}^*_+$, $f(z) = |z|$; iii) $f : \mathbb{C}^* \to H$, $f(z) = \dfrac{z}{|z|}$ sunt omomorfisme de grupuri şi se aplică prima teoremă de izomorfism.

2.156. Indicaţii. i) A constituie un sistem de reprezentanţi pentru $(\mathbb{Q}/\mathbb{Z}, +)$.
ii) O clasă din $\mathbb{Q}/\mathbb{Z}$ este de forma $\dfrac{p}{q} + \mathbb{Z}$ cu $p, q \in \mathbb{N}$, $p \neq 0$, $(p, q) = 1$, $p < q$, iar ordinul clasei $\dfrac{p}{q} + \mathbb{Z}$ este q.
iii) Subgrupul ciclic $H = \left\langle \dfrac{1}{n} + \mathbb{Z} \right\rangle = \left\{ \mathbb{Z}, \dfrac{1}{n} + \mathbb{Z}, \dfrac{2}{n} + \mathbb{Z}, \ldots, \dfrac{n-1}{n} + \mathbb{Z} \right\}$ are ordinul n. Dacă H' este un subgrup oarecare de ordinul n şi $\dfrac{p}{q} + \mathbb{Z} \in H'$ $(p, q \in \mathbb{N},\ (p, q) = 1)$ atunci $\dfrac{np}{q} + \mathbb{Z} = \mathbb{Z}$, adică $\dfrac{np}{q} \in \mathbb{Z}$ de unde, întrucât $p, q \in \mathbb{N},\ (p, q) = 1$ rezultă că există $n' \in \mathbb{N}$ astfel încât $n = n'q$. Aşadar, $\dfrac{p}{q} + \mathbb{Z} = \dfrac{n'p}{n} + \mathbb{Z} \in H$. Deci $H' \subseteq H$ şi $|H'| = n = |H|$, ceea ce implică $H = H'$.

2.157. Indicaţie. Se aplică prima teoremă de izomorfism omomorfismului de grupuri $f : \mathbb{Q} \to \mathbb{C}^*$, $f(x) = \cos(2\pi x) + i \sin(2\pi x)$.

2.158. Indicaţii. i) Se verifică uşor că $f_{a,b} \in S_{\mathbb{R}}$. Pentru orice $x \in \mathbb{R}$ avem

$$(f_{a,b} \circ f_{c,d})(x) = f_{a,b}(cx + d) = acx + ad + b = f_{ac,ad+b}(x),$$

iar dacă $a \neq 0$ şi $ax + b = y$ atunci $x = \dfrac{1}{a} y - \dfrac{b}{a}$, adică

$$(1) \qquad f_{a,b} \circ f_{c,d} = f_{ac,ad+b} \text{ şi } f_{a,b}^{-1} = f_{\frac{1}{a}, -\frac{b}{a}}.$$

Deci $f_{a,b} \circ f_{c,d} \in G$ şi $f_{a,b}^{-1} \in G$ pentru $a \neq 0 \neq c$, ceea ce arată că G este un subgrup al lui $(S_{\mathbb{R}}, \circ)$. Fie $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^3$. Avem $f \in S_{\mathbb{R}}$, dar $f^{-1} \circ f_{a,b} \circ f \notin G$ dacă $b \neq 0$, deci subgrupul G nu este normal.
ii) Din (1) rezultă că $f_{a,0} \circ f_{c,0} = f_{ac,0}$ şi $f_{a,0}^{-1} = f_{\frac{1}{a},0}$, ceea ce arată că $H \leq G$. Se arată că $f_{c,d}^{-1} \circ f_{a,0} \circ f_{c,d} \notin H$ pentru $a \neq 1$ şi $d \neq 0$. Deci subgrupul H nu este normal.
iii) Funcţia $\varphi : G \to \mathbb{R}^*$, $\varphi(f_{a,b}) = a$ este un omomorfism surjectiv al lui $(G, \circ)$ pe $(\mathbb{R}^*, \cdot)$. Se aplică prima teoremă de izomorfism lui φ.
iv) Din i) se deduce că N nu este normal în $(S_{\mathbb{R}}, \circ)$.

2.159. Indicaţii. i) $H^{-1} = \{h^{-1} \mid h \in H\}$ este un sistem de reprezentanţi pentru descompunerea la dreapta, dar $H^{-1} = H$.
iv) Funcţia $f : G \to H$, $f(g) = h$, unde $g = hn$, este un omomorfism. Se aplică prima teoremă de izomorfism lui f.

2.160. Indicaţie. b) Fie S_3' submulţimea lui S_4 formată din permutările din S_4 care lasă pe 4 neschimbat. S_3' este un subgrup al lui S_4 izomorf cu S_3 şi

$$\begin{aligned}
(1,2)\circ K &= \{(1,2),(3,4),(1,3,2,4),(1,4,2,3)\},\\
(1,3)\circ K &= \{(1,3),(1,2,3,4),(2,4),(1,4,3,2)\},\\
(2,3)\circ K &= \{(2,3),(1,3,4,2),(1,2,4,3),(1,4)\},\\
(1,2,3)\circ K &= \{(1,2,3),(1,3,4),(2,4,3),(1,4,2)\},\\
(1,3,2)\circ K &= \{(1,3,2),(2,3,4),(1,2,4),(1,4,3)\}.
\end{aligned}$$

Deci S_3' este un sistem de reprezentanţi pentru descompunerea lui S_4 în raport cu K la stânga. Din problema anterioară rezultă că $K \trianglelefteq S_4$ şi $S_4/K \simeq S_3'$.
c) Grupul $(A_4/K, \circ)$ are ordinul 3.

2.161. Indicaţie. iii) $t_a = 1_{G/\rho_H} = t_1 \Leftrightarrow axH = xH, \forall x \in G \Leftrightarrow ax \in xH, \forall x \in G \Leftrightarrow a \in xHx^{-1}, \forall x \in G$.

Observaţie: Această problemă constituie o generalizare a teoremei lui Cayley.

2.162. Indicaţii. Conjugatul unui produs este produsul conjugatelor, iar conjugatul unui ciclu este $\sigma \circ (i_1, \ldots, i_l) \circ \sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_l))$. Deducem că conjugata unei permutări τ prin σ se obţine astfel: considerăm ciclurile din descompunerea lui τ în produs de cicluri disjuncte, aplicăm pe σ la fiecare element ce intervine în acestea şi compunem ciclurile rezultate. Astfel, două permutări din S_n sunt conjugate dacă şi numai dacă descompunerile lor în cicluri disjuncte conţin acelaşi număr de cicluri de lungime dată. Aşa se obţine:

$$S_3 = \{e\} \cup \{(1,2),(1,3),(2,3)\} \cup \{(1,2,3),(1,3,2)\},$$

unde e este permutarea identică din S_3 şi

$$\begin{aligned}
S_4 = \{e\} &\cup \{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}\\
&\cup \{(1,2)\circ(3,4),(1,3)\circ(2,4),(1,4)\circ(2,3)\}\\
&\cup \{(1,2,3),(1,3,2),(1,2,4),(1,4,2),(1,3,4),(1,4,3),(2,3,4),(2,4,3)\}\\
&\cup \{(1,2,3,4),(1,2,4,3),(1,3,2,4),(1,3,4,2),(1,4,2,3),(1,4,3,2)\},
\end{aligned}$$

unde e este permutarea identică din S_4.

2.163. Indicaţii. a) Funcţia $i_g : G \to G$, $i_g(x) = g^{-1}xg$ este un automorfism. Se foloseşte problema **2.97**. b) Dacă $Y = g^{-1}Xg$ atunci funcţia $X \to Y$, $x \mapsto g^{-1}xg$ este bijectivă.

2.164. Din $\alpha = (1,2,5)\circ(4,6)$ şi $\beta = (1,5)\circ(2,3,4)$ rezultă că α şi β sunt conjugate. Avem:

$$\sigma^{-1}\circ\alpha\circ\sigma = \beta \Leftrightarrow \alpha = \sigma\circ\beta\circ\sigma^{-1} \Leftrightarrow (1,2,5)\circ(4,6) = (\sigma(2),\sigma(3),\sigma(4))\circ(\sigma(1),\sigma(5)),$$

adică $(1,2,5) = (\sigma(2),\sigma(3),\sigma(4))$ şi $(4,6) = (\sigma(1),\sigma(5))$. Deci σ este determinat de $\sigma(2) \in \{1,2,5\}$ şi $\sigma(1) \in \{4,6\}$. Rezultă că există şase permutări σ ce verifică condiţia din enunţ.

2.165. Răspuns. $H = \{1\} \cup \{-1\} \cup \{i, -i\} \cup \{j, -j\} \cup \{k, -k\}$.

2.166. Indicaţie. Dacă $(G, \cdot)$ este un grup şi $X \subseteq G$ atunci normalizatorul lui X este

$$N(X) = \{g \in G \mid gX = Xg\}.$$

În cazul nostru se caută matricele nesingulare $U = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$ şi $V = \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix}$ pentru care $UA = AU$ şi $VB = BV$ şi se obţine

$$N(A) = \left\{ \begin{pmatrix} x & 0 \\ 0 & x' \end{pmatrix} \mid x, x' \in \mathbb{R}^* \right\} \text{ şi } N(B) = GL_n(\mathbb{R}).$$

2.167. Indicaţie. Se verifică condiţiile din definiţia acţiunii unui grup pe o mulţime.

2.168. Indicaţie. Se verifică reflexivitatea, simetria şi tranzitivitatea relaţiei $\sim$.

2.169. Indicaţie. $x \sim x' \Leftrightarrow \exists g \in G:\ x' = g^{-1}xg$.

2.170. Indicaţie. $\forall x, x' \in G,\ \exists g \in G:\ gx = x' \Leftrightarrow\ \forall x, x' \in G,\ x \sim x'$.

2.171. Indicaţie. Corespondenţele de la i) şi ii) dau prin compunere funcţiile identice corespunzătoare.

2.172. Indicaţie. ii) Dacă O_x este orbita lui x atunci funcţia $\varphi : \{gF_x \mid g \in G\} \to O_x$, $\varphi(gF_x) = gx$ este bine definită şi este o bijecţie.

2.173. Indicaţie. Dacă G acţionează tranzitiv pe X atunci $X = \{gx_0 \mid g \in G\}$. Fie O_{gx_0} orbita lui gx_0 în raport cu acţiunea lui F pe X. Avem

$$\begin{aligned} g'x_0 \in O_{gx_0} &\Leftrightarrow \exists f \in F:\ f(g'x_0) = gx_0 \Leftrightarrow \exists f \in F:\ (g^{-1}fg')x_0 = x_0 \\ &\Leftrightarrow \exists f \in F:\ g^{-1}fg' \in F \Leftrightarrow g' \in FgF. \end{aligned}$$

Deci funcţia $\varphi : \{O_{gx_0} \mid g \in G\} \to \{FgF \mid g \in G\}$, $\varphi(O_{gx_0}) = FgF$ este bijectivă.

2.174. Indicaţie. Fie $t_g : X \to X$, $t_g(x) = gx$. Funcţia $t : G \to S_X$, $t(g) = t_g$ este un omomorfism şi $N = \mathrm{Ker}\, t$. Deci φ este un omomorfism injectiv furnizat de faptul că $G/N \simeq t(G) \subseteq S_X$.

2.175. Indicaţii. i) Dacă $x \in G$ atunci $|\{gxg^{-1} \mid g \in G\}| = |G : N(x)|$, unde $N(x)$ este normalizatorul lui x.
ii) Fie k numărul elementelor conjugate cu x. Atunci

$$\langle x \rangle \subseteq N(x) \subseteq G \Rightarrow |G : \langle x \rangle| = k \cdot |N(x) : \langle x \rangle| \Rightarrow \frac{n}{m} = k \cdot |N(x) : \langle x \rangle|.$$

iii) Fie k numărul elementelor conjugate cu x. Atunci

$$Z(G) \subseteq N(x) \subseteq G \Rightarrow |G : Z(G)| = |G : N(x)| \cdot |N(x) : Z(G)| \Rightarrow \frac{n}{m'} = k \cdot |N(x) : Z(G)|.$$

iv) $N(x) \subseteq N(x^l) \subseteq G$.

2.176. Indicaţii. Avem $N((2k+1, n)) = \{(2a, 0) \mid a \in \mathbb{Z}\} \cup \{(2a+1, b) \mid a, b \in \mathbb{Z}\}$ şi indicele acestui subgrup este infinit, iar $N((2k, n)) = \{(2a, b) \mid a, b \in \mathbb{Z}\}$, dacă $n \neq 0$ şi indicele acestui subgrup în G este 2, iar $N((2k, 0)) = G$.

2.177. Fie $(G,\cdot)$ un grup cu proprietatea cerută. Rezultă că $|Z(G)| \le 2$, deoarece $g \in Z(G)$ dacă şi numai dacă clasa de conjugare a lui g este $\{g\}$. Dacă $|Z(G)| = 2$ atunci $G = Z(G)$ ceea ce implică $G \simeq \mathbb{Z}_2$. Dacă $|Z(G)| = 1$ atunci $G \setminus \{1\}$ este o clasă de conjugare. Prin urmare, Dacă $|G| = n$ atunci $n-1$ divide pe n, ceea ce nu este posibil pentru $n > 2$. Deci, abstracţie făcând de un izomorfism, $(\mathbb{Z}_2, +)$ este singurul grup care are proprietatea cerută.

2.178. Indicaţii. i) Dacă $K_1 \cap K_2K_3 \ne \emptyset$ atunci există $x \in K_1$, $y \in K_2$, $z \in K_3$ astfel încât $x = yz$. Pentru orice $x' \in K_1$ există $g \in G$ astfel încât $x' = gxg^{-1} = (gyg^{-1})(gzg^{-1})$. Dar $gyg^{-1} \in K_2$ şi $gzg^{-1} \in K_3$. Deci $x' \in K_2K_3$.
ii) Fie $x \in K_1$ şi k_x numărul perechilor $(y,z) \in K_2 \times K_3$ pentru care $x = yz$. Avem $k_x = k_{x'}$ pentru orice $x' \in K_1$, iar dacă $k = k_x$ atunci $k_2k_3 = k_1k$.

2.179. Indicaţie. Avem $|H_1xH_2| = |x^{-1}(H_1xH_2)| = |(x^{-1}H_1x)H_2|$, $x^{-1}H_1x \le G$, $|x^{-1}H_1x| = |H_1|$ şi se aplică problema **2.75**.

2.180. Indicaţie. Fie $Z(G)$ centrul lui G şi $a_1, \ldots, a_k$ un sistem de reprezentanţi al mulţimii cât $(G \setminus Z(G))/\sim$, unde $\sim$ este relaţia de conjugare. Dacă n_i este numărul elementelor conjugate cu a_i atunci $n_i \mid |G|$, iar $n_i > 1$ implică $p \mid n_i$. Din ecuaţia claselor

$$|G| = |Z(G)| + n_1 + \cdots + n_k,$$

rezultă că $p \mid |Z(G)|$, deci $Z(G) \ne \{1\}$.

2.181. Indicaţii. Cazul $p = 2$ a fost cuprins în problema **2.122**. Fie $(G,\cdot)$ un grup de ordinul p^2. Din problema anterioară rezultă că $Z(G) \ne 1$, deci $|Z(G)| \in \{p, p^2\}$. Dacă G are un element de ordinul p^2 atunci G este ciclic şi deci este izomorf cu $(\mathbb{Z}_{p^2}, +)$. Presupunem că G nu are elemente de ordinul p^2. Dacă $|Z(G)| = p$ atunci G ar fi necomutativ şi grupul cât $G/Z(G)$ ar fi ciclic (având ordinul p), ceea ce, conform problemei **2.142**, nu este posibil. Deci $|Z(G)| = p^2$, adică $G = Z(G)$, ceea ce arată că G este abelian. Dacă $a \in G \setminus \{1\}$ atunci a are ordinul p. Alegând $b \in G \setminus \langle a \rangle$ avem $\langle a \rangle \cap \langle b \rangle = \{1\}$ şi $G = \langle a, b \rangle$. Rezultă că $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.

2.182. Indicaţie. Se aplică problema anterioară pentru $p = 3$.

2.183. Răspuns. Grupurile ciclice de ordinul p^2, cu p număr prim.

2.184. Indicaţii. i) Cum $Z(G) \ne \{1\}$ şi grupul G nu este comutativ, avem $|Z(G)| \in \{p, p^2\}$. Dacă $|Z(G)| = p^2$ atunci $|G/Z(G)| = p$ şi $G/Z(G)$ ar fi ciclic, ceea ce este imposibil (vezi problema **2.142**). Deci $|Z(G)| = p$. ii) Cum $|G/Z(G)| = p^2$ şi $G/Z(G)$ nu este ciclic, avem $G/Z(G) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ (vezi problema **2.181**).

2.185. Indicaţie. Dacă $g \in G_p$ şi $f \in End(G,\cdot)$ atunci $\operatorname{ord} f(g) \mid \operatorname{ord} g$.

2.186. Indicaţie. Dacă $f \in End(A,+)$, $a \in A$ şi $n \in \mathbb{N}^*$ atunci $f(na) = nf(a)$.

2.187. Indicaţie. ii) Dacă $f \in End(G)$ atunci $\overline{f} \in End(G/H)$, prin urmare avem $f(H')/H = \overline{f}(H'/H) \subseteq H'/H$, de unde rezultă $f(H') \subseteq H'$.

2.188. Dacă H_i, $i \in I$, este o familie de subgrupuri caracteristice (deplin invariante) şi $f : G \to G$ este un automorfism (endomorfism) atunci

$$f\left(\bigcap_{i\in I} H_i\right) \subseteq \bigcap_{i\in I} f(H_i) \subseteq \bigcap_{i\in I} H_i\,,$$

$$f\left(\left\langle \bigcup_{i\in I} H_i \right\rangle\right) = \left\langle f\left(\bigcup_{i\in I} H_i\right)\right\rangle = \left\langle \bigcup_{i\in I} f(H_i)\right\rangle \subseteq \left\langle \bigcup_{i\in I} H_i \right\rangle.$$

2.189. Indicaţie. i) Se arată că $\langle\bigcup\{f(X) \mid f \in Aut(G,\cdot)\}\rangle$ este un subgrup caracteristic al lui G care include pe X şi că dacă H este un subgrup caracteristic care include pe X atunci $\langle\bigcup\{f(X) \mid f \in Aut(G,\cdot)\}\rangle \subseteq H$. ii) Se procedează ca la i).

2.190. Indicaţie. Se aplică lema lui Zorn mulţimii subgrupurilor caracteristice (deplin invariante) disjuncte de X.

2.191. Indicaţii. i) Fie $a, b \in F(G)$. Dacă $\langle X \cup \{ab^{-1}\}\rangle = G$ atunci, întrucât are loc $\langle X \cup \{ab^{-1}\}\rangle \subseteq \langle X \cup \{a, b\}\rangle$ rezultă că $\langle X \cup \{a, b\}\rangle = G$, ceea ce implică $\langle X\rangle = G$. Aşadar $ab^{-1} \in F(G)$. Fie $a \in F(G)$ şi $f : G \to G$ un automorfism. Dacă $\langle X \cup \{f(a)\}\rangle = G$ atunci aplicăm pe f^{-1} şi avem $\langle f^{-1}(X) \cup \{a\}\rangle = G$ ceea ce implică $\langle f^{-1}(X)\rangle = G$. Aplicând pe f, obţinem $\langle X\rangle = G$. Deci $f(a) \in F(G)$.
ii) Fie $\{M_i \mid i \in I\}$ mulţimea subgrupurilor maximale ale lui $(G,\cdot)$ şi M intersecţia lor.

$$a \notin M \Rightarrow \exists i_0 \in I, a \notin M_{i_0} \Rightarrow \langle M_{i_0} \cup \{a\}\rangle = G \text{ şi } \langle M_{i_0}\rangle = M_{i_0} \neq G \Rightarrow a \notin F(G)\,.$$

Dacă $a \notin F(G)$ atunci există $X \subseteq G$ astfel încât $\langle X \cup \{a\}\rangle = G$ şi $\langle X\rangle \neq G$. Fie $\mathcal{S}$ mulţimea acelor subgrupuri H ale lui G pentru care avem $X \subseteq H$ şi $a \notin H$. Putem aplica lema lui Zorn mulţimii $(\mathcal{S}, \subseteq)$, deci există un subgrup maximal M' pentru care $a \notin M'$. Deci $a \notin M$.

2.192. Subgrupul Frattini al grupului abelian $(\mathbb{Q}, +)$ este $\mathbb{Q}$ deoarece grupul $(\mathbb{Q}, +)$ nu are subgrupuri maximale. Într-adevăr, dacă M ar fi un subgrup maximal al lui $\mathbb{Q}$ atunci, conform [34, Corolarul 2.9.2], grupul cât $\mathbb{Q}/M$ ar fi un grup simplu, ceea ce înseamnă că $\mathbb{Q}/M$ este un grup ciclic de ordin număr prim (vezi [34, Exemplul 2.8.8, b)]). Fie $|\mathbb{Q}/M| = p$. Rezultă că pentru orice $x \in \mathbb{Q}$ avem $p(x + M) = M$, adică $px \in M$. Deducem astfel că $p\mathbb{Q} \subseteq M$. Dar $p\mathbb{Q} = \mathbb{Q}$ şi $M \subseteq \mathbb{Q}$, deci $M = \mathbb{Q}$, ceea ce contrazice alegerea lui M.

Totuşi, subgrupoidul Frattini al lui $(\mathbb{Q}, +)$ nu este $\mathbb{Q}$ deoarece $\{x \in \mathbb{Q} \mid x \geq 0\}$ este un subgrupoid maximal al lui $\mathbb{Q}$. Într-adevăr, dacă B ar fi un subgrupoid al lui $\mathbb{Q}$ ce include strict pe $\{x \in \mathbb{Q} \mid x \geq 0\}$ atunci în B există un număr raţional negativ $b = \dfrac{p}{q}$ $(p \in \mathbb{Z}_-,\ q \in \mathbb{N}^*)$. Rezultă că $p = qb \in B$, cum $-p + 1 \in \mathbb{Q}_+ \subseteq B$ avem $-1 = p + (-p + 1) \in B$ şi astfel avem $\mathbb{Z}_- \subseteq B$. În consecinţă, orice număr raţional negativ x aparţine lui B deoarece $x = [x] + \{x\}$ este suma dintre un număr întreg negativ (partea întreagă a sa) şi un număr raţional nenegativ (partea sa fracţionară), de unde urmează că $B = \mathbb{Q}$.

2.193. Răspuns. $[A, B] = \begin{pmatrix} 7 & 4 \\ -2 & -1 \end{pmatrix}$, $[B, C] = \begin{pmatrix} 5 & -3 \\ -3 & 2 \end{pmatrix}$, $[C, A] = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$.

2.194. Indicaţii. i), ii) Se foloseşte definiţia comutatorului şi se efectuează calculele. iii), iv) rezultă din i) şi ii).

2.195. Indicaţie. Se efectuează calculele şi (unde e cazul) se completează raţionamentul prin inducţie matematică.

2.196. i) Dacă $A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ şi $B = \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix}$ atunci

$$AB = \begin{pmatrix} 1 & a'+a & b'+ac'+b \\ 0 & 1 & c'+c \\ 0 & 0 & 1 \end{pmatrix}.$$

Rezultă că $A^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$. Deci $G \leq GL_3(\mathbb{Z})$.

ii) Avem

$$(*) \qquad [A,B] = \begin{pmatrix} 1 & 0 & a'c-ac' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Deci

$$A \in Z(G) \Leftrightarrow a'c - ac' = 0,\ \forall a', c' \in \mathbb{Z} \Leftrightarrow a = 0 = c.$$

Acum din $(*)$ rezultă că pentru orice $A, B \in G$ avem $[A,B] \in Z(G)$. Invers, dacă $A \in Z(G)$ atunci

$$A = \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = [A', B'],$$

unde $A' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ şi $B' = \begin{pmatrix} 1 & b & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, adică $A \in G'$.

2.197. $N \trianglelefteq G \Leftrightarrow \forall n \in N, \forall g \in G, g^{-1}ng \in N \Leftrightarrow \forall n \in N, \forall g \in G, n^{-1}g^{-1}ng \in N \Leftrightarrow \forall n \in N, \forall g \in G, [n,g] \in N \Leftrightarrow [N,G] \subseteq N$.

2.198. Indicaţie. $\forall n_1 \in N_1, \forall n_2 \in N_2, n_1^{-1}n_2^{-1}n_1n_2 = n_1^{-1}(n_2^{-1}n_1n_2) \in n_1^{-1}N_1 = N_1$ şi $n_1^{-1}n_2^{-1}n_1n_2 = (n_1^{-1}n_2^{-1}n_1)n_2 \in N_2n_2 = N_2$.

2.199. Indicaţie. Folosind problemele **2.194** şi **2.195** deducem că oric element din G' este un produs finit de elemente de forma $g^{-1}[x,y]g$, cu $g \in G$ şi $x, y \in X$, deci aparţine lui N.

2.200. Răspuns. $H' = \{-1, 1\}$.

2.201. Răspuns. $S_3' = A_3$.

2.202. Indicaţie. Fie $n \geq 3$ şi S_n' subgrupul derivat al lui S_n. Avem $S_n' = A_n$. Într-adevăr, din faptul că grupul cât S_n/A_n este abelian, rezultă că $S_n' \subseteq A_n$. Fie transpoziţiile $\sigma_1 = (i,j)$ şi $\sigma_2 = (j,k)$. Avem $[\sigma_1, \sigma_2] = (i,j) \circ (j,k) \circ (i,j) \circ (j,k) = (i,k,j)$. Deci orice ciclu de lungime 3 este comutator, iar cum mulţimea ciclurilor de lungime 3 este un sistem de generatori pentru A_n (vexi problema **2.86**), rezultă că $S_n' = A_n$.

2.203. Subgrupul H este inclus într-un p-subgrup Sylow P. Fie p^n ordinul lui P. Demonstrăm prin inducţie după n că $N_G(H) \neq H$. Dacă $n = 1$ atunci $H = \{1\}$ şi $N_G(H) = G$. Presupunem afirmaţia adevărată pentru P de ordinul p^n. Pentru P de ordinul p^{n+1}, centrul $Z(P)$ al lui P este diferit de $\{1\}$. Dar $Z(P) \subseteq N_G(H)$ şi distingem două cazuri:
i) Dacă $Z(P) \nsubseteq H$ atunci, evident, $N_G(H) \neq H$.
ii) Dacă $Z(P) \subseteq H$ atunci, aplicând ipoteza inducţiei subgrupului $H' = H/Z(P)$ al lui $P' = P/Z(P)$, urmează că există $xZ(P) \in P'$, $xZ(P) \notin H'$ astfel încât

$$(xZ(P))^{-1}H'(xZ(P)) = H'.$$

Rezultă că $x \in P$, $x \notin H$ şi $x^{-1}Hx = H$, adică $x \notin H$ şi $x \in N_G(H)$. Deci $N_G(H) \neq H$.

2.204. i) Fie $N = N_G(P)$. Întâi observăm că P este un p-subgrup Sylow al lui H. Fie $g \in N_G(H)$. Atunci $g^{-1}Hg = H$ şi subgrupul $g^{-1}Pg$ este p-subgrup Sylow al lui H. Întrucât p-subgrupurile Sylow sunt conjugate, urmează că există $h \in H$ astfel încât $g^{-1}Pg = h^{-1}Ph$, adică $hg^{-1}Pgh^{-1} = P$, deci $gh^{-1} \in N \subseteq H$, ceea ce implică $g \in H$, adică $N_G(H) \subseteq H$. Incluzinea inversă are loc deoarece orice subgrup este inclus în normalizatorul său. Aşadar, $N_G(H) = H$.
ii) Fie $M = \{H, x_1H, \ldots, x_nH\}$ mulţimea claselor la stânga ale lui H' în raport cu H. Grupul P acţionează pe M prin înmulţire la stânga, iar $yH = H$ pentru orice $y \in P$, deoarece $P \subseteq H$. Deci orbita lui H este formată numai din H. Fie $x \in H'$. Atunci $xH \in M$ şi arătăm că dacă $xH \neq H$ atunci numărul elementelor din orbita lui xH este de forma p^k cu $k \geq 1$. Pentru aceasta este suficient să arătăm că stabilizatorul F al lui xH coincide cu P dacă şi numai dacă $yxH = xH$ pentru orice $y \in P$, adică $x^{-1}yx \in H$ pentru orice $y \in P$, ceea ce înseamnă că $x^{-1}Px \subseteq H$. Deci P şi $x^{-1}Px$ sunt P subgrupuri Sylow ale lui H, de unde urmează că ele sunt conjugate în H, adică există $h \in H$ astfel încât $h^{-1}x^{-1}Pxh = P$. Prin urmare, $xh \in N \subseteq H$ şi $x \in H$. Folosind, acum, faptul că $|M| = |H' : H|$ şi partiţia lui M în orbite, obţinem:

$$|H' : H| = 1 + p^{k_1} + \cdots + p^{k_m}, \text{ cu } k_i \geq 1,$$

adică $|H' : H| \equiv 1 \pmod{p}$.

2.205. Cum $|S_4| = 4! = 24 = 2^3 \cdot 3$, urmează că 2-subgrupurile Sylow ale lui S_4 sunt subgrupurile de ordinul 8, iar 3-subgrupurile Sylow sunt subgrupurile de ordinul 3. Subgrupurile de ordinul 3 ale lui S_4 sunt generate de elemente de ordinul 3, iar acestea sunt chiar 3-ciclurile din S_4. Astfel, numărul 3-subgrupurilor Sylow este $n_3 = 4$ şi acestea sunt

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

unde e este permutarea identică din S_4. Pentru a obţine 2-subgrupurile Sylow ale lui S_4 procedăm astfel: dacă $\sigma = (1,2,3,4)$ şi $\tau = (1,2) \circ (3,4)$ atunci $\sigma^4 = e$, $\tau^2 = e$ şi $\tau \circ \sigma = \sigma^3 \circ \tau$, de unde rezultă că subgrupul

$$H = \langle \sigma, \tau \rangle = \{e, (1,2,3,4), (1,3) \circ (2,4), (1,4,3,2), (1,2) \circ (3,4), (1,3), (2,4)\}$$

(este izomorf cu grupul diedral Δ_4 şi) are 8 elemente, iar 2-subgrupurile Sylow sunt conjugate cu H. Ştim, de asemenea, că numărul $n_2 = |S_4 : N_{S_4}(H)|$ al 2-subgrupurilor Sylow divide pe $|S_4 : H| = 3$, deci $n_2 = 1$ sau $n_2 = 3$. Dacă n_2 ar fi egal cu 1 atunci H ar fi subgrup normal în S_4, ceea ce nu este adevărat deoarece $(1,4)^{-1} \circ (2,4) \circ (1,4) = (1,2) \notin H$. Deducem că $n_2 = 3$, iar 3-subgrupurile Sylow ale lui S_4 sunt H, $H' = (1,4)^{-1} \circ H \circ (1,4)$, $H'' = (1,2)^{-1} \circ H \circ (1,2)$, adică H şi

$$\begin{aligned} H' &= \{e, (1,4,2,3), (1,2) \circ (3,4), (1,3,2,4), (1,3) \circ (2,4), (3,4), (1,2)\}, \\ H'' &= \{e, (1,3,4,2), (1,4) \circ (2,3), (1,2,4,3), (1,2) \circ (3,4), (2,3), (1,4)\}. \end{aligned}$$

2.206. Fie $(G, \cdot)$ un grup de ordinul 15. Din teorema lui Cauchy rezultă că G are un element a de ordinul 5 şi un element b de ordinul 3. Subgrupul $\langle a \rangle$ este un 5-subgrup Sylow. Întrucât numărul n_5 al 5-subgrupurilor Sylow este un divizor al lui 3 şi $n_5 \equiv 1 (\text{mod } 5)$. Urmează că $n_5 = 1$, aşadar $\langle a \rangle$ este singurul 5-subgrup Sylow. Deducem că $\langle a \rangle \trianglelefteq G$, iar din $a^{-1}, b^{-1}ab \in \langle a \rangle$ rezultă $a^{-1}b^{-1}ab \in \langle a \rangle$. Analog se demonstrează că $\langle b \rangle$ şi că $a^{-1}b^{-1}ab \in \langle b \rangle$. Cum orice element din $\langle a \rangle \setminus \{1\}$ are ordinul 5 şi orice element din $\langle b \rangle \setminus \{1\}$ are ordinul 3, folosind problema **2.99** avem $\langle a \rangle \cap \langle b \rangle = \{1\}$. Prin urmare, $bab^{-1} = a$, adică $ba = ab$. Acum, folosind problema **2.100**, deducem că $\text{ord}(ab) = 15$, deci G este ciclic şi $G \simeq \mathbb{Z}_{15}$.

2.207. Indicaţii. Această problemă este o generalizare a problemei anterioare. Din teorema lui Cauchy deducem că există $a, b \in G$ cu $\text{ord}\, a = p$ şi $\text{ord}\, b = q$. Fie n_p şi n_q numărul p-subgrupurilor Sylow, respectiv al q-subgrupurilor Sylow ale lui G. Avem $n_p | q$ şi $n_p \equiv 1 (\text{mod } p)$, prin urmare $n_p = 1$ sau $n_p = q$. Dar egalitatea $n_p = q$ poate avea loc numai în cazul când $q \equiv 1 (\text{mod } p)$. Analog $n_q = 1$ sau $n_q = p$, iar egalitatea $n_q = p$ poate avea loc numai în cazul când $p \equiv 1 (\text{mod } q)$. În condiţiile din enunţ avem $n_p = n_q = 1$, aşadar $\langle a \rangle \trianglelefteq G$ şi $\langle b \rangle \trianglelefteq G$. Ca în soluţia problemei anterioare deducem că $ab = ba$ este un element de ordinul pq, deci un generator al lui G.

2.208. Fie P un p-subgrup Sylow al lui G şi Q un q-subgrup Sylow al lui G. Avem $|P| = p^2$, $|Q| = q$, iar dacă n_p este numărul p-sugrupurilor Sylow şi n_q este numărul q-subgrupurilor Sylow ale lui G atunci $n_p | q$ şi $n_q | p^2$. Să presupunem că $n_p > 1$ şi $n_q > 1$. Urmează că $n_p = q$ şi că $n_q \in \{p, p^2\}$. Din $q = n_p \equiv 1 (\text{mod } p)$ avem $q > p$, iar din $n_q \equiv 1 (\text{mod } p)$ şi $q > p$ rezultă $n_q = p^2$. Este evident că orice element de ordinul q al lui G generează un q-subgrup Sylow şi că orice două subgrupuri diferite de ordinul q au intersecţia formată numai din elementul neutru ceea ce ne conduce la faptul că numărul elementelor de ordinul q din G este $n_q(q-1) = p^2(q-1)$, iar numărul elementelor din G care nu sunt de ordinul q este $p^2q - p^2(q-1) = p^2$. Cum $|P| = p^2$ şi nici un element din P nu are ordinul q, deducem că P este chiar mulţimea elementelor din G care nu au ordinul q. Dar aceasta se întâmplă pentru orice p-subgrup Sylow, deci $n_p = 1$, contradicţie. Prin urmare, $n_p = 1$ sau $n_q = 1$, adică $P \trianglelefteq G$ sau $Q \trianglelefteq G$ şi G nu este simplu.

Dacă, în plus, $q \nmid p^2 - 1$ şi $p \nmid q - 1$ atunci, conform celor de mai sus, avem $n_p = 1$ şi $n_q = 1$. Deducem că $P \trianglelefteq G$, $Q \trianglelefteq G$ şi (ca în problemele anterioare) că $a^{-1}b^{-1}ab \in P \cap Q$ pentru orice $a \in P$ şi $b \in Q$. Din $PQ = QP$ rezultă $PQ = \langle P \cup Q \rangle$. Din teorema lui Lagrange deducem că $|P \cap Q|$ divide pe $(|P|, |Q|) = (p^2, q) = 1$, de unde obţinem că $P \cap Q = \{1\}$ şi aplicând problema **2.75** urmează că $|PQ| = p^2q$ şi astfel, $G = PQ = \langle P \cup Q \rangle$. Aşadar, $ab = ba$ pentru orice $a \in P$, $b \in Q$, P şi Q sunt abeliene, deci G este abelian deoarece orice generatori ai săi comută.

2.209. Fie $(G, \cdot)$ un grup cu $|G| = 255 = 3 \cdot 5 \cdot 17$. Un 17-subgrup Sylow H al lui G are ordinul 17, deci este ciclic, iar dacă n_{17} este numărul 17-subgrupurilor Sylow ale lui G atunci $n_{17}|15$ şi $n_{17} \equiv 1 (\text{mod } 17)$. Rezultă că $n_{17} = 1$ şi $H \trianglelefteq G$. Grupul cât G/H are ordinul 15, de unde, conform problemei **2.206**, deducem că este ciclic. Fie $a, b \in G$ astfel încât $H = \langle a \rangle$ şi $G/H = \langle bH \rangle$ şi fie $n = \text{ord}(b)$. Aplicând problema **2.98** proiecţiei canonice determinate de factorizarea modulo H avem $15|n$. De asemenea, n divide pe $|G| = 15 \cdot 17$ ceea ce implică $n = 15$ sau $n = 255$. Dacă $n = 255$ atunci G este ciclic, generat de b. Dacă $n = 15$ atunci există $r \in \{0, \ldots, 16\}$ astfel încât $b^{-1}ab = a^r$, deoarece $b^{-1}ab \in H = \langle a \rangle$. Presupunem că pentru un $m \in \mathbb{N}$ avem $b^{-m}ab^m = a^{r^m}$ şi deducem că

$$b^{-(m+1)}ab^{m+1} = b^{-1}(b^{-m}ab^m)b = b^{-1}a^{r^m}b = (b^{-1}ab)^{r^m} = (a^r)^{r^m} = a^{r^{m+1}},$$

ceea ce arată că $b^{-m}ab^m = a^{r^m}$ pentru orice număr natural m. În particular, avem $a^{r^{15}} = b^{-15}ab^{15} = a$, de unde urmează $r^{15} \equiv 1 (\text{mod } 17)$. Din Teorema lui Fermat ştim că $r^{16} \equiv 1 (\text{mod } 17)$, aşadar $r \equiv 1 (\text{mod } 17)$ şi astfel, $r = 1$. Întrucât $b^{-1}ab = a$, avem $ab = ba$, iar din problema **2.100** deducem că $\text{ord}(ab) = 15 \cdot 17 = 255$ şi, prin urmare, că G este ciclic.

2.210. Indicaţii. i) Avem $f : H \times H' \to G,\ f(h, h') = hh'$.
ii) $\text{Ker} f = \{(h, h^{-1}) \mid h \in H \cap H'\}$ deoarece

$$(h, h') \in \text{Ker} f \Leftrightarrow hh' = 1 \Leftrightarrow h' = h^{-1}.$$

iii) Avem $\langle H \cup H' \rangle = HH'$ şi $f(H \times H') = HH'$, deci omomorfismul f este surjectiv dacă şi numai dacă $G = HH'$.

2.211. Indicaţie. Se foloseşte definiţia produsului direct.

2.212. Indicaţie. X generează pe P dacă şi numai dacă I este finită sau $|G_i| = 1$ pentru orice $i \in I$.

2.213. Răspuns. a) $X = \{(1, 0), (0, 1)\}$; b) Generalizarea se poate face la grupul $(\mathbb{Z}^n, +)$ luând $|X| = n$ şi atunci $X = \{(1, 0, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)\}$ sau la suma directă a familiei de grupuri $(A_i, +) = (\mathbb{Z}, +)$, $i \in I$, luând $|X| = |I|$ şi atunci $X = \{f_i : I \to \mathbb{Z} \mid i \in I\}$, unde $f_i(j) = \begin{cases} 1, & j = i\,; \\ 0, & j \in I \setminus \{i\}\,. \end{cases}$

2.214. Indicaţii. Dacă $a \in A$ şi $\text{ord}\, a = m = p_1^{r_1} \cdots p_n^{r_n}$, cu $p_1, \ldots, p_n$ numere prime diferite, atunci numerele $m_i = mp_i^{-r_i}$ $(i \in \{1, \ldots, n\})$ sunt relativ prime, de unde rezultă că există $s_1, \ldots, s_n \in \mathbb{Z}$ astfel încât $s_1m_1 + \cdots + s_nm_n = 1$. Avem $m_ia \in A_{p_i}$ deoarece $p_i^{r_i}m_iA = ma = 0$ şi astfel,

$$a = s_1m_1a + \cdots + s_nm_na \in \left\langle \bigcup_{p \in \mathbb{P}} A_p \right\rangle.$$

Mai mult, orice element din $A_{p_1}+\cdots+A_{p_k}$ se anulează prin înmulţire cu un produs de puteri ale numerelor prime $p_1,\ldots,p_k$, ceea ce arată că pentru orice număr prim p diferit de $p_1,\ldots,p_k$ avem

$$A_p\cap(A_{p_1}+\cdots+A_{p_k})=\{0\},$$

deci $A=\left\langle\bigcup\limits_{p\in\mathbb{P}}A_p\right\rangle=\bigoplus\limits_{p\in\mathbb{P}}A_p$.

2.215. Indicaţie. Conform problemei anterioare, grupul U al rădăcinilor unităţii este izomorf cu $\bigoplus\limits_{p\in\mathbb{P}}\mathbb{Z}(p^\infty)$ şi se foloseşte izomorfismul din problema **2.157**.

2.216. Din [34, Teorema 2.16.22] rezultă că determinarea tuturor grupurilor abeliene finite neizomorfe de ordinul $m>1$ se reduce la determinarea tuturor n-uplelor $(m_1,\ldots,m_n)\in\mathbb{N}^n$ cu proprietăţile: $m_i>1$, $m_{i+1}|m_i$ şi $m=m_1\cdots m_n$. De aici deducem că orice divizor prim al lui m este divizor şi al lui m_1. În cazul nostru $32=2^5$, deci n-uplele sunt: 32, (16,2), (8,4), (8,2,2), (4,4,2), (4,2,2,2), (2,2,2,2,2). Rezultă că grupurile neizomorfe de ordinul 32 sunt $\mathbb{Z}_{32}$, $\mathbb{Z}_{16}\times\mathbb{Z}_2$, $\mathbb{Z}_8\times\mathbb{Z}_4$, $\mathbb{Z}_8\times\mathbb{Z}_2\times\mathbb{Z}_2$, $\mathbb{Z}_4\times\mathbb{Z}_4\times\mathbb{Z}_2$, $\mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$ şi $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$.

2.217. Răspuns. $\mathbb{Z}_{64}$, $\mathbb{Z}_{32}\times\mathbb{Z}_2$, $\mathbb{Z}_{16}\times\mathbb{Z}_4$, $\mathbb{Z}_8\times\mathbb{Z}_8$, $\mathbb{Z}_{16}\times\mathbb{Z}_2\times\mathbb{Z}_2$, $\mathbb{Z}_8\times\mathbb{Z}_4\times\mathbb{Z}_2$, $\mathbb{Z}_4\times\mathbb{Z}_4\times\mathbb{Z}_4$, $\mathbb{Z}_8\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$, $\mathbb{Z}_4\times\mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_2$, $\mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$ şi $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$.

2.218. Răspuns. $\mathbb{Z}_{96}$, $\mathbb{Z}_{48}\times\mathbb{Z}_2$, $\mathbb{Z}_{24}\times\mathbb{Z}_4$, $\mathbb{Z}_{24}\times\mathbb{Z}_2\times\mathbb{Z}_2$, $\mathbb{Z}_{12}\times\mathbb{Z}_4\times\mathbb{Z}_2$, $\mathbb{Z}_{12}\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$, $\mathbb{Z}_6\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$.

2.219. Indicaţie. Orice şir descrescător de subgrupuri (normale) cu factorii grupuri simple este de forma

$$\mathbb{Z}\supset n_1\mathbb{Z}\supset n_1n_2\mathbb{Z}\supset\cdots,$$

cu $n_1,n_2,\ldots$ numere prime, ori un astfel de şir este infinit.

2.220. Indicaţii. Dacă $(A,+)$ are şiruri de compoziţie şi

$$(*)\qquad A\supset H_0\supset H_1\supset H_2\supset\cdots H_n=\{0\}$$

este un şir de compoziţie atunci H_{i+1} este un subgrup maximal în H_i, de unde urmează că grupul H_i/H_{i+1} este simplu, deci finit şi de ordin prim (vezi [34, Exemplul 2.8.8, b)]). De aici, având în vedere că $(*)$ implică

$$|A|=|H_0:H_1||H_1:H_2|\cdots|H_{n-1}:H_n|$$

urmează că grupul A este finit.

2.221. Indicaţie. Fie $A=\mathbb{Z}_6\times\mathbb{Z}_5$. Avem $A\simeq\mathbb{Z}_{30}$, adică grupul A este ciclic. Dacă $d|30$ şi $30=dq$ atunci A are un singur subgrup de ordinul d şi anume qA. Avem $qA\subseteq q'A$ dacă şi numai dacă $q'|q$.

$$A\supset 2A\supset 2\cdot 3A\supset 2\cdot 3\cdot 5A=\{(\overline{0},\widehat{0})\}$$

este un şir de compoziţie şi orice şir de compoziţie se obţine din acesta, aplicând numerelor $2,3,5$ o permutare. Deci A are $3!=6$ şiruri de compoziţie.

2.222. Indicaţie. Se procedează ca în problema anterioară.

2.223. Reamintim că un grup $(G, \cdot)$ este nilotent de clasă k dacă numărul $k \in \mathbb{N}$ este cel mai mic cu proprietatea că $Z_k(G) = G$, unde $Z_n(G)$ $(n \in \mathbb{N})$ sunt termenii şirului central ascendent. Prin urmare $k = 1$ dacă şi numai dacă $Z(G) = G$, adică G este abelian şi $G \neq \{1\}$.

2.224. Indicaţie. Fie k clasa de nilpotenţă a lui G. Dacă $k < 2$ atunci toţi membrii egalităţilor din enuţ sunt 1. Avem

$$k = 2 \Rightarrow Z_2(G) = G \Rightarrow Z(G/Z(G)) = G/Z(G).$$

Deci $G/Z(G)$ este abelian. Rezultă că pentru orice $x, y \in G$ avem $[x, y]Z(G) = Z(G)$, adică

$$[x, y] \in Z(G)$$

şi se folosesc egalităţile din problema **2.194**.

2.225. Indicaţie. Fie $H = \{-1, 1, -i, i, -j, j, -k, k\}$ grupul cuaternionilor. Avem $Z(H) = \{-1, 1\}$ şi

$$H/Z(H) = \{\{-1, 1\}, \{-i, i\}, \{-j, j\}, \{-k, k\}\},$$

iar $H/Z(H)$ este abelian. Rezultă că $Z(H/Z(H)) = H/Z(H)$, adică $Z_2(H) = H$.

2.226. Răspuns. $n \in \{1, 2\}$.

2.227. $(S_1, \circ)$ şi $(S_2, \circ)$ sunt abeliene, deci resolubile. Subgrupul derivat al lui S_n este A_n (vezi problema **2.202**), iar A_3 este abelian. Deci şirul derivat al lui S_3 este $S_3 \supset A_3 \supset \{e\}$, unde e este permutarea identică. Rezultă că S_3 este resolubil de clasă 2. Mulţimea

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

(unde e este permutarea identică din S_4) este un subgrup normal în S_4 şi grupul cât S_4/K este izomorf cu grupul simetric S_3 (vezi problema **2.160**). Grupul K este abelian, deci resolubil, iar S_3 am văzut că este resolubil. Aplicăm [34, Teorema 2.13.3, 3)] (care arată că orice exindere a unui grup resolubil printr-un grup resolubil este un grup resolubil) şi obţinem că S_4 este resolubil.

2.228. Fie $(G, \cdot)$ un grup de ordinul $2p$ (p prim). Grupul G are un subgrup H de ordinul p. Rezultă că H este ciclic şi de indice 2. Urmează că $H \trianglelefteq G$ şi că grupurile H şi G/H sunt resolubile, deci G este resolubil.

2.229. Fie $(G, \cdot)$ un grup de ordinul pq (p, q numere prime). Dacă $p = q$ atunci G este abelian (vezi problema **2.181**), deci resolubil. Dacă $p > q$ atunci numărul p-subgrupurilor Sylow este de forma $1 + kp$ şi divide ordinul lui G, adică pe pq. Rezultă $k = 0$, deci există un singur p-subgrup Sylow P. Întrucât conjugatele unui p-subgrup Sylow sunt p-subgrupuri Sylow, urmează că $P \trianglelefteq G$. Cum grupurile P şi G/P sunt ciclice, deci resolubile, avem G resolubil.

Capitolul 3

Inele şi corpuri

3.1. 1) Arătăm că că $(\mathbb{Z}, \perp)$ este grup abelian.
a) Pentru orice $x, y, z \in \mathbb{Z}$, folosind asociativitatea şi comutativitatea adunării numerelor întregi, avem:

$$(x \perp y) \perp z = (x + y + 3) \perp z = x + y + 3 + z + 3 = x + y + z + 6;$$
$$x \perp (y \perp z) = x \perp (y + z + 3) = x + y + z + 3 + 3 = x + y + z + 6,$$

de unde rezultă $(x \perp y) \perp z = x \perp (y \perp z)$, adică $\perp$ este asociativă.
b) Pentru orice $x, y \in \mathbb{Z}$, folosind comutativitatea adunării din $\mathbb{Z}$, avem

$$x \perp y = x + y + 3 = y + x + 3 = y \perp x,$$

adică $\perp$ este comutativă.
c) Există $e_0 \in \mathbb{Z}$ astfel încât, pentru orice $x \in \mathbb{Z}$, să avem

$$e_0 \perp x = x = x \perp e_0. \tag{1}$$

Întrucât $\perp$ este comutativă, avem:

$$(1) \Leftrightarrow e_0 \perp x = x \Leftrightarrow e_0 + x + 3 = x \Leftrightarrow e_0 = -3.$$

Deci $e_0 = -3 \in \mathbb{Z}$ este element neutru în $(\mathbb{Z}, \perp)$.
d) Pentru orice $x \in \mathbb{Z}$ există $x' \in \mathbb{Z}$ astfel încât

$$x' \perp x = -3 = x \perp x'. \tag{2}$$

Întrucât $\perp$ este comutativă, avem

$$(2) \Leftrightarrow x' \perp x = -3 \Leftrightarrow x' + x + 3 = -3 \Leftrightarrow x' = -6 - x \in \mathbb{Z}.$$

Deci orice element din $\mathbb{Z}$ este simetrizabil în $(\mathbb{Z}, \perp)$. Astfel, am arătat că $(\mathbb{Z}, \perp)$ este un grup abelian.
2) Arătăm că $(\mathbb{Z}, \top)$ este monoid comutativ.

a) Pentru orice $x, y, z \in \mathbb{Z}$, folosind proprietăţile operaţiilor $+$ şi $\cdot$ din $\mathbb{Z}$ avem:

$$\begin{aligned}
(x\top y)\top z &= (xy+3x+3y+6)\top z\\
&= (xy+3x+3y+6)z+3(xy+3x+3y+6)+3z+6\\
&= xyz+3xz+3yz+6z+3xy+9x+9y+18+3z+6\\
&= xyz+3xy+3xz+3yz+9x+9y+9z+24;\\
x\top(y\top z) &= x\top(yz+3y+3z+6)\\
&= x(yz+3y+3z+6)+3x+3(yz+3y+3z+6)+6\\
&= xyz+3xy+3xz+6x+3x+3yz+9y+9z+18+6\\
&= xyz+3xy+3xz+3yz+9x+9y+9z+24,
\end{aligned}$$

ceea ce ne arată că $(x\top y)\top z = x\top(y\top z)$, adică $\top$ este asociativă.
b) Pentru orice $x, y \in \mathbb{Z}$ avem

$$x\top y = xy+3x+3y+6 = yx+3y+3x+6 = y\top x,$$

adică $\top$ este comutativă.
c) Există $e_1 \in \mathbb{Z}$ astfel încât, pentru orice $x \in \mathbb{Z}$,

$$e_1\top x = x = x\top e_1. \tag{3}$$

Întrucât $\top$ este comutativă, avem:

$$(3) \Leftrightarrow e_1\top x = x \Leftrightarrow e_1x+3e_1+3x+6 = x \Leftrightarrow (x+3)(e_1+2) = 0,$$

care trebuie să aibă loc pentru orice $x \in \mathbb{Z}$. Deci $e_1 = -2 \in \mathbb{Z}$ este elementul neutru în $(\mathbb{Z}, \top)$.
3) Arătăm că $\top$ este distrbutivă faţă de $\perp$. Pentru orice $x, y, z \in \mathbb{Z}$ avem:

$$\begin{aligned}
(x\perp y)\top z &= (x+y+3)\top z = (x+y+3)z+3(x+y+3)+3z+6\\
&= xz+yz+3x+3y+6z+15;\\
(x\top z)\perp(y\top z) &= (xz+3x+3z+6)\perp(yz+3y+3z+6)\\
&= xy+3x+3z+6+yz+3y+3z+6+3\\
&= xz+yz+3x+3y+6z+15,
\end{aligned}$$

de unde rezultă $(x\perp y)\top z = (x\top z)\perp(y\top z)$. Din comutativitatea operaţiei $\top$ rezultă şi $z\top(x\perp y) = (x\top z)\perp(z\top y)$, deci $\top$ este distributivă în raport cu $\perp$.

Din 1), 2) şi 3) rezultă că $(\mathbb{Z}, \perp, \top)$ este un inel asociativ, comutativ şi cu unitate. În acest inel, $e_0 = -3$ este elementul zero şi $e_1 = -2$ este elementul unitate. Evident că $\mathbb{Z} \neq \{e_0\}$. Pentru a arăta că $(\mathbb{Z}, \perp, \top)$ este domeniu de integritate, mai trebuie arătat că $(\mathbb{Z}, \perp, \top)$ nu are divizori ai lui zero, adică

$$x\top y = e_0 \Rightarrow x = e_0 \text{ sau } y = e_0. \tag{4}$$

Într-adevăr,

$$x\top y = e_0 \Leftrightarrow xy+3x+3y+6 = -3 \Leftrightarrow (x+3)(y+3) = 0 \Rightarrow x = -3 \text{ sau } y = -3,$$

ceea ce arată că (4) este adevărată. În concluzie, $(\mathbb{Z}, \perp, \top)$ este un domeniu de integritate.

Determinăm elementele inversabile. Un element $x \in \mathbb{Z}$ este inversabil în $(\mathbb{Z}, \perp, \top)$ dacă şi numai dacă există $x'' \in \mathbb{Z}$ astfel încât $x'' \top x = e_1$, adică

$$\exists x'' \in \mathbb{Z}: \ x''x + 3x'' + 3x + 6 = -2 \Leftrightarrow \exists x'' \in \mathbb{Z}: \ x''(x+3) = -8 - 3x.$$

Elementul nul $e_0 = -3$ nu este inversabil, deci $x \neq -3$ şi

$$x'' = -\frac{3x+8}{x+3} = -\frac{3(x+3)-1}{x+3} = -3 + \frac{1}{x+3} \in \mathbb{Z} \Leftrightarrow x \in \{-2, -4\}.$$

Deci elementele inversabile în $(\mathbb{Z}, \perp, \top)$ sunt elementul unitate $e_1 = -2$ şi -4. Menţionăm că în orice inel nenul cu unitatea e_1 şi elementul nul e_0, e_0 nu este inversabil şi e_1 este inversabil.

Observaţie: Inelul de mai sus este un de domeniu de integritate care nu este corp.

3.2. Indicaţie. Elementul nul este 0, $i \neq 0$ şi $i * i = 0$, prin urmare, i este un divizor al lui zero.

3.3. Indicaţie. Se verifică condiţiile din definiţia corpului.

3.4. i) Observăm că $X + Y$ este diferenţa simetrică a mulţimilor X şi Y, iar din problema **2.94** deducem că $(\mathcal{P}(M), +)$ este grup abelian. Din proprietăţile intersecţiei şi definiţia operaţiei $\cdot$ rezultă că $\cdot$ este asociativă, comutativă şi M este element neutru. Deci $(\mathcal{P}(M), \cdot)$ este monoid comutativ.

Stabilim distributivitatea operaţiei $\cdot$ faţă de $+$. Într-adevăr,

$$\begin{aligned}
X \cdot Y + X \cdot Z &= (X \cap Y) + (X \cap Z) \\
&= [(X \cap Y) \cap C(X \cap Z)] \cup [(X \cap Z) \cap C(X \cap Y)] \\
&= [X \cap Y \cap (C(X) \cup C(Z))] \cup [X \cap Z \cap (C(X) \cup C(Y))] \\
&= [X \cap Y \cap C(X)] \cup [X \cap Y \cap C(Z)] \cup [X \cap Z \cap C(X)] \cup [X \cap Z \cap C(Y)] \\
&= \emptyset \cup [X \cap Y \cap C(Z)] \cup \emptyset \cup [X \cap Z \cap C(Y)] \\
&= [X \cap Y \cap C(Z)] \cup [X \cap Z \cap C(Y)] = X \cap [(Y \cap C(Z)) \cup (Z \cap C(Y))] \\
&= X \cdot (Y + Z),
\end{aligned}$$

ceea ce arată că $\cdot$ este distributivă în raport cu $+$. Deci $(\mathcal{P}(M), +, \cdot)$ este inel asociativ, comutativ, cu unitate. Elementul zero, respectiv elementul unitate este $\emptyset$, respectiv M.

ii) În acest inel avem, pentru orice $X \subseteq M$, $X^2 = X$, adică $X(X-1) = 0$, sau echivalent, $X(X + M) = \emptyset$, ceea ce arată că orice $X \in \mathcal{P}(M) \setminus \{\emptyset, M\}$ este divizor al lui zero.

iii) Din ii) rezultă că inelul $(\mathcal{P}(M), +, \cdot)$ este fără divizori ai lui zero dacă şi numai dacă $P(M) = \{\emptyset, M\}$, adică $|M| \leq 1$. Dacă $|M| = 0$ atunci $M = \emptyset$ şi $(\mathcal{P}(M), +, \cdot)$ este inelul nul, iar dacă $|M| = 1$ atunci $(\mathcal{P}(M), +, \cdot)$ este izomorf cu $(\mathbb{Z}_2, +, \cdot)$, de unde rezultă că $(\mathcal{P}(M), +, \cdot)$ este corp.

3.5. Pentru orice $a, b \in R$ avem

$$(1+1)(a+b) = 1(a+b) + 1(a+b) = 1\cdot a + 1\cdot b + 1\cdot a + 1\cdot b = a+b+a+b,$$
$$(1+1)(a+b) = (1+1)a + (1+1)b = 1\cdot a + 1\cdot a + 1\cdot b + 1\cdot b = a+a+b+b$$

de unde deducem $a+b+a+b = a+a+b+b$, adică $a+b = b+a$.

3.6. Răspuns. $(M_n(\mathbb{Z}_m), +, \cdot)$, cu $m, n \in \mathbb{N}$, $m \geq 2$, $n \geq 2$.

Observaţie: Nu există corpuri finite necomutative (vezi Teorema lui Wedderburn).

3.7. a) Dacă $(a+b)^2 = a^2 + 2ab + b^2$ atunci $a^2 + ab + ba + b^2 = a^2 + ab + ab + b^2$, iar cum în grupul $(R, +)$ se poate simplifica cu orice element, deducem că $ab = ba$. Din $a^2 - b^2 = (a-b)(a+b)$ rezultă $a^2 - b^2 = a^2 + ab - ba - b^2$, de unde urmează că $0 = ab - ba$, adică $ab = ba$. Dacă $ab = ba$ atunci cele două egalităţi se verifică imediat.
b) Ţinem seama de faptul că orice puteri (cu exponent natural nenul) ale elementelor a, b comută (vezi problema **2.58**) şi procedăm prin inducţie după n. Pentru $n = 1$ afirmaţia este, evident, adevărată, iar dacă egalitatea este adevărată pentru n atunci

$$\begin{aligned}(a+b)^{n+1} &= (a+b)^n(a+b) = (C_n^0 a^n + C_n^1 a^{n-1}b + \cdots + C_n^{n-1} ab^{n-1} + C_n^n b^n)a \\ &+ (C_n^0 a^n + C_n^1 a^{n-1}b + \cdots + C_n^{n-1} ab^{n-1} + C_n^n b^n)b \\ &= C_n^0 a^{n+1} + (C_n^1 + C_n^0)a^n b + \cdots + (C_n^{n-1} + C_n^n)ab^n + C_n^n b^{n+1}.\end{aligned}$$

Cum $C_n^0 = C_n^n = 1$ şi $C_n^k + C_n^{k-1} = C_{n+1}^k$ pentru orice $n \in \mathbb{N}^*$ şi $1 \leq k \leq n$, avem

$$(a+b)^{n+1} = C_{n+1}^0 a^{n+1} + C_{n+1}^1 a^n b + \cdots + C_{n+1}^n ab^n + C_{n+1}^{n+1} b^{n+1},$$

ceea ce finalizează raţionamentul prin inducţie. Celelalte egalităţi se obţin efectuând calculul din membrul drept.

3.8. Indicaţii. Cazul $n = 0$ este evident. Fie $n \in \mathbb{N}^*$ şi $x, y \in R$ arbitrare. Avem

$$x^n(xy^n - y^n x)y = x^{n+1}y^{n+1} - (x^n y^n)\, xy = (xy)^{n+1} - (xy)^n(xy) = (xy)^{n+1} - (xy)^{n+1} = 0,$$

adică $x^n(xy^n - y^n x)y = 0$. Înlocuind pe x cu $x+1$ şi efectuând calculele din paranteză obţinem $(x+1)^n\,(xy^n - y^n x)\,y = 0$. Cum x şi 1 comută, putem dezvolta $(x+1)^n$ după formula binomului lui Newton. Înmulţind la stânga egalitatea astfel obţinută cu x^{n-1} deducem că $x^{n-1}\,(xy^n - x^n y)\,y = 0$. Aplicarea succesivă a raţionamentului de mai sus ne conduce la egalitatea $(xy^n - y^n x)\,y = 0$.

Dacă începem procedeul de mai sus cu calculul lui $x^{n+1}\left(xy^{n+1} - y^{n+1}x\right)y$ (care este de asemenea 0), concluzia obţinută va fi $\left(xy^{n+1} - y^{n+1}x\right)y = 0$. Prin urmare,

$$\begin{aligned}(xy - yx)y^{n+1} &= xy^{n+2} - yxy^{n+1} = xy^{n+2} - y^{n+1}xy - yxy^{n+1} + y^{n+1}xy \\ &= (xy^{n+1} - y^{n+1}x)y - y(xy^n - y^n x)y = 0.\end{aligned}$$

Cum x, y sunt arbitrare, avem, de asemenea $(xy - yx)(y+1)^{n+1} = 0$, dezvoltăm binomial pe $(y+1)^{n+1}$, înmulţim la dreapta cu y^n şi obţinem $(xy - yx)y^n = 0$. Aplicăm succesiv acest raţionament şi ajungem în final la egalitatea $xy - yx = 0$.

3.9. Indicaţii. Din $x^3 = x$ rezultă $x^4 = x^2$. Folosind acest rezultat, prin calcul se obţine $\left(x^2yx^2 - x^2y\right)^2 = 0$ pentru orice $x, y \in R$. Urmează $x^2yx^2 - x^2y = \left(x^2yx^2 - x^2y\right)^3 = 0$, aşadar $x^2yx^2 = x^2y$. Analog se arată că $x^2yx^2 = yx^2$, prin urmare, $x^2y = yx^2$ pentru orice $x, y \in R$ şi astfel avem $xy = x^3y^3 = x^2(xyy^2) = [(xy)y^2]x^2 = y^2(xy)x^2 = y(yx)(yx)x = y(yx)^2x = (yx)^2(yx) = (yx)^3 = yx$.

3.10. Din $-x = (-x)^6 = x^6 = x$ rezultă $2x = x + x = x + (-x) = 0$ pentru orice $x \in R$. Atunci

$$x + x^2 = (x + x^2)^6 = x^6 + 6x^7 + 15x^8 + 20x^9 + 15x^{10} + 6x^{11} + x^{12} = x + x^3 + x^5 + x^2.$$

Prin urmare, $x^3 + x^5 = 0$ sau, echivalent, $x^5 = -x^3 = x^3$, ceea ce implică

$$x = x^6 = x^5x = x^3x = x^4 \text{ şi } x^2 = x^5 = x^3.$$

Astfel, avem $x = x^6 = x^2x^4 = x^2x = x^3 = x^2$.

3.11. ii)$\Rightarrow$i) Se ia $n = 2$.
i)$\Rightarrow$ii) Demonstrăm prin inducţie după $n \in \mathbb{N}^*$ că, dacă i) are loc, atunci

$$P(n): \ n \in \mathbb{N}^*, \ a^n = 0 \ \Rightarrow \ a = 0.$$

Afirmaţiile $P(1)$ şi $P(2)$ sunt, evident, adevărate. Fie $n \in \mathbb{N}$, $n \geq 3$. Presupunem că afirmaţia $P(k)$ este adevărată pentru orice $k \in \mathbb{N}^*$, $k < n$ şi arătăm că $P(n)$ este adevărată. Dacă $n = 2m$ este un număr par nenul atunci $m \in \mathbb{N}^*$, $m < n$ şi $a^n = a^{2m} = (a^m)^2$. Conform lui i) şi faptului că $P(m)$ este adevărată avem succesiv:

$$a^n = 0 \Leftrightarrow (a^m)^2 = 0 \Rightarrow a^m = 0 \Rightarrow a = 0.$$

Dacă $n = 2m - 1 \geq 3$ este un număr impar şi $a^n = 0$ atunci $a^{n+1} = a^n \cdot a = 0$, iar $n + 1 = 2m$ şi $m < n$. Prin urmare, aplicând succesiv i) şi faptul că $P(m)$ este adevărată, avem:

$$a^n = 0 \Rightarrow (a^m)^2 = a^{2m} = a^{n+1} = 0 \Rightarrow a^m = 0 \Rightarrow a = 0.$$

3.12. Această problemă generalizează situaţia întâlnită în soluţia problemei **3.4** ii). Pentru $x \in R$, egalitatea $x^2 = x$ are loc dacă şi numai dacă $x(x - 1) = 0$. Rezultă că orice $x \in R \setminus \{0, 1\}$ este divizor al lui zero.

3.13. Pentru orice idempotent $a \in R$, $a - 1$ este, de asemenea, idempotent şi $a(a - 1) = 0$, iar din $1 \neq 0$ rezultă $a - 1 \neq a$. Deducem că elementele idempotente ale lui R pot fi grupate în perechi care dau produsul zero. Prin urmare produsul cerut este 1 dacă 1 este singurul idempotent nenul, respectiv 0 dacă în R există elemente idempotente diferite de 0 şi 1.

3.14. Fie $a \in R$ un element idempotent şi $x \in R$ arbitrar. Atunci

$$\begin{aligned}(ax - axa)^2 &= (ax - axa)(ax - axa) = (ax - axa)ax - (ax - axa)axa \\ &= axax - axaax - axaxa + axaaxa = axax - axax - axaxa + axaxa = 0.\end{aligned}$$

Deducem că $ax - axa = 0$. Analog se obţine $xa - axa = 0$, deci $ax = axa = xa$.

3.15. Indicaţii. a) Dacă există $m \in \mathbb{N}$ astfel încât $(\widehat{a})^m = \widehat{0}$ atunci $n|a^m$, deci $p_i|a^m$ pentru orice $i \in \{1, \dots, k\}$. Cum numerele p_i sunt prime, rezultă $p_i|a$ pentru orice $i \in \{1, \dots, k\}$, iar din faptul că sunt distincte deducem că $p_1 \cdots p_k|a$. Reciproc, dacă $p_1 \cdots p_k|a$ şi luăm $m = \max\{\alpha_1, \dots, \alpha_k\}$ atunci $\widehat{a^m} = \widehat{0}$.
b) Este o consecinţă imediată a lui a).

3.16. Fie $\mathbb{P}$ mulţimea nunerelor prime, $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, cu $p_1, \dots, p_k \in \mathbb{P}$ distincte şi $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$, descompunerea lui n în factori primi şi M mulţimea părţilor mulţimii $A = \{p_1, \dots, p_k\}$. Avem

$$\{p \in \mathbb{P} \mid p|(x, n)\} = \{p \in A \mid p|x\},$$

iar dacă $p \in A$ divide pe x şi n divide pe $x - y$ atunci p divide şi pe $x - (x - y) = y$. Înseamnă că

$$\widehat{x} \mapsto \{p \in \mathbb{P} \mid p|(x, n)\}$$

defineşte o funcţie φ de la mulţimea elementelor idempotente ale lui $\mathbb{Z}_n$ la M. Mai mult, dacă $\widehat{x} \in \mathbb{Z}_n$ este un element idempotent atunci

$$(x, n) = \prod_{p_i \in \varphi(\widehat{x})} p_i^{\alpha_i}. \tag{1}$$

Într-adevăr, fie $d = (x, n)$, $x = dx'$, $n = dn'$ $(x', n' \in \mathbb{Z})$. Din $(\widehat{x})^2 = \widehat{x}$ sau, echivalent, $n|x(x - 1)$, deducem că $n'|x'(x - 1)$. Cum $(n', x') = 1$, avem $n'|x - 1$, ceea ce împreună cu $(x, x - 1) = 1$ şi $d|n$ conduce la $(d, n') = 1$. Aşadar, $p_i|d$ $(i \in \{1, \dots, k\})$ implică $p_i^{\alpha_i}|d$ şi astfel $\prod_{p_i \in \varphi(\widehat{x})} p_i^{\alpha_i}$ divide pe d. Cum d divide pe $\prod_{p_i \in \varphi(\widehat{x})} p_i^{\alpha_i}$, egalitatea (1) este verificată.

Funcţia φ este bijectivă, ceea ce ne permite să caracterizăm elementele idempotente ale lui $\mathbb{Z}_n$ cu ajutorul mulţimii M.

Arătăm că φ este injectivă. Fie $\widehat{x}, \widehat{y} \in \mathbb{Z}_n$ două elemente idempotente astfel ca $\varphi(\widehat{x}) = \varphi(\widehat{y})$. Din (1) rezultă că $(x, n) = (y, n)$. Păstrând notaţiile de mai sus, avem

$$n'|(x - 1) \text{ şi } n' = \frac{n}{(x, n)} = \frac{n}{(x, n)}\Bigg| (y - 1),$$

deci $n'|(x - y)$. De asemenea $d = (x, n) = (y, n)|(x - y)$ şi cum $(d, n') = 1$, rezultă că $n = dn'$ divide pe $x - y$, adică $\widehat{x} = \widehat{y}$.

Surjectivitatea lui φ se obţine astfel: dacă $I \subseteq \{1, \dots, k\}$ şi $\{p_i \mid i \in I\} \in M$, considerăm $a = 1$ dacă $I = \emptyset$ şi $a = \prod_{i \in I} p_i^{\alpha_i}$ altfel, şi avem

$$\left(a, \frac{n}{a}\right) = 1 \Rightarrow \exists u, v \in \mathbb{Z} : \ au + \frac{n}{a}\, v = 1.$$

Notăm $x = au$. Atunci $x(x - 1) = ua\left(-\frac{n}{a}\, v\right) = -uvn$ este un multiplu de n, deci $\widehat{x} \in \mathbb{Z}_n$ este idempotent, iar cum $(x, n) = a$ conform lui (1) avem

$$\varphi(\widehat{x}) = \{p_i \mid i \in I\}.$$

Demonstraţia surjectivităţii lui φ indică şi modul de obţinere a elementelor idempotente ale lui $\mathbb{Z}_n$ din submulţimile mulţimii A. Luând ca exemplu, $n = 12$ avem

$$n = 2^2 \cdot 3,\ A = \{2, 3\},\ M = \{\emptyset, \{2\}, \{3\}, \{2, 3\}\},$$

a ia valorile

$$1,\ 2^2 = 4,\ 3,\ 2^2 \cdot 3 = 12$$

şi u ia, respectiv, valorile

$$1,\ 1,\ -1,\ 0,$$

iar elementele idempotente ale lui $\mathbb{Z}_{12}$ sunt:

$$\widehat{1},\ \widehat{4},\ \widehat{9} \text{ şi } \widehat{0}.$$

3.17. Indicaţii. i) Cum $(R, +)$ este un grup, funcţia f este injectivă, ceea ce, în ipoteza R finită, înseamnă chiar f bijectivă.
ii) Din surjectivitatea lui f avem

$$\{f(0), f(1), f(a), f(b)\} = \{1 + 0, 1 + 1, 1 + a, 1 + b\} = f(A) = A = \{0, 1, a, b\}.$$

Obţinem astfel $f(0) + f(1) + f(a) + f(b) = 0 + 1 + a + b = 1 + a + b$ sau, echivalent,

$$1 + 1 + 1 + 1 + 1 + a + b = 1 + a + b,$$

adică $1 + 1 + 1 + 1 = 0$.
iii) Dacă R este corp, R nu are divizori ai lui zero şi din

$$(1 + 1)(1 + 1) = 1 + 1 + 1 + 1 = 0$$

deducem $1 + 1 = 0$.
iv) Dacă R este corp, din $1 + 1 = 0$ deducem $x + x = x(1 + 1) = 0$ pentru orice $x \in R$. Ştiind că în tabla unui grup un element apare o singură dată pe orice linie (coloană) putem construi tabla lui $(R, +)$ şi a lui $(R^*, \cdot)$ şi vom constata că $1+a = a^2$ şi $1+b = b^2$. Reciproc, cum 0 şi 1 nu verifică egalitatea $1+x = x^2$ deducem că $x \in \{a, b\}$. Dacă $1+a = a^2$ atunci

$$a(a - 1) = (a - 1)a = 1.$$

Dacă $a-1 = 0$ atunci $a = 1$, imposibil. Dacă $a-1 = 1$ atunci $a = 1+1$, iar din $1+a = a^2$ deducem $1 + 1 + 1 = 1 + 1 + 1 + 1$, deci $0 = 1$, imposibil. Dacă $a - 1 = a$ atunci $0 = 1$, imposibil. Rămâne doar posibilitatea ca $a - 1 = b$. Deducem că 1, a şi b sunt inversabile, şi $1^{-1} = 1$, $a^{-1} = b$ şi $b^{-1} = a$. Analog se procedează în cazul în care $1 + b = b^2$.

3.18. Pentru orice $x, y \in R$ avem $(x + y)^2 = x + y$ şi

$$(x+y)^2 = (x+y)(x+y) = (x+y)x+(x+y)y = x^2+yx+xy+y^2 = x+xy+yx+y,$$

de unde urmează $x + y = x + xy + yx + y$, adică

$$0 = yx + xy. \tag{1}$$

i) Luând $y = x$ în (1) obţinem $0 = x^2 + x^2$ pentru orice $x \in R$, ceea ce implică $x + x = 0$, adică

$$x = -x,\ \forall x \in R. \tag{2}$$

ii) Din (1) şi (2) rezultă

$$xy = -yx = yx, \ \forall x, y \in R,$$

adică R este comutativ.
iii) Presupunem că $|R| \geq 3$ şi că R nu are divizori ai lui zero. Rezultă că există $a, b \in R^*, \ a \neq b$. Cum $ab = (ab)^2 = (ab)(ab) = abab$, avem

$$0 = ab - abab = (a - aba)b.$$

Dar $b \neq 0$ şi R nu are divizori ai lui zero, prin urmare

$$a = aba = a(ba) = a(ab) = a^2b = ab.$$

În consecinţă, $a^2 = a = ab$ sau, echivalent,

$$0 = a^2 - ab = a(a - b).$$

Folosind, din nou, faptul că R nu are divizori ai lui zero, cum $a \neq 0$, rezultă $a = b$, ceea ce contrazice faptul că $a \neq b$. Dacă $|R| \leq 2$, inelul nul nu conţine divizori ai lui zero, iar dacă R este un inel cu 2 elemente atunci R este un corp (izomorf cu $(\mathbb{Z}_2, +, \cdot)$), prin urmare nu are divizori ai lui zero.
iv) Pentru a arăta că un inel Boole cu unitate $(R, +, \cdot)$ este corp numai dacă $|R| = 2$ se poate aplica punctul anterior. Folosind existenţa elementului unitate în R se poate da şi o altă demonstraţie a acestui fapt: din problema **3.12** rezultă că orice $x \in R \backslash \{0, 1\}$ este divizor al lui zero. Deci, pentru ca $(R, +, \cdot)$ să fie corp este necesar ca $|R| \geq 2$ şi $R \subseteq \{0, 1\}$, adică $|R| = 2$.

Observaţie: Inelul $(\mathcal{P}(M), +, \cdot)$ din problema **3.4** este inel Boole cu unitate. Această structură de inel Boole este indusă de structura de latice Boole a mulţimii $\mathcal{P}(M)$.

3.19. Indicaţii. i) Din problema **2.95** deducem că $(R, +)$ este grup abelian. Elementul său neutru este 0. Ca în problema **3.4** se arată că $(R, +, \cdot)$ este un inel asociativ, comutativ, cu unitate (1 fiind unitatea sa), iar dacă $x \in R$ atunci $x^2 = x \wedge x = x$.
ii) Folosim problema **2.22** pentru a arăta că $(R, \vee, \wedge)$ este o latice cu 0 cel mai mic element şi 1 cel mai mare element. Întrucât inelele Boole sunt comutative, operaţiile $\vee$ şi $\wedge$ sunt comutative. Asociativitatea operaţiei $\cdot$ implică asociativitatea operaţiei $\wedge$, iar pentru a arăta că $\vee$ este asociativă se demostrează egalităţile

$$(x \vee y) \vee z = x + y + z - xy - xz - yz + xyz = x \vee (y \vee z).$$

Operaţiile $\vee$ şi $\wedge$ verifică legile de absorbţie:

$$x \wedge (x \vee y) = x(x \vee x) = x(x + x - xx) = x(x + x - x) = x^2 = x,$$
$$x \vee (x \wedge y) = x \vee (xy) = x + xy - x^2y = x + xy - xy = x,$$

iar dacă $x \in R$ atunci $0 \wedge x = 0 \cdot x = 0$ şi $1 \wedge x = 1 \cdot x = x$, adică $0 \leq x$ şi $x \leq 1$ pentru orice $x \in R$. Distributivitatea laticii $(R, \vee, \wedge)$ rezultă arătând că

$$x \wedge (y \vee z) = xy + xz - xyz = (x \wedge y) \vee (x \wedge z),$$

iar probând egalităţile $(1 - x) \wedge x = 0$ şi $(1 - x) \vee x = 1$ deducem că orice $x \in R$ are complement şi anume pe $1 - x$.

iii) Mulţimea suport a laticii $g(f(R,\vee,\wedge))$ este, evident, mulţimea R, iar dacă notăm cu $\vee^*$, respectiv $\wedge^*$ operaţiile din $g(f(R,\vee,\wedge))$ atunci, pentru orice $x,y\in R$, avem

$$\begin{aligned}
x\vee^* y &= x+y-xy = x+(y+(xy)) = x+\{[y\wedge(x\wedge y)']\vee[y'\wedge(x\wedge y)]\}\\
&= x+\{[y\wedge(x'\vee y')]\vee(y'\wedge x\wedge y)\} = x+[(y\wedge x')\vee(y\wedge y')\vee 0] = x+[(y\wedge x')\vee 0]\\
&= x+(y\wedge x') = [x\wedge(y\wedge x')']\vee[x'\wedge(y\wedge x')] = [x\wedge(y'\vee x)]\vee(x'\wedge y\wedge x')\\
&= [(x\wedge y')\vee(x\wedge x)]\vee(x'\wedge y) = [(x\wedge y')\vee x]\vee(x'\wedge y) = x\vee(x'\wedge y)\\
&= (x\vee x')\wedge(x\vee y) = 1\wedge(x\vee y) = x\vee y
\end{aligned}$$

şi

$$x\wedge^* y = xy = x\wedge y.$$

Similar se procedează pentru a arata că $f(g(R,+,\cdot)) = (R,+,\cdot)$.

3.20. Indicaţie. Dacă $a\in R^*$ nu este divizor al lui zero atunci cu a se poate simplifica, prin urmare, funcţiile $t_a, t'_a : R\to R$, $t_a(x) = ax$, $t'_a(x) = xa$ sunt injective, ceea ce, împreună cu finitudinea lui R implică surjectivitatea acestor funcţii. Deci există $a', a''\in R$ astfel ca $1 = t_a(a') = aa'$ şi $1 = t'_a(a'') = a''a$. Folosind asociativitatea în calculul lui $a''aa'$ se obţine $a' = a'' = a^{-1}$.

3.21. Indicaţie. Se foloseşte problema anterioară.

3.22. Indicaţii. Fie a_0 un element fixat din mulţimea nevidă $A = \{a'\in R \mid a'a = 1\}$. Se arată că corespondenţa $a'\mapsto aa' - 1 + a_0$ defineşte o funcţie injectivă f de la A la o submulţime proprie a sa, ceea ce face ca A şi, implicit, R să fie infinită. Incluziunea strictă $f(A)\subset A$ se obţine demonstrând prin reducere la absurd că $a_0\notin f(A)$: presupunând contrariul, ar rezulta că există un $a'\in A$ pentru care $aa'-1+a_0 = a_0$, deci a' ar fi un invers pentru a, implicit unicul invers la stânga, ceea ce contrazice ipoteza.

3.23. Avem

$$\widehat{4}x+\widehat{5} = \widehat{9} \Leftrightarrow \widehat{4}x = \widehat{4} \Leftrightarrow x\in\{\widehat{1},\widehat{4},\widehat{7},\widehat{10}\},$$
$$\widehat{5}x+\widehat{5} = \widehat{9} \Leftrightarrow \widehat{5}x = \widehat{4} \Leftrightarrow x = (\widehat{5})^{-1}\cdot\widehat{4} \Leftrightarrow x = \widehat{8}.$$

Fie $X = \begin{pmatrix} a & b\\ c & d\end{pmatrix}$. Avem

$$\begin{pmatrix} 1 & 2\\ 1 & 2\end{pmatrix}\begin{pmatrix} a & b\\ c & d\end{pmatrix} = \begin{pmatrix} 1 & 2\\ 1 & 2\end{pmatrix} \Leftrightarrow \begin{cases} a+2c = 1\\ b+2d = 2\end{cases} \Leftrightarrow \begin{cases} a = 1-2c\\ b = 2-2d\end{cases}.$$

Prin urmare, mulţimea soluţiilor ecuaţiei matriceale date este

$$\left\{\begin{pmatrix} 1-2c & 2-2d\\ c & d\end{pmatrix} \mid c,d\in\mathbb{C}\right\}.$$

3.24. Folosind faptul că $U(\mathbb{Z}_{12},+,\cdot) = \{\widehat{a}\mid (a,12) = 1\} = \{\widehat{1},\widehat{5},\widehat{7},\widehat{11}\}$ şi problema **3.20** deducem că divizorii lui zero din $\mathbb{Z}_{12}$ sunt $\widehat{2},\widehat{3},\widehat{4},\widehat{6},\widehat{8},\widehat{9}$ şi $\widehat{10}$.

Coeficienţii lui x şi y fiind divizori ai lui zero, aplicarea metodei reducerii poate conduce la sisteme neechivalente. Adunând cele două ecuaţii ale sistemului dat obţinem

$$\widehat{7}x + y = \widehat{9} \Leftrightarrow y = \widehat{5}x+\widehat{9}. \tag{1}$$

Înlocuind pe y în prima ecuaţie a sistemului obţinem

$$\widehat{3}x+\widehat{8}x=\widehat{11}\Leftrightarrow\widehat{11}x=\widehat{11}\Leftrightarrow x=\widehat{1}.$$

Urmează imediat că $y=\widehat{5}+\widehat{9}=\widehat{2}$, deci sistemul dat are soluţie unică pe $(\widehat{1},\widehat{2})$.

Observaţii: a) Dacă înmulţirea unei ecuaţii cu un element care nu este divizor al lui zero sau adunarea ecuaţiilor sau ambele operaţiuni pot permite scrierea unei ecuaţii de tipul (1) care să conducă la substituirea unei necunoscute atunci rezolvarea unui sistem de ecuatii într-un inel R se poate face ca mai sus.
b) La rezolvarea sistemelor de ecuaţii în inele R care au divizori ai lui zero recomandăm aplicarea *metodei reducerii* doar atunci când inmulţirea ecuaţiilor se face cu elemente care nu sunt divizori ai lui zero. În ceea ce priveşte încercarea de a aplica *regula lui Cramer* ea are succes doar dacă determinantul sistemului este un element inversabil din R, ceea ce în cazul de mai sus are loc. Oricum, sugerăm cititorului ca atunci când nu este posibil să respecte indicaţiile de mai sus, să verifice soluţiile obţinute.

3.25. Indicaţie. $\mathbb{N}$, $\mathbb{N}^*$ şi $\{a\in\mathbb{R}\mid a\geq 0\}$ sunt părţi stabile în $(\mathbb{R},+)$ şi $(\mathbb{R},\cdot)$, dar nu sunt (sub)inele, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sunt părţi stabile în $(\mathbb{C},+)$ şi $(\mathbb{C},\cdot)$ care sunt inele în raport cu operaţiile induse; $\mathbb{Z}$ este subinel, iar $\mathbb{Q}$ şi $\mathbb{R}$ sunt subcorpuri ale lui $(\mathbb{C},+,\cdot)$.

3.26. Răspuns. $2\mathbb{Z}$ este un subinel al lui $(\mathbb{Z},+,\cdot)$ care nu conţine unitatea, iar $\mathbb{Z}$ este subinel al lui $\mathbb{Q}$, dar nu este subcorp.

3.27. Răspuns. $(R,+,\cdot)=(M_2(\mathbb{R}),+,\cdot)$ şi $S=\left\{\begin{pmatrix} a & 0\\ 0 & 0\end{pmatrix}\mid a\in\mathbb{R}\right\}$.

3.28. Indicaţie. Dacă S este un subinel al lui K ce conţine unitatea atunci $|S|\geq 2$ şi

$$a,b\in S\subseteq K \text{ şi } ab=0\Rightarrow a=0 \text{ sau } b=0.$$

Orice subinel al unui inel asociativ, comutativ este inel asociativ, comutativ.

3.29. Soluţia 1: 1) Pentru orice $A=\begin{pmatrix} a & b\\ 2b & a\end{pmatrix}$, $A'=\begin{pmatrix} a' & b'\\ 2b' & a'\end{pmatrix}\in R$ avem

$$A+A'=\begin{pmatrix} a+a' & b+b'\\ 2(b+b') & a+a'\end{pmatrix}\in R \text{ şi } AA'=\begin{pmatrix} aa'+2bb' & ab'+ba'\\ 2(ab'+ba') & aa'+2bb'\end{pmatrix}\in R.$$

Deci R este stabilă în raport cu $+$ şi $\cdot$ din $M_2(\mathbb{Z})$.
2) Arătăm că $(R,+,\cdot)$ este un domeniu de integritate.
a) Din asociativitatea şi comutativitatea operaţiei $+$ din $M_2(\mathbb{Z})$ rezultă asociativitatea şi comutativitatea operaţiei $+$ din R.
b) Avem

$$O_2=\begin{pmatrix} 0 & 0\\ 0 & 0\end{pmatrix}=\begin{pmatrix} 0 & 0\\ 2\cdot 0 & 0\end{pmatrix}\in R,$$

de unde rezultă că O_2 este elementul neutru în $(R,+)$.
c) Pentru orice $A=\begin{pmatrix} a & b\\ 2b & a\end{pmatrix}\in R$ avem $-A=\begin{pmatrix} -a & -b\\ 2(-b) & -a\end{pmatrix}\in R$. Urmează că $-A$ este simetricul lui A în $(R,+)$, ceea ce finalizează demonstaţia faptului că $(R,+)$ este un grup abelian.

d) Din asociativitatea lui $\cdot$ din $M_2(\mathbb{Z})$ rezultă asociativitatea operaţiei $\cdot$ din R.
e) Cu notaţiile de mai sus avem

$$A'A = \begin{pmatrix} aa' + 2bb' & ab' + ba' \\ 2(ab' + ba') & aa' + 2bb' \end{pmatrix}.$$

Folosind calculul lui AA' de la 1), deducem că operaţia $\cdot$ din R este comutativă.
f) Avem

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 \cdot 0 & 1 \end{pmatrix} \in R,$$

de unde urmează că I_2 este elementul neutru în $(R, \cdot)$.
g) Din distributivitatea operaţiei $\cdot$ faţă de $+$ în $M_2(\mathbb{Z})$ rezultă distributivitatea operaţiei $\cdot$ faţă de $+$ în R. Atfel, am arătat că $(R, +, \cdot)$ este inel asociativ, comutativ cu unitate. Evident, $|R| \geq 2$.

Mai trebuie arătat că $(R, +, \cdot)$ nu are divizori ai lui zero. Cu notaţiile de mai sus, presupunem că $A \neq O_2$ (ceea ce este echivalent cu $a \neq 0$ sau $b \neq 0$) şi că $AA' = O_2$, ceea ce este echivalent cu

$$\begin{cases} aa' + 2bb' = 0; \\ ba' + ab' = 0. \end{cases}$$

Aceste relaţii constituie un sistem liniar şi omogen în necunoscutele a' şi b'. Cum $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$, din $a \neq 0$ sau $b \neq 0$ rezultă că sistemul are determinantul

$$d = \begin{vmatrix} a & 2b \\ b & a \end{vmatrix} = a^2 - 2b^2 \neq 0,$$

de unde urmează că singura soluţie a sistemului este soluţia nulă $a' = b' = 0$, ceea ce arată că

$$AA' = O_2 \text{ şi } A \neq O_2 \Rightarrow A' = O_2,$$

adică $(R, +, \cdot)$ nu are divizori ai lui zero. În concluzie, $(R, +, \cdot)$ este un domeniu de integritate.

Soluţia 2: Este suficient să se arate că R este un subinel comutativ, cu cel puţin două elemente, al lui $(M_2(\mathbb{Z}), +, \cdot)$ şi că $(R, +, \cdot)$ nu are divizori ai lui zero. Evident, $R \neq \emptyset$. Cu notaţiile de mai sus, avem

$$A - A' = \begin{pmatrix} a - a' & b - b' \\ 2(b - b') & a - a' \end{pmatrix} \in R$$

şi ca la 1), Soluţia 1, se deduce că $AA' \in R$. Deci R este subinel în $(M_2(\mathbb{Z}), +, \cdot)$. Avem $|R| \geq 2$ şi, ca mai sus, se deduce că $(R, +, \cdot)$ este comutativ şi nu are divizori ai lui zero.

3.30. Arătăm că K este un subinel în $(M_2(\mathbb{Q}), +, \cdot)$. Într-adevăr, $K \neq \emptyset$ şi pentru orice $A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \in K$, $A' = \begin{pmatrix} a' & b' \\ 2b' & a' \end{pmatrix} \in K$ avem

$$A - A' = \begin{pmatrix} a - a' & b - b' \\ 2(b - b') & a - a' \end{pmatrix} \in R \text{ şi } AA' = \begin{pmatrix} aa' + 2bb' & ab' + ba' \\ 2(ab' + ba') & aa' + 2bb' \end{pmatrix} \in K,$$

aşadar, K este subinel al lui $(M_2(\mathbb{Q}),+,\cdot)$. Deci K este stabilă în raport cu operaţiile $+$ şi $\cdot$, iar $(K,+,\cdot)$ este inel asociativ. Cu notaţiile de mai sus avem

$$A'A=\begin{pmatrix} aa'+2bb' & ab'+ba' \\ 2(ab'+ba') & aa'+2bb' \end{pmatrix}=AA'.$$

Rezultă că inelul $(K,+,\cdot)$ este comutativ, iar din

$$I_2=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 2\cdot 0 & 1 \end{pmatrix}\in K,$$

urmează că inelul $(K,+,\cdot)$ este cu unitate. Evident $|K|\geq 2$. A rămas să arătăm că orice $A\in K\setminus\{O_2\}$ este inversabilă în K. Cu notaţiile de mai sus avem

$$A\neq O_2 \Leftrightarrow a\neq 0 \text{ sau } b\neq 0,$$

ceea ce împreună cu $\sqrt{2}\in\mathbb{R}\setminus\mathbb{Q}$ implică $d=\det A=a^2-2b^2\neq 0$. Deci A este inversabilă în $M_2(\mathbb{Q})$ şi

$$A^{-1}=\frac{1}{d}\begin{pmatrix} a & -b \\ -2b & a \end{pmatrix}=\begin{pmatrix} \dfrac{a}{d} & -\dfrac{b}{d} \\ 2\left(-\dfrac{b}{d}\right) & \dfrac{a}{d} \end{pmatrix}\in K,$$

adică A este inversabilă în K. Prin urmare, $(K,+,\cdot)$ este corp comutativ.

3.31. i) Evident $\mathbb{Z}[\sqrt{2}]\neq\emptyset$. Pentru orice $u=a+b\sqrt{2}$, $u'=a'+b'\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$ $(a,a',b,b'\in\mathbb{Z})$ avem:

$$u-u'=(a-a')+(b-b')\sqrt{2}\in\mathbb{Z}[\sqrt{2}],\ uu'=(aa'+2bb')+(ab'+a'b)\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$$

şi $1=1+0\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$. Deci $\mathbb{Z}[\sqrt{2}]$ este subinel şi $1\in\mathbb{Z}[\sqrt{2}]$. Arătăm că subinelul $\mathbb{Z}[\sqrt{2}]$ este generat de $\{1,\sqrt{2}\}$.
1) Evident $\{1,\sqrt{2}\}\subseteq\mathbb{Z}[\sqrt{2}]$.
2) Dacă A este un subinel al lui $(\mathbb{R},+,\cdot)$ şi $\{1,\sqrt{2}\}\subseteq A$ atunci $\mathbb{Z}[\sqrt{2}]\subseteq A$. Într-adevăr, din $1\in A$ şi din faptul că A este subgrup al lui $(\mathbb{R},+)$ rezultă $\mathbb{Z}\subseteq A$. Analog, din $\sqrt{2}\in A$ urmează $\mathbb{Z}\sqrt{2}\subseteq A$, iar din $\mathbb{Z},\mathbb{Z}\sqrt{2}\subseteq A$ şi din stabilitatea lui A faţă de $+$ rezultă $\mathbb{Z}+\mathbb{Z}\sqrt{2}\subseteq A$, adică $\mathbb{Z}[\sqrt{2}]\subseteq A$.

Din 1) şi 2) deducem că $\mathbb{Z}[\sqrt{2}]$ este cel mai mic subinel al lui $(\mathbb{R},+,\cdot)$ care include pe $\{1,\sqrt{2}\}$, adică $\mathbb{Z}[\sqrt{2}]$ este subinelul generat de $\{1,\sqrt{2}\}$. Acest rezultat se poate deduce şi dintr-o teoremă care ne arată că elementele subinelului generat de $\{1,\sqrt{2}\}$ sunt expresiile polinomiale în 1 şi $\sqrt{2}$ cu coeficienţi din $\mathbb{Z}$.
ii) Evident că $|\mathbb{Q}(\sqrt{2})|\geq 2$. Analog cu i) se arată că pentru orice $u,u'\in\mathbb{Q}(\sqrt{2})$ avem $u-u',uu'\in\mathbb{Q}(\sqrt{2})$. Fie $u=a+b\sqrt{2}\in\mathbb{Q}(\sqrt{2})$, $u\neq 0$. Aceasta înseamnă că $a,b\in\mathbb{Q}$ şi $a^2-2b^2\neq 0$ şi astfel,

$$u^{-1}=\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}\in\mathbb{Q}(\sqrt{2}).$$

Deci $\mathbb{Q}(\sqrt{2})$ este subcorp. Arătăm că subcorpul $\mathbb{Q}(\sqrt{2})$ este generat de $\sqrt{2}$.

1) Evident $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.
2) Dacă A este un subcorp al lui $(\mathbb{R}, +, \cdot)$ şi $\sqrt{2} \in A$ atunci $\mathbb{Q}(\sqrt{2}) \subseteq A$. Într-adevăr, din ipoteza că A este subcorp rezultă $1 \in A$ şi că A este subgrup al lui $(\mathbb{R}, +)$ ceea ce implică $\mathbb{Z} \subseteq A$. Tot din ipoteza că A este subcorp rezultă că A^* este subgrup în $(\mathbb{R}^*, \cdot)$ care, împreună cu $\mathbb{Z}^* \subseteq A^*$ implică $\mathbb{Q}^* \subseteq A^*$. Astfel am arătat că $\mathbb{Q} \subseteq A$, iar din $\sqrt{2} \in A$, urmează $\mathbb{Q} + \mathbb{Q}\sqrt{2} \subseteq A$, adică $\mathbb{Q}(\sqrt{2}) \subseteq A$.

Din 1) şi 2) deducem că $\mathbb{Q}(\sqrt{2})$ este cel mai mic subcorp al lui $(\mathbb{R}, +, \cdot)$ care conţine pe $\sqrt{2}$, adică $\mathbb{Q}(\sqrt{2})$ este subcorpul generat de $\sqrt{2}$.
iii) Fie $u = \sqrt[3]{2}$. Evident că $u \in S_1$. Arătăm că $u^2 \notin S_1$. Dacă am avea $u^2 \in S_1$ ar rezulta că $u^2 = a + bu$ cu $a, b \in \mathbb{Z}$, ceea ce implică $u^3 = au + bu^2$, adică

$$2 = au + b(a + bu) = ab + (a + b^2)u,$$

dar u fiind iraţional, urmează $ab = 2$ şi $a + b^2 = 0$. Acest sistem nu are soluţii în $\mathbb{Z}$. Deci S_1 nu este stabilă în raport cu $\cdot$ şi astfel S_1 nu este subinel în $(\mathbb{R}, +, \cdot)$.
iv) Se arată la fel ca şi în iii) că $u = \sqrt[3]{2} \in S_2$, dar $u^2 \notin S_2$.

Observaţii: 1) Subinelul $\mathbb{Z}[\sqrt{2}]$ este generat şi de $\mathbb{Z} \cup \{\sqrt{2}\}$, iar notaţia $\mathbb{Z}[\sqrt{2}]$ semnifică acest fapt.
2) Subcorpul $\mathbb{Q}(\sqrt{2})$ este generat şi de $\mathbb{Q} \cup \{\sqrt{2}\}$, iar notaţia $\mathbb{Q}(\sqrt{2})$ semnifică acest fapt.

3.32. Indicaţie. Această problemă generalizează prima parte a problemei anterioare.

3.33. Indicaţii. Se arată că $\delta(z_1 z_2) = \delta(z_1)\delta(z_2)$ pentru orice $z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$. Dacă z este inversabil şi z^{-1} este inversul său atunci $\delta(z)\delta(z^{-1}) = 1$ în $\mathbb{N}$, ceea ce implcă $\delta(z) = 1$. Reciproc, dacă $\delta(z) = 1$ atunci z este inversabil şi inversul lui z este $\overline{z}$ sau $-\overline{z}$.

3.34. Indicaţie. $a^2 + b^2 = \delta(a + bi) = 1$ $(a, b \in \mathbb{Z}) \Leftrightarrow$ $a + bi \in \{1, -1, i, -i\}$.

3.35. Indicaţie. Şirul puterilor lui $1 + \sqrt{2}$ este un şir infinit de elemente din $\mathbb{Z}[\sqrt{2}]$ ce satisfac condiţia din problema anterioară.

3.36. Indicaţie. a) Se procedează ca în soluţa problemei **3.31** i).
b) Se procedează ca în soluţa problemei **3.31** ii).
e) Se procedează ca în soluţa problemei **3.33**.

3.37. Considerăm ca reprezentanţi pentru numerele raţionale doar fracţii ireductibile şi observăm că dacă A este subinel al lui $(\mathbb{Q}, +, \cdot)$ care conţine o fracţie ireductibilă $\dfrac{p}{q}$ şi pe 1 şi dacă $mp + nq = 1$ $(m, n \in \mathbb{Z})$ atunci A conţine şi pe

$$m \cdot \frac{p}{q} + n = \frac{mp + nq}{q} = \frac{1}{q}\,.$$

Observăm, de asemenea, că cel mai mic subinel al lui $\mathbb{Q}$ ce conţine pe 1 este $\mathbb{Z}$.

Fie P o mulţime de numere prime. Folosind teorema de caracterizare a subinelului se arată că mulţimea $A(P)$ a numerelor raţionale reprezentate prin fracţii ireductibile pentru care divizorii primi ai numitorilor aparţin lui P este un subinel al lui $\mathbb{Q}$. Remarcăm că $\mathbb{Z} \subseteq A(P)$. De asemenea, dacă A este un subinel al lui $\mathbb{Q}$ ce conţine pe 1 şi notăm cu P_A mulţimea numerelor prime care divid numitorul a cel puţin unei fracţii ireductibile din A atunci $A(P_A) = A$. Într-adevăr, este evident că $A \subseteq A(P_A)$, iar dacă

$$\frac{m}{p_1^{\alpha_1} \cdots p_k^{\alpha_k}} \in A(P_A), \text{ cu } \alpha_i \in \mathbb{N}^*, \ (i \in \{1, \ldots, k\})$$

atunci $p_1 \in P_A$, prin urmare există $n_1 \in \mathbb{Z}$, $n_2, \beta_1 \in \mathbb{N}^*$ astfel încât $\dfrac{n_1}{p_1^{\beta_1} n_2} \in A$. Rezultă că $\dfrac{n}{p_1} \in A$, deci $\dfrac{1}{p_1} \in A$. Analog obţinem $\dfrac{1}{p_2}, \ldots, \dfrac{1}{p_n} \in A$, de unde deducem

$$\frac{m}{p_1^{\alpha_1} \cdots p_k^{\alpha_k}} \in A.$$

Aşadar, subinelele lui $\mathbb{Q}$ ce conţin pe 1 sunt subinelele $A(P)$ (inclusiv $A(\emptyset) = \mathbb{Z}$).

3.38. Indicaţie. Se arată că $\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\}$ este subinel în $(\mathbb{R}, +, \cdot)$, include mulţimea $\{1, \sqrt[3]{2}\}$ şi este cel mai mic subinel al lui $(\mathbb{R}, +, \cdot)$ cu această proprietate, deci este subinelul generat de $\{1, \sqrt[3]{2}\}$. Similar se arată că subcorpul lui $(\mathbb{R}, +, \cdot)$ generat de $\{1, \sqrt[3]{2}\}$ coincide cu subcorpul lui $(\mathbb{R}, +, \cdot)$ generat de $\sqrt[3]{2}$ şi este $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$.

3.39. Răspuns. i) $\mathbb{N}^*$; ii) $\mathbb{Z}$; iii) $\mathbb{Q}$.

3.40. i) Determinăm pe $a, b \in \mathbb{R}$ astfel încât $(\mathbb{R}, \perp)$ să fie un grup abelian.
1) Operaţia $\perp$ este asociativă dacă şi numai dacă pentru orice $x, y, z \in \mathbb{R}$ avem:

$$\begin{aligned}(x \perp y) \perp z = x \perp (y \perp z) &\Leftrightarrow (ax + by - 2) \perp z = x \perp (ay + bz - 2) \\ &\Leftrightarrow a^2x + aby - 2a + bz - 2 = ax + aby + b^2z - 2b - 2.\end{aligned}$$

Ţinând seama de faptul că două funcţii polinomiale cu coeficienţi în $\mathbb{R}$ sunt egale dacă şi numai dacă provin din polinoame egale (sau particularizând convenabil pe x, y, z) deducem că $\perp$ este asociativă dacă şi numai dacă a şi b verifică sistemul

$$\begin{cases} a^2 = a \\ -2a = -2b \\ b = b^2 \end{cases} \Leftrightarrow \begin{cases} a^2 = a \\ a = b \\ b = b^2 \end{cases}.$$

Acest sistem are soluţiile $a_1 = b_1 = 0$ şi $a_2 = b_2 = 1$. Pentru prima soluţie avem

$$x \perp y = 2, \ \forall x, y \in \mathbb{R},$$

şi se observă că $(\mathbb{R}, \perp)$ nu are element neutru. Rămâne soluţia a doua care ne dă

$$x \perp y = x + y - 2. \tag{1}$$

2) Operaţia $\perp$ definită de (1) este, evident, comutativă.
3) Există $e_0 \in \mathbb{R}$ astfel încât $e_0 \perp x = x$ pentru orice $x \in \mathbb{R}$ dacă şi numai dacă

$$e_0 + x - 2 = x, \ \forall x \in \mathbb{R},$$

adică $e_0 = 2 \in \mathbb{R}$. Deci $e_0 = 2$ este elementul neutru în $(\mathbb{R}, \perp)$.

4) Arătăm că pentru orice $x \in \mathbb{R}$ există $x' \in \mathbb{R}$ astfel încât $x' \perp x = e_0$. Avem

$$x' \perp x = e_0 \Leftrightarrow x' + x - 2 = 2 \Leftrightarrow x' = 4 - x,$$

ceea ce arată că orice element din $\mathbb{R}$ este simetrizabil în $(\mathbb{R}, \perp)$. Deci $(\mathbb{R}, \perp)$ este un grup abelian dacă şi numai dacă $a = b = 1$.

Determinăm pe $c \in \mathbb{R}$ astfel încât $(\mathbb{R}, \top)$ să fie monoid.

5) Operaţia $\top$ este asociativă dacă şi numai dacă, pentru orice $x, y, z \in \mathbb{R}$ avem

$$\begin{aligned}
(x \top y) \top z = x \top (y \top z) &\Leftrightarrow (xy - 2x - 2y + c) \top z = x \top (yz - 2y - 2z + c) \\
&\Leftrightarrow xyz - 2xz - 2yz + cz - 2xy + 4x + 4y - 2c - 2z + c \\
&= xyz - 2xy - 2xz + cx - 2x - 2yz + 4y + 4z - 2c + c \\
&\Leftrightarrow 4x + (c-2)z = (c-2)x + 4z \Leftrightarrow (c-6)(x-z) = 0\,,
\end{aligned}$$

ceea ce are loc pentru orice $x, z \in \mathbb{R}$ dacă şi numai dacă $c = 6$. Deci $\top$ este asociativă dacă şi numai dacă $c = 6$. În acest caz avem

$$x \top y = xy - 2x - 2y + 6. \tag{2}$$

6) Evident, operaţia $\top$ definită de (2) este comutativă.

7) Există $e_1 \in \mathbb{R}$ astfel încât $e_1 \top x = x$ pentru orice $x \in \mathbb{R}$ dacă şi numai dacă

$$e_1 x - 2e_1 - 2x + 6 = x, \ \forall x \in \mathbb{R},$$

adică $(x-2)(e_1 - 3) = 0$ pentru orice $x \in \mathbb{R}$, ceea ce are loc dacă şi numai dacă $e_1 = 3$. Deci $e_1 = 3$ este elementul neutru în $(\mathbb{R}, \top)$. Prin urmare, $(\mathbb{R}, \top)$ este monoid (comutativ) dacă şi numai dacă $c = 6$.

8) Operaţia definită de (2) este distributivă în raport cu operaţia definită de (1). Într-adevăr, pentru orice $x, y, z \in \mathbb{R}$ avem:

$$\begin{aligned}
x \top (y \perp z) &= x \top (y + z - 2) = xy + xz - 2x - 2x - 2y - 2z + 4 + 6 \\
&= xy + xz - 4x - 2y - 2z + 10, \\
(x \top y) \perp (x \top z) &= (xy - 2x - 2y + 6) \perp (xz - 2x - 2z + 6) \\
&= xy - 2x - 2y + 6 + xz - 2x - 2z + 6 - 2 \\
&= xy + xz - 4x - 2y - 2z + 10,
\end{aligned}$$

ceea ce ne arată că $x \top (y \perp z) = (x \top y) \perp (x \top z)$. Deci pentru $a = b = 1$ şi $c = 6$, $(\mathbb{R}, \perp, \top)$ este inel comutativ. Evident că $|\mathbb{R}| \geq 2$. A mai rămas să arătăm că:

9) Pentru orice $x \in \mathbb{R} \setminus \{e_0\}$ există $x'' \in \mathbb{R}$ astfel încât $x'' \top x = e_1$. Avem:

$$x'' \top x = e_1 \Leftrightarrow x'' x - 2x'' - 2x + 6 = 3 \Leftrightarrow x''(x-2) = 2x - 3$$

şi, cum $x \neq e_0 = 2$, urmează $x'' = \dfrac{2x-3}{x-2} \in \mathbb{R}$. În concluzie, $(\mathbb{R}, \perp, \top)$ este corp dacă şi numai dacă $a = b = 1$ şi $c = 6$.

ii) Condiţii necesare pentru ca f să fie omomorfism sunt

$$\begin{cases} f(0) = e_0 \\ f(1) = e_1 \end{cases} \Leftrightarrow \begin{cases} \beta = 2 \\ \alpha + \beta = 3 \end{cases} \Leftrightarrow \begin{cases} \alpha = 1 \\ \beta = 2 \end{cases},$$

ceea ce ne dă $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x + 2$. Funcţia f este bijectivă deoarece pentru orice $y \in \mathbb{R}$ ecuaţia $f(x) = y$ are soluţia unică $x = y - 2$ în $\mathbb{R}$. Funcţia f este omomorfism de corpuri. Într-adevăr,

$$\begin{aligned} f(x)\perp f(y) &= (x+2)\perp(y+2) = x+2+y+2-2 = x+y+2 = f(x+y), \\ f(x)\top f(y) &= (x+2)\top(y+2) = (x+2)(y+2) - 2(x+2) - 2(y+2) + 6 \\ &= xy + 2x + 2y + 4 - 2x - 4 - 2y - 4 + 6 = xy + 2 = f(xy). \end{aligned}$$

În concluzie, f este izomorfism dacă şi numai dacă $\alpha = 1$ şi $\beta = 2$.

3.41. Indicaţie. Funcţia $f : \mathbb{Z}[\sqrt{2}] \to R$, $f(a + b\sqrt{2}) = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ este izomorfism.

3.42. Indicaţie. Funcţia $f : \mathbb{Q}(\sqrt{2}) \to K$, $f(a + b\sqrt{2}) = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ este izomorfism.

3.43. Indicaţie. Funcţia $f : \mathbb{Z}[\sqrt{d}] \to R$, $f(a + b\sqrt{d}) = \begin{pmatrix} a & b \\ bd & a \end{pmatrix}$ este izomorfism.

3.44. Indicaţie. ii) $f : \mathbb{Q}(\sqrt{d}) \to K$, $f(a + b\sqrt{d}) = \begin{pmatrix} a & b \\ bd & a \end{pmatrix}$ este un izomorfism.

3.45. Presupunem că $f : \mathbb{Z} \to \mathbb{Z}$ este un izomorfism, rezultă că $f(0) = e_0$ şi $f(1) = e_1$, adică $f(0) = -3$ şi $f(1) = -2$. Pentru orice $n \in \mathbb{N}^*$ avem

$$f(n) = f(\underbrace{1 + \cdots + 1}_{n \text{ ori}}) = \underbrace{f(1)\perp \cdots \perp f(1)}_{n \text{ ori}} = (-2)\perp \cdots \perp(-2) = -2n + 3(n-1) = n - 3$$

şi $f(-n)$ coincide cu simetricul lui $f(n) = n - 3$ în $(\mathbb{Z}, \perp)$, adică

$$f(-n) = -6 - f(n) = -6 - (n-3) = -n - 3.$$

Deci $f(x) = x - 3$ pentru orice $x \in \mathbb{Z}$.

Acum arătăm că funcţia f definită mai sus este izomorfism. Într-adevăr, pentru orice $y \in \mathbb{Z}$ ecuaţia $f(x) = y$ are o soluţie unică $x = y + 3 \in \mathbb{Z}$, adică f este bijecţie. În plus, pentru orice $x_1, x_2 \in \mathbb{Z}$ avem

$$f(x_1)\perp f(x_2) = x_1 - 3 + x_2 - 3 + 3 = x_1 + x_2 - 3 = f(x_1 + x_2),$$

$$f(x_1)\top f(x_2) = (x_1 - 3)(x_2 - 3) + 3(x_1 - 3) + 3(x_2 - 3) + 6 = x_1x_2 - 3 = f(x_1x_2),$$

adică f este şi omomorfism. Deci f este izomorfism.

3.46. Indicaţie. Pentru orice $y_i \in R'$ esistă $x_i \in R$ astfel încât $y_i = f(x_i)$ $(i = 1, 2, 3)$ şi, folosind asociativitatea operaţiei $+$ avem:

$$\begin{aligned} (y_1\perp y_2)\perp y_3 &= (f(x_1)\perp f(x_2))\perp f(x_3) = f(x_1 + x_2)\perp f(x_3) = f((x_1 + x_2) + x_3) \\ &= f((x_1 + x_2) + x_3) = f(x_1)\perp f(x_2 + x_3) = f(x_1)\perp(f(x_2)\perp f(x_3)) \\ &= y_1\perp(y_2\perp y_3) \end{aligned}$$

Deci $\perp$ este asociativă. Comutativitatea şi distributivitatea se demonstrează analog. Elementul neutru în $(R, \perp)$ este $f(0)$, iar simetricul lui $f(x)$ în $(\mathbb{R}, \perp)$ este $f(-x)$.

3.47. Indicaţie. $f : \mathbb{N} \to \mathbb{Z}_6$, $f(n) = \widehat{n}$ este un omomorfism surjectiv al lui $(\mathbb{N}, +, \cdot)$ pe $(\mathbb{Z}_6, +, \cdot)$.

3.48. Indicaţie. $f : \mathbb{Z} \to \mathbb{Z}_4$, $f(n) = \widehat{n}$ este un omomorfism surjectiv al lui $(\mathbb{Z}, +, \cdot)$ pe $(\mathbb{Z}_4, +, \cdot)$.

3.49. a) Din $(f(a))^2 = f(a^2) = f(a)$ rezultă $f(a)$ idempotent în R'.
b) Dacă $n \in \mathbb{N}$ şi $a^n = 0$ atunci

$$(f(a))^n = f(a^n) = f(0) = 0',$$

deci $f(a)$ este nilpotent în R'.
c) Oricare ar fi $x' \in R'$, există $x \in R$ astfel încât $x' = f(x)$. Prin urmare, avem

$$f(a)x' = f(a)f(x) = f(ax) = f(xa) = f(x)f(a) = x'f(a),$$

deci $f(a) \in Z(R')$.
d) Dacă x^{-1} e inversul lui x în R atunci $f(x^{-1})$ este inversul lui $f(x)$ în R'.
e) Reciprocele implicaţiilor a), b), c), d) nu sunt, în general, adevărate. De exemplu, $f : \mathbb{Z} \to \mathbb{Z}_{12}$, $f(x) = \widehat{x}$ este un omomorfism surjectiv de inele cu unitate (deci unital), $\widehat{4}$ este idempotent în $\mathbb{Z}_{12}$, dar 4 nu este idempotent în $\mathbb{Z}$, $\widehat{6}$ este nilpotent în $\mathbb{Z}_{12}$, dar 6 nu este nilpotent în $\mathbb{Z}$, iar $\widehat{5}$ este inversabil în $\mathbb{Z}_{12}$, dar 5 nu este inversabil în $\mathbb{Z}$. Un exemplu banal pentru a arăta că reciproca implicaţiei c) nu are loc se obţine în cazul omorfismului (nul) de la un inel necomutativ la inelul nul. Un exemplu nebanal în acest sens va fi prezentat în observaţia de după problema **3.79**.

3.50. Indicaţie. *Unicitatea:* Presupunem că există $\perp$ şi $\top$ care verifică condiţiile cerute. Rezultă că $f(x+y) = f(x)\perp f(y)$ şi $f(xy) = f(x)\top f(y)$ pentru orice $x, y \in R$. Înlocuind pe x cu $f^{-1}(x)$ şi pe y cu $f^{-1}(y)$ primim:

$$x\perp y = f(f^{-1}(x) + f^{-1}(y)) \text{ şi } x\top y = f(f^{-1}(x) \cdot f^{-1}(y)).$$

3.51. Indicaţii. i) Funcţiile $f_i, g : R \to M_n(R)$ $(i \in \{1, \ldots, n\})$ pentru care $f_i(a)$ este matricea care are pe poziţia (i, i) pe a şi 0 în rest, iar

$$g(a) = \begin{pmatrix} a & 0 & \ldots & 0 \\ 0 & a & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & a \end{pmatrix}$$

sunt omomorfisme injective de inele.
ii) Dacă $a, b \in R$ luăm

$$A = \begin{pmatrix} a & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & 0 \end{pmatrix}, \ B = \begin{pmatrix} 0 & \ldots & 0 & b \\ 0 & \ldots & 0 & 0 \\ \vdots & & \vdots & \vdots \\ 0 & \ldots & 0 & 0 \end{pmatrix}$$

şi din $AB = BA$ deducem $ab = 0$.
iii) Pătratul matricei $\begin{pmatrix} 0 & a & 0 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & 0 \end{pmatrix}$ este matricea nulă.

iv) Dacă 1 este unitate în R atunci $I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$ este unitatea lui $M_n(R)$.
Reciproc, dacă $E = (e_{ij})$ este unitate în $M_n(R)$ atunci e_{11} este unitate în R. Aceasta rezultă din egalitatea elementelor din linia 1 – coloana 1 ale matricelor (egale) AE, EA şi A, unde $A = \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$, cu $a \in R$ arbitrar.

v) Matricea $\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$ este element idempotent în $M_n(R)$.

vi) Din iii) rezultă că n nu poate fi mai mare sau egal cu 2.

3.52. Indicaţie. Se arată că $Z(M_n(R)) = \{aI_n \mid a \in Z(R)\}$. Incluziunea $\subseteq$ se poate obţine astfel: orice matrice $A = (a_{ij}) \in Z(M_n(R))$ comută cu orice matrice

$$E_{kl} = (e_{ij}), \text{ cu } e_{ij} = \begin{cases} 0, \text{ dacă } (i,j) \neq (k,l) \\ 1, \text{ dacă } (i,j) = (k,l) \end{cases} \quad (k,l \in \{1,\dots,n\}),$$

prin urmare

$$a_{kk} = a_{ll},\ \forall\, k,l \in \{1,\dots,n\} \text{ şi } a_{kl} = 0,\ \forall\, k,l \in \{1,\dots,n\},\ k \neq l.$$

Notând $a_{11} = \cdots = a_{nn} = a$, din $A(rE_{11}) = (rE_{11})A$ pentru orice $r \in R$ rezultă $a \in Z(R)$.

3.53. Indicaţie. Dacă $q = a_1 + a_2 i + a_3 j + a_4 k \in Z(Q)$, din $qi = iq$ rezultă $a_3 = a_4 = 0$, iar din $qj = jq$ deducem $a_2 = 0$. Prin urmare $Z(Q) = \mathbb{R}$.

3.54. Indicaţii. iii) Se aplică problema **3.49** d) pentru izomorfismul $R \to R'$ şi pentru inversul său. iv) $U(\mathbb{Z}, +, \cdot) \simeq U(\mathbb{Z}_4, +, \cdot)$.

3.55. Indicaţii. i) Se foloseţe faptul că determinantul produsului a două matrice este produsul determinanţilor lor şi faptul că o matrice este inversabilă dacă şi numai dacă determinantul său este nenul.
ii) Din $A + B = AB$ rezultă $(A - I_n)(B - I_n) = I_n$, ceea ce, conform i), conduce la $(B - I_n)(A - I_n) = I_n$. Deci $(A - I_n)(B - I_n) = (B - I_n)(A - I_n)$, ceea ce implică $AB = BA$. În cazul $n = 2$, pentru matricele $A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 2 & -1 \\ 0 & 2 \end{pmatrix}$ avem $A + B = AB$.

3.56. Indicaţii. a) $U(\mathbb{Z}, +, \cdot) = \{-1, 1\}$, $U(M_n(K), +, \cdot) = \{A \in M_n(K) \mid \det A \neq 0\}$, $U(M_n(\mathbb{Z}), +, \cdot) = \{A \in M_n(\mathbb{Z}) \mid \det A = \pm 1\}$.
b) $U(M_n(R), +, \cdot) = \{A \in M_n(R) \mid \det A$ este inversabil în $(R, +, \cdot)\}$, $U(M_n(K), +, \cdot) = \{A \in M_n(K) \mid \det A \neq 0\}$.
c) Pentru orice $m \in \mathbb{Z}$, $\begin{vmatrix} 1 & m & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{vmatrix} = 1.$

Observaţie: Dacă $(R,+,\cdot)$ este un inel asociativ, cu unitate, atunci $U(M_n(R),+,\cdot)$ se notează cu $GL_n(R)$ şi se numeşte *grupul general liniar de gradul* n peste R.

3.57. Indicaţie. $(U(M_n(\mathbb{Z}),+,\cdot),\cdot)$ este infinit, iar $((U(\mathbb{Z},+,\cdot))^{n^2},\cdot)$ este finit.

3.58. Indicaţii. 2) $f : M \to R$ este element inversabil în $(R^M,+,\cdot)$ dacă şi numai dacă $f(M) \subseteq U(R,+,\cdot)$.

3.59. Indicaţie. i) Se ştie că $t_a : R \to R$, $t_a(x) = ax$ este un endomorfism al lui $(R,+)$, iar $\varphi : R \to End(R,+)$, $\varphi(a) = t_a$ este un omomorfism unital injectiv de inele. Condiţia de la i) afirmă că pentru orice $f \in End(R,+)$ avem $f = t_{f(1)}$, deci φ este şi surjectiv.
ii) Dacă $f \in End(R,+)$, $x \in R$ şi inelul $(End(R,+),+,\circ)$ este comutativ, atunci

$$f(x) = f(x\cdot 1) = f(t_x(1)) = (f\circ t_x)(1) = (t_x \circ f)(1) = t_x(f(1)) = x\cdot f(1) = f(1)\cdot x.$$

3.60. Răspuns. $End(\mathbb{Z},+) = \{t_a : \mathbb{Z}\to\mathbb{Z} \mid a \in \mathbb{Z}\}$, $Aut(\mathbb{Z},+) = \{-1_{\mathbb{Z}}, 1_{\mathbb{Z}}\}$, $End(\mathbb{Z},+,\cdot) = \{\theta = t_0, 1_{\mathbb{Z}}\}$, $Aut(\mathbb{Z},+,\cdot) = \{1_{\mathbb{Z}}\}$, $End(\mathbb{Q},+) = \{t_a : \mathbb{Q}\to\mathbb{Q} \mid a \in \mathbb{Q}\}$, $Aut(\mathbb{Q},+) = \{t_a : \mathbb{Q}\to\mathbb{Q} \mid a \in \mathbb{Q}^*\}$, $End(\mathbb{Q},+,\cdot) = \{\theta = t_0, 1_{\mathbb{Z}}\}$, $Aut(\mathbb{Q},+,\cdot) = \{1_{\mathbb{Z}}\}$, $End(\mathbb{Z}_n,+) = \{t_{\widehat{a}} : \mathbb{Z}_n \to \mathbb{Z}_n \mid \widehat{a} \in \mathbb{Z}_n\}$, $Aut(\mathbb{Z}_n,+) = \{t_{\widehat{a}} \mid (a,n) = 1\}$, $End(\mathbb{Z}_n,+,\cdot) = \{t_{\widehat{a}} \mid \widehat{a} \text{ idempotent în } \mathbb{Z}_n\}$, $Aut(\mathbb{Z}_n,+,\cdot) = \{1_{\mathbb{Z}_n}\}$.

3.61. Indicaţie. Dacă $*$ este o operaţie binară pe $\mathbb{Z}$ astfel încât $(\mathbb{Z},+,*)$ să fie un inel, din distributivitatea operaţiei $*$ faţă de $+$ avem pentru orice $m,n \in \mathbb{Z}$

$$m*n = (\underbrace{\widehat{1}+\cdots+\widehat{1}}_{m \text{ ori}}) * (\underbrace{\widehat{1}+\cdots+\widehat{1}}_{n \text{ ori}}) = \underbrace{\widehat{1*1}+\cdots+\widehat{1*1}}_{mn \text{ ori}} = mn(1*1),$$

prin urmare operaţia $*$ este determinată de $1*1$. Se verifică uşor că pentru orice $a \in \mathbb{Z}$, operaţia $*$ definită prin $m*n = mna$ determină o structură de inel pe $\mathbb{Z}$. Inelul astfel obţinut este cu unitate dacă şi numai dacă $a \in \{-1,1\}$.

3.62. Indicaţie. Fie $*$ o operaţie (binară) pe $\mathbb{Z}_n$ astfel încât $(A = \mathbb{Z}_n,+,*)$ este un inel cu unitatea e. Dacă $m = \mathrm{ord}_{(\mathbb{Z}_n,+)}(e)$ atunci $m|n$. Avem, de asemenea, $n|m$ deoarece

$$m\cdot\widehat{1} = \underbrace{\widehat{1}+\cdots+\widehat{1}}_{m \text{ ori}} = \underbrace{\widehat{1}*e+\cdots+\widehat{1}*e}_{m \text{ ori}} = \widehat{1}*(\underbrace{\widehat{e}+\cdots+\widehat{e}}_{m \text{ ori}}) = \widehat{1}*(m\cdot e) = \widehat{1}*\widehat{0} = \widehat{0}.$$

Rezultă că $\mathbb{Z}_n = \{\widehat{0},\widehat{1},\ldots,\widehat{n-1}\} = \{0\cdot e, 1\cdot e,\ldots,(n-1)e\} = A$ şi se demonstrează că $\varphi : \mathbb{Z}_n \to A$, $\varphi(\widehat{k}) = k\cdot e$ este un izomorfism de inele.

3.63. Indicaţii. Toate grupurile cu p elemente sunt abeliene şi sunt izomorfe cu $(\mathbb{Z}_p,+)$, iar pe acest grup se cunosc două structuri neizomorfe de inel: inelul de pătrat nul şi inelul $(\mathbb{Z}_p,+,\cdot)$ al claselor de resturi modulo p. Se poate arăta că, abstracţie făcând de un izomorfism, acestea sunt singurele structuri de inel ce se pot defini pe $\mathbb{Z}_p$ astfel: presupunând că $*$ este o operaţie binară pentru care există $a,b \in \mathbb{Z}_p$ astfel încât $(\mathbb{Z}_p,+,*)$ să fie inel şi $a*b \neq \widehat{0}$, submulţimea $A = \{x \in \mathbb{Z}_p \mid a*x = \widehat{0}\} \neq \mathbb{Z}_p$ este un subinel al lui $(\mathbb{Z}_p,+,\cdot)$. Dar atunci $A \neq \mathbb{Z}_p$ este un subgrup normal al grupului simplu $(\mathbb{Z}_p,+)$. Rezultă $A = \{\widehat{0}\}$, prin urmare a nu este divizor al lui zero la stânga. Urmează că $a \notin B = \{x \in \mathbb{Z}_p \mid x*a = 0\}$ şi, ca mai sus, deducem că a nu este nici divizor al lui zero la dreapta. Aşadar, cu a se poate simplifica în $(\mathbb{Z}_p,+,*)$. Atunci egalităţile $f(x) = x*a$ şi $g(x) = a*x$ definesc două funcţii injective $f,g : \mathbb{Z}_p \to \mathbb{Z}_p$ care vor fi implicit şi surjective. Atunci există $e \in \mathbb{Z}_p$ astfel încât $a*e = a$, iar cum orice $b \in \mathbb{Z}_p$ se scrie sub forma $b = x*a$ cu $x \in \mathbb{Z}_p$, vom avea $b*e = (x*a)*e = x*(a*e) = x*a = b$, deci e este element neutru la dreapta pentru $*$. Analog se arată că $*$ admite element neutru la stânga. Deci $(\mathbb{Z}_p,+,*)$ este inel cu unitate. Concluzia dorită urmează aplicând problema **3.62**.

3.64. Indicaţie. Dacă f este un omomorfism al grupului $(\mathbb{Q},+)$ în $(\mathbb{C},+)$ atunci

$$f(x) = f(1)x,\ \forall\, x \in \mathbb{Q}.$$

Dacă, în plus, $f(1 \cdot 1) = f(1) \cdot f(1)$ atunci $f(1) \in \{0,1\}$. Cerând ca f să fie nenul, rămâne

$$f(x) = x,\ \forall\, x \in \mathbb{Q}.$$

3.65. Presupunem că $f : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ este un automorfism. Se deduce, ca în indicaţia problemei anterioare, că $f(x) = x$ pentru orice $x \in \mathbb{Q}$. De aici şi din $(\sqrt{2})^2 = 2$ rezultă $[f(\sqrt{2})]^2 = 2$, ceea ce implică $f(\sqrt{2}) \in \{-\sqrt{2}, \sqrt{2}\}$. Deci $f \in \{f_1, f_2\}$, unde $f_1(a+b\sqrt{2}) = a+b\sqrt{2}$ şi $f_2(a+b\sqrt{2}) = a-b\sqrt{2}$. Din $f_1 = 1_{\mathbb{Q}(\sqrt{2})}$ rezultă că f_1 este automorfism. Avem $f_2 \circ f_2 = 1_{\mathbb{Q}(\sqrt{2})}$, ceea ce implică f_2 bijecţie şi $f_2^{-1} = f_2$. Se verifică uşor că f_2 este omomorfism. Deci şi f_2 este automorfism. În concluzie, automorfismele corpului $\mathbb{Q}(\sqrt{2})$ sunt f_1 şi f_2.

3.66. Fie f un endomorfism al lui $(\mathbb{R},+,\cdot)$. Avem $(f(1))^2 = f(1)$, deci $f(1) = 1$ sau $f(1) = 0$, caz în care f este omomorfismul nul. Dacă f este nenul atunci f este injectiv. Se arată uşor că $f(x) = x$ pentru orice $x \in \mathbb{Q}$, iar dacă $x \in \mathbb{R}$, $x > 0$ atunci $f(x) = f((\sqrt{x})^2) = (f(\sqrt{x}))^2 > 0$ (faptul că inegalitatea e strică provine din injectivitatea lui f). Rezultă că pentru orice $x, y \in \mathbb{R}$ cu $x < y$ avem

$$f(y) - f(x) = f(y - x) > 0,$$

deci f este strict crescătoare. Considerând pentru un $a \in \mathbb{R} \setminus \mathbb{Q}$ şirul $(a'_n)_{n\in\mathbb{N}}$ al aproximărilor sale raţionale prin lipsă şi şirul $(a''_n)_{n\in\mathbb{N}}$ al aproximărilor sale raţionale prin adaos, obţinem $a'_n \leq a \leq a''_n$ pentru orice $n \in \mathbb{N}$, prin urmare

$$a'_n = f(a'_n) \leq f(a) \leq f(a''_n) = a''_n$$

pentru orice $n \in \mathbb{N}$. Trecând la limită obţinem $f(a) = a$. Deci $f = 1_{\mathbb{R}}$.

3.67. Indicaţii. Dacă f este omomorfism al lui $(\mathbb{Z}_m,+)$ în $(\mathbb{Z}_n,+)$ atunci $f(\overline{x}) = x\widehat{a}$, unde $\widehat{a} = f(\overline{1})$ verifică egalitatea $m \cdot \widehat{a} = \widehat{1}$. Dacă, în plus, f este omomorfism al lui $(\mathbb{Z}_m,\cdot)$ în $(\mathbb{Z}_n,\cdot)$ atunci $\widehat{a}$ este idempotent în $\mathbb{Z}_n$. Dacă, de exemplu, $(m,n) = 1$ atunci $\widehat{a} = \widehat{0}$ şi singurul omomorfism este cel nul.

3.68. Cum $(\mathbb{Q},+,\cdot)$ este un corp, omomorfismele g, h sunt fie nule, fie injective. Dacă g, h sunt ambele nule, concluzia e imediată. Considerăm contrariul, iar din $g(n) = h(n)$ pentru orice $n \in \mathbb{Z}$ deducem că g şi h sunt injective. Atunci subinelele $g(\mathbb{Q})$ şi $h(\mathbb{Q})$ ale lui R sunt corpuri cu aceeaşi unitate $1' = g(1) = h(1)$, iar dacă A este subinelul lui R generat de $g(\mathbb{Q}) \cup h(\mathbb{Q})$ atunci A este, în raport cu operaţiile induse din $(R,+,\cdot)$, un inel cu unitatea $1'$ şi omomorfismele g, h pot fi privite ca omomorfisme (unitale) cu codomeniul A. Atunci $g(n), h(n)$ sunt inversabile în A pentru orice $n \in \mathbb{Z}^*$ şi, în plus,

$$g\left(\frac{1}{n}\right) = g\left(n^{-1}\right) = [g(n)]^{-1} = [h(n)]^{-1} = h\left(n^{-1}\right) = h\left(\frac{1}{n}\right).$$

Astfel, pentru orice $m, n \in \mathbb{Z},\ n \neq 0$, avem

$$g\left(\frac{m}{n}\right) = g(m)g\left(\frac{1}{n}\right) = h(m)h\left(\frac{1}{n}\right) = h\left(\frac{m}{n}\right).$$

Observaţie: Din problema de mai sus rezultă că omomorfismul de incluziune $\mathbb{Z} \to \mathbb{Q}$ este un exemplu de omomorfism nesurjectiv de inele cu care se poate simplifica la dreapta (într-o compunere de omomorfisme de inele).

3.69. Indicaţii. Subinelele lui $(\mathbb{Z}, +, \cdot)$ sunt de forma $n\mathbb{Z}$, cu $n \in \mathbb{N}$, iar dacă $n \in \mathbb{N}$ idealele inelului $(n\mathbb{Z}, +, \cdot)$ coincid cu subinelele sale şi sunt de forma $(mn)\mathbb{Z}$, cu $m \in \mathbb{N}$.

3.70. Indicaţii. i) Dacă $r, r' \in U : V$ şi $a \in R$ atunci, pentru orice $x \in V$, avem $rx, r'x \in U$ şi $ax \in V$, prin urmare, $(r - r')x = rx - r'x \in U$, $(ar)x = a(rx) \in U$ şi $(ra)x = r(ax) \in U$.
ii) Dacă $r \in U : (V_1 + V_2)$ atunci $r(x_1 + x_2) \in U$ pentru orice $x_1 \in V_1$, $x_2 \in V_2$. Luând $x_1 = 0$, respectiv $x_2 = 0$, obţinem $r \in U : V_2$, respectiv $r \in U : V_1$.
iii) $U : (U + V) = (U : U) \cap (U : V) = R \cap (U : V) = U : V$.
iv) Cum $rx \in V$ pentru orice $r \in R$, $x \in V$, din $V \subseteq U$ rezultă $U : V = R$. Reciproc, dacă R are unitate, $1 \in U : V$ implică $V = 1 \cdot V \subseteq U$.
v) $n\mathbb{Z} : m\mathbb{Z} = \{r \in \mathbb{Z} \mid rm\mathbb{Z} \subseteq n\mathbb{Z}\} = \{r \in \mathbb{Z} \mid n|rm\} = \left\{r \in \mathbb{Z} \mid \left.\frac{[m,n]}{m}\right| r\right\} = \frac{[m,n]}{m}\mathbb{Z}$.

3.71. Indicaţii. Dacă $r, s, a \in R$, $m, n \in \mathbb{N}$ şi $r^m, s^n \in I$ atunci folosind problema **3.7** şi faptul că I este ideal deducem că $(r - s)^{m+n} \in I$, iar din comutativitatea lui R şi I ideal, avem $(ar)^m = a^m r^m \in I$ şi $(ra)^m = r^m a^m \in I$. Egalităţile din enunţ se demonstrează verificând dubla incluziune.

3.72. Răspuns. În general, nu. De exemplu, $A = \left\{\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R}\right\}$ este ideal stâng în inelul $(M_2(\mathbb{R}), +, \cdot)$ şi $B = \left\{\begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} \mid a, b \in \mathbb{R}\right\}$ este ideal drept, dar intersecţia $A \cap B = \left\{\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R}\right\}$ nu este ideal în $(M_2(\mathbb{R}), +, \cdot)$.

3.73. Indicaţii. Trebuie verificat că pentru orice ideale U, V, T ale unui inel R cu $U \subseteq T$ avem $U + (V \cap T) = (U + V) \cap T$. Submodularitatea (adică incluziunea $\subseteq$) este verificată de orice latice, iar incluziunea $\supseteq$ se demostrează ca în soluţia problemei **2.141**.
Altfel: laticea idealelor unui inel este sublatice a laticii subgrupurilor grupului abelian $(R, +)$, care este modulară.

3.74. Indicaţii. Se poate folosi problema **3.71** de unde rezultă că mulţimea elementelor nipotente coincide cu $\sqrt{\{0\}}$, deci este un ideal al lui R. Se poate da şi o soluţie care să nu facă apel la problema **3.71** astfel: dacă $a, b \in R$ sunt elemente nilpotente, $m, n \in \mathbb{N}$, $a^m = 0 = b^n$ şi $r \in R$ atunci folosind problema **3.7** se arată că $(a - b)^{m+n} = 0$, iar $(ra)^m = r^m a^m = 0$.

3.75. Dacă $a \in R$ este nilpotent şi $a^n = 0$ $(n \in \mathbb{N})$ atunci

$$(1 + a)(1 - a + a^2 - \cdots + (-1)^{n-1}a^{n-1}) = 1 + (-1)^{n-1}a^n = 1,$$

deci $1 + a$ este inversabil. Dacă $x, y \in R$ cu x inversabil şi y nilpotent atunci, conform problemei anterioare, $x^{-1}y$ este un element nilpotent al lui R, prin urmare $x + y = x(1 + x^{-1}y)$ este inversabil fiind produsul a două elemente inversabile.

3.76. Indicaţii. i) Un inel Boole nenul simplu este un inel asociativ şi comutativ simplu care nu este de pătrat nul, deci un corp (vezi [34, Teorema 3.4.4]). Se foloseşte apoi problema **3.18**.
ii) Un raţionament inductiv simplu arată că este destul să arătăm că orice ideal U generat de o mulţime cu două elemente $\{a, b\} \subseteq R$ este principal. Cum orice element din R este idempotent (şi R este comutativ) avem $a = a(a + b - ab)$ şi $b = b(a + b - ab)$, prin urmare

$$U = aR + bR = (a + b - ab)R.$$

3.77. Indicaţii. Dacă U_1, U_2 sunt ideale în R_1, respectiv R_2 atunci $U_1 \times U_2$ este ideal în $R_1 \times R_2$. Reciproc, dacă U este un ideal al lui $R_1 \times R_2$ şi $p_i : R_1 \times R_2 \to R_i$ $(i = 1, 2)$ sunt proiecţiile canonice atunci $p_i(U)$ este ideal în $p_i(R_1 \times R_2) = R_i$ $(i = 1, 2)$ şi avem $U = p_1(U) \times p_2(U)$. Într-adevăr, incluziunea $U \subseteq p_1(U) \times p_2(U)$ este evidentă, iar dacă $(x, y) \in p_1(U) \times p_2(U)$ atunci există $x' \in R_1$, $y' \in R_2$ pentru care $(x, y'), (x', y) \in U$, ceea ce implică $(x, y) = (1, y)(x, y') + (x, 1)(x', y) - (x, y')(x', y) \in U$.

3.78. Indicaţie. Transformările unei matrice menţionate în enunţ ale se numesc transformări elementare. Pentru a efectua o transformare elementară, referitoare la linii (coloane), asupra unei matrice A se poate proceda astfel: se realizează transformarea respectivă asupra matricei unitate I_n şi înmulţim pe A cu matricea astfel obţinută pe stânga (dreapta). Evident, dacă $A \in \mathcal{U}$ atunci matricea rezultată este tot în $\mathcal{U}$.

3.79. Indicaţie. $T/U = \{A + U \mid A$ matrice diagonală$\}$ ($A = (a_{ij})$ este diagonală dacă $a_{ij} = 0$ pentru orice $i, j \in \{1, \ldots, n\}$, $i \neq j$).

Observaţie: Proiecţia canonică $T \to T/U$ este un omomorfism surjectiv care duce un inel necomutativ într-unul comutativ şi implicit elemente din $T \setminus Z(T)$ în $Z(T/U) = T/U$.

3.80. Indicaţii. i) Se arată uşor că dacă U este ideal al lui R atunci $M_n(U)$ este ideal în $M_n(R)$. Reciproc, dacă $\mathcal{U}$ este ideal în $M_n(R)$ atunci

$$U = \{a \in R \mid \exists A = (a_{ij}) \in \mathcal{U} \text{ cu } a_{11} = a\}$$

este un ideal al lui R şi $M_n(U) = \mathcal{U}$. Într-adevăr, dacă $A = (a_{ij}) \in \mathcal{U}$ atunci permutând succesiv linia 1 cu linia i şi coloana 1 cu coloana j se obţine o matrice din $\mathcal{U}$ care are pe a_{ij} în colţul stânga-sus, deci $a_{ij} \in U$. Dacă $B = (b_{ij}) \in M_n(U)$ atunci, pentru orice i şi j există o matrice $B_{ij} \in \mathcal{U}$ care are pe b_{ij} în colţul stânga-sus. Dacă luăm matricea $X = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & 0 \end{pmatrix}$ atunci $XB_{ij}X \in \mathcal{U}$ este matricea care are pe b_{ij} în poziţia (i, j) şi 0 în rest. Suma acestor matrice este chiar B şi aparţine lui $\mathcal{U}$.
ii) Corespondenţa $(a_{ij}) \mapsto (a_{ij} + U)$ defineşte un omomorfism surjectiv de inele f al lui $(M_n(R), +, \cdot)$ în $(M_n(R/U), +, \cdot)$. Aplicăm prima teoremă de izomorfism pentru inele lui f şi obţinem izomorfismul căutat.
iii) şi iv) urmează din i)
v) $\mathcal{U} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(2\mathbb{Z}) \mid 4|a \right\}$ este ideal în $M_2(2\mathbb{Z})$ pentru care nu există nici un ideal $\mathcal{U}$ al lui $2\mathbb{Z}$ cu proprietatea că $M_n(U) = \mathcal{U}$.
vi) Dacă U este ideal stâng al lui R atunci $M_n(U)$ este ideal stâng al lui $M_n(R)$, fără ca reciproca să fie, în general, adevărată. De exemplu, $\mathcal{U} = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ este un

ideal stâng al inelului $M_2(\mathbb{R})$, dar singurele ideale (unilaterale) ale lui $\mathbb{R}$ sunt $\{0\}$ şi $\mathbb{R}$, iar $M_n(\{0\}) \neq U \neq M_n(\mathbb{R})$. Menţionăm că acest exemplu poate fi generalizat pentru matrice pătrate de orice ordin $n \in \mathbb{N}$, $n \geq 2$, cu coeficienţi într-un corp.

3.81. Indicaţii. i) Se arată că $f : \mathcal{P}(M) \to \mathcal{P}(M \setminus N)$, $f(X) = X \cap (M \setminus N) = X \setminus N$ este un omomorfism surjectiv de inele şi se aplică prima teoremă de izomorfism.
ii) Dacă $N \subseteq M$, se verifică uşor că $\mathcal{P}(N)$ este ideal al lui $\mathcal{P}(M)$. Dacă $\mathcal{U}$ este un ideal al lui $\mathcal{P}(M)$ şi $X, Y \in \mathcal{U}$ atunci $X \cup Y = (X + Y) + (X \cdot Y) \in \mathcal{U}$. Inductiv, se obţine că $\mathcal{U}$ este închis la reuniuni finite, prin urmare, cum M este finită, $\mathcal{U}$ este finită, deci $N = \bigcup_{X \in \mathcal{U}} X \in \mathcal{U}$. De asemenea, dacă $X \in \mathcal{U}$ şi $Z \subseteq X$ atunci $Z = X \cap Z = X \cdot Z \in \mathcal{U}$. Rezultă că $\mathcal{P}(N) \subseteq \mathcal{U}$ şi cum $X \in \mathcal{U}$ implică $X \subseteq N$ (adică $X \in \mathcal{P}(N)$) avem $\mathcal{U} = \mathcal{P}(N)$.
iii) Dacă M este infinită, $\mathcal{U} = \{X \in \mathcal{P}(M) \mid X \text{ finită}\}$ este un ideal infinit al lui $\mathcal{P}(M)$, iar dacă ar exista $N \subseteq M$ pentru care $\mathcal{U} = \mathcal{P}(N)$ atunci $N \in \mathcal{U}$ ar fi finită, deci $\mathcal{P}(N) = \mathcal{U}$ este finită, contradicţie.

3.82. Indicaţie. Se aplică prima teoremă de izomorfism omomorfismului de inele rezultat din compunerea $R \xrightarrow{f} R' \xrightarrow{p'} R'/f(U)$ (p' este proiecţia canonică).

3.83. Indicaţie. Dacă $x \in R$ este un nondivizor al lui zero cu $\text{ord}_{(R,+)}(x) = n \in \mathbb{N}^*$ şi $y \in R$ atunci $0 = (nx)y = x(ny)$, prin urmare $ny = 0$.

Observaţii: a) Noţiunea de caracteristică se defineşte şi pentru inele $(R, +, \cdot)$ care nu au unitate astfel: dacă mulţimea $\{\text{ord}_{(R,+)}(x) \mid x \in R\}$ este o submulţime mărginită a lui $\mathbb{N}^*$ atunci caracteristica inelului R este cel mai mic multiplu comun al numerelor naturale $\text{ord}_{(R,+)}(x)$ $(x \in R)$; în caz contrar, caracteristica inelului R este ∞ (sau 0).
b) Din problema de mai sus rezultă că toţi nondivizorii lui zero dintr-un inel R au acelaşi ordinîn $(R, +)$, egal cu caracteristica inelului (şi cu ordinul unităţii în $(R, +)$, dacă aceasta există).

3.84. Indicaţie. Din problema anterioară rezultă că toate elementele nenule ale unui corp K au acelaşi ordin în grupul $(K, +)$, aşadar, pentru $a, b \in K^*$ nu putem avea $2a = 3b = 0$.

3.85. Răspuns. Dacă $0 = 1$ atunci caracteristica inelului este 1, în caz contrar este 2.

3.86. Răspuns. $\text{char}(\mathbb{Z}_m \times \mathbb{Z}_n, +, \cdot) = [m, n]$ (am notat cu $\text{char} R$ caracteristica inelului R).

3.87. Răspuns. $\text{char}(\mathbb{Z} \times \mathbb{Z}) = \text{char}(\mathbb{Z}_2 \times \mathbb{Z}) = \text{char}(\mathbb{Q} \times \mathbb{Z}_4) = \text{char}(End(\mathbb{Z}, +)) = \infty$, $\text{char}(End(\mathbb{Z}_3, +)) = 3$.

3.88. Răspuns. Orice inel Boole infinit (de exemplu, inelul $(\mathcal{P}(M), +, \cdot)$ din problema **3.4** cu M infinită), $\text{char}\, \mathbb{Z}_n[X] = n$ $(n \in \mathbb{N},\ n \geq 2)$.

3.89. Indicaţie. Dacă p este prim, $\text{char}\, \mathbb{Z}_p[X] = p$, $\text{char}(\mathbb{Z}_p \times \mathbb{Z}_p) = [p, p] = p$, dar inelele $(\mathbb{Z}_p[X], +, \cdot)$ şi $(\mathbb{Z}_p \times \mathbb{Z}_p, +, \cdot)$ nu sunt corpuri.

3.90. Indicaţie. Pentru ca mulţimea $\{0, 1\}$ să fie parte stabilă în $(K, +)$ este necesar (şi suficient) ca $1 + 1 = 0$. De aici rezultă că $\{0, 1\}$ este subcorp în K atunci şi numai atunci când $\text{char} K = 2$.

3.91. Indicaţie. Suma elementelor de pe prima diagonală a matricei AB este egală cu suma elementelor de pe prima diagonală a matricei BA, prin urmare, suma elementelor de pe prima diagonală a matricei $AB - BA$ este 0, iar suma elementelor de pe prima diagonală a matricei I_n este $n \cdot 1 \neq 0$.

3.92. Dacă R este de caracteristică $p > 2$ atunci ecuaţia $x^2 = 1$ are în $U(R, +, \cdot)$ două soluţii $x_1 = 1 \neq -1 = x_2$, iar ecuaţia $2x = 0$ are în $(R, +)$ o singură soluţie $x = 0$. Dacă R este de caracteristică 2 atunci ecuaţia $x^2 = 1$ are în $U(R+, \cdot)$ o singură soluţie $x = 1 = -1$, iar ecuaţia $2x = 0$ are în $(R, +)$ cel puţin două soluţii $x_1 = 0$ şi $x_2 = 1$. Dacă ar exista un izomorfism $\varphi : U(R, +, \cdot) \to R$ atunci acesta ar aplica bijectiv mulţimea soluţiilor ecuaţiei $x^2 = 1$ pe mulţimea soluţiilor ecuaţiei $2x = 0$. Deci cele două ecuaţii ar avea acelaşi număr de rădăcini, ceea ce nu este adevărat. Rezultă că grupurile $(U(R, +, \cdot), \cdot)$ şi $(R, +)$ nu sunt izomorfe.

3.93. Indicaţie. Se foloseşte problema anterioară.

3.94. Indicaţie. Se foloseşte definiţia produsului restrâns de grupuri şi definiţia polinoamelor ca şiruri de suport finit.

3.95. Dacă $g = b_0 + b_1X + \cdots \in R[[X]]$ şi $fg = 1$ atunci $a_0b_0 = 1$ deci a_0 este element inversabil în R. Invers, dacă a_0 este inversabil, luăm $b_0 = a_0^{-1}$ şi arătăm, prin inducţie după n, că pentru orice $n \in \mathbb{N}^*$ există $b_n \in R$ astfel încât $a_0b_n + a_1b_{n-1} + \cdots + a_nb_0 = 0$. Pentru $n = 1$, $b_1 = -a_0^{-1}a_1b_0 = -a_1b_0^2$ verifică egalitatea $a_0b_1 + a_1b_0 = 0$, iar dacă presupunem că $b_1, \ldots, b_{n-1}$ sunt determinaţi atunci

$$b_n = -a_0^{-1}(a_1b_{n-1} + \cdots + a_nb_0) \in R.$$

Seria formală $g = b_0 + b_1X + \cdots$ din $R[[X]]$ verifică egalitatea $fg = 1$.

3.96. Indicaţie. Se foloseşte faptul că dacă $(R, +, \cdot)$ este un domeniu de integritate atunci $U(R[X], +, \cdot) = U(R, +, \cdot)$.

3.97. Răspuns. $f = 1 + x \in \mathbb{R}[X]$ este inversabil în inelul $(\mathbb{R}[[X]], +, \cdot)$, dar nu este inversabil în inelul $(\mathbb{R}[X], +, \cdot)$.

3.98. Indicaţie. Fie $h = a_0 + a_1X + \cdots + a_nX^n$ cu $a_0, \ldots, a_n \in \mathbb{Z}_4$, $n \in \mathbb{N}^*$, $n \geq 3$. Avem $(\widehat{3} + \widehat{2}X + \widehat{2}X^2)h = \widehat{1}$ dacă şi numai dacă

$$\begin{aligned}
&\widehat{3}a_0 = \widehat{1},\\
&\widehat{3}a_1 + \widehat{2}a_0 = \widehat{0}\\
&\widehat{3}a_2 + \widehat{2}a_1 + \widehat{2}a_0 = \widehat{0}\\
&\widehat{3}a_3 + \widehat{2}a_2 + \widehat{2}a_1 = \widehat{0}\\
&\vdots\\
&\widehat{2}a_n + \widehat{2}a_{n-1} + \widehat{2}a_{n-2} = \widehat{0}\\
&\widehat{2}a_n + \widehat{2}a_{n-1} = \widehat{0}\\
&\widehat{2}a_n = \widehat{0}.
\end{aligned}$$

Rezultă că $a_0 = \widehat{3}$, $a_1 = \widehat{2}$, $a_2 = \widehat{2}$ şi $a_3 = \cdots = a_n = \widehat{0}$, deci $h = \widehat{2}X^2 + \widehat{2}X + \widehat{3}$.

3.99. a) Să remarcăm că un element din R este nilpotent în R dacă şi numai dacă este nilpotent în $R[X]$. Fie $i \in \{1, \dots, n\}$. Dacă a_i este nilpotent în $R[X]$ atunci, conform problemei **3.74**, $a_i X^i$ este nilpotent în $R[X]$, deci $a_1 X + \dots + a_n X^n$ este nilpotent în $R[X]$. Dacă a_0 este inversabil atunci, aplicând problema **3.75**, rezultă că f este inversabil în $R[X]$. Reciproc, să considerăm că există un polinom $g = b_0 + b_1 X + \dots + b_m X^m$ ($b_0, b_1, \dots, b_m \in R$) astfel încât $fg = 1$. Atunci

$$\begin{aligned}
&a_0 b_0 = 1,\\
&a_1 b_0 + a_0 b_1 = 0\\
&\vdots\\
&a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m = 0\\
&a_n b_{m-1} + a_{n-1} b_m = 0\\
&a_n b_m = 0.
\end{aligned}$$

Din prima egalitate deducem că a_0 şi b_0 sunt inversabile. Înmulţind penultima egalitate cu a_n şi ţinând cont de ultima, obţinem $a_n^2 b_{n-1} = 0$, care, împreună cu ultima egalitate şi cu cea rezultată din antepenultima prin înmulţire cu a_n^2, implică $a_n^3 b_{m-2} = 0$. Procedând în continuare ca mai sus se ajunge la egalitatea $a_n^{m+1} b_0 = 0$, adică la $a_n^{m+1} = 0$ şi astfel, a_n este nilpotent. Urmează că $a_n X^n$ este nilpotent, deci polinomul

$$f_1 = f - a_n X^n = a_0 + a_1 X + \dots + a_{n-1} X^{n-1}$$

este, de asemenea, inversabil, ca fiind suma dintre un element inversabil şi unul nilpotent. Ca mai sus, se arată că aceasta conduce la faptul că a_{n-1} este nilpotent. Aplicând succesiv acest raţionament se arată că $a_{n-2}, \dots, a_1$ sunt nilpotente.
b) Dacă $a_0, a_1, \dots, a_n$ sunt nilpotente, se arată, ca la a), că $a_1 X + \dots + a_n X^n$ este nilpotent, aşadar f este nilpotent fiind sumă a două elemente nilpotente. Reciproc, dacă f este nilpotent atunci $-1 + f = (-1 + a_0) + a_1 X + \dots + a_n X^n$ este suma dintre un element inversabil şi unul nilpotent, prin urmare este inversabil. Rezultă că $a_1, \dots, a_n$ sunt elemente nilpotente. Dar atunci şi $a_1 X + \dots + a_n X^n$ este nilpotent, deci şi $a_0 = f - (a_1 X + \dots + a_n X^n)$ este nilpotent.

3.100. Indicaţie. Se foloseşte caracterizarea elementelor inversabile din $\mathbb{Z}_n$, problema anterioară şi problema **3.15** şi se deduce

$$U(\mathbb{Z}_n[X]) = \{\widehat{a_0} + \widehat{a_1} X + \dots + \widehat{a_n} X^n \mid (a_0, n) = 1,\ p_1 \cdots p_k | a_i,\ i \in \{1, \dots, n\},\ n \in \mathbb{N}^*\},$$

unde $p_1, \dots, p_k$ sunt divizorii primi (distincţi) ai lui n.

3.101. Considerăm $f = a_0 + a_1 X + \dots + a_n X^n$, cu $a_0, \dots, a_n \in R$, $a_n \neq 0$ şi $g = b_0 + b_1 X + \dots + b_m X^m$, cu $b_0, b_1, \dots, b_m \in R$, $b_m \neq 0$ un polinom (nenul) de grad minim astfel încât $fg = 0$. Atunci $a_n b_m = 0$, prin urmare $f(a_n g) = 0$, ceea ce conform minimalităţii lui $m \in \mathbb{N}$ conduce la $a_n g = 0$, adică $a_n b_j = 0$ pentru orice $j \in \{0, \dots, m\}$. Dar atunci

$$(a_0 + a_1 X + \dots + a_{n-1} X^{n-1}) g = (f - a_n X^n) g = 0,$$

ceea ce implică $a_{n-1} b_m = 0$. Urmează că $f(a_{n-1} g) = 0$ şi din nou minimalitatea lui m conduce la $a_{n-1} g = 0$, adică $a_{n-1} b_j = 0$ pentru orice $j \in \{0, \dots, m\}$. Aplicând succesiv raţionamentul de mai sus obţinem

$$a_i b_j = 0, \ \forall i \in \{0, \dots, n\}, \ \forall j \in \{0, \dots, m\}.$$

Înseamnă că luând $a = b_m$ avem $a \neq 0$ şi $af = 0$. Mai mult, gradul lui g este atunci $m = 0$ şi $g = b_0 = b_m = a$. Implicaţia inversă este, evident, adevărată.

3.102. Indicaţie. Din indicaţiile de la problema **2.69** rezultă că orice $q = a_2 i + a_3 j + a_4 k$ cu $a_2, a_3, a_4 \in \mathbb{R}$ şi $a_2^2 + a_3^2 + a_4^2 = 1$ verifică egalitatea $x^2 + 1 = 0$.

3.103. Răspuns. Gradul polinomului $f = \widehat{4}X - \widehat{4} \in \mathbb{Z}_{12}[X]$ este 1, dar f are 4 rădăcini în $\mathbb{Z}_{12}$ şi anume: $\widehat{1}$, $\widehat{4}$, $\widehat{7}$, $\widehat{10}$.

3.104. Avem

$$aX^2 + bX + c = a\left(X^2 + \frac{b}{a}X + \frac{c}{a}\right) = a\left[\left(X + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2}\right].$$

Fie $z_0 \in \mathbb{C}$ o rădăcină de ordinul 2 a numărului complex $b^2 - 4ac$. Rădăcinile polinomului dat sunt $\alpha_1 = \dfrac{-b + z_0}{2a}$ şi $\alpha_2 = \dfrac{-b - z_0}{2a}$.

Observaţii: a) Să observăm că cealaltă rădăcină de ordinul 2 a numărului complex $b^2 - 4ac$ este $-z_0$, deci rădăcinile determinate de aceasta sunt tot α_1, α_2.
b) Dacă notăm pe z_0 cu $\sqrt{b^2 - 4ac}$, obţinem o formulă similară cu cea care dă forma rădăcinilor unui polinom de grad 2 cu coeficienţi reali.

3.105. Răspuns. a) $\dfrac{(-2 \pm \sqrt{3}) + i}{2}$; b) $\pm\dfrac{\sqrt{6}}{2} - i\dfrac{\sqrt{6}}{2}$; c) $\dfrac{-\sqrt{3} \pm (2 - i)}{2}$.

3.106. Indicaţii. a) Dacă $\alpha, \beta \in \mathbb{C}$ şi $\alpha + \beta$ este o soluţie a ecuaţiei $y^3 + py + q = 0$ atunci $(\alpha + \beta)^3 + p(\alpha + \beta) + q = 0$ sau, echivalent, $(\alpha^3 + \beta^3) + (3\alpha\beta + p)(\alpha + \beta) + q = 0$. Se observă că dacă $3\alpha\beta + p = 0$ atunci $\alpha^3 + \beta^3 = -q$ şi $\alpha^3\beta^3 = -\dfrac{p^3}{27}$, aşadar α^3 şi β^3 sunt soluţiile ecuaţiei $t^2 + qt - \dfrac{p^3}{27} = 0$, adică

$$\alpha^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \text{ şi } \beta^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \tag{1}$$

unde cu $\sqrt{\dfrac{q^2}{4} + \dfrac{p^3}{27}}$ s-a notat o rădăcină de ordinul 2 a lui $\dfrac{q^2}{4} + \dfrac{p^3}{27} \in \mathbb{C}$. Dacă α_1 şi β_1 sunt soluţii ale ecuaţiilor (1) atunci celelelalte soluţii ale ecuaţiilor (1) sunt $\varepsilon\alpha_1, \varepsilon^2\alpha_1$, respectiv $\varepsilon\beta_1, \varepsilon^2\beta_1$, unde $\varepsilon \in \mathbb{C} \setminus \{1\}$ este o rădăcină de ordinul 3 a unităţii. Ştim că α şi β verifică egalitatea $3\alpha\beta + p = 0$. Aşadar, putem lua α_1, β_1 astfel încât $\alpha_1\beta_1 = -\dfrac{p}{3}$ şi atunci soluţiile ecuaţiei $y^3 + py + q = 0$ sunt

$$y_1 = \alpha_1 + \beta_1, \ y_2 = \varepsilon\alpha_1 + \varepsilon^2\beta_1 \text{ şi } y_3 = \varepsilon^2\alpha_1 + \varepsilon\beta_1.$$

b) Se înmulţeşte ecuaţia $ax^3 + bx^2 + cx + d = 0$, $a \neq 0$ cu $\dfrac{1}{a}$. În ecuaţia rezultată, se substituie x cu $y - \dfrac{b}{3a}$ şi se obţine o ecuaţie de forma $y^3 + py + q = 0$.

3.107. Răspuns. a) $x_1 = \sqrt[3]{2+\sqrt{3}} + \sqrt[3]{2-\sqrt{3}}$, $x_2 = \varepsilon\sqrt[3]{2+\sqrt{3}} + \varepsilon^2\sqrt[3]{2-\sqrt{3}}$, $x_3 = \varepsilon^2\sqrt[3]{2+\sqrt{3}} + \varepsilon\sqrt[3]{2-\sqrt{3}}$; b) $x_1 = -3$, $x_{2,3} = \dfrac{-3 \pm 3i\sqrt{3}}{2}$.

3.108. Indicaţii. a) $h = \left(X^2 + \dfrac{p}{2} + m\right)^2 - \left[2mX^2 - qX + \left(m^2 + pm - r + \dfrac{p^2}{4}\right)\right]$. Polinomul $2mX^2 - qX + \left(m^2 + pm - r + \dfrac{p^2}{4}\right)$ este pătratul unui polinom $g \in \mathbb{C}[X]$ dacă şi numai dacă are două rădăcini egale, adică $q^2 - 8m\left(m^2 + pm - r + \dfrac{p^2}{4}\right) = 0$. Prin urmare $m \in \mathbb{C}$ trebuie să fie o soluţie a ecuaţiei

$$8m^3 + 8pm^2 + 8\left(-r + \frac{p^2}{4}\right) - q^2 = 0. \tag{1}$$

Menţionăm că în acest caz, avem $g = 2m\left(X - \dfrac{q}{4m}\right)$.

b) Înmulţind ecuaţia cu $\dfrac{1}{a}$ şi substituind apoi $x = y + \dfrac{b}{4a}$ se obţine o ecuaţie de forma

$$y^4 + py^3 + qy + r = 0, \tag{2}$$

cu $p, q, r \in \mathbb{C}$. Ecuaţia (2) se mai scrie $h(y) = 0$. Dacă m_0 este o soluţie a ecuaţiei (1) atunci ecuaţia (2) este echivalentă cu $[f(y) + g(y)][f(y) - g(y)] = 0$ şi astfel rezolvarea ecuaţiei (2) revine la rezolvarea ecuaţiilor de gradul 2

$$y^2 - \sqrt{2m_0}y + \left(\frac{p}{2} + m_0 + \frac{q}{2\sqrt{2m_0}}\right) = 0 \text{ şi } y^2 + \sqrt{2m_0}y + \left(\frac{p}{2} + m_0 - \frac{q}{2\sqrt{2m_0}}\right) = 0.$$

3.109. Răspuns. $\pm\dfrac{\sqrt{6}}{2} - i\dfrac{\sqrt{6}}{2}$, $\dfrac{i\sqrt{6} \pm 3i\sqrt{2}}{2}$.

3.110. a) Dacă R este un inel finit şi $R \neq \{0\}$ atunci $R[X]$ este infinit, iar R^R este finit, deci φ nu este injectiv.
b) Luăm $(R, +, \cdot) = (\mathbb{R}, +, \cdot)$ şi considerăm funcţia $\sin : \mathbb{R} \to \mathbb{R}$. Dacă aceasta ar fi definită de un polinom $f \in \mathbb{R}[X]$ atunci f ar avea o infinitate de rădăcini reale, deci $f = 0$ şi prin urmare funcţia sinus ar fi identic nulă, contradicţie.

3.111. Indicaţie. $\widetilde{f} = \widetilde{g}$ dacă şi numai dacă orice $a \in R$ este rădăcină a polinomului $f - g$. Dacă R este infinit atunci $f - g = 0$, iar dacă R este finit, se obţine condiţia de la b).

3.112. Răspuns. $f_1 = \widehat{2}X^3 + \widehat{2}X^2 + \widehat{1}$, $f_2 = f = X^3 + \widehat{2}X^2 + X + \widehat{1}$, $f_3 = \widehat{2}X^2 + \widehat{2}X + \widehat{1}$. Pentru cele de grad 4 (sau mai mare) se foloseşte problema anterioară.

3.113. Indicaţii. Dacă $R \neq \{0\}$ şi φ este surjectiv atunci funcţia

$$\alpha : R \to R,\ \alpha(r) = \begin{cases} 0, & r = 0 \\ 1, & r \neq 0 \end{cases}$$

este funcţia polinomială indusă de un polinom $p = a_0 + a_1X + \cdots + a_nX^n \in R[X]$. Din $E_0(p) = p(0) = \alpha(0) = 0$ rezultă că $a_0 = 0$, prin urmare $r(a_1 + a_2r \cdots + a_nr^{n-1}) = 1$ pentru orice $r \neq 0$. Aşadar, orice element nenul din R este inversabil de unde urmează că R este un corp. Pentru a arăta că R este finit, se demonstrează că dacă R ar fi corp infinit atunci φ nu ar fi surjectiv. Pentru aceasta se poate proceda ca în soluţia problemei **3.110** considerând o funcţie nenulă cu o infinitate de zerouri, de exemplu

$$\beta : R \to R,\ \beta(r) = \begin{cases} 1, & r = 0 \\ 0, & r \neq 0 \end{cases}.$$

Reciproc, fie $R = \{a_1, \ldots, a_n\}$ corp, $\gamma \in R^R$. Arătăm că există $f \in R[X]$ astfel încât $\widetilde{f} = \gamma$. Folosind teorema împărţirii cu rest în $R[X]$ şi problema **3.111**, deducem că f induce aceeaşi funcţie polinomială ca restul împărţirii lui f la $(X - a_1) \cdots (X - a_n)$, prin urmare, este suficient să considerăm că gradul lui f este cel mult $n - 1$. Luând $f = b_0 + b_1 X + \cdots + b_{n-1} X^{n-1}$, egalităţile $f(a_i) = \gamma(a_i)$ $(i \in \{1, \ldots, n\})$ dau un sistem de n ecuaţii cu n necunoscute $(b_0, \ldots, b_{n-1})$ al cărui determinant este

$$\begin{vmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \ldots & a_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n & a_n^2 & \ldots & a_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (a_j - a_i) \neq 0,$$

ceea ce arată compatibilitatea sistemului menţionat, deci existenţa lui f.

Observaţie: În soluţia indicată mai sus s-a arătat existenţa unui polinom f pentru care $\widetilde{f} = \gamma$ fără a urmări determinarea lui f. Se verifică cu uşurinţă că funcţia polinomială determinată de polinomul (de interpolare al lui Lagrange)

$$f = \sum_{i=1}^{n} \frac{(X - a_1) \cdots (X - a_{i-1})(X - a_{i+1}) \cdots (X - a_n)}{(a_i - a_1) \cdots (a_i - a_{i-1})(a_i - a_{i+1}) \cdots (a_i - a_n)} \gamma(a_i)$$

este funcţia γ (cu $\dfrac{1}{a}$ am notat aici inversul elementului $a \in R^*$).

3.114. Indicaţii. Din proprietatea de universalitate a inelului de polinoame rezultă că un omomorfism de inele cu domeniul $R[X]$ este determinat de restricţia sa la R şi de imaginea lui X.

a) Cum $\varphi|_R$ este omomorfismul de incluziune $i : R \to R[X]$, determinarea lui φ revine la determinarea lui $\varphi(X) \in R[X]$. Dacă $\varphi(X) \in R$ atunci $\varphi(R[X]) = R$, ceea ce contrazice surjectivitatea lui φ. Dacă grad$(\varphi(X)) \geq 2$ atunci polinoamele de grad 1 lipsesc din $\varphi(R[X])$, din nou conradicţie cu φ surjectivă. Aşadar, $\varphi(X)$ este un polinom $aX + b$ de grad 1, adică $\varphi = E_{aX+b}$, cu $a, b \in R$, $a \neq 0$.

b) Dacă ψ este inversul automorfismului φ, se verifică cu uşurinţă că $\psi|_R = i$. Ca mai sus, se obţine că există $c, d \in R$, $c \neq 0$ astfel încât $\psi = E_{cX+d}$. Din $(\varphi \circ \psi)(X) = (X)$ rezultă că $ac = 1$, deci a este inversabil cu $a^{-1} = c$. Mai mult, avem şi $ad + b = 0$, de unde primim $d = -a^{-1}b$. Reciproc, se verifică faptul că

$$E_{aX+b} \circ E_{a^{-1}X - a^{-1}b} = E_{a^{-1}X - a^{-1}b} \circ E_{aX+b} = 1_{R[X]}.$$

3.115. Indicaţii. Dacă $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{Z}_p\}$ se arată uşor că orice automorfism φ al lui $R[X]$, fiind unital, satisface egalitatea $\varphi(r) = r$ pentru orice $r \in R$. În continuare se foloseşte problema anterioară şi se obţine:

$$Aut(\mathbb{Z}[X]) = \bigcup_{b \in \mathbb{Z}} \{E_{x+b}, E_{-x+b}\},\ Aut(\mathbb{Q}[X]) = \{E_{ax+b} \mid a, b \in \mathbb{Q},\ a \neq 0\},$$

$$Aut(\mathbb{Z}_p[X]) = \{E_{ax+b} \mid a, b \in \mathbb{Z}_p,\ a \neq \widehat{0}\}.$$

3.116. Indicaţie. Din $[X+i+(X^2+1)][X-i+(X^2+1)]=(X^2+1)$ rezultă că inelul cât $\mathbb{C}[X]/(X^2+1)$ are divizori ai lui zero.

3.117. Indicaţie. Aplicăm prima teoremă de izomorfism omomorfismului de inele

$$E_{0,0}:\mathbb{Q}[X,Y]\to\mathbb{Q},\ E_{0,0}(a)=a,\ \forall a\in\mathbb{Q},\ E_{0,0}(X)=0,\ E_{0,0}(Y)=0.$$

3.118. Indicaţii. a) Aplicăm prima teoremă de izomorfism omomorfismului de inele

$$E_i:\mathbb{R}[X]\to\mathbb{C},\ E_i(a)=a,\ \forall a\in\mathbb{R},\ E_i(X)=i.$$

b) Aplicăm prima teoremă de izomorfism omomorfismului $p\circ E_0$ rezultat din compunerea proiecţiei canonice $p:\mathbb{Z}\to\mathbb{Z}_n,\ p(a)=\widehat{a}$ cu omomorfismul

$$E_0:\mathbb{Z}[X]\to\mathbb{Z},\ E_0(a)=a,\ \forall a\in\mathbb{Z},\ E_0(X)=0.$$

c) Proiecţia canonică $p:\mathbb{Z}\to\mathbb{Z}_n,\ p(a)=\widehat{a}$ induce un omomorfism

$$\overline{p}:\mathbb{Z}[X]\to\mathbb{Z}_n[X],\ \overline{p}(a)=\widehat{a},\ \forall a\in\mathbb{Z},\ \overline{p}(X)=X.$$

Izomorfismul căutat se obţine aplicând prima teoremă de izomorfism lui $\overline{p}$.

3.119. Indicaţii. Aplicăm prima teoremă de izomorfism omomorfismelor de inele:
a) $E_{-1}:K[X]\to K,\ E_{-1}(a)=a,\ \forall a\in K,\ E_{-1}(X)=-1$;
b) $E_{X,X}:K[X,Y]\to K[X],\ E_{X,X}(a)=a,\ \forall a\in K,\ E_{X,X}(X)=X,\ E_{X,X}(Y)=X$ şi $E_{X,-X}:K[X,Y]\to K[X],\ E_{X,X}(a)=a,\ \forall a\in K,\ E_{X,X}(X)=X,\ E_{X,X}(Y)=-X$.

3.120. Indicaţii. Se aplică problema **3.82** pentru: a) automorfismul $E_{\frac{X}{2}}$ şi idealul (X^2-1); b) automorfismul $E_{X+\widehat{1}}$ şi idealul $(X^2-\widehat{1})$; c) automorfismul E_{X+1} şi idealul (X^2+1); d) automorfismul E_{X+1} şi idealul (X^2+1).

3.121. Indicaţii. a) Folosind pasul de inducţie din demonstraţia teoremei fundamentale a polinoamelor simetrice ([34, Teorema 3.11.6]), vom descrie un algoritm care ne va permite să scriem cu ajutorul polinoamelor simetrice fundamentale orice *polinom simetric omogen* (adică orice polinom simetric în care toate monoamele care intervin au acelaşi grad). Reamintim că exponenţii termenului principal al unui polinom simetric sunt în ordine descrescătoare (nu neapărat strict) şi că inducţia se face relativ la ordonarea lexicografică a termenilor principali. Notăm

$$f=(X_1^2+X_2^2)(X_2^2+X_3^2)(X_3^2+X_1^2)\in\mathbb{R}[X_1,X_2,X_3] \tag{1}$$

polinomul dat. Polinoamele simetrice fundamentale din $\mathbb{R}[X_1,X_2,X_3]$ sunt

$$s_1=X_1+X_2+X_3,\ s_2=X_1X_2+X_2X_3+X_3X_1,\ s_3=X_1X_2X_3.$$

Termenul principal al lui f este $X_1^4X_2^2$. Acest termen principal induce în scrierea lui f cu ajutorul lui s_1,s_2,s_3 termenul $s_1^{4-2}s_2^{2-0}s_3^0=s_1^2s_2^2$. Cum f şi $s_1^2s_2^2$ sunt polinoame simetrice omogene (de acelaşi grad), termenul principal al lui $f-s_1^2s_2^2$ este un monom de grad 6 mai mic sau egal (în sensul ordonării lexicografice) decât $X_1^4X_2X_3$. Dacă acesta ar fi chiar $aX_1^4X_2X_3$ ($a\in\mathbb{R}$) atunci ar induce în scrierea lui f cu ajutorul lui s_1,s_2,s_3 termenul $as_1^{4-1}s_2^{1-1}s_3^1=as_1^3s_3$ şi procedeul continuă. Astfel, posibilii exponenţi pentru termenii principali care apar în discuţie sunt

$$(4,2,0),\ (4,1,1),\ (3,3,0),\ (3,2,1),\ (2,2,2)$$

şi, corespunzător, posibilii exponenţi ai monoamelor în s_1, s_2, s_3 ce apar în scrierea lui f cu ajutorul polinoamelor simetrice fundamentale sunt

$$(2,2,0),\ (3,0,1),\ (0,3,0),\ (1,1,1),\ (0,0,2).$$

Prin urmare, există $a, b, c, d \in \mathbb{R}$ astfel încât

$$f = s_1^2 s_2^2 + a s_1^3 s_3 + b s_2^3 + c s_1 s_2 s_3 + d s_3^2. \tag{2}$$

Rămâne doar să determinăm numerele reale a, b, c, d. Aceasta se poate face ca în exemplul de mai jos, înlocuind convenabil pe X_1, X_2, X_3 cu numere reale x_1, x_2, x_3:

x_1	x_2	x_3	$E(s_1)$	$E(s_2)$	$E(s_3)$	$E(f)$ dat de (1)	$E(f)$ dat de (2)
1	1	0	2	1	0	2	$4+b$
2	-1	-1	0	-3	2	50	$-27b+4d$
1	-2	-2	-3	0	4	200	$-108a+16d$
1	-1	-1	-1	-1	1	8	$1-a-b+c+d$

unde s-a notat $E = E_{x_1,x_2,x_3}$. Rezultă imediat că $b = -2$, $d = -1$, $a = -2$ şi $c = 4$, deci

$$f = s_1^2 s_2^2 - 2 s_1^3 s_3 - 2 s_2^3 + 4 s_1 s_2 s_3 - s_3^2. \tag{3}$$

b) Se procedează ca la punctul a).
c) Scriind polinomul dat astfel:

$$\begin{aligned} g &= (X_1^2 + X_1^3 + X_1^4) + (X_2^2 + X_2^3 + X_2^4) + (X_3^2 + X_3^3 + X_3^4) + (X_4^2 + X_4^3 + X_4^4) \\ &= (X_1^2 + X_2^2 + X_3^2 + X_4^2) + (X_1^3 + X_2^3 + X_3^3 + X_4^3) + (X_1^4 + X_2^4 + X_3^4 + X_4^4) \end{aligned}$$

obţinem o sumă de polinoame (simetrice) omogene. Procedăm cu fiecare dintre polinoamele

$$X_1^2 + X_2^2 + X_3^2 + X_4^2,\ X_1^3 + X_2^3 + X_3^3 + X_4^3 \text{ şi } X_1^4 + X_2^4 + X_3^4 + X_4^4)$$

ca la punctul a). Însumăm rezultatele obţinute şi avem scrierea polinomului g cu ajutorul polinoamelor simetrice fundamentale.
d) Fracţia raţională dată este o fracţie raţională simetrică ce poate fi scrisă ca un cât de polinoame simetrice (omogene) astfel

$$\frac{X_1^2X_2 + X_2^2X_1 + X_2^2X_3 + X_3^2X_2 + X_3^2X_1 + X_1^2X_3}{X_1X_2X_3},$$

după care se continuă ca la punctul a).

3.122. Indicaţie. Întrucât $E = E_{\alpha_1,\alpha_2,\alpha_3}$ este un omomorfism de inele pentru care $E|_{\mathbb{C}} = 1_{\mathbb{C}}$, odată ce am scris polinomul simetric

$$f = (X_1^2 + X_2^2)(X_2^2 + X_3^2)(X_3^2 + X_1^2) \in \mathbb{C}[X_1, X_2, X_3]$$

cu ajutorul polinoamelor simetrice fundamentale, numărul căutat este

$$E(f) = [E(s_1)]^2[E(s_2)]^2 - 2[E(s_1)]^3E(s_3) - 2[E(s_2)]^3 + 4E(s_1)E(s_2)E(s_3) - [E(s_3)]^2.$$

Dar din relaţiile lui Viéte rezultă $E(s_1) = 0$, $E(s_2) = -3$, $E(s_3) = 4$ şi astfel se obţine $E(f) = 54 - 16 = 38$. Să remarcăm că, fără a efectua calculele se poate arăta că din faptul că polinoamele $X^3 - 3X - 4$ şi f au coeficienţi întregi şi coeficientul lui X^3 este 1 rezultă $E(f) \in \mathbb{Z}$.

3.123. Indicaţii. Formulele pentru derivata sumei şi produsului a două polinoame se deduc folosind definiţia derivatei formale, celelealte egalităţi se deduc din derivata produsului a două polinoame astfel: din definiţia derivatei formale avem $\alpha' = 0$ pentru orice $\alpha \in K$, de unde rezultă $(\alpha f)' = \alpha f'$, iar formula derivatei unei puteri se obţine prin inducţie după $k \in \mathbb{N}^*$.

3.124. Indicaţii. Se demonstrează prin inducţie după $m \in \mathbb{N}^*$ că din $(X-a)^m | f$ rezultă $f(a) = f'(a) = \cdots = f^{(m-1)}(a) = 0$, iar dacă $f^{(m)}(a) = 0$ atunci $(X-a)^{m+1} | f$.

3.125. Derivata formală a polinomului f este

$$f' = nX^{n-1} - (n-1)s_1X^{n-2} + \cdots + (-1)^k(n-k)s_kX^{n-k-1} + \cdots + (-1)^{n-1}s_{n-1}.$$

Dar $f = (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$ implică

$$f' = (X-\alpha_2)\cdots(X-\alpha_n) + (X-\alpha_1)(X-\alpha_3)\cdots(X-\alpha_n) + \cdots + (X-\alpha_1)\cdots(X-\alpha_{n-1}),$$

de unde deducem

$$f' = \frac{f}{X-\alpha_1} + \frac{f}{X-\alpha_2} + \cdots + \frac{f}{X-\alpha_n}.$$

Cu ajutorul schemei lui Horner obţinem, pentru orice $i \in \{1, \ldots, n\}$,

$$\begin{aligned}\frac{f}{X-\alpha_i} &= X^{n-1} + (\alpha_i - s_1)X^{n-2} + (\alpha_i^2 - s_1\alpha_i + s_2)X^{n-3} + \cdots \\ &+ \left[\alpha_i^k - s_1\alpha_i^{k-1} + \cdots + (-1)^{k-1}s_{k-1}\alpha_i + (-1)^k s_k\right] X^{n-k-1} + \cdots \\ &+ \left[\alpha_i^{n-1} - s_1\alpha_i^{n-2} + \cdots + (-1)^{n-2}s_{n-2}\alpha_i + (-1)^{n-1}s_{n-1}\right].\end{aligned}$$

Însumând şi ţinând seama de egalitatea coeficienţilor lui X^{n-k-1} din cele două scrieri ale lui f' avem, pentru orice $k < n$,

$$S_k - s_1S_{k-1} + \cdots + (-1)^{k-1}s_{k-1}S_1 + (-1)^k s_kS_0 = (-1)^k(n-k)s_k,$$

adică

$$S_k - s_1S_{k-1} + \cdots + (-1)^{k-2}s_{k-2}S_2 + (-1)^{k-1}s_{k-1}S_1 + (-1)^k ks_k = 0, \ \forall k < n.$$

Cum $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ sunt rădăcini ale lui f au loc egalităţile

$$\alpha_i^n - s_1X^{n-1} + s_2\alpha_i^{n-2} + \cdots + (-1)^{n-1}s_{n-1}\alpha_i + (-1)^n s_n, \ \forall i \in \{1, \ldots, n\}.$$

Dacă $n \leq k$ atunci, înmulţind fiecare din aceste egalităţi cu α_i^{k-n} şi adunând egalităţile rezultate, primim

$$S_k - s_1S_{k-1} + \cdots + (-1)^{n-1}s_{n-1}S_{k-n+1} + (-1)^n s_nS_{k-n} = 0, \ \forall k \geq n.$$

3.126. Indicaţii. În cazurile $n = 2$ şi $n = 3$ determinarea lui S_k pentru $k \leq n$ poate fi făcută mai uşor utilizând relaţiile lui Viète şi formula care dă pătratul unui trinom. Pentru $n = 2$ şi $k < 2$ avem $S_0 = 2$ şi $S_1 = s_1$, iar pentru $n = 3$ şi $k < 3$ avem $S_0 = 3$, $S_1 = s_1$ şi $S_2 = x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_3x_1) = s_1^2 - 2s_2$.

3.127. Indicaţie. Se consideră corpul $K = R(X_1, \dots, X_n)$ şi polinomul

$$f = (X - X_1) \cdots (X - X_n) = X^n - s_1 X^{n-1} + s_2 X^{n-2} + \cdots + (-1)^{n-1} s_{n-1} X + (-1)^n s_n$$

din $K[X]$ şi se procedează ca în soluţia problemei **3.125** (unde se înlocuieşte $\mathbb{C}$ cu K).

3.128. Indicaţii. e) Dependenţa rezultantei de $\alpha_1, \dots, \alpha_n$ (respectiv de $\beta_1, \dots, \beta_m$) este polinomială iar polinoamele care o exprimă sunt polinoame simetrice în n (respectiv m) nedeterminate. Scrierea acestora cu ajutorul polinoamelor simetrice fundamentale şi utilizarea relaţiilor dintre rădăcinile şi coeficienţii lui f (respectiv g) ca în soluţia problemei **3.122** arată că proprietatea cerută are loc.

3.129. Indicaţii. Fie $j \in \{1, \dots, m\}$ şi $u_j = f(\beta_j) = E_{\beta_j}(f)$. Avem

$$\begin{aligned}
&a_n \beta_j^n + \cdots + a_1 \beta_j + (a_0 - u_j) = 0,\\
&a_n \beta_j^{n+1} + \cdots + a_1 \beta_j^2 + (a_0 - u_j)\beta_j = 0,\\
&\vdots\\
&a_n \beta_j^{n+m-1} + \cdots + a_1 \beta_j^m + (a_0 - u_j)\beta_j^{m-1} = 0,\\
&b_m \beta_j^m + \cdots + b_1 \beta_j + b_0 = 0,\\
&b_m \beta_j^{m+1} + \cdots + b_1 \beta_j^2 + b_0 \beta_j = 0,\\
&\vdots\\
&b_m \beta_j^{m+n-1} + \cdots + b_1 \beta_j^n + b_0 \beta_j^{n-1} = 0,
\end{aligned}$$

prin urmare sistemul liniar şi omogen de $m+n$ ecuaţiicu $m+n$ necunoscute

$$\begin{aligned}
a_n y_{n+m-1} + a_{n-1} y_{n+m-2} + \cdots + a_1 y_m + (a_0 - u_j) y_{m-1} &= 0,\\
a_n y_{n+m-2} + \cdots + a_1 y_{m-1} + (a_0 - u_j) y_{m-2} &= 0,\\
&\vdots\\
a_n y_n + \cdots + a_1 y_1 + (a_0 - u_j) y_0 &= 0,\\
b_m y_{m+n-1} + b_{m-1} y_{m+n-2} + \cdots + b_1 y_n + b_0 y_{n-1} &= 0,\\
b_m y_{m+n-2} + \cdots + b_1 y_{n-1} + b_0 y_{n-2} &= 0,\\
&\vdots\\
b_m y_m + \cdots + b_1 y_1 + b_0 y_0 &= 0,
\end{aligned}$$

are soluţie nenulă pe $(\beta_j^{m+n-1}, \dots, \beta_j^2, \beta_j, 1)$, ceea ce înseamnă că determinantul său

$$\left|\begin{array}{ccccccccc}
a_n & a_{n-1} & a_{n-2} & \dots & a_0 - u_j & 0 & 0 & \dots & 0\\
0 & a_n & a_{n-1} & \dots & a_1 & a_0 - u_j & 0 & \dots & 0\\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots\\
0 & 0 & 0 & \dots & & & & \dots & a_0 - u_j\\
b_m & b_{m-1} & b_{m-2} & \dots & & & & \dots & 0\\
0 & b_m & b_{m-1} & \dots & & & & \dots & 0\\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots\\
0 & 0 & 0 & \dots & & & & \dots & b_0
\end{array}\right| \begin{array}{l} \left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} m \text{ linii} \\ \left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} n \text{ linii} \end{array}$$

este nul. Înlocuind pe u_j cu X în determinantul de mai sus obţinem un polinom de grad m în X care are rădăcinile $u_1, \dots, u_m$. Înlocuind în acest polinom pe X cu 0 obţinem termenul liber al său, iar cum coeficientul lui X^m este $(-1)^{m(n+1)} b_m^n$, termenul liber este

$$(-1)^m (-1)^{m(n+1)} b_m^n u_1 \cdots u_m = (-1)^{mn} b_m^n f(\beta_1) \cdots f(\beta_m) = \mathbf{R}_{f,g}.$$

3.130. Răspuns. $\mathbf{R}_{f,g} = \begin{vmatrix} a_2 & a_1 & a_0 & 0 & 0 \\ 0 & a_2 & a_1 & a_0 & 0 \\ 0 & 0 & a_2 & a_1 & a_0 \\ b_3 & b_2 & b_1 & b_0 & 0 \\ 0 & b_3 & b_2 & b_1 & b_0 \end{vmatrix}$.

3.131. Indicaţii. Se pot folosi problemele **3.128** (punctul a)) şi **3.129**.

3.132. Indicaţii. Se pot folosi problemele **3.128** (punctul a)) şi **3.129**.

Observaţie: Indicaţiile oferite mai sus nu sunt neapărat cele care conduc cel mai repede la rezultat, dar sunt cele mai potrivite contextului creat — de exemplu, rezolvarea punctului b) de la problema de mai sus este imediată dacă se observă că cel de-l doilea polinom are rădăcinile $\alpha_1 = 1$ şi $\alpha_2 = 2$.

3.133. Indicaţii. Se folosesc problemele **3.124** şi **3.128** (punctul a)).

3.134. Avem $f = a_n(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$ şi

$$f' = \sum_{i=1}^{n} a_n(X-\alpha_1)\cdots(X-\alpha_{i-1})(X-\alpha_{i+1})\cdots(X-\alpha_n),$$

prin urmare

$$f'(\alpha_i) = a_n(\alpha_i-\alpha_1)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_n),\ \forall i \in \{1,\ldots,n\}.$$

Cum

$$\mathbf{D}_f = (-1)^{\frac{n(n-1)}{2}}\frac{1}{a_n}\mathbf{R}_{f,f'} = (-1)^{\frac{n(n-1)}{2}}a_n^{n-2}f'(\alpha_1)\cdots f'(\alpha_n)$$

(vezi problema **3.128** c)), obţinem

$$\begin{aligned}\mathbf{D}_f = (-1)^{n(n-1)}a_n^{2n-2}(\alpha_2-\alpha_1)^2(\alpha_3-\alpha_1)^2\cdots(\alpha_n-\alpha_1)^2 \\ (\alpha_3-\alpha_2)^2\cdots(\alpha_n-\alpha_2)^2 \\ \vdots \\ (\alpha_n-\alpha_{n-1})^2\end{aligned}$$

Dar

$$\prod_{1\le i<j\le n}(\alpha_j-\alpha_i) = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \ldots & \alpha_n^{n-1} \end{vmatrix} = \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{n-1} \end{vmatrix}.$$

Deci

$$\mathbf{D}_f = a_n^{2n-2} \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{vmatrix} \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1} \end{vmatrix}$$

$$= a_n^{2n-2} \begin{vmatrix} n & S_1 & S_2 & \dots & S_{n-1} \\ S_1 & S_2 & S_3 & \dots & S_n \\ S_2 & S_3 & S_4 & \dots & S_{n+1} \\ \vdots & \vdots & \vdots & & \vdots \\ S_{n-1} & S_n & S_{n+1} & \dots & S_{2n-2} \end{vmatrix}.$$

3.135. Răspuns. a) $b^2 - 4ac$; b) $-4p^3 - 27q^2$; c) -843; d) 2777.

3.136. Răspuns. a) $\lambda_{1,2} = \pm 2$; b) $\lambda_1 = -1$, $\lambda_2 = -\dfrac{3}{2}$, $\lambda_{3,4} = \dfrac{7}{2} \pm \dfrac{9}{2} i\sqrt{3}$.

Capitolul 4

Semigrupuri şi inele de fracţii

4.1. Pentru a putea scufunda izomorf un semigrup comutativ într-un grup este necesar ca în acest semigrup să se poată simplifica cu orice element. Prin urmare, semigrupurile $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{Z}_4, \cdot)$ nu pot fi scufundate izomorf într-un grup.

Observaţie: Problema ce a condus la construcţia semigrupurilor de fracţii se datorează încercării de a scufunda minimal un semigrup comutativ cu simplificare într-un grup.

4.2. Indicaţii. Notăm $M = \{as^{-1} \mid a \in A,\ s \in S\}$. Din $S \neq \emptyset$ rezultă că există un element $s_0 \in S$, de unde, pentru orice $a \in A$ şi $s \in S$ avem

$$a = a(s_0 s_0^{-1}) = (as_0)s_0^{-1} \in M \text{ şi } s^{-1} = (s_0 s_0^{-1})s^{-1} = s_0(s_0^{-1}s^{-1}) = s_0(ss_0)^{-1} \in M,$$

prin urmare $A \cup S^{-1} \subseteq M$. Se verifică uşor că M este un subsemigrup al lui $(G, \cdot)$ şi că orice subsemigrup al lui $(G, \cdot)$ care include mulţimea $A \cup S^{-1}$ include pe M. Aşadar, M este subsemigrupul lui $(G, \cdot)$ generat de $A \cup S^{-1}$. Aplicând proprietatea de universalitate a semigrupului de fracţii omomorfismului de incluziune $i : A \to G$ obţinem existenţa (şi unicitatea) unui omomorfism $\overline{i} : A_S \to G$ pentru care $\overline{i} \circ f = i$ (unde $f : A \to A_S$ este omomorfismul canonic). Rezultă că $\overline{i}(\overline{(a, s)}) = as^{-1}$ pentru orice $a \in A$, $s \in S$ şi se verifică imediat că $\overline{i}$ este injectiv, deci este un izomorfism între A_S şi $\overline{i}(A_S) = M$. Semigrupul total de fracţii al lui A este A_A şi este izomorf cu semigrupul lui $(G, \cdot)$ generat de $A \cup A^{-1}$ care este chiar subgrupul lui $(G, \cdot)$ generat de A.

4.3. Răspuns. a) $(\mathbb{Z}_{\mathbb{Z}^*}, \cdot) = (\mathbb{Q}, \cdot)$; b) $(\mathbb{Z}^*_{\mathbb{Z}^*}, \cdot) = (\mathbb{Q}^*, \cdot)$; c) $(\mathbb{Z}_{2\mathbb{Z}^*}, \cdot) = (\mathbb{Q}, \cdot)$; d) $(\mathbb{N}_{2\mathbb{N}}, +) = (\mathbb{Z}, +)$; e) $(2\mathbb{N}_{2\mathbb{N}}, +) = (2\mathbb{Z}, +)$; f) $(2\mathbb{Z}_{2\mathbb{Z}^*}, \cdot) = (\mathbb{Q}, \cdot)$; g) $(2\mathbb{Z}_{2\mathbb{Z}}, +) = (2\mathbb{Z}, +)$.

Observaţie: Din problema **4.2** rezultă că grupul de fracţii al unui grup comutativ $(G, \cdot)$ este $(G, \cdot)$. Aceasta se obţine şi dacă ţinem seama de faptul că apariţia semigrupurilor de fracţii se datorează încercării de a scufunda un semigrup comutativ cu simplificare într-un grup minimal.

4.4. Ştiind că dacă $a \in A$ şi $s \in S$ atunci

$$f(s)\overline{(a, s)} = \overline{(s^2, s)} \cdot \overline{(a, s)} = \overline{(as^2, s^2)} = \overline{(as, s)} = f(a) \in f(A), \tag{1}$$

problema se poate rezolva prin inducţie după n. Într-adevăr, dacă $n = 1$ şi $q_1 = \overline{(a_1, s_1)}$, din (1) rezultă că putem considera $s = s_1$, iar dacă $q_n = \overline{(a_n, s_n)}$ şi pentru $s \in S$ avem $f(s)q_1, \ldots, f(s)q_{n-1} \in f(A)$ atunci luând $s' = ss_n \in S$ obţinem

$$f(s')q_i = f(ss_n)q_i = f(s)f(s_n)q_i = f(s_n)[f(s)q_i] \in f(s_n)f(A) \subseteq f(A),$$

pentru orice $i \in \{1, \ldots, n-1\}$, şi

$$f(s')q_n = f(ss_n)q_n = f(s)\left[f(s_n)\overline{(a_n, s_n)}\right] = f(s)f(a_n) = f(sa_n) \in f(A).$$

Observaţie: Cu alte cuvinte, problema anterioară exprimă faptul că orice mulţime finită de fracţii din A_S are un numitor comun.

4.5. Monoidul $(A, +)$ fiind comutativ şi verificând condiţia

$$a, b, c \in A,\ a + b = a + c \Rightarrow b = c$$

rezultă că $(A, +)$ se scufundă izomorf în grupul diferenţelor $(A_A, +)$. Amintim pe scurt construcţia acestui grup. Relaţia $\sim$ definită pe $A \times A$ prin

$$(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1 + b_2 = a_2 + b_1$$

este o relaţie de echivalenţă, iar $A_A = (A \times A)/\sim$. Notăm cu $\overline{(a,b)}$ sau cu $a - b$ clasa perechii (a, b) în raport cu relaţia $\sim$, adică $\overline{(a,b)} = \{(a', b') \mid (a, b) \sim (a', b')\}$. Operaţia definită pe A_A prin

$$\overline{(a_1, b_1)} + \overline{(a_2, b_2)} = \overline{(a_1 + a_2, b_1 + b_2)}$$

este independentă de alegerea reprezentanţilor, iar $(A_A, +)$ este grup abelian. Elementul neutru în acest grup este $\overline{(0,0)}$ şi $\overline{(0,0)} = \{(a, a) \mid a \in A\}$, iar simetrica clasei $\overline{(a,b)}$ este clasa $\overline{(b,a)}$, notată $-\overline{(a,b)}$. Funcţia $f : A \to A_A$, $f(a) = \overline{(a,0)}$ este omomorfism injectiv şi orice $\overline{(a,b)} \in A_A$ se scrie sub forma $\overline{(a,b)} = f(a) - f(b)$. Pe grupul abelian $(A_A, +)$ există o singură operaţie $\cdot$ astfel încât $(A_A, +, \cdot)$ să fie inel, iar f să fie omomorfism şi pentru $\cdot$. Această operaţie este definită astfel:

$$\overline{(a_1, b_1)} + \overline{(a_2, b_2)} = \overline{(a_1a_2 + b_1b_2, a_1b_2 + a_2b_1)},$$

ceea ce se reţine uşor având în vedere înmulţirea formală $(a_1 - b_1) \cdot (a_2 - b_2)$.

4.6. Urmând procedeul din problema anterioară, semiinelul $(\mathbb{N}, +, \cdot)$ se scufundă izomorf în inelul minimal $(\mathbb{N}_\mathbb{N}, +, \cdot)$. Se verifică uşor că în acest inel avem $\overline{(a+b, b)} = \overline{(a, 0)}$, $\overline{(b, a+b)} = \overline{(0, a)}$ şi

$$\overline{(a,0)} = \overline{(a',0)} \Leftrightarrow a = a' \Leftrightarrow \overline{(0,a)} = \overline{(0,a,)},$$

de unde se deduce că orice clasă din $\mathbb{N}_\mathbb{N}$ are un reprezentant unic de una din formele: $(a, 0), (0, 0), (0, a)$, cu $a \in \mathbb{N}^*$. Prin urmare,

$$\mathbb{N}_\mathbb{N} = \{\ldots, -\overline{(2,0)}, -\overline{(1,0)}, \overline{(0,0)}, \overline{(1,0)}, \overline{(2,0)}, \ldots\}.$$

Injectivitatea omomorfismului f permite identificarea lui $x \in \mathbb{N}$ cu $\overline{(x,0)}$. După această identificare avem $\mathbb{N}_\mathbb{N} = \mathbb{Z}$. Deci inelul diferenţelor semiinelului $(\mathbb{N}, +, \cdot)$ este $(\mathbb{Z}, +, \cdot)$.

4.7. Pentru a putea scufunda izomorf un inel comutativ într-un corp este necesar ca în acest inel să nu avem divizori ai lui zero. Prin urmare, inelele $(\mathbb{Z}_n, +, \cdot)$ cu $n \in \mathbb{N}$, $n \geq 2$, număr compus nu pot fi scufundate izomorf într-un corp.

Observaţie: Construcţia inelelor de fracţii se datorează încercării de a scufunda minimal un inel comutativ fără divizori ai lui zero într-un corp.

4.8. Indicaţii. Soluţia este similară cu soluţia problemei **4.2**.

4.9. Indicaţie. Folosind problema **4.8** obţinem următoarele: a) $(\mathbb{Z}_{\mathbb{Z}^*}, +, \cdot) = (\mathbb{Q}, +, \cdot)$; b) $(2\mathbb{Z}_{2\mathbb{Z}^*}, +, \cdot) = (\mathbb{Q}, +, \cdot)$; c) $((\mathbb{Z}_3)_{\mathbb{Z}_3^*}, +, \cdot) = (\mathbb{Z}_3, +, \cdot)$; d) $(\mathbb{Q}_{\mathbb{Q}^*}, +, \cdot) = (\mathbb{Q}, +, \cdot)$.

Observaţii: a) Corpul fracţiilor unui corp comutativ $(K, +, \cdot)$ este (izomorf cu) $(K, +, \cdot)$.
b) Ştiind cum se realizează construcţia inelului de fracţii pornind de la semigrupul (multiplicativ) de fracţii, problema **4.8** se poate folosi pentru construcţia unor semigrupuri de fracţii: de exemplu, din problema anterioară deducem că $(\mathbb{Z}_{\mathbb{Z}^*}, \cdot) = (\mathbb{Q}, \cdot)$ şi $(\mathbb{Z}_{2\mathbb{Z}^*}, \cdot) = (\mathbb{Q}, \cdot)$.

4.10. Indicaţie. Se foloseşte problema **4.8** şi se obţine $(\mathbb{Z}_{2\mathbb{Z}^*\cup\{1\}}, +, \cdot) = (\mathbb{Q}, +, \cdot)$.

4.11. Răspuns. $\left(\mathbb{Z}[i]_{\mathbb{Z}[i]^*}, +, \cdot\right) = (\mathbb{Q}(i), +, \cdot)$, $\left(\mathbb{Z}[\sqrt{d}]_{\mathbb{Z}[\sqrt{d}]^*}, +, \cdot\right) = (\mathbb{Q}(\sqrt{d}), +, \cdot)$.

4.12. Indicaţie. c) Se foloseşte problema **4.8**.

4.13. Conform problemei **4.8**, pentru orice sistem multiplicativ $\emptyset \neq S \subseteq \mathbb{Z}$ ce nu conţine pe 0, inelul $\mathbb{Z}_S$ poate fi identificat cu subinelul $\left\{\frac{m}{n} \mid m \in \mathbb{Z},\ n \in S\right\}$ al lui $\mathbb{Q}$. Fie, acum, R un subinel cu unitate al lui $\mathbb{Q}$. Evident, unitatea lui R coincide cu unitatea lui $\mathbb{Q}$, prin urmare, $1 \in R$ ceea ce implică $\mathbb{Z} \subseteq R$. Considerând

$$S_R = \left\{n \in \mathbb{Z} \mid \frac{1}{n} \in R\right\}$$

obţinem un sistem multiplicativ (nevid) al lui $\mathbb{Z}$ ce nu conţine pe 0 şi $\mathbb{Z}_{S_R} \subseteq R$. Reciproc, dacă luăm un element din R reprezentat prin fracţia ireductibilă $\frac{m}{n}$ atunci există $p, q \in \mathbb{Z}$ astfel încât $mp + nq = 1$, de unde rezultă că

$$\frac{1}{n} = \frac{mp + nq}{n} = p \cdot \frac{m}{n} + q \in R,$$

aşadar $R \subseteq \mathbb{Z}_{S_R}$ şi astfel se obţine egalitatea $R = \mathbb{Z}_{S_R}$.

4.14. Indicaţii. Din proprietatea de universalitate a inelului $R[X]$ rezultă existenţa (şi unicitatea) unui omomorfism de inele $\overline{f} : R[X] \to R_S$ care extinde omomorfismul canonic $f : R \to R_S$ şi pentru care $\overline{f}(X) = \overline{(1, a)} = \frac{1}{a}$. Evident, $(aX - 1) \subseteq \mathrm{Ker} f$, iar dacă $p = a_0 + a_1X + \cdots + a_nX^n \in \mathrm{Ker} f$ atunci $\overline{f}(p) = 0$, prin urmare restul împărţirii polinomului p la $X - \frac{1}{a}$ în inelul $R_S[X]$ este 0, ceea ce implică existenţa unui polinom $q = c_0 + c_1X + \cdots + c_{n-1}X^n \in R_S[X]$ cu proprietatea că $p = q(aX - 1)$. De aici rezultă că

$$-c_0 = a_0,\ -c_1 + ac_0 = a_1,\ -c_2 + ac_1 = a_2, \ldots,\ -c_{n-1} + ac_{n-2} = a_{n-1},\ ac_{n-1} = a_n.$$

Deci $c_0, \ldots, c_{n-1} \in R$, ceea ce implică $p \in (aX - 1)R[X] = (aX - 1)$. Izomorfismul căutat se obţine aplicând lui $\overline{f}$ prima teoremă de izomorfism pentru inele.

4.15. a) Din ipoteză rezultă $g(f(a)) = h(f(a))$ pentru orice $a \in R$. Subinelele $g(R_S)$ şi $h(R_S)$ ale lui $(R', +, \cdot)$ sunt inele cu aceeaşi unitate

$$1' = g\left(\overline{(s,s)}\right) = h\left(\overline{(s,s)}\right) \ (s \in S).$$

Dacă A este subinelul lui R' generat de $g(R_S) \cup h(R_S)$ atunci A este, în raport cu operaţiile induse din $(R', +, \cdot)$, un inel cu unitatea $1'$, iar omomorfismele g, h pot fi privite ca omomorfisme (unitale) cu codomeniul A. Folosind acest fapt, cum $f(s)$ este inversabil în R_S pentru orice $s \in S$, deducem

$$g\left((f(s))^{-1}\right) = [g(f(s))]^{-1} = [h(f(s))]^{-1} = h\left((f(s))^{-1}\right).$$

Întrucât pentru orice $\overline{(a,s)} \in R_S$ avem $\overline{(a,s)} = f(a)[f(s)]^{-1}$ rezultă

$$g\left(\overline{(a,s)}\right) = h\left(\overline{(a,s)}\right),$$

adică $g = h$.
b) Dacă f este surjectiv atunci pentru orice $s \in S$, din $[f(s)]^{-1} = \overline{(1,s)} \in R_S$ rezultă existenţa unui element $a \in R$ astfel încât

$$f(a) = \overline{(as,s)} = \overline{(1,s)},$$

adică $as^2 = s$ sau, echivalent, $as = 1$. Deci $s \in U(R, +, \cdot)$. Reciproc, dacă $S \subseteq U(R, +, \cdot)$ atunci orice $\overline{(a,s)}$ din R_S se scrie astfel

$$\overline{(a,s)} = \overline{((as^{-1})\, s, s)} = f\left(as^{-1}\right),$$

deci f este şi surjectiv.

Observaţie: Se stie că pentru omomorfisme de inele simplificabilitatea la dreapta nu este echivalentă cu surjectivitatea, iar omomorfismul de incluziune $\mathbb{Z} \to \mathbb{Q}$ este un exemplu în acest sens (vezi problema **3.68**). Punctul a) al problemei de mai sus furnizează o generalizare a acestui exemplu.

4.16. Conform punctului b) a problemei anterioare, f este izomorfism dacă si numai dacă $S \subseteq U(R, +, \cdot)$. Dar, dacă $S \subseteq U(R, +, \cdot)$ atunci, identificând elementele din R cu imaginile lor prin f şi implicit orice $\overline{(a,s)} \in R_S$ cu as^{-1} deducem că orice $as^{-1} \in R_S$ este rădăcină a polinomului $X - as^{-1} \in R[X]$. Reciproc, cum pentru orice $s \in S$, $\overline{(1,s)}$ este rădăcină a unui polinom $X - a \in R[X]$ atunci egalitatea $\overline{(1,s)} - a = 0$ se traduce în R_S prin

$$\overline{(1,s)} - \overline{(as,s)} = \overline{(0,s)}$$

de unde rezultă $1 - as = 0$, deci s este inversabil şi $s^{-1} = a$.

4.17. Indicaţie. Nondivizorii lui zero din $(\mathbb{Z}_n, +, \cdot)$ coincid cu elementele inversabile şi se aplică punctul b) al problemei **4.15**.

4.18. Indicaţie. c) Fie $T = \{g \in \mathbb{R}^{\mathbb{R}} \mid \forall x \in \mathbb{R},\ f(x) \neq 0\}$. Inelul total de fracţii al lui $\mathbb{R}^{\mathbb{R}}$ este $\left(\mathbb{R}^{\mathbb{R}}\right)_T$, iar un izomorfism între $\mathbb{R}^{\mathbb{R}}$ şi $\left(\mathbb{R}^{\mathbb{R}}\right)_T$ este dat de corespondenţa $f \mapsto \overline{(f, \varepsilon)}$, unde ε este unitatea lui $\mathbb{R}^{\mathbb{R}}$. Inversul acestui izomorfism este dat de corespondenţa $\overline{(f,g)} \mapsto h$, unde $h : \mathbb{R} \to \mathbb{R}$ este definit prin $h(x) = \dfrac{f(x)}{g(x)}$.

4.19. Dacă g ar fi surjectiv atunci cum $\left(\dfrac{1}{n+1}\right)_{n\in\mathbb{N}} \in (\mathbb{Z}_{\mathbb{Z}^*})^{\mathbb{N}}$ ar exista $y \in \mathbb{Z}^*$ şi pentru orice $n \in \mathbb{N}$ ar exista $x_n \in \mathbb{Z}$ astfel încât $\dfrac{1}{n+1} \sim \dfrac{x_n}{y}$, prin urmare $y = (n+1)x_n$, ceea ce conduce la faptul că orice număr natural nenul îl divide pe y, deci $y = 0$, contradicţie.

4.20. Fie R, R' domenii de integritate, R_{R^*}, respectiv $R'_{R'^*}$ corpurile lor de fracţii şi $f : R \to R_{R^*}$, $f' : R' \to R'_{R'^*}$ omomorfismele canonice. Dacă $\alpha : R \to R'$ este un omomorfism de inele atunci $\beta = f' \circ \alpha$ este, de asemenea, un omomorfism.

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "\alpha"'] \arrow[dr, "\beta"] & R_{R^*} \arrow[d, dotted, "\overline{\beta}"] \\ R' \arrow[r, "f'"] & R'_{R'^*} \end{tikzcd}$$

Din proprietatea de universalitate a corpului de fracţii rezultă existenţa unui omomorfism $\overline{\beta} : R_{R^*} \to R'_{R'^*}$ astfel încât $\beta = \overline{\beta} \circ f$. Astfel, $\overline{\beta}$ este definit prin

$$\begin{aligned} \overline{\beta}\left(\overline{(a,s)}\right) &= \beta(a)[\beta(s)]^{-1} = f'(\alpha(a))[f'(\alpha(s))]^{-1} \\ &= \overline{(\alpha(a)\alpha(s), \alpha(s))} \cdot \overline{(\alpha(s), \alpha(s)\alpha(s))} = \overline{(\alpha(a), \alpha(s))} \end{aligned}$$

şi avem

$$\overline{(\alpha(a_1), \alpha(s_1))} = \overline{(\alpha(a_2), \alpha(s_2))} \Leftrightarrow \alpha(a_1)\alpha(s_2) = \alpha(a_2)\alpha(s_1) \Leftrightarrow \alpha(a_1 s_2) = \alpha(a_2 s_1),$$

ceea ce, în ipoteza α injectiv, are loc dacă şi numai dacă

$$a_1 s_2 = a_2 s_1 \Leftrightarrow (a_1, s_1) \sim (a_2, s_2) \Leftrightarrow \overline{(a_1, s_1)} = \overline{(a_2, s_2)}.$$

Prin urmare, omomorfismul $\overline{\beta}$ este injectiv. Din definiţia lui $\overline{\beta}$ deducem cu uşurinţă că α surjectiv implică $\overline{\beta}$ surjectiv şi, deci, că α izomorfism implică $\overline{\beta}$ izomorfism.

4.21. Se verifică uşor că dacă U este un ideal al lui $(R, +, \cdot)$ atunci

$$U_S = \left\{\overline{(x,s)} \in R_S \mid x \in U\right\},$$

este ideal al inelului $(R_S, +, \cdot)$, iar dacă U este (idealul principal) generat de $a \in R$ atunci egalitatea

$$\overline{(ar, s)} = \overline{(a, 1)} \cdot \overline{(r, s)}$$

ne asigură că idealul U_S este, de asemenea, principal, generat de $\overline{(a,1)}$. Aşadar, problema este rezolvată dacă arătăm că toate idealele lui R_S sunt de forma U_S unde U este un ideal al lui R. Fie, pentru aceasta, $\overline{U}$ un ideal al lui R_S şi

$$U = \left\{x \in R \mid \exists s \in S : \ \overline{(x,s)} \in \overline{U}\right\}.$$

Cum $\overline{(0,1)} \in \overline{U}$, avem $0 \in U$, prin urmare, $U \neq \emptyset$. Fie $r \in R$, $t \in S$ şi $x, x' \in U$. Atunci există $s, s' \in S$ astfel încât $\overline{(r,s)}, \overline{(r',s')} \in \overline{U}$ şi urmează

$$\overline{(x - x', ss')} = \overline{(1, s')} \cdot \overline{(x, s)} - \overline{(1, s)} \cdot \overline{(x', s')} \in \overline{U} \text{ şi } \overline{(rx, ts)} = \overline{(r, t)} \cdot \overline{(x, s)} \in \overline{U}.$$

Rezultă că $x - x', rx \in U$, deci U este un ideal al lui R. Este evident că $\overline{U} \subseteq U_S$, iar dacă $\overline{(x, s)} \in U_S$ cu $x \in U$ atunci există $s' \in S$ astfel încât $\overline{(x, s')} \in \overline{U}$ şi astfel,

$$\overline{(x, s)} = \overline{(s', s)} \cdot \overline{(x, s')} \in \overline{U},$$

ceea ce completează demonstraţia faptului că $\overline{U} = U_S$.

Capitolul 5

Divizibilitatea în monoizi comutativi cu simplificare şi în domenii de integritate

5.1. Indicaţie. Dacă A este monoid comutativ cu simplificare sau domeniu de integritate, iar $a, b \in A$ atunci

$$a \sim b \Leftrightarrow \exists x \in A \text{ inversabil } : \ b = ax.$$

Prin urmare, avem:
a) $\sim = \Delta_{\mathbb{N}^*}$, $\mathbb{N}^*/\sim = \{\{n\} \mid n \in \mathbb{N}^*\}$;
b) $\sim = \mathbb{Q}^* \times \mathbb{Q}^*$, $\mathbb{Q}^*/\sim = \{\mathbb{Q}^*\}$;
c) $\sim = \bigcup\limits_{n \in \mathbb{Z}} \{(n, n), (n, -n)\}$, $\mathbb{Z}/\sim = \{\{-n, n\} \mid n \in \mathbb{N}\}$;
d) $\sim = \{(0, 0)\} \cup (\mathbb{R}^* \times \mathbb{R}^*)$, $\mathbb{R}/\sim = \{\{0\}, \mathbb{R}^*\}$;
e) $\sim = \{(\widehat{0}, \widehat{0})\} \cup (\mathbb{Z}_2^* \times \mathbb{Z}_2^*) = \{(\widehat{0}, \widehat{0}), (\widehat{1}, \widehat{1})\} = \Delta_{\mathbb{Z}_2}$, $\mathbb{Z}_2/\sim = \{\{\widehat{0}\}, \{\widehat{1}\}\}$;
f) $\sim = \bigcup\limits_{z \in \mathbb{Z}[i]} \{\pm z, \pm iz\} \times \{\pm z, \pm iz\}$, $\mathbb{Z}[i]/\sim = \{\{z, -z, iz, -iz\} \mid z \in \mathbb{Z}[i]\}$.

5.2. Răspuns. Pentru $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\} \cup \{\mathbb{Z}_p \mid p \text{ număr prim}\}$ avem $\overline{f} = \{af \mid a \in K^*\}$ în $K[X]$, iar în $\mathbb{Z}[X]$ avem $\overline{f} = \{-f, f\}$.

5.3. Indicaţii. i) $U(\mathbb{Z}_2[X_1, \ldots, X_n]) = U(\mathbb{Z}_2) = \{\widehat{1}\}$.
ii) Dacă R are caracteristica diferită de 2 atunci în subinelul lui R generat de elementul unitate 1 (şi implicit în R) există elemente inversabile diferite de 1.
iii) Fie K un corp cu 4 elemente, deci comutativ (existenţa lui K rezultă din [34, Teorema 7.7.5]). Relaţia de divizibilitate în K, respectiv în $K[X]$, nu este relaţie de ordine.

5.4. Indicaţie. Toate elementele nenule sunt în clasa de asociere în divizibilitate a elementului unitate, deci sunt inversabile.

5.5. Indicaţie. Dacă ar exista $r \in R^*$ neinversabil atunci nici r^2 (care este produsul a două elemente neinversabile din R) nu ar fi inversabil, prin urmare, ar fi ireductibil, contradicţie.

5.6. Indicaţie. Fie $a, a_1, a_2 \in R$. Avem

$$a = a_1 a_2 \Leftrightarrow \varphi(a) = \varphi(a_1)\varphi(a_2)$$

şi φ conservă elementele inversabile.

5.7. Indicaţie. Cum pentru $f \in K[X]$ avem f inversabil în $K[X]$ dacă şi numai dacă f este inversabil în $K'[X]$ se deduce uşor că orice polinom din $K[X]$ ireductibil în $K'[X]$ este ireductibil şi în $K[X]$. Reciproca nu este, în general adevărată: de exemplu, polinomul $X^2+1 \in \mathbb{R}[X]$ este ireductibil peste $\mathbb{R}$, dar în $\mathbb{C}[X]$ avem $X^2+1=(X+i)(X-i)$.

Observaţie. Amintim că în unele manuale şcolare, polinoamele ireductibile (cu coeficienţi într-un corp comutativ) sunt introduse ca acele polinoame de grad mai mare sau egal cu 1 care nu sunt reductibile, unde polinomul reductibil este definit ca un polinom care se poate scrie ca produs de două polinoame de grad mai mare sau egal cu 1. Întrucât pentru un polinom f cu coeficienţi într-un corp comutativ K condiţia $\operatorname{grad} f \geq 1$ este echivalentă cu condiţia f nenul şi neinversabil, definiţia polinomului ireductibil coincide cu definiţia elementului ireductibil în $K[X]$. De asemenea, menţionăm că un *element* al unui domeniu de integritate R se numeşte *reductibil* dacă se poate scrie ca produs de două elemente neinversabile. Prin urmare, un element din R^* care nu este ireductibil este sau inversabil sau reductibil.

5.8. Indicaţie. Din $f\left(\frac{p}{q}\right)=0$ rezultă că $f=\left(X-\frac{p}{q}\right)g$, cu $g \in \mathbb{Q}[X]$, de unde, eliminând numitorii, primim $q^n f=(qX-p)g_1$ cu $g_1 \in \mathbb{Z}[X]$ şi $n = \operatorname{grad} f$, ceea ce implică $q^n f(\pm 1)=-(p \mp q)g_1(\pm 1)$, iar din $(p,q)=1$ rezultă $(p \mp q, q^n)=1$. Deci $p \mp q | f(\pm 1)$.

5.9. Indicaţie. În $\mathbb{Z}_2[X]$ există $2^4=16$ polinoame de grad mai mic sau egal cu 3, iar un polinom de grad 2 sau 3 cu coeficienţi într-un corp comutativ K este reductibil dacă şi numai dacă este nenul şi are o rădăcină în K.

5.10. Indicaţii. a), b) Se foloseşte faptul că $\operatorname{grad}(gh) = \operatorname{grad} g + \operatorname{grad} h$ pentru orice $g,h \in K[X]$; c) $(X^2+1)^2 \in \mathbb{R}[X]$ este reductibil, dar nu are rădăcini reale.

5.11. Răspuns. i) $f=6(x+2)$ este reductibil în $\mathbb{Z}[X]$, dar este ireductibil în $\mathbb{Q}[X]$.

5.12. Indicaţie. Pentru orice $a \in R^*$, $aX+a$ este un polinom ireductibil în $R[X]$, deci a este inversabil în R.

5.13. Indicaţii. a) Elementele ireductibile p din $(\mathbb{N}^*,\cdot)$ concid cu numerele prime (este de notat importanţa condiţiei $p \geq 2$ în definiţia numărului prim). Din *teorema fundamentală a aritmeticii — orice număr natural mai mare sau egal cu 2 se poate scrie ca un produs de numere prime în mod unic, abstracţie făcând de ordinea factorilor* — deducem că $(\mathbb{N}^*,\cdot)$ este un semigrup factorial, deci elementele ireductibile coincid cu elementele prime. Acelaşi lucru se întâmplă şi la b), c), d) deoarece domeniile de integritate analizate sunt euclidiene, deci factoriale.
b) Un număr întreg p este element ireductibil în $(\mathbb{Z},+,\cdot)$ dacă şi numai dacă p sau $-p$ este număr prim în $\mathbb{N}^*$.
c) Un polinom $f \in \mathbb{C}[X]$ este ireductibil dacă şi numai dacă $\operatorname{grad} f=1$. Aceasta rezultă din problema **5.10** şi din *teorema fundamentală a algebrei (d'Alembert-Gauss)*: *orice polinom de grad mai mare sau egal cu 1 din $\mathbb{C}[X]$ are cel puţin o rădăcină complexă.*
d) Un polinom $f \in \mathbb{R}[X]$ este ireductibil dacă şi numai dacă $\operatorname{grad} f=1$ sau f are gradul 2 şi discriminantul negativ. Pentru a demonstra că polinoamele menţionate mai sus sunt singurele polinoame ireductibile din $\mathbb{R}[X]$ trebuie arătat că dacă $f \in \mathbb{R}[X]$ şi $\operatorname{grad} f \geq 3$ atunci f este reductibil în $\mathbb{R}[X]$. Aceasta rezultă astfel: cum $f \in \mathbb{R}[X] \subseteq \mathbb{C}[X]$, f are o rădăcină complexă a. Dacă $a \in \mathbb{R}$ atunci $X-a$ divide pe f. Dacă $a \in \mathbb{C}\setminus\mathbb{R}$ atunci conjugatul lui a este, de asemenea, rădăcină a lui f, prin urmare $(X-a)(X-\overline{a}) \in \mathbb{R}[X]$ divide pe f.

5.14. Indicaţie. Se aplică teorema împărţirii cu rest pentru polinoame cu coeficienţi într-un domeniu de intergritate.

5.15. Indicaţie. În $\mathbb{Z}$ avem

$$\begin{aligned}&-4=3(-1)+(-1),\ \text{cu } 1=|-1|<|3|=3,\\&-4=3(-2)+2,\ \text{cu } 2=|2|<|3|=3.\end{aligned}$$

(Să remarcăm că doar a doua egalitate dă câtul şi restul împărţirii lui -4 la 3 în $\mathbb{Z}$.)

5.16. Indicaţii. Dacă q şi r sunt câtul şi restul împărţirii lui a la b în $\mathbb{Z}$ şi $0 \le r \le \frac{|b|}{2}$ atunci $q' = q$ şi $r' = r$, iar dacă $\frac{|b|}{2} < r < |b|$ atunci $q' = q + \frac{|b|}{b}$ şi $r' = r - |b|$. Numerele q', r' nu sunt unic determinate: de exemplu, $7 = 2 \cdot 3 + 1 = 2 \cdot 4 + (-1)$.

5.17. Răspuns. a) 68; b) $X^2 + X + 1$ şi $X^3 - 1$.

5.18. Indicaţie. Se ştie că dacă $(x, y) = d'$ atunci există $p, q \in R$ astfel încât $d' = xp+yq$ şi că $d = (a, b, c) = ((a, b), c)$. Dacă $1 = au + bv + ct$ şi p este un divizor comun pentru a, b, c atunci $p|(au + bv + ct)$ şi implicit $p \sim 1$.

5.19. i) Fie $d = (a, b)$. Dacă există $x, y \in R$ astfel îcât $ax + by = c$ atunci $d|c$. Reciproc, din $dR = aR + bR$ rezultă existenţa $x', y' \in R$ astfel încât $ax' + by' = d$. Înmulţind cu $c' = \frac{c}{d}$ obţinem $ac'x' + bc'y' = c$, prin urmare $c'x'$ şi $c'y'$ verifică ecuaţia dată.
ii) Fie $d = (a, b)$ şi $a' = \frac{a}{d}$, $b' = \frac{b}{d}$. Dacă (x_0, y_0), (x, y) sunt soluţii ale ecuaţiei date atunci $a(x - x_0) + b(y - y_0) = 0$ sau, echivalent, $a'(x - x_0) + b'(y - y_0) = 0$. Cum $(a', b') = 1$ rezultă că $x - x_0 = b't$ şi $y - y_0 = a't'$, cu $t, t' \in R$. Este imediat faptul că $t' = -t$, deci $x = x_0 + b't$, $y = y_0 - a't$.

5.20. i) Notăm $a = 31$ şi $b = 17$. Avem $(a, b) = 1$, ceea ce implică existenţa $m, n \in \mathbb{Z}$ astfel încât $am + bn = 1$. Folosind algoritmul lui Euclid avem $a = b \cdot 1 + r_1$ cu $r_1 = 14$, $b = r_1 \cdot 1 + r_2$ cu $r_2 = 3$, $r_1 = r_2 \cdot 4 + r_3$ cu $r_3 = 2$ şi $r_2 = r_3 \cdot 1 + r_4$ cu $r_4 = 1 = (a, b)$, de unde deducem $11b - 6a = 1$. Deci $m = -6$ şi $-n = -11$ este o soluţie din $\mathbb{Z}$ a ecuaţiei date. Soluţia generală este

$$x = m - k(-17) = -6 + 17k,\ y = -n + k \cdot 31 = -11 + 31k,\ \text{cu } k \in \mathbb{Z}.$$

ii) Folosind i) avem $x, y \in \mathbb{N}^*$ dacă şi numai dacă $k > \max\left\{\frac{6}{17}, \frac{11}{31}\right\}$, $k \in \mathbb{N}^*$, ceea ce are loc pentru orice $k \in \mathbb{N}^*$. Deci

$$x = -6 + 17k,\ y = -11 + 31k,\ \text{cu } k \in \mathbb{N}^*.$$

5.21. Indicaţii. a) Avem $x = 2 + 7m = 3 + 6n$ $(m, n \in \mathbb{Z})$ de unde rezultă $7m - 6n = 1$. Se deduce $m = 1 + 6k$, $n = 1 + 7k$ cu $k \in \mathbb{Z}$ prin urmare $x \equiv 9 (\bmod 42)$.
b) Congruenţa $3x \equiv 2 (\bmod 5)$ este echivalentă cu $x \equiv 4 (\bmod 5)$ şi sistemul dat devine

$$\begin{cases} x \equiv 4 (\bmod 5) \\ x \equiv 6 (\bmod 7) \\ x \equiv 1 (\bmod 6) \end{cases}.$$

Ca mai sus, din primele două congruenţe se obţine $x \equiv -1 (\bmod 35)$, ceea ce, împreună cu ultima congruenţă conduce la $x \equiv 139 (\bmod 210)$.

5.22. Avem

$$mx \equiv c (\mathrm{mod}\, a) \Leftrightarrow \exists z \in \mathbb{Z}: \ mx - az = c,$$
$$(m,a) = 1 \Leftrightarrow \exists p, q \in \mathbb{Z}: \ ms - at = 1 \Rightarrow mcp - acq = c,$$

de unde deducem că $x_0 = cq$ este o soluţie a primei congruenţe. Un număr întreg x este o soluţie a primei congruenţe dacă şi numai dacă $m(x - x_0) \equiv 0(\text{mod } a)$, iar cum $(m,a) = 1$, avem $x \equiv x_0(\text{mod } a)$. Analog se poate obţine o soluţie particulară y_0 pentru congruenţa a doua, iar $y \in \mathbb{Z}$ este, de asemenea, soluţie a celei de-a doua congruenţe dacă şi numai dacă $y \equiv y_0(\text{mod } b)$. Pentru ca cele două congruenţe să aibă o soluţie comună este necesar şi suficient să existe $r, s \in \mathbb{Z}$ astfel încât $x_0 + ar = y_0 + bs$, adică $ar - bs = y_0 - x_0$, ceea ce rezultă imediat din $(a,b) = 1$.

Observaţie: Se verifică cu uşurinţă că soluţia comună a congruenţelor din problema de mai sus este unică modulo ab.

5.23. Indicaţie. Afirmaţia din enunţ este o generalizare a *teoremei chineze a resturilor* (pentru 2 congruenţe) (vezi [34, Corolarul 5.5.7 a)]) şi se demonstrează, pornind de la aceasta, prin inducţie după k.

5.24. $mx \equiv c(\bmod a)$ dacă şi numai dacă există $y \in \mathbb{Z}$ astfel încât

$$mx - ay = c. \tag{1}$$

Aşadar, congruenţa dată are soluţie dacă şi numai dacă ecuaţia (1) are soluţie în $\mathbb{Z} \times \mathbb{Z}$, ceea ce, conform problemei **5.19**, are loc dacă şi numai dacă $(m,a)|c$. Dacă (x_0, y_0) este o soluţie a ecuaţiei (1) atunci soluţiile lui (1) sunt aceleaşi cu soluţiile ecuaţiei

$$\frac{m}{(m,a)}(x - x_0) - \frac{a}{(m,a)}(y - y_0) = 0. \tag{2}$$

Cum $\left(\frac{m}{(m,a)}, \frac{a}{(m,a)}\right) = 1$, (2) conduce la congruenţa $x \equiv x_0 \left(\bmod \frac{a}{(m,a)}\right)$, care are (m,a) soluţii necongruente modulo a.

5.25. 1) Fie $d = (x,y)$ şi $x = dx'$, $y = dy'$ atunci $d|z$, iar dacă $z = dz'$ atunci

$$x^2 + y^2 = z^2 \Leftrightarrow x'^2 + y'^2 = z'^2.$$

2) Dacă x şi y sunt impare, adică $x \equiv 1(\text{mod } 2)$ şi $y \equiv 1(\text{mod } 2)$ se deduce că $x^2 + y^2 \equiv 2(\text{mod } 4)$ adică $z^2 \equiv 2(\text{mod } 4)$. Dar, dacă z este par atunci $z^2 \equiv 0(\text{mod } 4)$, iar dacă z este impar atunci $z^2 \equiv 1(\text{mod } 4)$, ceea ce înseamnă că congruenţa $z^2 \equiv 2(\text{mod } 4)$ nu poate avea loc.

Dacă x este impar şi y este par atunci z este impar şi $y^2 = (z+x)(z-x)$. Numerele $z + x$ şi $z - x$ sunt ambele pare şi 2 este singurul lor divizor comun prim. Într-adevăr, un alt divizor comun prim p al lor ar fi impar, ar divide pe y^2, pe $(z+x) + (z-x) = 2z$ şi pe $(z+x) - (z-x) = 2x$. Urmează că $p|x$ şi $p|y$, contradicţie cu $(x,y) = 1$. Rezultă că $\frac{z+x}{2}$ şi $\frac{z-x}{2}$ sunt numere întregi prime între ele ale căror produs $\frac{y^2}{4} = \frac{z+x}{2} \cdot \frac{z-x}{2}$ este un pătrat perfect. Cum factorii primi din descompunerea lui $\dfrac{y^2}{4}$ au toţi exponent par, pentru a nu contrazice condiţia $\left(\dfrac{z+x}{2}, \dfrac{z-x}{2}\right) = 1$ este necesar ca factorii primi din descompunerea lui $\dfrac{y^2}{4}$ să apară fie numai în descompunerea lui $\dfrac{z+x}{2}$, fie numai în descompunerea lui $\dfrac{z-x}{2}$, cu acelaşi exponent ca în descompunerea lui $\dfrac{y^2}{4}$. Prin urmare, $\dfrac{z+x}{2}$ şi $\dfrac{z-x}{2}$ sunt, de asemenea, pătrate perfecte, deci putem considera $z+x = 2m^2$ şi $z-x = 2n^2$, cu $m, n \in \mathbb{Z}$, şi astfel obţinem

$$x = m^2 - n^2, \; z = m^2 + n^2 \text{ şi } y = 2mn.$$

Se verifică uşor că dacă x, y, z au forma de mai sus atunci ele verifică ecuaţia $x^2+y^2 = z^2$.

5.26. Indicaţii. Se foloseşte faptul că $\delta(z_1z_2) = \delta(z_1)\delta(z_2)$ pentru orice $z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$ şi că $z \in \mathbb{Z}[\sqrt{d}]$ este inversabil dacă şi numai dacă $\delta(z) = 1$ (vezi problema **3.33**).
ii) Dacă $z_2 = z_1z$ ($z \in \mathbb{Z}[\sqrt{d}]$) atunci $\delta(z_2) = \delta(z_1)\delta(z)$. Din $\delta(z_1) = \delta(z_2)$ rezultă că $z_1 = z_2 = 0$ sau $\delta(z) = 1$, adică z e inversabil, prin urmare $z_1 \sim z_2$.
iii) În $\mathbb{Z}[i]$, $\delta(1+2i) = \delta(1-2i) = 5$, dar $\dfrac{1+2i}{1-2i} \notin \mathbb{Z}[i]$.
iv) Dacă $z = z_1z_2$ în $\mathbb{Z}[\sqrt{d}]$ atunci $\delta(z) = \delta(z_1)\delta(z_2)$ în $\mathbb{N}$ cu $\delta(z)$ număr prim, prin urmare sau $\delta(z_1) = 1$ sau $\delta(z_2) = 1$.

5.27. Să remarcăm pentru început că funcţia $\delta : \mathbb{Z}[i] \to \mathbb{N}$, $\delta(z) = |z\overline{z}|$ este o restricţie a funcţiei $\delta_0 : \mathbb{Q}(i) \to \mathbb{Q}$, $\delta_0(z) = |z\overline{z}|$ care are, de asemenea, proprietatea că $\delta_0(z_1z_2) = \delta_0(z_1)\delta_0(z_2)$ pentru orice $z_1, z_2 \in \mathbb{Q}(i)$. Fie $z_1 = a_1+b_1i$, $z_2 = a_2+b_2i \neq 0$, cu $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Arătăm că există numerele $q, r \in \mathbb{Z}[i]$ astfel încât $z_1 = z_2q + r$, unde $\delta(r) < \delta(z_2)$ (să observăm că această condiţie cuprinde şi posibilitatea ca $r = 0$). Avem $z = \dfrac{z_1}{z_2} \in \mathbb{Q}(i)$, adică $z = a + bi$ cu $a, b \in \mathbb{Q}$. Considerăm numerele întregi m, n cele mai apropiate de a, respectiv b, adică $m, n \in \mathbb{Z}$ astfel încât $|a-m| \leq \dfrac{1}{2}$ şi $|b-n| \leq \dfrac{1}{2}$. Luând $q = m + ni \in \mathbb{Z}[i]$ şi $z_3 = z - q = (a-m) + (b-n)i \in \mathbb{Q}(i)$ avem $z_1 = z_2z = z_2q + z_2(z-q) = z_2q + z_2z_3$, prin urmare $z_2z_3 = z_1 - z_2q \in \mathbb{Z}[i]$. Notăm $r = z_2z_3$ şi avem:

$$\begin{aligned}\delta(r) &= \delta(z_2z_3) = \delta_0(z_2z_3) = \delta_0(z_2)\delta_0(z_3) = \delta(z_2)\delta_0(z_3)\\ &= \delta(z_2)\left[(a-m)^2 + (b-n)^2\right] \leq \delta(z_2)\left(\frac{1}{4}+\frac{1}{4}\right) = \frac{\delta(z_2)}{2} < \delta(z_2).\end{aligned}$$

a) Aplicăm algoritmul lui Euclid pentru a determina c.m.m.d.c. al lui z_1 şi z_2. Conform celor de mai sus, avem $z_1 = z_2q + r$, unde $q, r \in \mathbb{Z}[i]$, cu $\delta(r) < \delta(z_2)$, se obţin astfel: din

$$\frac{z_1}{z_2} = \frac{12-3i}{3+6i} = \frac{4-i}{1+2i} = \frac{2}{5} - \frac{9}{5}\,i$$

rezultă $q = -2i$, prin urmare,

$$r = z_1 - z_2q = (12-3i) + 2i(3+6i) = 3i.$$

Determinăm acum $q_1, r_1 \in \mathbb{Z}[i]$ cu $\delta(r_1) < \delta(r)$, astfel încât $z_2 = rq_1 + r_1$. Din

$$\frac{z_2}{r} = \frac{3+6i}{3i} = \frac{1+2i}{i} = 2 - i \in \mathbb{Z}[i]$$

rezultă $q_1 = \dfrac{z_2}{r}$ şi astfel $r_1 = z_2 - rq_1 = 0$. Prin urmare,

$$(z_1, z_2) = 3i \sim -3i \sim 3 \sim -3 \text{ şi } [z_1, z_2] \sim \frac{z_1 z_2}{(z_1, z_2)} = (12 - 3i)(2 - i) = 30 - 18i.$$

b) Cum toate idealele unui domeniu euclidian sunt principale, corespondenţa $\widehat{z} \mapsto (z) = z\mathbb{Z}[i]$, unde $\widehat{z}$ este clasa de elemente asociate în divizibilitate cu z, stabileşte un antiizomorfism de ordine (deci şi laticial) între laticea $(\mathbb{Z}[i]/\sim, \leq)$ şi laticea idealelor lui $\mathbb{Z}[i]$. De aici rezultă

$$(z_1) \cap (z_2) = z_1\mathbb{Z}[i] \cap z_2\mathbb{Z}[i] = z_1\mathbb{Z}[i] \wedge z_2\mathbb{Z}[i] = (30 - 18i)\mathbb{Z}[i],$$
$$(z_1) + (z_2) = z_1\mathbb{Z}[i] + z_2\mathbb{Z}[i] = z_1\mathbb{Z}[i] \vee z_2\mathbb{Z}[i] = 3i\mathbb{Z}[i].$$

5.28. Fie $z_1, z_2 \in \mathbb{Z}[\theta]$ cu $z_2 \neq 0$. Notăm $N(z_2) = z_2\overline{z_2} \neq 0$ şi avem

$$\frac{z_1}{z_2} = \frac{z_1\overline{z_2}}{z_2\overline{z_2}} = \frac{z_3}{N(z_2)}, \text{ unde } z_3 = z_1\overline{z_2}.$$

Dar $z_3 \in \mathbb{Z}[\theta]$, rezultă că există $m, n \in \mathbb{Z}$ astfel încât $z_3 = m + n\theta$. Aplicând problema **5.16** deducem că există $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ astfel încât

$$(1) \qquad m = N(z_2)q_1 + r_1,\ n = N(z_2)q_2 + r_2 \text{ şi } |r_1|, |r_2| \leq \frac{|N(z_2)|}{2},$$

ceea ce implică

$$\frac{z_1}{z_2} = \frac{m + n\theta}{N(z_2)} = \frac{N(z_2)q_1 + r_1 + N(z_2)q_2\theta + r_2\theta}{N(z_2)} = (q_1 + q_2\theta) + \frac{r_1 + r_2\theta}{N(z_2)}.$$

Dacă notăm $Q = q_1 + q_2\theta$ şi $R = \dfrac{z_2(r_1 + r_2\theta)}{N(z_2)}$ atunci $Q \in \mathbb{Z}[\theta]$ şi $z_1 = z_2Q + R$. Urmează că $R = z_1 - z_2Q \in \mathbb{Z}[\theta]$, iar cum $RN(z_2) = z_2(r_1 + r_2\theta)$ avem şi

$$\delta(R)[N(z_2)]^2 = \delta(R)\delta(N(z_2)) = \delta(z_2)\delta(r_1 + r_2\theta) = |N(z_2)|\delta(r_1 + r_2\theta).$$

Cum $\delta(z_2) = |N(z_2)|$, rezultă, prin împărţire la $[N(z_2)]^2 \neq 0$, că

$$\delta(R) = \frac{\delta(r_1 + r_2\theta)}{\delta(z_2)} = \frac{1}{\delta(z_2)}\left|r_1^2 - pr_1r_2 + qr_2^2\right|.$$

Dar $|r_1^2 - pr_1r_2 + qr_2^2| \leq |r_1|^2 + |p||r_1||r_2| + |q||r_2|^2$ şi, folosind (1), avem

$$(2) \qquad \delta(R) \leq \frac{1}{\delta(z_2)} \cdot \frac{\delta(z_2)^2}{4}(1 + |p| + |q|) = \delta(z_2)(1 + |p| + |q|).$$

Dacă $|p| + |q| < 3$ atunci $\delta(R) < \delta(z_2)$ şi problema este rezolvată.

5.29. Răspuns. $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}\left[\sqrt{2}\right]$, $\mathbb{Z}\left[i\sqrt{2}\right]$, $\mathbb{Z}\left[\dfrac{1+i\sqrt{3}}{2}\right]$, $\mathbb{Z}\left[\dfrac{1+\sqrt{5}}{2}\right]$.

5.30. Indicaţie. Dacă $\theta \in \left\{\dfrac{1+i\sqrt{7}}{2}, \dfrac{1+i\sqrt{11}}{2}\right\}$ atunci orice $z = m + n\theta$ se scrie sub forma $z = \left(m + \dfrac{n}{2}\right) + \dfrac{n}{2}\sqrt{d}$, unde $d \in \{-7, -11\}$. Fie $\delta : \mathbb{Z}[\theta] \to \mathbb{N}$, $\delta(z) = |z\overline{z}|$ şi $z_1, z_2 \in \mathbb{Z}[\theta]$ cu $z_2 \neq 0$. Se pot găsi $q, r \in \mathbb{Z}[\theta]$, $\delta(r) < \delta(z_2)$ cu proprietatea că $z_1 = z_2q + r$ astfel: dacă $\dfrac{z_1}{z_2} = a + b\theta = \left(a + \dfrac{b}{2}\right) + \dfrac{b}{2}\sqrt{d} \in \mathbb{Q}(\theta)$ $(a, b \in \mathbb{Q})$ aunci considerăm n numărul întreg cel mai apropiat de b şi m numărul întreg cel mai apropiat de $a + \dfrac{b}{2} - \dfrac{n}{2}$ şi luăm $q = m + n\theta$ şi $r = z_1 - z_2q$.

5.31. Cum $\mathbb{Z}[i]$ este cu ideale principale, există $a, b \in \mathbb{Z}$, nu ambele nule, astfel încât $U = (a + bi) = (a + bi)\mathbb{Z}[i]$. Dar orice $z \in \mathbb{Z}[i]$ se scrie sub forma

$$z = (a + bi)q + r, \text{ cu } q, r \in \mathbb{Z}[i] \text{ şi } \delta(r) < a^2 + b^2.$$

Dar, pentru $a, b \in \mathbb{Z}$ fixate, mulţimea $\{r = m + ni \in \mathbb{Z}[i] \mid \delta(r) < a^2 + b^2\}$ coincide cu mulţimea punctelor din plan de coordonate întregi situate în interiorul cercului de rază $\sqrt{a^2 + b^2}$ cu centrul în originea axelor, care este o mulţime finită. Prin urmare, şi mulţimea $\mathbb{Z}[i]/U = \{r + U \mid \delta(r) < a^2 + b^2\}$ este finită.

5.32. 1) a) Cum $2 = (1 + i)(1 - i)$ este un produs de elementele neinversabile $(\delta(1 + i) = \delta(1 - i) = 2 \neq 1)$ rezultă că 2 este reductibil în $\mathbb{Z}[i]$. De asemenea, $5 = (1 + 2i)(1 - 2i)$ şi $17 = (1 + 4i)(1 - 4i)$ sunt produse de elemente neinversabile.
b) Cum $\delta(3) = 9$ avem 3 neinversabil, iar dacă $z_k = a_k + b_ki \in \mathbb{Z}[i]$, $k = 1, 2$ şi $3 = z_1z_2$ atunci $9 = \delta(z_1)\delta(z_2)$. Cum $\delta(z_k) = a_k^2 + b_k^2 \in \mathbb{N}$ $(k = 1, 2)$, această egalitate are loc doar în următoarele cazuri:
• $\delta(z_1) = 1$ şi $\delta(z_2) = 9$, caz în care z_1 este inversabil;
• $\delta(z_1) = \delta(z_2) = 3$, caz care nu convine deoarece nu există $a_k, b_k \in \mathbb{Z}$ astfel încât $a_k^2 + b_k^2 = 3$ (dacă $a_k = 0$ atunci $b_k^2 = 3$ şi $b_k \notin \mathbb{Z}$, dacă $|a_k| = 1$ atunci $b_k^2 = 2$ şi, din nou, $b_k \notin \mathbb{Z}$, iar dacă $|a_k| \geq 2$ atunci $b_k^2 < 0$, prin urmare numărul b_k nu e nici măcar real).
• $\delta(z_1) = 9$ şi $\delta(z_2) = 1$, caz în care z_2 este inversabil.
Aşadar, $3 = z_1z_2$ implică z_1 inversabil sau z_2 inversabil, prin urmare 3 este ireductibil în $\mathbb{Z}[i]$. Analog se arată că 7 este element ireductibil în $\mathbb{Z}[i]$.
c) Numerele $\delta(1 + i) = 2$, $\delta(1 + 2i) = 5$ sunt prime şi se aplică problema **5.26** iv).
2) $4 = (1 + i)^2(1 - i)^2 = -(1 + i)^4$, $18 + 36i = 18(1 + 2i) = (-i)3^2(1 + i)^2(1 + 2i)$.

5.33. Indicaţii. a) Dacă $z \in \mathbb{Z}[i]$ este un element ireductibil (deci şi prim) atunci z divide pe $z\overline{z} = \delta(z) \in \mathbb{N}$. Considerând descompunerea lui $\delta(z)$ în produs de numere prime şi presupunând că z este element prim, obţinem concluzia dorită.
b) Pentru $k \in \mathbb{N}$ ecuaţia $a^2 + b^2 = 4k + 3$ nu are soluţii $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ deoarece dacă a şi b au aceeaşi paritate atunci $2 \mid (a^2 + b^2)$, iar în caz contrar $a^2 + b^2 \equiv 1 (\mathrm{mod}\ 4)$.

c) Evident p este impar. Avem

$$\begin{aligned} p-1 &\equiv -1 (\operatorname{mod} p) \\ p-2 &\equiv -2 (\operatorname{mod} p) \\ &\vdots \\ \frac{p-1}{2}+1 &\equiv -\frac{p-1}{2} (\operatorname{mod} p), \end{aligned}$$

prin urmare,

$$(p-1)(p-2)\cdots\left(\frac{p-1}{2}+1\right) \equiv (-1)^{\frac{p-1}{2}}\left(1\cdot 2\cdots\frac{p-1}{2}\right)(\operatorname{mod} p).$$

Cum $p \equiv 1(\operatorname{mod} 4)$ avem $(-1)^{\frac{p-1}{2}} = 1$, aşadar,

$$(p-1)(p-2)\cdots\left(\frac{p-1}{2}+1\right) \equiv \left(\frac{p-1}{2}\right)!(\operatorname{mod} p),$$

de unde, înmulţind cu $\left(\frac{p-1}{2}\right)!$, rezultă

$$(p-1)! \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 (\operatorname{mod} p).$$

Dar, conform teoremei lui Wilson avem $(p-1)!+1 \equiv 0(\operatorname{mod}\ p)$. Notând $n = \left(\frac{p-1}{2}\right)!$, obţinem $1+n^2 \equiv 0(\operatorname{mod}\ p)$, adică p divide pe $1+n^2 = (1-ni)(1+ni)$. Presupunând că p ar fi element prim în $\mathbb{Z}[i]$, am avea $p|(1-ni)$ sau $p|(1+ni)$. Dacă $p|(1-ni)$ ar rezulta că există $a, b \in \mathbb{Z}$ astfel încât $1-ni = p(a+bi)$, ceea ce ar implica $pa = 1$, adică $p \in \{-1, 1\}$, contradicţie cu p număr prim. Deci p nu este element prim în $\mathbb{Z}[i]$, ceea ce înseamnă că poate fi scris ca un produs de cel puţin două elemente ireductibile $z_1, \ldots, z_k \in \mathbb{Z}[i]$

$$p = z_1 \cdots z_k \Rightarrow p^2 = \delta(p) = \delta(z_1)\cdots\delta(z_k).$$

Cum p este număr prim, avem $k = 2$, adică $p = z_1 z_2$. Prin urmare, $z_1\overline{z_1} = \delta(z_1)$ divide pe $p = z_1 z_2$, adică $\overline{z_1}$ divide elementul ireductibil z_2. Rezultă $\overline{z_1} \in \{z_2, -z_2, iz_2, -iz_2\}$, ceea ce, împreună cu $z_1 z_2 = p \in \mathbb{N}$, implică $\overline{z_1} = z_2$. Presupunerea că $\overline{z_1} \sim z_1 = a+bi$ ($a, b \in \mathbb{Z}$ nu ambele nule) ar conduce la $(a^2+b^2)|(a^2-b^2)$ deoarece

$$\frac{a^2-b^2}{a^2+b^2} + \frac{2ab}{a^2+b^2} i = \frac{a+bi}{a-bi} \in \{-1, 1, -i, i\}.$$

Urmează că $a = \pm b$, ceea ce înseamnă că $z_1 = a(1+i)$ cu $a \in \{-1, 1, -i, i\}$, sau $b = 0$, adică $z_1 = a$. Dar atunci $p = 2$ sau $p = a^2$, contradicţie cu ipoteza p prim şi $4|(p-1)$.

Observaţie: Orice număr prim $p \in \mathbb{N}$ este de forma $4k+1$ sau $4k+3$ cu $k \in \mathbb{N}$.

5.34. a) Ca în soluţia problemei **5.32** punctul b) se arată că 3 este ireductibil în $\mathbb{Z}\left[i\sqrt{5}\right]$, dar 3 nu este element prim deoarece 3 divide pe $6 = \left(1+i\sqrt{5}\right)\left(1-i\sqrt{5}\right)$ dar cum $\delta(3) = 9$ nu divide pe $\delta\left(1+i\sqrt{5}\right) = \delta\left(1-i\sqrt{5}\right) = 6$ rezultă că 3 nu divide nici pe $1+i\sqrt{5}$ nici pe $1-i\sqrt{5}$.

b) Presupunând că $d = a + bi,\ a, b \in \mathbb{Z}$ ar fi un c.m.m.d.c. al lui 6 şi $2\left(1 + i\sqrt{5}\right)$ am avea $d\,|\,6$ şi $d\,|\,2\left(1 + i\sqrt{5}\right)$, ceea ce ar implica

$$\delta(d)\,|\,\delta(6) = 36 \text{ şi } \delta(d)\,|\,\delta(2(1 + i\sqrt{5})) = \delta(2)\delta(1 + i\sqrt{5}) = 4 \cdot 6 = 24.$$

Aşadar, $\delta(d)|(36, 24) = 12$. Dar 2 şi $1 + i\sqrt{5}$ sunt divizori comuni pentru 6 şi $2\left(1 + i\sqrt{5}\right)$, prin urmare, ar fi şi divizori ai lui d. Ar rezulta că

$$\delta(2) = 4\,|\,\delta(d) \text{ şi } 6 = \delta(1 + i\sqrt{5})\,|\,\delta(d),$$

de unde am deduce că $12 = [4, 6]|\delta(d)$. Astfel, am obţine $a^2 + 5b^2 = \delta(d) = 12$ cu $a, b \in \mathbb{Z}$, ceea ce nu este posibil (dacă $|b| \leq 1$ atunci $a \in \mathbb{R} \setminus \mathbb{Q}$, iar dacă $|b| \geq 2$ atunci $a \in \mathbb{C} \setminus \mathbb{Q}$).
c) Cum 3 este element ireductibil, singurii săi divizori sunt (abstracţie făcând de o asociere în divizibilitate) 1 şi 3. Cum 3 nu divide pe $\left(1 + i\sqrt{5}\right)$, singurul divizor comun pentru 3 şi $1 + i\sqrt{5}$ este 1, care este şi cel mai mare divizor comun al lor.

5.35. Indicaţii. Fie $d = (m, n)$. Cum pentru orice $k \in \mathbb{N}^*$, $x, y \in R$, $x - y$ divide pe $x^k - y^k$ în R, avem $a^d - b^d$ divide pe $a^m - b^m$ şi pe $a^n - b^n$. Dacă numerele naturale q, r sunt câtul şi restul împărţirii lui m la n atunci

$$a^m - b^m = a^{nq+r} - b^{nq+r} = a^{nq}a^r - a^{nq}b^r + a^{nq}b^r - b^{nq}b^r = a^{nq}\left(a^r - b^r\right) + \left(a^{nq} - b^{nq}\right)b^r.$$

Întrucât un element α care divide pe $a^d - b^d$ va divide pe $a^m - b^m$ şi pe $a^{nq} - b^{nq}$, rezultă că va divide şi pe $a^{nq}\left(a^r - b^r\right)$. Dacă $(\alpha, a^{nq}) \neq 1$ atunci un element prim p care ar divide pe α şi pe a^{nq} ar divide pe a şi pe $a^m - b^m$, deci şi pe b, contradicţie cu $(a, b) = 1$. Rezultă că $\alpha|\left(a^r - b^r\right)$. Aplicând cele de mai sus resturilor ce se obţin din algoritmul lui Euclid pentru aflarea $(m, n) \in \mathbb{N}$ se va constata că $\alpha|\left(a^d - b^d\right)$.

5.36. Cum f este primitiv şi $p|a_0, \ldots, p|a_{n-1}$ avem $a_n \neq 0$ şi p nu divide pe a_n, deci $\operatorname{grad} f \geq 1$ de unde rezultă că f este neinversabil. Să presupunem că $f = gh$, unde polinoamele

$$g = b_0 + b_1X + \cdots + b_mX^m \text{ şi } h = c_0 + c_1X + \cdots + c_pX^p,$$

sunt neinversabile în $\mathbb{Z}[X]$ $(b_0, \ldots, b_m, c_0, \ldots, c_p \in \mathbb{Z},\ m, p \in \mathbb{N},\ b_m \neq 0 \neq c_p)$. Evident $m + p = n$, iar dacă $m = 0$ şi $g = b_0$ este neinversabil în $\mathbb{Z}$ atunci $b_0|f$ implică $b_0|(a_0, \ldots, a_n) = 1$, contradicţie. Aşadar, $m \geq 1$ şi $p \geq 1$ şi avem

$$b_0c_0 = a_0,\ b_1c_0 + b_0c_1 = a_1\ \ldots,\ b_mc_p = a_n. \tag{1}$$

Cum p este prim şi $p|a_0 = b_0c_0$ avem $p|b_0$ sau $p|c_0$. Dar p^2 nu divide pe a_0. Rezultă că dacă $p|b_0$ atunci p nu divide pe c_0, iar dacă $p|c_0$ atunci p nu divide pe b_0. Să considerăm că $p|b_0$ şi p nu divide pe c_0. Din $p|a_1 = b_1c_0 + b_0c_1$ şi $p|b_0$ deducem că $p|b_1c_0$, iar cum p nu divide pe c_0, avem $p|b_1$. Procedând analog şi cu celelalte egalităţi din (1) obţinem $p|b_m$, deci $p|a_n = b_mc_p$, ceea ce contrazice faptul că $(a_0, \ldots, a_{n-1}, a_n) = 1$.

5.37. Indicaţie. Folosind criteriul lui Eisenstein se atrată că pentru orice $n \in \mathbb{N}^*$, polinomul $f = X^n + 2$ este ireductibil în $\mathbb{Z}[X]$ deci şi în $\mathbb{Q}[X]$. Dacă $p \in \mathbb{Z}$ este prim atunci p este ireductibil în $\mathbb{Z}$, dar nu este ireductibil în $\mathbb{Q}$.

5.38. Indicaţie. Se aplică problemele **3.114** şi **5.6**.

5.39. Arătăm că $f = \dfrac{X^p - 1}{X - 1}$ este ireductibil peste $\mathbb{Z}$, deci şi peste $\mathbb{Q}$. Din problema anterioară avem f ireductibil în $\mathbb{Z}[X]$ dacă şi numai dacă

$$f(X+1) = E_{X+1}(f) = \frac{(X+1)^p - 1}{(X+1) - 1} = X^{p-1} + \sum_{k=1}^{p-1} C_p^k X^{p-k} + p$$

este ireductibil în $\mathbb{Z}[X]$. Dar fiecare factor din numitorul lui

$$C_p^k = \frac{p(p-1)\cdots(p-k+1)}{2\cdots k} \in \mathbb{N}^*$$

este relativ prim cu p, prin urmare $2\cdots k = k!|(p-1)\cdots(p-k+1)$ şi astfel,

$$p|C_p^1, \dots,\ p|C_p^p - 1,\ p|p,\ \text{dar } p^2 \text{ nu divide pe } p,$$

deci $E_{X+1}(f)$ este ireductibil în $\mathbb{Z}[X]$.

5.40. Indicaţii. b) Este un caz particular al lui c).
c) Se procedează ca în problema anterioară, se obţine

$$E_{X+1}(X^{p^n} + p - 1) = X^{p^n} + \sum_{k=1}^{p^n - 1} C_{p^n}^k X^k + p,$$

iar $C_{p^n}^k = \dfrac{p^n(p^n-1)\cdots(p^n-k+1)}{k!}$ se divide cu p pentru orice $1 \le k \le p^n - 1$.

5.41. Indicaţii. Conform problemei anterioare, polinoamele $X^4 + 1$ şi $X^8 + 1$ sunt ireductibile în $\mathbb{Z}[X]$ şi în $\mathbb{Q}[X]$. În $\mathbb{Z}[X]$ descompunerile celorlalte polinoame sunt: i) $40X^2 - 20X = 2^2 \cdot 5 \cdot X(2X-1)$; ii) $10X^2 + 5X - 5 = 5(X+1)(2X-1)$; iii) $X^3 - 8 = (X-2)(X^2+2X+4)$; iv) $X^3+8 = (X+2)(X^2-2X+4)$; v) $X^4-1 = (X+1)(X-1)(X^2+1)$; vii) $X^6-1 = (X+1)(X-1)(X^2+X+1)(X^2-X+1)$; viii) $X^6+1 = (X^2+1)(X^4-X^2+1)$; ix) $X^8 - 1 = (X+1)(X-1)(X^2+1)(X^4+1)$.

În $\mathbb{Q}[X]$ descompunerile sunt: i) $40X^2 - 20X = X(40X-20)$; ii) $10X^2 + 5X - 5 = (5X+5)(2X-1)$; iii) $X^3 - 8 = (X-2)(X^2+2X+4)$; iv) $X^3+8 = (X+2)(X^2-2X+4)$; v) $X^4-1 = (X+1)(X-1)(X^2+1)$; vii) $X^6-1 = (X+1)(X-1)(X^2+X+1)(X^2-X+1)$; viii) $X^6+1 = (X^2+1)(X^4-X^2+1)$; ix) $X^8-1 = (X+1)(X-1)(X^2+1)(X^4+1)$.

În $\mathbb{R}[X]$ descompunerile sunt: i) $40X^2 - 20X = X(40X-20)$; ii) $10X^2 + 5X - 5 = (5X+5)(2X-1)$; iii) $X^3 - 8 = (X-2)(X^2+2X+4)$; iv) $X^3+8 = (X+2)(X^2-2X+4)$; v) $X^4 - 1 = (X+1)(X-1)(X^2+1)$; vi) $X^4+1 = (X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1)$; vii) $X^6-1 = (X+1)(X-1)(X^2+X+1)(X^2-X+1)$; viii) $X^6+1 = (X^2+1)(X^2+\sqrt{3}X+1)(X^2-\sqrt{3}X+1)$; ix) $X^8-1 = (X+1)(X-1)(X^2+1)(X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1)$; x) $X^8+1 = (X^2+\sqrt{2+\sqrt{2}}X+1)(X^2-\sqrt{2+\sqrt{2}}X+1)(X^2+\sqrt{2-\sqrt{2}}X+1)(X^2-\sqrt{2-\sqrt{2}}X+1)$. Descompunerile din $\mathbb{C}[X]$ rezultă prin descompunerea în factori de grad 1 a factorilor de grad 2 din descompunerile din $\mathbb{R}[X]$.

5.42. Răspuns. Descompunerea peste $\mathbb{Q}$ este $f = (X^2-3)(X^2-2)$, peste $\mathbb{Q}(\sqrt{2})$ este $f = (X^2-3)(X+\sqrt{2})(X-\sqrt{2})$, iar peste $\mathbb{R}$ este $f = (X+\sqrt{3})(X-\sqrt{3})(X+\sqrt{2})(X-\sqrt{2})$.

5.43. Indicaţii. Reducerea modulo p defineşte un omomorfism surjectiv de la $\mathbb{Z}[X]$ la $\mathbb{Z}_p[X]$. a) Cum orice factor din descompunerea lui f este polinom unitar, redusul său modulo p va avea acelaşi grad. b) Dacă $f \in \mathbb{Z}[X] \setminus \mathbb{Z}$ este reductibil peste $\mathbb{Q}$ atunci f este reductibil peste $\mathbb{Z}$. Aplicând a) deducem că pentru orice p prim, redusul modulo p al lui f este reductibil peste $\mathbb{Z}_p$.

5.44. Indicaţii. Polinomul f este ireductibil peste $\mathbb{Q}$ deoarece redusul modulo 3 al lui f, $X^3 + \widehat{2}X + \widehat{1} \in \mathbb{Z}_3[X]$ nu are rădăcini în $\mathbb{Z}_3$. Redusul modulo 3 al lui g este, de asemenea ireductibil. Redusul modulo 3 al lui h este

$$X^4 + \widehat{2}X^3 + X^2 + \widehat{2}X + \widehat{2} = (X + \widehat{1})(X^3 + X^2 + \widehat{2}),$$

iar factorii din descompunerea de mai sus sunt ireductibili. Conform problemei anterioare şi unicităţii descompounerii unui polinom din $Z_3[X]$, deducem că dacă h ar fi reductibil, atunci s-ar scrie ca produsul dintre un polinom (unitar) de grad 1 şi un polinom (unitar) de grad 3. Aplicând din nou problema anterioară rezultă că redusul modulo 3 al factorului (unitar) de gard 1 este $X + \widehat{1}$, deci acest factor nu poate fi decât $X + 1$ sau $X - 5$. Cum redusul modulo 2 al celor două polinoame este $X - \overline{1}$ şi redusul modulo 2 al lui h, $X^4 + X^2 + \overline{1}$ nu se divide cu $X - \overline{1}$, urmează că h este ireductibil peste $\mathbb{Z}$, deci şi peste $\mathbb{Q}$.

5.45. Indicaţie. Dacă g ar avea o descompunere

$$g = (b_m + b_{m-1}X + \cdots + b_0X^m)(c_p + c_{p-1}X + \cdots + c_0X^p)$$

atunci $f = (b_0 + b_1X + \cdots + b_mX^m)(c_0 + c_1X + \cdots + c_pX^p)$ ar fi o descompunere a lui f.

5.46. i) Cum $\mathbb{Z}$ este un domeniu factorial, şi $\mathbb{Z}[X]$ este domeniu factorial. În $\mathbb{Z}[X]$ idealul $(2, X)$ este format din polinoamele care au termenul liber par deoarece

$$\begin{aligned}(2, X) &= 2\mathbb{Z}[X] + X\mathbb{Z}[X] = \{2f + Xg \mid f, g \in \mathbb{Z}[X]\}\\ &= \{2a_0 + a_1X + \cdots + a_nX^n \mid a_0, \dots, a_n \in \mathbb{Z},\ n \in \mathbb{N}\}.\end{aligned}$$

Dar acest ideal nu este principal, deoarece existenţa unui polinom $h \in \mathbb{Z}[X]$ astfel încât $(2, X) = (h)$ ar implica $h|2$ şi $h|X$, ceea ce ar conduce la faptul că h este inversabil, adică $(2, X) = (h) = \mathbb{Z}[X]$, ceea ce este fals, deoarece $1 + X \in \mathbb{Z}[X]$ nu are termenul liber par. Remarcăm că dacă $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$ atunci (a, X) nu este principal.

Observaţie: În Teoremele 5.7.9 şi 5.7.11 din [34] este demonstrat că dacă R este un domeniu factorial care nu este corp atunci $R[X]$ este un domeniu factorial şi are ideale care nu sunt principale, ceea ce generalizează problema de mai sus.

5.47. Indicaţie. Idealul (X, Y) este format din toate polinoamele cu termenul liber nul şi se arată, ca mai sus, că acesta nu poate fi generat cu un singur element.

5.48. Indicaţii. Dacă ar exista un polinom din $K[X, Y]$ care să genereze idealul $\left(X^2, XY, Y^2\right)$, acesta ar fi un divizor comun al lui X^2 şi Y^2, prin urmare, ar fi inversabil şi $\left(X^2, XY, Y^2\right) = K[X, Y]$, ceea ce e fals pentru că $0 \neq a + bX + cY \notin \left(X^2, XY, Y^2\right)$.

Dacă ar exista $f, g \in K[X, Y]$ astfel încât $\left(X^2, XY, Y^2\right) = (f, g)$ atunci

$$f = aX^2 + bXY + cY^2 + \cdots,\ g = a'X^2 + b'XY + c'Y^2 + \cdots$$

prin urmare, există $\alpha, \alpha', \beta, \beta', \gamma, \gamma' \in K$ astfel încât

$$\begin{aligned}
\alpha\left(aX^2+bXY+cY^2+\cdots\right)+\alpha'\left(a'X^2+b'XY+c'Y^2+\cdots\right)&=X^2,\\
\beta\left(aX^2+bXY+cY^2+\cdots\right)+\beta'\left(a'X^2+b'XY+c'Y^2+\cdots\right)&=XY,\\
\gamma\left(aX^2+bXY+cY^2+\cdots\right)+\gamma'\left(a'X^2+b'XY+c'Y^2+\cdots\right)&=Y^2,
\end{aligned}$$

ceea ce conduce la

$$\begin{array}{lll}
\alpha a+\alpha' a'=1; & \beta a+\beta' a'=0; & \gamma a+\gamma' a'=0;\\
\alpha b+\alpha' b'=0; & \beta b+\beta' b'=1; & \gamma b+\gamma' b'=0;\\
\alpha c+\alpha' c'=0; & \beta c+\beta' c'=0; & \gamma c+\gamma' c'=1.
\end{array}$$

Privim aceste egalităţi ca sisteme de ecuaţii liniare în $\alpha, \alpha', \beta, \beta', \gamma, \gamma'$. Existenţa elementelor $\alpha, \alpha', \beta, \beta', \gamma, \gamma' \in K$ este echivalentă cu faptul că sistemele de mai sus sunt compatibile, ceea ce se dovedeşte a fi fals.

Dacă notăm $U = \left(X^2, XY, Y^2\right)$ atunci $K[X,Y]/U = \{(a+bX+cY)+U \mid a,b,c \in K\}$ şi idealul $(X+U, Y+U)$ nu este principal.

5.49. i) $X^3 - Y^3 = (X-Y)(X^2+XY+Y^2)$. Polinomul $X-Y$, considerat ca polinom în X peste $\mathbb{Q}[Y]$ este primitiv şi de grad 1, prin urmare este ireductibil în $\mathbb{Q}[X,Y] = (\mathbb{Q}[Y])[X]$. Polinomul X^2+XY+Y^2, considerat ca polinom în X peste $\mathbb{Q}[Y]$ este primitiv. Arătăm prin reducere la absurd că, privit ca polinom în X peste corpul $\mathbb{Q}(Y)$, este ireductibil. Într-adevăr, cum $\operatorname{grad}_X(X^2+XY+Y^2)=2$, polinomul X^2+XY+Y^2 este reductibil peste corpul $\mathbb{Q}(Y)$ dacă şi numai dacă are o rădăcină $f = \dfrac{f_1}{f_2} \in \mathbb{Q}(Y)$ $(f_1, f_2 \in \mathbb{Q}[Y])$. În acest caz, $f^2+fY+Y^2=0$, prin urmare $[f(a)]^2+f(a)a+a^2=0$ pentru orice $a \in \mathbb{Q}^*$ care nu este rădăcină a lui f_2. Dar $a \in \mathbb{Q}^*$ şi $f(a) \in \mathbb{Q}$ implică $[f(a)]^2+f(a)a+a^2 \neq 0$, contradicţie.
ii) $Y^4 - X^2 = (Y^2-X)(Y^2+X)$. Polinoamele Y^2-X şi Y^2+X, considerate ca polinoame în X peste $\mathbb{Q}[Y]$ sunt primitive şi de grad 1, deci sunt ireductibile în $\mathbb{Q}[X,Y] = (\mathbb{Q}[Y])[X]$.
iii) $X^2 - Y^6 = (X-Y^3)(X+Y^3)$. Ireductibilitatea factorilor poate fi justificată ca la ii).
iv) Arătăm că polinomul $f = X^7+2X^3Y+3X^2+9Y$ este ireductibil în $\mathbb{Q}[X,Y]$. Într-adevăr, $\operatorname{grad}_Y f = 1$ şi f, privit ca polinom în Y peste $\mathbb{Q}[X]$, este primitiv pentru că $f = (2X^3+9)Y+(X^7+3X^2)$, descompunerea lui X^7+3X^2 în factori ireductibili în $\mathbb{Q}[X]$ este $X^7+3X^2 = x^2(X^5+3)$ (ireductibilitatea lui X^5+3 se poate justifica cu criteriul lui Eisenstein) şi nici unul dintre aceşti factori nu divide pe $2X^3+9$. Rezultă că f este ireductibil în $\mathbb{Q}[X,Y] = (\mathbb{Q}[X])[Y]$.

5.50. ii) Arătăm că polinomul omogen

$$f = a_0X^m + a_1X^{m-1}Y + \ldots + a_{m-1}XY^{m-1} + a_mY^m$$

este ireductibil în $K[X,Y]$ dacă şi numai dacă $a_0 \neq 0$ şi polinomul

$$g = a_0X^m + a_1X^{m-1} + \ldots + a_{m-1}X + a_m$$

este ireductibil în $K[X]$ (ceea ce, evident, va rezolva şi punctul i)). Să notăm că

$$a_0 = 0 \Leftrightarrow y \mid f.$$

Rămâne să analizăm cazul $a_0 \neq 0$. Cum a_0 este inversabil în K, rezultă că f, considerat ca polinom în X peste $K[Y]$, este primitiv. Deci f este ireductibil în $K[X,Y] = (K[Y])[X]$ dacă şi numai dacă f este ireductibil în $(K(Y))[X]$. Întrucât polinomul Y^m este inversabil în $(K(Y))[X]$ urmează că f este ireductibil în $(K(Y))[X]$ dacă şi numai dacă

$$f_1 = \frac{1}{Y^m} f = a_0 \left(\frac{X}{Y}\right)^m + a_1 \left(\frac{X}{Y}\right)^{m-1} + \ldots + a_{m-1}\left(\frac{X}{Y}\right) + a_m$$

este ireductibil în $(K(Y))[X]$. Din proprietatea de universalitate a inelului de polinoame în nedeterminata X cu coeficienţi în $K(Y)$ deducem existenţa unui (singur) endomorfism φ al inelului $(K(Y))[X]$ astfel încât

$$\varphi|_{K(Y)} = 1_{K(Y)} \text{ şi } \varphi(X) = \frac{X}{Y}.$$

Acest endomorfism este chiar automorfism (vezi problema **3.114**), prin urmare, polinomul f_1 este ireductibil în $(K(Y))[X]$ dacă şi numai dacă polinomul

$$g = a_0X^m + a_1X^{m-1} + \ldots + a_{m-1}X + a_m \in K[X] \subseteq (K(Y))[X]$$

este ireductibil în $(K(Y))[X]$, deci şi în $K[X]$ (vezi problema **5.7**).
iii) Fie $f = a_0X^m + a_1X^{m-1}Y + \ldots + a_{m-1}XY^{m-1} + a_mY^m \in K[X,Y]$ un polinom omogen. Dacă $a_0 = a_1 = \cdots = a_k = 0$, $k < m$, atunci f are k factori ireductibili egali cu Y (care este omogen de grad 1), iar $\frac{f}{Y^k}$ este un un polinom omogen cu primul termen nenul. Este, deci, suficient să analizăm cazul $a_0 \neq 0$. Dacă $g = a_0X^m + a_1X^{m-1} + \ldots + a_{m-1}X + a_m \in K[X]$ nu este ireductibil atunci

$$g = a_0 g_1 \cdots g_l, \tag{1}$$

unde $g_i \in K[X]$ ($i = \{1,\ldots,l\}$) este ireductibil de grad m_i cu $m = m_1 + \cdots + m_l$, iar coeficientul termenului de grad maxim din g_i este 1. Aplicând φ^{-1} egalităţii (1) obţinem $f = \varphi^{-1}(g) = a_0\varphi^{-1}(g_1)\cdots\varphi^{-1}(g_l)$, care este o descompunere a lui f în factori ireductibili în domeniul factorial $(K[Y])[X]$ (unica, pâna la o asociere în divizibilitate a factorilor).

5.51. Indicaţie. Se folosesc problemele **5.32**, **5.33** şi faptul că într-un domeniu cu ideale principale (p) este ideal prim dacă şi numai dacă p este un element prim.

5.52. Indicaţie. Inelul cât $4\mathbb{Z}/8\mathbb{Z}$ este simplu, dar nu are unitate.

5.53. Folosind problema **3.49** se deduce că dacă U este un ideal al unui inel Boole $(R,+,\cdot)$ atunci inelul cât R/U este, de asemenea, inel Boole. Un ideal U al lui R este prim dacă şi numai dacă inelul cât R/U nu conţine divizori ai lui zero, ceea ce, conform punctului iii) al problemei **3.18** are loc dacă şi numai dacă $|R/U| = 2$, adică inelul $(R/U,+,\cdot)$ este izomorf cu $(\mathbb{Z}_2,+,\cdot)$. Conform problemei **3.76**, pentru inelul Boole R/U aceasta echivalează cu faptul că R/U este simplu, adică U este ideal maximal în R.

5.54. Indicaţie. Aplicând prima teoremă de izomorfism omomorfismului de inele

$$E_0 : \mathbb{Z}[X] \to \mathbb{Z},\ E_0(a) = a,\ \forall a \in \mathbb{Z},\ E_0(X) = 0,$$

deducem că inelul cât $\mathbb{Z}/(X)$ este izomorf cu $\mathbb{Z}$, deci este un domeniu de integritate care nu este corp.

5.55. Indicaţie. Se poate proceda ca mai sus cu omomorfismul

$$E_0 : \mathbb{Q}[X] \to \mathbb{Q},\ E_0(a) = a,\ \forall a \in \mathbb{Q},\ E_0(X) = 0$$

sau se poate folosi faptul că un ideal al unui domeniu cu ideale principale este maximal dacă şi numai dacă este generat de un element ireductibil.

5.56. Indicaţie. Se foloseşte punctul b) al problemei **3.118**.

5.57. Indicaţie. Se aplică prima teoremă de izomorfism omomorfismelor de inele

$$E_{0,0} : \mathbb{C}[X,Y] \to \mathbb{C},\ E_{0,0}(a) = a,\ \forall a \in \mathbb{C},\ E_{0,0}(X) = 0,\ E_{0,0}(Y) = 0,$$
$$E_{2,3} : \mathbb{C}[X,Y] \to \mathbb{C},\ E_{2,3}(a) = a,\ \forall a \in \mathbb{C},\ E_{2,3}(X) = 2,\ E_{2,3}(Y) = 3.$$

5.58. Indicaţii. Cum polinoamele $Y-3$ şi X^2+1 sunt ireductibile în $\mathbb{Q}[X,Y]$, idealele principale pe care le generează sunt prime, dar idealele $(Y-3)$ şi $\left(X^2-1\right)$ sunt strict incluse în $\left(Y-3, X^2-1\right) \neq \mathbb{Q}[X,Y]$.

5.59. Indicaţie. Idealul $\left(X^2\right)$ al lui $\mathbb{Q}[X]$ nu este prim deoarece $X \cdot X \in \left(X^2\right)$, dar $X \notin \left(X^2\right)$.

5.60. Dacă M este un ideal maximal al lui R şi $x \notin M$ atunci $M + xR = R$, prin urmare $1 \in R$ se poate scrie sub forma $m + rx$ cu $m \in M$, $r \in R$, deci există $r \in R$ astfel încât $1 - rx \in M$. Reciproc, dacă N este un ideal a lui R care conţine strict pe M şi $x \in N \setminus M$ atunci există $r \in R$ astfel încât $1 - rx \in M \subseteq N$, ceea ce, împreună cu $rx \in N$, implică $1 \in N$, deci $N = R$. Aşadar, M este maximal.

5.61. Dacă $r, x \in R$ şi $rx = xr$ este inversabil atunci x este inversabil, prin urmare, $x \in R$ neinversabil implică rx neinversabil, oricare ar fi $r \in R$.
2) i)$\Rightarrow$ii) Fie M (singurul) ideal maximal al lui R. Dacă $x \in M$ atunci x este neinversabil, iar dacă $x \in R$ nu este inversabil atunci Rx este un ideal al lui R format numai din elemente neinversabile, deci propriu, şi astfel, $M = Rx \ni x$. Aşadar, $x \in M$ dacă şi numai dacă x este neinversabil, ceea ce înseamnă că elementele neinversabile din R formează chiar idealul M.
ii)$\Rightarrow$iii) este evidentă.
iii)$\Rightarrow$i) Fie N mulţimea elementelor inversabile din R. Din iii) şi din observaţia de la începutul acestei soluţii rezultă că N este un ideal al lui R, evident, propriu. Orice ideal propriu U al lui R este format din elemente neinversabile prin urmare este inclus în N. Aşadar, N este singurul ideal maximal al lui R.

5.62. Indicaţii. ii) Mulţimea elementelor neinversabile din inelul R_S este

$$N = \{ab^{-1} \mid a \in P,\ b \in R \setminus P\}$$

şi $x, y \in N$ implică $x + y \in N$.
iii) Se aplică prima parte a problemei inelului $\mathbb{Z}$ şi idealului său prim $2\mathbb{Z}$.

5.63. Indicaţie. Se foloseşte problema **3.95** pentru a arăta că suma a două serii formale neinversabile este o serie formală neinversabilă.

Capitolul 6

Spaţii vectoriale

6.1. Indicaţii. a) Pentru $\alpha = 0$ afirmaţia nu este adevărată. b) Pentru $u = 0$ afirmaţia nu este adevărată. Afirmaţiile c), d), e) sunt adevŭrate.

6.2. Indicaţie. Se verifică axiomele spaţiului vectorial. Funcţia $f : \mathbb{R} \to \mathbb{R}_+^*$, $f(x) = e^x$ realizează un izomorfism.

6.3. Indicaţii. i) În general, nu. De exemplu, când K este un corp de caracteristică ∞ nu are loc egalitatea $(\alpha + \beta)^{-1} = \alpha^{-1} + \beta^{-1}$, cu $\alpha \neq 0 \neq \beta$ şi $\alpha \neq -\beta$, prin urmare nu are loc egalitatea $(\alpha + \beta)(x, 1) = \alpha(x, 1) + \beta(x, 1)$. Totuşi, dacă $K = \mathbb{Z}_2$ atunci V este K-spaţiu vectorial. ii) Se verifică axiomele spaţiului vectorial. iii) Pentru $y \neq 0$ nu are loc egalitatea $1 \cdot (x, y) = (x, y)$.

6.4. Indicaţie. Se verifică axiomele spaţiului vectorial.

6.5. Indicaţie. iii) Corespondenţele stabilite la i) şi ii) între operaţiile externe pe V care introduc pe $(V, +)$ o structură de K-spaţiu vectorial şi omomorfismele injective de inele $\varphi : K \to End(V, +)$ sunt bijecţii, una inversa celeilalte.

6.6. Indicaţie. Dacă φ este omomorfismul injectiv de la ii) din problema anterioară atunci $\varphi(K)$ este subinelul căutat.

6.7. Indicaţie. Inelul $(End(\mathbb{Z}, +), +, \circ)$ este izomorf cu $(\mathbb{Z}, +, \cdot)$, iar acesta nu are nici un subinel care să fie corp.

6.8. Indicaţie. Inelul $(End(\mathbb{Q}, +), +, \circ)$ este izomorf cu $(\mathbb{Q}, +, \cdot)$ care este corp prim.

6.9. Indicaţie. Dacă V este un K-spaţiu vectorial (cu operaţia externă $*$), $n \in \mathbb{N}^*$ şi $0 \neq x \in V$ atunci $nx = n(1 * x) = (n \cdot 1) * x$, prin urmare $nx = 0$ dacă şi numai dacă $n \cdot 1 = 0$.

6.10. Fie V o mulţime finită şi K un corp infinit. Dacă V are un singur element, atunci există o singură structură de K-spaţiu vectorial pe V şi anume spaţiul vectorial nul. Dacă $|V| \geq 2$, presupunând că există o structură de K-spaţiu vectorial pe V şi luând $x \neq 0$, funcţia $t'_x : K \to V$, $t'_x(\alpha) = \alpha x$ este injectvă. Deducem că $|K| \leq |V|$, contradicţie cu V finită.

6.11. Indicaţie. Se procedează ca în soluţia problemei anterioare.

Observaţii: i) Din cele de mai sus rezultă că dacă V este un spaţiu vectorial nenul peste corpul K atunci $|K| \leq |V|$.
ii) Dacă V este un spaţiu vectorial real nenul atunci cardinalul mulţimii V este mai mare decât, sau egal cu, puterea continuului.

6.12. Indicaţie. Grupul lui Klein este izomorf cu $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$.

6.13. Răspuns. a) i) ${}_{\mathbb{Z}_2}\mathbb{Z}_2$; ii) ${}_{\mathbb{Z}_2}(\mathbb{Z}_2)^2$; iii) ${}_{\mathbb{Z}_2}(\mathbb{Z}_2)^n$; iv) ${}_{\mathbb{Z}_p}(\mathbb{Z}_p)^n$. b) Nu (se foloseşte problema **6.9**).

6.14. Indicaţie. Pentru a arăta că $P_n(K)$ este subspaţiu al lui $K[X]$ se foloseşte teorema de caracterizare a subspaţiului. Polinomul nul nu aparţine celorlalte două submulţimi ale lui $K[X]$.

6.15. Indicaţie. Avem $0 \notin C_V S$. În general, $C_V S \cup \{0\}$ nu este subspaţiu al lui V. De exemplu, $C_{\mathbb{R}[X]}(P_2(\mathbb{R})) \cup \{0\}$ nu este stabilă în raport cu adunarea polinoamelor (polinomul $-X^3 + (X^3 + 1) = 1$ are gradul mai mic decât 2).

6.16. Indicaţie. Luând succesiv în condiţia din enunţ $\alpha = 1$ şi $y = 0$ obţinem condiţiile din teorema de caracterizare a subspaţiului.

6.17. Din $x \in \langle S, y\rangle$ rezultă că există $s_1, \ldots, s_n \in S$ şi $\alpha_1, \ldots, \alpha_n, \alpha \in K$ astfel încât $x = \alpha_1 s_1 + \cdots + \alpha_n s_n + \alpha y$. Presupunerea $\alpha = 0$ ne-ar conduce la $x = \alpha_1 s_1 + \cdots + \alpha_n s_n \in S$, ceea ce contrazice ipoteza, prin urmare, $\alpha \neq 0$ este inversabil în K. Deducem $y = -\alpha^{-1}\alpha_1 s_1 - \cdots - \alpha^{-1}\alpha_n s_n + \alpha^{-1}x \in \langle S, x\rangle$.

6.18. Indicaţie. E destul să arătăm că $x \in \langle y, z\rangle$ şi $z \in \langle x, y\rangle$, ceea ce se obţine ca în problema anterioară din egalitatea dată şi faptul că $\alpha, \gamma \in K^*$.

6.19. Evident $S \subseteq P_n(K)$. Dacă $a_0^0 \in K^*$ este un polinom de grad 0 din S, din inversabilitatea lui a_0^0 în K şi faptul că S este un subspaţiu deducem că

$$1 = (a_0^0)^{-1} a_0^0 \in S,$$

prin urmare, pentru orice $\alpha \in K$ avem $\alpha = \alpha \cdot 1 \in S$. Dacă $a_1^1 X + a_0^1 \in S$ este un ponom de gradul 1 atunci $a_1^1 \neq 0$ este inversabil în K. Cum $a_0^1 \in S$ avem $a_1^1 X + a_0^1 - a_0^1 \in S$, de unde şi $X = (a_1^1)^{-1} a_1^1 X \in S$. De aici urmează $\alpha X \in S$ pentru orice $\alpha \in K$. Presupunând că am arătat că toate monoamele de grad 0,1,. . . ,$n - 1$ din $K[X]$ sunt şi în S şi considerând $a_n^n X^n + a_{n-1}^n X^{n-1} + \cdots + a_0^n \in S$ un polinom de grad n, avem $a_n^n \neq 0$ este inversabil în K,

$$a_n^n X^n = a_n^n X^n + a_{n-1}^n X^{n-1} + \cdots + a_0^n - a_0^n - \cdots - a_{n-1}^n X^{n-1} \in S,$$

aşadar $X^n = (a_n^n)^{-1} a_n^n X^n \in S$. Astfel, orice combinaţie liniară de $1, X, \ldots, X^n$ este în S adică orice polinom de grad cel mult n este în S. Deci $P_n(K) \subseteq S$.

6.20. Indicaţie. Nu. Scriind, de exemplu, polinomul 1 ca o combinaţie liniară de f_1, f_2, f_3 rezultă un sistem incompatibil de 4 ecuaţii liniare cu 3 necunoscute.
Altfel: Răspunsul se poate deduce şi din faptul că $\dim P_3(\mathbb{R}) = 4$.

6.21. Indicaţie. Se ştie că $V_1 + V_2 = \langle V_1 \cup V_2\rangle$ şi se poate folosi problema **2.73**.

6.22. Fie V_1, V_2, V_3 subspaţii ale unui K-spaţiu vectorial V. Arătăm că

$$V_1 \subseteq V_3 \Rightarrow V_1 + (V_2 \cap V_3) = (V_1 + V_2) \cap V_3.$$

Incluziunea $\subseteq$ are loc datorită proprietăţii de submodularitate (care are loc în orice latice). Fie $v_3 \in (V_1 + V_2) \cap V_3$. Atunci $v_3 \in V_3$ şi există $v_1 \in V_1(\subseteq V_3)$, $v_2 \in V_2$ astfel încât $v_3 = v_1 + v_2$. Deducem că $v_2 = v_3 - v_1 \in V_3$. Prin urmare, $v_2 \in V_2 \cap V_3$ şi astfel, $v_3 = v_1 + v_2 \in V_1 + (V_2 \cap V_3)$. Un exemplu care arată că laticea subspaţiilor unui spaţiu vectorial nu este, în general, distributivă este următorul: în $\mathbb{R}$-spaţiul vectorial $\mathbb{R}^2$ considerăm subspaţiile

$$V_1 = \{(x, 0) \mid x \in \mathbb{R}\},\ V_2 = \{(0, x) \mid x \in \mathbb{R}\},\ V_3 = \{(x, x) \mid x \in \mathbb{R}\}$$

şi avem $V_1 \cap V_3 = V_2 \cap V_3 = \{(0, 0)\}$, $V_1 + V_2 = \mathbb{R}^2$, deci

$$(V_1 + V_2) \cap V_3 = \mathbb{R}^2 \cap V_3 = V_3 \neq \{(0, 0)\} = (V_1 \cap V_3) + (V_2 \cap V_3).$$

Altă soluţie: Prima parte a acestei probleme rezultă şi din faptul că laticea subspaţiilor lui V este sublatice a laticei subgrupurilor (normale ale) lui $(V, +)$, care este modulară.

6.23. Indicaţie. $V = A_1 \oplus \cdots \oplus A_n$ dacă şi numai dacă f este bijectivă. Surjectivitatea sa rezultă din definiţia sumei de subspaţii, iar injectivitatea, din faptul că suma este directă.

6.24. Fie V_1, V_2, V_3, V_4 subspaţii ale unui K-spaţiu vectorial V cu proprietatea că $V = V_1 \oplus V_2$ şi $V_1 = V_3 \oplus V_4$. Rezultă că $V = V_1 + V_2 = V_3 + V_4 + V_2$. Mai mult, dacă $v_3 \in V_3 \cap (V_4 + V_2)$ atunci există $v_4 \in V_4$, $v_2 \in V_2$ astfel încât $v_3 = v_4 + v_2$. Urmează că $v_2 = v_3 - v_4 \in V_3 + V_4 = V_1$, prin urmare $v_2 \in V_1 \cap V_2 = \{0\}$. Obţinem $v_2 = 0$ şi $v_3 = v_4 \in V_3 \cap V_4 = \{0\}$. Aşadar, $V_3 \cap (V_4 + V_2) = \{0\}$ şi astfel, $V = V_3 \oplus (V_4 + V_2)$, ceea ce înseamnă că V_3 este sumand direct în V.

6.25. Indicaţie. În exemplul dat în soluţia problemei **6.22** pentru a infirma distributivitatea laticii subspaţiilor unui spaţiu vectorial, V_1 şi V_2 sunt complemenţi direcţi diferiţi ai lui V_3.

6.26. Indicaţii. Orice funcţie $f : \mathbb{R} \to \mathbb{R}$ se scrie $f = f_1 + f_2$, unde $f_1 : \mathbb{R} \to \mathbb{R}$, $f_1(x) = \dfrac{f(x) + f(-x)}{2}$ este o funcţie pară şi $f_2 : \mathbb{R} \to \mathbb{R}$, $f_2(x) = \dfrac{f(x) - f(-x)}{2}$ este o funcţie impară, iar singura funcţie din $\mathbb{R}^{\mathbb{R}}$ care este şi pară şi impară este funcţia nulă.

6.27. Indicaţie. Subspaţiile planului xOy sunt $\{O(0, 0)\}$, întregul plan şi dreptele care trec prin origine. Orice două puncte distincte care nu sunt pe o astfel de dreaptă formează un sistem de generatori pentru întregul plan.

6.28. Indicaţie. Subspaţiile spaţiului $Oxyz$ sunt $\{O(0, 0, 0)\}$, întregul spaţiu şi dreptele şi planele care trec prin origine. Orice trei puncte distincte care nu sunt într-un astfel de plan formează un sistem de generatori pentru întregul spaţiu.

6.29. Indicaţie. Luând succesiv în condiţia din enunţ $\alpha = 1$ şi $y = 0$ obţinem condiţiile din definiţia transformării liniare.

6.30. Indicaţie. $g(x_1) = f(x_1, 0)$, $h(x_2) = f(0, x_2)$.

6.31. Indicaţie. Fie $\alpha, \beta \in K$, $x, y \in V$. Avem $h(\alpha x + \beta y) = (f(\alpha x + \beta y), g(\alpha x + \beta y))$ şi $\alpha h(x) + \beta h(y) = (\alpha f(x) + \beta f(y), \alpha g(x) + \beta g(y))$.

6.32. Indicaţii. a) Dacă $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0), \ldots,$ $e_n = (0, \ldots, 0, 1)$ atunci $a_i = f(e_i)$ pentru orice $i \in \{1, \ldots, n\}$.
b) $f : \mathbb{R}^m \to \mathbb{R}^n$ este o transformare liniară de $\mathbb{R}$-spaţii vectoriale dacă şi numai dacă există $a_{ij} \in \mathbb{R}$ ($i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, n\}$) unic determinate, astfel încât

$$f(x_1, \ldots, x_m) = (a_{11}x_1 + \cdots + a_{m1}x_m, a_{12}x_1 + \cdots + a_{m2}x_m, \ldots, a_{1n}x_1 + \cdots + a_{mn}x_m),$$

pentru orice $(x_1, \ldots, x_m) \in \mathbb{R}^m$.

6.33. Indicaţii. Folosind problema anterioară putem stabili forma transformării liniare care verifică egalităţile $f(1,1) = (2,5)$ şi $f(1,0) = (1,4)$. Se obţine $f(2,3) = (5,14)$, iar folosind definiţia injectivităţii şi surjectivităţii se poate arăta că f este izomorfism.
Altfel: Vectorii $v_1 = (1,1)$ şi $e_1 = (1,0)$ formează o bază a lui $\mathbb{R}^2$. Folosind [34, Teorema 6.4.11], deducem că o transformare liniară $f : \mathbb{R}^2 \to \mathbb{R}^2$ este unic determinată de restricţia $f|_{\{v_1, e_1\}}$. Urmează că $f(2,3) = f(2v_1 + e_1) = (5,14)$, iar cum $f(v_1)$ şi $f(e_1)$ formează o bază a lui $\mathbb{R}^2$, rezultă că f este izomorfism.

6.34. Nu, pentru că $f(-2,0,-6) \neq (-2)f(1,0,3)$ deoarece $f(-2,0,-6) = (2,1)$ şi $(-2)f(1,0,3) = (-2)(1,1) = (-2,-2)$.

6.35. Indicaţie. Fie $V = S \oplus T$. Aplicând prima teoremă de izomorfism proiecţiei canonice $p_2 : V = S \oplus T \to T$, $p_2(s+t) = t$, obţinem $T \simeq V/S$.

6.36. Indicaţie. Se folosesc definiţia mulţimii libere şi a mulţimii legate, Observaţiile 6.4.2 şi Teorema 6.4.3 din [34].

6.37. Indicaţie. ii) Un exemplu pentru cazul în care incluziunea este strictă se poate obţine în $\mathbb{R}$-spaţiul vectorial $\mathbb{R}^2$ astfel luând $X = \{(1,0), (0,1)\}$ şi $Y = \{(2,0), (0,2)\}$. iii) Dacă ar exista un element nenul în $\langle X \rangle \cap \langle Y \rangle$ atunci ar exista $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m \in K$ nu toţi nuli, $x_1, \ldots, x_n \in X$ şi $y_1, \ldots, y_m \in Y$ astfel încât

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = \beta_1 y_1 + \cdots + \beta_m y_m.$$

Presupunând $\alpha_1 \neq 0$ rezultă $x_1 \in \langle X \cup Y \rangle$, contradicţie cu $X \cup Y$ liberă.

6.38. Indicaţie. Avem $K[X] = \langle \{X^k \mid k \in \mathbb{N}\} \rangle$, $V_1 = \langle \{X^{2k} \mid k \in \mathbb{N}\} \rangle$, $V_2 = \langle \{X^{2k+1} \mid k \in \mathbb{N}\} \rangle$ şi se aplică problema anterioară.

6.39. Indicaţie. i) Scriind polinomul nul ca o combinaţie liniară de f_1, f_2, f_3 rezultă un sistem omogen de 3 ecuaţii liniare cu 3 necunoscute care are doar soluţia nulă atunci şi numai atunci când determinantul său este nenul.

6.40. Indicaţii. Notăm $u_1 = v_2 + v_3$, $u_2 = v_3 + v_1$, $u_3 = v_1 + v_2$ şi atunci

$$v_1 = \frac{1}{2}(-u_1 + u_2 + u_3),\ v_2 = \frac{1}{2}(u_1 - u_2 + u_3),\ v_3 = \frac{1}{2}(u_1 + u_2 - u_3).$$

Proprietatea nu se păstrează în spaţii vectoriale peste corpuri de caracteristică 2. De exemplu, în $\mathbb{Z}_2$-spaţiul vectorial $(\mathbb{Z}_2)^3$, vectorii $v_1 = (\widehat{1}, \widehat{0}, \widehat{0})$, $v_2 = (\widehat{1}, \widehat{1}, \widehat{0})$, $v_3 = (\widehat{1}, \widehat{1}, \widehat{1})$ sunt liniar independenţi, dar $u_1 = (\widehat{0}, \widehat{0}, \widehat{1})$, $u_2 = (\widehat{0}, \widehat{1}, \widehat{1})$, $u_3 = (\widehat{0}, \widehat{1}, \widehat{0})$ nu sunt liniar independenţi.

6.41. L este liberă dacă şi numai dacă pentru orice $n_1, \dots, n_k \in \mathbb{N}$ distincţi, vectorii $f_{n_1}, \dots, f_{n_k}$ sunt liniar independenţi. Vom indica două metode pentru a deemonstra acest fapt:
I. Fie $\alpha_1, \dots, \alpha_k \in \mathbb{R}$ astfel încât $\alpha_1 f_{n_1} + \dots + \alpha_k f_{n_k} = \theta$ (unde cu θ am notat funcţia identic nulă). Rezultă că

$$\forall x \in \mathbb{R},\ \alpha_1 \sin^{n_1} x + \dots + \alpha_k \sin^{n_k} x = 0,$$

de unde deducem că polinomul

$$p = \alpha_1 X^{n_1} + \dots + \alpha_k X^{n_k} \in \mathbb{R}[X]$$

are ca ră dăcină orice număr $t(= \sin x) \in [-1, 1]$, adică are o infinitate de rădăcini. Aceasta implică $p = 0$, aşadar $\alpha_1 = \dots = \alpha_k = 0$.
II. Mulţimea formată din vectorii $f_{n_1}, \dots, f_{n_k}$ poate fi privită ca o submulţime a mulţimii $\{f_0, \dots, f_{\max\{n_1,\dots,n_k\}}\}$. Prin urmare, este suficient să arătăm că pentru orice $m \in \mathbb{N}$, vectorii $f_0, \dots, f_m$ sunt liniar independenţi. Dacă $\alpha_0, \dots, \alpha_m \in \mathbb{R}$ atunci $\alpha_0 f_0 + \alpha_1 f_1 + \dots + \alpha_m f_m = \theta$ dacă şi numai dacă pentru orice $x \in \mathbb{R}$ avem

$$\alpha_0 + \alpha_1 \sin x + \dots + \alpha_m \sin^m x = 0. \tag{1}$$

Considerăm $x_0, \dots, x_m \in \mathbb{R}$ astfel încât $\sin x_0, \dots, \sin x_m$ sunt distincte şi înlocuim în (1). Rezultă un sistem omogen de $m+1$ ecuaţii liniare cu necunoscutele $\alpha_0, \dots, \alpha_m$ al cărui determinant trebuie să fie nenul. Determinantul acestui sistem este un determinant de tip Vandermonde şi anume:

$$\begin{vmatrix} 1 & \sin x_0 & \sin^2 x_0 & \dots & \sin^m x_0 \\ 1 & \sin x_1 & \sin^2 x_1 & \dots & \sin^m x_1 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \sin x_m & \sin^2 x_m & \dots & \sin^m x_m \end{vmatrix} = \prod_{1 \le i < j \le m} (\sin x_j - \sin x_i) \neq 0.$$

6.42. Fie $\alpha_1, \dots, \alpha_n \in \mathbb{R}$ astfel încât

$$\alpha_1 f_1 + \dots + \alpha_n f_n = \theta. \tag{0}$$

Aceasta înseamnă că pentru orice $x \in \mathbb{R}$ avem

$$\alpha_1 \sin(\lambda_1 x) + \dots + \alpha_n \sin(\lambda_n x) = 0. \tag{1}$$

Derivăm de două ori în (1), înmulţim cu -1 şi obţinem

$$\alpha_1 \lambda_1^2 \sin(\lambda_1 x) + \dots + \alpha_n \lambda_n^2 \sin(\lambda_n x) = 0. \tag{2}$$

Repetăm procedeul pentru a obţinem încă $n-2$ egalităţi similare. Ultima este:

$$\alpha_1 \lambda_1^{2(n-1)} \sin(\lambda_1 x) + \dots + \alpha_n \lambda_n^{2(n-1)} \sin(\lambda_n x) = 0. \tag{n}$$

Fie $x_0 \in [0, 2\pi)$ astfel încât toate numerele $\sin(\lambda_1 x_0), \dots, \sin(\lambda_n x_0)$ să fie nenule (un astfel de număr ar putea fi şi precizat; oricum el există pentru că altfel, ştiind că funcţia sin are o mulţime numărabilă de zerouri $[0, 2\pi)$ ar fi o reuniune finită de mulţimi numărabile, deci ar fi numărabilă, cea ce este fals). Înlocuim în $(1), (2), \dots, (n)$ pe x cu

x_0 şi obţinem un sistem omogen de n ecuaţii cu necunoscutele $\alpha_1, \ldots, \alpha_n$ al cărui determinant este

$$d = \begin{vmatrix} \sin(\lambda_1 x_0) & \sin(\lambda_2 x_0) & \ldots & \sin(\lambda_n x_0) \\ \lambda_1^2 \sin(\lambda_1 x_0) & \lambda_2^2 \sin(\lambda_2 x_0) & \ldots & \lambda_n^2 \sin(\lambda_n x_0) \\ (\lambda_1^2)^2 \sin(\lambda_1 x_0) & (\lambda_2^2)^2 \sin(\lambda_2 x_0) & \ldots & (\lambda_2^2)^2 \sin(\lambda_n x_0) \\ \vdots & \vdots & & \vdots \\ (\lambda_1^2)^{n-1} \sin(\lambda_1 x_0) & (\lambda_2^2)^{n-1} \sin(\lambda_2 x_0) & \ldots & (\lambda_n^2)^{n-1} \sin(\lambda_n x_0) \end{vmatrix} =$$

$$= \prod_{i=1}^{n} \sin(\lambda_i x_0) \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \lambda_1^2 & \lambda_2^2 & \ldots & \lambda_n^2 \\ (\lambda_1^2)^2 & (\lambda_2^2)^2 & \ldots & (\lambda_2^2)^2 \\ \vdots & \vdots & & \vdots \\ (\lambda_1^2)^{n-1} & (\lambda_2^2)^{n-1} & \ldots & (\lambda_n^2)^{n-1} \end{vmatrix} = \prod_{i=1}^{n} \sin(\lambda_i x_0) \prod_{1 \le i < j \le m} (\lambda_j^2 - \lambda_i^2).$$

Conform alegerii lui x_0 şi condiţiilor din ipoteză, avem $d \neq 0$, prin urmare, $\alpha_1 = \cdots = \alpha_n = 0$.

6.43. Indicaţie. Scrierea unică a unui vector ca o combinaţie liniară de v_1 şi v_2 conduce la un sistem de 2 ecuaţii liniare cu 2 necunoscute care trebuie să aibă o soluţie unică.

6.44. Indicaţie. Scrierea lui $(0, 0, 0)$ ca o combinaţie liniară de cei trei vectori conduce la un sistem omogen de 3 ecuaţii liniare cu 3 necunoscute care are o infinitate de soluţii.

6.45. Indicaţie. Se procedează ca în problema **6.43**.

6.46. Indicaţie. Vezi problema **6.43**.

6.47. Indicaţie. Cum rangul unei matrice este egal cu numărul maxim de linii (coloane) care sunt liniar independente, pentru vectorii dintr-un K-spaţiu K^n dependenţa sau independenţa liniară poate fi studiată calculând rangul matricii care are aceşti vectori ca linii (coloane). Cum $\dim_{\mathbb{R}} \mathbb{R}^3 = 3$, în cazul nostru, rangul matricei formate cu cei trei vectori este 3 dacă şi numai dacă ei formează o bază a lui $\mathbb{R}^3$.

6.48. Indicaţie. Scrierea un vector $(x_1, \ldots, x_n) \in \mathbb{R}^n$ ca o combinaţie liniară de vectorii daţi ne conduce la un sistem de ecuaţii liniare care se rezolvă cu uşurinţă prin scăderea succesivă a câte două ecuaţii din sistem. Se obţin unicitatea acestei scrierei şi coordonatele cerute.

6.49. Răspuns. $A = -5E_1 - E_2 + 6E_3 - 2E_4$.

6.50. Răspuns. Există. Aceasta este $\{E_{ij} \mid i \in \{1, \ldots, m\}, j \in \{1, \ldots, n\}\}$, unde matricea E_{ij} are pe poziţia (i, j) pe 1 şi 0 în rest.

6.51. Indicaţie. $\dim M_n(K) = n^2$.

6.52. Răpuns. a) $\{1, X, \ldots, X^n, \ldots\}$; b) $f = f(a) + \frac{f'(a)}{1!}(X - a) + \frac{f''(a)}{2!}(X - a)^2 + \cdots + \frac{f^{(n)}}{n!}(X - a)^n$.

6.53. Indicaţie. a) Există. Aceasta este $\{1, i\}$. b) Funcţia $\mathbb{R}^2 \to \mathbb{C}$, $(a, b) \mapsto a + bi$ este un izomorfism de $\mathbb{R}$-spaţii vectoriale.

6.54. Indicaţie. V este un subspaţiul lui ${}_{\mathbb{Q}}\mathbb{R}$ generat de $\{1, \sqrt[3]{p}, \sqrt[3]{p^2}\}$. Arătăm că $1, \sqrt[3]{p}, \sqrt[3]{p^2}$ sunt liniar independente. Dacă $a, b, c \in \mathbb{Q}$ şi $a + b\sqrt[3]{p} + c\sqrt[3]{p^2} = 0$ atunci, prin înmulţire cu $\sqrt[3]{p}$ obţinem $a\sqrt[3]{p} + b\sqrt[3]{p^2} + cp = 0$. Eliminând pe $\sqrt[3]{p^2}$ între cele două egalităţi rezultă $(ab - c^2p) + (b^2 - ac)\sqrt[3]{p} = 0$, care, în baza faptului că $\sqrt[3]{p} \notin \mathbb{Q}$, conduce la $ab - c^2p = 0 = b^2 - ac$. Presupunând că $a \neq 0$ avem $c = \dfrac{b^2}{a}$, prin urmare $ab - \dfrac{b^4}{a^2}\sqrt[3]{p} = 0$, adică $\sqrt[3]{p} = \dfrac{b^3}{a^3}$. Aceasta implică $\sqrt[3]{p} = \dfrac{b}{a} \in \mathbb{Q}$, contradicţie cu $\sqrt[3]{p} \notin \mathbb{Q}$. Deci $a = 0$, ceea ce implică şi $b = c = 0$.

6.55. Indicaţie. iii) Fie $v \in V,\ v \neq 0$. Pentru orice $x \in X$ definim

$$f : X \to V,\ f_x(x') = \begin{cases} v, & \text{dacă } x' = x \\ 0, & \text{dacă } x' \neq x \end{cases}.$$

Submulţimea $\{f_x \mid x \in X\} \subseteq V^{(X)}$ este infinită şi liberă.

6.56. Indicaţie. Se foloseşte problema **6.37**.

6.57. Indicaţie. Dacă $(e_1, \ldots, e_n)$ este bază în ${}_KV$ şi $(\alpha_1, \ldots, \alpha_m)$ este bază în ${}_{K'}K$ atunci $(\alpha_i e_j \mid i \in \{1, \ldots, m\},\ j \in \{1, \ldots, n\})$ este bază în ${}_{K'}V$.

6.58. a) Notând $V = (\mathbb{Z}_2)^2$ avem $V = \{(\widehat{0}, \widehat{0}), (\widehat{0}, \widehat{1}), (\widehat{1}, \widehat{0}), (\widehat{1}, \widehat{1})\}$ şi $\dim V = 2$. O pereche ordonată $(v_1, v_2) \in V^2$ formează o bază dacă şi numai dacă v_1 şi v_2 sunt liniar independenţi. Întrucât orice vector $v_1 \in V \setminus \{(\widehat{0}, \widehat{0})\}$ face parte dintr-o bază, rezultă că v_1 poate fi ales în $2^2 - 1$ moduri. Dacă $v_2 \in V$ atunci v_1, v_2 sunt liniar independenţi dacă şi numai dacă $v_2 \in V \setminus \langle v_1 \rangle$, iar $|\langle v_1 \rangle| = 2$. Deci v_2 poate fi ales în $2^2 - 2$ moduri. Prin urmare, numărul bazelor ordonate ale lui V este $(2^2 - 1)(2^2 - 2) = 3 \cdot 2 = 6$. Urmând un raţionament analog cu cel de mai sus, se obţine: b) $(2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 7 \cdot 6 \cdot 4 = 168$; c) $(3^2 - 1)(3^2 - 3) = 8 \cdot 6 = 48$; d) $(3^3 - 1)(3^3 - 3)(3^3 - 3^2) = 26 \cdot 24 \cdot 18 = 11232$.

6.59. Această problemă este o generalizare a problemei anterioare. Cum $\dim V = n$ avem $V \simeq K^n$, prin urmare $|V| = q^n$. Fie B_n numărul bazelor ordonate $(v_1, \ldots, v_n)$ ale lui V. Orice vector $v_1 \in V \setminus \{0\}$ face parte dintr-o bază, rezultă că v_1 poate fi ales în $q^n - 1$ moduri. Dacă $v_2 \in V$ atunci v_1, v_2 sunt liniar independenţi dacă şi numai dacă $v_2 \in V \setminus \langle v_1 \rangle$, iar $|\langle v_1 \rangle| = q$. Deci v_2 poate fi ales în $q^n - q$ moduri. Dacă $v_3 \in V$ atunci v_1, v_2, v_3 sunt liniar independenţi dacă şi numai dacă $v_3 \in V \setminus \langle v_1, v_2 \rangle$, iar $|\langle v_1, v_2 \rangle| = q^2$. Deci v_2 poate fi ales în $q^n - q^2$ moduri. Continuând raţionamentul ajungem la concluzia că v_n poate fi ales în $q^n - q^{n-1}$ moduri. Deci numărul bazelor ordonate ale lui V este $B_n = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$.

6.60. Indicaţie. Dacă $A \in M_n(K)$ atunci $\det A \neq 0$ dacă şi numai dacă liniile matricei A formează o bază a lui K^n. Rezultă că ordinul lui $GL_n(K)$ coincide cu B_n (vezi problema anterioară).

6.61. Cum $\dim V = n$ avem $V \simeq K^n$, prin urmare $|V| = q^n$.
i) Singurul spaţiu al lui V de dimensiune 0, respectiv n este $\{0\}$, respectiv V. Deci $G_n^0(q) = 1 = G_n^n(q)$.
ii) Printr-un raţionament analog cu cel din problema **6.58** se deduce că numărul sistemelor ordonate $(v_1, \ldots, v_k) \in V^k$ formate din k vectori liniar independenţi este

$(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})$, iar numărul unor astfel de sisteme care generează acelaşi subspaţiu V' al lui V coincide cu numărul bazelor ordonate ale lui V', adică cu $(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})$ pentru că $\dim V'=k$. Prin urmare,

$$G_n^k(q)=\frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}. \tag{1}$$

iii) Din (1) rezultă că

$$G_n^k(q)=\frac{\prod\limits_{i=1}^{n}(q^i-1)}{\prod\limits_{i=1}^{k}(q^i-1)\prod\limits_{i=1}^{n-k}(q^i-1)}=G_n^{n-k}(q). \tag{2}$$

iv) Folosind pe (2) avem

$$q^kG_{n-1}^k(q)+G_{n-1}^{k-1}(q)=q^k\frac{\prod\limits_{i=1}^{n-1}(q^i-1)}{\prod\limits_{i=1}^{k}(q^i-1)\prod\limits_{i=1}^{n-k-1}(q^i-1)}+\frac{\prod\limits_{i=1}^{n-1}(q^i-1)}{\prod\limits_{i=1}^{k-1}(q^i-1)\prod\limits_{i=1}^{n-k}(q^i-1)}$$

$$=\prod_{i=1}^{n-1}(q^i-1)\frac{q^k(q^{n-k}-1)+(q^k-1)}{\prod\limits_{i=1}^{k}(q^i-1)\prod\limits_{i=1}^{n-k}(q^i-1)}=\frac{\prod\limits_{i=1}^{n}(q^i-1)}{\prod\limits_{i=1}^{k}(q^i-1)\prod\limits_{i=1}^{n-k}(q^i-1)}=G_n^k(q).$$

6.62. Indicaţie. $K=\mathbb{R}$, $V=\mathbb{R}[X]$, $S=\langle\{X^{2k+1}\mid k\in\mathbb{N}\}\rangle$.

6.63. Din $V_1\neq V_2$ şi $\dim V_1=\dim V_2$ rezultă $V_2\nsubseteq V_1$. Prin urmare

$$V_1\subsetneqq V_1+V_2\subseteq V,$$

ceea ce implică $\dim(V_1+V_2)=3$ şi

$$\dim(V_1\cap V_2)=\dim V_1+\dim V_2-\dim(V_1+V_2)=1.$$

În $\mathbb{R}^3$ aceasta se interpretează geometric prin faptul că intersecţia a două plane diferite care trec prin origine este o dreaptă care trece prin origine.

6.64. Din $V_2\nsubseteq V_1$ rezultă că $V_1\cap V_2\subsetneqq V_2$, prin urmare $\dim(V_1\cap V_2)<\dim V_2$, adică $\dim V_2-\dim(V_1\cap V_2)\geq 1$. Atunci

$$n=\dim V\geq\dim(V_1+V_2)=\dim V_1+\dim V_2-\dim(V_1\cap V_2)\geq n-1+1=n.$$

Aşadar, $\dim(V_1+V_2)=n=\dim V$, ceea ce implică $V=V_1+V_2$.

6.65. Arătăm că

$$(1) \qquad V_1 \nsubseteq V_2 \text{ şi } V_2 \nsubseteq V_1 \Rightarrow \dim(V_1+V_2) - \dim(V_1\cap V_2) \neq 1.$$

În ipoteza implicaţiei (1), egalitatea $\dim(V_1+V_2) - \dim(V_1 \cap V_2) = 0$ nu poate avea loc, prin urmare, trebuie verificat că $\dim(V_1+V_2) - \dim(V_1\cap V_2) \geq 2$. Ca în problemele anterioare avem

$$\begin{aligned} &V_1 \nsubseteq V_2 \Rightarrow V_1 \subsetneqq V_1+V_2 \Rightarrow \dim(V_1+V_2) - \dim V_1 \geq 1,\\ &V_2 \nsubseteq V_1 \Rightarrow V_1\cap V_2 \subsetneqq V_1 \Rightarrow \dim V_1 - \dim(V_1\cap V_2) \geq 1, \end{aligned}$$

aşadar,

$$\dim(V_1+V_2) - \dim(V_1\cap V_2) = \dim(V_1+V_2) - \dim V_1 + \dim V_1 - \dim(V_1\cap V_2) \geq 2.$$

6.66. Indicaţie. $\dim(V/(V_1\cap S_1)) = \dim V - \dim(V_1\cap S_1) = \dim V - \dim V_1 - \dim S_1 + \dim(V_1+S_1) \leq \dim V - \dim V_1 + \dim V - \dim S_1 = \dim V_2 + \dim S_2$.

6.67. Din $f(g(x)) = 0$ pentru orice $x \in V$ rezultă că $g(x) \in \operatorname{Ker} f$ pentru orice $x \in V$, prin urmare, $\operatorname{Ker} f \supseteq g(V)$. Deducem de aici că $\dim(\operatorname{Ker} f) \geq \dim g(V)$ şi astfel avem

$$(1) \qquad \dim V = \dim f(V) + \dim(\operatorname{Ker} f) \geq \dim f(V) + \dim g(V).$$

Din $f+g$ automorfism deducem $V = (f+g)(V) \subseteq f(V)+g(V) \subseteq V$. Atunci $V = f(V)+g(V)$ şi avem

$$(2) \quad \dim V = \dim f(V) + \dim g(V) - \dim(f(V)\cap g(V)) \leq \dim f(V) + \dim g(V).$$

Din (1) şi (2) rezultă egalitatea dorită.

Observaţie: Din cele de mai sus urmează imediat faptul că $\dim(f(V)\cap g(V)) = 0$, ceea ce înseamnă că $f(V)\cap g(V) = \{0\}$, deci $V = f(V) \oplus g(V)$. Aceasta indică o altă abordare a problemei bazată pe faptul că $\operatorname{Ker} f \supseteq g(V)$, $V = f(V)+g(V)$ şi $V = \operatorname{Ker} f \oplus f(V)$.

6.68. Indicaţii. V_1 este generat de vectorii

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

care sunt liniar independenţi, V_2 este generat de vectorii

$$\begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix}, \begin{pmatrix} 0 & 0\\ 0 & 1\end{pmatrix},$$

care sunt, de asemenea, liniar independenţi. Subspaţiul V_1+V_2 este generat de reuniunea generatorilor lui V_1 şi V_2, adică de

$$\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix} 0 & 1\\ 0 & 0\end{pmatrix}, \begin{pmatrix} 0 & 0\\ 1 & 0\end{pmatrix}, \begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix}, \begin{pmatrix} 0 & 0\\ 0 & 1\end{pmatrix},$$

iar dintre aceştia, vectorii

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

sunt liniar independenţi.

6.69. Indicaţie. Folosind indicaţia de la problema **6.47**, se obţine $\dim\langle c, d, e\rangle = 2$ şi c, d liniar independenţi. Folosind aceeaşi metodă obţinem că a, c, d sunt liniar dependenţi şi b, c, d sunt liniar dependenţi, prin urmare $\langle a, b\rangle \subseteq \langle c, d\rangle$, iar egalitatea dimensiunilor conduce la egalitatea cerută.

6.70. Indicaţie. Se foloseşte indicaţia de la problema **6.47** şi faptul că suma este generată de reuniunea generatorilor lui S şi T. De exemplu, la punctul d), $\dim S = \dim T = 3$ şi $\dim(S + T) = 4$. Un minor nenul de ordinul 4 poate fi ,,decupat" din coloanele corespunzătoare vectorilor u_1, u_2, u_3, v_2, deci ei formează o bază pentru $S + T$. Atunci $\dim(S \cap T) = 2$ şi $v \in S \cap T$ dacă şi numai dacă există $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \in \mathbb{R}$ astfel încât $v = \alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_3 = \beta_1 v_1 + \beta_2 v_2 + \beta_3 v_3$. Sistemul $(*)$ rezultat este compatibil nedeterminat, determinantul său are rangul 4, iar un minor principal se obţine chiar considerând coeficienţii necunoscutelor $\alpha_1, \alpha_2, \alpha_3, \beta_2$. Prin urmare, β_1 şi β_3 sunt necunoscutele secundare. Menţionăm că pentru a obţine 2 vectori liniar independenţi din $S \cap T$ nu este necesară rezolvarea sistemului $(*)$. Este suficient să dăm valori reale necunoscutelor secundare astfel încât vectorii rezultaţi să fie liniar independenţi şi să determinăm pe β_2 în aceste cazuri. Astfel, dacă $\beta_1 = 1$ şi $\beta_3 = 0$ atunci $\beta_2 = 0$ şi se obţine vectorul $v = v_1 \in S \cap T$, iar dacă $\beta_1 = 0$ şi $\beta_3 = 5$ atunci $\beta_2 = 1$ şi se obţine vectorul $v' = v_2 + 5v_3 \in S \cap T$. Cei doi vectori sunt liniar independenţi, deci formează o bază a lui $S \cap T$.

6.71. Indicaţie. Se foloseşte faptul că $\dim V_1 = \dim(\mathrm{Ker} f) + \dim(\mathrm{Im} f)$ şi faptul că f este injectivă dacă şi numai dacă $\mathrm{Ker} f = \{0\}$.

6.72. Indicaţie. $\varphi : K[X] \to K[X]$ definită prin $\varphi(f) = f(X^2)$, adică $\varphi = E_{X^2}$, este liniară, injectivă, dar nu este surjectivă. Pe de altă parte, funcţia liniară $\psi : K[X] \to K[X]$, definită pe baza $\{X^n \mid n \in \mathbb{N}\}$ prin $\psi(X^{2k}) = X^k$ şi $\psi(X^{2k+1}) = 0$ este surjectivă, dar nu este injectivă.

6.73. Răspuns. $\dim(\mathrm{Im}\varphi) = 2$, $\dim(\mathrm{Ker}\varphi) = 1$.

6.74. Indicaţie. Matricea lui f în baza canonică $[f]_e = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$ este inversabilă.

6.75. Indicaţie. $[f]_e = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $[g]_e = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ sunt inversabile. Se foloseşte teorema care dă legătura dintre operaţiile cu matrici şi operaţiile cu transformări liniare.

6.76. Cum rangul matricei formate cu vectorii din v este 2, iar rangul matricei formate cu vectorii din v' este 3, rezultă că v este bază în $\mathbb{R}^2$ şi v' este bază în $\mathbb{R}^3$. Coloanele matricei $[f]_{v,v'} = (a_{ij}) \in M_{3,2}(\mathbb{R})$ rezultă din egalităţile

$$\begin{gathered} (3, 0, 7) = f(1, 2) = a_{11}(1, -1, 0) + a_{21}(-1, 0, 1) + a_{31}(1, 1, 1), \\ (-1, -5, -4) = f(-2, 1) = a_{12}(1, -1, 0) + a_{22}(-1, 0, 1) + a_{32}(1, 1, 1). \end{gathered}$$

Cele două egalităţi conduc la sistemele

$$\begin{cases} a_{11} - a_{21} + a_{31} = 3 \\ -a_{11} \phantom{- a_{21}} + a_{31} = 0 \\ \phantom{a_{11} -} a_{21} + a_{31} = 7 \end{cases} \text{ şi } \begin{cases} a_{12} - a_{22} + a_{32} = -1 \\ -a_{12} \phantom{- a_{22}} + a_{32} = -5 \\ \phantom{a_{12} -} a_{22} + a_{32} = -4 \end{cases}$$

care au, respectiv, soluţiile $\left(\frac{10}{3}, \frac{11}{3}, \frac{10}{3}\right)$ şi $\left(\frac{5}{3}, -\frac{2}{3}, -\frac{10}{3}\right)$. prin urmare,

$$[f]_{v,v'} = \begin{pmatrix} \frac{10}{3} & \frac{5}{3} \\ \frac{11}{3} & -\frac{2}{3} \\ \frac{10}{3} & -\frac{10}{3} \end{pmatrix}.$$

Altă soluţie: Matricea de trecere de la baza canonică e' a lui $\mathbb{R}^3$ la baza v' este $T = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$, iar matricea lui f în perechea de baze v, e' este

$$[f]_{v,e'} = \begin{pmatrix} 3 & -1 \\ 0 & -5 \\ 7 & -4 \end{pmatrix},$$

(colanele sale fiind coordonatele lui $f(1,2)$ şi $f(-2,1)$ în baza e') prin urmare,

$$[f]_{v,v'} = T^{-1}[f]_{v,e'} = \begin{pmatrix} \frac{10}{3} & \frac{5}{3} \\ \frac{11}{3} & -\frac{2}{3} \\ \frac{10}{3} & -\frac{10}{3} \end{pmatrix}.$$

6.77. Indicaţie. ii) Matricea lui f în bazele canonice este matricea care are pe $f(e_1)$, $f(e_2)$ şi $f(e_3)$ ca şi coloane.
iii) $\operatorname{Im} f = \langle f(e_1), f(e_2), f(e_3)\rangle$, deci $\dim(\operatorname{Im} f)$ este rangul matricii de la ii).

6.78. Rangul matricelor formate din vectorii v_1, v_2, v_3, respectiv v_1', v_2', v_3' este 3, prin urmare sunt vectori independenţi într-un spaţiu de dimensiune 3, deci formează câte o bază. Dacă x_1, x_2, x_3 sunt coordonatele unui vector v în baza v_1, v_2, v_3 şi x_1', x_2', x_3' sunt coordonatele lui v în baza v_1', v_2', v_3' atunci

$$\begin{pmatrix} x_1' \\ x_2' \\ x_3' \end{pmatrix} = S \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \text{ şi } \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = S^{-1} \begin{pmatrix} x_1' \\ x_2' \\ x_3' \end{pmatrix}$$

unde S este matricea de trecere de la v la v'. Coloanele matricii $S = (a_{ij}) \in M_{3,3}(\mathbb{R})$ rezultă din egalităţile

$$\begin{aligned} (3,1,4) = v_1' &= a_{11}v_1 + a_{21}v_2 + a_{31}v_3 = a_{11}(1,2,1) + a_{21}(2,3,3) + a_{31}(3,7,1), \\ (5,2,1) = v_2' &= a_{12}v_1 + a_{22}v_2 + a_{32}v_3 = a_{12}(1,2,1) + a_{22}(2,3,3) + a_{32}(3,7,1), \\ (1,1,-6) = v_3' &= a_{13}v_1 + a_{23}v_2 + a_{33}v_3 = a_{13}(1,2,1) + a_{23}(2,3,3) + a_{33}(3,7,1). \end{aligned}$$

Cele trei egalităţi conduc la sistemele

$$\begin{cases} a_{11} + 2a_{21} + 3a_{31} = 3 \\ 2a_{11} + 3a_{21} + 7a_{31} = 1 \\ a_{11} + 3a_{21} + a_{31} = 4 \end{cases}, \quad \begin{cases} a_{12} + 2a_{22} + 3a_{32} = 5 \\ 2a_{12} + 3a_{22} + 7a_{32} = 2 \\ a_{12} + 3a_{22} + a_{32} = 1 \end{cases} \text{ şi } \begin{cases} a_{13} + 2a_{23} + 3a_{33} = 1 \\ 2a_{13} + 3a_{23} + 7a_{33} = 1 \\ a_{13} + 3a_{23} + a_{33} = -6 \end{cases}$$

care au, respectiv, soluţiile $(-33, 11, 5)$, $(-71, 20, 12)$ şi $(-41, 9, 8)$ prin urmare,

$$S = \begin{pmatrix} -33 & -71 & -41 \\ 11 & 20 & 9 \\ 5 & 12 & 8 \end{pmatrix}.$$

Altă soluţie. Avem

$$\begin{pmatrix} x_1' \\ x_2' \\ x_3' \end{pmatrix} = [1_{\mathbb{R}^3}]_{v,v'} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix},$$

iar matricea $S = [1_{\mathbb{R}^3}]_{v,v'}$ poate fi obţinută ca în problema **6.76**.

6.79. Indicaţii. $[f]_u = S^{-1}[f]_v S$, unde $S = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ este matricea de trecere de la baza v la baza u. Cum S^{-1} este matricea de trecere de la baza u la baza v, ea rezultă şi dacă, din cele patru egalităţi, se exprimă v_1, v_2, v_3, v_4 în funcţie de u_1, u_2, u_3, u_4.

6.80. Indicaţie. $[f]_v = S[f]_u S^{-1}$, unde S este matricea de trecere de la baza v la u.

6.81. Indicaţie. $[f]_b$ se determină cu uşurinţă, iar $[f]_{b'}$ rezultă ca în problemele anterioare.

6.82. Indicaţii. ii) $\dim(\mathrm{Im} f) = \mathrm{rang}[f]_{a,b}$; iii) $[f]_{a',b'} = T^{-1}[f]_{a,b}S$, unde S este matricea de trecere de la baza a la baza a' şi T este matricea de trecere de la baza b la baza b'.

6.83. Indicaţie. ii) Elementele din mulţimea cât $\mathbb{R}^2/S$ se reprezintă ca translatatele în plan ale dreptei S.

6.84. Indicaţie. Vezi problema anterioară.

6.85. Indicaţie. iii) Elementele din $\mathbb{R}^3/S$ se reprezintă ca translatatele în spaţiu ale dreptei S, Elementele din $\mathbb{R}^3/T$ se reprezintă ca translatatele în spaţiu ale planului T.

6.86. Indicaţie. Vezi problema anterioară.

6.87. Indicaţii. i) $\dim(\mathrm{Im}\, f) = \mathrm{rang}[f]_{v,v'} = 2$, $\dim(\mathrm{Ker}\, f) = \dim V - \dim(\mathrm{Im}\, f) = 3 - 2 = 1$, iar cum coloanele 2 şi 3 ale matricii $[f]_{v,v'}$ sunt proporţionale, avem

$$f(v_3) = -5f(v_1) \Leftrightarrow f(v_3 - 5v_1) = 0 \Leftrightarrow v_3 - 5v_1 \in \mathrm{Ker}\, f.$$

iii) Din teorema întâi de izomorfism, avem $f(V) \simeq V/\mathrm{Ker}\, f$. Izomorfismul este dat de corespondenţa $f(x) \mapsto x+\mathrm{Ker}\, f$ şi duce o bază a lui $f(V)$ înr-o bază a lui $V/\mathrm{Ker}\, f$. Avem $\dim(V'/\mathrm{Im}\, f = 3 - 2 = 1$. Un vector nenul din $V'/\mathrm{Im}\, f$ este de forma $v'+\mathrm{Im}\, f$ cu $v' \in V' \backslash \mathrm{Im}\, f$. Avem $f(v_1) = v_2' \in \mathrm{Im}\, f$ şi $f(v_2) = -v_1' + v_3'$. Dacă am avea $v_1' \in \mathrm{Im}\, f$ atunci ar rezulta că şi $v_3' \in \mathrm{Im}\, f$, prin urmare $V' = \langle v_1', v_2', v_3' \rangle \subseteq \mathrm{Im}\, f$, imposibil, deoarece $\dim(\mathrm{Im}\, f) = 2$.

6.88. Indicaţie. a) Pentru determinarea unei baze în $\operatorname{Ker} f$ se observă că $7(c_1 - c_3) = c_2 - c_4$, unde cu c_i am notat coloana i a matricei date.
b) Pentru determinarea lui $\operatorname{Ker} f$ şi a unei baze a sale se rezolvă sistemul

$$[f]_e \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

6.89. Indicaţie. Funcţia $f : K^n \to K$, $f(x_1, \cdots, x_n) = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ este liniară şi $S_0 = \operatorname{Ker} f$.

6.90. Indicaţie. Rezolvând sistemul obţinem

$$S_B = \left\{ \left(\frac{1}{3} + \frac{x_5}{3}, \frac{1}{3} + x_3 + x_4 + \frac{5x_5}{3}, x_3, x_4, x_5 \right) \mid x_3, x_4, x_5 \in \mathbb{R} \right\},$$

adică $S_B = \left(\frac{1}{3}, \frac{1}{3}, 0, 0, 0 \right) + S_0$, unde

$$S_0 = \left\{ \left(\frac{x_5}{3}, x_3 + x_4 + \frac{5x_5}{3}, x_3, x_4, x_5 \right) \mid x_3, x_4, x_5 \in \mathbb{R} \right\}.$$

Înlocuind în S_0 succesiv $x_3 = 1$, $x_4 = x_5 = 0$; $x_4 = 1$, $x_3 = x_5 = 0$; $x_5 = 3$, $x_3 = x_4 = 0$ primim sistemul fundamental de soluţii $(0, 1, 1, 0, 0)$, $(0, 1, 0, 1, 0)$, $(1, 5, 0, 0, 3)$.

6.91. Indicaţie. Se rezolvă sistemele şi se particularizează convenabil necunoscutele secundare (vezi soluţia problemei anterioare).

6.92. Din $\dim_{\mathbb{Z}_p} V = 1$ rezultă că $V \simeq Z_p$, deci $|V| = p$. Cum orice transformare liniară este determinată în mod unic de restricţia sa la o bază a domeniului, fixăm o bază, adică un element nenul v din V şi $|End_{\mathbb{Z}_p}(V)|$ este egal cu numărul funcţiilor de la $\{v\}$ la V, adică $|V|^1 = |V| = p$.

6.93. Indicaţii. a) Din f aditivă rezultă $f(mx) = mf(x)$ pentru orice $m \in \mathbb{Z}$ şi $x \in V$. Dacă $n \in \mathbb{N}^*$ şi $x \in V$ atunci $f(x) = f\left(n\left(\frac{1}{n}x\right)\right) = nf\left(\frac{1}{n}x\right)$, prin urmare $f\left(\frac{1}{n}x\right) = \frac{1}{n}f(x)$.
b) $\mathbb{R}$ poate fi privit atât $\mathbb{Q}$-spaţiu vectorial cât şi $\mathbb{R}$-spaţiu vectorial. $\mathbb{R}$ privit ca un $\mathbb{Q}$-spaţiu vectorial are o bază infinită B. Fie $x, y \in B$, $x \neq y$. Cum x, y unt liniar independenţi peste $\mathbb{Q}$ avem $\alpha = \frac{x}{y} \in \mathbb{R} \setminus \mathbb{Q}$. Funcţia

$$\varphi : B \to \mathbb{R},\ \varphi(z) = \begin{cases} y & , \text{dacă } z = x, \\ x & , \text{dacă } z = y, \\ z & , \text{dacă } z \in B \setminus \{x, y\}, \end{cases}$$

se extinde în mod unic la o transformare $\mathbb{Q}$-liniară $f : \mathbb{R} \to \mathbb{R}$. Avem $f(\alpha x) = f(y) = x$, $\alpha f(x) = \alpha y = \frac{y^2}{x}$. Dar $x^2 \neq y^2$ pentru că $x^2 = y^2$ ar implica $\alpha \in \mathbb{Q}$. Deci $f(\alpha x) \neq \alpha f(x)$, adică f nu este $\mathbb{R}$-liniară.

6.94. a)⇒b) Fie Y o bază a lui V_2. Din surjectivitatea lui f rezultă că pentru orice $y \in Y$ mulţimea $S_y = \{x \in V_1 \mid f(x) = y\}$ este nevidă. Folosind axioma alegerii, alegem câte un $x_y \in S_y$ pentru orice $y \in Y$ şi definim $s_0 : Y \to V_1$, $s_0(y) = x_y$. Întrucât Y este o bază a lui V_2, urmează că s_0 se poate prelungi în mod unic la o aplicaţie liniară $s : V_2 \to V_1$. Pentru orice $y \in V_2$ avem $(f \circ s)(y) = f(s(y)) = f(x_y) = y = 1_{V_2}(y)$, ceea ce implică $f \circ s = 1_{V_2}$.
Implicaţia b)⇒c) este evidentă.
Implicaţia c)⇒a) este echivalentă cu faptul că negaţia lui a) implică negaţia lui c). Din negaţia lui a) rezultă că $V_2 \backslash \mathrm{Im}\, f \neq \emptyset$, ceea ce arată că există $y_0 \in V_2$ astfel încât în spaţiul vectorial cât $V_2/\mathrm{Im}\, f$ avem $y_0 + \mathrm{Im}\, f \neq \mathrm{Im}\, f$. Luând $V = V_2/\mathrm{Im}\, f$, $\alpha(y) = \mathrm{Im}\, f$, $\beta(y) = y + \mathrm{Im}\, f$, obţinem funcţiile liniare diferite α şi β, dar

$$(\alpha \circ f)(x) = \alpha(f(x)) = \mathrm{Im}\, f = \beta(f(x)) = (\beta \circ f)(x),\ \forall x \in V_1,$$

ceea ce ne arată că $\alpha \circ f = \beta \circ f$.

Observaţii: i) În cazul grupurilor şi inelelor se menţine echivalenţa dintre a) şi c), dar demonstaţia este mai complicată (vezi [33]). Pentru grupuri abeliene demonstraţia este simplă. Chiar în caz abelian b) nu mai este echivalentă cu a). De exemplu, aplicaţia canonică $p : \mathbb{Z} \to \mathbb{Z}_n$, $p(i) = \widehat{i}$ este omomorfism surjectiv al lui $(\mathbb{Z}, +)$ pe $(\mathbb{Z}_n, +)$, dar nici o secţiune a lui p nu este omomorfism pentru că $Hom(\mathbb{Z}_n, \mathbb{Z})$ este format doar din omomorfismul nul (vezi **2.109**). În cazul inelelor asociative, nici a) şi c) nu mai sunt echivalente. De exemplu, omorfismul nesurjectiv $i : \mathbb{Z} \to \mathbb{Q}$ verifică pe c).
ii) Condiţia b) arată că orice spaţiu vectorial este modul proiectiv (vezi [30]).

6.95. Indicaţii. a) Folosind notaţiile din problema anterioară, o transformare liniară h care satisface condiţiile cerute este $h = s \circ g$.
b) Orice $(a, b) \in \mathbb{R}^2$ poate fi scris $(2 \cdot 0 - (-a), b) = f(0, -a, b)$, ceea ce demonstrează surjectivitatea lui f şi indică faptul că transformarea h poate fi definită prin $h(x, y) = (0, -x, y)$. Acelaşi lucru se obţine procedând ca la punctul anterior: fie $\{e_1 = (1, 0), e_2 = (0, 1)\}$ baza canonică a lui $\mathbb{R}^2$ şi $\overline{e_1} = (0, -1, 0), \overline{e_2} = (0, 0, 1)$; atunci $f(\overline{e_1}) = (1, 0) = e_1$, $f(\overline{e_2}) = (0, 1) = e_2$ şi

$$h(x, y) = xh(e_1) + yh(e_2) = x\overline{e_1} + y\overline{e_2} = x(0, -1, 0) + y(0, 0, 1) = (0, -x, y).$$

6.96. a)⇒b) Fie X o bază a lui V_1. Din injectivitatea lui f se deduce că $f(X)$ este liberă în V_2, deci se poate completa la o bază Y a lui V_2. Restricţia lui f la X defineşte o bijecţie de la X la $f(X)$. Fie $r_0 : f(X) \to X$ inversa acestei bijecţii, adică $r_0(f(x)) = x$, iar $\overline{r_0} : Y \to V_1$ o prelungire a lui r_0. Întrucât Y este o bază a lui V_2 urmează că $\overline{r_0}$ se poate prelungi în mod unic la o aplicaţie liniară $r : V_2 \to V_1$. Pentru orice $x \in X$ avem $(r \circ f)(x) = r(f(x)) = x = 1_{V_1}(x)$, ceea ce implică $r \circ f = 1_{V_1}$.
Implicaţia b)⇒c) este evidentă.
Implicaţia c)⇒a) este echivalentă cu faptul că negaţia lui a) implică negaţia lui c). Din negaţia lui a) rezultă că $\mathrm{Ker}\, f \neq \{0\}$. Luând $V = \mathrm{Ker}\, f$, $\alpha(x) = x$, $\beta(x) = 0$ pentru orice $x \in V$, obţinem funcţiile liniare diferite α, β, dar

$$(f \circ \alpha)(x) = f(\alpha(x)) = f(x) = 0 = f(\beta(x)) = (f \circ \beta)(x),\ \forall x \in V,$$

ceea ce arată că $f \circ \alpha = f \circ \beta$.

Observaţii: i) În cazul grupurilor şi inelelor se menţine echivalenţa dintre a) şi c), dar b) nu mai este echivalentă cu a). De exemplu, $i : \mathbb{Z} \to \mathbb{Q}$ este omomorfism injectiv între $(\mathbb{Z}, +)$ şi $(\mathbb{Q}, +)$, dar nici o retractă a lui f nu este omomorfism pentru că $Hom(\mathbb{Q}, \mathbb{Z})$ este format doar din omomorfismul nul (vezi **2.109**).
ii) Condiţia b) arată că orice spaţiu vectorial este modul injectiv (vezi [30]).

6.97. Indicaţii. a) Folosind notaţiile din problema anterioară, o transformare liniară h care satisface condiţiile cerute este $h = g \circ r$.
b) Fie $\{e_1, e_2\}$ baza canonică a lui $\mathbb{R}^2$ şi $\{e'_1, e'_2, e'_3\}$ baza canonică a lui $\mathbb{R}^3$. Avem $f(e_1) = f(1, 0) = (1, 1, 2)$, $f(e_2) = f(0, 1) = (-1, 1, 0)$, iar vectorii $f(e_1)$, $f(e_2)$ şi $e'_3 = (1, 0, 0)$ sunt liniar independenţi, deci formează o bază în $\mathbb{R}^3$. Procedând ca mai sus, considerăm $h(f(e_1)) = e_1$, $h(f(e_2)) = e_2$ şi $h(e'_3) = (0, 0)$. Prin urmare,

$$e_1 = h(1,1,2) = h(e'_1 + e'_2 + 2e'_3) = h(e'_1) + h(e'_2) + 2h(e'_3) = h(e'_1) + h(e'_2),$$
$$e_2 = h(-1,1,0) = h(-e'_1 + e'_2) = -h(e'_1) + h(e'_2).$$

Deducem că $h(e'_1) = \dfrac{1}{2}(e_1 - e_2) = \left(\dfrac{1}{2}, 0, 0\right)$, $h(e'_2) = \dfrac{1}{2}(e_1 + e_2) = \left(0, \dfrac{1}{2}, 0\right)$ şi, astfel,

$$h(x,y,z) = xh(e'_1) + yh(e'_2) + zh(e'_3) = \left(\frac{x}{2}, 0, 0\right) + \left(0, \frac{y}{2}, 0\right) = \left(\frac{x}{2}, \frac{y}{2}, 0\right).$$

6.98. Indicaţie. Se folosesc problemele **6.71**, **6.96** şi **6.94**.

6.99. Indicaţie. Scriind vectorii din K^n sub formă de matrice coloană, aplicaţia $f_A : K^n \to K^n$, $f_A(x) = Ax$ este liniară şi matricea lui f_A în baza canonică a lui K^n este A. Corespondenţa $f_A \mapsto A$ realizează un izomorfism atât între K-spaţiile $End_K(K^n)$ şi $M_n(K)$ cât şi între inelele $End_K(K^n)$ şi $M_n(K)$.

Observaţie: În cazul $K = \mathbb{C}$ echivalenţele ii) $\Leftrightarrow$ iii) $\Leftrightarrow$ iv) sunt conţinute în problema **3.55**.

6.100. Indicaţie. Scriind vectorii din K^m şi K^n sub formă de matrice coloane, aplicaţia $f_A : K^n \to K^m$, $f_A(x) = Ax$ este liniară şi matricea lui f_A în perechea formată din bazele canonice ale lui K^n şi K^m este A. Avem

$$\operatorname{rang} A = n \Leftrightarrow \dim(\operatorname{Im} f_A) = n \Leftrightarrow \dim(\operatorname{Ker} f_A) = 0 \Leftrightarrow \operatorname{Ker} f_A = \{0\} \Leftrightarrow f_A \text{ injectivă},$$
$$\operatorname{rang} A = m \Leftrightarrow \dim(\operatorname{Im} f_A) = m = \dim K^m \Leftrightarrow f_A \text{ surjectivă}.$$

6.101. Indicaţii. i) În cazul $\dim V = \infty$ cerinţa se deduce din problema **6.55** pentru că $Hom_K(V, V') \simeq V'^X$, unde X este o bază a lui V. Dacă $\dim V < \infty$, X este o bază a lui V şi $x_0 \in X$ atunci $\{f : X' \to V' \mid \operatorname{supp} f = \{x_0\}\}$ este un subspaţiu al lui V'^X izomorf cu V'. ii) $Hom_K(V, V') \simeq M_{m,n}(K)$.

6.102. Indicaţie. Fie $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, $\ldots$, $e_n = (0, \ldots, 0, 1)$. Ca în problema **6.32** se obţine $a_i = f(e_i)$ $(i \in \{1, \ldots, n\})$. Mai mult, $a_1, \ldots, a_n$ sunt coordonatele lui f în duala bazei $(e_1, \ldots, e_n)$. De asemenea, avem

$$e'_1 = e_1,\ e'_2 = e_1 + e_2,\ \ldots,\ e'_n = e_1 + \cdots + e_n,$$

de unde rezultă că

$$a'_1 = f(e'_1) = a_1,\ a'_2 = f(e'_2) = a_1 + a_2,\ \ldots,\ a'_n = f(e'_n) = a_1 + \cdots + a_n$$

sunt coordonatele lui f în duala bazei $(e'_1, \ldots, e'_n)$.

6.103. Indicaţie. iii) Se foloseşte punctul ii) şi problemele **6.96**, **6.94**.

6.104. Indicaţie. Se foloseşte definiţia formei n-liniare.

6.105. Indicaţie. ii) Dacă (e_1, e_2) este baza canonică a lui K^2 atunci $a_{ij} = f(e_i, e_j)$ $(i, j = 1, 2)$.

6.106. Trebuie arătat că

$$v_i = v_{i+k},\ k \in \mathbb{N}^*,\ i + k \leq n \Rightarrow f(v_1, \dots, v_n) = 0.$$

Pentru simplificarea scrierii considerăm $i = 1$. Demonstrăm această implicaţie prin inducţie după k. Proprietatea este adevărată pentru $k = 1$. O presupunem adevărată pentru $k = l - 1$ cu $1 < l < n$ şi considerăm $v_1 = v_{l+1}$. Din ipoteza inducţiei şi din multiliniaritate deducem

$$\begin{aligned}0 =& f(v_1, \dots, v_1 + v_l, v_1 + v_l, \dots, v_n) = f(v_1, \dots, v_1, v_1 + v_l, \dots, v_n) + \\ &+ f(v_1, \dots, v_l, v_1 + v_l, \dots, v_n) = f(v_1, \dots, v_1, v_1, \dots, v_n) + \\ &+ f(v_1, \dots, v_1, v_l, \dots, v_n) + f(v_1, \dots, v_l, v_1, \dots, v_n) + f(v_1, \dots, v_l, v_l, \dots, v_n) = \\ &= f(v_1, \dots, v_l, v_1, \dots, v_n) = f(v_1, \dots, v_l, v_{l+1}, \dots, v_n),\end{aligned}$$

ceea ce arată că proprietatea este adevărată pentru $k = l$.

6.107. Indicaţie. 1) i)$\Rightarrow$ii) $f(v_1, \dots, v_i, \dots, v_j, \dots, v_n) + f(v_1, \dots, v_j, \dots, v_i, \dots, v_n) = f(v_1, \dots, v_i + v_j, \dots, v_i + v_j, \dots, v_n) = 0$.
ii)$\Rightarrow$i) Dacă $v_i = v_{i+1}$ atunci $f(v_1, \dots, v_i, v_{i+1}, \dots, v_n) = f(v_1, \dots, v_{i+1}, v_i, \dots, v_n)$, iar f fiind antisimetrică $f(v_1, \dots, v_i, v_{i+1}, \dots, v_n) = -f(v_1, \dots, v_{i+1}, v_i, \dots, v_n)$, ceea ce implică $2f(v_1, \dots, v_i, v_{i+1}, \dots, v_n) = 0$.
2) Funcţia $f : K \times K \to K$, $f(x, y) = xy$ este biliniară şi antisimetrică pentru că

$$f(x, y) = xy = -xy = -yx = -f(y, x),$$

dar nu este alternă pentru că $f(1, 1) = 1 \cdot 1 = 1 \neq 0$.

6.108. Indicaţie. Analizăm cazul $n = 2$ (cazul general se tratează în mod analog).
i) Fie $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ şi A_1, A_2 coloanele matricei A. Avem $A_1 = a_{11}e_1 + a_{21}e_2$ şi $A_2 = a_{12}e_1 + a_{22}e_2$, unde $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Scriind pe $A = (A_1, A_2)$ şi folosind condiţiile impuse lui f avem:

$$\begin{aligned}f(A) &= f(a_{11}e_1 + a_{21}e_2, a_{12}e_1 + a_{22}e_2) \\ &= a_{11}a_{12}f(e_1, e_1) + a_{11}a_{22}f(e_1, e_2) + a_{21}a_{12}f(e_2, e_1) + a_{21}a_{22}f(e_2, e_2) \\ &= a_{11}a_{22}f(e_1, e_2) - a_{12}a_{21}f(e_1, e_2) = (a_{11}a_{22} - a_{12}a_{21})f(I_2) \\ &= a_{11}a_{22} - a_{12}a_{21} = \det A\end{aligned}$$

ii) Repetând raţionamentul de mai sus în cazul $f(I_2) = a$ primim $f(A) = a \det A$.

6.109. Funcţia $g : (K^m)^m \to K$, $g(A) = \begin{vmatrix} A & B \\ O & C \end{vmatrix}$ este o formă m-liniară de coloanele lui A, de unde rezultă că $g(A) = \begin{vmatrix} I_m & B \\ O & C \end{vmatrix} \cdot |A|$. Raţionând analog asupra liniilor lui C se deduce $\begin{vmatrix} I_m & B \\ O & C \end{vmatrix} = \begin{vmatrix} I_m & B \\ O & I_n \end{vmatrix} \cdot |C|$. Matricea $\begin{pmatrix} I_m & B \\ O & I_n \end{pmatrix}$ este o matrice de formă triunghiulară din $M_{m+n}(K)$ cu 1 pe diagonala principală, prin urmare $\begin{vmatrix} I_m & B \\ O & I_n \end{vmatrix} = 1$. Aşadar, $g(A) = |C| \cdot |A| = |A| \cdot |C|$.

6.110. Indicaţii. i) Se verifică implicaţiile

$$[f, g \in \mathcal{B}(V) \Rightarrow f + g \in \mathcal{B}(V)] \text{ şi } [\alpha \in K,\ g \in \mathcal{B}(V) \Rightarrow \alpha f \in \mathcal{B}(V)]$$

unde $(f+g)(x,y) = f(x,y) + g(x,y)$ şi $(\alpha f)(x,y) = \alpha f(x,y)$, de unde se deduce că $\mathcal{B}(V)$ este subspaţiu al lui $K^{V\times V}$.
ii) Avem

$$\begin{aligned} f(x,y) =& f(x_1v_1 + \cdots + x_nv_n, y) = \sum_{i=1}^{n} x_i f(v_i, y) = \sum_{i=1}^{n} x_i f(v_i, y_1v_1 + \cdots + y_nv_n) \\ =& \sum_{i=1}^{n} x_i \sum_{j=1}^{n} y_j f(v_i, v_j) = \sum_{i=1}^{n} x_i \sum_{j=1}^{n} a_{ij} y_j = {}^tX \cdot A \cdot Y. \end{aligned}$$

iii) Se foloseşte ii).
iv) Din iii) rezultă că $\dim \mathcal{B}(V) = \dim M_n(K) = n^2$.
v) Notând X', respectiv Y', matricea coloană formată din coordonatele lui x, respectiv y, în baza w şi folosind formulele de schimbare a coordonatelor, avem $X = SX'$ şi $Y = SY'$. Acum din ii) rezultă $f(x,y) = {}^t(SX')A(SY') = {}^tX'({}^tSAS)Y'$, ceea ce implică $B = {}^tSAS$.

6.111. Indicaţie. Vezi problema **6.110**.

6.112. Indicaţie. Se aplică problema **6.110**, punctul ii).

6.113. Indicaţie. Vezi problema **6.110**.

6.114. Amintim că o *matrice* $A = (a_{ij}) \in M_n(K)$ este *simetrică*, respectiv *antisimetrică*, dacă $A = {}^tA$, respectiv $-A = {}^tA$, adică $a_{ij} = a_{j\,i}$, respectiv $a_{ij} = -a_{j\,i}$, pentru orice $i, j \in \{1, \ldots, n\}$.
i)⇒ii) Dacă $A = (a_{ij}) \in M_n(K)$ este matricea lui f în baza v şi f este simetrică, respectiv antisimetrică, atunci avem $a_{ij} = f(v_i, v_j) = f(v_j, v_i) = a_{j\,i}$, respectiv $a_{ij} = f(v_i, v_j) = -f(v_j, v_i) = -a_{j\,i}$, ceea ce ne arată că A este simetrică, respectiv antisimetrică.
Implicaţia ii)⇒iii) este evidentă.
iii)⇒i) Dacă matricea $A = (a_{ij})$ a lui f în baza v este simetrică, respectiv antisimetrică, şi $x = x_1v_1 + \cdots + x_nv_n,\ y = y_1v_1 + \cdots + y_nv_n$ atunci din biliniaritatea lui f avem $f(x,y) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_iy_j$, deci $f(y,x) = \sum_{j=1}^{n}\sum_{i=1}^{n} a_{ji}y_jx_i = f(x,y)$, respectiv $f(y,x) = -\sum_{j=1}^{n}\sum_{i=1}^{n} a_{ji}y_jx_i = -f(x,y)$.

6.115. Indicaţie. i) $f_s = \frac{1}{2}(f+g)$, $f_a = \frac{1}{2}(f-g)$, unde $g(x,y) = f(y,x)$.
ii) $A_s = \frac{1}{2}(A + {}^tA)$, $A_a = \frac{1}{2}(A - {}^tA)$.

6.116. Indicaţie. i) Dacă q este o formă pătratică atunci există o formă biliniară simetrică $f' : V \times V \to K$ astfel încât $q(x) = f'(x,x)$ pentru orice $x \in V$. Acum din (1) rezultă $f(x,y) = \frac{1}{2}[f'(x+y,x+y) - f'(x,x) - f'(y,y)]$, ceea ce implică $f = f'$. Deci funcţia f definită în (1) este singura formă biliniară simetrică pentru care $q(x) = f(x,x)$ pentru orice $x \in V$.
ii) Din (1) urmează implicaţia

$$q(x) = 0,\ \forall x \in V \Rightarrow f(x,y) = 0,\ \forall x,y \in V.$$

Observaţie: Din problema de mai sus rezultă că dacă corpul K are caracteristica diferită de 2 atunci există o bijecţie între mulţimea formelor pătratice definite pe V şi mulţimea formelor biliniare simetrice definite pe V.

6.117. Răspuns. Notând $x_1 = x$, $x_2 = y$, $x_3 = z$ şi $A_k = (a_{ij})$ matricea lui q_k ($k \in \{1,2,3,4,5\}$) avem: a_{ii} este coeficientul lui x_i^2 şi $a_{ij} = a_{ji} = \frac{1}{2}a$, unde a este coeficientul lui x_ix_j. Deci avem: 1) $A_1 = \begin{pmatrix} 2 & \frac{3}{2} \\ \frac{3}{2} & 6 \end{pmatrix}$, 2) $A_2 = \begin{pmatrix} 0 & 4 \\ 4 & 4 \end{pmatrix}$, 3) $A_3 = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 3 & \frac{1}{2} \\ 2 & \frac{1}{2} & 7 \end{pmatrix}$,
4) $A_4 = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$, 5) $A_5 = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 4 & 1 \\ 1 & 1 & 1 \end{pmatrix}$.

6.118. i) Întrucât matricele diagonale sunt simetrice, din problema **6.114** urmează că f este simetrică.
ii) Demonstrăm afirmaţia din enunţ prin inducţie după n. Pentru $n = 1$, orice formă biliniară $f : V \times V \to K$ este diagonalizabilă. Presupunem că $n \geq 1$ şi afirmaţia adevărată pentru spaţii vectoriale cu dimensiunea mai mică decât n. Dacă f este forma nulă atunci f este diagonalizabilă. Presupunem că f este nenulă şi simetrică. Din problema **6.116** rezultă că există $x \in V$ astfel încât $f(x,x) \neq 0$, iar f fiind biliniară deducem că că $x \neq 0$. Definind

$$g : V \to K,\ g(z) = f(x,z)$$

urmează că g este liniară şi nenulă, ceea ce ne arată că $\operatorname{Im} g$ este subspaţiu nenul al lui K, ceea ce implică $\operatorname{Im} g = K$, pentru că singurele subspaţii ale lui K sunt $\{0\}$ şi K. Din $\dim V = \dim(\operatorname{Ker} g) + \dim(\operatorname{Im} g)$ rezultă $\dim(\operatorname{Ker} g) = n-1$, pentru că $\dim K = 1$. Întrucât restricţia lui f la $\operatorname{Ker} g$ este simetrică, din ipoteza inducţiei urmează că există o bază $v = (v_1, \ldots, v_{n-1})$ a lui $\operatorname{Ker} g$ în care matricea restricţiei $f|_{\operatorname{Ker} f}$ este diagonală, adică $f(v_i, v_j) = 0$ pentru $i \neq j$, $i,j \in \{1, \ldots, n-1\}$. Din $f(x,x) \neq 0$ rezultă $x \notin \operatorname{Ker} g$, de unde deducem că $\overline{v} = (v_1, \ldots, v_{n-1}, x)$ este bază a lui V pentru că $\dim V = \dim(\operatorname{Ker} g) + 1$. Întrucât $v_i \in \operatorname{Ker} g$ urmează

$$f(x, v_i) = 0 = f(v_i, x),\ \forall i \in \{1, \ldots, n-1\}.$$

Astfel am arătat că matricea lui f în baza $\overline{v}$ are forma diagonală.

6.119. i) Efectuând succesiv câte o transformare elementară pe coloane, urmată de analoga pe linii, aducem pe A la forma diagonală

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \xrightarrow{c_1} \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} \xrightarrow{l_1} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = D.$$

Pornind de la I_2 şi efectuând transformările de mai sus asupra coloanelor obţinem matricea care diagonalizează pe A:

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \xrightarrow{c_1} \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} = S,$$

adică ${}^tSAS = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = D$. Fie (e_1, e_2) baza canonică. Efectuând schimbarea de bază $(v_1, v_2) = (e_1, e_2)S$, care conduce la schimbarea de coordonate

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = S \begin{pmatrix} x_1' \\ x_2' \end{pmatrix},$$

obţinem

$$f(x, y) = (x_1', x_2')D \begin{pmatrix} y_1' \\ y_2' \end{pmatrix} = x_1'y_1' - x_2'y_2',$$

unde $x_1',\ x_2'$, respectiv $y_1',\ y_2'$, sunt coordonatele lui x, respectiv y, în baza (v_1, v_2).
ii) Procedăm analog cu i). Efectuând succesiv o transformare elementară pe coloane, urmată de analoga pe linii, avem:

$$B = \begin{pmatrix} 0 & 1 & 2 \\ 1 & -1 & 3 \\ 2 & 3 & 4 \end{pmatrix} \xrightarrow{c_1} \begin{pmatrix} 1 & 0 & 2 \\ -1 & 1 & 3 \\ 3 & 2 & 4 \end{pmatrix} \xrightarrow{l_1} \begin{pmatrix} -1 & 1 & 3 \\ 1 & 0 & 2 \\ 3 & 2 & 4 \end{pmatrix}$$

$$\xrightarrow{c_2} \begin{pmatrix} -1 & 0 & 3 \\ 1 & 1 & 2 \\ 3 & 5 & 4 \end{pmatrix} \xrightarrow{l_2} \begin{pmatrix} -1 & 0 & 3 \\ 0 & 1 & 5 \\ 3 & 5 & 4 \end{pmatrix} \xrightarrow{c_3} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 5 \\ 3 & 5 & 13 \end{pmatrix}$$

$$\xrightarrow{l_3} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 5 \\ 0 & 5 & 13 \end{pmatrix} \xrightarrow{c_4} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 5 & -12 \end{pmatrix} \xrightarrow{l_4} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix} = D.$$

Pornind de la I_3 şi efectuând transformările de mai sus asupra coloanelor obţinem matricea care diagonalizează pe B:

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{c_1} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{c_2} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{c_3} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{c_4} \begin{pmatrix} 0 & 1 & -5 \\ 1 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} = S.$$

Deci ${}^tSBS = D$. Efectuând schimbarea de bază $(v_1, v_2, v_3) = (e_1, e_2, e_3)S$ unde (e_1, e_2, e_3) este baza canonică, care conduce la schimbarea de coordonate

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = S \begin{pmatrix} x_1' \\ x_2' \\ x_3' \end{pmatrix},$$

obţinem $f(x, y) = -x_1'y_1' + x_2'y_2' - 12x_3'y_3'$, unde $x_1',\ x_2',\ x_3'$, respectiv $y_1',\ y_2',\ y_3'$, sunt coordonatele lui x, respectiv y, în baza (v_1, v_2, v_3).

6.120. Din soluţia problemei anterioare rezultă: i) $q(x) = f(x,x) = x_1'^2 - x_2'^2$, ii) $q(x) = f(x,x) = -x_1'^2 + x_2'^2 - 12x_3'^2$.

6.121. 1) $q_1(x,y) = 2\left(x^2 + \frac{3}{2}xy\right) + 6y^2 = 2\left(x^2 + \frac{3}{2}xy\right) - \frac{18}{16}y^2 + 6y^2 =$
$= 2\left(x + \frac{3}{4}y\right)^2 + \frac{39}{8}y^2$;
2) $q_2(x,y) = (2x+2y)^2 - 4x^2$;
3) $q_3(x,y,z) = (x+y+2z)^2 + 2y^2 + 3z^2 - 3yz = (x+y+2z)^2 + 2\left(y^2 + z^2 - \frac{3}{2}yz\right) +$
$+3z^2 = (x+y+2z)^2 + 2\left(y - \frac{3}{4}z\right)^2 + \frac{15}{8}z^2$;
4) $q_4(x,y) = (x+y)^2 - (x-y)^2$;
5) $q_5(x,y,z) = (x+2y+z)^2 - 2yz = (x+2y+z)^2 - \frac{1}{2}(y+z)^2 + \frac{1}{2}(y-z)^2$.

6.122. Matricea lui f în baza canonică este $A = \begin{pmatrix} \widehat{0} & \widehat{1} \\ \widehat{1} & \widehat{0} \end{pmatrix}$. Presupunem că este diagonalizabilă, adică există $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_2)$ inversabilă astfel încât ${}^tSAS = \begin{pmatrix} \widehat{1} & \widehat{0} \\ \widehat{0} & \widehat{1} \end{pmatrix}$ ceea ce conduce în $\mathbb{Z}_2$ la egalitatea imposibilă $2ac = \widehat{1}$.

6.123. Indicaţie. Se folosesc egalităţile ${}^t(X \pm Y) = {}^tX \pm {}^tY$ şi ${}^t(XY) = {}^tY\,{}^tX$, unde $X, Y \in M_n(K)$. f) Din $A = -{}^tA$ rezultă că $\det A = (-1)^n \det A$.

6.124. Indicaţii. i) În K avem $1 = -1$, deci $a = -a$ pentru orice $a \in K$.
ii) Se vrifică uşor că suma a două matrici simetrice este o matrice simetrică. Dacă ii) nu ar fi adevărată atunci, conform lui i), matricea $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ar fi suma a două matrici simetrice, deci ar fi simetrică, ceea ce este fals.

6.125. Răspuns. $\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R} \right\}$.

6.126. $p_A = \det(A - XI_n) = \det({}^t(A - XI_n)) = \det({}^tA - XI_n)p_{\,{}^tA}$.

6.127. Se foloseşte problema **6.109** şi avem

$$p_M = \begin{vmatrix} A - XI_n & O_{m,n} \\ B & C - XI_m \end{vmatrix} = |A - XI_n| \cdot |C - XI_m| = p_A \cdot p_C.$$

6.128. Dacă A este inversabilă atunci

$$p_{AB} = |AB - XI_n| = |A^{-1}(AB - XI_n)A| = |BA - XI_n| = p_{BA}.$$

6.129. Fie $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$. Întrucât $p_A = X^2 - (a+d)X + (ad - bc)$, avem

$$\begin{cases} p_A(1) = 0 \\ p_A(-1) = 0 \end{cases} \Leftrightarrow \begin{cases} a + d = 0 \\ ad - bc = 1 \end{cases} \Leftrightarrow \begin{cases} d = -a \\ bc = -1 - a^2. \end{cases}$$

Deci matricele cerute sunt $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ cu $bc = -1 - a^2$.

6.130. i) Din $p_A(\lambda) = \det(A - \lambda I_n)$ rezultă că $p_A(0) = 0$ dacă şi numai dacă $\det A = 0$.
ii) Dacă $A = (a_{ij})$ atunci, adunând în $\det(A - I_n) = p_A(1)$ toate coloanele la ultima coloană primim:

$$p_A(1) = \begin{vmatrix} a_{11}-1 & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22}-1 & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn}-1 \end{vmatrix} = \begin{vmatrix} a_{11}-1 & a_{12} & \dots & a_{1\,n-1} & 0 \\ a_{21} & a_{22}-1 & \dots & a_{2\,n-1} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{n\,n-1} & 0 \end{vmatrix} = 0.$$

6.131. i) Din $p_A(\lambda) = \det(A - \lambda I_n)$ rezultă $p_A(0) = \det A$. Deci A este inversabilă dacă şi numai dacă $p_A(0) \neq 0$. Folosind proprietăţile operaţiilor cu matrice şi proprietăţile determinanţilor, avem:

$$\begin{aligned} p_{A^{-1}}(\lambda) &= \det(A^{-1} - \lambda I_n) = \det(A^{-1} - \lambda A^{-1}A) = \det(A^{-1}(I_n - \lambda A)) = \\ &= \det(A^{-1})\det(I_n - \lambda A) = (\det A)^{-1}\det\left(-\lambda\left(A - (\lambda)^{-1}I_n\right)\right) = \\ &= (-\lambda)^n(\det A)^{-1}\det(A - \lambda^{-1}I_n) = (-1)^n\lambda^n(\det A)^{-1}p_A(\lambda^{-1}). \end{aligned}$$

ii) Dacă λ este valoare proprie a lui A şi A este inversabilă atunci din i) rezultă că $\lambda \neq 0$ şi λ^{-1} este valoare proprie a lui A.

6.132. Pentru cazul $\dim V < \infty$ această problemă este o consecinţă a problemei anterioare. Menţionăm, însă, că cele două cazuri nu necesită a fi tratate diferenţiat. Presupunând că 0 este valoare proprie a lui f rezultă că există $x \in V$, $x \neq 0$ astfel încât $f(x) = 0 \cdot x = 0 = f(0)$, ceea ce contrazice injectivitatea lui f. Dacă $x \neq 0$ şi $\lambda \neq 0$ sunt vector, respectiv valoare proprie (corespunzătoare) pentru f atunci $f(x) = \lambda x$ implică $x = f^{-1}(f(x)) = f^{-1}(\lambda x) = \lambda f^{-1}(x)$, de unde deducem $f^{-1}(x) = \lambda^{-1}x$. Transformarea liniară $\varphi : K[X] \to K[X]$ care se obţine ca o extindere a aplicaţiei $\{X^k \mid k \in \mathbb{N}\} \to K[X]$, $X^k \mapsto X^{2k}$ nu este surjectivă, dar este injectivă, prin urmare egalitatea $\varphi(f) = 0 \cdot f = 0$ are loc dacă şi numai dacă $f = 0$.

6.133. Întrucât restul împărţirii lui p la $X - \lambda$ este $p(\lambda)$, există $q \in K[X]$ astfel încât $p = (X - \lambda)q + p(\lambda)$. Rezultă că $p(A) - p(\lambda)I_n = (A - \lambda I_n)q(A)$, de unde urmează că $\det(p(A) - p(\lambda)I_n) = \det(A - \lambda I_n)\det q(A) = 0 \cdot \det q(A) = 0$. Deci $p(\lambda)$ este valoare proprie a lui $p(A)$. Considerând $p = X^n$ se obţine partea a doua din enunţ.

6.134. Pentru cazul $\dim V < \infty$ această problemă este o consecinţă a problemei anterioare, însă cele două cazuri nu necesită a fi tratate diferenţiat. Dacă $x \neq 0$ şi $\lambda \in K$ sunt vector, respectiv valoare proprie (corespunzătoare) pentru f atunci $f(x) = \lambda x$ implică $f^2(x) = f(f(x)) = f(\lambda x) = \lambda f(x) = \lambda^2 x$. Inductiv, se obţine $f^n(x) = \lambda^n x$, pentru orice $n \in \mathbb{N}^*$. Prin urmare,

$$\begin{aligned} p(f)(x) &= (a_0 1_V + a_1 f + \cdots + a_n f^n)(x) = a_0 x + a_1 f(x) + \cdots + a_n f^n(x) \\ &= a_0 x + a_1 \lambda x + \cdots + a_n \lambda^n x = (a_0 + a_1\lambda + \cdots + a_n\lambda^n)x = p(\lambda)x. \end{aligned}$$

6.135. i) Amintim definiţia determinantului unei matrice $B = (b_{ij})$ de tipul (n, n) cu elemente dintr-un inel comutativ:

$$\det B = \sum_{\sigma \in S_n} (-1)^{\operatorname{inv}\sigma} b_{1\sigma(1)} b_{2\sigma(2)} \cdots b_{n\sigma(n)}.$$

Luând $B = A - XI_n$ deducem

$$\det B = (a_{11} - X)(a_{22} - X)\cdots(a_{nn} - X) + \sum_{\sigma\in S_n\setminus\{e\}} (-1)^{\operatorname{inv}\sigma} b_{1\sigma(1)}b_{2\sigma(2)}\cdots b_{n\sigma(n)},$$

unde primul termen este dat de permutatrea identică $\sigma = e$. Dacă $\sigma \neq e$ atunci există $i \in \{1, \ldots, n\}$ astfel încât $j = \sigma(i) \neq i$, de unde rezultă că produsul corespunzător lui σ nu conţine factorii $(X - a_{ii})$ şi $(X - a_{jj})$, deci are gardul cel mult $n - 2$. Cerinţa din enunţ se obţine notând $q = \sum\limits_{\sigma\neq e}(-1)^{\operatorname{inv}\sigma} b_{1\sigma(1)}b_{2\sigma(2)}\cdots b_{n\sigma(n)}$.

ii) Din i) rezultă $a_n = (-1)^n$ şi $a_{n-1} = (-1)^n(a_{11} + a_{22} + \cdots + a_{nn})$, iar din $p_A = \det(A - XI_n)$ urmează $a_0 = p_A(0) = \det A$.

iii) Rezultă din ii) şi din relaţiile lui Viète.

iv) Din i) deducem că termenul lui p_A de gradul $n - 2$ se obţine adunând termenul de gradul $n - 2$ din $(a_{11} - X)(a_{22} - X)\cdots(a_{nn} - X)$ care este

$$(-1)^{n-2}(a_{11}a_{22} + a_{11}a_{33} + \cdots + a_{11}a_{nn} + \cdots + a_{n-1\,n-1}a_{nn})$$

cu termenii de gradul $n - 2$ din produsele furnizate de $\sigma = (ij)$, $i \neq j$, care sunt

$$-(a_{11}-X)\cdots(a_{i-1\,i-1}-X)a_{ij}(a_{i+1\,i+1}-X)\cdots(a_{j-1\,j-1}-X)a_{ji}(a_{j+1\,j+1}-X)\cdots(a_{nn}-X),$$

cu $i < j$. Rezultă că a_{n-2} este egal cu

$$(-1)^{n-2}(a_{11}a_{22}+a_{11}a_{33} + \cdots + a_{11}a_{nn} + \cdots + a_{n-1\,n-1}a_{nn}) - (-1)^{n-2}\sum_{i<j} a_{ij}a_{ji} =$$
$$=(-1)^{n-2}\sum_{i<j}\begin{vmatrix} a_{ii} & a_{ij} \\ a_{ji} & a_{jj}\end{vmatrix} = (-1)^n\sum_{i<j}\begin{vmatrix} a_{ii} & a_{ij} \\ a_{ji} & a_{jj}\end{vmatrix}.$$

6.136. i) $f = b_m(X - x_1)\cdots(X - x_m) \Rightarrow f(A) = b_m(A - x_1I_n)\cdots(A - x_mI_n) \Rightarrow \det f(A) = b_m^n \det(A - x_1I_n)\cdots\det(A - x_mI_n) = b_m^n p_A(x_1)\cdots p_A(x_m)$.

ii) Din $p_A = \det(A - XI_n) = (\lambda_1 - X)(\lambda_2 - X)\cdots(\lambda_n - X)$ şi

$$f(A) = b_m(A - x_1I_n)\cdots(A - x_mI_n)$$

rezultă

$$\begin{aligned}&\det f(A) = b_m^n \det(A - x_1I_n)\cdots\det(A - x_mI_n)\\ &= b_m^n[(\lambda_1 - x_1)\cdots(\lambda_n - x_1)][(\lambda_1 - x_2)\cdots(\lambda_n - x_2)]\cdots[(\lambda_1 - x_n)\cdots(\lambda_n - x_n)]\\ &= f(\lambda_1)f(\lambda_2)\cdots f(\lambda_n).\end{aligned}$$

Aplicând cele de mai sus polinomului $g = f - \lambda$ primim

$$\det g(A) = \det(f(A) - \lambda I_n) = (f(\lambda_1) - \lambda)\cdots(f(\lambda_n) - \lambda),$$

adică $p_{f(A)}(\lambda) = (f(\lambda_1) - \lambda)\cdots(f(\lambda_n) - \lambda)$, de unde rezultă că valorile proprii ale lui $f(A)$ sunt $f(\lambda_1), \ldots, f(\lambda_n)$.

6.137. a) Valorile proprii ale lui f sunt soluţiile ecuaţiei $\det([f]_v - \lambda I_4) = 0$, adică

$$\begin{vmatrix} 1-\lambda & 1 & 0 & 2 \\ 0 & -1-\lambda & 1 & 2 \\ 0 & 0 & 2-\lambda & 3 \\ 0 & 0 & 0 & -2-\lambda \end{vmatrix} = 0 \Leftrightarrow (1-\lambda)(-1-\lambda)(2-\lambda)(-2-\lambda) = 0.$$

Acestea sunt $\lambda_1 = 1$, $\lambda_2 = -1$, $\lambda_3 = 2$, $\lambda_4 = -2$. Vectorii proprii ai lui f sunt elementele mulţimii $(V(1) \cup V(-1) \cup V(2) \cup V(-2)) \setminus \{0\}$. Avem

$$V(1) = \left\{ x_1v_1 + x_2v_2 + x_3v_3 + x_4v_4 \mid ([f]_v - I_4) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\},$$

adică $V(1)$ este dat de soluţiile sistemului

$$\begin{pmatrix} 0 & 1 & 0 & 2 \\ 0 & -2 & 1 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & -3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{cases} x_1 = \alpha \\ x_2 = 0 \\ x_3 = 0 \\ x_4 = 0 \end{cases}, \ \alpha \in \mathbb{R}.$$

Obţinem $V(1) = \{\alpha v_1 \mid \alpha \in \mathbb{R}\} = \langle v_1 \rangle$. În mod analog se obţine

$$V(-1) = \langle v_1 - 2v_2 \rangle,\ V(2) = \langle v_1 + v_2 + 3v_3 \rangle,\ V(-2) = \langle v_1 + 5v_2 + 3v_3 - 4v_4 \rangle.$$

b) Întrucât valorile proprii ale lui f sunt distincte, vectorii proprii

$$v_1' = v_1,\ v_2' = v_1 - 2v_2,\ v_3' = v_1 + v_2 + 3v_3,\ v_4' = v_1 + 5v_2 + 3v_3 - 4v_4$$

sunt liniar independenţi, deci $v' = (v_1', v_2', v_3', v_4')$ este o bază a lui V.
c) Folosind definiţia matricei unei transformări liniare se obţine

$$[f]_{v'} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & -2 \end{pmatrix}.$$

6.138. Indicaţie. $f(v_1 + 2v_2) = v_1 + 2v_2 \in S$ şi $f(v_2 + v_3 + 2v_4) = v_2 + v_3 + 2v_4 \in S$.

6.139. Dacă A este similară cu o matrice triunghiulară T, adică există o matrice $S \in GL_n(K)$ astfel încât $S^{-1}AS = T$, atunci

$$\begin{aligned} p_T(\lambda) &= \det(S^{-1}AS - \lambda I_n) = \det(S^{-1}AS - \lambda S^{-1}S) \\ &= \det(S^{-1}) \det(A - \lambda I_n) \det S = \det(A - \lambda I_n) = p_A(\lambda). \end{aligned}$$

Rezultă că elementele de pe diagonala principală a lui $T \in M_n(K)$ sunt rădăcinile lui p_A. Demonstrăm prin inducţie după n că dacă p_A are toate rădăcinile în K atunci A este similară cu o matrice triunghiulară. Această proprietate este adevărată pentru $n = 1$. O presupunem adevărată pentru $n - 1$ cu $n > 1$. Fie λ_1 o valoare proprie şi

v_1 un vector propriu corespunzător lui λ_1. Există o bază $v = (v_1, \cdots, v_n)$ a lui K^n. Relativ la v, endomorfismul

$$t_A : K^n \to K^n,\ t_A(x_1, \ldots, x_n) = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

are matricea de forma

$$A' = \begin{pmatrix} \lambda_1 & a'_{12} & \ldots & a'_{1n} \\ 0 & a'_{22} & \ldots & a'_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & a'_{n2} & \ldots & a'_{nn} \end{pmatrix}$$

şi $p_A(\lambda) = p_{A'}(\lambda) = (\lambda_1 - \lambda) \begin{vmatrix} a'_{22} - \lambda & \ldots & a'_{2n} \\ \vdots & & \vdots \\ a'_{n2} & \ldots & a'_{nn} - \lambda \end{vmatrix} = (\lambda_1 - \lambda)p_{A''}$, unde A'' este matricea obţinută din A' prin suprimarea primei linii şi primei coloane. Din ipoteza problemei şi din $p_A(\lambda) = (\lambda_1 - \lambda)p_{A''}$ rezultă că $p_{A''}$ are toate rădăcinile în K. Acum, din ipoteza inducţiei, urmează că A'' este similară cu matricea triunghiulară T'', adică există $P \in GL_{n-1}(K)$ astfel încât $P^{-1}A''P = T''$. Luând $Q = \begin{pmatrix} 1 & O \\ O & P \end{pmatrix}$ şi $L = (a'_{12} \ldots a'_{1n})$ avem

$$Q^{-1}A'Q = \begin{pmatrix} \lambda_1 & LP \\ O & P^{-1}AP \end{pmatrix} = \begin{pmatrix} \lambda_1 & LP \\ O & T'' \end{pmatrix},$$

iar ultima matrice este triunghiulară şi similară cu A.

6.140. i) Matricele transformărilor date în bazele canonice sunt

$$[f]_e = \begin{pmatrix} -3 & 4 \\ 2 & -1 \end{pmatrix} = A,\ [g]_e = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = B,\ [h]_{e'} = \begin{pmatrix} -1 & 2 & 2 \\ 2 & 2 & 2 \\ -3 & -6 & -6 \end{pmatrix} = C,$$

prin urmare, $p_f = \det(A - XI_2) = X^2 + 4X - 5$, $p_g = \det(B - XI_2) = X^2 - 2$, $p_h = \det(C - XI_2) = -X(X^2 + 5X + 6)$.
ii) Valorile proprii ale endomorfismului f sunt soluţiile ecuaţiei $p_f(\lambda) = 0$, adică $\lambda_1 = 1$, $\lambda_2 = -5$, valorile proprii ale lui g sunt soluţiile ecuaţiei $p_g(\lambda) = 0$, adică $\lambda'_1 = -\sqrt{2}$, $\lambda'_2 = \sqrt{2}$, iar valorile proprii ale lui h sunt soluţiile ecuaţiei $p_h(\lambda) = 0$, adică $\lambda''_1 = 0$, $\lambda''_2 = -2$, $\lambda''_3 = -3$.
iii) Subspaţiul propriu $V_f(\lambda_i)$ al lui f corespunzător valorii proprii λ_i este format din soluţiile sistemului liniar şi omogen scris sub formă matriceală astfel:

$$(A - \lambda_i I_2) \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Notând $A = (a_{ij})$ se obţine sistemul

$$\begin{cases} (a_{11} - \lambda_i)x + \quad a_{12}y \quad = 0 \\ \quad a_{21}x \quad + (a_{22} - \lambda_i)y = 0. \end{cases}$$

Prin calcule se obţine

$$V_f(\lambda_1) = \{(a,a) \mid a \in \mathbb{R}\} = \langle(1,1)\rangle,\ V_f(\lambda_2) = \{(-2a,a) \mid a \in \mathbb{R}\} = \langle(-2,1)\rangle.$$

Analog se obţin subspaţiile $V_g(\lambda_1') = \{(a, -(1+\sqrt{2})a) \mid a \in \mathbb{R}\} = \langle(1, -1-\sqrt{2})\rangle$ şi $V_g(\lambda_2') = \{(a, (\sqrt{2}-1)a) \mid a \in \mathbb{R}\} = \langle(1, \sqrt{2}-1)\rangle$. Subspaţiul propriu $V_h(\lambda_i'')$ al lui h corespunzător valorii proprii λ_i'' este format din soluţiile sistemului liniar şi omogen scris sub formă matriceală astfel:

$$(C - \lambda_i I_3)\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Notând $C = (c_{ij})$ se obţine sistemul

$$\begin{cases} (c_{11} - \lambda_i)x + \quad c_{12}y \quad + \quad c_{13}z \quad = 0 \\ \quad c_{21}x \quad + (c_{22} - \lambda_i)y + \quad c_{23}z \quad = 0 \\ \quad c_{31}x \quad + \quad c_{23}y \quad + (c_{32} - \lambda_i)z = 0. \end{cases}$$

Astfel, avem

$$V_h(\lambda_1'') = \{(0,-a,a) \mid a \in \mathbb{R}\} = \langle(0,-1,1)\rangle, V_h(\lambda_2'') = \{(-2a,a,0) \mid a \in \mathbb{R}\} = \langle(-2,1,0)\rangle,$$
$$V_h(\lambda_1'') = \{(-a,0,a) \mid a \in \mathbb{R}\} = \langle(-1,0,1)\rangle.$$

iv) Din faptul că valorile proprii ale lui f, g şi h sunt din $\mathbb{R}$ şi sunt diferite rezultă că f, g şi h sunt diagonalizabile, sistemele de vectori $v = (v_1, v_2)$, cu $v_1 = (1,1)$, $v_2 = (-2,1)$ şi $v' = (v_1', v_2')$, cu $v_1' = (1, -1-\sqrt{2})$, $v_2' = (1, \sqrt{2}-1)$ formează baze în $\mathbb{R}^2$, $v'' = (v_1'', v_2'', v_3'')$, cu $v_1'' = (0,-1,1)$, $v_2'' = (-2,0,1)$, $v_3'' = (-1,0,1)$ formează o bază în $\mathbb{R}^3$ şi

$$[f]_v = \begin{pmatrix} 1 & 0 \\ 0 & -5 \end{pmatrix},\ [g]_{v'} = \begin{pmatrix} -\sqrt{2} & 0 \\ 0 & \sqrt{2} \end{pmatrix},\ [h]_{v''} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -3 \end{pmatrix}.$$

Matricea de trecere de la e la v, respectiv v' este

$$S = \begin{pmatrix} 1 & -2 \\ 1 & 1 \end{pmatrix},\ T = \begin{pmatrix} 1 & 1 \\ -1-\sqrt{2} & \sqrt{2}-1 \end{pmatrix}$$

iar de la e' la v'' este

$$U = \begin{pmatrix} 0 & -2 & -1 \\ -1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Avem

$$S^{-1} = \frac{1}{3}\begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix},\ T^{-1} = \frac{1}{2\sqrt{2}}\begin{pmatrix} \sqrt{2}-1 & -1 \\ 1+\sqrt{2} & 1 \end{pmatrix},\ U^{-1} = \begin{pmatrix} -1 & -2 & -1 \\ -1 & -1 & -1 \\ 1 & 2 & 2 \end{pmatrix}$$

şi

$$[f]_e = S[f]_v S^{-1},\ [g]_e = T[g]_{v'} T^{-1},\ [h]_{e'} = U[h]_{v''} U^{-1}.$$

Rezultă că

$$([f]_e)^n = S\begin{pmatrix} 1 & 0 \\ 0 & (-5)^n \end{pmatrix} S^{-1},\ ([g]_e)^n = T\begin{pmatrix} (-\sqrt{2})^n & 0 \\ 0 & (\sqrt{2})^n \end{pmatrix} T^{-1},$$

$$([h]_{e'})^n = U\begin{pmatrix} 0 & 0 & 0 \\ 0 & (-2)^n & 0 \\ 0 & 0 & (-3)^n \end{pmatrix} U^{-1}.$$

6.141. Răspuns. 1) i) Polinoamele caracteristice sunt $p_f = -X^3 + 6X^2 - 11X + 6$, $p_g = (4 - X)(-2 - X)(7 - X)$. ii) Valorile proprii ale lui f respectiv g sunt $\lambda_1 = 1$, $\lambda_2 = 2$, $\lambda_3 = 3$, respectiv $\lambda_1 = -2$, $\lambda_2 = 4$, $\lambda_3 = 7$. iii) Subspaţiile proprii ale lui f respectiv g sunt $V_f(1) = \langle(1, 0, -1)\rangle$, $V_f(2) = \langle(2, -1, 0)\rangle$, $V_f(3) = \langle(0, 1, -1)\rangle$ respectiv $V_g(-2) = \langle(3, -2, 0)\rangle$, $V_g(4) = \langle(1, 0, 0)\rangle$, $V_g(7) = \langle(24, 8, 9)\rangle$.

6.142. Indicaţie. Nu are valori proprii în $\mathbb{R}$.

6.143. Indicaţie. Nu are valori proprii în $\mathbb{R}$.

6.144. Indicaţie. i) A are două valori proprii distinte în $\mathbb{R} \setminus \mathbb{Q}$. ii) B are două valori proprii distinte în $\mathbb{C} \setminus \mathbb{R}$.

6.145. Indicaţie. Se procedează ca în problema **6.140**.

6.146. i) $p_A(\lambda) = \begin{vmatrix} a - \lambda & b \\ b & d - \lambda \end{vmatrix} = \lambda^2 - (a+d)\lambda + (ad - bc) = \lambda^2 - \mathrm{Tr}(A)\lambda + \det A$, unde $\mathrm{Tr}(A) = a + d$ este urma lui A.
ii) Din teorema lui Cayley-Hamilton rezultă că $p_A(A) = O_2$, ceea ce implică $A^2 = (a + d)A$, de unde se deduce $A^n = (a + d)^{n-1}A$.
iii) $p_A(A) = O_2 \Rightarrow A(A - (a + d)I_2) = (ad - bc)I_2 \Rightarrow A^{-1} = \dfrac{1}{\det A}(A - (a + d) \cdot I_2)$.
iv) Matricea $A \in M_n(\mathbb{R})$ este diagonalizabilă în $M_n(\mathbb{R})$, respectiv $M_n(\mathbb{C})$ numai în următoarele situaţii:
1) polinomul caracteristic al lui A are două rădăcini diferite în $\mathbb{R}$, respectiv $\mathbb{C}$ — ceea ce înseamnă că A are două valori proprii distincte — în acest caz avem $\Delta > 0$, respectiv $\Delta \neq 0$;
2) polinomul caracteristic al lui A are o rădăcină (reală) dublă $\lambda_1 = \lambda_2 = \dfrac{a + d}{2}$ şi $\dim V(\lambda_1) = 2 - \mathrm{rang}(A - \lambda_1 I_2) = 2$, ceea ce este echivalent cu $\mathrm{rang}(A - \lambda_1 I_2) = 0$ şi are loc dacă şi numai dacă $a = d$ şi $b = c = 0$.

6.147. Indicaţie. i) Fie e o bază a lui V. Procedând ca la punctul iv) al problemei anterioare avem f diagonalizabil dacă şi numai dacă $\mathrm{rang}([f]_e - \lambda I_n) = 0$, ceea ce are loc dacă şi numai dacă $[f]_e = \lambda I_n$.

6.148. Fie $p_A = (-1)^n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ polinomul caracteristic al lui A. Avem $a_0 = \det A \neq 0$, iar din teorema lui Cayley-Hamilton rezultă că $p_A(A) = O_n$. Deducem că

$$A((-1)^n A^{n-1} + a_{n-1}A^{n-2} + \cdots + a_1 I_n) = a_0 I_n = ((-1)^n A^{n-1} + a_{n-1}A^{n-2} + \cdots + a_1 I_n)A,$$

deci $A^{-1} = g(A)$, cu $g = \dfrac{1}{a_0}((-1)^n X^{n-1} + a_{n-1}X^{n-2} + \cdots + a_1)$.

6.149. Polinomul caracteristic al lui A este $p_A = -X^3 + 4X^2 - 5X - 2$. Dacă q şi r sunt câtul, respectiv restul împărţirii în $\mathbb{R}[X]$ a polinomului $f = X^4 - 11X^2 + 22X$ la p_A atunci $f(A) = p_A(A)q(A) + r(A) = r(A)$. Avem $r = 8$, prin urmare $f(A) = 8I_3$.

6.150. a) i) Polinomul caracteristic al lui A este

$$p_A = \det(A - XI_4) = (X-2)^3(X-3)$$

cu rădăcinile $\lambda_1 = 2$, $\lambda_2 = 3$ care au ordinele de multiplicitate $m_1 = 3$ şi $m_2 = 1$. Subspaţiul propriu corespunzător lui 2 este $V(2) = \mathrm{Ker}(f - 2 \cdot 1_V)$, iar

$$[f - 2 \cdot 1_V]_e = A - 2I_4 = \begin{pmatrix} 0 & -1 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix} = A_1.$$

Din formula $\dim V(2) = \dim(\mathrm{Ker}(f - 2 \cdot 1_V)) + \dim(\mathrm{Im}(f - 2 \cdot 1_V))$ şi din faptul că

$$\dim(\mathrm{Im}(f - 2 \cdot 1_V)) = \mathrm{rang}\, A_1 = 2$$

rezultă

$$r_1 = \dim V(2) = 4 - \mathrm{rang}\, A_1 = 4 - 2 = 2 < m_1,$$

de unde urmează că A nu este diagonalizabilă şi că există în J două blocuri Jordan care au pe 2 situat pe diagonala principală. Dacă $V_g(2)$ este subspaţiu propriu generalizat al lui f corespunzător lui 2 atunci

$$\dim V_g(2) = m_1 = 3 \text{ şi } V_g(2) = \mathrm{Ker}(f - 2 \cdot 1_V)^3.$$

Avem

$$A_2 = (A - 2I_4)^2 = \begin{pmatrix} 0 & -2 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & -2 & 1 & 1 \end{pmatrix} = (A - 2I_4)^3$$

şi $r_2 = \mathrm{rang}\, A_1 - \mathrm{rang}\, A_2 = 2 - 1 = 1$. Formăm următoarea schemă de puncte

$$\begin{matrix} \bullet & \bullet \\ \bullet & \end{matrix}$$

Prima linie conţine r_1 puncte, iar a doua r_2 puncte. Numărul coloanelor, adică r_1 indică numărul blocurilor Jordan corespunzătoare lui $\lambda_1 = 2$. Deci fiecărei coloane îi corespunde un bloc Jordan, iar numărul punctelor de pe coloană coincide cu ordinul matricei bloc corespunzătoare. Prin urmare, primei colane îi corespunde matricea

$$\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix},$$

iar celei de-a doua îi corespunde matricea $(\,2\,)$ şi submatricea lui J corespunzătoare lui $\lambda_1 = 2$ este

$$J_1 = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Remarcăm că numărul total de puncte din schemă coincide cu $\dim V_g(2)$. Rădăcina $\lambda_2 = 3$ fiind simplă, rezultă că $V(3) = V_g(3)$ şi $\dim V(3) = m_2 = 1$. Deci submatricea lui J corespunzătoare lui $\lambda_2 = 3$ este $J_2 = (\,3\,)$. În concluzie, forma canonică Jordan a lui A este

$$J = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

ii) Avem $V = V_g(2) \oplus V_g(3)$ şi subspaţiile $V_g(2)$, $V_g(3)$ sunt invariante relativ la f. Baza căutată se obţine reunind bazele canonice Jordan ale restricţiilor $f_i = f|_{V_g(\lambda_i)}$, $i = 1, 2$. Determinăm baza canonică Jordan a lui f_1. Avem

$$(x_1, x_2, x_3, x_4) \in V(2) \Leftrightarrow A_1 \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{cases} -x_2 + x_4 = 0 \\ x_2 - x_3 = 0 \\ x_2 - x_3 = 0 \\ -x_2 + x_4 = 0 \end{cases} \Leftrightarrow \begin{cases} x_3 = x_2 \\ x_4 = x_2 \end{cases}$$

şi

$$(x_1, x_2, x_3, x_4) \in V_g(2) \Leftrightarrow A_2 \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow x_4 = 2x_2 - x_3,$$

de unde deducem

$$V(2) = \{(a, b, b, b) \mid a, b \in \mathbb{R}\}, \;\; V_g(2) = \{(a, b, c, 2b - c) \mid a, b, c \in \mathbb{R}\}.$$

Vectorii $v_1 = (1, 0, 0, 0)$, $v_2 = (0, 1, 2, 0)$, $v_3 = (0, 1, 0, 2)$ formează o bază a lui $V_g(2)$ şi $v_2, v_3 \in V_g(2) \setminus V(2)$. Alegem un vector din $V_g(2) \setminus V(2)$, de exemplu pe v_2 şi un vector din $V(2)$, de exemplu pe v_1, liniar independent de $(f - 2 \cdot 1_V)(v_2)$ şi formăm o bază Jordan a lui f_1 folosind schema de la i) astfel:

$\bullet\ (f - \lambda_1 1_V)(v_2) \quad \bullet\ v_1$

$\bullet\ v_2$

Avem $(f - \lambda_1 1_V)(v_2) = (-1, -1, -1, -1) = v_2'$, iar baza Jordan a lui f_1 este formată din ciclurile $c_1 = (v_2', v_2)$ şi $c_2 = (v_1)$.

Rădăcina $\lambda_2 = 3$ fiind simplă, rezultă că $V(3) = V_g(3)$ şi f_2 este diagonalizabilă. Întrucât

$$A - 3I_4 = \begin{pmatrix} -1 & -1 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} = B$$

avem

$$(x_1, x_2, x_3, x_4) \in V(3) \Leftrightarrow B \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{cases} -x_1 - x_2 + x_4 = 0 \\ -x_3 = 0 \\ x_2 - 2x_3 = 0 \\ -x_2 = 0 \end{cases} \Leftrightarrow \begin{cases} x_1 = x_4 \\ x_2 = 0 \\ x_3 = 0 \end{cases}$$

de unde deducem $V(3) = \{(a, 0, 0, a) \mid a \in \mathbb{R}\}$. Orice vector nenul din $V(3)$, de exemplu, vectorul $v_3 = (1, 0, 0, 1)$ formează o bază Jordan pentru f_2. Prin urmare, $v = (v_2', v_2, v_1, v_3)$ este bază Jordan pentru f şi $[f]_v = J$.
iii) Dacă S este matricea de trecere de la baza e la baza v, adică

$$S = \begin{pmatrix} -1 & 0 & 1 & 1 \\ -1 & 1 & 0 & 0 \\ -1 & 2 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}$$

atunci $J = S^{-1}AS$.
b) i) Polinomul caracteristic al lui A este

$$p_A = \det(A - XI_4) = (X-2)^2(X-4)^2$$

cu rădăcinile $\lambda_1 = 2$ şi $\lambda_2 = 4$ care au ordinele de multiplicitate $m_1 = 2$ şi $m_2 = 2$. Subspaţiul propriu corespunzător lui 2 este $V(2) = \mathrm{Ker}(f - 2 \cdot 1_V)$, iar

$$[f - 2 \cdot 1_V]_e = A - 2I_4 = \begin{pmatrix} 0 & -4 & 2 & 2 \\ -2 & -2 & 1 & 3 \\ -2 & -2 & 1 & 3 \\ -2 & -6 & 3 & 5 \end{pmatrix} = A_1$$

şi $r_1 = \dim V(2) = \dim V - \mathrm{rang}\, A_1 = 4 - 2 = 2 = m_1$, adică multiplicitatea geometrică a lui λ_1 coincide cu multiplicitatea sa algebrică. Deci $V_g(2) = V(2)$. Notând $f_1 = f|_{V(2)}$ rezultă că f_1 este diagonalizabilă, iar schema asociată matricei sale Jordan este

$$\bullet \quad \bullet$$

ceea ce ne arată că submatricea lui J_1 a lui J corespunzătoare lui $\lambda_1 = 2$ este formată din blocurile $(\,2\,)$, $(\,2\,)$, adică

$$J_1 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

Subspaţiul propriu corespunzător lui $\lambda_2 = 4$ este $V(4) = \mathrm{Ker}(f - 4 \cdot 1_V)$, iar

$$[f - 4 \cdot 1_V]_e = A - 4I_4 = \begin{pmatrix} -2 & -4 & 2 & 2 \\ -2 & -4 & 1 & 3 \\ -2 & -2 & -1 & 3 \\ -2 & -6 & 3 & 3 \end{pmatrix} = B_1,$$

$r_2 = \dim V(4) = \dim V - \mathrm{rang}\, B_1 = 4 - 3 = 1$ şi $\dim V_g(4) = m_2 = 2$. Notând $f_2 = f|_{V_g(4)}$ rezultă că f_2 nu este diagonalizabilă, iar schema asociată matricei sale Jordan este

$$\begin{array}{c} \bullet \\ \bullet \end{array}$$

ceea ce ne arată că submatricea lui J_2 a lui J corespunzătoare lui $\lambda_2 = 4$ este formată dintr-un singur bloc, adică

$$J_2 = \begin{pmatrix} 4 & 1 \\ 0 & 4 \end{pmatrix}.$$

În concluzie,

$$J = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

ii) Avem $V = V(2) \oplus V_g(4)$ şi

$$(x_1, x_2, x_3, x_4) \in V(2) \Leftrightarrow A_1 \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{cases} -4x_2 + 2x_3 + 2x_4 = 0 \\ -2x_1 - 2x_2 + x_3 + 3x_4 = 0 \\ -2x_1 - 2x_2 + x_3 + 3x_4 = 0 \\ -2x_2 - 6x_2 + 3x_3 + 5x_4 = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} 2x_3 + 2x_4 = 4x_2 \\ x_3 + 3x_4 = 2x_1 + 2x_2 \end{cases} \Leftrightarrow \begin{cases} x_3 = -x_1 + 2x_2 \\ x_4 = x_1 \end{cases}$$

ceea ce arată că $V(2) = \{(a, b, 2b - a, a) \mid a, b \in \mathbb{R}\}$ şi

$$v_1 = (2, 1, 0, 2),\ v_2 = (0, 1, 2, 0)$$

formează o bază a lui $V(2)$. Conform schemei asociate lui $\lambda_1 = 2$, orice doi vectori liniar independenţi ai lui $V(2)$, de exemplu v_1 şi v_2 formează o bază Jordan pentru f_1. Acum determinăm o bază Jordan pentru f_2. Avem

$$(x_1, x_2, x_3, x_4) \in V(4) \Leftrightarrow B_1 \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{cases} -2x_2 + 2x_3 + 2x_4 = 0 \\ -2x_1 - 4x_2 + x_3 + 3x_4 = 0 \\ -2x_1 - 2x_2 - x_3 + 3x_4 = 0 \\ -2x_2 - 6x_2 + 3x_3 + 7x_4 = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} -2x_1 - 4x_2 + 2x_3 = -2x_4 \\ -2x_1 - 4x_2 + x_3 = -3x_4 \\ -2x_1 - 2x_2 - x_3 = -3x_4 \end{cases} \Leftrightarrow \begin{cases} x_1 = 0 \\ x_2 = x_4 \\ x_3 = x_4 \end{cases}$$

de unde deducem $V(4) = \{(0, a, a, a, a) \mid a, b \in \mathbb{R}\}$ şi $(0, 1, 1, 1)$ formează o bază a lui $V(4)$. Urmărind scema asociată lui $\lambda_2 = 4$ deducem că baza Jordan a lui f_2 se obţine din schema

- $(f - 4 \cdot 1_V)(v_3)$
- v_3

unde $v_3 \in V_g(4) \backslash V(4)$. Pentru a afla pe v_3 putem urma calea de la a) de determinare a lui $V_g(4)$ care conduce la rezolvarea ecuaţiei matriceale

$$B_2 \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},\ \text{unde } B_2 = (A - 4I_4)^2,$$

ceea ce necesită calcule mai dificile. Vectorul v_3 se poate alege dintre vectorii din $\mathbb{R}^4$ care verifică ecuaţia

$$B_1 \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

Rezolvând sistemul de ecuaţii provenit din această ecuaţie se deduce că v_3 poate fi $v_3 = (1, -1, -1, 0)$. Deci $(f - 4 \cdot 1_V)(v_3) = (0, 1, 1, 1) = v_3'$ şi baza Jordan a lui f_2 este formată din ciclul $c = (v_3', v_3)$. Prin urmare, $v = (v_1, v_2, v_3', v_3)$ este o bază Jordan pentru f şi $[f]_v = J$.
iii) Dacă S este matricea de trecere de la baza e la v, adică

$$S = \begin{pmatrix} 2 & 0 & 0 & 1 \\ 1 & 1 & 1 & -1 \\ 0 & 2 & 1 & -1 \\ 2 & 0 & 1 & 0 \end{pmatrix}$$

atunci $J = S^{-1}AS$.

6.151. i) Polinomul caracteristic al lui A este $p_A = \det(A - XI_6) = X^6$. Deci f are o singură valoare proprie $\lambda = 0$ cu multiplicitatea $m = 6$. Rezultă că $V_g(0) = V$ şi $r_1 = \dim V(0) = \dim V - \operatorname{rang} A = 6 - 3 = 3$. Întrucât

$$A^2 = \begin{pmatrix} 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

urmează că $r_2 = \operatorname{rang} A - \operatorname{rang}(A^2) = 3 - 1 = 2$. Din $r_1 = 3$, $r_2 = 2$ şi din faptul că schema asociată are $6 = \dim V_g(0)$ puncte rezultă $r_3 = 1$. Întrucât există o singură valoare proprie, forma canonică Jordan este determinată de schema

$$\begin{array}{ccc} \bullet & \bullet & \bullet \\ \bullet & \bullet & \\ \bullet & & \end{array}$$

de unde deducem că J este formată din 3 blocuri care corespund la cele trei coloane din schemă:

$$J_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad J_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad J_3 = (\,0\,),$$

deci

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

ii) Avem

$$f(x_1, x_2, x_3, x_4, x_5, x_6) = (x_2, 2x_4, x_6, 0, 0, 0),$$
$$f^2(x_1, x_2, x_3, x_4, x_5, x_6) = f(x_2, 2x_4, x_6, 0, 0, 0) = (2x_4, 0, 0, 0, 0, 0),$$
$$f^3(x_1, x_2, x_3, x_4, x_5, x_6) = (0, 0, 0, 0, 0, 0),$$

$$f - 0 \cdot 1_{\mathbb{R}^6} = f,\ (f - 0 \cdot 1_{\mathbb{R}^6})^2 = f^2,\ (f - 0 \cdot 1_{\mathbb{R}^6})^3 = f^3.$$

Deci

$$V(0) = \mathrm{Ker}(f - 0 \cdot 1_{\mathbb{R}^6}) = \{(x_1, 0, x_3, 0, x_5, 0) \mid x_1, x_3, x_5 \in \mathbb{R}\},$$

$$\mathrm{Ker}(f - 0 \cdot 1_{\mathbb{R}^6})^2 = \{(x_1, x_2, x_3, 0, x_5, x_6) \mid x_1, x_2, x_3, x_5, x_6 \in \mathbb{R}\},$$

$$V_g(0) = \mathrm{Ker}(f - 0 \cdot 1_{\mathbb{R}^6})^3 = \mathbb{R}^3.$$

Folosind baza canonică a lui $\mathbb{R}^3 = V_g(0)$ vom construi o bază canonică alui f. Având în vedere schema de mai sus, baza Jordan va fi formată din trei cicluri date de coloanele schemei

$$\begin{array}{lll} \bullet\ f^2(v_1) & \bullet\ f(v_2) & \bullet\ v_3 \\ \bullet\ f(v_1) & \bullet\ v_2 & \\ \bullet\ v_1 & & \end{array}$$

unde

$$v_1 \in V_g(0) \setminus \mathrm{Ker}\, f^2,\ v_2 \notin \mathrm{Ker}\, f \text{ şi } v_2 \notin \langle v_1, f(v_1), f^2(v_1)\rangle,$$

iar v_3 este liniar independent de $f(v_2)$. Luând $v_1 = (0, 0, 0, 1, 0, 0) = e_4$ avem

$$v_1 \notin \mathrm{Ker}\, f^2,\ f(v_1) = (0, 2, 0, 0, 0, 0) = 2e_2 = v_1',\ f^2(v_1) = (2, 0, 0, 0, 0, 0) = 2e_1 = v_1''$$

de unde obţinem primul ciclu $c_1 = (v_1'', v_1', v_1)$. Luând $v_2 = (0, 0, 0, 0, 0, 1) = e_6$ avem

$$v_2 \notin Ker\, f,\ v_2 \notin \langle c_1\rangle,\ f(v_2) = (0, 0, 1, 0, 0, 0) = e_3 = v_2'$$

de unde obţinem al doilea ciclu $c_2 = (v_2', v_2)$. În final putem lua $v_3 = e_5$ şi obţinem $c_3 = (\ v_3\ )$. Reunind cele trei cicluri, obţinem baza Jordan

$$v = (v_1'', v_1', v_1, v_2', v_2, v_3).$$

Menţionăm că $J = S^{-1}AS$, unde

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

este matricea de trecere de la baza e la baza v.

6.152. Polinomul caracteristic al lui A este

$$p_A = \det(A - \lambda I_4) = (a - X)^4.$$

Deci A are o singură valoare proprie cu multiplicitatea $m = 4$. Avem

$$A - aI_4 = \begin{pmatrix} 0 & a & a & a \\ 0 & 0 & a & a \\ 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 \end{pmatrix} = A_1,\ r_1 = 4 - \mathrm{rang}\, A_1 = 4 - 3 = 1,$$

de unde rezultă că valorii proprii a îi corespunde un singur bloc în forma canonică Jordan J a lui A. Întrucât a este singura valoare proprie, rezultă că J coincide cu acest bloc, care are schema

$$\begin{array}{c}\bullet\\ \bullet\\ \bullet\\ \bullet\end{array}$$

Deci

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

Altă soluţie: Prezentăm în continuare o altă metodă pentru determinarea formei canonice Jordan a unei matrici $A \in M_n(K)$, apoi o vom ilustra folosind matricea din enunţ. Această metodă este comodă întrucât se bazează pe efectuarea de transformări elementare asupra matricei $A - XI_n \in M_n(K[X])$. Menţionăm, însă, că avantajul metodei prezentate anterior constă în faptul că dacă A este matricea unui endomorfism f atunci odată cu obţinerea formei canonice Jordan se obţine şi o bază canonică Jordan pentru f. Numim transformări elementare asupra unei matrice $A' \in M_n(K[X])$ înmulţirea elementelor unei linii (coloane) cu un element nenul din K, adunarea la o linie (coloană) a altei linii (coloane) înmulţite cu un polinom şi permutatea a două linii (coloane) ale matricii. Matricile obţinute prin transformări elementare din A' sunt echivalente cu A'. Prin transformări elementare, matricea A' poate fi adusă la o formă diagonală în care elementele de pe diagonală divid fiecare pe cel care îi urmează (înspre dreapta-jos) în felul următor: între toate matricele echivalente cu A', alegem pe cea care are în colţul stânga-sus polinomul nenul de grad cel mai mic dintre toate polinomele care sunt elemente în toate matricile echivalente cu A'; acest polinom divide toate elementele din prima linie şi prima coloană, prin urmare, putem forma elemente nule pe prima linie şi prima coloană; se consideră apoi submatricea rezultată prin eliminarea primei linii şi primei coloane, cu care se procedează analog, ş.a.m.d. Matricea astfel obţinută se numeşte *forma diagonală canonică.* Fie $r = \operatorname{rang} A'$ şi

$$\begin{pmatrix} d_{11} & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & d_{22} & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & d_{rr} & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

forma diagonală canonică a matricei A'. Avem $d_{11}|d_{22}$, $d_{22}|d_{33}$,..., $d_{r-1\,r-1}|d_{rr}$. Polinoamele $I_{r-k} = d_{kk}$ $(1 \leq k \leq r)$ se numesc *factorii invarianţi* ai lui A', iar puterile maxime ale polinoamelor ireductibile care apar în descompunerea fiecărui factor invariant se numesc *divizori elementari* ai lui A'. Pentru a determina forma canonică Jordan a unei matrici A se procedează astfel:

i) se calculează valorile proprii ale lui A;

ii) se determină divizorii elementari ai matricei $A' = A - XI_n$;

iii) dacă λ e valoare proprie şi $(X-\lambda)^{k_1}$,...,$(X-\lambda)^{k_l}$ sunt divizorii elementari asociaţi lui λ atunci în forma canonică Jordan J vor apărea blocurile Jordan

$$J_{k_i}(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & \lambda \end{pmatrix} \in M_{k_i}(K),\ (i=1,\dots,l).$$

Matricea J este suma directă a tuturor blocurilor astfel obţinute. În cazul nostru,

$$A' = A - XI_4 = \begin{pmatrix} a-X & a & a & a \\ 0 & a-X & a & a \\ 0 & 0 & a-X & a \\ 0 & 0 & 0 & a-X \end{pmatrix}.$$

Schimarea primelor două coloane aduce în colţul stânga-sus pe a care este polinom de grad 0 şi care divide toate elementele din linia şi coloana sa. Prin urmare, avem

$$A' \sim \begin{pmatrix} a & a-X & a & a \\ a-X & 0 & a & a \\ 0 & 0 & a-X & a \\ 0 & 0 & 0 & a-X \end{pmatrix} \sim \begin{pmatrix} a & a(a-X) & a & a \\ a-X & 0 & a & a \\ 0 & 0 & a-X & a \\ 0 & 0 & 0 & a-X \end{pmatrix}$$

(s-a înmulţit coloana 2 cu $a \in \mathbb{R}^*$). Efectuăm transformări elementare asupra coloanelor matricei obţinute pentru a obţine elemente nule în prima linie şi obţinem matricea

$$\begin{pmatrix} a & 0 & 0 & 0 \\ a-X & -(a-X)^2 & X & X \\ 0 & 0 & a-X & a \\ 0 & 0 & 0 & a-X \end{pmatrix}.$$

Efectuăm transformări elementare asupra liniilor matricei obţinute pentru a obţine elemente nule în prima coloană şi obţinem matricea

$$\begin{pmatrix} a & 0 & 0 & 0 \\ 0 & -(a-X)^2 & X & X \\ 0 & 0 & a-X & a \\ 0 & 0 & 0 & a-X \end{pmatrix}.$$

Permutând liniile 2 şi 3, iar apoi coloanele 2 şi 4, în poziţia (2,2) va ajunge polinomul a de grad 0, care divide toate elementele din linia şi coloana sa. Cu matricea obţinută procedăm ca mai sus şi obţinem succesiv:

$$A' \sim \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & a & a-X & 0 \\ 0 & X & X & -(a-X)^2 \\ 0 & a-X & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & a & a(a-X) & 0 \\ 0 & X & aX & -(a-X)^2 \\ 0 & a-X & 0 & 0 \end{pmatrix}$$

$$\sim \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & X & X^2 & -(a-X)^2 \\ 0 & a-X & -(a-X)^2 & 0 \end{pmatrix} \sim \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & X^2 & -(a-X)^2 \\ 0 & 0 & -(a-X)^2 & 0 \end{pmatrix}$$

$$\stackrel{c_4+c_3}{\sim}\begin{pmatrix} a & 0 & 0 & 0\\ 0 & a & 0 & 0\\ 0 & 0 & X^2 & -a^2+2aX\\ 0 & 0 & -a^2+2aX-X^2 & -a^2+2aX-X^2 \end{pmatrix}$$

Din terorema împărţirii cu rest în $\mathbb{R}[X]$ avem

$$-X^2+2aX-a^2=(2aX-a^2)\left(-\frac{1}{2a}X+\frac{3}{4}\right)-\frac{a^2}{4}.$$

Rezultă că scăzând din linia 4 linia 3 înmulţită cu $\frac{1}{2a}X+\frac{3}{4}$ şi înmulţind apoi linia 4 cu $4a$ avem

$$A'\sim\begin{pmatrix} a & 0 & 0 & 0\\ 0 & a & 0 & 0\\ 0 & 0 & X^2 & -a^2+2aX\\ 0 & 0 & 2X^3-7aX^2+8a^2X-4a^3 & -a^3 \end{pmatrix}$$

Înmulţim coloana 4 cu $-\frac{1}{a}$, în matricea rezultată înmulţim linia 3 cu a^2 şi permutăm coloanele 3 şi 4 apoi liniile 3 şi 4 şi avem

$$A'\sim\begin{pmatrix} a & 0 & 0 & 0\\ 0 & a & 0 & 0\\ 0 & 0 & a^2 & 2X^3-7aX^2+8a^2X-4a^3\\ 0 & 0 & a^2(a-2X) & a^2X^2 \end{pmatrix}$$

$$\stackrel{l_4-(a-2X)l_3}{\sim}\begin{pmatrix} a & 0 & 0 & 0\\ 0 & a & 0 & 0\\ 0 & 0 & a^2 & 2X^3-7aX^2+8a^2X-4a^3\\ 0 & 0 & 0 & a^2X^2-(a-2X)(2X^3-7aX^2+8a^2X-4a^3) \end{pmatrix}$$

$$\sim\begin{pmatrix} a & 0 & 0 & 0\\ 0 & a & 0 & 0\\ 0 & 0 & a^2 & 0\\ 0 & 0 & 0 & 4(a-X)^4 \end{pmatrix}\sim\begin{pmatrix} a & 0 & 0 & 0\\ 0 & a & 0 & 0\\ 0 & 0 & a & 0\\ 0 & 0 & 0 & (a-X)^4 \end{pmatrix}$$

Rezultă că $\lambda=a$ este singura valoare proprie a lui A şi avem un singur divizor elementar şi anume $(a-X)^4$ căruia îi corespunde un singur bloc Jordan care coincide cu forma canonică Jordan

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

6.153. Matricele similare au acelaşi polinom caracteristic, deci aceeaşi urmă şi acelaşi determinant. Urmele acestor matrice sunt $\operatorname{Tr}A=5=\operatorname{Tr}B=\operatorname{Tr}C$, $\operatorname{Tr}D=3$. Rezultă că D nu este similară cu niciuna dintre matricile A,B,C. Determinanţii matricelor A, B şi C sunt $\det A=4=\det B=\det C$ şi polinoamele lor caracteristice sunt $p_A=-(X-1)(X-2)^2=p_B=p_C$, prin urmare A,B,C pot fi similare. Pentru a stabili dacă sunt sau nu similare, se determină forma canonică

Jordan pentru fiecare dintre cele trei matrici, respectiv J_A, J_B, J_C. Întrucât $\lambda_1 = 1$ este rădăcină simplă, blocul corespunzător lui λ_1 în J_A, J_B, J_C este $(\,1\,)$. Determinăm blocurile corespunzătoare rădăcinii duble $\lambda_2 = 2$. Avem

$$A - 2I_3 = \begin{pmatrix} -5 & 3 & -2 \\ -7 & 4 & -3 \\ 1 & -1 & 0 \end{pmatrix}, \; B - 2I_3 = \begin{pmatrix} -2 & 1 & -1 \\ -4 & 2 & -2 \\ -2 & 1 & -1 \end{pmatrix},$$

$$C - 2I_3 = \begin{pmatrix} -2 & -1 & -1 \\ -3 & -3 & -2 \\ 7 & 5 & 4 \end{pmatrix},$$

$$3 - \text{rang}(A - 2I_3) = 3 - \text{rang}(C - 2I_3) = 1, \; 3 - \text{rang}(B - 2I_3) = 2.$$

Rezultă că lui $\lambda_2 = 2$ îi corespunde în J_A şi J_C un singur bloc, $\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$, iar în J_C două blocuri, $(\,2\,)$ şi $(\,2\,)$. Prin urmare, avem

$$J_A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}, \; J_B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \; J_C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix},$$

adică $J_A = J_C \neq J_B$, de unde deducem că A este similară cu C, iar B nu este similară nici cu A, nici cu C.

6.154. Răspuns.

a) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1 \end{pmatrix}$, b) $\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix}$, c) $\begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$, d) $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Capitolul 7

Corpuri comutative. Teoria lui Galois

7.1. Răspuns. Orice număr $a \in \mathbb{Q}$ este algebric pentru că este rădăcină a apolinomului nenul $f = X - a \in \mathbb{Q}[X]$. Numerele iraţionale $\sqrt[n]{2}$, $\sqrt[n]{3}$ cu $n \in \mathbb{N}$, $n \geq 2$ sunt algebrice pentu că $f_n = X^n - 2 \in \mathbb{Q}[X]^*$, $g_n = X^n - 3 \in \mathbb{Q}[X]^*$ şi $f_n(\sqrt[n]{2}) = 0 = g_n(\sqrt[n]{3})$. Polinoamele f, f_n, g_n sunt ireductibile peste $\mathbb{Q}$ (ireductibilitatea lui f_n şi g_n se poate stabili cu criteriul lui Eisenstein). Deci f, respectiv f_n, g_n este polinomul minimal al lui a, respectiv $\sqrt[n]{2}$, $\sqrt[n]{3}$. Numerele e^n, π^n cu $n \in \mathbb{N}^*$ sunt trancendente. Justificarea acestei afirmaţii în cazul $n = 1$ necesită mijloace analitice.

7.2. Indicaţie. Fie A mulţimea numerelor algebrice. Din $i^2 + 1 = 0$ rezultă $i \in A$, ceea ce, împreună cu $\mathbb{Q} \subseteq A$ şi cu faptul că A este subcorp al lui $\mathbb{C}$ implică $a + bi \in A$ pentru orice $a, b \in \mathbb{Q}$, adică $\mathbb{Q}(i) \subseteq A$. Această incluziune rezultă şi din faptul că extinderea $\mathbb{Q} \leq \mathbb{Q}(i)$ este finită, deci algebrică. Numerele de forma $\pi + ai$, $a + \pi i$, cu $a \in \mathbb{Q}$, sunt transcendente pentru că din apartenenţa lor la A ar rezulta $\pi \in A$, ceea ce este fals.

7.3. Indicaţie. Avem $1 + \pi,\ 1 - \pi,\ \dfrac{1}{1+\pi} \in T$ dar $(1 + \pi) + (1 - \pi) = 2 \notin T$ şi $(1 + \pi) \cdot \dfrac{1}{1+\pi} = 1 \notin T$.

7.4. Fie A mulţimea numerelor algebrice şi $\overline{z} = a - bi$. Din $z \in A$ rezultă că există $f \in \mathbb{Q}[X]$, $f \neq 0$ astfel încât $f(z) = 0$, ceea ce implică $f(\overline{z}) = 0$, adică $\overline{z} \in A$. Din $z, \overline{z}, i \in A$ şi din faptul că A este un subcorp al lui $\mathbb{C}$ rezultă că $\dfrac{z + \overline{z}}{2} = a \in A$ şi $\dfrac{z - \overline{z}}{2i} = b \in A$. Invers, din $a, b, i \in A$ deducem $a + bi \in A$.

7.5. Folosind incluziunea $K \subseteq A$ şi faptul că A este un subcorp al lui K', se deduc imediat implicaţiile

$$u \in A \Rightarrow u + a \in A \text{ şi } u \in A \Rightarrow u^2 \in A.$$

Reciproc, dacă $u + a \in A$ atunci există $h \in K[X]^*$ astfel încât $h(u + a) = 0$, de unde deducem că u este o rădăcină a polinomului $g = h(X + a) \in K[X]^*$, aşadar $u \in A$. Dacă $u^2 \in A$ atunci există $p \in K[X]^*$ astfel încât $p(u^2) = 0$, prin urmare u este o rădăcină a polinomului $q = p(X^2) \in K[X]^*$ deci $u \in A$.

Partea a doua este o generalizare a primei părţi a problemei. Din $K \subseteq A$ şi A subcorp în K', se deduce că $u \in A$ implică $f(u) \in A$. Invers, din $f(u) \in A$ urmează că există $g \in K[X]^*$ astfel încât $g(f(u)) = 0$. Luând $h = g(f(X)) \in K[X]$ avem $\operatorname{grad} h = (\operatorname{grad} f)^{\operatorname{grad} g} \geq 1$ şi $h(u) = 0$ ceea ce arată că $u \in A$.

7.6. Indicaţie. Se foloseşte problema anterioară.

7.7. Soluţia 1. Folosind definiţia subcorpului generat, avem

$$\sqrt{2} + i\sqrt{3} - \sqrt{2} = i\sqrt{3} \in \mathbb{R}(\sqrt{2} + i\sqrt{3}) \Rightarrow \frac{i\sqrt{3}}{\sqrt{3}} = i \in \mathbb{R}(\sqrt{2} + i\sqrt{3}),$$

prin urmare

$$\mathbb{R} \cup \{i\} \subseteq \mathbb{R}(\sqrt{2} + i\sqrt{3}) \Rightarrow \mathbb{C} \subseteq \mathbb{R}(\sqrt{2} + i\sqrt{3}) \Rightarrow \mathbb{C} = \mathbb{R}(\sqrt{2} + i\sqrt{3}).$$

Rezultă imediat că subcorpul prim al lui $\mathbb{R}(\sqrt{2} + i\sqrt{3})$ este $P(\mathbb{C}) = \mathbb{Q}$.
Soluţia 2. Conform problemei **7.4**, numărul $\sqrt{2}+i\sqrt{3}$ este algebric. Un polinom cu coeficienţi reali care are ca rădăcină pe $\sqrt{2}+i\sqrt{3}$ va avea ca rădăcină şi pe $\sqrt{2}-i\sqrt{3}$, prin urmare se divide cu polinomul

$$f = [X - (\sqrt{2} + i\sqrt{3})][X - (\sqrt{2} - i\sqrt{3})] = X^2 - 2\sqrt{2}X - 1 \in \mathbb{R}[X].$$

Rezultă imediat că polinomul miniml al lui $\sqrt{2} + i\sqrt{3}$ peste $\mathbb{R}$ este f, că gradul extinderii $\mathbb{R} \leq \mathbb{R}(\sqrt{2} + i\sqrt{3})$ este 2 şi că $\{1, \sqrt{2} + i\sqrt{3}\}$ este o bază a $\mathbb{R}$-spaţiului vectorial $\mathbb{R}(\sqrt{2} + i\sqrt{3})$. Aşadar,

$$\mathbb{R}(\sqrt{2} + i\sqrt{3}) = \{a + b(\sqrt{2} + i\sqrt{3}) \mid a, b \in \mathbb{R}\} = \{(a + b\sqrt{2}) + ib\sqrt{3}\} \mid a, b \in \mathbb{R}\},$$

iar cum orice $z = x + yi \in \mathbb{C}$ $(x, y \in \mathbb{R})$ poate fi scris sub forma $(a + b\sqrt{2}) + ib\sqrt{3}$, cu $a = x - \dfrac{y\sqrt{2}}{\sqrt{3}} \in \mathbb{R}$ şi $b = \dfrac{y}{\sqrt{3}} \in \mathbb{R}$, avem $\mathbb{R}(\sqrt{2} + i\sqrt{3}) = \mathbb{C}$.

7.8. Indicaţie. Se foloseşte definiţia subcorpului generat. Având în vedere că $\mathbb{C} = \mathbb{R}(i)$, rezolvarea acestei probleme se obţine prin generalizarea **Soluţiei 1** a problemei anterioare.

7.9. Indicaţie. Un polinom cu coeficienţi raţionali care are ca rădăcină pe $1 + \sqrt{2}$ are ca rădăcină şi pe $1 - \sqrt{2}$, prin urmare polinomul minimal al lui $1 + \sqrt{2}$ peste $\mathbb{Q}$ este $f = [X - (1 + \sqrt{2})][X - (1 - \sqrt{2})] = X^2 - 2X - 1 \in \mathbb{Q}[X]$.

7.10. Indicaţie. Fie $\alpha_1 = \sqrt{2} + \sqrt{3}$, $\alpha_2 = \sqrt{2} - \sqrt{3}$, $\alpha_3 = -\sqrt{2} + \sqrt{3}$, $\alpha_4 = -\sqrt{2} - \sqrt{3}$. Polinomul $f = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)(X - \alpha_4) = X^4 - 10X^2 + 1$ este ireductibil peste $\mathbb{Q}$ deoarece nu are rădăcini raţionale, iar dacă scriem $f = gh$ cu $\operatorname{grad} g = \operatorname{grad} h = 2$ atunci polinoamele g, h sunt de forma $a(X - \alpha_i)(X - \alpha_j)$ $(a \in \mathbb{Q}^*,\ i, j \in \{1, 2, 3, 4\},\ i \neq j)$ prin urmare $g, h \notin \mathbb{Q}[X]$. Se deduce că f este polinomul minimal al lui α_1 peste $\mathbb{Q}$.

Observaţie: Faptul că $\sqrt{2} + \sqrt{3}$ este algebric se poate deduce şi astfel:

$$x = \sqrt{2} + \sqrt{3} \Rightarrow x^2 - 2\sqrt{2}x + 2 = 0 \Rightarrow x^2 - 1 = 2\sqrt{2}x \Rightarrow x^4 - 10x + 1 = 0$$

sau deducând că $\sqrt{2}$ şi $\sqrt{3}$ sunt algebrice şi folosind faptul că numerele algebrice formează un subcorp al lui $\mathbb{C}$.

7.11. Polinoamele $f = X^2 - 2$ şi $g = X^3 - 2$ (din $\mathbb{Q}[X]$) sunt ireductibile peste $\mathbb{Q}$ pentru că $\operatorname{grad} f = 2$, $\operatorname{grad} g = 3$ şi f, g nu au rădăcini în $\mathbb{Q}$. Întrucât $f(\sqrt{2}) = 0$ şi $g(\sqrt[3]{2}) = 0$, iar coeficienţii termenilor de grad maxim din f şi g sunt 1, rezultă că f, respectiv g, este polinomul minimal al lui $\sqrt{2}$, respectiv $\sqrt[3]{2}$. Prin urmare,

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2, \ [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

şi $\{1, \sqrt{2}\}$, respectiv $\left\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\right\}$ este o bază a $\mathbb{Q}$-spaţiului vectorial $\mathbb{Q}(\sqrt{2})$, respectiv $\mathbb{Q}(\sqrt[3]{2})$. Rezultă că

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \text{ şi } \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}.$$

Din $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2})$ şi $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2})$ şi din faptul că $\mathbb{Q}$ este un corp prim se deduce că $P(\mathbb{Q}(\sqrt{2})) = \mathbb{Q} = P(\mathbb{Q}(\sqrt[3]{2}))$.

7.12. Răspuns. Fie $d \in \{2, 3\}$. Avem

$$\mathbb{Q}(\sqrt[n]{d}) = \left\{a_0 + a_1\sqrt[n]{d} + \cdots + a_{n-1}(\sqrt[n]{d})^{n-1} \mid a_i \in \mathbb{Q},\ i \in \{0, \ldots, n-1\}\right\}.$$

7.13. Indicaţie. Se poate folosi problema anterioară.

7.14. Indicaţie. $K = \mathbb{Q}(\sqrt[n]{2})$.

7.15. Întrucât orice $z \in \mathbb{C}$ se scrie în mod unic sub forma $z = a + bi$, $a, b \in \mathbb{R}$, rezultă că $\{1, i\}$ este o bază a lui $\mathbb{C}$ în $\mathbb{R}$. Deci $[\mathbb{C} : \mathbb{R}] = 2$. Extinderea $\mathbb{R} \leq \mathbb{C}$ fiind finită, este şi algebrică, adică orice $z \in \mathbb{C}$ este algebric peste $\mathbb{R}$. Dacă $z = a + bi$, $a, b \in \mathbb{R}$, $b \neq 0$, $\overline{z} = a - bi$ atunci din $f \in \mathbb{R}[X]^*$ şi $f(z) = 0$ rezultă $f(\overline{z}) = 0$, de unde deducem că $(X - z)(X - \overline{z}) = X^2 - 2aX + a^2 + b^2 \in \mathbb{R}[X]$ este polinomul mininal al lui z peste $\mathbb{R}$. Deci $[\mathbb{R}(z) : \mathbb{R}] = 2$, $\mathbb{R}(z) \leq C$, ceea ce împreună cu $[\mathbb{C} : \mathbb{R}] = 2$ implică $\mathbb{C} = \mathbb{R}(z)$

Observaţie: Egalitatea $\mathbb{R}(z) = \mathbb{C}$ se deduce şi din $\mathbb{R}(z) \subseteq \mathbb{C} = \mathbb{R}(i)$, $i = -\dfrac{a}{b} + \dfrac{1}{b}\, z \in \mathbb{R}(z)$.

7.16. Răspuns. $\mathbb{R}$ şi $\mathbb{C}$.

7.17. Indicaţie. Cum $\mathbb{Q}$ este subcorpul prim al lui $\mathbb{C}$ avem $\mathbb{Q} \subseteq K$. Deci $K = \mathbb{Q}(z)$. Pentru $b = 0$ avem $K = \mathbb{Q}$, iar pentru $b \neq 0$ se deduce $K = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$.

7.18. Indicaţii. Din soluţia problemei **7.11** rezultă că $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Subcorpul prim al lui $\mathbb{Q}(\sqrt{2})$ este $\mathbb{Q}$ şi $\mathbb{Q} \neq \mathbb{Q}(\sqrt{2})$. Prin urmare, subcorpul lui K generat de $u = a + b\sqrt{2}$ coincide cu subcorpul generat de $\mathbb{Q} \cup \{u\}$. Deci, pentru $b = 0$ avem $K = \mathbb{Q}(a) = \mathbb{Q}$, iar dacă $b \neq 0$ atunci $K = \mathbb{Q}(u) \subseteq \mathbb{Q}(\sqrt{2})$ şi $\sqrt{2} = -\dfrac{a}{b} + \dfrac{1}{b}\, u$, ceea ce implică $K = \mathbb{Q}(\sqrt{2})$. Astfel, am arătat că un număr $u \in \mathbb{Q}(\sqrt{2})$ generează corpul $\mathbb{Q}(\sqrt{2})$ dacă şi numai dacă $u \in \mathbb{Q}(\sqrt{2}) \setminus \mathbb{Q}$. Această concluzie se poate deduce şi din faptul că $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

7.19. Elementul $\sqrt{2} \in \mathbb{Q}(i, \sqrt{2})$ este element algebric peste $\mathbb{Q}$ cu polinomul minimal $f = X^2 - 2$, iar elementul $i \in \mathbb{Q}(i, \sqrt{2})$ este algebric peste $\mathbb{Q}(\sqrt{2})$ cu polinomul minimal $g = X^2 + 1$ (ireductibilitatea lui g peste $\mathbb{Q}(\sqrt{2})$ este o consecinţă a ireductibilităţii lui g peste $\mathbb{R}$). Prin urmare

$$[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4.$$

Mai mult, 1, $\sqrt{2}$ formează o bază a lui $\mathbb{Q}(\sqrt{2})$ peste $\mathbb{Q}$ şi 1, i formează o bază a lui $\mathbb{Q}(i, \sqrt{2})$ peste $\mathbb{Q}(\sqrt{2})$, de unde, înmulţind aceste baze termen cu termen, deducem că o bază a lui $\mathbb{Q}(i, \sqrt{2})$ peste $\mathbb{Q}$ este formată din 1, $\sqrt{2}$, i şi $i\sqrt{2}$. Deci

$$\mathbb{Q}(i, \sqrt{2}) = \{a + b\sqrt{2} + ci + di\sqrt{2} \mid a, b, c, d \in \mathbb{Q}\}.$$

7.20. 1) Din $u \in K' \setminus K$ rezultă $K(u) \neq K$, ceea ce implică $[K(u) : K] > 1$, iar din $K < K(u) \leq K'$ urmează $[K' : K] = [K' : K(u)] \cdot [K(u) : K]$, ceea ce, având în vedere că numărul $[K' : K]$ este prim, implică $[K' : K(u)] = 1$, de unde deducem $K' = K(u)$.
2) Din 1) şi din faptul că în acest caz K este subcorpul prim al lui K' rezultă că subcorpul generat de $K \cup \{u\}$, adică $K(u)$, coincide cu subcorpul generat de u.

7.21. Din punctul 2) al problemei anterioare rezultă că subcorpurile lui K' sunt K şi K'.

7.22. Avem

$$u = 2 + \sqrt{3} \Rightarrow (u - 2)^2 = 3 \Rightarrow u^2 - 4u - 1 = 0,$$
$$v = \sqrt[4]{5} + \sqrt{5} \Rightarrow (v - \sqrt{5})^2 = \sqrt{5} \Rightarrow v^2 - 2v\sqrt{5} + 5 = \sqrt{5} \Rightarrow v^2 + 5 = (2v + 1)\sqrt{5}$$
$$\Rightarrow v^4 + 10v^2 + 25 = 20v^2 + 20v + 5 \Rightarrow v^4 - 10v^2 - 20v + 20 = 0,$$

$$w = \sqrt[3]{2} + \sqrt[3]{4} \Rightarrow w^3 = 2 + 3\sqrt[3]{2} \cdot \sqrt[3]{4}(\sqrt[3]{2} + \sqrt[3]{4}) + 4 \Rightarrow w^3 = 6 + 6w \Rightarrow w^3 - 6w - 6 = 0,$$

ceea ce ne arată că $f(u) = 0$, $g(v) = 0$ şi $h(w) = 0$, unde $f = X^2 - 4X - 1 \in \mathbb{Q}[X]$, $g = X^4 - 10X^2 - 20X + 20 \in \mathbb{Q}[X]$ şi $h = X^3 - 6X - 6 \in \mathbb{Q}[X]$. Aşadar, numerele u, v, w sunt algebrice — ceea ce se poate deduce şi din faptul că termenii lui u, v şi w sunt numere algebrice şi mulţimea numerelor algebrice formează subcorp în $\mathbb{C}$. Din $\operatorname{grad} f = 2$, $\operatorname{grad} h = 3$ şi din faptul că f şi h nu au rădăcini în $\mathbb{Q}$ rezultă că f şi h sunt ireductibile peste $\mathbb{Q}$. Ireductibilitatea lui g se deduce din criteriul lui Eisenstein luând $p = 5$. Menţionăm că şi ireductibilitatea lui h se poate deduce folosind criteriul lui Eisenstein. Prin urmare, f, respectiv g şi h sunt polinoamele minimale ale lui u, respectiv v şi w peste $\mathbb{Q}$. Rezultă că extinderile $Q \leq \mathbb{Q}(u)$, $\mathbb{Q} \leq \mathbb{Q}(v)$, $\mathbb{Q} \leq \mathbb{Q}(w)$ au gradele 2, respectiv 4 şi 3 şi că $\{1, u\}$, respectiv $\{1, v, v^2, v^3\}$, $\{1, w, w^2\}$ sunt baze ale $\mathbb{Q}$-spaţiilor vectoriale $\mathbb{Q}(u)$, respectiv $\mathbb{Q}(v)$ şi $\mathbb{Q}(w)$. Deci,

$$\mathbb{Q}(u) = \{a + bu \mid a, b \in \mathbb{Q}\} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2}),$$
$$\mathbb{Q}(v) = \{a + bv + cv^2 + dv^3 \mid a, b, c, d \in \mathbb{Q}\},\ \mathbb{Q}(w) = \{a + bw + cw^2 \mid a, b, c \in \mathbb{Q}\}.$$

7.23. Indicaţie. $\sqrt{\dfrac{3}{2}} = \dfrac{1}{2}\sqrt{6}$.

7.24. Indicaţie. Această problemă generalizează problema anterioară. Dacă $u = \dfrac{p}{q}$, $p, q \in \mathbb{Z}$, $q \neq 0$ atunci $q\sqrt{u} = \sqrt{pq}$, iar pq se poate scrie $pq = a^2 d$, unde $a \in \mathbb{N}^*$ şi $d \in \mathbb{Z} \setminus \{1\}$ este liber de pătrate. Rezultă $\dfrac{q}{a}\sqrt{u} = \sqrt{d}$.

7.25. Dacă $d \in \mathbb{Z} \setminus \{1\}$ este liber de pătrate atunci $\sqrt{d}$ este un număr algebric şi $f = X^2 - d$ este polinomul său minimal. Rezultă că extinderea $\mathbb{Q} \leq \mathbb{Q}(\sqrt{d})$ are gradul 2 şi $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$. Presupunem că extinderea $\mathbb{Q} \leq K$ are gradul 2. Rezultă că pentru orice $u \in K \setminus \mathbb{Q}$ elementele $1, u$ formează o bază a lui K peste $\mathbb{Q}$, de unde urmează $K = \mathbb{Q}(u)$ şi că există $a, b \in \mathbb{Q}$ astfel încât $u^2 = a + bu$, ceea ce implică $\left(u - \frac{b}{2}\right)^2 = a - \frac{b^2}{4}$. Notând $v = u - \frac{b}{2}$, avem $\mathbb{Q}(v) = \mathbb{Q}(u) = K$. Mai mult, $v \notin \mathbb{Q}$ este rădăcină a unui polinom de forma $X^2 - a$, cu $a \in \mathbb{Q}$ şi, desigur, $\sqrt{a} \notin \mathbb{Q}$. Prin urmare $\mathbb{Q}(u) = \mathbb{Q}(v) = \mathbb{Q}(\sqrt{a})$ şi aplicând problema anterioară obţinem existenţa unui întreg liber de pătrate d pentru care $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{d})$. Deci, $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{d})$.

7.26. Indicaţie. Fie $0'$ şi $1'$ elementul zero, respectiv elementul unitate din P. Avem $P = \{(m \cdot 1')(n \cdot 1')^{-1} \mid m, n \in \mathbb{Z},\ n \cdot 1' \neq 0'\}$.

7.27. Presupunem că există un izomorfism de corpuri $f : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$. Din problema anterioară rezultă că $f(x) = x$ pentru orice $x \in \mathbb{Q}$. Din $f(\sqrt{2}) \in \mathbb{Q}(\sqrt{3})$ rezultă $f(\sqrt{2}) = a + b\sqrt{3} \neq 0$ $(a, b \in \mathbb{Q})$, de unde, prin ridicare la pătrat, se obţine

$$2 = a^2 + 3b^2 + 2ab\sqrt{3},$$

ceea ce, împreună cu faptul că $\sqrt{3}$ este iraţional, implică $a = 0$ sau $b = 0$. Primul caz ne conduce la absurditata $\sqrt{\frac{2}{3}} \in \mathbb{Q}$, iar al doilea la absuditatea $\sqrt{2} \in \mathbb{Q}$.

7.28. Dacă $f : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d'})$ este un izomorfism atunci, ca în problema anterioară se deduce că $f(x) = x$ pentru orice $x \in \mathbb{Q}$. Din $f(\sqrt{d}) \in \mathbb{Q}(\sqrt{d'})$ rezultă $f(\sqrt{d}) = a + b\sqrt{d'} \neq 0$ $(a, b \in \mathbb{Q})$, de unde, prin ridicare la pătrat, se obţine

$$d = a^2 + d'b^2 + 2ab\sqrt{d'},$$

ceea ce, împreună cu $\sqrt{d'} \in \mathbb{C} \setminus \mathbb{Q}$, implică $a = 0$ sau $b = 0$. Din $b = 0$ se deduce absurditatea $\sqrt{d} \in \mathbb{Q}$. Deci $b \neq 0$ şi $a = 0$ ceea ce implică $d = b^2 d'$, de unde urmează $\frac{d}{d'} = b^2$. De aici şi din faptul că d şi d' sunt întregi liberi de pătrate rezultă $d = d'$. Implicaţia inversă este o urmare a faptului că aplicaţia identică $1_{\mathbb{Q}(\sqrt{d})}$ este izomorfism.

7.29. Indicaţii. Dacă $f : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$ este un automorfism atunci $f(x) = x$ pentru orice $x \in \mathbb{Q}$. Din $d = f(d) = f(\sqrt{d} \cdot \sqrt{d}) = [f(\sqrt{d})]^2$ rezultă $f(\sqrt{d}) \in \{-\sqrt{d}, \sqrt{d}\}$. Deci $f \in \{f_1, f_2\}$, unde $f_1(a + b\sqrt{d}) = a + b\sqrt{d}$ şi $f_2(a + b\sqrt{d}) = a - b\sqrt{d}$. Evident $f_1 = 1_{\mathbb{Q}(\sqrt{d})}$ este automorfism. Se verifică cu uşurinţă că şi f_2 este automorfism. Prin urmare, $Aut(\mathbb{Q}(\sqrt{d})) = \{f_1, f_2\}$.

7.30. Indicaţie. Polinomul minimal al elementului $\sqrt[4]{2}$ este $f = X^4 - 2$ şi are rădăcinile $\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$. Subcorpul $K = \mathbb{Q}(i\sqrt[4]{2})$ al lui $\mathbb{C}$ nu este inclus în $\mathbb{R}$ şi

$$\mathbb{Q}(\sqrt[4]{2}) \simeq \mathbb{Q}[X]/(f) \simeq K.$$

7.31. Răspuns. $\mathbb{Q}(\varepsilon\sqrt[3]{2})$, unde ε este o rădăcină a lui $X^3 - 1$ diferită de 1.

7.32. Indicaţii. a) Ca în soluţia problemei **7.19** deducem că $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = 4$ şi că $\{1, \sqrt{3}, i, i\sqrt{3}\}$ este o bază a lui $\mathbb{Q}(\sqrt{3}, i)$ peste $\mathbb{Q}$.
c) Din $\sqrt{18} = 3\sqrt{2} = 3(\sqrt[4]{2})^2 \in \mathbb{Q}(\sqrt[4]{2})$ urmează $\mathbb{Q}(\sqrt{18}, \sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2})$. Din criteriul lui Eisenstein rezultă că polinomul $f = X^4 - 2$ este ireductibil peste $\mathbb{Q}$, ceea ce, împreună cu $f(\sqrt[4]{2}) = 0$, ne arată că f este polinomul minimal al lui $\sqrt[4]{2}$. Deci $[Q(\sqrt{18}, \sqrt[4]{2}) : \mathbb{Q}] = 4$ şi $\{1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}\}$ este o bază a extinderii $\mathbb{Q} \leq \mathbb{Q}(\sqrt{18}, \sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2})$.
d) Extinderea $\mathbb{Q} \leq \mathbb{Q}(\sqrt{3}, i\sqrt{5}, \sqrt{7})$ poate fi realizată astfel:

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{3}) \leq \mathbb{Q}(\sqrt{3}, \sqrt{7}) \leq \mathbb{Q}(\sqrt{3}, \sqrt{7}, i\sqrt{5}),$$

de unde rezultă

$$[\mathbb{Q}(\sqrt{3}, i\sqrt{5}, \sqrt{7}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \cdot [\mathbb{Q}(\sqrt{3}, \sqrt{7}) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}, i\sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{3}, \sqrt{7})].$$

Determinăm gradele din membrul secund al acestei egalităţi. Din ireductibilitatea polinomului $f_1 = X^2 - 3$ peste $\mathbb{Q}$ şi din $f_1(\sqrt{3}) = 0$ urmează că f_1 este polinomul minimal al lui $\sqrt{3}$ peste $\mathbb{Q}$, că $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ şi că $\{1, \sqrt{3}\}$ este o bază a extinderii

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}.$$

Întrucât egalitatea $7 = (a + b\sqrt{3})^2$, $a, b \in \mathbb{Q}$ este imposibilă, rezultă că $f_2 = X^2 - 7$ este polinomul minimal al lui $\sqrt{7}$ peste $\mathbb{Q}(\sqrt{3})$, de unde deducem că $[\mathbb{Q}(\sqrt{3}, \sqrt{7}) : \mathbb{Q}(\sqrt{3})] = 2$ şi că $\{1, \sqrt{7}\}$ este o bază a extinderii $\mathbb{Q}(\sqrt{3}) \leq \mathbb{Q}(\sqrt{3}, \sqrt{7})$. Din ireductibilitatea polinomului $f_3 = X^2 + 5$ peste $\mathbb{R}$ urmează ireductibilitatea lui f_3 peste $\mathbb{Q}(\sqrt{3}, \sqrt{7})$, ceea ce, împreună cu $f_3(i\sqrt{5}) = 0$ arată că f_3 este polinomul minimal al lui $i\sqrt{5}$ peste $\mathbb{Q}(\sqrt{3}, \sqrt{7})$. Aşadar,

$$[\mathbb{Q}(\sqrt{3}, i\sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{3}, \sqrt{7})] = 2$$

şi $\{1, i\sqrt{5}\}$ este bază a extinderii $\mathbb{Q}(\sqrt{3}, \sqrt{7}) \leq \mathbb{Q}(\sqrt{3}, i\sqrt{5}, \sqrt{7})$. Din cele de mai sus obţinem $[\mathbb{Q}(\sqrt{3}, i\sqrt{5}, \sqrt{7}) : \mathbb{Q}] = 8$ şi că

$$\{1,\ \sqrt{3},\ \sqrt{3}\sqrt{7} = \sqrt{21},\ i\sqrt{5},\ i\sqrt{3}\sqrt{5} = i\sqrt{15},\ i\sqrt{5}\sqrt{7} = i\sqrt{35},\ i\sqrt{3},\ i\sqrt{3}\sqrt{5}\sqrt{7} = i\sqrt{105}\}$$

este o bază a extinderii $\mathbb{Q} \leq \mathbb{Q}(\sqrt{3}, i\sqrt{5}, \sqrt{7})$.

7.33. a) Din criteriul lui Eisenstein rezultă că f este ireductibil peste $\mathbb{Q}$. Deci $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ şi $1, \alpha, \alpha^2$ formează o bază a extinderii $\mathbb{Q} \leq \mathbb{Q}(\alpha)$.
b) Din $f(\alpha) = 0$ deducem că $\alpha^3 = 6\alpha^2 - 9\alpha - 3$ şi

$$\alpha^4 = 6\alpha^3 - 9\alpha^2 - 3\alpha = 6(6\alpha^2 - 9\alpha - 3) - 9\alpha^2 - 3\alpha = 27\alpha^2 - 57\alpha - 18.$$

Egalitatea de mai sus ne dă coordonatele lui α^4. Folosind acest rezultat şi $f(\alpha) = 0$ deducem coordonatele lui α^5:

$$\alpha^5 = 27\alpha^3 - 57\alpha^2 - 18\alpha = 27(6\alpha^2 - 9\alpha - 3) - 57\alpha^2 - 18 = 105\alpha^2 - 261\alpha - 81.$$

Folosind coordonatele lui α^4 şi α^5 obţinem coordonatele lui $3\alpha^5 - \alpha^4 + 2$:

$$3\alpha^5 - \alpha^4 + 2 = -288\alpha^2 - 762\alpha - 223.$$

Coordonatelel lui $\dfrac{1}{\alpha}$ se deduc din $f(\alpha) = 0$ astfel:

$$f(\alpha) = 0 \Rightarrow \alpha(\alpha^2 - 6\alpha + 9) = -3 \Rightarrow \frac{1}{\alpha} = -\frac{1}{3}\alpha^2 + 2\alpha - 3.$$

Coordonatele inversului unui element $a = a_2\alpha^2 + a_1\alpha + a_0 \in \mathbb{Q}(\alpha)^*$ se pot determina astfel: polinomul f fiind ireductibil, urmează că f este relativ prim cu polinomul $g = a_2X^2 + a_1X + a_0$, ceea ce implică existenţa a două polinoame $u, v \in \mathbb{Q}[X]$ astfel încât $uf + vg = 1$; rezultă $v(\alpha)g(\alpha) = 1$, ceea ce implică $a^{-1} = v(\alpha)$. Polinoamele u şi v se determină cu algoritmul lui Euclid. Folosind acest procedeu obţinem

$$f = (X + 1)(X^2 - 7X + 16) - 13$$

care, împreună cu $f(\alpha) = 0$, implică $(\alpha + 1)(\alpha^2 - 7\alpha + 16) = 13$, de unde rezultă

$$\frac{1}{\alpha + 1} = \frac{1}{13}\alpha^2 - \frac{7}{13}\alpha + \frac{16}{13}.$$

Prin împărţiri succesive avem:

	$X = q_1$	$X - 9 = q_2$
$X^3 - 6X^2 + 9X + 3$	$X^2 - 6X + 8$	$X + 3$
$-X^3 + 6X^2 - 8X$	$-X^2 - 3X$	
$r_1 = X + 3$	$-9X + 8$	
	$9X + 27$	
	$r_2 = 35$	

de unde deducem

$$f = (X^2 - 6X + 8)q_1 + r_1 \text{ şi } X^2 - 6X + 8 = (X - 9)r_1 + r_2,$$

ceea ce implică

$$\begin{aligned} 35 = r_2 = X^2 - 6X + 8 - r_1(X - 9) &= X^2 - 6X + 8 - [f - (X^2 - 6X + 8)q_1](X - 9) \\ &= -(X - 9)f + (X^2 - 6X + 8)[1 + X(X - 9)]. \end{aligned}$$

Rezulă $35 = (\alpha^2 - 6\alpha + 8)(\alpha^2 - 9\alpha + 1)$, adică

$$\frac{1}{\alpha^2 - 6\alpha + 8} = \frac{1}{35}\alpha^2 - \frac{9}{35}\alpha + \frac{1}{35}.$$

7.34. a) Polinoamele ireductibile din $\mathbb{Z}_2[X]$ au gradul cel puţin 1. Polinoamele de grad 1 sunt ireductibile. Acestea sunt

$$f_1 = X \text{ şi } f_2 = X + \widehat{1}.$$

Un polinom de gradul 2 este de forma $g = X^2 + aX + b$, cu $a, b \in \mathbb{Z}_2$. Deci există 4 polinoame de grad 2 în $\mathbb{Z}_2[X]$. Dintre acestea sunt reductibile polinoamele $g_1 = X^2$, $g_2 = (X + \widehat{1})^2 = X^2 + \widehat{1}$, $g_3 = X(X + \widehat{1}) = X^2 + X$, iar

$$g_4 = X^2 + X + \widehat{1}$$

este ireductibil. Un polinom de grad 3 este de forma $g = X^3 + aX^2 + bX + c$, cu $a, b, c \in \mathbb{Z}_2$. Deci există 8 polinoame de grad 3 în $\mathbb{Z}_2[X]$. Dintre acestea sunt reductibile acelea care se descompun în produse cu factorii (ireductibili) f_1, f_2 şi g_4 adică $h_1 = X^3$, $h_2 = (X + \widehat{1})^3 = X^3 + X^2 + X + \widehat{1}$, $h_3 = X^2(X + \widehat{1}) = X^3 + X^2$,

$h_4 = X(X+\widehat{1})^2 = X(X^2+\widehat{1}) = X^3+X$, $h_5 = X(X^2+X+\widehat{1}) = X^3+X^2+X$ şi $h_6 = (X+\widehat{1})(X^2+X+\widehat{1}) = X^3+\widehat{1}$, iar

$$h_7 = X^3+X^2+\widehat{1} \text{ şi } h_8 = X^3+X+\widehat{1}$$

sunt ireductibile.
b) Dacă K este un corp cu 4 elemente atunci subcorpul său prim este izomorf cu $\mathbb{Z}_2$, deoarece caracteristica sa este un număr prim care divide pe 4. Deci K se poate considera ca o extindere a lui $\mathbb{Z}_2$. Polinomul $f = X^2+X+1 \in \mathbb{Z}_2[X]$ are gradul 2 şi nu are nici o rădăcină în $\mathbb{Z}_2$, prin urmare este ireductibil. Rezultă că adjuncţionând la $\mathbb{Z}_2$ o rădăcină α a lui f se obţine o extindere $\mathbb{Z} \leq \mathbb{Z}_2(\alpha)$ de gradul 2. Urmează că 1 şi α formează o bază a acestei extinderi. Amintim că $\mathbb{Z}_2(\alpha) = \mathbb{Z}_2[X]/(f)$ şi $\alpha = X+(f)$. Deci $\mathbb{Z}_2(\alpha) = \{a+b\alpha \mid a,b \in \mathbb{Z}_2\}$, de unde rezultă că $\mathbb{Z}_2(\alpha)$ este un corp cu patru elemente. Notăm $K = \mathbb{Z}_2(\alpha)$. Avem $K = \{\widehat{0}, \widehat{1}, \alpha, \widehat{1}+\alpha\}$. Din $f(\alpha) = 0$ rezultă $\alpha^2 = -\alpha-\widehat{1} = \widehat{1}+\alpha$, egalitate care determină înmulţirea din K. De exemplu, $\alpha(\widehat{1}+\alpha) = \alpha+\alpha^2 = \alpha+\alpha+\widehat{1} = \widehat{1}$. Astfel, tablele de adunare şi înmulţire din K sunt

$+$	$\widehat{0}$	$\widehat{1}$	α	$\widehat{1}+\alpha$
$\widehat{0}$	$\widehat{0}$	$\widehat{1}$	α	$\widehat{1}+\alpha$
$\widehat{1}$	$\widehat{1}$	$\widehat{0}$	$\widehat{1}+\alpha$	α
α	α	$\widehat{1}+\alpha$	$\widehat{0}$	$\widehat{1}$
$\widehat{1}+\alpha$	$\widehat{1}+\alpha$	α	$\widehat{1}$	$\widehat{0}$

$\cdot$	$\widehat{0}$	$\widehat{1}$	α	$\widehat{1}+\alpha$
$\widehat{0}$	$\widehat{0}$	$\widehat{0}$	$\widehat{0}$	$\widehat{0}$
$\widehat{1}$	$\widehat{0}$	$\widehat{1}$	α	$\widehat{1}+\alpha$
α	$\widehat{0}$	α	$\widehat{1}+\alpha$	$\widehat{1}$
$\widehat{1}+\alpha$	$\widehat{0}$	$\widehat{1}+\alpha$	$\widehat{1}$	α

c) Polinomul $g = X^3+X+1 \in \mathbb{Z}_2[X]$ este ireductibil, prin urmare, extinderea $\mathbb{Z}_2 \leq \mathbb{Z}_2(\alpha)$, unde $g(\alpha) = 0$, are gradul 3 şi $1,\ \alpha,\ \alpha^2$ este o bază a sa. Deci

$$\mathbb{Z}_2(\alpha) = \{a+b\alpha+c\alpha^2 \mid a,b,c \in \mathbb{Z}_2\},$$

de unde deducem că $\mathbb{Z}_2(\alpha)$ este un corp cu 8 elemente.

7.35. a) Un polinom $f = X^2+aX+b \in \mathbb{Z}_3[X]$ este ireductibil dacă şi numai dacă $f(\widehat{0}) \neq \widehat{0}$, $f(\widehat{1}) \neq \widehat{0}$ şi $f(\widehat{2}) = f(-\widehat{1}) \neq \widehat{0}$. Prin urmare polinoamele ireductibile de forma $f = X^2+aX+b \in \mathbb{Z}_3[X]$ sunt: $f_1 = X^2+\widehat{1}$, $f_2 = X^2+X+\widehat{2}$,$f_3 = X^2+\widehat{2}X+\widehat{2}$. Celelalte polinoame ireductibile din $\mathbb{Z}_3[X]$ sunt asociate în divizibilitate cu acestea, deci sunt $\widehat{2}f_1 = \widehat{2}X^2+\widehat{2}$, $\widehat{2}f_2 = \widehat{2}X^2+\widehat{2}X+\widehat{1}$, $\widehat{2}f_3 = \widehat{2}X^2+X+\widehat{1}$.
b) Polinomul $f_1 = X^2+\widehat{1}$ fiind ireductibil peste $\mathbb{Z}_3$, rezultă că extinderea $\mathbb{Z}_3 \leq \mathbb{Z}_3(\alpha)$, unde $f_1(\alpha) = 0$, are gradul 2 şi $1, \alpha$ este o bază a sa. Prin urmare,

$$\mathbb{Z}_3(\alpha) = \{a+b\alpha \mid a,b \in \mathbb{Z}_3\}.$$

Deci $\mathbb{Z}_3(\alpha)$ este un corp cu 9 elemente. Adunarea în $\mathbb{Z}_3$ se efectuează pe componente, iar înmulţirea este dată de relaţia $f_1(\alpha) = 0$, adică $\alpha^2 = -\widehat{1} = \widehat{2}$. Astfel, dacă $u = a+b\alpha$, $u' = a'+b'\alpha \in \mathbb{Z}_3(\alpha)$ atunci $u+u' = (a+a')+(b+b')\alpha$ şi

$$uu' = aa'+(ab'+a'b)\alpha+bb'\alpha^2 = (aa'-bb')+(ab'+a'b)\alpha.$$

7.36. a) Corespondenţa $(a,b) \mapsto X^2+aX+b$ realizează o bijecţie între $K \times K$ şi mulţimea P_2 a polinoamelor de gradul 2 unitare din $K[X]$. Deci numărul polinoamelor din P_2 este q^2. Un polinom din P_2 este reductibil peste K dacă şi umai dacă are rădăcinile în K. Corespondenţa $\{\alpha,\beta\}\mapsto(X-\alpha)(X-\beta)$ realizează o bijecţie între submulţimile cu câte 2 elemente ale lui K şi polinoamele din P_2 care au în K rădăcini diferite, iar corespondenţa $\alpha\mapsto(X-\alpha)^2$ realizează o bijecţie între K şi polinoamele din P_2 care au o rădăcină dublă în K. Deci numărul cerut este

$$q^2-C_q^2-q=q^2-\frac{q(q-1)}{2}-q=\frac{q^2-q}{2}.$$

b) Fie P_3 mulţimea polinoamelor unitare de gradul 3 din $K[X]$. Numărul polinoamelor din P_3 este q^3. Un polinom din P_3 este reductibil peste K dacă şi numai dacă are cel puţin o rădăcină în K. Polinoamele din P_3 care au o singură rădăcină în K se descompun sub forma $(X-\alpha)(X^2+aX+b)$, unde $\alpha\in K$ şi $X^2+aX+b\in P_2$ este ireductibil peste K, deci numărul lor este $q\cdot\dfrac{q^2-q}{2}$. Polinoamele din P_3 care au o rădăcină multiplă în K se descompun sub forma $(X-\alpha)^2(X-\beta)$ cu $(\alpha,\beta)\in K^2$, deci numărul acestora este q^2. Polinoamele din P_3 care au trei rădăcini diferite în K se descompun sub forma $(X-\alpha)(X-\beta)(X-\gamma)$, unde $\{\alpha,\beta,\gamma\}$ este o submulţime a lui K formată din 3 elemente, deci numărul acestor polinoame este C_q^3. Din cele de mai sus rezultă că numărul cerut este

$$q^3-q\cdot\frac{q(q-1)}{2}-q^2-\frac{q(q-1)(q-2)}{6}=\frac{q^3-q}{3}.$$

7.37. Răspuns. Notând cu $D_f(K)$ corpul de descompunere al lui $f\in K[X]$ avem:
a) $D_f(\mathbb{Q})=\mathbb{Q}(-\sqrt{2},\sqrt{2})=\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$, $D_f(\mathbb{R})=\mathbb{R}(-\sqrt{2},\sqrt{2})=\mathbb{R}$;
b) $D_f(\mathbb{Q})=\mathbb{Q}(-i\sqrt{2},i\sqrt{2})=\mathbb{Q}(i\sqrt{2})=\{a+bi\sqrt{2}\mid a,b\in\mathbb{Q}\}$, $D_f(\mathbb{R})=\mathbb{R}(i\sqrt{2})=\mathbb{C}$;
c) Dacă ε este o rădăcină a lui X^3-1 diferită de 1 atunci $D_f(\mathbb{Q})=\mathbb{Q}(\varepsilon)=\{a+b\varepsilon\mid a,b\in\mathbb{Q}\}$ şi $D_f(\mathbb{R})=\mathbb{R}(\varepsilon)=\mathbb{C}$;
d) $D_f(\mathbb{Q})=\mathbb{Q}\left(1,\dfrac{1\pm i\sqrt{3}}{2}\right)=\mathbb{Q}(i\sqrt{3})=\{a+bi\sqrt{3}\mid a,b\in\mathbb{Q}\}$, $D_f(\mathbb{R})=\mathbb{R}(i\sqrt{3})=\mathbb{C}$;
e) $D_f(\mathbb{Q})=\mathbb{Q}(-\sqrt[4]{2},\sqrt[4]{2},-i\sqrt[4]{2},i\sqrt[4]{2})=\mathbb{Q}(\sqrt[4]{2},i)=\{a+b\sqrt[4]{2}+c\sqrt[4]{4}+d\sqrt[4]{8}+ei+fi\sqrt[4]{2}+gi\sqrt[4]{4}+hi\sqrt[4]{8}\mid a,b,c,d,e,f,g,h\in\mathbb{Q}\}$, $D_f(\mathbb{R})=\mathbb{C}$;
f) $D_f(\mathbb{Q})=\mathbb{Q}(\sqrt[4]{2},i)$ pentru că $x_1,x_2x_3,x_4\in\mathbb{Q}(\sqrt[4]{2},i)$ şi $i=\dfrac{x_1}{x_2}$, $\sqrt[4]{2}=\dfrac{1}{4}\left(\dfrac{x_1+x_3}{i}\right)^3\in\mathbb{Q}(x_1,x_2,x_3,x_4)$, unde $x_{1,2}=\dfrac{\sqrt{2}}{2}(1\pm i)\sqrt[4]{2}$, $x_{1,2}=\dfrac{\sqrt{2}}{2}(-1\pm i)\sqrt[4]{2}$ sunt rădăcinile lui f, $D_f(\mathbb{R})=\mathbb{C}$;
g) $D_f(\mathbb{Q})=\mathbb{Q}(i\sqrt{3})=\{a+bi\sqrt{3}\mid a,b\in\mathbb{Q}\}$, $D_f(\mathbb{R})=\mathbb{C}$.

7.38. a) Cum ε este generator al grupului U_n, rezultă că rădăcinile lui f sunt $1,\varepsilon,\varepsilon^2,\ldots,\varepsilon^{n-1}$. Prin urmare, $D_f(\mathbb{Q})=\mathbb{Q}(1,\varepsilon,\varepsilon^2,\ldots,\varepsilon^{n-1})=\mathbb{Q}(\varepsilon)$.
b) Rădăcinile lui g sunt $u,u\varepsilon,u\varepsilon^2,\ldots,u\varepsilon^{n-1}$, deci

$$D_g(\mathbb{Q})=\mathbb{Q}(u,u\varepsilon,u\varepsilon^2,\ldots,u\varepsilon^{n-1})=\mathbb{Q}(u,\varepsilon).$$

7.39. Răspuns. $G(\mathbb{Q},\mathbb{R})=\{1_{\mathbb{R}}\}$, $G(\mathbb{R},\mathbb{C})=\{1_{\mathbb{C}},\sigma\}$, unde $\sigma(a+bi)=a-bi$, şi $G(\mathbb{Q},\mathbb{Q}(i))=\{1_{\mathbb{Q}(i)},\delta\}$, unde $\delta(a+bi)=a-bi$.

7.40. Indicaţie. $K=\{(m\cdot 1')(n\cdot 1')^{-1}\mid m,n\in\mathbb{Z},\ n\cdot 1'\neq 0'\}$, unde $0'$, respectiv $1'$, este elementul zero, respectiv unitate, din K'.

7.41. 1) Rădăcinile lui f sunt $x_1 = \sqrt[3]{2} = u$, $x_2 = \varepsilon u$, $x_3 = \varepsilon u^2$, unde ε este o rădăcină primitivă de ordinul 3 a unităţii, adică o rădăcină a lui $g = X^2 + X + 1$. Rezultă că $D = D_f(\mathbb{Q}) = \mathbb{Q}(u, \varepsilon u, \varepsilon^2 u) = \mathbb{Q}(\varepsilon, u)$. Polinomul munimal al lui u peste $\mathbb{Q}$ este f, iar al lui ε peste $\mathbb{Q}(u)$ este g. Acum din $\mathbb{Q} \leq \mathbb{Q}(u) \leq \mathbb{Q}(u, i) = D$ deducem $[D : \mathbb{Q}] = [\mathbb{Q}(u) : \mathbb{Q}] \cdot [D : \mathbb{Q}(u)] = 3 \cdot 2 = 6$, iar o bază a extinderii $\mathbb{Q} \leq D$ este $\{1, u, u^2, \varepsilon, \varepsilon u, \varepsilon u^2\}$. Deci

$$D = \{a_1 + a_2 u + a_3 u^2 + a_4 \varepsilon + a_5 \varepsilon u + a_6 \varepsilon u^2 \mid a_i \in \mathbb{Q},\ i \in \{1, \ldots, 6\}\}. \tag{1}$$

Polinomul f fiind separabil, rezultă că ordinul grupului $G = G_f(\mathbb{Q})$ este 6. Din problema anterioară urmează că $G = Aut(D)$. Un automorfism $\sigma : D \to D$ din G este determinat de $\sigma(\varepsilon)$ şi $\sigma(u)$. Întrucât polinomul g este ireductibil peste $\mathbb{Q}(u)$, urmează că există un singur $\mathbb{Q}(u)$-automorfism $\sigma_1 : D \to D$ pentru care avem $\sigma_1(\varepsilon) = \varepsilon^2$, rezultă că σ_1 este un $\mathbb{Q}$-automorfism şi $\sigma_1(u) = u$, $\sigma_1(\varepsilon) = \varepsilon^2$, de unde deducem $\sigma_1^2 = 1_D$. Polinomul f este ireductibil peste $\mathbb{Q}(\varepsilon)$, deci există un singur $\mathbb{Q}(\varepsilon)$-automorfism $\sigma_2 : D \to D$ pentru care avem $\sigma_2(u) = \varepsilon u$. Prin urmare, σ_2 este un $\mathbb{Q}$-automorfism şi $\sigma_2(\varepsilon) = \varepsilon$, $\sigma_2(u) = \varepsilon u$. Rezultă $\sigma_2^2(\varepsilon) = \varepsilon$, $\sigma_2^2(\varepsilon u) = \varepsilon^2 u$ şi $\sigma_2^3 = 1_D$. Prin urmare,

$$(\sigma_2 \circ \sigma_1)(\varepsilon) = \varepsilon^2,\ (\sigma_2 \circ \sigma_1)(u) = \varepsilon u \text{ şi } (\sigma_2^2 \circ \sigma_1)(\varepsilon) = \varepsilon^2,\ (\sigma_2^2 \circ \sigma_1)(u) = \varepsilon^2 u.$$

Din cele de mai sus rezultă $G_f(\mathbb{Q}) = \{1_D, \sigma_1, \sigma_2, \sigma_2^2, \sigma_2 \circ \sigma_1, \sigma_2^2 \circ \sigma_1\}$. Sistematizăm valorile restricţiilor automorfismelor din $G_f(\mathbb{Q})$ la $\{\varepsilon, u\}$ în următorul tabel:

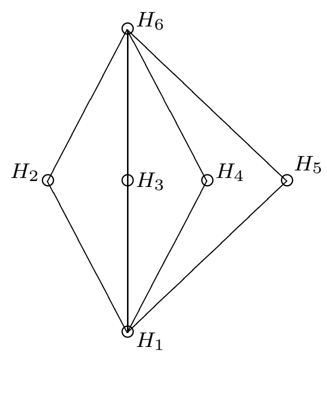
	1_D	σ_1	σ_2	σ_2^2	$\sigma_2 \circ \sigma_1$	$\sigma_2^2 \circ \sigma_1$
ε	ε	ε^2	ε	ε	ε^2	ε^2
u	u	u	εu	$\varepsilon^2 u$	εu	$\varepsilon^2 u$

Grupul $G_f(\mathbb{Q})$ este necomutativ deoarece $\sigma_2 \circ \sigma_1 \neq \sigma_1 \circ \sigma_2 = \sigma_2^2 \circ \sigma_1$. Rezultă că grupul $G_f(\mathbb{Q})$ este izomorf cu S_3. Funcţia $\varphi : G_f(\mathbb{Q}) \to S_3$ definită prin

σ	1_D	σ_1	σ_2	σ_2^2	$\sigma_2 \circ \sigma_1$	$\sigma_2^2 \circ \sigma_1$
$\varphi(\sigma)$	e	(x_2, x_3)	(x_1, x_2, x_3)	(x_1, x_3, x_2)	(x_1, x_2)	(x_1, x_3)

este un izomorfism.

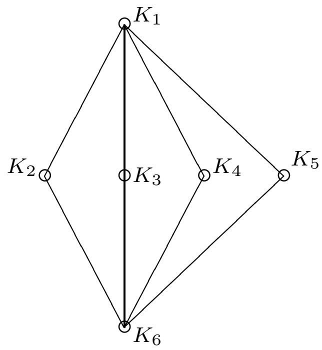
2) Subgrupurile lui $G_f(\mathbb{Q})$ sunt $H_1 = \{1_D\}, H_2 = \langle \sigma_1 \rangle = \{1_D, \sigma_1\}$, $H_3 = \langle \sigma_2 \rangle = \{1_D, \sigma_2, \sigma_2^2\}$, $H_4 = \{1_D, \sigma_2 \circ \sigma_1\}$, $H_5 = \{1_D, \sigma_2^2 \circ \sigma_1\}$ şi $H_6 = G_f(\mathbb{Q})$. Diagrama laticei subgrupurilor lui $G_f(\mathbb{Q})$ este



3) Fiecare H_i determină un subcorp al lui D

$$(2) \qquad K_i = \{x \in D \mid \sigma(x) = x,\ \forall \sigma \in H_i\},$$

numit *subcorpul invarianţilor* lui H_i. Conform teoremei fundamentale a teoriei lui Galois, corespondenţa $H_i \mapsto K_i$ realizează un antiizomorfism între laticea subgrupurilor lui $G_f(\mathbb{Q})$ şi laticea subcorpurilor lui D. Din (1) şi (2) rezultă $K_1 = D$, $K_2 = \mathbb{Q}(u)$, $K_3 = \mathbb{Q}(\varepsilon)$, $K_4 = \mathbb{Q}(\varepsilon^2 u)$, $K_5 = \mathbb{Q}(\varepsilon u)$ şi $K_6 = \mathbb{Q}$. Prin urmare, diagrama laticei subcorpurilor lui D este



7.42. 1) Rădăcinile lui f sunt $x_1 = \sqrt[4]{2} = u$, $x_2 = -u$, $x_3 = iu$, $x_4 = -iu$. Rezultă că $D = D_f(\mathbb{Q}) = \mathbb{Q}(u, -u, iu, -iu) = \mathbb{Q}(i, u)$. Polinomul minimal al lui u peste $\mathbb{Q}$ este f, iar al lui i peste $\mathbb{Q}(u)$ este $g = X^2 + 1$. Acum din

$$\mathbb{Q} \leq \mathbb{Q}(u) \leq \mathbb{Q}(u, i) = D$$

deducem $[D : \mathbb{Q}] = [\mathbb{Q}(u) : \mathbb{Q}] \cdot [D : \mathbb{Q}(u)] = 4 \cdot 2 = 8$, iar o bază a extinderii $\mathbb{Q} \leq D$ este $\{1, u, u^2, u^3, i, iu, iu^2, iu^3\}$. Deci

$$(1) \quad D = \{a_1 + a_2 u + a_3 u^2 + a_4 u^3 + a_5 i + a_6 iu + a_7 iu^2 + a_8 iu^3 \mid a_1 \in \mathbb{Q},\ i \in \{1, \ldots, 8\}\}$$

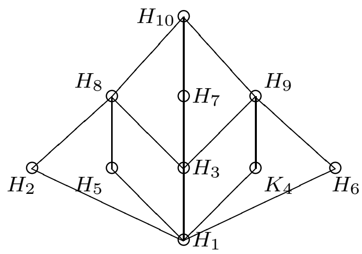
Polinomul f fiind separabil rezultă că ordinul grupului $G = G_f(\mathbb{Q})$ este 8, deci $G_f(\mathbb{Q})$ nu este izomorf cu S_4. Din problema **7.40** urmează $G = Aut(D)$. Un automorfism $\sigma : D \to D$ din G este determinat de $\sigma(i)$ şi $\sigma(u)$. Întrucât polinomul g este polinom ireductibil peste $\mathbb{Q}(u)$ urmează că există un singur $\mathbb{Q}(u)$-automorfism $\sigma_1 : D \to D$ pentru care avem $\sigma_1(i) = -i$. Rezultă că σ_1 este un $\mathbb{Q}$-automorfism şi $\sigma_1(u) = u$, $\sigma_1(i) = -i$, de unde deducem că $\sigma_1^2 = 1_D$. Polinomul f este ireductibil peste $\mathbb{Q}(i)$, deci există un singur $\mathbb{Q}(i)$-automorfism $\sigma_2 : D \to D$ pentru care avem $\sigma_2(u) = iu$. Deci σ_2 este un $\mathbb{Q}$-automorfism pentru care avem $\sigma_2(i) = i$, $\sigma_2(u) = iu$, de unde deducem $\sigma_2^2(u) = -u$, $\sigma_2^2(i) = i$, $\sigma_2^3(u) = -iu$, $\sigma_2^3(i) = i$ şi $\sigma_2^4 = 1_D$. Prin urmare,

$$(\sigma_2 \circ \sigma_1)(u) = iu,\ (\sigma_2 \circ \sigma_1)(i) = -i;$$
$$(\sigma_2^2 \circ \sigma_1)(u) = -u,\ (\sigma_2^2 \circ \sigma_1)(i) = -i;$$
$$(\sigma_2^3 \circ \sigma_1)(u) = -iu,\ (\sigma_2^3 \circ \sigma_1)(i) = -i.$$

Din cele de mai sus rezultă $G_f(\mathbb{Q}) = \{1_D, \sigma_1, \sigma_2, \sigma_2^2, \sigma_2^3, \sigma_2 \circ \sigma_1, \sigma_2^2 \circ \sigma_1, \sigma_2^3 \circ \sigma_1\}$ şi

$$(2) \qquad \sigma_1^2 = 1_D,\ \sigma_2^4 = 1_D,\ \sigma_1 \circ \sigma_2 = \sigma_2^3 \circ \sigma_1,$$

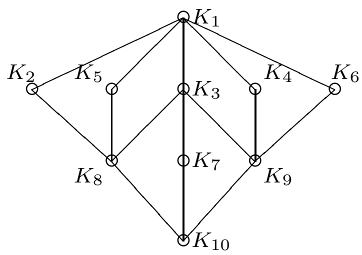
adică $G_f(\mathbb{Q})$ este generat de σ_1 şi σ_2 cu relaţiile (2), de unde urmează că $G_f(\mathbb{Q})$ este izomorf cu grupul diedral Δ_4. Din (2) rezultă că $\sigma_1 \circ \sigma_2 \circ \sigma_1 = \sigma_2^{-1}$ ceea ce implică $\sigma_1 \circ \sigma_2^k \circ \sigma_1 = \sigma_2^{-k}$, de unde urmează $\sigma_2^j \sigma_1 \circ \sigma_2^k \circ \sigma_1 = \sigma_2^{j-k}$.
2) Folosind teorema lui Lagrange şi relaţiile stabilite, vom determina subgrupurile lui $G_f(\mathbb{Q})$. Subgrupurile proprii ale lui $G_f(\mathbb{Q})$ pot avea ordinul 2 sau 4. Subgrupurile de ordinul 2 sunt ciclice şi sunt generate de elemete de ordinul 2. Acestea sunt $H_2 = \langle \sigma_1 \rangle = \{1_D, \sigma_1\}$, $H_3 = \langle \sigma_2^2 \rangle = \{1_D, \sigma_2^2\}$, $H_4 = \langle \sigma_2 \circ \sigma_1 \rangle = \{1_D, \sigma_2 \circ \sigma_1\}$, $H_5 = \langle \sigma_2^2 \circ \sigma_1 \rangle = \{1_D, \sigma_2^2 \circ \sigma_1\}$, $H_6 = \langle \sigma_2^3 \circ \sigma_1 \rangle = \{1_D, \sigma_2^3 \circ \sigma_1\}$. Elementele de ordinul 4 sunt σ_2 şi σ_2^3 aşadar, există un singur subgrup ciclic de ordinul 4, şi anume $H_7 = \langle \sigma_2 \rangle = \{1_D, \sigma_2, \sigma_2^2, \sigma_2^3\} = \langle \sigma_2^3 \rangle$. Fiecare subgrup neciclic de ordinul 4 conţine pe 1_D şi 3 elemente de ordinul 2, deci un astfel de subgrup nu conţine pe σ_2 şi σ_2^3 şi nu include pe $\{\sigma_1, \sigma_2 \circ \sigma_1\}$, $\{\sigma_1, \sigma_2^3 \circ \sigma_1\}$. Rezultă că subgrupurile neciclice de ordinul 4 sunt $H_8 = \langle \sigma_1, \sigma_2^2 \rangle = \{1_D, \sigma_1, \sigma_2^2, \sigma_2^2 \circ \sigma_1\}$ şi $H_9 = \langle \sigma_2^2, \sigma_2 \circ \sigma_1 \rangle = \{1_D, \sigma_2^2, \sigma_2 \circ \sigma_1, \sigma_2^3 \circ \sigma_1\}$. Mai notăm $H_1 = \{1_D\}$ şi $H_{10} = G_f(\mathbb{Q})$. Diagrama laticei subgrupurilor grupului $G_f(\mathbb{Q})$ este



3) Subcorpul invarianţilor unui subgrup H_i este

$$K_i = \{x \in D \mid \sigma(x) = x, \ \forall \sigma \in H_i\}. \tag{3}$$

Corespondenţa $H_i \mapsto K_i$ realizează un antiizomorfism între laticea subgrupurilor lui $G_f(\mathbb{Q})$ şi laticea subcorpurilor lui D. Din (1) şi (3) rezultă $K_1 = D$, $K_2 = \mathbb{Q}(\sqrt[4]{2})$, $K_3 = \mathbb{Q}(i, \sqrt[4]{4})$, $K_4 = \mathbb{Q}((1+i)\sqrt[4]{2})$, $K_5 = \mathbb{Q}(i\sqrt[4]{2})$, $K_6 = \mathbb{Q}((1-i)\sqrt[4]{2})$, $K_7 = \mathbb{Q}(i)$, $K_8 = \mathbb{Q}(\sqrt[4]{4})$, $K_9 = \mathbb{Q}(i\sqrt[4]{4})$, $K_{10} = \mathbb{Q}$. Prin urmare, diagrama laticei subcorpuilor lui D este



7.43. 1) $D = D_f(K) = K(\sqrt[3]{2}, \varepsilon\sqrt[3]{2}, \varepsilon^2\sqrt[3]{2}) = \mathbb{Q}(\varepsilon, \sqrt[3]{2}) = K(\sqrt[3]{2})$. Polinomul minimal al lui $\sqrt[3]{2}$ peste K este f. Rezultă că $[D : K] = 3$,

$$D = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in K\}$$

şi $|G_f(K)| = 3$. Orice automorfism $\sigma \in G_f(K)$ este determinat de $\sigma(\sqrt[3]{2})$ şi $\sigma(\sqrt[3]{2})$ este o rădăcină a lui f. Din ireductibilitatea lui f peste K rezultă că există un singur K-automorfism $\sigma_1 : D \to D$ astfel încât $\sigma_1(\sqrt[3]{2}) = \varepsilon\sqrt[3]{2}$, de unde urmează

$$\sigma_1^2(\sqrt[3]{2}) = \varepsilon^2\sqrt[3]{2} \text{ şi } \sigma_1^3 = 1_D.$$

Deci $G_f(K) = \{1_D, \sigma_1, \sigma_1^2\} \simeq \mathbb{Z}_3$.
2) Subgrupurile lui $G_f(K)$ sunt $H_1 = \{1_D\}$ şi $H_2 = G_f(K)$ şi diagrama laticei subgruprilor lui $G_f(K)$ este

$$\begin{array}{c} H_2 \\ | \\ H_1 \end{array}$$

3) Subcorpul invarianţilor lui H_1, respectiv H_2, este $K_1 = D$, respectiv $K_2 = K$ şi diagrama cerută este

$$\begin{array}{c} K_1 \\ | \\ K_2 \end{array}$$

7.44. 1) $D = D_f(K) = K(\sqrt[p]{2}, \varepsilon\sqrt[p]{2}, \ldots, \varepsilon^{p-1}\sqrt[p]{2}) = \mathbb{Q}(\varepsilon, \sqrt[p]{2}) = K(\sqrt[p]{2})$. Polinomul minimal al lui $\sqrt[p]{2}$ peste $\mathbb{Q}$ este f, iar al lui ε peste $\mathbb{Q}$ este

$$g = \frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1.$$

Ireductibilitatea lui g rezultă din problema **5.39**. Prin urmare,

$$[\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] = p,\ [K : \mathbb{Q}] = 1 \text{ şi } [K(\sqrt[p]{2}) : K] \leq p.$$

Din

$$(*) \qquad [D : \mathbb{Q}] = [D : K] \cdot [K : \mathbb{Q}] = [D : K] \cdot (p - 1)$$

şi

$$[D : \mathbb{Q}] = [D : \mathbb{Q}(\sqrt[p]{2})] \cdot [\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] = [D : \mathbb{Q}(\sqrt[p]{2})] \cdot p$$

deducem că p şi $p - 1$ divid pe $[D : \mathbb{Q}]$ şi $[D : \mathbb{Q}] \leq p(p - 1)$, iar cum $(p, p - 1) = 1$, urmează că $[D : \mathbb{Q}] = p(p - 1)$, ceea ce, împreună cu $(*)$ implică $[D : K] = p$, adică $[K(\sqrt[p]{2}) : K] = p$. Rezultă că gradul lui $\sqrt[p]{2}$ peste K este p, deci f este polinomul minimal al lui $\sqrt[p]{2}$ peste K, $[D : K] = p$,

$$D = \{a_1 + a_2\sqrt[p]{2} + \cdots + a_n\sqrt[p]{2^{p-1}} \mid a_i \in K,\ i \in \{1, \ldots, n\}\}$$

şi $|G_f(K)| = 3$. Orice automorfism $\sigma \in G_f(K)$ este determinat de $\sigma(\sqrt[p]{2})$ şi $\sigma(\sqrt[p]{2})$ este o rădăcină a lui f. Din ireductibilitatea lui f peste K rezultă că există un singur K-automorfism $\sigma_1 : D \to D$ astfel încât $\sigma_1(\sqrt[p]{2}) = \varepsilon\sqrt[p]{2}$, de unde urmează

$$\sigma_1^k(\sqrt[p]{2}) = \varepsilon^k\sqrt[p]{2},\ k \in \{1, \ldots, p\}.$$

Deci $\sigma_1^p = 1_D$ şi $G_f(K) = \{1_D, \sigma_1, \ldots, \sigma_1^{p-1}\} \simeq \mathbb{Z}_p$.
2) Subgrupurile lui $G_f(K)$ sunt $H_1 = \{1_D\}$ şi $H_2 = G_f(K)$ şi diagrama laticei subgruprilor lui $G_f(K)$ este

$$\begin{array}{c} H_2 \\ | \\ H_1 \end{array}$$

3) Subcorpul invarianţilor lui H_1, respectiv H_2, este $K_1 = D$, respectiv $K_2 = K$ şi diagrama cerută este

$$\begin{array}{c} K_1 \\ | \\ K_2 \end{array}$$

7.45. Fie $q = p^n$, $f = X^q - X \in \mathbb{Z}_p[X]$ şi $D = D_f(K)$ corpul rădăcinilor lui f peste $\mathbb{Z}_p$. Funcţia $\varphi : D \to D$, $\varphi(a) = a^p$ este un automorfism al lui D, deci $\psi = \varphi^p$ este un automorfism al lui D, iar $\alpha \in D$ este rădăcină a lui f dacă şi numai dacă $\psi(\alpha) = \alpha$, de unde se deduce că rădăcinile lui f formează un subcorp al lui D. Rezultă că D coincide cu acest subcorp, deci $|D| = q$ pentru că f nu are rădăcini multiple, ceea ce implică $[D : \mathbb{Z}_p] = n$. Grupul $(D^*, \cdot)$ fiind ciclic, există $a \in D^*$ care generează pe $(D^*, \cdot)$. Rezultă că $D = \mathbb{Z}_p(a)$, de unde se deduce că polinomul minimal $g = \mathbb{Z}_p[X]$ al lui a are gradul n. Deci g este un polinom ireductibil de gradul n.

7.46. Indicaţie. P este izomorf cu $\mathbb{Q}$ sau $\mathbb{Z}_p$.

7.47. Fie x_1, x_2 rădăcinile lui f din $\mathbb{C} \setminus \mathbb{R}$ şi D corpul de descompunere al lui f peste K. Din ireductibilitatea lui f peste K rezultă $[K(x_1) : K] = p$, ceea ce împreună cu $K \leq K(x_1) \leq D$ ne arată că p divide pe $[D : K]$. Corpul K fiind perfect (pentru că are caracteristica ∞) şi $f \in K[X]$ fiind ireductibil urmează că f este separabil, de unde deducem că $|G_f(K)| = [D : K]$. Deci numărul prim p divide ordinul grupului $G_f(K)$, de unde rezultă că există $\sigma \in G_f(K)$ de ordinul p. Amintim că restricţia unui automorfism $\tau \in G_f(K)$ la rădăcinile $x_1, x_2, x_3, \ldots, x_p$ ale lui f este o permutare $\tau' \in S_p$, iar funcţia $\varphi : G_f(K) \to S_p$, $\varphi(\tau) = \tau'$ este un omomorfism injectiv. Rezultă că permutarea $\sigma' = \varphi(\tau)$ are în grupul S_p ordinul p, de unde deducem că σ' este un ciclu de lungime p, pentru că orice permutare din S_p se descompune în produs de cicluri disjuncte şi ordinul unui produs este c.m.m.m.c. al ordinelor factorilor. Pe de altă parte, din $D = K(x_1, x_2, x_3, \ldots, x_p)$ unde $x_3, \ldots, x_p$ sunt rădăcinile lui f din $\mathbb{R}$ şi din faptul că conjugarea complexă permută pe x_1 cu x_2 şi lasă fixe elementele din $K(x_3, \ldots, x_p)$ urmează că conjugarea induce un $K(x_3, \ldots, x_p)$-automorfism al lui D, care prin φ trece în transpoziţia (x_1, x_2). Deci subgrupul $\operatorname{Im}\varphi$ al lui S_p conţine un ciclu de lungime p şi o transpoziţie. Întrucât un ciclu de lungime p şi o transpoziţie generează pe S_p (vezi problema **2.85**) rezultă că $\operatorname{Im}\varphi = S_p$. Astfel am arătat că φ este un izomorfism.

7.48. Notând $f = X(X^2 - 4)(X^2 + 2) - 2$, avem $f \in \mathbb{Q}[X]$ şi $\operatorname{grad} f = 5$. Reprezentând grafic funcţia $g : \mathbb{R} \to \mathbb{R}$, $g(x) = x(x^2 - 4)(x^2 + 2)$ constatăm că graficul lui g intersectează dreapta $y = 2$ în trei puncte. Deci f are exact $3 = 5 - 2$ rădăcini reale. Folosind Criteriul lui Eisenstein se deduce că f este ireductibil peste $\mathbb{Q}$. Acum, din problema anterioară se deduce că $G_f(\mathbb{Q}) \simeq S_5$, iar S_5 fiind neresolubil, urmează că ecuaţia $f(x) = 0$ nu este rezolvabilă prin radicali.

Bibliografie

[1] Andrica, D.; Duca, I. D.; Purdea, I.; Pop, I.: Matematica de bază, *Editura Studium, Cluj-Napoca*, 2002.

[2] Andrica, D.; Deaconescu, M.; Schechter, M.; Culegere de probleme de algebră liniară, *Litografia Univ. ,,Babeş–Bolyai", Cluj-Napoca*, fasc. 1 (Spaţii liniare), 1976, fasc. 2 (Omomorfisme de spaţii liniare), 1979.

[3] Albu, T.; Ion, I. D.: Itinerar elementar în algebra superioară, *Editura ALL, Bucureşti*, 1997.

[4] Both, N.: Culegere de probleme de algebră, fasc. II, *Litografia Univ. ,,Babeş–Bolyai", Cluj-Napoca*, 1978.

[5] Both, N.; Crivei, S.: Culegere de probleme de algebră, *Litografia Univ. ,,Babeş–Bolyai", Cluj-Napoca*, 1997.

[6] Bourbaki, N.: Théorie des ensembles, *Hermann, Paris*, 1970.

[7] Breaz, S.; Covaci, R.: Elemente de logică, teoria mulţimilor şi aritmetică, *Editura Fundaţiei pentru Studii Europene, Cluj-Napoca*, 2006.

[8] Călugăreanu, Gr.: Lecţii de algebră liniară, *Litografia Univ. ,,Babeş–Bolyai", Cluj-Napoca*, 1995.

[9] Călugăreanu, Gr.; Breaz, S.; Modoi, C.; Pelea, C.; Vălcan, D.: Exercises in Abelian Group Theory, *Kluwer Academic Publishers, Dordrecht–Boston–London*, 2003.

[10] Călugăreanu, Gr.; Hamburg, P.: Exercises in Basic Ring Theory, *Kluwer Academic Publishers, Dordrecht–Boston–London*, 1998.

[11] Cohn, P. M., Universal algebra, *Harper and Row, New York, Evanston and London*, 1965.

[12] Covaci, R.: Algebră şi programare liniară, *Litografia Univ. ,,Babeş–Bolyai", Cluj-Napoca*, 1986.

[13] Fuchs, L.: Infinite Abelian Groups. Vol. I, Pure and Applied Mathematics, Vol. 36, *Academic Press, New York–London*, 1970.

[14] Grätzer, G., Universal algebra. Second edition, *Springer–Verlag*, 1979.

[15] Ion, I. D.; Ghioca, A. P.; Nediţă, N. I.: Matematică, Algebră, Manual pentru clasa a XII-a, *Editura Didactică şi Pedagogică, Bucureşti*, 1988.

[16] Ion, I. D.; Niţă, C.; Năstăsescu, C.: Complemente de algebră, *Editura Ştiinţifică şi Enciclopedică, Bucureşti*, 1984.

[17] Ion, I. D.; Niţă, C.; Popescu, D.; Radu, N.: Probleme de algebră, *Editura Didactică şi Pedagogică, Bucureşti*, 1981.

[18] Ion, I. D.; Radu, N.: Algebră, *Editura Didactică şi Pedagogică, Bucureşti*, 1991.

[19] Kargapolov, M.; Merzliakov, I.: Osnovî teorii grupp, *Moscova*, 1972.

[20] Lavrov, I. A.; Maksimova, I. I.: Probleme de teoria mulţimilor şi logică matematică, *Editura Tehnică, Bucureşti*, 1974.

[21] Kuroş, A. G.: Teoria grupurilor, *Editura Tehnică, Bucureşti*, 1959.

[22] Liapin, E., etc.: Uprajneniia po teorii grupp, *Moscova*, 1967.

[23] MacLane, S.; Birkhoff, G.: Algebra, *Macmillan Company, New York*, 1967.

[24] Mac Lane, S.; Birkhoff, G.: Algèbre. Solutions développées des exercices, *Gauthier–Villars, Paris*, 1^{re} partie (Ensembles, groupes, anneaux, corps - Weil, J.; Hocquemiller, J.) 1972, 2^{e} partie (Algèbre linéaire - Allouch, D.; Mézard, A.; Vaillant, J. C.; Weil, J.) 1973, 3^{e} partie (Les grands théorèmes - Mézard, A.; Delorme, Ch.; Lavit, Ch.; Raoult, J. C.) 1976.

[25] Năstăsescu, C.: Introducere în teoria mulţimilor, *Editura Didactică şi Pedagogică, Bucureşti*, 1974.

[26] Năstăsescu, C.; Niţă, C.; Vraciu, C.: Bazele algebrei. Vol. I, *Editura Academiei, Bucureşti*, 1986.

[27] Năstăsescu, C.; Ţena, M.; Andrei, G.; Otărăşanu. I.: Probleme de structuri algebrice, *Editura Academiei, Bucureşti*, 1988.

[28] Niţa, C.; Spircu, T.: Probleme de structuri algebrice, *Editura Tehnică, Bucureşti*, 1974.

[29] Pic, Gh.: Algebră superioară, *Editura Didactică şi Pedagogică, Bucureşti*, 1966.

[30] Purdea, I.: Tratat de algebră moderna. Vol. II, *Editura Academiei, Bucureşti*, 1982.

[31] Purdea, I.: Culegere de probleme de algebră. Relaţii, funcţii şi algebre universale, *Litografia Univ. ,,Babeş–Bolyai", Cluj-Napoca*, 1996.

[32] Purdea, I.: Culegere de probleme de teoria grupurilor, *Litografia Univ. ,,Babeş–Bolyai", Cluj-Napoca*, 1997.

[33] Purdea, I.; Pic, Gh.: Tratat de algebră modernă. Vol. I, *Editura Academiei, Bucureşti*, 1977.

[34] Purdea, I.; Pop, I.: Algebră. *Editura GIL, Zalău*, 2003.

[35] Riguet, J.: Relations binaires, fermetures, correspondances de Galois, *Bull. Soc. Math. France*, **76, 1-4** (1948), 114–155.

[36] Sierpiński, W., Cardinal and ordinal numbers, *PWN – Polish Scientific Publishers, Warsaw*, 1961.

[37] Szász, G.: Théorie des treillis, *Akadémiai Kiadó, Budapest*, 1971.

[38] Vagner, V. V.: Teoria otnoşenii i algebra ciasticinîh otobrajenii, *Saratov*, 1965.

Index