Probleme de algebră

Cornel Băeţica, Crina Boboc, Sorin Dăscălescu, Gabriel Mincu

PREFAŢĂ

Lucrarea de faţă îşi propune să vină în sprijinul studenţilor de la secţiile de matematică şi informatică pentru o mai bună aprofundare a unor noţiuni fundamentale din algebra modernă. De asemenea culegerea conţine chestiuni mai complicate care sunt de interes pentru studenţii care urmează un program de Master în matematică. Ea este o ediţie revizuită şi completată a culegerii publicate de primul şi al treilea autor în 1993 la Editura Universităţii Bucureşti.

Culegerea conţine soluţii complete ale problemelor propuse, precum şi câte un scurt breviar teoretic la începutul fiecărui capitol. Referinţele la alte probleme le facem citând doar numărul problemei atunci când ne referim la o problemă din acelaşi capitol, şi citând numărul problemei şi numărul capitolului atunci când ne referim la o problemă din alt capitol. Pentru elementele de teorie necesare trimitem cititorul la una dintre cărţile: "Algebră" de I. D. Ion şi N. Radu, "Bazele algebrei" de C. Năstăsescu, C. Niţă şi C. Vraciu, sau "Algebră" de T. Dumitrescu.

Dorim să mulţumim colegilor şi studenţilor care ne-au ajutat la scrierea acestei culegeri prin furnizarea de probleme sau soluţii. Mulţumiri speciale adresăm lui Tiberiu Dumitrescu pentru discuţiile matematice care ne-au fost de mare ajutor.

17 Martie 2008

Cornel Băeţica, Crina Boboc, Sorin Dăscălescu şi Gabriel Mincu

Cuprins

Capitolul 1

Mulţimi

• Dacă A şi B sunt mulţimi, notăm cu $A - B$ (sau cu $A \setminus B$) *diferenţa* celor două mulţimi, adică $A - B = \{x \mid x \in A \text{ şi } x \notin B\}$.
• Dacă $B \subseteq A$, atunci $A - B$ se mai notează $C_A B$ şi se numeşte *complementara* lui B în A.
• Vom nota cu $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, respectiv, mulţimile numerelor naturale, întregi, raţionale, reale, complexe, respectiv. Dacă M este una din aceste mulţimi, vom nota $M^* = M - \{0\}$.
• Dacă A este o mulţime, atunci mulţimea tuturor submulţimilor lui A se notează cu $\mathcal{P}(A)$ şi se numeşte *mulţimea părţilor* lui A.
• O mulţime A se numeşte *finită* dacă $A = \emptyset$ sau dacă există o bijecţie între A şi mulţimea $\{1, \ldots, n\}$ pentru un $n \in \mathbb{N}^*$. În acest caz notăm cu $|A|$ numărul elementelor lui A. Dacă A nu este finită, atunci spunem că A este *infinită*.
• Dacă X este o mulţime nevidă, notăm cu 1_X (sau cu Id_X) *funcţia identică* a mulţimii X, unde $1_X : X \to X$ şi este definită prin $1_X(x) = x$ pentru orice $x \in X$.
• Un element $x \in M$ se numeşte *punct fix* pentru funcţia $f : M \to M$ dacă $f(x) = x$.
• Compunerea a două funcţii $f : A \to B$ şi $g : B \to C$ se notează $g \circ f$ sau gf.
• Dacă $f : A \to B$ este o funcţie, $X \subseteq A$ şi $Y \subseteq B$, notăm $f(X) = \{f(x) \mid x \in X\}$, care este o submulţime a lui B şi $f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}$, care este o submulţime a lui A. Mulţimea $f(X)$ se numeşte *imaginea* lui X prin f, iar mulţimea $f^{-1}(Y)$ se numeşte *preimaginea* sau *imaginea inversă* a lui Y prin f.
• Dacă $f : A \to B$ este o funcţie şi A' este o submulţime nevidă a lui A,

notăm cu $f_{|A'}$ *restricţia* lui f la A', unde $f_{|A'} : A' \to B$ şi este definită prin $f_{|A'}(x) = f(x)$ pentru orice $x \in A'$.
• Dacă X şi Y sunt mulţimi nevide, notăm cu $\mathrm{Fun}(X, Y)$ sau cu Y^X mulţimea tuturor funcţiilor definite pe X cu valori în Y.
• Spunem că mulţimile A şi B sunt *echipotente* (şi notăm aceasta prin $A \sim B$) dacă există o bijecţie între A şi B.
• Dacă A este o mulţime care este în bijecţie cu $\mathbb{N}$, spunem că A este *numărabilă*. Dacă A este finită sau numărabilă, spunem că A este *cel mult numărabilă*. În caz contrar, A se numeşte *nenumărabilă*.
• Dacă $\sim$ este o relaţie de echivalenţă pe mulţimea A, notăm cu $A/\sim$ *mulţimea factor*, iar aceasta este mulţimea tuturor claselor de echivalenţă relativ la $\sim$. *Proiecţia canonică* $p : A \to A/\sim$ asociază unui element $a \in A$ clasa sa de echivalenţă în raport cu $\sim$.
• Dacă $f : A \to B$ este o funcţie, atunci notăm cu ρ_f relaţia de echivalenţă definită de f pe mulţimea A astfel: $x \rho_f y$ dacă şi numai dacă $f(x) = f(y)$.
• Mulţimile factor au următoarea *proprietate de universalitate*: fie A, B două mulţimi, $\sim$ o relaţie de echivalenţă pe A şi $f : A \to B$ o funcţie cu proprietatea că $\sim \subseteq \rho_f$. Atunci există şi este unică o funcţie $\overline{f} : A/\sim \to B$ care satisface condiţia $\overline{f}p = f$.

1. Fie $r, s \in \mathbb{N}^*$ astfel încât $r+1 \leq s$. Dacă $A_1, \ldots, A_s$ sunt mulţimi finite având fiecare r elemente şi intersecţia oricăror $r+1$ dintre aceste mulţimi este nevidă, să se arate că $\bigcap_{i=1,s} A_i \neq \emptyset$.

2. Fie A o mulţime finită cu n elemente. Să se arate că ecuaţia

$$X_1 \cup X_2 \cup \cdots \cup X_m = A$$

are $(2^m - 1)^n$ soluţii.

3. (*Principiul includerii şi excluderii*) Fie $A_1, \ldots, A_s$ mulţimi finite. Să se arate că

$$|\bigcup_{i=1,n} A_i| = \sum_{i=1,n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \cdots + (-1)^{n+1} |\bigcap_{i=1,n} A_i|.$$

4. Fie A o mulţime finită şi $f : A \to A$ o funcţie. Să se arate că următoarele afirmaţii sunt echivalente:

(a) f este injectivă.
(b) f este surjectivă.
(c) f este bijectivă.

5. Fie M şi N două mulţimi finite astfel încât $|M| = m$ şi $|N| = n$. Să se determine:
(a) Numărul funcţiilor definite pe M cu valori în N.
(b) Numărul funcţiilor injective definite pe M cu valori în N.
(c) Numărul funcţiilor surjective definite pe M cu valori în N.

6. Să se determine numărul permutărilor unei mulţimi cu n elemente care au cel puţin un punct fix şi al celor care au exact un punct fix.

7. Fie $f, g : \mathbb{N} \to \mathbb{N}$ două funcţii. Dacă mulţimea $A = \{x \in \mathbb{N} \mid f(x) \leq x\}$ este finită, să se arate că mulţimea $B = \{x \in \mathbb{N} \mid g(x) \leq g(f(x))\}$ este infinită.

8. Fie $f : \mathbb{N} \to \mathbb{N}$ o funcţie cu următoarele proprietăţi:
(a) f este strict crescătoare.
(b) $f(2) = 2$.
(c) $f(mn) = f(m)f(n)$ pentru orice $m, n \in \mathbb{N}$ prime între ele.
Să se arate că $f = 1_{\mathbb{N}}$.

9. Fie $f, g : \mathbb{N} \to \mathbb{N}$ astfel încât $\max(f, g)$ este surjectivă şi $\min(f, g)$ este injectivă. Să se arate că $f = g$.

10. Pentru fiecare din mulţimile $M = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ să se dea exemple de funcţii $f : M \to M$ care sunt injective dar nu sunt surjective, şi exemple de funcţii $g : M \to M$ care sunt surjective şi nu sunt injective.

11. Fie M o mulţime şi A, B două submulţimi ale sale. Definim $f : \mathcal{P}(M) \to \mathcal{P}(A) \times \mathcal{P}(B)$ prin $f(X) = (X \cap A, X \cap B)$. Să se arate că :
(a) f este injectivă dacă şi numai dacă $A \cup B = M$.
(b) f este surjectivă dacă şi numai dacă $A \cap B = \emptyset$.
(c) f este bijectivă dacă şi numai dacă $A = C_M B$. În acest caz să se calculeze f^{-1}.

12. Fie A o mulţime nevidă. Să se arate că nu există nicio funcţie surjectivă $f : A \to \mathcal{P}(A)$.

13. Fie $f : M \to N$ o funcţie. Să se arate că următoarele afirmaţii sunt echivalente:
(a) f este injectivă.
(b) f este *monomorfism*, adică pentru orice mulţime X şi orice funcţii $u, v : X \to M$ astfel încât $fu = fv$, rezultă că $u = v$.
(c) Există o funcţie $g : N \to M$ astfel încât $gf = 1_M$.

14. Fie $f : M \to N$ o funcţie. Să se arate că următoarele afirmaţii sunt echivalente:
(a) f este injectivă.
(b) Pentru orice familie $(M_i)_{i\in I}$ de submulţimi ale lui M are loc egalitatea $f(\bigcap\limits_{i\in I} M_i) = \bigcap\limits_{i\in I} f(M_i)$.

15. Fie $f : M \to N$ o funcţie. Să se arate că următoarele afirmaţii sunt echivalente:
(a) f este surjectivă.
(b) f este *epimorfism*, adică pentru orice mulţime Y şi orice funcţii $u, v : N \to Y$ astfel încât $uf = vf$, rezultă că $u = v$.
(c) Există o funcţie $g : N \to M$ astfel încât $fg = 1_N$.

16. Fie $f : M \to N$ o funcţie. Definim aplicaţiile $f_* : \mathcal{P}(M) \to \mathcal{P}(N)$ şi $f^* : \mathcal{P}(N) \to \mathcal{P}(M)$ prin $f_*(X) = f(X)$ şi $f^*(Y) = f^{-1}(Y)$.
(i) Să se arate că următoarele afirmaţii sunt echivalente:
  (a) f este injectivă.
  (b) f_* este injectivă.
  (c) $f^* \circ f_* = 1_{\mathcal{P}(M)}$.
  (d) f^* este surjectivă.
  (e) $f(C_M X) \subseteq C_N f(X)$ pentru orice $X \subseteq M$.

(ii) Să se arate că următoarele afirmaţii sunt echivalente:
  (a) f este surjectivă.
  (b) f_* este surjectivă.
  (c) $f_* \circ f^* = 1_{\mathcal{P}(N)}$.
  (d) f^* este injectivă.
  (e) $C_N f(X) \subseteq f(C_M X)$ pentru orice $X \subseteq M$.

17. Fie A, B, C mulţimi nevide. Să se arate că există o bijecţie între:
(a) $\mathrm{Fun}(A, \mathrm{Fun}(B, C))$ şi $\mathrm{Fun}(A \times B, C)$.
(b) $\mathrm{Fun}(A, B \times C)$ şi $\mathrm{Fun}(A, B) \times \mathrm{Fun}(A, C)$.

Dacă în plus $A \cap B = \emptyset$, atunci există o bijecţie între $\text{Fun}(A \cup B, C)$ şi $\text{Fun}(A, C) \times \text{Fun}(B, C)$.

18. Pe $\mathbb{R}$ definim relaţia $\sim$ astfel: $x \sim y$ dacă şi numai dacă $x - y \in \mathbb{Z}$. Să se arate că $\sim$ este relaţie de echivalenţă şi că există o bijecţie între mulţimea factor $\mathbb{R}/\sim$ şi intervalul $[0, 1)$.

19. Pe $\mathbb{R}$ definim relaţia ρ astfel: $x \rho y$ dacă şi numai dacă $x - y \in \mathbb{N}$. Să se arate că ρ este relaţie de ordine care nu este totală.

20. Fie M o mulţime nevidă şi ρ o relaţie binară pe M. Notăm $\Delta_M = \{(x, x) \mid x \in M\}$, $\rho^{-1} = \{(x, y) \mid y \rho x\}$ şi pentru orice număr $n \in \mathbb{N}^*$

$$\rho^n = \{(x, y) \mid \text{există } s_1, \ldots, s_{n-1} \in M \text{ cu } x \rho s_1, s_1 \rho s_2, \ldots, s_{n-1} \rho y\}$$

Să se arate că relaţia

$$\rho' = \Delta_M \cup (\rho \cup \rho^{-1}) \cup (\rho \cup \rho^{-1})^2 \cup \ldots$$

este cea mai mică relaţie de echivalenţă pe M care include pe ρ.

21. Fie $M_1, \ldots, M_n$ mulţimi nevide şi $\rho_1, \ldots, \rho_n$, respectiv, relaţii de echivalenţă pe acestea. Fie $M = M_1 \times \cdots \times M_n$ şi relaţia ρ definită pe M astfel: $(x_1, \ldots, x_n) \rho (y_1, \ldots, y_n)$ dacă şi numai dacă $x_i \rho_i y_i$ pentru orice $i = 1, ..., n$. Să se arate că ρ este relaţie de echivalenţă pe M şi că M/ρ este în bijecţie cu $M_1/\rho_1 \times \cdots \times M_n/\rho_n$.

22. Să se determine numărul relaţiilor de echivalenţă care se pot defini pe o mulţime M cu m elemente, $m \in \mathbb{N}$.

23. Fie A o mulţime nevidă, B o submulţime nevidă a sa şi ρ o relaţie pe $\mathcal{P}(A)$ definită astfel: $X \rho Y$ dacă şi numai dacă $X \cap B = Y \cap B$. Să se arate că ρ este o relaţie de echivalenţă şi că $\mathcal{P}(A)/\rho$ este în bijecţie cu $\mathcal{P}(B)$.

24. Fie A, B două mulţimi nevide şi A' o submulţime nevidă a lui A. Pe mulţimea $B^A = \{f \mid f : A \to B \text{ funcţie}\}$ considerăm relaţia binară ρ definită astfel: $f \rho g$ dacă şi numai dacă $f_{|A'} = g_{|A'}$. Să se arate că ρ este o relaţie de echivalenţă şi că B^A/ρ este în bijecţie cu $B^{A'}$.

25. Reamintim că mulţimile A şi B se numesc *echipotente* (şi notăm aceasta prin $A \sim B$) dacă există o bijecţie între A şi B. Să se arate că

pentru orice mulţimi A, B, C au loc:
(a) $A \sim A$.
(b) Dacă $A \sim B$, atunci $B \sim A$.
(c) Dacă $A \sim B$ şi $B \sim C$, atunci $A \sim C$.
Vom numi *număr cardinal* o clasă formată din toate mulţimile echipotente cu o mulţime dată A şi vom nota acest număr cardinal cu $|A|$.
Dacă A este o mulţime finită, identificăm numărul cardinal $|A|$ cu numărul elementelor lui A (care a fost notat tot cu $|A|$). Dacă A este mulţime infinită, spunem că numărul cardinal $|A|$ este *infinit*.

26. (a) (*Teorema Cantor-Schröder-Bernstein*) Fie $X_2 \subseteq X_1 \subseteq X_0$ mulţimi astfel încât $X_0 \sim X_2$. Să se arate că $X_0 \sim X_1$.
(b) Dacă $\alpha = |A|$ şi $\beta = |B|$ sunt numere cardinale, spunem că $\alpha \leq \beta$ dacă există o funcţie injectivă $f : A \to B$. Să se arate că definiţia relaţiei "$\leq$" nu depinde de reprezentanţii A şi B aleşi în cele două clase.
(c) Dacă α şi β sunt două numere cardinale astfel încât $\alpha \leq \beta$ şi $\beta \leq \alpha$, să se arate că $\alpha = \beta$.

27. Fie α şi β numere cardinale. Să se arate că are loc exact una din afirmaţiile: (i) $\alpha < \beta$ (adică $\alpha \leq \beta$ şi $\alpha \neq \beta$); (ii) $\alpha = \beta$; (iii) $\beta < \alpha$.

28. Fie X o mulţime infinită. Să se arate că:
(a) $|\mathbb{N}| \leq |X|$, adică orice mulţime infinită are o submulţime numărabilă.
(b) Dacă F este o submulţime finită a lui X, atunci $|X - F| = |X|$.

29. Fie $\alpha = |A|$ şi $\beta = |B|$ numere cardinale, reprezentanţii A şi B fiind aleşi astfel încât $A \cap B = \emptyset$. Definim *suma numerelor cardinale* α şi β prin $\alpha + \beta = |A \cup B|$. Să se arate că:
(a) Definiţia nu depinde de reprezentanţii aleşi.
(b) Dacă α, β, γ sunt numere cardinale, atunci $\alpha+\beta = \beta+\alpha$ şi $(\alpha+\beta)+\gamma = \alpha + (\beta + \gamma)$.
(c) Dacă α şi β sunt numere cardinale cu α infinit şi $\beta \leq \alpha$, atunci $\alpha+\beta = \alpha$.

30. Fie $\alpha = |A|$ şi $\beta = |B|$ două numere cardinale. Definim *produsul numerelor cardinale* α şi β prin $\alpha\beta = |A \times B|$. Să se arate că:
(a) Definiţia lui $\alpha\beta$ nu depinde de reprezentanţii A şi B aleşi.
(b) Dacă α, β, γ sunt numere cardinale, atunci $\alpha\beta = \beta\alpha$, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ şi $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

(c) Dacă α şi β sunt numere cardinale astfel încât α este infinit, $\beta \neq |\emptyset|$ şi $\beta \leq \alpha$, să se arate că $\alpha\beta = \alpha$.

31. (a) Fie α un număr cardinal şi $(A_i)_{i\in I}$ o familie de mulţimi astfel încât $|A_i| \leq \alpha$ pentru orice $i \in I$. Să se arate că $|\bigcup_{i\in I} A_i| \leq \alpha|I|$.
(b) Să se arate că o reuniune numărabilă de mulţimi cel mult numărabile este cel mult numărabilă.
(c) Dacă A este o mulţime infinită şi $\mathcal{P}_f(A)$ mulţimea tuturor submulţimilor finite ale lui A, atunci $|\mathcal{P}_f(A)| = |A|$.

32. Fie $\alpha = |A|$ şi $\beta = |B|$ două numere cardinale. Definim $\alpha^\beta = |\operatorname{Fun}(B, A)|$. Să se arate că:
(a) Definiţia lui α^β nu depinde de reprezentanţii A şi B aleşi.
(b) Dacă α, β, γ sunt numere cardinale, atunci $\alpha^{\beta+\gamma} = \alpha^\beta\alpha^\gamma$, $(\alpha\beta)^\gamma = \alpha^\gamma\beta^\gamma$ şi $(\alpha^\beta)^\gamma = \alpha^{\beta\gamma}$.
(c) Pentru orice mulţime A are loc $|\mathcal{P}(A)| = 2^{|A|}$ (prin 2 înţelegem aici numărul cardinal asociat unei mulţimi cu două elemente).

33. Să se arate că $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| < |\mathbb{R}| = |\mathbb{C}|$ şi că pentru orice $a, b \in \mathbb{R}$, $a < b$, avem $|(a, b)| = |[a, b)| = |(a, b]| = |[a, b]| = |\mathbb{R}|$.

34. Să se arate că nu există funcţii $f : \mathbb{R} \to \mathbb{R}$ cu proprietatea că $|f(x) - f(y)| > 1$ pentru orice $x, y \in \mathbb{R}, x \neq y$.

35. Fie $f : \mathbb{R} \to (0, \infty)$ o funcţie. Să se arate că există $k \in \mathbb{N}^*$ şi $a_1, \ldots, a_k \in \mathbb{R}$ distincte astfel încât $f(a_1) + \cdots + f(a_k) > 1$.

36. Pentru o funcţie $f : \mathbb{R} \to \mathbb{R}$ un element $x_0 \in \mathbb{R}$ se numeşte *punct de minim local strict* dacă există o vecinătate V_0 a sa cu proprietatea că $f(x) > f(x_0)$ pentru orice $x \in V_0 - \{x_0\}$. Analog se defineşte şi noţiunea de *punct de maxim local strict*. Un element al lui $\mathbb{R}$ care este punct de minim sau de maxim local strict se numeşte *punct de extrem local strict*.
Să se arate că mulţimea punctelor de extrem local strict ale unei funcţii $f : \mathbb{R} \to \mathbb{R}$ este cel mult numărabilă.

37. Pe $\mathbb{R}$ definim relaţia $\sim$ astfel: $x \sim y$ dacă şi numai dacă $x - y \in \mathbb{Q}$. Să se arate că $\sim$ este relaţie de echivalenţă şi că există o bijecţie între mulţimea factor $\mathbb{R}/\sim$ şi $\mathbb{R}$.

38. Să se dea exemplu de relaţie de ordine pe $\mathbb{Z}$ împreună cu care $\mathbb{Z}$ devine o mulţime bine ordonată.

Capitolul 2

Legi de compoziţie. Semigrupuri şi monoizi

• Fie M o mulţime nevidă. O funcţie $\varphi : M \times M \to M$ se numeşte *lege de compoziţie* pe M. Dacă nu menţionăm altfel, legea de compoziţie va fi notată multiplicativ, adică $\varphi(x, y) = xy$. Dacă legea de compoziţie este asociativă, adică $(xy)z = x(yz)$ pentru orice $x, y, z \in M$, atunci (M, φ) se numeşte semigrup. Dacă în plus există un element neutru $e \in M$ (pentru care $xe = ex = x$ pentru orice $x \in M$), atunci semigrupul M se numeşte monoid. Dacă nu există nici un pericol de confuzie, în loc de (M, φ) vom scrie simplu M.
• Dacă M este monoid, atunci mulţimea $U(M) = \{x \in M \mid x$ este simetrizabil$\}$ este grup cu legea de compoziţie indusă din cea a lui M şi se numeşte *grupul unităţilor* lui M.
• Fie S un semigrup. Spunem că S este *semigrup cu simplificare la stânga* dacă din $ax = ay$ rezultă $x = y$, unde $a, x, y \in S$. Analog definim şi noţiunea de *semigrup cu simplificare la dreapta*. Un semigrup cu simplificare atât la stânga cât şi la dreapta se numeşte *semigrup cu simplificare*.
• Fie S un semigrup. Un element $e \in S$ cu proprietatea că $e^2 = e$ se numeşte element *idempotent*.
• Fie S un semigrup şi S' o submulţime nevidă a sa. Dacă S' este semigrup în raport cu legea indusă (echivalent, $xy \in S'$ pentru orice $x, y \in S'$), atunci S' se numeşte *subsemigrup* al lui S. Dacă X este o submulţime a lui S, atunci intersecţia tuturor subsemigrupurilor lui S care conţin pe X se numeşte *subsemigrupul generat* de X.
• Fie M un monoid şi M' o submulţime nevidă a sa. Dacă M' este monoid

în raport cu legea indusă (echivalent, $xy \in M'$ pentru orice $x, y \in M'$ şi elementul identitate al lui M se află în M'), atunci M' se numeşte *submonoid* al lui M. Dacă X este o submulţime a lui M, atunci intersecţia tuturor submonoizilor lui M care conţin pe X se numeşte *submonoidul generat* de X.

• Dacă S, S' sunt semigrupuri şi $f : S \to S'$ o funcţie cu proprietatea că $f(xy) = f(x)f(y)$ pentru orice $x, y \in S$, atunci f se numeşte *morfism de semigrupuri*. Dacă M, M' sunt monoizi, iar $f : M \to M'$ este o funcţie cu proprietatea că $f(xy) = f(x)f(y)$ pentru orice $x, y \in M$ şi $f(e) = e'$, unde e, e' sunt elementele identitate ale celor doi monoizi, atunci f se numeşte *morfism de monoizi*.

1. Fie M o mulţime cu n elemente, $n \in \mathbb{N}^*$. Să se determine:
(i) Numărul legilor de compoziţie ce pot fi definite pe M;
(ii) Numărul legilor de compoziţie comutative ce pot fi definite pe M;
(iii) Numărul legilor de compoziţie cu element neutru ce pot fi definite pe M.

2. Fie M o mulţime înzestrată cu o lege de compoziţie (nu neapărat asociativă). Să se arate că dacă $x_1, \ldots, x_n \in M$, atunci numărul de moduri în care se pot aranja corect parantezele în produsul $x_1 x_2 \ldots x_n$ este $\frac{1}{n} C_{2n-2}^{n-1}$. (O abordare diferită pentru calculul acestui număr va fi dată în problema 38 din Capitolul 5.)

3. Fie $f : A \to B$ un morfism de monoizi. Să se arate că următoarele afirmaţii sunt echivalente:
(i) f este injectiv;
(ii) f este *monomorfism* de monoizi, adică pentru orice monoid X şi pentru orice morfisme de monoizi $u, v : X \to A$ astfel încât $fu = fv$, rezultă că $u = v$.

4. Fie $f : A \to B$ un morfism surjectiv de monoizi. Să se arate că f este *epimorfism* de monoizi, adică pentru orice monoid Y şi pentru orice morfisme de monoizi $u, v : B \to Y$ astfel încât $uf = vf$, rezultă că $u = v$.

Să se arate că morfismul incluziune $i : \mathbb{Z} \to \mathbb{Q}$, unde $\mathbb{Z}$ şi $\mathbb{Q}$ sunt considerate cu structurile de monoizi date de înmulţire, este epimorfism de monoizi, dar nu este surjectiv.

5. Fie S un semigrup. Să se arate că S se poate scufunda într-un monoid, adică există un monoid M şi un morfism injectiv de semigrupuri $f : S \to M$.

6. Fie S un semigrup cu simplificare. Să se arate că S are cel mult un element idempotent.

7. Fie S un semigrup finit şi $a \in S$. Să se arate că există $n \in \mathbb{N}^*$ astfel încât a^n să fie element idempotent.

8. Să se determine tipurile de izomorfism de semigrupuri cu două elemente.

9. Fie G un grup astfel încât orice subsemigrup generat de o mulţime finită este finit. Să se arate că orice subsemigrup al lui G este subgrup.

10. Fie S un semigrup şi $e \in S$ un element idempotent. Fie

$$H_e = \{a \in S \mid ea = ae = a \text{ şi există } x, y \in S \text{ cu } xa = ay = e\}.$$

Să se arate că:
(i) $(H_e, \cdot)$ este grup;
(ii) Dacă $H \subseteq S$, $e \in H$ şi $(H, \cdot)$ este grup, atunci $H \subseteq H_e$.

11. (i) Să se arate că un semigrup S conţine un grup (cu operaţia indusă) dacă şi numai dacă S are cel puţin un element idempotent.
(ii) Să se dea exemplu de semigrup care nu conţine niciun grup.

12. Fie S un semigrup şi $e \in S$ element idempotent.
(i) Să se arate că mulţimea $eSe = \{ese \mid s \in S\}$ este subsemigrup. Mai mult, aceasta este un monoid.
(ii) Notând cu H_e mulţimea elementelor inversabile din monoidul eSe, să se arate că H_e este grup şi H_e include orice grup $G \subseteq S$ pentru care $G \cap H_e \neq \emptyset$.

13. Fie S un semigrup. Să se arate că:
(i) Dacă S are subgrupuri (adică subsemigrupuri care împreună cu operaţia indusă sunt grupuri), atunci orice subgrup este conţinut într-un subgrup maximal.
(ii) Dacă G şi G' sunt subgrupuri maximale în S, atunci $G = G'$ sau $G \cap G' = \emptyset$.

14. Fie S un semigrup care se scrie ca o reuniune de subgrupuri. Să se arate că S se poate scrie ca reuniune de subgrupuri disjuncte.

15. Să se dea exemplu de semigrup care nu este grup şi se scrie ca o reuniune de subgrupuri.

16. Să se arate că un semigrup comutativ S se poate scufunda într-un grup dacă şi numai dacă S este semigrup cu simplificare.

17. Să se arate că legea de compoziţie dată de $(i,j)(k,l) = (i+k, 2^k j+l)$ defineşte pe $\mathbb{N} \times \mathbb{N}$ o structură de semigrup.

18. (i) Dacă X este o mulţime nevidă notăm cu $I(X)$ mulţimea funcţiilor injective $f : X \to X$. Să se arate că $(I(X), \circ)$ este monoid.
(ii) Să se arate că un semigrup S se poate scufunda într-un monoid de forma $I(X)$ dacă şi numai dacă S este semigrup cu simplificare la stânga.

19. (i) Să se arate că un monoid M se poate scufunda în monoidul $(\mathrm{Fun}(M,M), \circ)$.
(ii) Fie M un monoid finit. Dacă $a, b \in M \setminus U(M)$, atunci $ab \in M \setminus U(M)$. Arătaţi că pentru un monoid infinit această proprietate nu mai este neapărat adevărată.

20. Să se dea un exemplu de monoid M care are un element inversabil la stânga, având un număr finit > 1 de inverşi la stânga.

21. Fie $n \in \mathbb{N}^*$. Să se arate că:
(i) Există un monoid infinit cu exact n elemente inversabile;
(ii) Există un monoid finit care nu este grup şi care are exact n elemente inversabile.

22. Fie $(M, \cdot)$ un semigrup finit. Să se arate că există un şir de numere naturale $n_1 < n_2 < \ldots < n_k < \ldots$ astfel încât pentru orice $x \in M$ are loc $x^{n_1} = x^{n_2} = \ldots = x^{n_k} = \ldots$.

23. Să se arate că monoidul liber generat de o mulţime cu un element este izomorf cu $(\mathbb{N}, +)$.

24. Fie $(M, +)$ un submonoid al lui $(\mathbb{N}, +)$. Să se arate că există o submulţime finită A a lui $\mathbb{N}$ şi $d, n_0 \in \mathbb{N}$ astfel încât $M = A \cup \{nd \mid n \geq n_0\}$.

25. (i) Să se arate că monoidul $(\mathbb{N}^*, \cdot)$ este izomorf cu monoidul $(M_2, \cdot)$, unde $M_2 = \{2n+1 \mid n \geq 0\}$.
(ii) Fie $M_3 = \{3n+1 \mid n \geq 0\}$ şi $M_5 = \{5n+1 \mid n \geq 0\}$. Să se arate că $(M_3, \cdot)$ şi $(M_5, \cdot)$ sunt monoizi şi că oricare doi dintre monoizii $(\mathbb{N}^*, \cdot)$, $(M_3, \cdot)$ şi $(M_5, \cdot)$ sunt neizomorfi.

26. Fie $m, n \in \mathbb{N}$, $m, n \geq 2$ şi $M_m = \{mk+1 \mid k \in \mathbb{N}\}$, $M_n = \{nk+1 \mid k \in \mathbb{N}\}$ monoizi multiplicativi. Să se arate că aceştia sunt izomorfi dacă şi numai dacă grupurile $U(\mathbb{Z}_m)$ şi $U(\mathbb{Z}_n)$ sunt izomorfe.

27. Să se arate că există o infinitate de submonoizi ai lui $(\mathbb{N}^*, \cdot)$ care sunt izomorfi cu el şi o infinitate de submonoizi care nu sunt izomorfi cu el.

Capitolul 3

Grupuri

• Dacă G este un grup multiplicativ, atunci dacă nu se precizează altfel, elementul neutru se notează cu e (sau cu 1).
• Dacă A şi B sunt grupuri, mulţimea morfismelor de grupuri de la A la B o notăm cu $\mathrm{Hom}_{gr}(A, B)$.
• Ordinul unui element g al unui grup se notează $\mathrm{ord}(g)$.
• Scriem că H este un subgrup (normal) al lui G astfel: $H \leq G$ (respectiv $H \trianglelefteq G$).
• Dacă H este subgrup normal al lui G, notăm cu G/H *grupul factor*. Aplicaţia $p : G \to G/H$, $p(a) = \hat{a}$ pentru orice $a \in G$, este morfism de grupuri şi se numeşte *proiecţia canonică*.
• Grupurile factor au următoarea *proprietate de universalitate*: fie G, G' două grupuri, H subgrup normal al lui G şi $f : G \to G'$ morfism de grupuri cu proprietatea că $H \subseteq \mathrm{Ker}(f)$. Atunci există şi este unic un morfism de grupuri $\overline{f} : G/H \to G'$ care satisface condiţia $\overline{f}p = f$, unde $p : G \to G/H$ este proiecţia canonică.
• Un subgrup propriu H al lui G se numeşte subgrup *maximal* dacă pentru orice $K \leq G$ cu $H \subseteq K$, rezultă că $K = H$ sau $K = G$.
• Fie $Z(G) = \{x \in G \mid xg = gx \text{ pentru orice } g \in G\}$. Mulţimea $Z(G)$ se numeşte *centrul* grupului G şi este subgrup normal al lui G.
• Fie $g \in G$ şi $C(g) = \{x \in G \mid xg = gx\}$. Mulţimea $C(g)$ se numeşte *centralizatorul* elementului g şi este subgrup al lui G.
• Un grup G se numeşte *simplu* dacă singurele subgrupuri normale ale lui G sunt G şi $\{e\}$.
• Fie G un grup, $H \leq G$ şi $H_G = \bigcap_{x \in G} xHx^{-1}$. H_G se numeşte *interiorul*

normal al lui H în G.
• Spunem că un grup $(G, \cdot)$ este *divizibil* dacă pentru orice $a \in G$ şi orice $n \in \mathbb{N}^*$ ecuaţia $x^n = a$ are soluţii în G.
• Dacă X este o mulţime nevidă, mulţimea bijecţiilor de la X la X este grup cu compunerea funcţiilor. Acest grup se numeşte *grupul simetric* al mulţimii X şi se notează cu $S(X)$. Elementele lui $S(X)$ se numesc *permutări*. Dacă $X = \{1, \ldots, n\}$, atunci $S(X)$ se mai notează cu S_n. Subgrupul lui S_n care constă din toate permutările pare se notează cu A_n şi se numeşte *grupul altern* de grad n.
• Grupul izometriilor unui poligon regulat cu n laturi se numeşte *grupul diedral* de grad n şi se notează cu D_n. Acesta are $2n$ elemente şi poate fi prezentat prin doi generatori r şi s, $D_n = < r, s >$, care satisfac relaţiile $s^2 = e, r^n = e, sr = r^{n-1}s$. Geometric, s corespunde unei simetrii a poligonului regulat faţă de o axă de simetrie şi r corespunde unei rotaţii de unghi $2\pi/n$ în jurul centrului cercului circumscris poligonului.
• $GL(n, R)$ reprezintă grupul multiplicativ al matricelor inversabile de ordin n cu elemente în inelul R şi se numeşte *grupul liniar general* de ordin n peste R.

1. Fie $(S, \cdot)$ un semigrup astfel încât:
(i) Există un element $e \in S$ cu proprietatea că $ea = a$ pentru orice $a \in S$;
(ii) Pentru orice $a \in S$ există $a' \in S$ cu $a'a = e$.
Să se arate că S este grup.
Arătaţi că dacă înlocuim (ii) prin
(ii') Pentru orice $a \in S$ există $a' \in S$ cu $aa' = e$,
atunci nu mai rezultă că S este grup.

2. Fie $(S, \cdot)$ un semigrup. Arătaţi că următoarele afirmaţii sunt echivalente:
(i) S este grup;
(ii) Pentru orice $a, b \in S$ ecuaţiile $ax = b$ şi $ya = b$ au soluţii în S.

3. Fie $(S, \cdot)$ un semigrup finit cu simplificare (adică $ax = ay \Rightarrow x = y$ şi $xa = ya \Rightarrow x = y$, pentru orice $a, x, y \in S$). Să se arate că S este grup.

4. Dacă G şi G' sunt grupuri, notăm cu $\mathrm{Hom}_{gr}(G, G')$ mulţimea morfismelor de grupuri de la G la G'. Să se determine: $\mathrm{Hom}_{gr}(\mathbb{Z}, \mathbb{Z})$, $\mathrm{Hom}_{gr}(\mathbb{Z}, \mathbb{Q})$,

$\mathrm{Hom}_{gr}(\mathbb{Q},\mathbb{Z})$, $\mathrm{Hom}_{gr}(\mathbb{Q},\mathbb{Q})$, $\mathrm{Hom}_{gr}(\mathbb{Z}_n,\mathbb{Z}_n)$ şi $\mathrm{Hom}_{gr}(\mathbb{Z}_m,\mathbb{Z}_n)$, unde $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_m$ şi $\mathbb{Z}_n$ sunt considerate cu structurile aditive ($m,n\in\mathbb{N}$, $m,n>1$).

5. Să se determine care dintre următoarele grupuri sunt izomorfe: $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$, $(\mathbb{Q}_+^*,\cdot)$, $(\mathbb{R}_+^*,\cdot)$.

6. Dacă $(G,\cdot)$ este un grup şi $A,B\subset G$, notăm cu $AB=\{ab\mid a\in A \text{ şi } b\in B\}$. Presupunem că G este finit. Să se arate că:
(i) Dacă $A,B\subset G$ şi $|A|+|B|>|G|$, atunci $AB=G$;
(ii) Dacă există $M\subset G$ astfel încât $|M|>(1/2)|G|$ şi $ab=ba$ pentru orice $a,b\in M$, atunci G este comutativ.

7. Fie $(G,\cdot)$ un grup şi H o submulţime finită a lui G. Să se arate că H este subgrup dacă şi numai dacă H este parte stabilă.

8. Să se determine subgrupurile şi subgrupurile normale ale grupului diedral D_4.

9. Arătaţi că un grup nu se poate scrie ca reuniune de două subgrupuri proprii. Daţi exemple de grupuri care se scriu ca o reuniune de trei subgrupuri proprii.

10. Fie G un grup şi H,K,L trei subgrupuri ale lui G cu proprietatea că $G=H\cup K\cup L$. Arătaţi că $x^2\in H\cap K\cap L$ pentru orice $x\in G$.

11. Fie $m\in\mathbb{N}$, $m>2$ şi G un grup finit cu proprietatea că $\mathrm{ord}(x)>m$, oricare ar fi $x\in G-\{e\}$. Arătaţi că G nu se poate scrie ca reuniune de m subgrupuri proprii.

12. Fie G un grup finit. Să se arate că G are un element de ordin 2 dacă şi numai dacă $|G|$ este par.

13. Fie $(G,\cdot)$ un grup şi $f:G\to G$ definită prin $f(x)=x^2$. Atunci:
(i) f este morfism de grupuri dacă şi numai dacă G este grup abelian;
(ii) Dacă G este grup abelian finit, atunci f este izomorfism dacă şi numai dacă $|G|$ este impar.

14. Fie G un grup cu proprietatea că $x^2=e$ pentru orice $x\in G$. Să se arate că:
(i) G este grup abelian;

(ii) Dacă G este finit, atunci există $n \in \mathbb{N}$ astfel încât $|G| = 2^n$. Mai mult, în acest caz

$$G \simeq \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2,$$

produsul direct conţinând n factori.

15. Să se arate că un grup infinit are o infinitate de subgrupuri.

16. Să se determine toate grupurile care au exact două, trei, patru, respectiv cinci subgrupuri.

17. Fie G un grup generat de familia de elemente $(a_i)_{i\in I}$ şi fie $g \in G$. Să se arate că $< g >$ este subgrup normal în G dacă şi numai dacă $a_i g {a_i}^{-1} \in < g >$ şi ${a_i}^{-1} g a_i \in < g >$, pentru orice $i \in I$.

18. Fie elementele

$$\mathbf{j} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

şi

$$\mathbf{k} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

în $GL(2, \mathbb{C})$. Notăm $J = < \mathbf{j} >$, $K = < \mathbf{k} >$ şi $Q = < \mathbf{j}, \mathbf{k} >$. Să se arate că:
(i) $|J| = 4$, $|K| = 4$ şi $|J \cap K| = 2$;
(ii) J şi K sunt subgrupuri normale în Q şi $|Q| = 8$;
(iii) $\mathbf{j}^2 = \mathbf{k}^2$ este singurul element de ordin 2 din Q;
(iv) Q nu este grup abelian, dar orice subgrup al său este normal.
(Q se numeşte *grupul cuaternionilor*).

19. Fie $(G, \cdot)$ un grup şi $x, y \in G$.
(i) Dacă $xy = yx$, $\text{ord}(x)$ şi $\text{ord}(y)$ sunt finite şi $(\text{ord}(x), \text{ord}(y)) = 1$, atunci $\text{ord}(xy) = \text{ord}(x)\,\text{ord}(y)$. Dacă cele două ordine nu sunt relativ prime, mai este adevărat rezultatul?
(ii) Dacă $\text{ord}(x)$ şi $\text{ord}(y)$ sunt finite, rezultă că $\text{ord}(xy)$ este finit?
(iii) Dacă $\text{ord}(xy)$ este finit, rezultă că $\text{ord}(x)$ şi $\text{ord}(y)$ sunt finite?
(iv) Dacă G este grup abelian şi $|G| = p_1 \cdots p_n$, unde $p_1, \ldots, p_n$ sunt numere prime distincte, atunci G este grup ciclic.

20. (i) Să se arate că un grup cu 4 elemente este izomorf cu $\mathbb{Z}_4$ sau cu $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(ii) Să se arate că un grup cu 6 elemente este izomorf cu $\mathbb{Z}_6$ sau cu S_3.
(iii) Să se arate că un grup neabelian cu 8 elemente este izomorf cu D_4 sau cu Q, iar un grup abelian cu 8 elemente este izomorf cu unul din grupurile $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
(iv) Dacă p este un număr prim, atunci orice grup cu p elemente este izomorf cu $\mathbb{Z}_p$.

21. Fie X un subgrup al lui $(\mathbb{Q}, +)$ astfel încât $X + \mathbb{Z} = \mathbb{Q}$. Arătaţi că $X = \mathbb{Q}$.

22. Să se arate că dacă H este un subgrup finit generat al lui $(\mathbb{Q}, +)$, atunci H este ciclic. Deduceţi că $(\mathbb{Q}, +)$ nu este grup finit generat.

23. Să se arate că grupul $(\mathbb{Q}, +)$ nu are un sistem minimal de generatori. Mai mult, pentru orice sistem de generatori S şi orice $s \in S$ mulţimea $S - \{s\}$ este un sistem de generatori.

24. Fie G un grup finit cu $|G| > 1$ şi notăm cu $d(G)$ numărul minim de generatori ai lui G. Să se arate că $2^{d(G)} \leq |G|$.

25. Să se determine sisteme minimale de generatori pentru grupurile $S_3 \times \mathbb{Z}_4$ şi $Q \times \mathbb{Z}_3$, unde Q este grupul cuaternionilor.

26. Fie $(G, \cdot)$ un grup şi $H_1 \subset H_2 \subset \ldots \subset H_n \subset \ldots$ un şir crescător de subgrupuri. Să se arate că:
(i) $H = \bigcup_{n \geq 1} H_n$ este subgrup al lui G;
(ii) Dacă $H_n \neq H_{n+1}$ pentru orice $n \in \mathbb{N}^*$, atunci H nu este finit generat.

27. Fie $S(\mathbb{R})$ grupul simetric al mulţimii numerelor reale. Considerăm funcţiile $f, g \in S(\mathbb{R})$ definite prin $f(x) = x + 1$, $g(x) = 2x$ pentru orice $x \in \mathbb{R}$. Notăm $f_n = g^{-n} f g^n$, $G = < f, g >$ şi $H_n = < f_n >$. Să se arate că $H = \bigcup_{n \geq 1} H_n$ este un subgrup al grupului finit generat G, dar H nu este finit generat.

28. Să se arate că dacă G este un grup finit generat şi H este un subgrup de indice finit al lui G, atunci H este finit generat.

29. Fie $(G, \cdot)$ un grup şi H, K, L subgrupuri ale sale. Notăm cu $HK = \{hk \mid h \in H, k \in K\}$. Să se arate că:

(i) $|HK||H \cap K| = |H||K|$;
(ii) $[G : H \cap K] \leq [G : H][G : K]$. Dacă $[G : H]$ şi $[G : K]$ sunt finite şi prime între ele, atunci are loc chiar egalitate şi, în plus, $G = HK$;
(iii) Dacă $K \subset H$, atunci $[L \cap H : L \cap K] \leq [H : K]$.

30. (i) Fie G şi H două grupuri şi $x = (g, h) \in G \times H$ astfel încât $\text{ord}(g)$ şi $\text{ord}(h)$ să fie finite. Atunci $\text{ord}(x) = [\text{ord}(g), \text{ord}(h)]$.
(ii) Să se determine elementele de ordin 8 din $\mathbb{Z}_6 \times \mathbb{Z}_{10}$, elementele de ordin 4 din $\mathbb{Z}_{12} \times \mathbb{Z}_{15}$ şi elementele de ordin 6 din $\mathbb{Z}_{12} \times \mathbb{Z}_{36}$.

31. Fie G un grup finit cu $|G| = n$. Să se arate că:
(i) G este ciclic dacă şi numai dacă pentru orice divizor pozitiv d al lui n există cel mult un subgrup cu d elemente al lui G;
(ii) G este ciclic dacă şi numai dacă pentru orice divizor pozitiv d al lui n ecuaţia $x^d = 1$ are cel mult d soluţii în G;
(iii) Dacă G este comutativ, atunci G este ciclic dacă şi numai dacă pentru orice divizor prim p al lui n ecuaţia $x^p = 1$ are cel mult p soluţii în G.
Afirmaţia (iii) mai este adevărată dacă G nu este grup comutativ?

32. Fie K un corp comutativ. Să se arate că orice subgrup finit al grupului multiplicativ $(K^*, \cdot)$ este ciclic.

33. Fie G un grup abelian finit.
(i) Dacă există $x, y \in G$ cu $\text{ord}(x) = m$ şi $\text{ord}(y) = n$, atunci există $z \in G$ astfel încât $\text{ord}(z) = [m, n]$.
(ii) Fie $m_0 = \max\{\text{ord}(x) \mid x \in G\}$. Arătaţi că $\text{ord}(x)$ divide pe m_0, oricare ar fi $x \in G$.
(iii) Deduceţi din (i) o altă soluţie pentru exerciţiul 19(iv).
(iv) Deduceţi din (ii) o altă soluţie pentru exerciţiul 32.

34. (i) Să se arate că pentru orice $n \in \mathbb{N}^*$, grupul $(\mathbb{C}^*, \cdot)$ are exact un subgrup cu n elemente şi anume $U_n = \{z \in \mathbb{C}^* \mid z^n = 1\}$.
(ii) Dacă p este un număr prim, arătaţi că $C_{p^\infty} = \bigcup_{n \geq 0} U_{p^n}$ este un subgrup al lui $(\mathbb{C}^*, \cdot)$ care nu este finit generat.
(iii) Arătaţi că dacă H este un subgrup propriu al lui C_{p^∞}, atunci există $n \in \mathbb{N}^*$ cu $H = U_{p^n}$.
(iv) Dacă G este un subgrup infinit al lui $(\mathbb{C}^*, \cdot)$ cu proprietatea că orice subgrup propriu al său este finit, atunci există p număr prim astfel încât

$G = C_{p^\infty}$.
(v) Să se arate că pentru orice $n \in \mathbb{N}$ avem $C_{p^\infty} \cong C_{p^\infty}/U_{p^n}$.

35. (i) Să se arate că grupurile $(\mathbb{Q}, +)$ şi $(C_{p^\infty}, \cdot)$ sunt divizibile.
(ii) Să se arate că un grup divizibil netrivial (adică cu mai mult de un element) este infinit.
(iii) Să se arate că un grup factor al unui grup divizibil este divizibil. Este orice subgrup al unui grup divizibil tot un grup divizibil?
(iv) Să se dea un exemplu de grup divizibil neabelian.
(v) Să se arate că un grup divizibil nu are subgrupuri proprii de indice finit.
(vi) Să se arate că un grup divizibil nu se poate scrie ca reuniune finită de subgrupuri proprii.

36. Fie G un grup finit. Să se determine $\mathrm{Hom}_{gr}(\mathbb{Q}, G)$.

37. (i) Să se arate că dacă G este un grup finit generat şi X este un subgrup propriu al lui G, atunci există un subgrup maximal H al lui G astfel încât $X \subseteq H$. În particular, un grup netrivial finit generat are un subgrup maximal.
(ii) Să se arate că un grup abelian divizibil nu are subgrupuri maximale. În particular, grupul $(\mathbb{Q}, +)$ nu are subgrupuri maximale.

38. Fie G un grup finit. Să se arate că G are un unic subgrup maximal dacă şi numai dacă există un număr prim p şi $n \in \mathbb{N}$, $n \geq 2$, astfel încât $G \simeq \mathbb{Z}_{p^n}$.

39. Fie G un grup. Pentru $g \in G$ definim $\varphi_g : G \to G$ prin $\varphi_g(x) = gxg^{-1}$, pentru orice $x \in G$. Să se arate că:
(i) φ_g este un automorfism al lui G;
(ii) $\mathrm{Inn}(G) = \{\varphi_g \mid g \in G\}$ este un subgrup normal al lui $\mathrm{Aut}(G)$, numit *grupul automorfismelor interioare* ale lui G;
(iii) $\mathrm{Inn}(G) \simeq G/Z(G)$.

40. Fie G un grup. Să se arate că dacă $G/Z(G)$ este grup ciclic, atunci G este grup abelian.

41. Să se arate că există un grup care nu este izomorf cu $\mathrm{Aut}(G)$ pentru niciun grup G.

42. Să se arate că:
(i) $\mathrm{Aut}(\mathbb{Z})$ este izomorf cu $(\mathbb{Z}_2, +)$;
(ii) $\mathrm{Aut}(\mathbb{Q})$ este izomorf cu $(\mathbb{Q}^*, \cdot)$;
(iii) $\mathrm{Aut}(\mathbb{Z}_n)$ este izomorf cu $(U(\mathbb{Z}_n), \cdot)$;
(iv) $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ este izomorf cu grupul de permutări S_3.

43. Să se arate că $\mathrm{Aut}(S_3)$ este izomorf cu S_3 şi $\mathrm{Aut}(D_4)$ este izomorf cu D_4.

44. Să se arate că:
(i) Grupurile $\mathbb{Z}$ şi $\mathbb{Z} \times \mathbb{Z}$ nu sunt izomorfe;
(ii) Grupurile $\mathbb{Q}$ şi $\mathbb{Q} \times \mathbb{Q}$ nu sunt izomorfe;
(iii) Grupurile $\mathbb{R}$ şi $\mathbb{R} \times \mathbb{R}$ sunt izomorfe.

45. Considerăm grupurile multiplicative $S^1 = \{z \in \mathbb{C}^* \mid |z| = 1\}$ şi $U_\infty = \{z \in \mathbb{C}^* \mid \text{există } n \in \mathbb{N}^* \text{ cu } z^n = 1\}$. Să se arate că:
(i) $\mathbb{R}/\mathbb{Z}$ este izomorf cu S^1;
(ii) $\mathbb{Q}/\mathbb{Z}$ este izomorf cu U_∞;
(iii) $\mathbb{R}/\mathbb{Q}$ este izomorf cu $\mathbb{R}$;
(iv) S^1/U_∞ este izomorf cu $\mathbb{R}$.

46. Să se dea un exemplu de două grupuri neizomorfe, dar fiecare izomorf cu un grup factor al celuilalt.

47. Să se arate că grupurile $(\mathbb{C}^*, \cdot)$, $(S^1, \cdot)$ şi $(\mathbb{C}/\mathbb{Z}, +)$ sunt izomorfe.

48. Să se dea un exemplu de grup G care are două subgrupuri H şi K astfel încît K este subgrup normal în H şi H este subgrup normal în G, dar K nu este subgrup normal în G.

49. Fie G un grup şi H, K două subgrupuri. Să se arate că:
(i) Dacă $H \trianglelefteq G$, atunci $HK = KH$ şi HK este subgrup în G;
(ii) Dacă $H \trianglelefteq G$, $[G : H] < \infty$, $|K| < \infty$ şi $([G : H], |K|) = 1$, atunci $K \subseteq H$;
(iii) Dacă $H \trianglelefteq G$, $|H| < \infty$, $[G : K] < \infty$ şi $([G : K], |H|) = 1$, atunci $H \subseteq K$.

50. Să se dea un exemplu de două grupuri G_1, G_2 şi de două subgrupuri H_1, H_2 normale în G_1, respectiv G_2 astfel încât:

(i) G_1 este izomorf cu G_2, H_1 este izomorf cu H_2, dar G_1/H_1 nu este izomorf cu G_2/H_2;
(ii) G_1 este izomorf cu G_2, G_1/H_1 este izomorf cu G_2/H_2, dar H_1 nu este izomorf cu H_2.
(iii) H_1 este izomorf cu H_2, G_1/H_1 este izomorf cu G_2/H_2, dar G_1 nu este izomorf cu G_2.

51. Să se dea exemplu de două grupuri neizomorfe astfel încât fiecare să fie izomorf cu un subgrup al celuilalt.

52. Fie G un grup finit, $\alpha \in \mathrm{Aut}(G)$ şi $I = \{x \in G \mid \alpha(x) = x^{-1}\}$. Să se arate că:
(i) Dacă $|I| > (3/4)|G|$, atunci G este grup abelian;
(ii) Dacă $|I| = (3/4)|G|$, atunci G are un subgrup de indice 2.

53. Fie X, Y două mulţimi. Să se arate că dacă grupurile simetrice $S(X)$ şi $S(Y)$ sunt izomorfe, atunci X şi Y sunt echipotente.

54. Fie $n > 1$ şi $H = \{\sigma \in S_n \mid \sigma(n) = n\}$. Să se arate că:
(i) H este subgrup al lui S_n cu $(n-1)!$ elemente;
(ii) H este subgrup normal în S_n dacă şi numai dacă $n = 2$;
(iii) H este izomorf cu S_{n-1};
(iv) Se pot alege $[(n-1)!]^n$ sisteme de reprezentanţi pentru clasele la stânga (dreapta) modulo H.

55. Să se arate că $Z(S_n) = \{e\}$ pentru orice $n \geq 3$ şi $Z(A_n) = \{e\}$ pentru orice $n \geq 4$.

56. Să se arate că pentru orice grup finit G există $n \in \mathbb{N}^*$ şi un morfism injectiv de grupuri $f : G \to A_n$.

57. Fie $\tau = (i_1 \dots i_s)$ un ciclu de lungime s din S_n. Să se arate că τ^k se descompune în produs de $d = (k, s)$ cicli disjuncţi de lungime s/d.

58. Fie $\sigma \in S_n$ şi $\sigma = \pi_1 \dots \pi_r$ descompunerea sa în produs de cicli disjuncţi. Să se arate că $\mathrm{ord}(\sigma) = [\mathrm{ord}(\pi_1), \dots, \mathrm{ord}(\pi_r)]$.

59. Să se arate că $A_n = \{\sigma^2 \mid \sigma \in S_n\}$ dacă şi numai dacă $n \leq 5$.

60. Fie $\sigma \in S_n$ şi p un număr prim astfel încât p nu divide n. Dacă $\sigma^p = e$, atunci σ are cel puţin un punct fix.

61. Să se arate că S_n este generat de fiecare din următoarele mulţimi de permutări:
(i) $(12), (13), \ldots, (1n)$;
(ii) $(12), (23), \ldots, (n-1, n)$;
(iii) $(12), (12 \ldots n)$.

62. Să se arate că numărul minim de transpoziţii care generează grupul S_n este $n-1$.

63. Să se arate că A_n este generat de mulţimea ciclilor de lungime 3 pentru $n \geq 3$.

64. Să se arate că A_n este grup simplu pentru $n \geq 5$.

65. Fie $n \in \mathbb{N}$, $n \geq 3$, $n \neq 4$. Să se arate că singurele subgrupuri normale ale lui S_n sunt $\{e\}$, A_n şi S_n.

66. Fie $K = \{e, (12)(34), (13)(24), (14)(23)\} \subseteq S_4$. Să se arate că:
(i) K este subgrup normal în S_4 (deci şi în A_4);
(ii) S_4/K este izomorf cu S_3;
(iii) A_4 nu are subgrupuri de ordin 6;
(iv) K este singurul subgrup normal propriu al lui A_4;
(v) Subgrupurile normale ale lui S_4 sunt $\{e\}$, K, A_4 şi S_4.

67. Fie $n \in \mathbb{N}^*$. Să se determine:
(i) $\mathrm{Hom}_{gr}(S_n, \mathbb{Z})$;
(ii) $\mathrm{Hom}_{gr}(S_n, \mathbb{Q}^*)$;
(iii) $\mathrm{Hom}_{gr}(S_n, \mathbb{Z}_6)$.

68. Să se determine:
(i) $\mathrm{Hom}_{gr}(S_n, \mathbb{Z}_2 \times \mathbb{Z}_2)$;
(ii) $\mathrm{Hom}_{gr}(S_3, \mathbb{Z}_3)$;
(iii) $\mathrm{Hom}_{gr}(\mathbb{Z}_3, S_3)$.

69. Să se determine morfismele de grupuri $f : S_4 \to S_3$.

70. Fie $f : S_n \to G$ un morfism de grupuri, unde G are proprietatea că $H = \{x \in G \mid x^2 = e\}$ este subgrup. Arătaţi că există $a \in H$ cu $f(\sigma) = a$ pentru orice $\sigma \in S_n$ permutare impară şi $f(\sigma) = e$ pentru orice $\sigma \in S_n$ permutare pară.

71. (i) Dacă G este un subgrup al lui S_n care nu este conţinut în A_n, atunci G conţine un subgrup de indice 2.
(ii) Dacă G este un grup finit şi $|G| = 4n + 2$, atunci G conţine un unic subgrup de indice 2.

72. Să se determine centrul grupului diedral D_n, $n \geq 3$.

73. (i) Fie R un inel comutativ şi unitar. Să se determine centrul grupului $GL(n, R)$.
(ii) Să se arate că oricare două dintre grupurile $GL(2, \mathbb{Z})$, $GL(2, \mathbb{Q})$, $GL(2, \mathbb{R})$, respectiv $GL(2, \mathbb{C})$ nu sunt izomorfe.

74. Să se arate că grupurile $GL(2, \mathbb{Z})$ şi $GL(3, \mathbb{Z})$ nu sunt izomorfe.

75. Fie G un grup şi H un subgrup al său. Să se arate că:
(i) $H_G = \bigcap_{x \in G} xHx^{-1}$ este subgrup normal al lui G conţinut în H;
(ii) Dacă N este un subgrup normal al lui G conţinut în H, atunci N este conţinut în H_G;
(iii) Dacă $[G : H] = n$, să se arate că există un morfism injectiv de grupuri $f : G/H_G \to S_n$. În particular, dacă un grup are un subgrup de indice finit, atunci are un subgrup normal de indice finit.

76. Fie K corp, $G = GL(n, K)$ şi H subgrupul lui G format din matricele diagonale. Determinaţi H_G.

77. Fie $G = GL(2, \mathbb{Z}_3)$ şi

$$H = \left\{ \left(\begin{array}{cc} \hat{a} & \hat{b} \\ \hat{0} & \hat{c} \end{array} \right) \middle| \, \hat{a}\hat{c} \neq \hat{0} \right\}$$

Să se arate că H este subgrup al lui G, $|H| = 12$, $|Z(G)| = 2$ şi $H_G = Z(G)$.

78. Fie G un grup simplu infinit. Să se arate că G nu are subgrupuri proprii de indice finit.

79. Fie G un grup finit şi p cel mai mic divizor prim al lui $|G|$.
(i) Să se arate că orice subgrup de indice p este normal.
(ii) Să se arate că orice subgrup normal cu p elemente este conţinut în $Z(G)$.

80. Să se arate că un grup finit generat G are doar un număr finit de subgrupuri de indice n, unde n este un număr natural dat. Fie acestea $H_1, \ldots, H_r$ şi $H = \bigcap_{i=1}^{r} H_i$. Să se arate că pentru orice $\alpha \in \mathrm{Aut}(G)$ avem $\alpha(H) = H$.

81. Fie p un număr prim şi G un grup finit cu p^2 elemente. Arătaţi că:
(i) G este grup abelian;
(ii) G este izomorf cu $\mathbb{Z}_{p^2}$ sau cu $\mathbb{Z}_p \times \mathbb{Z}_p$.

82. Determinaţi subgrupurile Sylow ale lui S_4, respectiv A_4.

83. (i) Fie G un grup abelian finit. Atunci G este grup ciclic dacă şi numai dacă orice p-subgrup Sylow al său este ciclic.
(ii) Arătaţi că grupurile S_3 şi D_n, pentru $n > 2$ impar, au toate subgrupurile Sylow ciclice.

84. Arătaţi că S_5 nu conţine un subgrup izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

85. Fie G un grup finit, p un divizor prim al lui $|G|$ şi H un p-subgrup Sylow al lui G. Să se arate că:
(i) Dacă $n_p = 1$, atunci H este normal în G;
(ii) Dacă $|H| = p$, atunci numărul elementelor de ordin p din G este $n_p(p-1)$.

86. (i) Fie N şi H două grupuri şi $\varphi : H \to \mathrm{Aut}(N)$ un morfism de grupuri. Să se arate că $G = N \times H$ este grup în raport cu operaţia

$$(n_1, h_1) * (n_2, h_2) = (n_1\varphi(h_1)(n_2), h_1h_2).$$

Acest grup se notează cu $N \rtimes_\varphi H$ şi se numeşte *produsul semidirect extern* al lui N cu H.
Dacă $N' = \{(n, e_H) \mid n \in N\}$ şi $H' = \{(e_N, h) \mid h \in H\}$, atunci $N' \trianglelefteq G$, $H' \leq G$, $G = N'H'$ şi $N' \cap H' = \{(e_N, e_H)\}$.
(ii) Fie G un grup şi H, N subgrupuri ale lui G, $N \trianglelefteq G$, cu proprietatea că $G = NH$ şi $N \cap H = \{e\}$. (Se spune că G este *produsul semidirect intern* al lui N cu H.)
Să se arate că $G \simeq N \rtimes_\varphi H$, unde $\varphi : H \to \mathrm{Aut}(N)$ este dată prin $\varphi(h)(n) = hnh^{-1}$.

87. (i) Fie p şi q numere prime astfel încât $p < q$ şi p nu divide pe $q - 1$. Să se arate că orice grup cu pq elemente este ciclic.

(ii) Fie p şi q numere prime astfel încât $p < q$ şi p divide pe $q - 1$. Să se arate că orice grup cu pq elemente este izomorf cu un produs semidirect al grupurilor $\mathbb{Z}_q$ şi $\mathbb{Z}_p$. Deduceţi că există exact două tipuri de izomorfism de grupuri cu pq elemente.

88. Fie p, q, r trei numere prime distincte şi G un grup cu proprietatea că $|G| \in \{p^n, pq, p^2q, pqr\}$, unde $n > 1$. Să se arate că G nu este grup simplu.

89. (i) Fie $G_1, \ldots, G_n$ grupuri finite, $G = G_1 \times \cdots \times G_n$ produsul lor direct şi p un divizor prim al lui $|G|$. Să se arate că un subgrup H al lui G este p-subgrup Sylow dacă şi numai dacă $H = H_1 \times \cdots \times H_n$, unde H_i este p-subgrup Sylow al lui G_i sau $H_i = \{e\}$, $i = 1, \ldots, n$.
(ii) Determinaţi subgrupurile Sylow ale lui $\mathbb{Z}_6 \times S_3$.

90. Fie G un grup cu $|G| = p_1 \cdots p_n$, unde $p_1, \ldots, p_n$ sunt numere prime distincte. Fie $H_1, \ldots, H_n$ subgrupuri Sylow corespunzătoare acestor numere prime. Să se arate că dacă orice subgrup H_i este normal în G, atunci G este grup abelian izomorf cu $H_1 \times \cdots \times H_n$.

Capitolul 4

Inele şi corpuri

• Prin *inel* vom înţelege o mulţime R înzestrată cu două legi de compoziţie: adunarea "$+$" şi înmulţirea "$\cdot$", astfel încât $(R, +)$ este grup abelian, iar înmulţirea este asociativă şi distributivă la stânga şi la dreapta faţă de adunare. Dacă, în plus, există un element neutru pentru înmulţire (notat de obicei cu 1), atunci $(R, +, \cdot)$ se numeşte *inel unitar*.
• Dacă R şi S sunt inele, un *morfism* de inele $f : R \to S$ este o funcţie pentru care $f(a+b) = f(a)+f(b)$ şi $f(ab) = f(a)f(b)$ pentru orice $a, b \in R$. Dacă R şi S sunt inele unitare şi morfismul de inele $f : R \to S$ verifică şi $f(1_R) = 1_S$ (unde 1_R şi 1_S sunt elementele identitate la înmulţire pentru R şi S), atunci f se numeşte *morfism unitar* de inele. Dacă R şi S sunt inele unitare, atunci, dacă nu precizăm altfel, prin morfism de inele de la R la S se înţelege morfism unitar.
• Pentru orice submulţime nevidă A a unui inel R se notează $C_R(A) = \{r \in R \mid ra = ar \text{ pentru orice } a \in A\}$ şi se numeşte *centralizatorul* lui A în R. În particular, $C_R(R)$, care se notează cu $Z(R)$ (sau $C(R)$), se numeşte *centrul* lui R.
• Fie R un inel unitar. Un element $x \in R$ se numeşte *inversabil la stânga* (respectiv la *dreapta*) dacă există $y \in R$ astfel încât $yx = 1$ (respectiv $xy = 1$). Elementul y se numeşte *invers la stânga* (respectiv *la dreapta*) al lui x. Dacă x este inversabil la stânga şi la dreapta, atunci se numeşte element *inversabil*.
• Fie R un inel. Un element $a \in R$ se numeşte *divizor al lui zero la stânga* (respectiv *la dreapta*) dacă există $b \in R$, $b \neq 0$, astfel încât $ab = 0$ (respectiv $ba = 0$). Dacă a este divizor al lui zero la stânga şi la dreapta, atunci se numeşte *divizor al lui zero*. (De exemplu, 0 este divizor al lui zero.) Un

element care nu este divizor al lui zero nici la stânga şi nici la dreapta se numeşte *nondivizor al lui zero* sau element *regulat*. Un inel fără divizori ai lui zero la stânga şi la dreapta (diferiţi de 0) se numeşte *inel integru*. (Echivalent, dacă $ab = 0$, atunci $a = 0$ sau $b = 0$.) Un inel integru comutativ (cu $0 \neq 1$) se numeşte *domeniu de integritate*.

• Fie R un inel şi $x \in R$. x se numeşte *nilpotent* dacă există un $n \in \mathbb{N}$ astfel încât $x^n = 0$. Cel mai mic n cu proprietatea că $x^n = 0$ se numeşte *indicele de nilpotenţă* al lui x. Elementul x se numeşte *idempotent* dacă $x^2 = x$.

• Fie R un inel şi $I \subseteq R$, $I \neq \emptyset$. I se numeşte *ideal stâng* (respectiv *ideal drept*) al lui R dacă $x - y \in I$ pentru orice $x, y \in I$ şi $ax \in I$ (respectiv $xa \in I$) pentru orice $a \in R$, $x \in I$. Dacă I este şi ideal stâng şi ideal drept, atunci se numeşte *ideal bilateral*. Dacă R este inel comutativ, atunci cele trei definiţii de mai sus coincid şi spunem că I este *ideal*.

• Dacă I este ideal bilateral în inelul R, notăm cu R/I *inelul factor*. Aplicaţia $p : R \to R/I$, $p(a) = \hat{a}$ pentru orice $a \in R$, este morfism de inele şi se numeşte *proiecţia canonică*.

• Inelele factor au următoarea *proprietate de universalitate*: fie R, R' două inele, I ideal bilateral al lui R şi $f : R \to R'$ morfism de inele cu proprietatea că $I \subseteq \mathrm{Ker}(f)$. Atunci există şi este unic un morfism de inele $\overline{f} : R/I \to R'$ care satisface condiţia $\overline{f}p = f$, unde $p : R \to R/I$ este proiecţia canonică.

• (*Teorema a III-a de izomorfism pentru inele*) Dacă R este un inel şi $I \subseteq J$ două ideale bilaterale ale sale, atunci există un izomorfism canonic $\frac{R/I}{J/I} \simeq R/J$.

• Fie $u : R \to S$ un morfism de inele comutative.

Pentru orice ideal I al lui R vom nota cu I^e idealul lui S generat de $u(I)$. I^e se numeşte *extensia* lui I prin morfismul u.

Pentru orice ideal J al lui S vom nota $J^c = u^{-1}(J)$. J^c se numeşte *contracţia* lui J prin morfismul u.

• Fie R un inel comutativ şi $P \subseteq R$ un ideal.

P se numeşte *ideal prim* dacă $P \neq R$ şi $ab \in P$ implică $a \in P$ sau $b \in P$, unde $a, b \in R$. Echivalent, R/P este domeniu de integritate.

P se numeşte *ideal maximal* dacă $P \neq R$ şi nu există un alt ideal propriu al lui R care să conţină strict pe P. Echivalent, R/P este corp.

• Pentru un inel R se vor folosi următoarele notaţii:

$U(R)$ = mulţimea elementelor inversabile din R,

$D(R)$ = mulţimea divizorilor lui zero din R,

$N(R)$ = mulţimea elementelor nilpotente din R,

$\mathrm{Idemp}(R)$ = mulţimea elementelor idempotente din R,
$\mathrm{Spec}(R)$ = mulţimea idealelor prime ale lui R,
$\mathrm{Max}(R)$ = mulţimea idealelor maximale ale lui R.
• Dacă I şi J sunt ideale în inelul comutativ R, notăm cu IJ mulţimea elementelor lui R de forma $x_1y_1 + \ldots + x_ny_n$, cu $n \in \mathbb{N}^*$, $x_1, \ldots, x_n \in I$ şi $y_1, \ldots, y_n \in J$, iar cu $I + J$ mulţimea elementelor lui R de forma $x + y$, cu $x \in I$ şi $y \in J$. Atunci IJ (respectiv $I + J$) este ideal al lui R şi se numeşte *produsul* (respectiv *suma*) idealelor I şi J. Puterile I^n ale idealului I se definesc recurent prin $I^1 = I$ şi $I^n = II^{n-1}$ pentru $n \geq 2$.
• Fie R un inel comutativ unitar. R se numeşte *inel noetherian* dacă orice şir crescător de ideale ale lui R este staţionar, adică dacă $I_0 \subseteq I_1 \subseteq \ldots I_n \subseteq \ldots$ sunt ideale ale lui R, atunci există $n_0 \in \mathbb{N}$ astfel încât $I_n = I_{n+1}$ pentru orice $n \geq n_0$.

1. Să se determine numărul structurilor neizomorfe de inel care pot fi definite pe o mulţime cu p elemente, unde p este un număr prim.

2. Să se determine numărul structurilor de inel unitar ce pot fi definite pe $(\mathbb{Z}_n, +)$ şi să se arate că acestea sunt izomorfe.

3. Fie R un inel cu grupul $(R, +)$ ciclic. Să se arate că R este inel comutativ. În particular, orice inel cu $p_1 \cdots p_n$ elemente, unde $p_1, \ldots, p_n$ sunt numere prime distincte, este comutativ.

4. Să se arate că orice inel unitar cu p^2 elemente este comutativ, unde p este un număr prim. Să se arate că există inele neunitare cu p^2 elemente care nu sunt comutative.

5. Fie p un număr prim. Să se arate că există un inel unitar cu p^3 elemente care nu este comutativ.

6. Fie R un inel. Să se arate că există un inel unitar S astfel încât R este izomorf cu un subinel al lui S. Mai mult, dacă există $n \in \mathbb{N}^*$ astfel ca $nr = 0$ pentru orice $r \in R$, atunci S poate fi ales astfel ca $ns = 0$ pentru orice $s \in S$.

7. Fie R un inel. Să se arate că există un inel unitar S şi un morfism de inele $\phi : R \to S$ cu proprietatea că pentru orice inel unitar A şi orice morfism

de inele $\alpha : R \to A$ există un morfism unitar de inele $\bar{\alpha} : S \to A$ astfel încât $\bar{\alpha}\phi = \alpha$. Mai mult, S este unic până la un izomorfism.

8. (i) Să se determine în inelul $\mathbb{Z}_n$ elementele inversabile, elementele nilpotente, divizorii lui zero şi să se afle numărul acestora.
(ii) Să se dea exemplu de două inele neizomorfe cu exact 36 de elemente nilpotente.

9. Se consideră numărul natural n care are r factori primi distincţi în descompunerea sa. Să se arate că numărul idempotenţilor lui $\mathbb{Z}_n$ este 2^r. Să se determine idempotenţii inelului $\mathbb{Z}_{72}$.

10. Fie R un inel unitar. Dacă există un element în R care este inversabil la stânga şi nu este inversabil la dreapta, atunci acesta are o infinitate de inverşi la stânga. În particular, dacă un element din R are cel puţin doi inverşi la stânga, atunci el are o infinitate de inverşi la stânga.

11. Să se arate că într-un inel unitar finit orice element nenul este fie inversabil, fie divizor al lui zero la stânga sau la dreapta. În particular, orice inel integru finit este corp.

12. Fie R un inel unitar care are un număr finit, strict mai mare decât 1, de divizori ai lui zero la stânga sau la dreapta. Să se arate că R este finit. Mai mult, dacă $|R| = n$, atunci $|U(R)| \leq n - [\sqrt{n}]$.

13. Fie R un inel unitar şi $a, b \in R$. Să se arate că:
(i) Dacă $1 - ba$ are un invers la stânga (dreapta), atunci şi $1 - ab$ are un invers la stânga (dreapta).
(ii) $1 - ba$ este inversabil dacă şi numai dacă $1 - ab$ este inversabil.

14. Fie R un inel. Definim pe R legea de compoziţie "$\circ$" astfel: $a \circ b = a + b - ab$, $a, b \in R$. Să se arate că:
(i) $(R, \circ)$ este monoid.
(ii) Dacă R este inel unitar, monoizii $(R, \circ)$ şi $(R, \cdot)$ sunt izomorfi.
(iii) Convenim să numim *element quasi-regulat la stânga (dreapta)* un element inversabil la stânga (dreapta) în monoidul $(R, \circ)$. Să se arate că pentru orice $a, b \in R$, ab este quasi-regulat la stânga (dreapta) dacă şi numai dacă ba este quasi-regulat la stânga (dreapta).
(iv) Orice element nilpotent din R este quasi-regulat la stânga şi la dreapta.

15. Fie R un inel unitar. Să se demonstreze echivalenţa următoarelor afirmaţii:
(i) R este corp;
(ii) Pentru orice $a \in R \setminus \{1\}$ există $b \in R$ astfel încât $a + b = ab$;
(iii) Pentru orice $a \in R \setminus \{1\}$ există $b \in R$ astfel încât $a + b = ba$.

16. Fie R un inel unitar şi $u, v \in R$. Să se arate că următoarele afirmaţii sunt echivalente:
(i) u este inversabil şi $v = u^{-1}$;
(ii) $uvu = u$ şi $vu^2v = 1$;
(iii) $uvu = u$ şi v este unic cu această proprietate.

17. Să se determine endomorfismele unitare ale inelelor $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

18. (i) Fie R un inel. Să se arate că există o corespondenţă bijectivă între mulţimea morfismelor de inele (nu neapărat unitare, chiar dacă R este unitar) $f : \mathbb{Z} \to R$ şi mulţimea $\mathrm{Idemp}(R)$.
(ii) Să se arate că există o corespondenţă bijectivă între mulţimea morfismelor de inele $f : \mathbb{Z}_m \to \mathbb{Z}_n$ şi $\mathrm{Idemp}(\mathbb{Z}_n) \cap \{\hat{a} \in \mathbb{Z}_n \mid m\hat{a} = 0\}$. Să se determine numărul de elemente al acestei mulţimi.

19. Fie R, S inele unitare şi $f : R \to S$ un morfism de inele unitare.
(i) Să se arate că f este injectiv dacă şi numai dacă f este *monomorfism* de inele unitare, adică pentru orice inel unitar A şi pentru orice morfisme unitare de inele $u, v : A \longrightarrow R$ astfel încât $fu = fv$, rezultă că $u = v$.
(ii) Să se arate că dacă f este surjectiv, atunci f este *epimorfism* de inele unitare, adică pentru orice inel unitar A şi pentru orice morfisme unitare de inele $u, v : S \longrightarrow A$ astfel încât $uf = vf$, rezultă că $u = v$.
Să se dea exemplu de epimorfism de inele unitare care nu este surjectiv.

20. Fie R un inel comutativ unitar. Să se arate că:
(i) $\mathrm{Idemp}(R)$ are o structură de grup în raport cu legea de compoziţie "$*$" definită prin: $e * f = e + f - 2ef$ pentru orice $e, f \in \mathrm{Idemp}(R)$.
(ii) Dacă R are un număr finit de idempotenţi, atunci există $n \in \mathbb{N}^*$ astfel încât $|\mathrm{Idemp}(R)| = 2^n$.

21. Fie $C = \{f \mid f : [0, 1] \to \mathbb{R}, f \text{ funcţie continuă}\}$ cu structura de inel unitar dată de adunarea şi înmulţirea funcţiilor. Dacă $t \in [0, 1]$ notăm cu $\phi_t : C \to \mathbb{R}$ aplicaţia dată de $\phi_t(f) = f(t)$. Să se arate că:

(i) ϕ_t este morfism de inele.
(ii) Orice morfism de inele $\phi : C \to \mathbb{R}$ este de forma ϕ_t pentru un $t \in [0, 1]$.

22. Fie $u : R \to S$ un morfism de inele comutative.
(i) Arătaţi că dacă J este ideal al lui S, atunci $u^{-1}(J)$ este ideal al lui R.
(ii) Arătaţi că dacă I este ideal al lui R, atunci $u(I)$ nu este neapărat ideal al lui S.
(iii) Arătaţi că $I^e = \{\sum_{i=1}^{n} u(x_i) \mid n \in \mathbb{N}, i \in S, x_i \in I\}$.
(iv) Arătaţi că pentru orice ideal I al lui R avem $I \subset (I^e)^c$; daţi exemple de situaţii când această incluziune este strictă.
(v) Arătaţi că pentru orice ideal J al lui S avem $(J^c)^e \subset J$; daţi exemple de situaţii când această incluziune este strictă.
(vi) Arătaţi că pentru orice ideal I al lui R avem $((I^e)^c)^e = I^e$.
(vii) Arătaţi că pentru orice ideal J al lui S avem $((J^c)^e)^c = J^c$.

23. Fie R un inel comutativ şi I, J ideale ale lui R. Să se arate că:
(i) Dacă se consideră I^e, extinsul lui I via proiecţia canonică $\pi : R \to R/J$, atunci $I^e = \overline{I}\,\overline{R}$, unde $\overline{I} = \pi(I)$ şi $\overline{R} = R/J$.
(ii) $I^e = (I + J)/J$.
(iii) $\overline{R}/\overline{I}\,\overline{R} \simeq R/(I + J)$.

24. (i) Arătaţi că un inel R este noetherian dacă şi numai dacă orice ideal al său este finit generat.
(ii) (*Cohen*) Arătaţi că R este noetherian dacă şi numai dacă orice ideal prim al său este finit generat.
(iii) Arătaţi că orice inel factor al unui inel noetherian este noetherian.

25. Să se determine idealele, idealele prime şi idealele maximale din $\mathbb{Z}_n$ şi numărul lor, unde $n \in \mathbb{N}, n \geq 2$.

26. (i) Fie $R_1, \ldots, R_n$ inele unitare şi $R = R_1 \times \cdots \times R_n$. Să se arate că idealele lui R sunt de forma $I = I_1 \times \cdots \times I_n$, unde $I_1, \ldots, I_n$ sunt ideale în $R_1, \ldots, R_n$, respectiv.
(ii) Cu notaţiile de la punctul (i) să se arate că inelele R/I şi $R_1/I_1 \times \cdots \times R_n/I_n$ sunt izomorfe.
(iii) Să se arate că rezultatul de la (i) nu mai rămâne adevărat când avem un produs infinit de inele.

27. Fie R un inel comutativ. Un ideal I al lui R se numeşte *ideal nilpotent* dacă există $n \in \mathbb{N}^*$ astfel încât $I^n = 0$. Să se arate că:
(i) Suma a două ideale nilpotente este un ideal nilpotent.
(ii) Dacă I este un ideal finit generat, atunci I este nilpotent dacă şi numai dacă orice element al său este nilpotent.
Dacă I nu este finit generat mai rămâne adevărată afirmaţia?

28. Fie R un inel comutativ şi unitar şi $I_1, \ldots, I_n$ ideale în R. Considerăm morfismul de inele $\phi : R \to R/I_1 \times \cdots \times R/I_n$ definit astfel: $\phi(x) = (x \pmod{I_1}, \ldots, x \pmod{I_n})$. Să se arate că:
(i) $\mathrm{Ker}(\phi) = I_1 \cap \ldots \cap I_n$.
(ii) ϕ este surjectiv dacă şi numai dacă idealele $I_1, \ldots, I_n$ sunt oricare două *comaximale* (adică $I_j + I_k = R$ pentru orice $j \neq k$).
(iii) (*Lema chineză a resturilor*) Dacă idealele date sunt oricare două comaximale, atunci ϕ induce un izomorfism între inelele $R/I_1 \cap \ldots \cap I_n$ şi $R/I_1 \times \cdots \times R/I_n$.

29. Fie R un inel comutativ şi unitar. Să se arate că următoarele afirmaţii sunt echivalente:
(i) R are un singur ideal maximal;
(ii) $R \setminus U(R)$ este ideal în R;
(iii) Dacă $a, b \in R$ şi $a + b \in U(R)$ atunci $a \in U(R)$ sau $b \in U(R)$.
Un inel care verifică una dintre condiţiile echivalente de mai sus se numeşte *inel local*.

30. Să se arate că un inel local are doar idempotenţii 0 şi 1.

31. Să se arate că inelul $\mathbb{Z}_n$ este local dacă şi numai dacă n este putere a unui număr prim.

32. Fie R un inel unitar.
(i) Dacă $a, b \in R$ şi $ab \in U(R)$, rezultă că $a, b \in U(R)$?
(ii) Dacă $a \in R$ şi $a^n \in U(R)$, să se arate că $a \in U(R)$.
(iii) Dacă a este inversabil la stânga şi nu este divizor al lui zero la dreapta, atunci $a \in U(R)$.

33. Să se dea un exemplu de inel R şi $x \in R$ astfel încât $Rx \subseteq xR$ dar $Rx \neq xR$.

34. Fie R un inel. Un element $e \in R$ se numeşte *element identitate la stânga* (respectiv *la dreapta*) dacă $er = r$ (respectiv $re = r$) pentru orice $r \in R$.
(i) Să se arate că un element identitate la stânga nu este neapărat şi element identitate la dreapta.
(ii) Dacă $e \in R$ este unicul element identitate la stânga, atunci e este şi element identitate la dreapta.

35. Fie R un inel şi A o submulţime nevidă a lui R. Să se arate că:
(i) $C_R(A)$ este subinel al lui R. În particular, $Z(R)$ este subinel.
(ii) $C_R(C_R(C_R(A))) = C_R(A)$.

36. Fie R un inel unitar care nu are alte ideale bilaterale în afară de (0) şi R. Să se arate că centrul lui R este corp. În particular, un inel comutativ unitar care nu are alte ideale în afară de (0) şi R este corp.

37. Fie D un corp. Se numeşte *comutator aditiv* în D un element de forma $xa - ax$ cu $x, a \in D$. Să se arate că dacă un element $y \in D$ comută cu toţi comutatorii aditivi ai lui D, atunci $y \in Z(D)$.

38. Fie D un corp. Pentru orice $a \in D$ fie aplicaţia $\delta_a : D \to D$ definită prin $\delta_a(x) = ax - xa$. Să se arate că:
(i) $\delta_a(x+y) = \delta_a(x) + \delta_a(y)$ şi $\delta_a(xy) = x\delta_a(y) + \delta_a(x)y$ pentru orice $a, x, y \in D$.
(ii) Dacă D are caracteristica diferită de 2 şi K este un subcorp al lui D pentru care $\delta_a(K) \subseteq K$ pentru orice $a \in D$, atunci $K \subseteq Z(D)$.

39. Fie D un corp. Se numeşte *comutator multiplicativ* în D un element de forma $a^{-1}bab^{-1}$, cu $a, b \in D \setminus \{0\}$. Să se arate că dacă un element $c \in D$ comută cu toţi comutatorii multiplicativi din D, atunci $c \in Z(D)$.

40. Fie D un corp şi K un subcorp al lui D pentru care $xKx^{-1} \subseteq K$ oricare ar fi $x \in D$. Atunci $K \subseteq Z(D)$.

41. Fie R un inel unitar şi I un ideal bilateral cu proprietatea că $I \subseteq N(R)$. Atunci orice idempotent din R/I se ridică la un idempotent în R (adică pentru orice $f \in R/I$ cu $f^2 = f$, există $e \in R$ cu $e^2 = e$ astfel încât $f = \hat{e}$).

42. Fie R un inel comutativ şi unitar, P un ideal prim al său şi I idealul generat de elementele idempotente din P. Să se arate că R/I nu are idempotenţi netriviali (adică diferiţi de 0 şi 1).

43. Fie R un inel unitar. R se numeşte *inel Boole* dacă $x^2 = x$ pentru orice $x \in R$. Să se arate că:
(i) Dacă R este inel Boole, atunci R este comutativ şi $2x = 0$ pentru orice $x \in R$.
(ii) $\mathrm{Spec}(R) = \mathrm{Max}(R)$.
(iii) Dacă X este o mulţime, atunci $(\mathcal{P}(X), \Delta, \cap)$ este inel Boole.
(iv) Dacă R este inel Boole finit, atunci există o mulţime finită X cu proprietatea că R este izomorf cu $(\mathcal{P}(X), \Delta, \cap)$. În particular, un inel Boole finit are 2^r elemente, $r \in \mathbb{N}$.
(v) Pe orice mulţime infinită X se poate defini o structură de inel Boole.

44. Fie R un inel comutativ şi unitar.
(i) Să se arate că $N(R)$ coincide cu intersecţia idealelor prime ale lui R. În particular, $N(R)$ este ideal.
(ii) Dacă $x \in N(R)$ şi $u \in U(R)$, atunci $x + u \in U(R)$.
(iii) Dacă $J(R)$ este *radicalul Jacobson* al lui R, definit ca fiind intersecţia idealelor maximale ale lui R, atunci

$$J(R) = \{x \in R \mid 1 - ax \in U(R) \text{ pentru orice } a \in R\}.$$

(iv) Să se dea exemple de inele R pentru care $N(R) \neq J(R)$ şi de inele R pentru care $N(R) = J(R)$.

45. Fie $R_1, \ldots, R_n$ inele comutative unitare şi $R = R_1 \times \cdots \times R_n$. Atunci:
(i) P este ideal prim al lui R dacă şi numai dacă există $1 \leq i \leq n$ şi P_i ideal prim al lui R_i astfel încât $P = R_1 \times \cdots \times R_{i-1} \times P_i \times R_{i+1} \times \cdots \times R_n$.
(ii) M este ideal maximal al lui R dacă şi numai dacă există $1 \leq i \leq n$ şi M_i ideal maximal al lui R_i astfel încât $M = R_1 \times \cdots \times R_{i-1} \times M_i \times R_{i+1} \times \cdots \times R_n$.
(iii) $N(R) = N(R_1) \times \cdots \times N(R_n)$ şi $J(R) = J(R_1) \times \cdots \times J(R_n)$.

46. Dacă $R = \mathbb{Z}_{20} \times \mathbb{Q} \times \mathbb{Z}_{19}$, să se determine idealele lui R, inelele factor ale lui R, $\mathrm{Spec}(R)$, $\mathrm{Max}(R)$, $N(R)$, $J(R)$ şi $\mathrm{Idemp}(R)$.

47. Fie R un inel comutativ unitar şi I un ideal al său. Definim

$$\mathrm{Rad}(I) = \{a \in R \mid \text{ există } n \in \mathbb{N} \text{ astfel încât } a^n \in I\}.$$

Să se arate că:
(i) $\mathrm{Rad}(I)$ este ideal al lui R şi $I \subseteq \mathrm{Rad}(I)$.
(ii) $N(R/I) = \mathrm{Rad}(I)/I$.
(iii) $\mathrm{Rad}(I) = \bigcap_{P \in V(I)} P$, unde $V(I) = \{P \mid P \text{ este ideal prim şi } I \subseteq P\}$.
(iv) $\mathrm{Rad}(I) = \mathrm{Rad}(\mathrm{Rad}(I))$ şi $\mathrm{Rad}(I) \subseteq \mathrm{Rad}(J)$ dacă şi numai dacă $V(J) \subseteq V(I)$.
(v) $\mathrm{Rad}(IJ) = \mathrm{Rad}(I \cap J) = \mathrm{Rad}(I) \cap \mathrm{Rad}(J)$ şi $\mathrm{Rad}(I+J) = \mathrm{Rad}(\mathrm{Rad}(I) + \mathrm{Rad}(J))$.

48. Dacă R este un inel comutativ unitar integru infinit cu $|U(R)| < \infty$, să se arate că R are o infinitate de ideale maximale.

49. Fie $R = d\mathbb{Z}/n\mathbb{Z}$ inel comutativ neunitar cu $n = dm$, m fiind un număr natural nenul care nu este prim. Să se arate că:
(i) Idealele lui R sunt de forma $kd\mathbb{Z}/n\mathbb{Z}$, unde $k|m$.
(ii) Idealele prime ale lui R sunt de forma $pd\mathbb{Z}/n\mathbb{Z}$, unde p este un număr prim, $p|m$ şi p nu divide pe d.
(iii) Idealele maximale ale lui R sunt de forma $pd\mathbb{Z}/n\mathbb{Z}$, unde p este un număr prim şi $p|m$.
Deci $\mathrm{Spec}(R) \subset \mathrm{Max}(R)$ şi $\mathrm{Spec}(R) \neq \mathrm{Max}(R)$.

50. Fie $R = n\mathbb{Z}$ inel comutativ neunitar. Să se arate că:
(i) Idealele lui R sunt de forma $kn\mathbb{Z}$, $k \in \mathbb{Z}$.
(ii) Idealele prime nenule ale lui R sunt de forma $pn\mathbb{Z}$, unde p este număr prim astfel încât p nu divide pe n.
(iii) Idealele maximale ale lui R sunt de forma $pn\mathbb{Z}$, unde p este un număr prim.
Deci $\mathrm{Spec}(R) \setminus \{0\} \subset \mathrm{Max}(R)$ şi $\mathrm{Spec}(R) \setminus \{0\} \neq \mathrm{Max}(R)$.

51. Să se dea exemplu de inel (neunitar) care nu are ideale maximale.

52. Fie $A_1, \ldots, A_m, B_1, \ldots, B_n$ inele comutative unitare care nu au idempotenţi netriviali (adică diferiţi de 0 şi 1). Atunci $A_1 \times \cdots \times A_m \simeq B_1 \times \cdots \times B_n$ dacă şi numai dacă $m = n$ şi există $\sigma \in S_n$ astfel încât $A_i \simeq B_{\sigma(i)}$ pentru orice $1 \leq i \leq n$.

53. Fie $k \subset K, k \neq K$ două corpuri. Să se arate că dacă $[K^* : k^*] < \infty$, atunci $|k| < \infty$.

54. Să se arate că un corp K nu se poate scrie ca reuniune finită de subcorpuri proprii.

55. Fie K un corp finit de caracteristică 3. Arătaţi că există $x, y \in K$ cu proprietatea că $x^2 + y^2 \neq a^2$ pentru orice $a \in K$.

Capitolul 5

Construcţii de inele: inele de matrice, inele de polinoame, inele de serii formale şi inele de fracţii

În acest capitol prin inel vom înţelege inel unitar, iar prin morfism de inele morfism unitar. (Uneori vom preciza acest lucru şi în mod explicit.) În problemele în care se va lucra cu inele neunitare acest lucru va fi menţionat explicit.

• Prin $R[X_1, \ldots, X_n]$, $n \in \mathbb{N}^*$, vom nota inelul polinoamelor în nedeterminatele $X_1, \ldots, X_n$ cu coeficienţi într-un inel R. Pentru $n = 1$ notăm $R[X]$. Putem considera că $R[X_1, \ldots, X_n] \subset R[X_1, \ldots, X_{n+1}]$ pentru orice $n \in \mathbb{N}^*$ şi definim $R[X_1, \ldots, X_n, \ldots] = \bigcup_{n \geq 1} R[X_1, \ldots, X_n]$ *inelul de polinoame într-o infinitate numărabilă de nedeterminate* peste R.

Inelele de polinoame au următoarea *proprietate de universalitate*: pentru orice morfism de inele $f : R \to S$ şi pentru orice elemente $s_1, \ldots, s_n \in S$, există şi este unic un morfism $\overline{f} : R[X_1, \ldots, X_n] \to S$ astfel încât $\overline{f}\epsilon = f$ (unde $\epsilon : R \to R[X_1, \ldots, X_n]$, $\epsilon(a) = a$ pentru orice $a \in R$, este morfismul canonic) şi $\overline{f}(X_i) = s_i$ pentru orice $i = 1, \ldots, n$.

Dacă $f \in R[X_1, \ldots, X_n]$ şi $1 \leq i \leq n$ fixat, atunci prin $\deg_{X_i}(f)$ notăm *gradul* lui f considerat ca polinom în nedeterminata X_i cu coeficienţi în inelul format cu celelalte nedeterminate.

Dacă I este ideal (stâng, drept, bilateral) al lui R, atunci prin $I[X_1, \ldots, X_n]$

notăm mulţimea polinoamelor din $R[X_1, \ldots, X_n]$ cu toţi coeficienţii în I. Se observă că $I[X_1, \ldots, X_n]$ este ideal (stâng, drept, bilateral) al inelului $R[X_1, \ldots, X_n]$.
Pentru un polinom $f \in R[X_1, \ldots, X_n]$ vom nota cu $\tilde{f}$ *funcţia polinomială* ataşată lui f. Deci $\tilde{f} : R^n \to R$ astfel încât $\tilde{f}(x) = f(x)$ pentru orice $x \in R^n$.
• *Teorema lui Hilbert a bazei.* Dacă R este inel noetherian, atunci inelul de polinoame $R[X_1, \ldots, X_n]$ este noetherian.
• Un polinom $f \in R[X_1, \ldots, X_n]$ se numeşte *simetric* dacă pentru orice permutare $\sigma \in S_n$ avem $f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = f(X_1, \ldots, X_n)$. Polinoamele simetrice fundamentale din $R[X_1, \ldots, X_n]$ se notează cu $s_1, \ldots, s_n$ şi sunt date de formulele

$$\begin{aligned} s_1 &= \sum_{1 \le i \le n} X_i \\ s_2 &= \sum_{1 \le i < j \le n} X_i X_j \\ \ldots &\quad \ldots \quad \ldots\ldots\ldots \\ s_n &= X_1 X_2 \ldots X_n \end{aligned}$$

• Prin $M_n(R)$, $n \in \mathbb{N}^*$, notăm inelul matricelor pătratice de ordin n cu coeficienţi într-un inel R.
Dacă I este un ideal (stâng, drept, bilateral) al lui R, atunci se notează cu $M_n(I)$ mulţimea matricelor cu toate elementele în I. Se observă că $M_n(I)$ este ideal (stâng, drept, bilateral) al lui $M_n(R)$.
Pentru $1 \le i, j \le n$ fixaţi se notează cu E_{ij} (sau e_{ij}) matricea care are 1 pe poziţia (i, j) şi 0 în rest.
• Fie R un inel comutativ şi unitar. Prin $R[[X]]$ vom nota inelul de serii formale în nedeterminata X cu coeficienţi în R. Dacă $f = a_0 + a_1 X + \ldots$ este o serie formală nenulă, atunci *ordinul* lui f se notează cu $\mathrm{ord}(f)$ şi este cel mai mic n cu proprietatea că $a_n \neq 0$.
Dacă I este ideal al lui R, atunci prin $I[[X]]$ notăm mulţimea seriilor formale din $R[[X]]$ cu toţi coeficienţii în I. Se observă că $I[[X]]$ este ideal al lui $R[[X]]$.
• Fie R un inel comutativ şi unitar iar $S \subset R$ un *sistem multiplicativ* (adică $1 \in S$ şi pentru orice $s, t \in S$ avem $st \in S$). Inelul de fracţii al lui R cu numitori în S se notează cu $S^{-1}R = \{a/s \mid a \in R,\ s \in S\}$. Reamintim că pentru $a, b \in R$ şi $s, t \in S$ avem $a/s = b/t$ dacă şi numai dacă există $u \in S$ astfel încât $u(at - bs) = 0$.
Inelele de fracţii au următoarea *proprietate de universalitate*: pentru orice

morfism de inele comutative $f : R \to R'$ şi pentru orice sistem multiplicativ $S \subset R$ cu proprietatea că $f(S) \subset U(R')$ există şi este unic un morfism $\overline{f} : S^{-1}R \to R'$ astfel încât $\overline{f}\phi = f$, unde $\phi : R \to S^{-1}R$, $\phi(a) = a/1$ pentru orice $a \in R$, este morfismul canonic.
Dacă R este un domeniu de integritate şi $S = R \setminus \{0\}$, atunci inelul de fracţii $S^{-1}R$ este corp, se notează cu $Q(R)$ şi se numeşte *corpul de fracţii* al lui R.
Dacă I este ideal al lui R, atunci se notează cu $S^{-1}I$ mulţimea fracţiilor cu numărătorii în I. Se observă că $S^{-1}I$ este ideal al lui $S^{-1}R$.
• *Simbolul lui Kronecker* δ_{ij} este egal cu 0 dacă $i \neq j$ şi cu 1 dacă $i = j$.

1. Fie R un inel. Să se arate că inelul de matrice $M_n(R)$ este comutativ dacă şi numai dacă este satisfăcută una din următoarele două condiţii:
(i) $n = 1$ şi R este comutativ;
(ii) $ab = 0$ pentru orice $a, b \in R$.

2. Fie $p > 0$ un număr prim.
(i) Să se determine matricele idempotente din $M_2(\mathbb{Z}_p)$ şi numărul acestora.
(ii) Dacă $A, B \in M_2(\mathbb{Z}_p)$ şi A este inversabilă, să se arate că $A^q = I_2$ şi $B^{q+2} = B^2$, unde $q = (p^2 - 1)(p^2 - p)$.

3. Fie K un corp comutativ şi $A \in M_n(K)$. Să se arate că A este inversabilă sau divizor al lui zero.

4. Fie R un inel. Să se arate că $Z(M_n(R)) = \{aI_n \mid a \in R\}$ şi că $Z(M_n(R)) \simeq R$.

5. Fie K şi L corpuri comutative. Să se arate că $M_m(K) \simeq M_n(L)$ dacă şi numai dacă $K \simeq L$ şi $m = n$.

6. Fie R un inel şi $n \in \mathbb{N}^*$. Să se arate că idealele bilaterale ale lui $M_n(R)$ sunt de forma $M_n(I)$, unde I este ideal bilateral al lui R, şi pentru orice astfel de ideal avem $M_n(R)/M_n(I) \simeq M_n(R/I)$.
Este adevărat că orice ideal stâng al lui $M_n(R)$ este de forma $M_n(J)$, cu J ideal stâng în R?

7. Fie K un corp şi $n > 1$. Să se arate că nu există morfisme de inele $f : M_n(K) \to K$.

8. Fie $\mathbb{H} = \left\{ \begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} \middle| \ u, v \in \mathbb{C} \right\}$.
(i) Să se arate că $\mathbb{H}$ este un corp necomutativ cu adunarea şi înmulţirea matricelor, numit *corpul cuaternionilor*.
(ii) Să se arate că $\mathbb{C}$ este izomorf cu un subcorp al lui $\mathbb{H}$.
(iii) Fie elementele $\mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $\mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ din $\mathbb{H}$. Să se arate că orice element $x \in \mathbb{H}$ se scrie în mod unic sub forma $x = a_0 I_2 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$ cu $a_0, a_1, a_2, a_3 \in \mathbb{R}$. Notând $\overline{x} = a_0 I_2 - a_1\mathbf{i} - a_2\mathbf{j} - a_3\mathbf{k}$, $N(x) = x\overline{x}$ şi $T(x) = x + \overline{x}$, să se arate că $x^2 - T(x)x + N(x) = 0$ şi că $N(xy) = N(yx)$ pentru orice $x, y \in \mathbb{H}$.
(iv) Să se determine $Z(\mathbb{H})$.
(v) Să se arate că ecuaţia $x^2 = -1$ are o infinitate de soluţii în $\mathbb{H}$.

9. Fie S un inel şi $n \in \mathbb{N}^*$. Să se arate că următoarele afirmaţii sunt echivalente:
(a) Există un inel R astfel încât $S \simeq M_n(R)$.
(b) Există o familie $(e_{ij})_{1 \leq i,j \leq n}$ de elemente din S cu proprietatea că $\sum_{1 \leq i \leq n} e_{ii} = 1$ şi $e_{ij}e_{kl} = \delta_{jk}e_{il}$ pentru orice $1 \leq i, j, k, l \leq n$ (unde δ_{jk} este simbolul lui Kronecker).

10. Fie S un inel unitar cu proprietatea că $S \simeq M_n(R)$ pentru un $n \in \mathbb{N}^*$ şi un inel R. Fie A un inel factor al lui S şi B un inel pentru care S este subinel în B. Să se arate că A şi B sunt şi ele izomorfe cu inele de matrice $n \times n$ peste anumite inele.

11. Fie $k \in \mathbb{Z}$ şi $R_k = \left\{ \begin{pmatrix} a & b \\ kb & a \end{pmatrix} \middle| \ a, b \in \mathbb{Z} \right\}$. Să se arate că:
(i) R_k este inel comutativ.
(ii) $R_k \simeq \mathbb{Z}[X]/(X^2 - k)$.
(iii) $R_k \simeq R_l$ dacă şi numai dacă $l = k$.

12. Fie R un inel. Să se arate că $M_n(R[X]) \simeq M_n(R)[X]$.

13. Fie R un inel comutativ şi $a_1, \ldots, a_n \in R$. Să se arate că

$$R[X_1, \ldots, X_n]/(X_1 - a_1, \ldots, X_n - a_n) \simeq R.$$

14. Fie R un inel comutativ şi I un ideal al lui R. Arătaţi că:
(i) $I[X_1, \ldots, X_n]$ este ideal al lui $R[X_1, \ldots, X_n]$ şi coincide cu extinsul lui I via injecţia canonică $\epsilon : R \to R[X_1, \ldots, X_n]$.
(ii) $R[X_1, \ldots, X_n]/I[X_1, \ldots, X_n] \simeq (R/I)[X_1, \ldots, X_n]$.
(iii) I este ideal prim în R dacă şi numai dacă $I[X_1, \ldots, X_n]$ este ideal prim în $R[X_1, \ldots, X_n]$.

15. Să se arate că există următoarele izomorfisme de inele:
(i) $\mathbb{Z}[X]/(X^2 - d) \simeq \mathbb{Z}[\sqrt{d}]$, unde d este un număr întreg liber de pătrate, iar $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ este inel cu adunarea şi înmulţirea numerelor reale.
(ii) $\mathbb{Q}[X]/(X^2 + X + 1) \simeq \mathbb{Q}(\varepsilon)$, unde ε este o rădăcină primitivă de ordinul 3 a unităţii şi $\mathbb{Q}(\varepsilon) = \{a + b\varepsilon \mid a, b \in \mathbb{Q}\}$ este inel cu adunarea şi înmulţirea numerelor complexe.
(iii) $\mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}$.

16. Fie $d \in \mathbb{Z}$ care nu este pătrat perfect. Arătaţi că pentru orice $a, b \in \mathbb{Z}$ cu $a \neq 0$ sau $b \neq 0$, inelul $\mathbb{Z}[\sqrt{d}]/(a + b\sqrt{d})$ are $|a^2 - db^2|$ elemente.

17. Fie $a, b, c \in \mathbb{R}$, $a \neq 0$ şi $\Delta = b^2 - 4ac$. Notăm $R = \mathbb{R}[X]/(aX^2 + bX + c)$. Să se arate că:
(i) Dacă $\Delta > 0$, atunci $R \simeq \mathbb{R} \times \mathbb{R}$.
(ii) Dacă $\Delta < 0$, atunci $R \simeq \mathbb{C}$.
(iii) Dacă $\Delta = 0$, atunci R este un inel local cu divizori ai lui zero.

18. Să se arate că $R = \mathbb{Z}[X]/(2, X^2 + 1)$ este un inel cu 4 elemente, dar R nu este izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_2$.

19. Considerăm idealul $I = (3, X^3 - X^2 + 2X + 1)$ în $\mathbb{Z}[X]$. Să se arate că I nu este ideal principal şi că $\mathbb{Z}[X]/I$ nu este corp.

20. Fie $R = \{f \in \mathbb{R}[X] \mid f(0) \in \mathbb{Q}\}$ şi $I = \{f \in R \mid f(0) = 0\}$. Să se arate că R este inel comutativ, I este ideal maximal al lui R şi I nu este finit generat.

21. Fie K un corp comutativ şi $R = K[X_1, \ldots, X_n, \ldots]$ inelul de polinoame într-o infinitate numărabilă de nedeterminate peste K. Să se arate că idealul $I = (X_1, \ldots, X_n, \ldots)$ nu este finit generat.

22. Fie $R = \mathbb{Z}[X, Y]$ şi $I = (X^r, Y^s)$, $r, s \in \mathbb{N}^*$. Să se calculeze $\mathrm{Rad}(I)$ şi să se arate că dacă $f, g \in R$ astfel încât $fg \in I$, atunci $f \in I$ sau $g \in \mathrm{Rad}(I)$ ($\mathrm{Rad}(I)$ s-a definit în problema 47 din Capitolul 4).

23. Fie K un corp comutativ şi $R = K[X, Y]/(X^2 - Y^3)$. Să se arate că:
(i) R este inel integru.
(ii) R este izomorf cu subinelul B al lui $K[T]$ format din polinoamele de forma $P(T) = a_0 + \sum_{2 \leq i \leq n} a_i T^i$, cu $n \in \mathbb{N}$ şi $a_0, a_2, \ldots, a_n \in K$.

24. Fie K un corp comutativ de caracteristică $\neq 2$. Să se arate că inelul $R = K[X, Y]/(Y^2 - X^3 - X^2)$ este integru, dar $K[[X, Y]]/(Y^2 - X^3 - X^2)$ (*completatul* lui R în topologia idealului maximal $(\hat{X}, \hat{Y})$) nu este integru.

25. Fie R un inel comutativ şi $f = a_0 + a_1 X + \ldots + a_n X^n \in R[X]$. Să se arate că:
(i) f este nilpotent dacă şi numai dacă a_i este nilpotent pentru orice $0 \leq i \leq n$.
(ii) f este inversabil dacă şi numai dacă a_0 este inversabil şi a_i este nilpotent pentru orice $1 \leq i \leq n$.
(iii) f este divizor al lui zero dacă şi numai dacă există $a \in R$, $a \neq 0$, cu $af = 0$.
(iv) f este idempotent dacă şi numai dacă $f = a_0$ şi $a_0^2 = a_0$.

26. Fie R un inel comutativ şi $f = a_0 + a_1 X + \cdots \in R[[X]]$. Să se arate că:
(i) Dacă f este nilpotent, atunci a_i este nilpotent pentru orice $i \geq 0$. Reciproc este adevărat?
(ii) f este inversabil dacă şi numai dacă a_0 este inversabil.
(iii) f este idempotent dacă şi numai dacă $f = a_0$ şi $a_0^2 = a_0$.

27. Fie R un inel comutativ. Să se arate că:
(i) Dacă M este un ideal maximal al lui $R[[X]]$, atunci $M \cap R$ este ideal maximal al lui R şi $M = (M \cap R)R[[X]] + XR[[X]]$.
(ii) Dacă R este inel local cu idealul maximal m, atunci $R[[X]]$ este inel local cu idealul maximal $mR[[X]] + XR[[X]]$.
(iii) Inelul $R[X]$ nu poate fi inel local.

28. Fie R inel noetherian. Arătaţi că inelul de serii formale $R[[X]]$ este noetherian.

29. Să se arate că $\mathbb{Z}[[X]]/(X-2)$ nu este izomorf cu $\mathbb{Z}$ (deci izomorfismul din problema 13 nu mai este valabil pentru inele de serii formale).

30. Fie R un inel comutativ. Să se arate că $J(R[X]) = N(R[X])$ şi $J(R[[X]]) = J(R)[[X]]$.

31. Fie K un corp comutativ şi considerăm inelul neunitar $R = XK[[X]]$.
(i) Fie I un ideal al lui R şi n cel mai mic ordin al unei serii formale nenule din I. Definim

$$G_I = \{a \in K \mid \text{există } f \in I \text{ cu } f = aX^n + \alpha_{n+1}X^{n+1} + \dots\}.$$

Să se arate că G_I este subgrup al grupului abelian $(K, +)$. Mai mult, dacă I este ideal maximal în R, atunci să se arate că G_I este subgrup maximal în $(K, +)$.
(ii) Fie G un subgrup al lui $(K, +)$. Să se arate că

$$I_G = \{f \in R \mid \text{există } a \in G \text{ cu } f = aX + \alpha_2X^2 + \dots\}$$

este ideal în R. Mai mult, să se arate că dacă G este subgrup maximal al lui $(K, +)$, atunci I_G este ideal maximal al lui R.
(iii) Deduceţi că R are ideale maximale dacă şi numai dacă grupul $(K, +)$ are subgrupuri maximale.
(iv) Să se arate că grupul $(K, +)$ este divizibil dacă şi numai dacă $\text{char}(K) = 0$.
(v) Deduceţi că grupul $(K, +)$ are subgrupuri maximale dacă şi numai dacă $\text{char}(K) \neq 0$.
(vi) Să se arate că R are ideale maximale dacă şi numai dacă $\text{char}(K) \neq 0$.

32. Fie K un corp comutativ. Să se arate că:
(i) Idealele nenule proprii ale inelului $K[[X]]$ sunt de forma (X^n), $n \in \mathbb{N}^*$. În particular, $K[[X]]$ este inel local.
(ii) Inelul R format din toate seriile formale de tipul $f = a_0 + a_2X^2 + a_3X^3 + \dots$ este un inel local, iar idealele nenule proprii ale lui R sunt de forma $(X^n + aX^{n+1})$ sau (X^n, X^{n+1}), cu $n \in \mathbb{N}$, $n \geq 2$ şi $a \in K$.

33. Fie K un corp comutativ, $K[[X]]$ inelul seriilor formale peste K şi $U_1(K[[X]])$ mulţimea seriilor formale de forma $f = 1 + a_1X + a_2X^2 + \dots$. Să se arate că $U_1(K[[X]])$ este grup cu înmulţirea seriilor formale şi că pentru

orice număr întreg N care nu se divide cu caracteristica lui K, aplicaţia $\phi_N : U_1(K[[X]]) \to U_1(K[[X]])$, $\phi_N(f) = f^N$, este izomorfism de grupuri.

34. Dacă $F = \sum_{n\geq 0} a_n X^n$ este o serie formală cu coeficienţi în corpul K, definim seria formală derivată F' prin $F' = \sum_{n\geq 1} n a_n X^{n-1}$. Să se arate că:
(i) Pentru orice $F, G \in K[[X]]$ avem $(F+G)' = F' + G'$, $(FG)' = F'G + FG'$ şi $(F^n)' = nF^{n-1}F'$ pentru orice $n \in \mathbb{N}^*$.
(ii) Pentru $\operatorname{char} K = 0$, dacă $A, B \in U_1(K[[X]])$ şi $A'B = AB'$, atunci $A = B$.
(iii) Pentru $\operatorname{char} K = 0$, dacă $A, B \in XK[[X]]$ şi $A' = B'$, atunci $A = B$.

35. Fie K un corp comutativ. Spunem că o familie $(F_i)_{i\geq 0}$ de serii formale din $K[[X]]$, $F_i = \sum_{j\geq 0} a_{ij} X^j$, este *sumabilă* dacă pentru orice $r \geq 0$ şirul $(a_{ir})_{i\geq 0}$ are doar un număr finit de termeni nenuli. În acest caz definim seria formală $F = \sum_{i\geq 0} F_i$ ca fiind $F = \sum_{i\geq 0} b_i X^i$, unde $b_i = \sum_{r\geq 0} a_{ri}$ (prin această sumă formală infinită înţelegem suma finită a termenilor nenuli din sumare). Să se arate că dacă familia $(F_i)_{i\geq 0}$ este sumabilă, atunci:
(i) Familia $(F_i')_{i\geq 0}$ este sumabilă şi $F' = \sum_{i\geq 0} F_i'$.
(ii) Dacă $G \in K[[X]]$, atunci familia $(F_i G)_{i\geq 0}$ este sumabilă şi $(\sum_{i\geq 0} F_i)G = \sum_{i\geq 0} F_i G$.

36. Fie K un corp de caracteristică zero. Identificăm mulţimea numerelor raţionale cu cel mai mic subcorp al lui K. Pentru orice $f \in XK[[X]]$ definim

$$\exp(f) = 1 + \sum_{n>0} \frac{1}{n!} f^n \in U_1(K[[X]]).$$

(Să observăm că familia de serii formale $(\frac{1}{n!} f^n)_{n>0}$ este sumabilă şi atunci suma din membrul drept se defineşte ca în problema 35.)
De asemenea, pentru orice $g \in U_1(K[[X]])$ definim

$$\log(g) = -\sum_{n>0} \frac{1}{n} (1-g)^n \in XK[[X]].$$

(Şi aici observăm că deoarece $1 - g \in XK[[X]]$, familia $(\frac{1}{n}(1-g)^n)_{n>0}$ este sumabilă.) Să se arate că:
(i) $(\exp(f))' = (\exp(f))f'$ pentru orice $f \in XK[[X]]$.
(ii) $g(\log(g))' = g'$ pentru orice $g \in U_1(K[[X]])$.
(iii) $\exp(\log(g)) = g$ pentru orice $g \in U_1(K[[X]])$.

(iv) $\log(\exp(f)) = f$ pentru orice $f \in XK[[X]]$.
(v) $\exp(f+h) = \exp(f)\exp(h)$ pentru orice $f, h \in XK[[X]]$.
(vi) Deduceţi că funcţiile exp şi log sunt izomorfisme inverse unul celuilalt între grupurile $(XK[[X]], +)$ şi $(U_1(K[[X]], \cdot)$.

37. Fie K un corp de caracteristică zero. Identificăm mulţimea numerelor raţionale cu cel mai mic subcorp al lui K. Fie $\alpha = \frac{a}{N}$ un număr raţional, unde $a, N \in \mathbb{Z}$, $N \neq 0$. Definim seria formală $(1+X)^\alpha$ din $K[[X]]$ prin $(1+X)^\alpha = (\phi_N^{-1}(1+X))^a$, unde ϕ_N este izomorfismul din problema 33. Să se arate că:
(i) Definiţia lui $(1+X)^\alpha$ nu depinde de reprezentarea lui α ca fracţie raţională.
(ii) $(1+X)^\alpha = \exp(\alpha \log(1+X))$.
(iii) Pentru orice $n \geq 0$, coeficientul lui X^n din seria formală $(1+X)^\alpha$ este o funcţie polinomială de α.
(iv) $(1+X)^\alpha = 1 + \sum_{n>0} \binom{\alpha}{n} X^n$, unde $\binom{\alpha}{n} = \frac{\alpha(\alpha-1)\ldots(\alpha-n+1)}{n!}$ pentru orice $n > 0$.

38. Pentru $n \geq 2$ notăm cu T_n numărul de moduri în care se pot pune parantezele în produsul $x_1 x_2 \ldots x_n$, unde $x_1, \ldots, x_n$ sunt elemente ale unei mulţimi pe care s-a definit o operaţie notată multiplicativ. Notăm $T_1 = 1$. Ştim din soluţia problemei 2 din Capitolul 2 că $T_n = \sum_{k=1,n-1} T_k T_{n-k}$. Considerăm seria formală $F = T_1 X + T_2 X^2 + \ldots + T_n X^n + \ldots \in \mathbb{Q}[[X]]$.
(i) Să se arate că $F^2 = F - X$.
(ii) Deduceţi că $F = \frac{1}{2} - \frac{1}{2}\phi_2^{-1}(1-4X)$ (unde ϕ_2 are semnificaţia din problema 33).
(iii) Să se arate că $\phi_2^{-1}(1-4X) = \sum_{n\geq 0} -\frac{2}{n} C_{2n-2}^{n-1} X^n$.
(iv) Să se deducă din (ii) şi (iii) că $T_n = \frac{1}{n} C_{2n-2}^{n-1}$.

39. (i) Fie k un corp comutativ şi $f \in k[X]$. Arătaţi că inelul factor $k[X]/(f)$ este corp dacă şi numai dacă f este ireductibil.
(ii) Fie R un domeniu de integritate şi Q corpul său de fracţii. Arătaţi că pentru orice polinom neconstant $f \in R[X]$ există un corp care conţine Q ca subcorp şi în care f are cel puţin o rădăcină.
(iii) Cu notaţiile de la (ii), demonstraţi că pentru orice polinom $f \in R[X]$ cu $\operatorname{grad} f \geq 1$ există un corp K care conţine pe Q ca subcorp şi în care f are toate rădăcinile.

40. Fie $a \in \mathbb{Z}$, $n \in \mathbb{N}^*$ şi $f(X) = X^n - a \in \mathbb{Z}[X]$. Dacă pentru orice $m \in \mathbb{N}$, $m \geq 2$ polinomul $\hat{f} \in \mathbb{Z}_m[X]$, $\hat{f}(X) = X^n - \hat{a}$ are o rădăcină în $\mathbb{Z}_m$,

să se arate că f are o rădăcină în $\mathbb{Z}$.

41. Fie R un domeniu de integritate infinit şi $f \in R[X_1, \ldots, X_n]$. Dacă există o submulţime $A = A_1 \times \ldots \times A_n$ a lui R^n, astfel încât A_i este infinită pentru orice $1 \leq i \leq n$, cu proprietatea că $\tilde{f}(a) = 0$ pentru orice $a \in A$, atunci $f = 0$ ($\tilde{f}$ este funcţia polinomială ataşată polinomului f).
Mai rămâne adevărată afirmaţia dacă ştim doar că $\tilde{f}(a) = 0$ pentru o infinitate de elemente $a \in R^n$?
Să se arate că rezultatul nu mai este adevărat dacă R nu este inel comutativ.

42. Fie K un corp comutativ, $q \in \mathbb{N}$, $q > 1$ şi $f \in K[X_1, \ldots, X_n]$. Să se arate că f se poate scrie astfel: $f = \sum_{1 \leq i \leq n} (X_i^q - X_i)g_i + g_0$, cu $g_i \in K[X_1, \ldots, X_n]$ pentru orice $0 \leq i \leq n$, $\deg_{X_i}(g_0) < q$ pentru orice $1 \leq i \leq n$, şi $\deg(g_0) \leq \deg(f)$.

43. Fie K un corp finit, $|K| = q$, şi fie $g \in K[X_1, \ldots, X_n]$ cu proprietatea că $\deg_{X_i}(g) < q$ pentru orice $1 \leq i \leq n$. Dacă $\tilde{g} = 0$, să se arate că $g = 0$.

44. Fie K un corp finit, $|K| = q$, şi fie $g \in K[X_1, \ldots, X_n]$. Să se arate că $\tilde{g} = 0$ dacă şi numai dacă $g \in (X_1^q - X_1, \ldots, X_n^q - X_n)$.

45. Fie K un corp finit şi $n \in \mathbb{N}^*$. Să se arate că orice funcţie $\phi : K^n \to K$ este polinomială, adică există $f \in K[X_1, \ldots, X_n]$ cu $\phi = \tilde{f}$.

46. Fie K un corp finit, $|K| = q$, şi fie $f \in K[X_1, \ldots, X_n]$ astfel încât $\deg(f) = d < n$ şi $f(0, \ldots, 0) = 0$. Să se arate că:
(i) Există $a \in K^n$, $a \neq (0, \ldots, 0)$, cu $\tilde{f}(a) = 0$.
(ii) Dacă $|\{a \in K^n \mid \tilde{f}(a) = 0\}| = N$ şi $p = \text{char}(K)$, atunci $p|N$.

47. Fie K un corp finit, $|K| = q$, şi fie $f(X) = a_0 + a_1X + \ldots + a_{q-2}X^{q-2} \in K[X]$ cu $a_{q-2} \neq 0$. Atunci $|\{a \in K^* \mid \tilde{f}(a) = 0\}| = q - 1 - \text{rang}(A)$, unde A este matricea

$$A = \begin{pmatrix} a_0 & a_1 & \ldots & a_{q-2} \\ a_1 & a_2 & \ldots & a_0 \\ \ldots & \ldots & \ldots & \ldots \\ a_{q-2} & a_0 & \ldots & a_{q-3} \end{pmatrix}.$$

48. Fie R un inel comutativ, $S \subseteq R$ un sistem multiplicativ şi $\phi : R \to S^{-1}R$ morfismul canonic. Să se arate că:

(i) ϕ este injectiv dacă şi numai dacă S este inclus în mulţimea nondivizorilor lui zero din R.
(ii) ϕ este bijectiv dacă şi numai dacă $S \subseteq U(R)$.

49. Fie R un inel comutativ, $S \subseteq R$ un sistem multiplicativ şi I, J ideale ale lui R. Notăm $S^{-1}I = \{a/s \mid a \in I, s \in S\}$. Să se arate că:
(i) $S^{-1}I$ este ideal al lui $S^{-1}R$. În plus, orice ideal al lui $S^{-1}R$ este de forma $S^{-1}I$ pentru un ideal I al lui R.
(ii) $S^{-1}I = S^{-1}R$ dacă şi numai dacă $I \cap S \neq \emptyset$.
(iii) Mulţimea $T = \{\hat{s} \mid s \in S\}$ este sistem multiplicativ în R/I şi avem $S^{-1}R/S^{-1}I \simeq T^{-1}(R/I)$.
(iv) $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$, $S^{-1}(I + J) = S^{-1}I + S^{-1}J$ şi $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$ pentru orice ideale I şi J.

50. Fie R un inel comutativ şi S un sistem multiplicativ în R. Să se arate că:
(i) Dacă p este ideal prim al lui R cu $p \cap S = \emptyset$, atunci $S^{-1}p$ este ideal prim al lui $S^{-1}R$.
(ii) Există o corespondenţă bijectivă între $\mathrm{Spec}(R) \cap \Sigma$ şi $\mathrm{Spec}(S^{-1}R)$, unde $\Sigma = \{I \mid I \text{ ideal al lui } R \text{ cu } I \cap S = \emptyset\}$.
(iii) Dacă p este ideal prim al lui R şi $S = R - p$, atunci $S^{-1}R$ este inel local cu idealul maximal $S^{-1}p$ şi $S^{-1}R/S^{-1}p$ este izomorf cu $Q(R/p)$, corpul de fracţii al domeniului de integritate R/p. (În acest caz $S^{-1}R$ se notează cu R_p şi se numeşte *localizatul* lui R în idealul prim p).

51. Fie R inel noetherian. Arătaţi că orice inel de fracţii al lui R este noetherian.

52. Fie $S = \{2k + 1 \mid k \in \mathbb{Z}\}$. Să se arate că S este sistem multiplicativ în $\mathbb{Z}$ şi că $S^{-1}\mathbb{Z}$ este inel local. Care este idealul său maximal?

53. Fie $S = (3\mathbb{Z} - \{0\}) \cup \{1\}$. Să se arate că S este sistem multiplicativ al lui $\mathbb{Z}$ şi că $S^{-1}\mathbb{Z} = \mathbb{Q}$.

54. Fie R un domeniu de integritate. Să se arate că $R = \bigcap_{m \in \mathrm{Max}(R)} R_m$ (R şi orice localizat al său sunt considerate ca subinele în corpul de fracţii al lui R).

55. Fie R un inel comutativ şi $a \in R$ un element care nu este nilpotent. Să se arate că $S = \{1, a, a^2, \ldots\}$ este sistem multiplicativ al lui R şi că $S^{-1}R \simeq R[X]/(aX - 1)$.

56. Fie R un inel comutativ finit şi S un sistem multiplicativ al lui R. Să se arate că morfismul canonic $\phi : R \to S^{-1}R$ este surjectiv. În particular, orice inel de fracţii al lui $\mathbb{Z}_n$ este izomorf cu un $\mathbb{Z}_d$, $d|n$.
Este adevărat şi reciproc: pentru orice $n \in \mathbb{N}^*$ şi orice $d|n$ există un sistem multiplicativ S al lui $\mathbb{Z}_n$ cu proprietatea că $S^{-1}\mathbb{Z}_n \simeq \mathbb{Z}_d$?

57. Fie R un domeniu de integritate în care orice ideal este principal. Fie K corpul de fracţii al lui R şi fie A un subinel al lui K care îl include pe R. Să se arate că există un sistem multiplicativ S al lui R cu proprietatea că $A = S^{-1}R$.
Să se dea exemplu de domeniu de integritate R pentru care proprietatea de mai sus nu este adevărată.

58. Fie R un inel comutativ şi S un sistem multiplicativ al lui R. Să se arate că există un izomorfism canonic între $S^{-1}(R[X])$ şi $(S^{-1}R)[X]$. Mai rămâne adevărată proprietatea pentru inele de serii formale?

59. Fie $(R_i)_{i\in I}$ o familie de inele comutative şi considerăm pentru orice $i \in I$ un sistem multiplicativ S_i al lui R_i. Fie $R = \prod_{i\in I} R_i$. Să se arate că $S = \prod_{i\in I} S_i$ este sistem multiplicativ al lui R şi că există un izomorfism canonic între $S^{-1}R$ şi $\prod_{i\in I}(S_i^{-1}R_i)$.

60. Să se arate că un inel comutativ R este redus dacă şi numai dacă R_m este redus pentru orice $m \in \mathrm{Max}(R)$. (Un inel comutativ se numeşte *redus* dacă nu are elemente nilpotente nenule.)
Mai rămâne adevărată proprietatea dacă înlocuim redus cu integru?

61. Fie K un corp comutativ, $\mathrm{char}(K) \neq 2$ şi fie $D_n, \Delta_n \in K[X_1, \ldots, X_n]$, $D_n = \prod_{1\leq i,j\leq n} (X_i - X_j)$, $\Delta_n = D_n^2$. Să se arate că:
(i) $D_n(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = \varepsilon(\sigma)D_n(X_1, \ldots, X_n)$ pentru orice $\sigma \in S_n$.
(ii) Δ_n este polinom simetric.
(iii) Dacă $f \in K[X_1, \ldots, X_n]$ are proprietatea că

$$f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = \varepsilon(\sigma)f(X_1, \ldots, X_n)$$

pentru orice $\sigma \in S_n$, atunci există $g \in K[X_1, \ldots, X_n]$ polinom simetric cu $f = gD_n$.
(iv) Dacă $f \in K[X_1, \ldots, X_n]$ are proprietatea că

$$f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = f(X_1, \ldots, X_n)$$

pentru orice $\sigma \in A_n$, atunci există $f_1, f_2 \in K[X_1, \ldots, X_n]$ polinoame simetrice cu $f = f_1 + f_2 D_n$.

62. Să se scrie ca polinom de polinoamele simetrice fundamentale fiecare din următoarele polinoame simetrice:
(i) $(X_1 - X_2)^2(X_1 - X_3)^2(X_2 - X_3)^2$.
(ii) $(X_1^2 + X_2^2)(X_1^2 + X_3^2)(X_2^2 + X_3^2)$.
(iii) $(-X_1+X_2+\ldots+X_n)(X_1-X_2+\ldots+X_n)\cdots(X_1+X_2+\ldots+X_{n-1}-X_n)$.
(iv) $X_1^3 + \ldots + X_n^3$.

63. (*Formulele lui Newton*) Fie K un corp comutativ. Pentru fiecare $i \in \mathbb{N}$, $i > 0$, considerăm polinoamele $p_i = X_1^i + \ldots + X_n^i \in K[X_1, \ldots, X_n]$. De asemenea considerăm $p_0 = n$. Să se arate că:
(i) $p_k - s_1 p_{k-1} + \ldots + (-1)^n s_n p_{k-n} = 0$ pentru orice $k \geq n$.
(ii) $p_k - s_1 p_{k-1} + \ldots + (-1)^{k-1} s_{k-1} p_1 + (-1)^k k s_k = 0$ pentru orice $1 \leq k \leq n-1$.

64. Fie K un corp comutativ de caracteristică zero. Considerăm elementele $x_1, \ldots, x_n \in K$ cu proprietatea că $x_1^k + \ldots + x_n^k = 0$ pentru orice $1 \leq k \leq n$. Să se arate că $x_1 = \ldots = x_n = 0$.
Mai rămâne adevărată concluzia dacă $x_1^k + \ldots + x_n^k = 0$ pentru n valori ale lui k, care nu sunt neapărat consecutive? Dar dacă caracteristica lui K nu este zero?

65. Să se calculeze $x_1^{10} + x_2^{10} + x_3^{10}$, unde x_1, x_2, x_3 sunt rădăcinile polinomului $X^3 - 3X + 1$.

66. Să se calculeze $x_1^i + \ldots + x_n^i$, $1 \leq i \leq n$, unde $x_1, \ldots, x_n$ sunt rădăcinile polinomului:
(i) $X^n + (a+b)X^{n-1} + (a^2+b^2)X^{n-2} + \ldots + (a^n + b^n)$, unde $a, b \in K$, K corp.
(ii) $X^n + (a+b)X^{n-1} + (a^2+ab+b^2) + \ldots + (a^n + a^{n-1}b + \ldots + ab^{n-1} + b^n)$, unde $a, b \in K$, K corp.

Capitolul 6

Aritmetică în inele integre

În acest capitol prin inel vom înţelege inel comutativ şi unitar, iar prin morfism de inele morfism unitar. (Uneori vom preciza acest lucru şi în mod explicit.) În problemele în care se va lucra cu inele care nu sunt neapărat comutative acest lucru va fi menţionat explicit.

• Fie R un inel comutativ unitar şi $a, b \in R$. Spunem că a *divide* pe b în R (şi notăm $a|_R b$ sau $a|b$) dacă există $c \in R$ astfel încât $b = ac$. Spunem că a este *asociat în divizibilitate* cu b în inelul R (şi notăm $a \sim_R b$ sau $a \sim b$) dacă $a|_R b$ şi $b|_R a$. Relaţia de asociere în divizibilitate este o relaţie de echivalenţă. În cazul în care R este domeniu, $a \sim_R b$ dacă şi numai dacă există $u \in R$ inversabil astfel încât $b = ua$.

• Spunem că $d \in R$ este un *cel mai mare divizor comun* (prescurtat c.m.m.d.c.) pentru elementele a şi b din R dacă sunt îndeplinite următoarele condiţii:
(i) $d|a$ şi $d|b$.
(ii) Pentru orice $d' \in R$ care divide a şi b avem $d'|d$.
Vom nota $d = (a, b)_R$ sau $d = (a, b)$.
Spunem că $m \in R$ este un *cel mai mic multiplu comun* (prescurtat c.m.m.m.c.) pentru elementele a şi b din R dacă sunt îndeplinite următoarele condiţii:
(i) $a|m$ şi $b|m$.
(ii) Pentru orice $m' \in R$ care se divide prin a şi b avem $m|m'$.
Vom nota $m = [a, b]_R$ sau $m = [a, b]$.

• Spunem că inelul R are *proprietatea c.m.m.d.c.* dacă orice două elemente ale sale admit un c.m.m.d.c..
Fie R un inel cu proprietatea c.m.m.d.c. şi $a, b, c \in R$. Atunci:

(i) pentru $a, b \neq 0$ cu $(a, b) = d$ există a', b' cu $a = da'$, $b = db'$ şi $(a', b') = 1$;
(ii) $(ac, bc) = (a, b)c$;
(iii) există $[a, b]$ şi $(a, b)[a, b] = ab$;
(iv) $(a, b) = 1$ şi $(a, c) = 1$ implică $(a, bc) = 1$;
(v) $a|bc$ şi $(a, b) = 1$ implică $a|c$;
(vi) $a|c$, $b|c$ şi $(a, b) = 1$ implică $ab|c$.
• Un element nenul şi neinversabil a al unui domeniu de integritate R se numeşte element *ireductibil* dacă din $a = bc$ rezultă $a \sim b$ sau $a \sim c$.
Descompunerea $a = bc$ a lui $a \in R$ se va numi *relevantă* dacă $b, c \in R \setminus U(R)$.
Un element nenul şi neinversabil p al unui domeniu de integritate R se numeşte element *prim* dacă din $p|ab$ rezultă $p|a$ sau $p|b$.
Orice element prim este ireductibil.
Dacă inelul R are proprietatea c.m.m.d.c., atunci orice element ireductibil al lui R este element prim.
• Un domeniu de integritate R se numeşte *inel euclidian* dacă există o aplicaţie $\varphi : R \setminus \{0\} \to \mathbb{N}$ astfel încât pentru orice $a \in R$ şi orice $b \in R \setminus \{0\}$ există $q, r \in R$ cu proprietăţile:
(i) $a = bq + r$.
(ii) $r = 0$ sau $\varphi(r) < \varphi(b)$.
Un domeniu de integritate R se numeşte *inel principal* dacă orice ideal al său este principal.
Un domeniu de integritate R se numeşte *inel factorial* dacă orice element nenul şi neinversabil al său se poate scrie ca produs de elemente prime.
• Orice inel euclidian este principal.
Orice inel principal este factorial.
Orice inel factorial are proprietatea c.m.m.d.c..
• Dacă R este inel principal, atunci orice şir ascendent de ideale ale sale este staţionar.
• Fie R un domeniu. Următoarele afirmaţii sunt echivalente:
(i) R este inel factorial.
(ii) Orice element nenul şi neinversabil din R se scrie ca produs de elemente ireductibile şi orice element ireductibil este prim.
(iii) Orice element nenul şi neinversabil din R se scrie ca produs de elemente ireductibile şi această scriere este unică abstracţie făcând de asocierea în divizibilitate şi de ordinea factorilor.
(iv) Orice element nenul şi neinversabil din R se scrie ca produs de elemente ireductibile şi R are proprietatea c.m.m.d.c.
• *Teorema lui Gauss:* Dacă R este inel factorial, atunci $R[X]$ este inel facto-

rial.
• Dacă R este un inel cu proprietatea c.m.m.d.c. şi $f \in R[X]$, atunci c.m.m.d.c al coeficienţilor lui f se numeşte *conţinutul* polinomului f şi se notează cu $c(f)$ (acesta este determinat până la o asociere în divizibilitate). Dacă R este un inel cu proprietatea c.m.m.d.c., atunci polinomul $f \in R[X]$ se numeşte *primitiv* dacă $c(f) = 1$.
• Dacă R este un inel factorial cu corpul de fracţii Q, atunci pentru $f \in R[X]$ sunt echivalente afirmaţiile:
(i) f este ireductibil.
(ii) f este primitiv şi ireductibil în $Q[X]$.
• *Criteriul lui Eisenstein:* Fie R un inel factorial cu corpul de fracţii Q, $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ şi p un element prim al lui R cu proprietăţile:
(i) $p|a_0, p|a_1, \ldots, p|a_{n-1}$.
(ii) $p \nmid a_n$.
(iii) $p^2 \nmid a_0$.
Atunci f este ireductibil în $Q[X]$.
• *Criteriul reducerii:* Fie R un inel factorial cu corpul de fracţii Q, S un domeniu, $u : R \to S$ un morfism unitar de inele şi $\overline{u} : R[X] \to S[X]$ extinsul acestuia (adică $\overline{u}(a_0+a_1X+\cdots+a_nX^n) = u(a_0)+u(a_1)X+\cdots+u(a_n)X^n$). Dacă pentru $f \in R[X]$ avem că $\overline{u}(f)$ este ireductibil în $S[X]$ şi $\operatorname{grad}\overline{u}(f) = \operatorname{grad} f$, atunci f este ireductibil în $Q[X]$.
• Dacă S este un inel, R un subinel al său iar $a, b \in R$, vom folosi notaţiile $R[a] = \{\tilde{f}(a) \mid f \in R[X]\}$ şi $R[a, b] = \{\tilde{f}(a, b) \mid f \in R[X, Y]\}$, unde $\tilde{f}$ este funcţia polinomială asociată polinomului f.

1. (i) Pentru fiecare pereche de elemente a, b din mulţimea $\{1 + i, 2 + i, 1 - i, 1 + 2i, 1 - 2i, -2 + i\} \subset \mathbb{Z}[i]$ decideţi dacă $a|b$, respectiv dacă $a \sim b$.
(ii) Acelaşi enunţ pentru $1 + 3i\sqrt{2}, 3 + i\sqrt{2}, 1 - 3i\sqrt{2}, 3 - i\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$.
(iii) Acelaşi enunţ pentru $5, 5\rho, 5\rho + 5, 5\rho - 5, 5 - 5\rho, 3 + 2\rho, 3 - 2\rho \in \mathbb{Z}[\rho]$, $\rho = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.
(iv) Acelaşi enunţ pentru $1 + 2\sqrt{2}, 1 - 2\sqrt{2}, 3 + \sqrt{2}, 3 - \sqrt{2}, 2 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.
(v) Acelaşi enunţ pentru $2+X, 1+X+X^2+\ldots, 2X^2+3X^3+4X^4+\ldots, a_rX^r+a_{r+1}X^{r+1}+\ldots (a_r \neq 0), b_sX^s + b_{s+1}X^{s+1} + \ldots (b_s \neq 0) \in \mathbb{Q}[[X]]$.
(vi) Acelaşi enunţ pentru $2 + X, \frac{3}{7} + \frac{3}{14}X, 2\pi X + \pi X^2, \frac{\pi}{5}X + \frac{\pi}{10}X^2, 3\pi^2 X + \frac{3\pi^2}{2}X^2, 2 + 3X + X^2 \in \mathbb{Q} + X\mathbb{R}[X]$.

2. Fie $d \in \mathbb{Z}$ care nu e pătrat perfect şi $N : \mathbb{Q}[\sqrt{d}] \longrightarrow \mathbb{Q}$ definită prin $N(a+b\sqrt{d}) = |a^2 - db^2|$. Să se arate că:
(i) $N(z) = |z\bar{z}|$, unde $z = a + b\sqrt{d}$, $\bar{z} = a - b\sqrt{d}$; dacă $d < 0$, atunci $N(z) = z\bar{z}$.
(ii) $N(z_1 z_2) = N(z_1)N(z_2)$, oricare ar fi $z_1, z_2 \in \mathbb{Q}[\sqrt{d}]$.
(iii) $N(\mathbb{Z}[\sqrt{d}]) \subset \mathbb{N}$. (Aplicaţia $N : \mathbb{Z}[\sqrt{d}] \longrightarrow \mathbb{N}$ se numeşte *normă* pe inelul $\mathbb{Z}[\sqrt{d}]$.)
(iv) $z \in \mathbb{Z}[\sqrt{d}]$ este inversabil dacă şi numai dacă $N(z) = 1$.
(v) Dacă $N(z)$ este număr prim, atunci z este element ireductibil. Daţi exemple în care reciproca acestei afirmaţii nu este adevărată.
(vi) Dacă d este de forma $4k+1$, atunci afirmaţiile de la punctele (iii), (iv) şi (v) sunt adevărate şi pentru inelul $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.
(vii) Determinaţi elementele de normă 112 din $\mathbb{Z}[i\sqrt{3}]$, $\mathbb{Z}[i\sqrt{5}]$, $\mathbb{Z}[i\sqrt{11}]$ şi $\mathbb{Z}\left[\frac{1+i\sqrt{7}}{2}\right]$.

3. Fie $d \in \mathbb{Z}$ care nu e pătrat perfect şi $a, b \in \mathbb{Z}[\sqrt{d}]$.
(i) Arătaţi că dacă $a|b$ în $\mathbb{Z}[\sqrt{d}]$, atunci $N(a)|N(b)$.
(ii) Daţi exemple de situaţii în care reciproca afirmaţiei de la (i) nu este adevărată.
(iii) Dacă $a|_{\mathbb{Z}\sqrt{d}} b$ şi $N(a) = N(b)$, atunci $a \sim_{\mathbb{Z}\sqrt{d}} b$.
(iv) Arătaţi că dacă $(N(a), N(b)) = 1$, atunci 1 este c.m.m.d.c. pentru a şi b.
(v) Este adevărat că dacă a şi b admit c.m.m.d.c. în $\mathbb{Z}[\sqrt{d}]$, atunci norma acestuia este egală cu $(N(a), N(b))$?
(vi) Arătaţi că dacă d este de forma $4k+1$, atunci afirmaţiile de la punctele (i), (iii) şi (iv) sunt adevărate şi pentru inelul $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

4. (i) Determinaţi elementele inversabile ale inelului $\mathbb{Z}[\sqrt{d}]$, unde $d \in \mathbb{Z}$ şi $d < 0$.
(ii) Arătaţi că grupul $U(\mathbb{Z}[\sqrt{2}])$ este izomorf cu grupul $\mathbb{Z}_2 \times \mathbb{Z}$.

5. Arătaţi că grupul $U(\mathbb{Z}[(1+i\sqrt{3})/2])$ este izomorf cu grupul $\mathbb{Z}_6$.

6. Fie $k \in \mathbb{Z}$ şi $R_k = \left\{ \begin{pmatrix} a & b \\ kb & a \end{pmatrix} \middle| \; a, b \in \mathbb{Z} \right\}$. Să se arate că R_k are divizori ai lui zero dacă şi numai dacă k este pătrat perfect.

7. Daţi exemple de inele integre în care orice element ireductibil este element prim, dar care nu au proprietatea c.m.m.d.c..

8. Arătaţi că inelul $\mathbb{Z}[i\sqrt{n}]$, unde $n \in \mathbb{N}$, $n \neq 1$ şi n este un număr impar, nu are proprietatea c.m.m.d.c..

9. (i) Arătaţi că în inelul $\mathbb{Z}[i\sqrt{5}]$ elementele $2(1+i\sqrt{5})$ şi 6 nu au un c.m.m.d.c., dar elementele $1+i\sqrt{5}$ şi 3 au un c.m.m.d.c..
(ii) Găsiţi toate descompunerile lui 6 în factori ireductibili, respectiv primi în $\mathbb{Z}[i\sqrt{5}]$.

10. Arătaţi că în inelul $\mathbb{Z}[i\sqrt{3}]$ elementele 2 şi $1+i\sqrt{3}$ sunt ireductibile, au un c.m.m.d.c. şi nu sunt prime, iar elementele 4 şi $2(1+i\sqrt{3})$ nu au un c.m.m.d.c..

11. Decideţi dacă elementele
(i) $4+i\sqrt{5}$ şi $1+3i\sqrt{5}$
(ii) $6+2i\sqrt{5}$ şi 14
(iii) $4+i\sqrt{5}$ şi $1+2i\sqrt{5}$
(iv) $6+3i\sqrt{5}$ şi 9
(v) $2+8i\sqrt{5}$ şi 18
din inelul $\mathbb{Z}[i\sqrt{5}]$ admit sau nu un c.m.m.d.c. iar în caz afirmativ să se determine.

12. Fie inelul $R = \{f \in \mathbb{Z}[X] \mid f = a_0 + a_2X^2 + \ldots + a_nX^n, a_i \in \mathbb{Z}, n \in \mathbb{N}, n \neq 1\}$. Să se arate că:
(i) $R = \mathbb{Z}[X^2, X^3]$;
(ii) c.m.m.d.c.$(X^2, X^3) = 1$ şi c.m.m.m.c.(X^2, X^3) nu există;
(iii) c.m.m.d.c.(X^5, X^6) şi c.m.m.m.c.(X^5, X^6) nu există;
(iv) X^2 este element ireductibil, dar nu este element prim.

13. Fie R un inel cu proprietatea c.m.m.d.c. şi Q corpul său de fracţii.
(i) Arătaţi că pentru orice $f \in R[X]$ există $\overline{f} \in R[X]$ cu $c(\overline{f}) = 1$ astfel încât $f = c(f)\overline{f}$.
Fie acum $f, g \in R[X]$. Arătaţi că:
(ii) $c(fg) = c(f)c(g)$.
(iii) $\overline{fg} = u\overline{f}\overline{g}$, $u \in U(R)$.
(iv) Dacă $c(f) = c(g) = 1$, atunci $f|_{Q[X]}g$ dacă şi numai dacă $f|_{R[X]}g$.

(v) $f|_{R[X]}g$ dacă şi numai dacă $c(f)|_R c(g)$ şi $\overline{f}|_{R[X]}\overline{g}$.
(vi) $f|_{R[X]}g$ dacă şi numai dacă $c(f)|_R c(g)$ şi $\overline{f}|_{Q[X]}\overline{g}$.

14. Să se arate că dacă R este un inel cu proprietatea c.m.m.d.c., atunci şi inelul de polinoame $R[X]$ are proprietatea c.m.m.d.c..

15. Să se arate că inelul $R = \{f \in \mathbb{Q}[X] \mid f = a_0 + a_1X + \ldots + a_nX^n, a_0 \in \mathbb{Z}\}$ este un inel cu proprietatea c.m.m.d.c., dar nu este factorial.

16. Să se arate că inelul $R = \{f \in \mathbb{Q}[[X]] \mid f = a_0 + a_1X + \ldots + a_nX^n + \ldots, a_0 = r/s$, unde $r, s \in \mathbb{Z}$ cu $(r, s) = 1$ şi s este impar$\}$ este un inel cu proprietatea c.m.m.d.c., dar nu este factorial.

17. Să se arate că inelele $\mathbb{Z}[\sqrt{2}]$ şi $\mathbb{Z}[(1 + \sqrt{5})/2]$ sunt euclidiene.

18. Fie $d \in \mathbb{N}$ de forma $4k + 3$ ($k \in \mathbb{N}$). Atunci inelul $\mathbb{Z}[\frac{1+i\sqrt{d}}{2}]$ este euclidian dacă şi numai dacă $d \in \{3, 7, 11\}$.

19. Fie R un domeniu de integritate. Următoarele afirmaţii sunt echivalente:
(i) R este factorial.
(ii) Orice ideal prim nenul al lui R conţine un element prim.

20. Fie R un inel euclidian (principal, respectiv factorial) şi $S \subset R$ un sistem multiplicativ. Să se arate că inelul de fracţii $S^{-1}R$ este inel euclidian (principal, respectiv factorial).

21. (*Nagata*) Fie R un domeniu de integritate cu proprietatea că orice şir ascendent de ideale principale este staţionar. Fie $(p_i)_{i\in I}$ o mulţime de elemente prime din R şi S sistemul multiplicativ generat de această mulţime. Dacă $S^{-1}R$ e factorial, atunci R e factorial.

22. (i) Să se arate că inelul $K[X, Y]/(XY - 1)$, K corp comutativ, este inel euclidian.
(ii) Să se arate că inelul $\mathbb{C}[X, Y]/(X^2 + Y^2 - 1)$ este inel euclidian.

23. Fie R un domeniu de integritate. Arătaţi că inelul de polinoame $R[X_1, \ldots, X_n]$ este inel principal dacă şi numai dacă R este corp şi $n = 1$.

24. Considerăm $R = \mathbb{Z}[i\sqrt{3}]$ şi idealul $P = (2, 1 + i\sqrt{3})$ al lui R. Arătaţi că:

(i) $P = \{a + bi\sqrt{3} \mid a, b \in \mathbb{Z} \text{ şi } a \equiv b \pmod 2\}$;
(ii) P este ideal prim, dar nu este ideal principal;
(iii) Localizatul R_P al inelului R în idealul prim P nu este inel principal;
(iv) Inelul R_P nu are elemente prime.

25. Fie R un domeniu de integritate. Să se arate că dacă există o funcţie $\varphi : R \to \mathbb{N}$ cu următoarele proprietăţi:
(i) $\varphi(a) = 0$ dacă şi numai dacă $a = 0$;
(ii) Pentru orice $x, y \in R$, $y \neq 0$, $y \nmid x$, există $u, v \in R$ astfel încât $0 < \varphi(xu - yv) < \varphi(y)$,
atunci R este inel principal.

26. Arătaţi că inelele $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$, $\mathbb{Z}\left[\frac{1+i\sqrt{43}}{2}\right]$, $\mathbb{Z}\left[\frac{1+i\sqrt{67}}{2}\right]$ şi $\mathbb{Z}\left[\frac{1+i\sqrt{163}}{2}\right]$ sunt principale, dar nu sunt euclidiene.

27. Arătaţi că dacă R este inel principal, atunci inelul de serii formale $R[[X]]$ este factorial.

28. (*Samuel*) Fie k corp comutativ şi $r, s, t \in \mathbb{N}^* \setminus \{1\}$ cu $(r, s) = 1$ şi $t \equiv 1 \pmod{rs}$. Notăm $R = k[X, Y, Z]/(X^r + Y^s - Z^t)$.
(i) Arătaţi că R este inel factorial.
(ii) Arătaţi că $R[[X]]$ nu este inel factorial.

29. Să se arate că următoarele inele nu sunt factoriale: $\mathbb{Z}[i\sqrt{6}]$, $\mathbb{Z}[\sqrt{10}]$, $\mathbb{Z}[\sqrt{26}]$, $K[X, Y, Z, T]/(XT - YZ)$, K corp comutativ cu $\operatorname{char} K \neq 2$.

30. Fie $d \in \mathbb{N}^*$. Atunci inelul $\mathbb{Z}[i\sqrt{d}]$ este euclidian dacă şi numai dacă $d \in \{1, 2\}$.

31. (i) Fie R un inel factorial care nu este corp şi care are doar un număr finit de elemente inversabile. Să se arate că inelul R are o infinitate de elemente prime neasociate.
(ii) Fie R un domeniu de integritate. Să se arate că inelul de polinoame $R[X]$ are o infinitate de elemente prime neasociate.

32. Se consideră inelul $R = K[X, Y]/(X^2 + Y^2 - 1)$, K corp comutativ cu $\operatorname{char} K \neq 2$. Arătaţi că:
(i) R este inel integru;
(ii) Dacă elementul $\hat{X}$ este reductibil în R, atunci polinomul $Z^2 + 1 \in K[Z]$

are rădăcini în K;
(iii) R este inel factorial dacă şi numai dacă polinomul $Z^2+1 \in K[Z]$ are rădăcini în K.

33. (i) Arătaţi că inelul $\mathbb{R}[X,Y]/(X^2+Y^2-1)$ nu este inel factorial.
(ii) Arătaţi că inelul $\mathbb{R}[X,Y]/(X^2+Y^2+1)$ este inel factorial.

34. (i) Fie $d \in \mathbb{Z}$ care nu e pătrat perfect. Arătaţi că dacă $\pi \in \mathbb{Z}[\sqrt{d}]$ este prim, atunci π este asociat în R cu un element prim din $\mathbb{Z}$ sau $\pi\overline{\pi}$ este prim în $\mathbb{Z}$.
(ii) Fie $d \in \mathbb{Z}$ care nu e pătrat perfect, $d \equiv 1 \pmod 4$. Arătaţi că, dacă $\pi \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ este prim, atunci π este asociat în R cu un element prim din $\mathbb{Z}$ sau $\pi\overline{\pi}$ este prim în $\mathbb{Z}$.

35. Fie $d \in \mathbb{Z} \setminus \{\alpha^2 | \ \alpha \in \mathbb{Z}\}$ şi $x = a+b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ cu $(a,b)=1$. Arătaţi că x este prim în $\mathbb{Z}[\sqrt{d}]$ dacă şi numai dacă $N(\pi)$ este prim în $\mathbb{Z}$.

36. (*Aritmetica inelului* $\mathbb{Z}[i]$) Arătaţi că un element din inelul $\mathbb{Z}[i]$ este prim dacă şi numai dacă este asociat în divizibilitate cu unul din următoarele elemente:
(i) $1+i$;
(ii) $p \in \mathbb{N}$ număr prim cu $p \equiv 3 \pmod 4$;
(iii) $a+bi$, $a,b \in \mathbb{Z}$, astfel încât $p = a^2+b^2$ este număr prim cu $p \equiv 1 \pmod 4$.

37. (*Aritmetica inelului* $\mathbb{Z}[i\sqrt{2}]$) Arătaţi că un element din inelul $\mathbb{Z}[i\sqrt{2}]$ este prim dacă şi numai dacă este asociat în divizibilitate cu unul din următoarele elemente:
(i) $i\sqrt{2}$;
(ii) $p \in \mathbb{N}$ număr prim cu $p \equiv 5 \pmod 8$ sau $p \equiv 7 \pmod 8$;
(iii) $a+bi\sqrt{2}$, $a,b \in \mathbb{Z}$, astfel încât $p = a^2+2b^2$ este număr prim cu $p \equiv 1 \pmod 8$ sau $p \equiv 3 \pmod 8$.

38. (*Aritmetica inelului* $\mathbb{Z}[\sqrt{2}]$) Arătaţi că un element din inelul $\mathbb{Z}[\sqrt{2}]$ este prim dacă şi numai dacă este asociat în divizibilitate cu unul din următoarele elemente:
(i) $\sqrt{2}$;
(ii) $p \in \mathbb{N}$ număr prim cu $p \equiv 3 \pmod 8$ sau $p \equiv 5 \pmod 8$;
(iii) $a+b\sqrt{2}$, $a,b \in \mathbb{Z}$, astfel încât $p = |a^2-2b^2|$ este număr prim cu $p \equiv 1 \pmod 8$ sau $p \equiv 7 \pmod 8$.

39. (*Aritmetica inelului* $\mathbb{Z}[\sqrt{3}]$) Arătaţi că un element din inelul $\mathbb{Z}[\sqrt{3}]$ este prim dacă şi numai dacă este asociat în divizibilitate cu unul din următoarele elemente:
(i) $\sqrt{3}$ sau $1+\sqrt{3}$;
(ii) $p \in \mathbb{N}$ număr prim cu $p \equiv 5 \pmod{12}$ sau $p \equiv 7 \pmod{12}$;
(iii) $a+b\sqrt{3}$, $a, b \in \mathbb{Z}$, astfel încât $p = |a^2 - 3b^2|$ este număr prim cu $p \equiv 1 \pmod{12}$ sau $p \equiv 11 \pmod{12}$.

40. (*Aritmetica inelului* $\mathbb{Z}[(-1+i\sqrt{3})/2]$) Arătaţi că un element din inelul $\mathbb{Z}[\rho]$, $\rho = (-1+i\sqrt{3})/2)$, este prim dacă şi numai dacă este asociat în divizibilitate cu unul din următoarele elemente:
(i) $1-\rho$;
(ii) $p \in \mathbb{N}$ număr prim cu $p \equiv 2 \pmod{3}$;
(iii) $a+b\rho$, $a, b \in \mathbb{Z}$, astfel încât $p = a^2 - ab + b^2$ este număr prim cu $p \equiv 1 \pmod{3}$.

41. Să se rezolve în numere întregi ecuaţia $x^2 + y^2 = z^2$.

42. Să se rezolve în numere întregi ecuaţia $x^2 + 2y^4 = 17z^4$.

43. Să se rezolve în numere întregi ecuaţia $x^3 + y^3 = z^3$.

44. Să se rezolve în numere întregi ecuaţia $x^3 + y^3 = 5z^3$.

45. Fie K un corp. Să se arate că:
(i) polinoamele X^2-Y, X^2-Y^2Z şi X^2-YZ^2 sunt ireductibile în $K[X,Y,Z]$;
(ii) dacă $\operatorname{char} K \neq 2$, atunci polinomul X^2+Y^2-1 este ireductibil în $K[X,Y]$.

46. Fie K un corp. Să se arate că:
(i) polinomul $X^r + Y^s$, $r, s \in \mathbb{N}^*$, $(r,s) = 1$, este ireductibil în $K[X,Y]$;
(ii) polinomul $X^r + Y^s + Z^t$, $r, s, t \in \mathbb{N}^*$ cu $r \equiv 1 \pmod{st}$, este ireductibil în $K[X,Y,Z]$.

47. (i) Arătaţi că polinomul $f \in \mathbb{Z}[\sqrt{3}][X], f = \sqrt{3}X^5 + 25X^4 + (5 + 5\sqrt{3})X - 15$ este ireductibil;
(ii) Arătaţi că polinomul $f \in \mathbb{Z}[X,Y], f = X^4Y^2 - 2X^3Y^3 + XY^4 + X^5 + Y^4 - 12XY^3 + 6X^2Y^2 + 6X^3 - 4Y^3 + 2XY^2 + 2X^2$ este ireductibil.

48. Să se arate că următoarele polinoame sunt ireductibile:
(i) $f \in \mathbb{Q}[X], f = X^n - 2$;

(ii) $f \in \mathbb{Q}[X], f = X^{p-1} + \ldots + X + 1$, unde $p \in \mathbb{N}$ este număr prim;
(iii) $f \in \mathbb{Q}[X], f = X^{p^n} + p - 1$, unde $n, p \in \mathbb{N}$ şi p este număr prim;
(iv) $f \in \mathbb{Z}[X], f = X^p - X + a$, unde $a, p \in \mathbb{Z}$, p este număr prim şi $(a, p) = 1$.

49. Să se arate că următoarele polinoame sunt ireductibile:
(i) $f \in \mathbb{Q}[X], f = (X^4+X^3+1)^n+4(X^4+X^3+1)^m+2$, unde $m, n \in \mathbb{N}, n > m$;
(ii) $f \in \mathbb{Z}[X], f = X^4 + 3X^3 + 3X^2 - 5$.

50. Fie K un corp algebric închis cu $\operatorname{char} K \neq 2$ şi $f \in K[X_1, \ldots, X_n]$, $f = X_1^2 + \ldots + X_n^2$. Să se arate că f este polinom ireductibil dacă şi numai dacă $n \geq 3$.

51. Fie $f \in \mathbb{Z}[X]$, $f = X^4 + 1$. Arătaţi că f este polinom ireductibil, dar $\overline{f} \in \mathbb{Z}_p[X]$ este reductibil pentru orice $p \in \mathbb{N}$ număr prim.

52. Să se arate că polinomul $f_n \in \mathbb{Z}[\{X_{ij} | 1 \leq i, j \leq n\}]$,

$$f_n = \det \begin{pmatrix} X_{11} & X_{12} & \ldots & X_{1n} \\ X_{21} & X_{22} & \ldots & X_{2n} \\ \vdots & \vdots & & \vdots \\ X_{n1} & X_{n2} & \ldots & X_{nn} \end{pmatrix}$$

este ireductibil.

53. Să se arate că polinomul $f_n \in \mathbb{Z}[\{X_{ij} | 1 \leq i \leq j \leq n\}]$,

$$f_n = \det \begin{pmatrix} X_{11} & X_{12} & \ldots & X_{1n} \\ X_{12} & X_{22} & \ldots & X_{2n} \\ \vdots & \vdots & & \vdots \\ X_{1n} & X_{2n} & \ldots & X_{nn} \end{pmatrix}$$

este ireductibil.

54. Să se arate că polinomul $f_n \in \mathbb{Z}[X_1, \ldots, X_{2n-1}]$,

$$f_n = \det \begin{pmatrix} X_1 & X_2 & \ldots & X_n \\ X_2 & X_3 & \ldots & X_{n+1} \\ \vdots & \vdots & & \vdots \\ X_n & X_{n+1} & \ldots & X_{2n-1} \end{pmatrix}$$

este ireductibil.

55. (*Van der Waerden*) Fie K un corp comutativ, $r, n \in \mathbb{N}$, $r \geq 1$, $n \geq 2$, $R = K[X_1, \ldots, X_r]$ şi polinoamele neconstante $f_1, \ldots, f_n \in R$ cu $(f_1, \ldots, f_n) = 1$. Atunci polinomul $T_1 f_1 + \cdots + T_n f_n \in R[T_1, \ldots T_n]$ este ireductibil.

Capitolul 7

Soluţii: Mulţimi

1. **Soluţia 1.** Presupunem prin absurd că $\bigcap_{i=1,s} A_i = \emptyset$. Fie $A_1 = \{x_1, \ldots, x_r\}$. Atunci există $i_1, \ldots, i_r \in \{1, \ldots, s\}$ astfel încât $x_1 \notin A_{i_1}$, $\ldots$, $x_r \notin A_{i_r}$. Rezultă că $A_1 \cap A_{i_1} \cap \cdots \cap A_{i_r} = \emptyset$, deoarece dacă intersecţia ar fi nevidă ea ar conţine unul din elementele $x_1, \ldots, x_r$ ale lui A_1, ceea ce este în contradicţie cu alegerea mulţimilor A_{i_j}.
Aşadar am găsit o familie constând din cel mult $r+1$ dintre mulţimile date care au intersecţia vidă, aceasta contrazicând ipoteza.
Soluţia 2. Demonstrăm afirmaţia prin inducţie după $s \geq r+1$. Dacă $s = r+1$ este clar. Fie acum $A'_1, A'_2, \ldots, A'_{s+1}$ mulţimi finite având fiecare r elemente. Din ipoteza de inducţie rezultă că intersecţia oricăror s dintre acestea este nevidă. Presupunem că $\bigcap_{i=1,s+1} A'_i = \emptyset$. Definim $B_i = \bigcap_{j \neq i} A'_j$ pentru $1 \leq i \leq s+1$ şi observăm că $B_i \neq \emptyset$ pentru orice i, iar $B_k \bigcap B_l = \emptyset$ pentru orice $k \neq l$. Cum $B_i \subseteq A'_1$ pentru orice $2 \leq i \leq s+1$, rezultă că $\bigcup_{i=2,s+1} B_i \subseteq A'_1$. Dar atunci obţinem că

$$s \leq \sum_{i=2,s+1} |B_i| = |\bigcup_{i=2,s+1} B_i| \leq |A'_1| = r,$$

adică $s \leq r$, contradicţie.

2. Demonstrăm afirmaţia prin inducţie după $m \geq 1$. Pentru $m = 1$ este clar. Dacă $m > 1$, atunci presupunem că $A' = X_1 \cup \cdots \cup X_{m-1}$ este o submulţime fixată a lui A. Atunci ecuaţia $A' \bigcup X_m = A$ are 2^t soluţii, unde $t = |A'|$. Dar din ipoteza de inducţie ecuaţia $X_1 \cup \cdots \cup X_{m-1} = A'$ are

$(2^{m-1}-1)^t$ soluţii. Cum există C_n^t submulţimi distincte cu t elemente ale lui A, numărul soluţiilor ecuaţiei date este

$$\sum_{t=0,n} C_n^t (2^{m-1}-1)^t 2^t = (2^m - 2 + 1)^n = (2^m - 1)^n.$$

3. Demonstrăm afirmaţia prin inducţie după $n \geq 2$. Pentru $n = 2$ este evident. Dacă $n > 2$, atunci $\bigcup_{i=1,n} A_i = (\bigcup_{i=1,n-1} A_i) \cup A_n$ şi aplicând formula din cazul $n = 2$ şi apoi ipoteza de inducţie, obţinem

$$\begin{aligned}
|\bigcup_{i=1,n} A_i| &= |\bigcup_{i=1,n-1} A_i| + |A_n| - |(\bigcup_{i=1,n-1} A_i) \cap A_n| \\
&= |\bigcup_{i=1,n-1} A_i| + |A_n| - |\bigcup_{i=1,n-1} (A_i \cap A_n)| \\
&= \sum_{i=1,n-1} |A_i| - \sum_{1\leq i<j\leq n-1} |A_i \cap A_j| + \cdots + (-1)^n |\bigcap_{i=1,n-1} A_i| \\
&\quad + |A_n| - \sum_{i=1,n-1} |A_i \cap A_n| + \sum_{1\leq i<j\leq n-1} |A_i \cap A_j \cap A_n| - \\
&\quad \cdots + (-1)^{n+1} |\bigcap_{i=1,n-1} (A_i \cap A_n)| \\
&= \sum_{i=1,n} |A_i| - \sum_{1\leq i<j\leq n} |A_i \cap A_j| + \cdots + (-1)^{n+1} |\bigcap_{i=1,n} A_i|.
\end{aligned}$$

4. Fie $A = \{x_1, \ldots, x_r\}$. Dacă f este injectivă, atunci $f(x_1), \ldots, f(x_r)$ sunt distincte şi cum $\{f(x_1), \ldots, f(x_r)\} \subseteq A$ rezultă că avem egalitate în ultima incluziune, deci $f(A) = A$, adică f este surjectivă.
Dacă f este surjectivă, atunci $f(A) = A$ şi deci mulţimea $f(A)$ are r elemente. Rezultă că $f(x_1), \ldots, f(x_r)$ sunt distincte, deci f este injectivă.
Am demonstrat aşadar că (a) şi (b) sunt echivalente. Aceasta arată şi că oricare dintre ele implică (c) (pentru că dacă f este injectivă şi surjectivă rezultă că f este bijectivă). Faptul că (c) implică atât (a), cât şi (b) este evident.

5. (a) Numărul funcţiilor definite pe M cu valori în N este n^m, după cum se poate verifica uşor prin inducţie după m.
(b) Pentru ca să existe funcţii injective trebuie ca $m \leq n$. În acest caz, numărul funcţiilor injective este $(n-m+1)\cdots(n-1)n$, după cum se poate

verifica simplu prin inducţie după m.
(c) Pentru ca să existe funcţii surjective trebuie ca $m \geq n$. În acest caz, fie $N = \{a_1, \ldots, a_n\}$ şi pentru fiecare $1 \leq i \leq n$ considerăm mulţimea

$$A_i = \{f : M \to N \mid f(x) \neq a_i \text{ pentru orice } x \in M\}.$$

Atunci mulţimea funcţiilor nesurjective de la M la N este $\bigcup_{1 \leq i \leq n} A_i$, deci numărul funcţiilor surjective de la M la N este $n^m - |\bigcup_{1 \leq i \leq n} A_i|$.
Folosind principiul includerii şi excluderii (vezi problema 3), avem

$$|\bigcup_{i=1,n} A_i| = \sum_{i=1,n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \cdots + (-1)^{n+1} |\bigcap_{i=1,n} A_i|.$$

Dar $|A_i| = (n-1)^m$ pentru orice $1 \leq i \leq n$. De asemenea $|A_i \cap A_j| = (n-2)^m$ pentru orice $1 \leq i < j \leq n$. În general $|A_{i_1} \cap \ldots \cap A_{i_r}| = (n-r)^m$ pentru orice $1 \leq i_1 < \ldots < i_r \leq n$ (acest număr fiind de fapt numărul funcţiilor definite pe o mulţime cu m elemente cu valori într-o mulţime cu $n - r$ elemente) şi atunci obţinem că

$$|\bigcup_{i=1,n} A_i| = C_n^1 (n-1)^m - C_n^2 (n-2)^m + \ldots + (-1)^n C_n^{n-1}.$$

Rezultă că numărul funcţiilor surjective de la M la N este

$$n^m - \sum_{k=1,n-1} (-1)^{k+1} C_n^k (n-k)^m.$$

6. Notăm cu S_n mulţimea permutărilor mulţimii $\{1, 2, \ldots, n\}$. Pentru fiecare $1 \leq i \leq n$ considerăm mulţimea $A_i = \{\sigma \in S_n \mid \sigma(i) = i\}$. Atunci mulţimea permutărilor care au cel puţin un punct fix este $\bigcup_{1 \leq i \leq n} A_i$ şi folosind principiul includerii şi excluderii (vezi problema 3) acest număr este

$$|\bigcup_{1 \leq i \leq n} A_i| = C_n^1 (n-1)! - C_n^2 (n-2)! + \ldots + (-1)^{n+1} C_n^n.$$

Pe de altă parte, mulţimea permutărilor care au exact un punct fix este

$\bigcup\limits_{1\le i\le n}(A_i-(\bigcup\limits_{j\neq i}A_j))$, deci numărul lor este

$$\begin{aligned}\sum_{1\le i\le n}|A_i-(\bigcup_{j\neq i}A_j)| &= \sum_{1\le i\le n}(|A_i|-|A_i\cap(\bigcup_{j\neq i}A_j))|)\\ &= \sum_{1\le i\le n}|A_i|-\sum_{1\le i\le n}|\bigcup_{j\neq i}(A_i\cap A_j)|\\ &= n(n-1)!-C_{n-1}^1(n-2)!+C_{n-1}^2(n-3)!-\ldots+(-1)^{n-1}C_{n-1}^{n-1}.\end{aligned}$$

7. Presupunem că B ar fi finită şi fie $x_0\in\mathbb{N}$ cu proprietatea că $x_0>x$ pentru orice $x\in A\cup B$. Rezultă că $g(f(x_0))<g(x_0)$. Fie $x_1=f(x_0)$. Atunci $g(x_1)<g(x_0)$ şi $x_1>x_0$. Fie $x_2=f(x_1)$. Atunci $x_2>x_1$ şi $g(x_2)<g(x_1)$. Continuând procedeul, obţinem un şir strict crescător de numere naturale $(x_n)_{n\ge0}$ şi unul strict descrescător $(g(x_n))_{n\ge0}$ tot de numere naturale, contradicţie.

8. Din (a) şi (b) rezultă că $f(0)<f(1)<f(2)=2$, deci $f(0)=0$ şi $f(1)=1$. Arătăm că $f(3)=3$. Într-adevăr, avem $2=f(2)<f(3)$, iar pe de altă parte $f(15)<f(18)$, de unde $f(3)f(5)=f(15)<f(18)=2f(9)<2f(10)=4f(5)$, adică $f(3)<4$.
Mai departe $3=f(3)<f(4)<f(5)<f(6)=f(2)f(3)=6$, de unde $f(n)=n$ pentru $n\le6$.
Observăm că pentru a arăta că $f=1_{\mathbb{N}}$ este suficient să arătăm că $f(k)=k$ pentru o infinitate de $k\in\mathbb{N}$. Demonstrăm prin inducţie după $n\ge1$ că $f(n(n+1))=n(n+1)$. Pentru $n=1$ şi $n=2$ este adevărat. Fie $n>2$ şi presupunem că afirmaţia este adevărată pentru $n-1$. Cum $f(n(n-1))=n(n-1)$, rezultă că $f(k)=k$ pentru $k\le n(n-1)$. Cum $f(n(n+1))=f(n)f(n+1)$ şi $n\le n(n-1)$, $n+1\le n(n-1)$, iar $(n,n+1)=1$, obţinem că $f(n(n+1))=f(n)f(n+1)=n(n+1)$, ceea ce trebuia demonstrat.

Observaţie. P. Erdös a demonstrat următorul rezultat mai general: dacă $f:\mathbb{N}^*\to\mathbb{R}$ este o funcţie strict crescătoare şi $f(mn)=f(m)f(n)$ pentru orice $m,n\in\mathbb{N}^*$ prime între ele, atunci există $\alpha\in\mathbb{R}$, $\alpha>0$, astfel încât $f(n)=n^\alpha$ pentru orice $n\in\mathbb{N}^*$.

9. **Soluţia 1.** Demonstrăm că dacă $u,v:\mathbb{N}\to\mathbb{N}$ sunt funcţii astfel încât u este injectivă, v este surjectivă şi $u\le v$, atunci $u=v$. Presupunem prin absurd că mulţimea $A=\{n\in\mathbb{N}\mid u(n)<v(n)\}$ este nevidă. Fie atunci $B=\{u(n)\mid n\in A\}$, care este o muţime nevidă de numere naturale, deci are

un cel mai mic element. Fie acesta $b = u(a)$, cu $a \in A$. Dar v este surjectivă, deci există $x \in \mathbb{N}$ cu $v(x) = b$. Dacă $x \in A$, atunci $u(x) < v(x) = b$, deci $u(x) \in B$ şi este mai mic decât b, contradicţie. Dacă $x \notin A$, atunci $u(x) = v(x) = b = u(a)$ şi cum u este injectivă, rezultă că $a = x \notin A$, contradicţie. Aşadar $A = \emptyset$ şi $u = v$.

Soluţia 2. Notăm $u = \max(f, g)$ şi $v = \min(f, g)$. Presupunem că $f \neq g$, deci există $x_0 \in \mathbb{N}$ astfel încât $f(x_0) \neq g(x_0)$. Fie de exemplu $f(x_0) > g(x_0)$. Atunci $u(x_0) = f(x_0)$ şi $v(x_0) = g(x_0)$. Cum u este surjectivă, există $x_1 \in \mathbb{N}$ cu $u(x_1) = v(x_0)$. Dar $u(x_1) \geq v(x_1)$, deci $v(x_0) \geq v(x_1)$. Dacă am avea $v(x_0) = v(x_1)$, ar rezulta că $x_0 = x_1$, deci $u(x_0) = v(x_0)$, ceea ce este fals. Rămâne că $v(x_0) > v(x_1)$.

Fie acum $x_2 \in \mathbb{N}$ astfel încât $u(x_2) = v(x_1)$. Atunci $v(x_1) \geq v(x_2)$, iar dacă am avea $v(x_1) = v(x_2)$, ar rezulta că $x_1 = x_2$, de unde $u(x_1) = v(x_1)$ şi $v(x_0) = v(x_1)$, contradicţie. Aşadar $v(x_1) > v(x_2)$. Continuând similar găsim două şiruri de numere naturale $(x_n)_{n\geq 0}$ şi $(v(x_n))_{n\geq 0}$, cel din urmă strict descrescător, ceea ce este imposibil.

10. Dacă $M = \mathbb{N}$ sau $M = \mathbb{Z}$, fie funcţiile $f, g : M \to M$ definite prin $f(x) = 2x+1$, $g(x) = [x/2]$, unde $[t]$ reprezintă partea întreagă a lui t. Atunci f este injectivă şi nesurjectivă, iar g este surjectivă şi nu este injectivă.

Funcţia $f : \mathbb{Q} \to \mathbb{Q}$, $f(x) = x^3$, este injectivă şi nu este surjectivă. Considerăm $g : \mathbb{Q} \to \mathbb{Q}$ definită prin $g(x) = x$ pentru $x \geq 0$ şi $g(x) = x + 1$ pentru $x < 0$. Atunci g este surjectivă şi nu este injectivă.

Funcţia $f : \mathbb{R} \to \mathbb{R}$, $f(x) = e^x$, este injectivă şi nu este surjectivă. Funcţia $g : \mathbb{R} \to \mathbb{R}$ definită prin $g(x) = x$ pentru $x \geq 0$ şi $g(x) = x + 1$ pentru $x < 0$, este surjectivă şi nu este injectivă.

Funcţia $f : \mathbb{C} \to \mathbb{C}$ definită prin $f(a + bi) = e^a + bi$ pentru orice $a, b \in \mathbb{R}$, este injectivă şi nu este surjectivă. Funcţia $g : \mathbb{C} \to \mathbb{C}$, $g(z) = z^2$, este surjectivă şi nu este injectivă.

11. (a) "$\Rightarrow$" Presupunem că f este injectivă. Dacă $A \cup B \neq M$, fie $x \in M$, $x \notin A \cup B$. Atunci pentru $X = \{x\}$ avem $f(X) = (\emptyset, \emptyset) = f(\emptyset)$, de unde $X = \emptyset$, contradicţie. Aşadar $A \cup B = M$.

"$\Leftarrow$" Presupunem că $A \cup B = M$. Fie $X, Y \subseteq M$ cu $f(X) = f(Y)$, deci

$X \cap A = Y \cap A$ şi $X \cap B = Y \cap B$. Atunci

$$\begin{aligned} X &= X \cap M \\ &= X \cap (A \cup B) \\ &= (X \cap A) \cup (X \cap B) \\ &= (Y \cap A) \cup (Y \cap B) \\ &= Y \cap (A \cup B) \\ &= Y \cap M \\ &= Y \end{aligned}$$

deci f este injectivă.
(b) "$\Rightarrow$" Presupunem că f este surjectivă. Dacă $A \cap B \neq \emptyset$, fie $x \in A \cap B$. Considerăm $(\{x\}, B - \{x\}) \in \mathcal{P}(A) \times \mathcal{P}(B)$. Cum f este surjectivă, există $X \in \mathcal{P}(M)$ cu $X \cap A = \{x\}$ şi $X \cap B = B - \{x\}$. Atunci $x \in X$ şi deci $x \in X \cap B$, de unde $x \in B - \{x\}$, contradicţie. Aşadar $A \cap B = \emptyset$.
"$\Leftarrow$" Presupunem că $A \cap B = \emptyset$. Fie $(X, Y) \in \mathcal{P}(A) \times \mathcal{P}(B)$. Arătăm că $f(X \cup Y) = (X, Y)$ şi de aici va rezulta că f este surjectivă. Într-adevăr, $(X \cup Y) \cap A = (X \cap A) \cup (Y \cap A) = X$ deoarece $X \subseteq A$ şi $Y \cap A \subseteq B \cap A = \emptyset$ şi $(X \cup Y) \cap B = (X \cap B) \cup (Y \cap B) = Y$ deoarece $Y \subseteq B$ şi $X \cap B \subseteq A \cap B = \emptyset$.
(c) Echivalenţa rezultă din (a) şi (b). În situaţia în care $A = C_M B$, deci f este bijectivă, inversa ei este $f^{-1} : \mathcal{P}(A) \times \mathcal{P}(B) \to \mathcal{P}(M)$, $f^{-1}(X, Y) = X \cup Y$, după cum rezultă din soluţia punctului (b).

12. Dacă ar exista o funcţie surjectivă $f : A \to \mathcal{P}(A)$, considerăm mulţimea $M = \{a \in A \mid a \notin f(a)\}$. Din surjectivitatea lui f rezultă că există $b \in A$ cu $f(b) = M$. Dacă $b \in M$, atunci din definiţia lui M rezultă că $b \notin f(b) = M$, contradicţie. Dacă $b \notin M$, atunci $b \in f(b) = M$, din nou contradicţie.

13. (a) $\Rightarrow$ (b) Fie $u, v : X \to M$ funcţii astfel încât $fu = fv$. Dacă $x \in X$ avem $fu(x) = fv(x)$, deci $f(u(x)) = f(v(x))$, şi cum f este injectivă rezultă că $u(x) = v(x)$. Obţinem că $u = v$.
(b) $\Rightarrow$ (c) Fie $y \in N$ astfel încât există $x \in M$ cu $f(x) = y$. Arătăm că există un unic x cu această proprietate. Într-adevăr, dacă $x_1, x_2 \in M$ şi $f(x_1) = f(x_2) = y$, atunci fie $u, v : \{0\} \to M$ definite prin $u(0) = x_1$, $v(0) = x_2$. Atunci $fu = fv$, de unde $u = v$, ceea ce arată că $x_1 = x_2$.
Acum fixăm un element $a \in M$ şi definim $g : N \to M$ astfel:

• Dacă $y \in N - f(M)$, atunci $g(y) = a$.
• Dacă $y \in f(M)$, atunci $g(y) = x$, unde x este unicul element din M cu proprietatea că $f(x) = y$.
Este evident că $gf = 1_M$.
(c) $\Rightarrow$ (a) Fie $x, y \in M$ cu proprietatea că $f(x) = f(y)$. Ştim că există o funcţie $g : N \to M$ astfel încât $gf = 1_M$. Atunci $g(f(x)) = g(f(y))$ implică $x = y$.

14. (a) $\Rightarrow$ (b) Deoarece $\bigcap_{i\in I} M_i \subseteq M_j$ pentru orice $j \in I$, rezultă că $f(\bigcap_{i\in I} M_i) \subseteq f(M_j)$, şi deci $f(\bigcap_{i\in I} M_i) \subseteq \bigcap_{i\in I} f(M_i)$.
Fie acum $y \in \bigcap_{i\in I} f(M_i)$. Atunci, pentru orice $i \in I$ există $x_i \in M_i$ cu $y = f(x_i)$. Deoarece f este injectivă rezultă că $x_i = x_j$ pentru orice $i, j \in I$, de unde $x = x_i \in M_j$ pentru orice $j \in I$, deci $x \in \bigcap_{i\in I} M_i$. Cum $y = f(x)$, rezultă că $y \in f(\bigcap_{i\in I} M_i)$.
(b) $\Rightarrow$ (a) Presupunem prin absurd că f nu ar fi injectivă şi fie $x, y \in M$, $x \neq y$, cu $f(x) = f(y)$. Fie $M_1 = \{x\}$ şi $M_2 = \{y\}$. Atunci $f(M_1) \cap f(M_2) = \{f(x)\}$, dar $f(M_1 \cap M_2) = f(\emptyset) = \emptyset$, contradicţie.

15. (a) $\Rightarrow$ (c) Pentru fiecare $n \in N$ alegem un element $x_n \in M$ astfel încât $f(x_n) = n$. Definim $g : N \to M$ prin $g(n) = x_n$ pentru orice $n \in N$. Evident are loc $fg = 1_N$.
(c) $\Rightarrow$ (b) Fie $u, v : N \to Y$ astfel încât $uf = vf$. Atunci $ufg = vfg$, deci $u1_N = v1_N$, de unde rezultă că $u = v$.
(b) $\Rightarrow$ (a) Presupunem prin absurd că f nu este surjectivă. Atunci alegem un $n_0 \in N - f(M)$. Fie $Y = \{0, 1\}$ şi funcţiile $u, v : N \to Y$ definite prin $u(n) = 0$ dacă $n \neq n_0$, $u(n_0) = 1$ şi $v(n) = 0$ pentru orice $n \in N$. Atunci $uf = vf$, dar $u \neq v$, contradicţie.

16. (i) (a) $\Rightarrow$ (b) Fie $X, Y \subseteq M$ cu $f_*(X) = f_*(Y)$, deci $f(X) = f(Y)$. Fie $x \in X$. Atunci $f(x) \in f(X) = f(Y)$, deci există $y \in Y$ cu $f(x) = f(y)$. Cum f este injectivă, rezultă că $x = y \in Y$. Aşadar $X \subseteq Y$ şi analog $Y \subseteq X$, de unde $X = Y$.
(b) $\Rightarrow$ (c) Fie $X \subseteq M$. Trebuie să arătăm că $f^{-1}(f(X)) = X$. Dacă $x \in X$, atunci $f(x) \in f(X)$, deci $x \in f^{-1}(f(X))$, ceea ce arată că $X \subseteq f^{-1}(f(X))$. Invers, dacă $a \in f^{-1}(f(X))$, atunci $f(a) \in f(X)$, deci există $x \in X$ cu

$f(a) = f(x)$. Atunci $f_*(\{a\}) = f_*(\{x\})$ şi cum f_* este injectivă rezultă că $\{a\} = \{x\}$, deci $a = x \in X$. Aşadar $f^{-1}(f(X)) \subseteq X$, ceea ce arată egalitatea.
(c) $\Rightarrow$ (d) Cum $f^* \circ f_*$ este surjectivă, rezultă că şi f^* este surjectivă.
(d) $\Rightarrow$ (e) Presupunem prin absurd că există $X \subseteq M$ şi $y \in N$ cu $y \in f(C_M X)$ şi $y \notin C_N f(X)$. Atunci $y = f(a)$ cu $a \notin X$ şi $y \in f(X)$, deci $y = f(x)$ cu $x \in X$. Folosind surjectivitatea lui f^* rezultă că pentru $\{a\} \in \mathcal{P}(M)$ există $Y \subseteq N$ astfel încât $\{a\} = f^*(Y) = f^{-1}(Y)$ cu $Y \subseteq N$. Atunci $y = f(a) \in Y$, de unde rezultă că şi $x \in f^{-1}(Y) = \{a\}$, contradicţie.
(e) $\Rightarrow$ (a) Presupunem prin absurd că f nu este injectivă. Fie $a, b \in M$ cu $a \neq b$ şi $f(a) = f(b)$. Atunci pentru $X = \{a\}$ avem $b \in C_M X$, deci $f(b) \in f(C_M X)$. Pe de altă parte $f(a) \in f(X)$, deci $f(a) \notin C_N f(X)$, contradicţie.
(ii) Se demonstrează similar cu (i).

17. (a) Definim aplicaţiile $f : \mathrm{Fun}(A, \mathrm{Fun}(B, C)) \to \mathrm{Fun}(A \times B, C)$ şi $g : \mathrm{Fun}(A \times B, C) \to \mathrm{Fun}(A, \mathrm{Fun}(B, C))$ prin $f(u)(a, b) = u(a)(b)$ şi $g(v)(a)(b) = v(a, b)$ pentru orice $u \in \mathrm{Fun}(A, \mathrm{Fun}(B, C))$, $v \in \mathrm{Fun}(A \times B, C)$, $a \in A, b \in B$. Atunci

$$\begin{aligned}(f \circ g)(v)(a, b) &= f(g(v))(a, b) \\ &= g(v)(a)(b) \\ &= v(a, b)\end{aligned}$$

şi

$$\begin{aligned}(g \circ f)(u)(a)(b) &= g(f(u))(a)(b) \\ &= f(u)(a, b) \\ &= u(a)(b)\end{aligned}$$

ceea ce arată că $f \circ g$ şi $g \circ f$ sunt aplicaţiile identice, deci f şi g sunt inverse una celeilalte.
(b) Notăm cu $p_B : B \times C \to B$ şi $p_C : B \times C \to C$ proiecţiile canonice.
Definim aplicaţia $f : \mathrm{Fun}(A, B \times C) \to \mathrm{Fun}(A, B) \times \mathrm{Fun}(A, C)$ prin $f(u) = (p_B u, p_C u)$.
Dacă $f(u) = f(v)$, atunci $p_B u = p_B v$ şi $p_C u = p_C v$, de unde $u(a) = (p_B u(a), p_C u(a)) = (p_B v(a), p_C v(a)) = v(a)$, deci $u = v$. Obţinem că f este injectivă.

Fie acum $(\phi_1, \phi_2) \in \mathrm{Fun}(A, B) \times \mathrm{Fun}(A, C)$. Definim $u \in \mathrm{Fun}(A, B \times C)$ prin $u(a) = (\phi_1(a), \phi_2(a))$. Atunci $p_B u = \phi_1$ şi $p_C u = \phi_2$, deci $f(u) = (\phi_1, \phi_2)$. Aceasta arată că f este şi surjectivă, deci este o bijecţie.
Dacă $A \cap B = \emptyset$, atunci aplicaţia $f : \mathrm{Fun}(A, C) \times \mathrm{Fun}(B, C) \to \mathrm{Fun}(A \cup B, C)$ definită prin $f(u, v)(x) = u(x)$ dacă $x \in A$ şi $f(u, v)(x) = v(x)$ dacă $x \in B$, este bine definită şi bijectivă. Într-adevăr, dacă $f(u, v) = f(g, h)$ pentru $u, g \in \mathrm{Fun}(A, C)$ şi $v, h \in \mathrm{Fun}(B, C)$, atunci $u(a) = f(u, v)(a) = f(g, h)(a) = g(a)$ pentru orice $a \in A$ şi $v(b) = f(u, v)(b) = f(g, h)(b) = h(b)$ pentru orice $b \in B$, deci f este injectivă. De asemenea, dacă $g \in \mathrm{Fun}(A \cup B, C)$, definim $u \in \mathrm{Fun}(A, C)$ şi $v \in \mathrm{Fun}(B, C)$ prin $u(a) = g(a)$ pentru orice $a \in A$ şi $v(b) = g(b)$ pentru orice $b \in B$. Atunci $g = f(u, v)$, deci f este şi surjectivă.

18. Este imediat că $\sim$ este reflexivă, simetrică şi tranzitivă. Fie $f : \mathbb{R} \to [0, 1)$, $f(x) = \{x\}$, unde prin $\{x\}$ notăm partea fracţionară a lui x. Pentru orice $x, y \in \mathbb{R}$ avem că

$$\begin{aligned} x \sim y &\Leftrightarrow x - y \in \mathbb{Z} \\ &\Leftrightarrow [x] + \{x\} - [y] - \{y\} \in \mathbb{Z} \\ &\Leftrightarrow \{x\} - \{y\} \in \mathbb{Z} \\ &\Leftrightarrow \{x\} = \{y\} \\ &\Leftrightarrow f(x) = f(y) \end{aligned}$$

deci $\sim = \rho_f$, unde ρ_f este relaţia de echivalenţă asociată funcţiei f. Din proprietatea de universalitate a mulţimii factor rezultă că există o funcţie $f' : \mathbb{R}/\sim \to [0, 1)$ astfel încât $f'p = f$, unde $p : \mathbb{R} \to \mathbb{R}/\sim$ este proiecţia canonică. Cum $\sim = \rho_f$, avem că f' este injectivă, iar surjectivitatea lui f arată că f' este surjectivă. Prin urmare f' este o bijecţie.

19. Se verifică imediat că ρ este reflexivă, antisimetrică şi tranzitivă, deci este relaţie de ordine. Dacă $x = 1$ şi $y = 3/2$, atunci nici una din relaţiile $x \rho y$ şi $y \rho x$ nu este adevărată, deci ρ nu este totală.

20. ρ' este reflexivă deoarece $\Delta_M \subseteq \rho'$.
Arătăm că ρ' este simetrică. Fie $x, y \in M$ cu $x \rho' y$. Atunci $x \Delta_M y$ sau există $n \geq 1$ cu $x(\rho \cup \rho^{-1})^n y$, deci $x = y$ sau există $n \geq 1$ şi $s_1, \ldots, s_{n-1} \in M$ cu $x(\rho \cup \rho^{-1})s_1, \ldots, s_{n-1}(\rho \cup \rho^{-1})y$. Este uşor de văzut că relaţia $\rho \cup \rho^{-1}$ este simetrică şi atunci obţinem că $y \Delta_M x$ şi $y(\rho \cup \rho^{-1})s_{n-1}, \ldots, s_1(\rho \cup \rho^{-1})x$, deci $y \Delta_M x$ sau $y(\rho \cup \rho^{-1})^n x$, ceea ce arată că $y \rho' x$.

Arătăm că ρ' este tranzitivă. Presupunem că $x\rho' y$ şi $y\rho' z$.Dacă $x = y$ sau $y = z$ este clar că $x\rho' z$. Altfel, există $m, n \geq 1$ cu $x(\rho \cup \rho^{-1})^m y$ şi $y(\rho \cup \rho^{-1})^n z$. Aceasta arată că $x(\rho \cup \rho^{-1})^{m+n} z$, de unde $x\rho' z$.
Arătăm că ρ' este cea mai mică relaţie de echivalenţă care include pe ρ. Fie ρ'' o altă relaţie de echivalenţă cu $\rho \subseteq \rho''$. Este clar că $\rho \cup \rho^{-1} \subseteq \rho''$ şi $\Delta_M \subseteq \rho''$. Dacă $x(\rho \cup \rho^{-1})^n y$, atunci există $s_1, \ldots, s_{n-1} \in M$ cu $x(\rho \cup \rho^{-1}) s_1, \ldots, s_{n-1}(\rho \cup \rho^{-1}) y$. Cum $\rho \cup \rho^{-1} \subseteq \rho''$, avem şi $x\rho'' s_1, \ldots, s_{n-1}\rho'' y$, deci cum ρ'' este tranzitivă avem şi $x\rho'' y$. Obţinem că $(\rho \cup \rho^{-1})^n \subseteq \rho''$ pentru orice n, şi de aici rezultă că $\rho' \subseteq \rho''$.

21. Verificăm mai întâi că ρ este relaţie de echivalenţă.
• ρ este reflexivă: avem $(x_1, \ldots, x_n)\rho(x_1, \ldots, x_n)$ deoarece $x_i \rho_i x_i$ pentru orice $1 \leq i \leq n$, ρ_i fiind reflexivă.
• ρ este simetrică: dacă $(x_1, \ldots, x_n)\rho(y_1, \ldots, y_n)$, atunci $x_i \rho_i y_i$, de unde $y_i \rho_i x_i$ pentru fiecare $1 \leq i \leq n$, ρ_i fiind simetrică, deci $(y_1, \ldots, y_n)\rho(x_1, \ldots, x_n)$.
• ρ este tranzitivă: dacă $(x_1, \ldots, x_n)\rho(y_1, \ldots, y_n)$ şi $(y_1, \ldots, y_n)\rho(z_1, \ldots, z_n)$, atunci pentru orice i avem $x_i \rho_i y_i$ şi $y_i \rho_i z_i$, şi din tranzitivitatea lui ρ_i rezultă că $x_i \rho_i z_i$, ceea ce arată că $(x_1, \ldots, x_n)\rho(z_1, \ldots, z_n)$.

Vom construi o bijecţie de la M/ρ la $M_1/\rho_1 \times \cdots \times M_n/\rho_n$ folosind proprietatea de universalitate a mulţimii factor. Fie $f : M \to M_1/\rho_1 \times \cdots \times M_n/\rho_n$ funcţia definită prin $f(x_1, \ldots, x_n) = (\widehat{x_1}, \ldots, \widehat{x_n})$, unde pe poziţia i am notat prin $\widehat{x_i}$ clasa de echivalenţă a lui x_i în mulţimea factor M_i/ρ_i. Notăm cu ρ_f relaţia de echivalenţă pe M asociată funcţiei f. Avem $(x_1, \ldots, x_n)\rho_f(y_1, \ldots, y_n) \Leftrightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n) \Leftrightarrow \widehat{x_i} = \widehat{y_i}$ pentru orice $i \Leftrightarrow x_i \rho_i y_i$ pentru orice $i \Leftrightarrow (x_1, \ldots, x_n)\rho(y_1, \ldots, y_n)$, deci $\rho = \rho_f$. Atunci există $f' : M/\rho \longrightarrow M_1/\rho_1 \times \cdots \times M_n/\rho_n$ astfel încât $f'p = f$, unde $p : M \to M/\rho$ este proiecţia canonică. Cum $\rho = \rho_f$, avem că f' este injectivă. Este evident că f este surjectivă, de unde şi f' este surjectivă. Prin urmare f' este bijectivă.

22. Fie R_k mulţimea relaţiilor de echivalenţă ρ pe M cu proprietatea că mulţimea factor M/ρ are k elemente. Notăm cu $N_{m,k} = |R_k|$. Numărul relaţiilor de echivalenţă pe M este $N_{m,1} + \ldots + N_{m,m}$.

Pentru a calcula $N_{m,k}$ să observăm că oricărui $\rho \in R_k$ îi putem asocia o surjecţie de la M la mulţimea $\{1, \ldots, k\}$ în modul următor: compunem o bijecţie de la M/ρ la $\{1, \ldots, k\}$ cu proiecţia canonică $p : M \to M/\rho$. Invers, oricărei surjecţii $f : M \to \{1, \ldots, k\}$ îi asociem relaţia de echivalenţă ρ_f, care se află în R_k, deoarece din proprietatea de universalitate a mulţimii factor

există $f' : M/\rho_f \to \{1, \ldots, k\}$ cu $f'p = f$, şi atunci f' este bijectivă, deci $|M/\rho_f| = k$.

Fie acum $f, g : M \to \{1, \ldots, k\}$ surjective. Vom arăta că $\rho_f = \rho_g \Leftrightarrow$ există o permutare $\sigma \in S_k$ cu $g = \sigma f$. Implicaţia "$\Leftarrow$" este evidentă. Invers, fie $\rho_f = \rho_g = \rho$. Atunci există $f', g' : M/\rho \longrightarrow \{1, \ldots, k\}$ bijective astfel încât $f'p = f$ şi $g'p = g$. Luăm $\sigma = g'(f')^{-1} \in S_k$ şi rezultă că $g = \sigma f$.

Aşadar, la $k!$ surjecţii corespunde aceeaşi relaţie de echivalenţă în corespondenţa descrisă mai sus, deci $N_{m,k} = S_{m,k}/k!$, unde $S_{m,k}$ este numărul surjecţiilor definite pe o mulţime cu m elemente cu valori într-o mulţime cu k elemente, care a fost calculat în problema 5.

23. Este imediat că ρ este o relaţie de echivalenţă. Fie $f : \mathcal{P}(A) \to \mathcal{P}(B)$ definită prin $f(X) = X \cap B$. Este clar că $\rho = \rho_f$. Din proprietatea de universalitate a mulţimii factor rezultă că există $f' : \mathcal{P}(A)/\rho \to \mathcal{P}(B)$ injectivă astfel încât $f'p = f$. Atunci f' este şi surjectivă. Într-adevăr, dacă $Y \in \mathcal{P}(B)$, atunci $f(Y) = Y$. Aşadar f' este bijectivă.

24. Este imediat că ρ este relaţie de echivalenţă. Fie $F : B^A \to B^{A'}$ definită prin $F(f) = f_{|A'}$. Atunci $f \rho g \Leftrightarrow f_{|A'} = g_{|A'} \Leftrightarrow F(f) = F(g)$, deci $\rho = \rho_F$ şi din proprietatea de universalitate a mulţimii factor există $F' : B^A/\rho \to B^{A'}$ injectivă cu $F'p = F$, unde $p : B^A \to B^A/\rho$ este proiecţia canonică. Pentru a arăta că F' este şi surjectivă este suficient să arătăm că F este surjectivă. Pentru aceasta fie $g \in B^{A'}$ şi fie $b \in B$. Definim $f : A \to B$ prin $f(a) = g(a)$ dacă $a \in A'$ şi $f(a) = b$ dacă $a \in A - A'$. Atunci avem $F(f) = g$, deci F este surjectivă. Prin urmare F' este bijectivă.

25. (a) Evident $A \sim A$ deoarece $1_A : A \to A$ este bijectivă.
(b) Cum $A \sim B$, există o bijecţie $f : A \to B$. Atunci $f^{-1} : B \to A$ este bijecţie, deci $B \sim A$.
(c) Dacă $f : A \to B$ şi $g : B \to C$ sunt bijecţii, atunci $gf : A \to C$ este bijecţie, deci $A \sim C$.

26. (a) Fie $f : X_0 \to X_2$ o bijecţie. Definim prin recurenţă şirul de mulţimi $(X_n)_{n \geq 3}$ prin $X_n = f(X_{n-2})$ pentru orice $n \geq 3$. Se demonstrează imediat prin inducţie că $X_n \supseteq X_{n+1}$ pentru orice $n \geq 0$. Notăm $A = \bigcap_{n \geq 0} X_n$

şi $B_n = X_n - X_{n+1}$ pentru orice $n \geq 0$. Arătăm că

$$X_0 = A \cup (\bigcup_{n\geq 0} B_n) \text{ şi } X_1 = A \cup (\bigcup_{n\geq 1} B_n).$$

Pentru prima egalitate, fie $a \in X_0$. Dacă $a \in A$, atunci evident a aparţine membrului drept. Dacă $a \notin A$, fie n cel mai mic număr natural pentru care $a \notin X_n$. Evident $n > 0$. Atunci $a \in X_{n-1}$ şi $a \notin X_n$, deci $a \in B_{n-1}$, aşadar a aparţine şi membrului drept. Incluziunea inversă este clară, toate mulţimile din reuniune fiind submulţimi ale lui X_0. A doua egalitate se demonstrează similar.
În plus, observăm că în fiecare din cele două relaţii demonstrate în membrul drept avem o reuniune disjunctă de mulţimi (adică intersecţia oricăror două mulţimi din reuniune este vidă).
Arătăm acum că pentru orice $n \geq 0$ are loc $f(B_n) = B_{n+2}$. Într-adevăr, avem $B_{n+2} = X_{n+2} - X_{n+3} = f(X_n) - f(X_{n+1}) = f(X_n - X_{n+1}) = f(B_n)$ (pentru a treia egalitate am folosit faptul că f este injectivă).
Atunci putem defini funcţia $g_n : B_n \to B_{n+2}$ prin $g_n(x) = f(x)$ pentru orice $x \in B_n$. Este clar că g_n este bijectivă. Definim acum $g : X_0 \to X_1$ astfel:
• $g(x) = x$ pentru orice $x \in A \cup (\bigcup_{n\geq 0} B_{2n+1})$.
• $g(x) = g_{2n}(x)$ dacă $x \in B_{2n}$, $n \in \mathbb{N}$.
Atunci g este bijectivă, şi aceasta arată că există o bijecţie între X_0 şi X_1.
(b) Fie $\alpha = |A| = |A'|$ şi $\beta = |B| = |B'|$ numere cardinale. Considerăm bijecţiile $u : A \to A'$ şi $v : B \to B'$ şi presupunem că există o funcţie injectivă $f : A \to B$. Atunci $vfu^{-1} : A' \to B'$ este injectivă, deci definiţia nu depinde de reprezentanţii A şi B.
(c) Fie $\alpha = |A|$ şi $\beta = |B|$. Cum $\alpha \leq \beta$ şi $\beta \leq \alpha$, rezultă că există funcţii injective $f : A \to B$ şi $g : B \to A$. Atunci $f(A) \subseteq B$ şi $gf(A) \subseteq g(B) \subseteq A$. Dar dacă $u : X \to Y$ este o funcţie injectivă, atunci $X \sim u(X)$. Aplicând această observaţie de două ori obţinem că $A \sim f(A) \sim gf(A)$ şi atunci conform punctului (a) rezultă că $A \sim g(B)$. Dar $g(B) \sim B$, de unde $A \sim B$.

27. Fie $\alpha = |A|$ şi $\beta = |B|$. Considerăm mulţimea

$$\mathcal{F} = \{(X, f) \mid X \subseteq A \text{ şi } f : X \to B \text{ funcţie injectivă}\}.$$

Evident $\mathcal{F}$ este nevidă (putem alege o submulţime a lui A cu un singur element şi $f : X \to B$ o funcţie arbitrară). În plus, $\mathcal{F}$ poate fi ordonată astfel: $(X_1, f_1) \leq (X_2, f_2)$ dacă şi numai dacă $X_1 \subseteq X_2$ şi restricţia lui f_2 la

X_1 este f_1. Arătăm că $\mathcal{F}$ este inductiv ordonată cu această relaţie de ordine. Fie $(X_i, f_i)_{i\in I}$ un lanţ (submulţime total ordonată) în $\mathcal{F}$. Arătăm că el are un majorant în $\mathcal{F}$. Pentru aceasta fie $X = \bigcup_{i\in I} X_i$ şi $f : X \to B$ funcţia definită astfel: dacă $x \in X$, alegem un $i \in I$ cu $x \in X_i$, şi definim $f(x) = f_i(x)$. Definiţia lui f este corectă. Într-adevăr, fie $x \in X_i$ şi $x \in X_j$. Avem $(X_i, f_i) \leq (X_j, f_j)$ sau $(X_j, f_j) \leq (X_i, f_i)$. În primul caz (al doilea este similar) ştim că f_i este restricţia lui f_j la X_i, deci cum $x \in X_i$, avem că $f_j(x) = f_i(x)$.
Funcţia f definită mai sus este injectivă, deoarece dacă $x, y \in X$ cu $f(x) = f(y)$, atunci există $i, j \in I$ cu $x \in X_i$ şi $y \in X_j$. Presupunem, de exemplu, că $(X_j, f_j) \leq (X_i, f_i)$, şi atunci $f(x) = f_i(x)$ şi $f(y) = f_j(y) = f_i(y)$. Din injectivitatea lui f_i rezultă că $x = y$. Aşadar $(X, f) \in \mathcal{F}$ şi $(X_i, f_i) \leq (X, f)$ pentru orice $i \in I$.
Din lema lui Zorn rezultă că $\mathcal{F}$ are un element maximal (Y, g). Dacă g este surjectivă, atunci există o funcţie injectivă $g' : B \to Y$ şi atunci $\beta = |B| \leq |Y| \leq |A| = \alpha$. Dacă g nu este surjectivă, atunci fie $b \in B - g(Y)$. Dacă $Y \neq A$, considerăm $a \in A - Y$ şi definim funcţia $f : Y \cup \{a\} \to B$ prin $f_{|Y} = g$ şi $f(a) = b$. Atunci $(Y \cup \{a\}, f) \in \mathcal{F}$ şi această pereche este strict mai mare ca (Y, g), contradicţie. Aşadar $Y = A$ şi atunci $\alpha = |A| \leq |B| = \beta$. Am demonstrat deci că avem $\alpha \leq \beta$ sau $\beta \leq \alpha$. De aici rezultă că are loc una din (i) $\alpha < \beta$; (ii) $\alpha = \beta$; (iii) $\beta < \alpha$. Folosind problema 26, rezultă că nu pot avea loc simultan două dintre aceste condiţii.

28. (a) Fie X o mulţime infinită şi $x_0 \in X$. Atunci $X - \{x_0\}$ este nevidă, deci există $x_1 \in X$, $x_1 \neq x_0$. Construim inductiv un şir $(x_n)_{n\in\mathbb{N}}$ astfel: dacă am definit $x_0, \ldots, x_n \in X$, oricare două distincte, atunci $X - \{x_0, \ldots, x_n\}$ este nevidă (altfel ar rezulta $X = \{x_0, \ldots, x_n\}$), deci există $x_{n+1} \in X$ şi x_{n+1} să fie diferit de toţi $x_0, \ldots, x_n$.
Definim acum funcţia injectivă $f : \mathbb{N} \to X$ prin $f(n) = x_n$ pentru orice $n \in \mathbb{N}$. Rezultă că $|\mathbb{N}| \leq |X|$.
(b) Fie $F = \{y_0, \ldots, y_r\}$. Mulţimea $X - F$ este infinită, altfel $X = F \cup (X - F)$ ar fi finită. Atunci, din (i), există o submulţime numărabilă A a lui $X - F$. Fie $A = \{a_0, a_1, \ldots\}$. Definim funcţia $f : X \to X - F$ astfel:
• $f(x) = x$ pentru orice $x \in X - (F \cup A)$.
• $f(y_i) = a_i$ pentru orice $0 \leq i \leq r$.
• $f(a_j) = a_{j+r}$ pentru orice $j \in \mathbb{N}$.
Atunci este clar că f este bijectivă, deci $|X - F| = |X|$.

29. Să observăm mai întâi că pentru orice numere cardinale α şi β putem alege mulţimi A şi B cu $|A| = \alpha$, $|B| = \beta$ şi $A \cap B = \emptyset$. Într-adevăr, dacă U şi V sunt mulţimi cu $|U| = \alpha$ şi $|V| = \beta$, putem lua $A = U \times \{1\}$ şi $B = V \times \{2\}$.
(a) Dacă $\alpha = |A| = |A'|$ şi $\beta = |B| = |B'|$ cu $A \cap B = \emptyset$ şi $A' \cap B' = \emptyset$, fie $f : A \to A'$ şi $g : B \to B'$ bijecţii. Atunci funcţia $u : A \cup B \to A' \cup B'$ definită prin $u(x) = f(x)$ dacă $x \in A$, şi $u(x) = g(x)$ dacă $x \in B$, este bijectivă deci $|A \cup B| = |A' \cup B'|$.
(b) Fie $\alpha = |A|, \beta = |B|, \gamma = |C|$, cu A, B, C două câte două disjuncte. Atunci $\alpha + \beta = |A \cup B| = |B \cup A| = \beta + \alpha$ şi $(\alpha + \beta) + \gamma = |(A \cup B) \cup C| = |A \cup (B \cup C)| = \alpha + (\beta + \gamma)$.
(c) Demonstrăm mai întâi că $\alpha + \alpha = \alpha$. Fie $\alpha = |A|$, unde A este mulţime infinită. Considerăm mulţimea

$$\mathcal{F} = \{(X, f) \mid \emptyset \neq X \subseteq A \text{ şi } f : X \times \{0, 1\} \to X \text{ funcţie bijectivă}\}.$$

Arătăm că $\mathcal{F}$ este nevidă. Pentru aceasta fie o funcţie injectivă $u : \mathbb{N} \to A$ (existenţa unei astfel de funcţii este asigurată de problema 28). Notăm $X = u(\mathbb{N})$ şi $x_n = u(n)$ pentru orice $n \in \mathbb{N}$. Atunci aplicaţia $f : X \times \{0, 1\} \to X$ definită prin $f(x_n, 0) = x_{2n}$ şi $f(x_n, 1) = x_{2n+1}$ pentru orice $n \in \mathbb{N}$, este bijectivă, deci $(X, f) \in \mathcal{F}$.
Definim pe $\mathcal{F}$ o relaţie de ordine astfel: $(X, f) \leq (Y, g)$ dacă şi numai dacă $X \subseteq Y$ şi $g(t) = f(t)$ pentru orice $t \in X \times \{0, 1\}$. Atunci $(\mathcal{F}, \leq)$ este o mulţime inductiv ordonată. Într-adevăr, fie $(X_i, f_i)_{i \in I}$ un lanţ în $\mathcal{F}$. Luăm $X = \bigcup_{i \in I} X_i$ şi definim $f : X \times \{0, 1\} \to X$ astfel: dacă $t \in X \times \{0, 1\}$, atunci există $i \in I$ cu $t \in X_i \times \{0, 1\}$ şi punem $f(t) = f_i(t)$. Definiţia este corectă, deoarece dacă $t \in X_i \times \{0, 1\}$ şi $t \in X_j \times \{0, 1\}$, atunci din condiţia de lanţ putem presupune, de exemplu, că $(X_i, f_i) \leq (X_j, f_j)$ şi obţinem $f_i(t) = f_j(t)$. Deoarece fiecare f_i este surjectivă, rezultă că şi f este surjectivă.
Arătăm că f este injectivă. Dacă $f(t) = f(t')$, fie $i, j \in I$ cu $t \in X_i \times \{0, 1\}$ şi $t' \in X_j \times \{0, 1\}$. Ca mai sus putem presupune că $(X_i, f_i) \leq (X_j, f_j)$ şi atunci $f(t) = f_i(t) = f_j(t)$ şi $f(t') = f_j(t')$. Cum f_j este injectivă, rezultă că $t = t'$.
Prin urmare $(X, f) \in \mathcal{F}$ şi această pereche este un majorant pentru lanţul dat. Din lema lui Zorn rezultă că $\mathcal{F}$ are un element maximal (Y, g).
Arătăm că $A - Y$ este finită. Altfel, dacă $A - Y$ ar fi infinită, fie C o submulţime numărabilă a lui $A - Y$ şi $h : C \times \{0, 1\} \to C$ o bijecţie construită

ca în prima parte a soluţiei. Atunci aplicaţia $p : (Y \cup C) \times \{0,1\} \to (Y \cup C)$ definită prin $p(t) = g(t)$ dacă $t \in Y \times \{0,1\}$ şi $p(t) = h(t)$ dacă $t \in C \times \{0,1\}$, este bijectivă, deoarece g şi h sunt bijecţii. Prin urmare $(Y \cup C, p) \in \mathcal{F}$ şi $(Y, g) < (Y \cup C, p)$, contradicţie cu maximalitatea lui (Y, g).
Aşadar $A - Y$ este finită şi cum A este infinită rezultă că $|Y| = |A| = \alpha$. Avem atunci

$$\alpha = |Y| = |Y \times \{0,1\}| = |(Y \times \{0\}) \cup (Y \times \{1\})| = |Y \times \{0\}| + |Y \times \{1\}| = \alpha + \alpha.$$

Dacă β este un număr cardinal cu $\beta \leq \alpha$, atunci $\alpha \leq \alpha + \beta \leq \alpha + \alpha = \alpha$, de unde, conform problemei 26, rezultă că $\alpha + \beta = \alpha$.

30. (a) Fie $\alpha = |A| = |A'|$ şi $\beta = |B| = |B'|$. Considerăm bijecţiile $f : A \to A'$ şi $g : B \to B'$. Atunci aplicaţia $u : A \times B \to A' \times B'$ definită prin $u(a,b) = (f(a), g(b))$ este bijectivă, deci $|A \times B| = |A' \times B'|$.
(b) Fie $\alpha = |A|, \beta = |B|, \gamma = |C|$, unde putem presupune că $B \cap C = \emptyset$. Atunci aplicaţia $f : (A \times B) \times C \to A \times (B \times C)$, $f((a,b),c) = (a,(b,c))$ este bijectivă, deci $(\alpha\beta)\gamma = |(A \times B) \times C| = |A \times (B \times C)| = \alpha(\beta\gamma)$.
Apoi $g : A \times B \to B \times A$, $g(a,b) = (b,a)$, este bijectivă, deci $\alpha\beta = |A \times B| = |B \times A| = \beta\alpha$ şi $A \times (B \cup C) = (A \times B) \cup (A \times C)$, deci $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.
(c) Dacă α este un număr cardinal infinit, arătăm mai întâi că $\alpha\alpha = \alpha$. Considerăm mulţimea

$$\mathcal{F} = \{(X, f) \mid \emptyset \neq X \subseteq A \text{ şi } f : X \times X \to X \text{ bijecţie}\}.$$

Pentru a arăta că $\mathcal{F}$ este nevidă, observăm mai întâi că există o bijecţie $u : \mathbb{N}^* \times \mathbb{N}^* \to \mathbb{N}^*$ definită prin $u(m,n) = 2^{m-1}(2n-1)$. Considerăm o submulţime numărabilă X a lui A şi atunci u induce o bijecţie $u' : X \times X \to X$ via o bijecţie între $\mathbb{N}^*$ şi X. Rezultă că $(X, u') \in \mathcal{F}$.
Definim pe $\mathcal{F}$ o relaţie de ordine astfel: $(X, f) \leq (Y, g)$ dacă şi numai dacă $X \subseteq Y$ şi $g(t) = f(t)$ pentru orice $t \in X \times X$. Arătăm că $(\mathcal{F}, \leq)$ este o mulţime inductiv ordonată. Fie $(X_i, f_i)_{i \in I}$ un lanţ din $\mathcal{F}$. Luăm $X = \bigcup_{i \in I} X_i$ şi definim $f : X \times X \to X$ astfel: dacă $t \in X \times X$, atunci există $i \in I$ cu $t \in X_i \times X_i$ şi definim $f(t) = f_i(t)$. Definiţia este corectă, deoarece dacă $t \in X_i \times X_i$ şi $t \in X_j \times X_j$, atunci din condiţia de lanţ putem presupune, de exemplu, că $(X_i, f_i) \leq (X_j, f_j)$ şi obţinem $f_i(t) = f_j(t)$.
Deoarece fiecare f_i este surjectivă, rezultă că şi f este surjectivă.
Arătăm că f este injectivă. Dacă $f(t) = f(t')$, fie $i, j \in I$ cu $t \in X_i \times X_i$ şi

$t' \in X_j \times X_j$. Ca mai sus putem presupune că $(X_i, f_i) \leq (X_j, f_j)$ şi atunci $f(t) = f_i(t) = f_j(t)$ şi $f(t') = f_j(t')$. Cum f_j este injectivă, rezultă că $t = t'$. Prin urmare $(X, f) \in \mathcal{F}$ şi această pereche este un majorant pentru lanţul dat.
Din lema lui Zorn rezultă că $\mathcal{F}$ are un element maximal (Y, g). Arătăm că $|A - Y| < |Y|$. Altfel, am avea $|Y| \leq |A - Y|$ şi putem alege $D \subseteq A - Y$ cu $|D| = |Y|$. Atunci $(Y \cup D) \times (Y \cup D) = (Y \times Y) \cup (Y \times D) \cup (D \times Y) \cup (D \times D)$ şi evident reuniunea din membrul drept al ultimei egalităţi este disjunctă. Atunci

$$\begin{aligned} |(Y \times D) \cup (D \times Y) \cup (D \times D)| &= |Y \times D| + |D \times Y| + |D \times D| \\ &= |Y||D| + |D||Y| + |D||D| \\ &= |Y||Y| + |Y||Y| + |Y||Y| \\ &= |Y| + |Y| + |Y| \\ &= |Y| \\ &= |D|. \end{aligned}$$

Am folosit că $|Y||Y| = |Y|$, fapt care rezultă din existenţa bijecţiei g, şi de asemenea faptul că $|Y| + |Y| = |Y|$, care rezultă din problema 29. Prin urmare există o bijecţie $h : (Y \times D) \cup (D \times Y) \cup (D \times D) \to D$ şi atunci putem obţine din g şi h o bijecţie $u : (Y \cup D) \times (Y \cup D) \to Y \cup D$. Aceasta este o contradicţie, deoarece ar rezulta că $(Y \cup D, u)$ este un element din $\mathcal{F}$ mai mare strict ca (Y, g).
Aşadar $|A - Y| < |Y|$ şi atunci $|Y| \leq |A| = |Y| + |A - Y| \leq |Y| + |Y| = |Y|$, de unde $|A| = |Y|$. În concluzie, $\alpha\alpha = |Y \times Y| = |Y| = \alpha$.
Dacă β este un cardinal cu $\beta \neq |\emptyset|$ şi $\beta \leq \alpha$, atunci $\alpha \leq \alpha\beta \leq \alpha\alpha = \alpha$, de unde rezultă că $\alpha\beta = \alpha$.

31. (a) Fie A o mulţime cu $|A| = \alpha$. Cum $|A_i| \leq \alpha$, există o aplicaţie injectivă $f_i : A_i \to A$. Definim o funcţie $f : \bigcup_{i \in I} A_i \to A \times I$ astfel: dacă $a \in \bigcup_{i \in I} A_i$, alegem $i \in I$ cu $a \in A_i$ şi definim $f(a) = (f_i(a), i)$. Să observăm că se pot obţine mai multe astfel de funcţii, depinzând de alegerile făcute, dar noi considerăm una dintre aceste funcţii. Este clar că f este injectivă şi atunci $|\bigcup_{i \in I} A_i| \leq |A \times I| = \alpha|I|$.
(b) Rezultă imediat din (a), considerând $\alpha = |\mathbb{N}|$ şi I o mulţime numărabilă.
(c) Aplicaţia $A \to \mathcal{P}_f(A)$ care duce $a \in A$ în $\{a\} \in \mathcal{P}_f(A)$ este injectivă,

deci $|A| \leq |\mathcal{P}_f(A)|$. Pe de altă parte, la fiecare submulţime finită S a lui A, $S = \{a_1, \ldots, a_n\}$, asociem elementul $(a_1, \ldots, a_n) \in A^n$. Aceasta defineşte o aplicaţie injectivă $\mathcal{P}_f(A) \to \bigcup_{n \in \mathbb{N}^*} A^n$, deci $|\mathcal{P}_f(A)| \leq |\bigcup_{n \in \mathbb{N}^*} A^n| \leq |A||\mathbb{N}^*| = |A|$, ultima inegalitate rezultând din (a). Aplicăm acum Teorema Cantor-Schröder-Bernstein (vezi problema 26) şi obţinem $|A| = |\mathcal{P}_f(A)|$.

32. (a) Fie $\alpha = |A| = |A'|$ şi $\beta = |B| = |B'|$. Considerăm bijecţiile $u : A \to A'$ şi $v : B \to B'$. Atunci aplicaţia $\Phi : \mathrm{Fun}(B, A) \to \mathrm{Fun}(B', A')$ definită prin $\Phi(f) = ufv^{-1}$ este bijectivă, după cum se poate verifica imediat, şi deci definiţia lui α^β nu depinde de reprezentanţi.
(b) Rezultă din problema 17.
(c) Pentru fiecare submulţime $B \subseteq A$ considerăm funcţia caracteristică asociată, mai precis funcţia $\chi_B : A \to \{0, 1\}$, $\chi_B(a) = 0$ dacă $a \notin B$ şi $\chi_B(a) = 1$ dacă $a \in B$. Se verifică imediat că funcţia $\Psi : \mathcal{P}(A) \to \mathrm{Fun}(A, \{0, 1\})$, $\Psi(B) = \chi_B$, este bijectivă. De aici rezultă că $|\mathcal{P}(A)| = 2^{|A|}$.

33. Notăm cu A mulţimea numerelor întregi strict negative. Evident $|A| = |\mathbb{N}|$. Atunci $|\mathbb{N}| \leq |\mathbb{Z}| = |\mathbb{N} \cup A| = |\mathbb{N}| + |A| = |\mathbb{N}| + |\mathbb{N}| = |\mathbb{N}|$, deci $|\mathbb{Z}| = |\mathbb{N}|$.
Apoi avem o funcţie surjectivă $f : \mathbb{Z} \times \mathbb{Z}^* \to \mathbb{Q}$, $f(m, n) = m/n$, şi de aici rezultă că $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}^*| = |\mathbb{Z}||\mathbb{Z}^*| = |\mathbb{Z}||\mathbb{Z}| = |\mathbb{Z}|$. Cum evident $|\mathbb{Z}| \leq |\mathbb{Q}|$, obţinem că $|\mathbb{Z}| = |\mathbb{Q}|$.
Funcţia $g : \mathbb{R} \times \mathbb{R} \to \mathbb{C}$, $g(a, b) = a + bi$, este o bijecţie, şi deci $|\mathbb{C}| = |\mathbb{R} \times \mathbb{R}| = |\mathbb{R}||\mathbb{R}| = |\mathbb{R}|$.
Funcţia $\tan : (-\frac{\pi}{2}, \frac{\pi}{2}) \to \mathbb{R}$ este bijectivă, deci $|(-\frac{\pi}{2}, \frac{\pi}{2})| = |\mathbb{R}|$. De asemenea pentru orice numere reale $a < b$ şi $c < d$, funcţia liniară $f : (a, b) \to (c, d)$, $f(x) = \frac{d-c}{b-a}x + \frac{cb-da}{b-a}$, este bijectivă, deci $|(a, b)| = |(c, d)|$. În consecinţă avem că $|(a, b)| = |\mathbb{R}|$ pentru orice $a < b$. Faptul că $|(a, b)| = |[a, b)| = |(a, b]| = |[a, b]|$ rezultă din problema 28(ii).
Rămâne de arătat că $|\mathbb{N}| < |\mathbb{R}|$. Fie $B = [0, 1)$. Atunci $|B| \leq |\mathbb{R}|$ şi $|\mathbb{N}| \leq |B|$ (pentru a doua inegalitate observăm, de exemplu, că funcţia $g : \mathbb{N} \to B$, $g(n) = \frac{1}{n+2}$, este injectivă). Arătăm că $|\mathbb{N}| \neq |B|$. Într-adevăr, dacă $|\mathbb{N}| = |B|$, am avea o bijecţie $h : \mathbb{N}^* \to [0, 1)$. Pentru fiecare $n \in \mathbb{N}^*$ considerăm scrierea zecimală a lui $h(n)$, $h(n) = 0, a_{n1}a_{n2}\ldots$, unde a_{ni} sunt cifre de la 0 la 9. Reamintim că scrierea zecimală a unui număr din $[0, 1)$ poate fi orice reprezentare de forma $0, u_1u_2\ldots$ cu $u_1, u_2, \ldots$ cifre cu proprietatea că nu există k astfel încât $u_n = 9$ pentru orice $n \geq k$. Mai mult,

această reprezentare este unică. Acum pentru fiecare $n \in \mathbb{N}^*$ alegem o cifră u_n diferită de 9 şi de a_{nn}. Fie $y = 0, u_1u_2 \ldots \in [0,1)$. Atunci $y \notin \mathrm{Im}(h)$, deoarece dacă $y = h(n)$, atunci $u_i = a_{ni}$ pentru orice i, în particular $u_n = a_{nn}$, fals. Ar rezulta că h nu este surjectivă, contradicţie. Rămâne că $|\mathbb{N}| \neq |B|$. Atunci $|\mathbb{N}| < |B| \leq |\mathbb{R}|$, deci $|\mathbb{N}| < |\mathbb{R}|$.

34. Să presupunem că ar exista o funcţie f cu proprietatea din enunţ. Fie $I_n = [n, n+1)$, $n \in \mathbb{Z}$. Atunci $|\mathrm{Im}(f) \cap I_n| \leq 1$, altfel ar exista $x, y \in \mathbb{R}$, $x \neq y$, cu $f(x), f(y) \in I_n$, deci $|f(x) - f(y)| < 1$, imposibil.
Atunci $\mathrm{Im}(f) = \mathrm{Im}(f) \cap \mathbb{R} = \mathrm{Im}(f) \cap (\bigcup_{n\in\mathbb{Z}} I_n) = \bigcup_{n\in\mathbb{Z}} (\mathrm{Im}(f) \cap I_n)$, care este o reuniune numărabilă de mulţimi de cardinal 0 sau 1, deci este cel mult numărabilă. Dar relaţia dată arată că f este injectivă, deci $\mathbb{R}$ este în bijecţie cu $\mathrm{Im}(f)$. Ar rezulta că $\mathbb{R}$ este cel mult numărabilă, contradicţie (ţinem cont de problema 33).

35. Pentru fiecare $k \in \mathbb{N}^*$ considerăm $I_k = (\frac{1}{k+1}, \frac{1}{k}]$. De asemenea fie $I_0 = (1, \infty)$. Atunci orice $x \in (0, \infty)$ aparţine exact unui interval I_k. Definim $g : \mathbb{R} \to \mathbb{N}$ prin $g(x) = k$, unde k este unicul număr natural pentru care $f(x) \in I_k$. Cum $\mathbb{R}$ este nenumărabilă şi $\mathbb{R} = g^{-1}(\mathbb{N}) = \bigcup_{k\in\mathbb{N}} g^{-1}(\{k\})$, unde $g^{-1}(\{k\}) = \{x \in \mathbb{R} \mid g(x) = k\} = \{x \in \mathbb{R} \mid \frac{1}{k+1} < f(x) \leq \frac{1}{k}\}$, rezultă că există k astfel încât $g^{-1}(\{k\})$ este infinită (chiar nenumărabilă). Alegem atunci $x_1, \ldots, x_{k+1} \in g^{-1}(\{k\})$ distincte şi obţinem că $f(x_1), \ldots, f(x_{k+1}) > \frac{1}{k+1}$, deci $f(x_1) + \cdots + f(x_{k+1}) > 1$.

36. Notăm cu A mulţimea punctelor de maxim local strict ale lui f. Pentru fiecare $a \in A$ alegem o vecinătate a lui a astfel încât $f(x) < f(a)$ pentru orice $x \in V_a$, $x \neq a$. Alegem $p_a, q_a \in V_a \cap \mathbb{Q}$ cu $p_a < a < q_a$ şi definim $g : A \to \mathbb{Q} \times \mathbb{Q}$ prin $g(a) = (p_a, q_a)$.
Arătăm că g este injectivă. Într-adevăr, dacă pentru $a, b \in A$, $a \neq b$, am avea $g(a) = g(b)$, deci $p_a = p_b = p$ şi $q_a = q_b = q$, atunci $(p, q) \subseteq V_a \cap V_b$, de unde $f(b) < f(a)$ şi $f(a) < f(b)$, contradicţie.
Din injectivitatea lui g rezultă că $|A| \leq |\mathbb{Q}\times\mathbb{Q}|$ şi cum $\mathbb{Q}\times\mathbb{Q}$ este numărabilă, rezultă că A este cel mult numărabilă.
Similar mulţimea punctelor de minim local strict ale lui f este cel mult numărabilă, de unde rezultă că mulţimea punctelor de extrem local strict ale lui f este cel mult numărabilă ca reuniune de două mulţimi cel mult

numărabile.

37. Este imediat că $\sim$ este relaţie de echivalenţă.
Să observăm că pentru $x \in \mathbb{R}$ avem $\hat{x} = \{x + q \mid q \in \mathbb{Q}\}$, deci $\hat{x}$ este mulţime numărabilă. Fie $(x_i)_{i\in I}$ un sistem de reprezentanţi pentru clasele de echivalenţă. Atunci $\mathbb{R} = \bigcup_{i\in I} \widehat{x_i}$. De aici rezultă că I nu poate fi cel mult numărabilă, altfel $\mathbb{R}$ ar fi reuniune cel mult numărabilă de mulţimi numărabile, deci numărabilă. Aşadar $|\mathbb{N}| < |\mathbb{R}/\sim|$. Pe de altă parte este clar că $|\mathbb{R}/\sim| \leq |\mathbb{R}|$. Folosind ipoteza continuului, care spune că între $|\mathbb{N}|$ şi $|\mathbb{R}|$ nu mai există alte numere cardinale, obţinem că $|\mathbb{R}/\sim| = |\mathbb{R}|$.

38. Este suficient să considerăm o bijecţie între $\mathbb{N}$ şi $\mathbb{Z}$ şi să transferăm relaţia de ordine uzuală de pe $\mathbb{N}$ (împreună cu care $\mathbb{N}$ este mulţime bine ordonată) la o relaţie de ordine pe $\mathbb{Z}$.
De exemplu, scriem elementele lui $\mathbb{Z}$ sub forma unui şir astfel: $0, 1, -1, 2, -2, \ldots$. Definim pe $\mathbb{Z}$ relaţia ρ astfel: $a\rho b$ dacă şi numai dacă a este la stânga lui b în acest şir. Atunci ρ este relaţie de ordine pe $\mathbb{Z}$ şi $(\mathbb{Z}, \rho)$ este bine ordonată.

Capitolul 8

Soluţii: Legi de compoziţie. Semigrupuri şi monoizi

1. (i) A defini o lege de compoziţie pe M este acelaşi lucru cu a da o aplicaţie $f : M \times M \to M$. Cum M are n elemente, $M \times M$ are n^2 elemente, deci acest lucru se poate face în n^{n^2} moduri.
(ii) Notăm $M = \{x_1, \ldots, x_n\}$. A da o lege de compoziţie comutativă pe M este acelaşi lucru cu a da o aplicaţie $f : M \times M \to M$ cu $f(x, y) = f(y, x)$ pentru orice $x, y \in M$. Dar aceasta este tot una cu a da o aplicaţie $g : \{(x_i, x_j) \mid 1 \leq i \leq j \leq n\} \to M$. Cum prima mulţime are $n(n+1)/2$ elemente iar a doua are n elemente, acest lucru se poate face în $n^{n(n+1)/2}$ moduri.
(iii) Dacă $e \in M$, atunci a da pe M o lege de compoziţie care are elementul neutru e este acelaşi lucru cu a da o funcţie $f : M \times M \to M$ pentru care $f(x, e) = f(e, x) = x$ pentru orice $x \in M$. Aceasta este echivalent cu a da o aplicaţie $g : \{(x, y) \mid x, y \in M - \{e\}\} \to M$, ceea ce se poate face în $n^{(n-1)^2}$ moduri. Dar oricare element al lui M poate fi ales ca element neutru şi cum elementul neutru este unic rezultă că avem $n^{(n-1)^2+1}$ legi de compoziţie cu element neutru definite pe M.

2. Fie T_n numărul de moduri în care se pot pune parantezele în produsul $x_1 x_2 \ldots x_n$ pentru $n \geq 2$. Prin convenţie notăm $T_1 = 1$. Pentru a stabili o relaţie de recurenţă pentru T_n, observăm că atunci când punem corect parantezele în produsul $x_1 x_2 \ldots x_n$ avem două posibilităţi:
• Există o singură pereche de paranteze care nu sunt conţinute în interior de alte paranteze. Atunci această pereche conţine în interior pe $x_1, \ldots, x_{n-1}$ şi

lasă în afară pe x_n sau conţine în interior pe $x_2, \ldots, x_n$ şi lasă în afară pe x_1. În fiecare din cazuri parantezele se pot pune în T_{n-1} moduri.
• Există două perechi de paranteze care nu sunt conţinute în interior de alte paranteze, prima pereche conţinând în interior pe $x_1, \ldots, x_k$ iar a doua pe $x_{k+1}, \ldots, x_n$. Pentru fiecare k parantezele se pot pune în $T_k T_{n-k}$ moduri.
Obţinem astfel relaţia de recurenţă

$$T_n = T_1 T_{n-1} + T_2 T_{n-2} + \ldots + T_{n-1} T_1 = \sum_{k=1,n-1} T_k T_{n-k}.$$

Demonstrăm acum prin inducţie că $\frac{T_{n+2}}{T_{n+1}} = \frac{4n+2}{n+2}$ pentru orice $n \geq 0$. Pentru $n = 0$ este clar. Presupunem că $\frac{T_{i+2}}{T_{i+1}} = \frac{4i+2}{i+2}$ pentru orice $0 \leq i < n$. Considerăm suma $S = T_1 T_{n+1} + 2T_2 T_n + \ldots + (n+1) T_{n+1} T_1$. Aplicând ipoteza de inducţie obţinem că $S = T_{n+1} + 2T_1 T_n + \ldots + (4n-2) T_n T_1$. Notăm $R = 2T_1 T_n + \ldots + (4n-2) T_n T_1$. Atunci avem

$$\begin{aligned}
2R &= R + R \\
&= (2T_1 T_n + 4T_2 T_{n-1} + \ldots + (4n-2) T_n T_1) \\
&\quad + (2T_n T_1 + 4T_{n-1} T_2 + \ldots + (4n-2) T_1 T_n) \\
&= (2T_1 T_n + 4T_1 T_{n-1} + \ldots + (4n-2) T_n T_1) \\
&\quad + ((4n-2) T_1 T_n + \ldots + 4T_{n-1} T_2 + 2T_n T_1) \\
&= 4n(T_1 T_n + T_2 T_{n-1} + \ldots + T_n T_1) \\
&= 4n T_{n+1}
\end{aligned}$$

ceea ce arată că $R = 2nT_{n+1}$. Rezultă că $S = T_{n+1} + R = T_{n+1} + 2nT_{n+1} = (2n+1) T_{n+1}$.
Pe de altă parte avem

$$\begin{aligned}
2S &= S + S \\
&= (T_1 T_{n+1} + 2T_2 T_n + \ldots + (n+1) T_{n+1} T_1) \\
&\quad + (T_{n+1} T_1 + 2T_n T_2 + \ldots + (n+1) T_1 T_{n+1}) \\
&= (T_1 T_{n+1} + 2T_2 T_n + \ldots + (n+1) T_{n+1} T_1) \\
&\quad + ((n+1) T_{n+1} + \ldots + 2T_n T_2 + T_{n+1} T_1) \\
&= (n+2)(T_1 T_{n+1} + T_2 T_n + \ldots + T_{n+1} T_1) \\
&= (n+2) T_{n+2}
\end{aligned}$$

deci $S = \frac{n+2}{2} T_{n+2}$.
Din cele două formule obţinute mai sus pentru S rezultă că $(2n+1) T_{n+1} =$

$\frac{n+2}{2}T_{n+2}$, adică $\frac{T_{n+2}}{T_{n+1}} = \frac{4n+2}{n+2}$, ceea ce trebuia demonstrat.
Demonstrăm acum prin inducţie că $T_{n+1} = \frac{1}{n+1}C_{2n}^n$. Pentru $n = 0$ este clar. Presupunem adevărat pentru n. Atunci

$$\begin{aligned} T_{n+2} &= \frac{4n+2}{n+2}T_{n+1} \\ &= \frac{4n+2}{n+2} \cdot \frac{1}{n+1}C_{2n}^n \\ &= \frac{2(2n+1)(2n)!}{(n+1)(n+2)n!n!} \\ &= \frac{(2n+2)!}{(n+2)(n+1)!(n+1)!} \\ &= \frac{1}{n+2}C_{2n+2}^{n+1} \end{aligned}$$

deci formula este adevărată şi pentru $n+1$.
Rescriind formula demonstrată pentru n, avem $T_n = \frac{1}{n}C_{2n-2}^{n-1}$.

3. (i) $\Rightarrow$ (ii) Dacă f este injectiv şi $u, v : X \to A$ verifică $fu = fv$, atunci pentru orice $x \in X$ avem $f(u(x)) = f(v(x))$ şi cum f este injectiv obţinem $u(x) = v(x)$. Aşadar $u = v$ şi f este monomorfism de monoizi.
(ii) $\Rightarrow$ (i) Reciproc, presupunem că f este monomorfism de monoizi. Dacă prin absurd f nu este injectiv, atunci există $a, b \in A$, $a \neq b$ cu $f(a) = f(b)$. Considerăm monoidul $(\mathbb{N}, +)$ şi morfismele de monoizi $u, v : \mathbb{N} \to A$ definite prin $u(n) = a^n$ şi $v(n) = b^n$ pentru orice $n \in \mathbb{N}$. Evident $u \neq v$, dar $fu(n) = f(u(n)) = f(a^n) = (f(a))^n = (f(b))^n = f(b^n) = f(v(n)) = fv(n)$, deci $fu = fv$, contradicţie cu faptul că f este monomorfism de monoizi. Rezultă că f este injectiv.

4. Ştim că f este surjectiv şi $uf = vf$, unde u şi v sunt morfisme de monoizi ca în enunţ. Fie $b \in B$ arbitrar ales şi $a \in A$ cu $f(a) = b$. Atunci $u(b) = u(f(a)) = u(f(b)) = v(b)$, deci $u = v$. Aşadar f este epimorfism de monoizi.

Evident, morfismul de monoizi multiplicativi $i : \mathbb{Z} \to \mathbb{Q}$ nu este surjectiv. Arătăm că i este epimorfism de monoizi. Fie $u, v : \mathbb{Q} \to Y$ două morfisme de monoizi pentru care $ui = vi$. Deci $u(n) = v(n)$ pentru orice $n \in \mathbb{Z}$. Fie $m \in \mathbb{Z} - \{0\}$. Atunci $u(m)u(1/m) = u(1/m)u(m) = u(m \cdot \frac{1}{m}) = u(1) = e$, e fiind elementul neutru al lui Y. Rezultă că $u(m)$ este simetrizabil în Y

şi are simetricul $u(1/m)$. Analog, $v(m)$ este simetrizabil şi simetricul său este $v(1/m)$. Cum $u(m) = v(m)$, rezultă că $u(1/m) = v(1/m)$. Atunci $u(n/m) = u(n)u(1/m) = v(n)v(1/m) = v(n/m)$, deci $u = v$ şi f este epimorfism de monoizi.

5. Fie S un semigrup. Dacă S este monoid, îl scufundăm pe S în el însuşi cu aplicaţia identică. Dacă S nu are element neutru, fie e un obiect care nu se găseşte în S şi fie $M = S \cup \{e\}$. Introducem pe M o structură de monoid astfel: dacă $x, y \in S$, atunci xy este produsul lor din S şi $xe = ex = x$ pentru orice $x \in M$. Este clar că M este monoid cu elementul neutru e iar aplicaţia $f : S \to M$ definită prin $f(x) = x$, pentru orice $x \in S$, este un morfism injectiv de semigrupuri.

6. Fie S un semigrup cu simplificare şi e un element idempotent al lui S. Dacă $x \in S$, avem $ex = e^2x$, deci $ex = e(ex)$ şi cum S este cu simplificare la stânga rezultă că $x = ex$. Analog $x = xe$, deci e este element neutru în S. Din unicitatea elementului neutru rezultă că există cel mult un idempotent.

7. Fie $a \in S$. Cum mulţimea $\{a^p \mid p \in \mathbb{N}^*\}$ este finită, există $p, t \in \mathbb{N}^*$ cu $a^p = a^{p+t}$. Dacă $m > p$, atunci avem $a^m = a^{m-p}a^p = a^{m-p}a^{p+t} = a^{m+t}$. De aici rezultă că $a^m = a^{m+rt}$ pentru orice $m > p$ şi $r \in \mathbb{N}^*$. Alegem r astfel încât $rt > p$ şi $m = rt$. Atunci $a^m = a^{m+rt} = a^{2m}$, deci a^m este idempotent.

8. Fie S un semigrup (cu operaţia notată multiplicativ) cu două elemente. Dacă S este grup, atunci S este izomorf cu grupul ciclic de ordin 2. Notăm cu S_1 acest semigrup.
Dacă S este monoid care nu este grup, fie $S = \{e, a\}$, unde e este elementul neutru. Atunci $a^2 = a$ (altfel, dacă $a^2 = e$ rezultă că S este grup), şi deci avem un singur tip de izomorfism de monoid cu două elemente care nu este grup. Notăm acest tip cu S_2.
Presupunem acum că $S = \{a, b\}$ este semigrup care nu este monoid. Numim element zero un element $x \in S$ cu proprietatea că $xy = yx = x$ pentru orice $y \in S$. Evident, dacă există, un element zero este unic. Distingem două situaţii:
• S are un element zero, fie acesta a. Atunci $a^2 = ab = ba = a$. Atunci avem sau $b^2 = b$, ceea ce ar implica faptul că S este monoid (cu elementul neutru b), deci acest caz este exclus, sau $b^2 = a$. Obţinem semigrupul $S_3 = \{a, b\}$ cu operaţia definită de $a^2 = ab = ba = a, b^2 = a$ (este imediat de verificat

asociativitatea şi că S_3 nu este monoid).
• S nu are un element zero. Ştim din problema 7 că S are cel puţin un idempotent. Presupunem de exemplu că a este idempotent. Dacă $ab = a$, atunci trebuie să avem $ba = b$ (altfel a este un element zero), şi în continuare $b^2 = baba = ba^2 = ba = b$. Obţinem semigrupul $S_4 = \{a, b\}$ cu operaţia dată de $a^2 = a, ab = a, ba = b, b^2 = b$ (se verifică imediat asociativitatea). Dacă $ab = b$, atunci $ba = a$ (altfel a ar fi element neutru, deci S ar fi monoid) şi în continuare $b^2 = abab = a^2b = ab = b$. Obţinem semigrupul $S_5 = \{a, b\}$ cu operaţia dată de $a^2 = a, ab = b, ba = a, b^2 = b$ (din nou se verifică imediat asociativitatea). Este clar că semigrupurile S_4 şi S_5 nu sunt izomorfe deoarece în S_4 are loc $xy = x$ pentru orice $x, y \in S_4$, în timp ce în S_5 are loc $xy = y$ pentru orice $x, y \in S_5$.
Prin urmare există exact 5 tipuri de izomorfism de semigrupuri cu două elemente: un grup, un monoid care nu este grup şi 3 semigrupuri care nu sunt monoizi.

9. Fie $a \in G$. Atunci subsemigrupul generat de a este $\{a^n \mid n \in \mathbb{N}^*\}$. Conform ipotezei, acest subsemigrup este o mulţime finită, deci există $i, j \in \mathbb{N}^*$, $i \neq j$, cu $a^i = a^j$. Cum G este grup, rezultă că $a^{j-i} = e$, unde e este elementul identitate din G. Deci orice element al lui G are ordin finit. Fie acum S un subsemigrup al lui G şi fie $a \in S$. Cum a are ordin finit şi $a^n \in S$ pentru orice $n \in \mathbb{N}^*$, rezultă că $e \in S$. De asemenea, $a^{-1} = a^{m-1} \in S$, unde $m = \text{ord}(a)$, deci S este subgrup.

10. (i) Arătăm că H_e este parte stabilă în raport cu operaţia din S. Fie $a, b \in H_e$. Avem $ea = ae = a$, $eb = be = b$ şi există $x, y, x', y' \in S$ cu $xa = ay = e$ şi $x'b = by' = e$. Atunci $e(ab) = (ea)b = ab$ şi $(ab)e = a(be) = ab$. De asemenea, $x'xab = x'eb = x'b = e$ şi $aby'y = aey = ay = e$. Rezultă că $ab \in H_e$. Evident $e \in H_e$, deoarece $ee = e$, şi în plus, e este element neutru în H_e. Rămâne să arătăm că orice element din H_e este simetrizabil. Fie $a \in H_e$ şi $x, y \in S$ cu $xa = ay = e$. Atunci $(xe)a = xa = e$ şi $a(ey) = ay = e$. Apoi $xe = xay = ey$. Arătăm că $xe \in H_e$. Mai întâi observăm că $(xe)e = xe$ şi $e(xe) = e(ey) = ey = xe$. Apoi $a(xe) = aey = ay = e$ şi $(xe)a = xa = e$. Rezultă că $xe \in H_e$ şi acesta este inversul lui a.
(ii) Fie $H \subset S$ astfel încât $e \in H$ şi H este grup cu operaţia indusă. Cum $e^2 = e$, rezultă că e este elementul neutru din grupul H. Fie $a \in H$. Rezultă că $ae = ea = a$. Apoi există $a' \in H$ cu $a'a = aa' = e$. Deci $a \in H_e$, de unde rezultă că $H \subseteq H_e$.

11. (i) Dacă semigrupul S conţine un idempotent e, atunci mulţimea $\{e\}$ este un subgrup al lui S. Reciproc, dacă S are un subgrup G, atunci elementul neutru e al lui G verifică relaţia $e^2 = e$.
(ii) Este suficient să dăm un exemplu de semigrup care nu are elemente idempotente. Un astfel de exemplu este $(\mathbb{N}^*, +)$.

12. (i) Dacă $a = ese$ şi $b = ete$ sunt elemente din eSe, atunci $ab = eseete = esete = e(set)e \in eSe$. Rezultă că eSe este subsemigrup. Evident $e(ese) = (ese)e = ese$, deci e este element neutru în eSe.
(ii) Se ştie că mulţimea elementelor inversabile ale unui monoid este grup în raport cu operaţia indusă. Rezultă că H_e este grup.
Fie acum un grup G inclus în S şi $a \in G \cap H_e$. Fie f elementul neutru din G şi b, c inversele lui a în G şi respectiv H_e. Atunci $e = ca = caf = ef = eab = ab = f$. Rezultă că e este elementul neutru din G. Dar $G = eGe \subseteq eSe$ şi cum elementele lui G sunt inversabile, rezultă că $G \subseteq H_e$.

13. (i) Fie G un subgrup al lui S şi fie e elementul neutru al lui G. Conform problemei 12 avem că $G \subseteq H_e$, deoarece $e \in G \cap H_e$. Mai mult, H_e este subgrup maximal al lui S. Într-adevăr, conform problemei 12, dacă H este un subgrup astfel încât $H_e \subseteq H$, rezultă că $H \cap H_e \neq \emptyset$ şi deci $H \subseteq H_e$, de unde se obţine că $H = H_e$.
(ii) Fie G şi G' două subgrupuri maximale ale lui S. Notăm cu e şi respectiv e' elementele neutre ale acestora. Obţinem ca la punctul (i) că $G = H_e$ şi $G' = H_{e'}$. Dacă G şi G' nu sunt disjuncte, aplicăm din nou problema 12(ii) şi obţinem că $G = H_e \subseteq H_{e'} = G'$ şi analog $G' \subseteq G$. Rezultă că $G = G'$.

14. Deoarece S are subgrupuri, rezultă din problema 11 că S are elemente idempotente. Fie I mulţimea acestora. Arătăm că $S = \bigcup_{e \in I} H_e$, unde notaţiile sunt cele din problema 12. Într-adevăr, fie $a \in S$. Cum S este o reuniune de grupuri, există G un subgrup al lui S cu proprietatea că $a \in G$. Fie e elementul neutru al lui G. Atunci $G \subseteq H_e$ (din problema 12), deci $a \in H_e$. Mai mult, dacă $e, e' \in I$, $e \neq e'$, atunci H_e şi $H_{e'}$ sunt egale sau disjuncte. Ele nu pot fi egale deoarece elementele neutre sunt diferite, deci sunt disjuncte. Am scris aşadar pe S ca o reuniune disjunctă de subgrupuri.

15. Fie $S = \{e_0, e_1, \ldots, e_n\}$ o mulţime cu $n + 1$ elemente pe care definim

o lege de compoziţie astfel: $e_ie_i = e_i$ pentru orice i şi $e_ie_j = e_0$ pentru orice $i \neq j$. Atunci S este semigrup care nu este grup şi S este reuniunea subgrupurilor $\{e_i\}$ cu $i \in \{0, \ldots, n\}$.

16. Presupunem că există un morfism injectiv de semigrupuri $f : S \to G$, unde G este grup. Dacă $a, x, y \in S$ şi $ax = ay$, atunci $f(ax) = f(ay)$, deci $f(a)f(x) = f(a)f(y)$ şi cum G este grup obţinem că $f(x) = f(y)$. Dar f este injectiv, de unde rezultă că $x = y$. Prin urmare S este semigrup cu simplificare.
Reciproc, presupunem că semigrupul comutativ S este semigrup cu simplificare. Pe mulţimea $S \times S$ considerăm relaţia $\sim$ definită astfel:

$$(a, b) \sim (c, d) \text{ dacă şi numai dacă } ad = bc.$$

Arătăm că $\sim$ este relaţie de echivalenţă pe $S \times S$:
• reflexivitatea: $(a, b) \sim (a, b) \Leftrightarrow ab = ba$, adevărat.
• simetria: dacă $(a, b) \sim (c, d)$, atunci $ad = bc$, deci şi $cb = da$, adică $(c, d) \sim (a, b)$.
• tranzitivitatea: $(a, b) \sim (c, d)$ şi $(c, d) \sim (e, f)$ este echivalent cu $ad = bc$ şi $cf = de$. Atunci $adf = bcf = deb$ şi cum putem simplifica cu d rezultă $af = eb$, adică $(a, b) \sim (e, f)$.

Notăm cu G mulţimea factor $S \times S/\sim$ şi cu s/t clasa lui $(s, t) \in S \times S$ în raport cu $\sim$. Pe G definim o lege de compoziţie astfel:

$$(a/b)(c/d) = (ac)/(bd).$$

Arătăm că definiţia de mai sus nu depinde de reprezentanţi. Într-adevăr, dacă $a/b = a'/b'$ şi $c/d = c'/d'$, adică $ab' = ba'$ şi $cd' = dc'$, atunci $ab'cd' = ba'dc' \Leftrightarrow (ac)(b'd') = (bd)(a'c')$, deci $(ac, bd) \sim (a'c', b'd')$, ceea ce înseamnă că $(ac)/(bd) = (a'c')/(b'd')$.
Este evident că această operaţie definită pe G este asociativă. De asemenea, elementul s/s, $s \in S$, este element neutru în G, deoarece $(a/b)(s/s) = as/bs = a/b$ (aceasta este adevărat pentru că $asb = bsa$) şi în mod analog $(s/s)(a/b) = a/b$. Dacă $a/b \in G$, atunci $(a/b)(b/a) = ab/ab = s/s$ (deoarece $abs = abs$) şi analog $(b/a)(a/b) = s/s$. Rezultă că orice element al lui G este inversabil, deci G este grup.

Aplicaţia $f : S \to G$ dată prin $f(a) = (as)/s$ este morfism de semigrupuri, deoarece $f(a)f(b) = (as/s)(bs/s) = (abss)/(ss) = (abs)/s = f(ab)$. Mai mult, f este injectivă deoarece $f(a) = f(b) \Rightarrow as/s = bs/s \Rightarrow ass = bss$

şi cum S este semigrup cu simplificare rezultă $a = b$. Deci S se poate scufunda în G.

17. Un calcul simplu arată că $((i,j)(k,l))(p,r) = (i,j)((k,l)(p,r)) = (i+k+p, 2^{k+p}j + 2^p l + r)$. De aici rezultă că legea de compoziţie este asociativă.

18. (i) Dacă $f, g : X \to X$ sunt funcţii injective, atunci fg este injectivă, deci $I(X)$ este parte stabilă în raport cu compunerea. Ştim că această operaţie este asociativă şi are elementul neutru $1_X \in I(X)$.
(ii) Fie S un semigrup. Dacă S se poate scufunda într-un monoid de forma $I(X)$, fie atunci $f : S \to I(X)$ un morfism injectiv de semigrupuri. Dacă $a, b, c \in S$ şi $ab = ac$, atunci $f(ab) = f(ac)$, deci $f(a)f(b) = f(a)f(c)$ şi cum $f(a)$ este injectivă rezultă că $f(b) = f(c)$, deci $b = c$. Reciproc, dacă S are simplificare la stânga, fie $f : S \to I(S)$ definită prin $f(s)(a) = sa$. Evident f este injectivă şi f este morfism de semigrupuri.

19. (i) Pentru un element $a \in M$ definim funcţia $f_a : M \to M$, $f_a(x) = ax$ pentru orice $x \in M$. Să observăm că $f_a \circ f_b = f_{ab}$ şi $f_e = \mathrm{Id}_M$, unde e este elementul identitate al lui M. Definim acum funcţia $f : M \to \mathrm{Fun}(M, M)$, $f(a) = f_a$ pentru orice $a \in M$. Avem că f este morfism de monoizi. Întradevăr, $f(ab) = f_{ab} = f_a \circ f_b = f(a) \circ f(b)$ pentru orice $a, b \in M$ şi $f(e) = f_e = \mathrm{Id}_M$. Mai mult, f este morfism injectiv, deoarece $f(a) = f(b) \Rightarrow f_a = f_b \Rightarrow f_a(e) = f_b(e) \Rightarrow ae = be \Rightarrow a = b$.
(ii) Dacă $ab \in U(M)$, atunci există $c \in M$ astfel încât $(ab)c = c(ab) = e$. Din $c(ab) = e$ deducem că $(ca)b = e$, deci b este inversabil la stânga în M. Conform punctului (i), f_b va fi un element inversabil la stânga în monoidul $(\mathrm{Fun}(M, M), \circ)$, în particular f_b va fi funcţie injectivă. Cum M este mulţime finită, rezultă că f_b va fi funcţie bijectivă. Aşadar, există $g \in \mathrm{Fun}(M, M)$ astfel încât $g \circ f_b = f_b \circ g = \mathrm{Id}_M$. De aici obţinem că $f_b(g(x)) = x$ pentru orice $x \in M$. În particular, pentru $x = e$ se obţine $bg(e) = e$, deci b este inversabil la dreapta în M. În concluzie, $b \in U(M)$, contradicţie.
Considerăm acum monoidul $(\mathrm{Fun}(\mathbb{N}, \mathbb{N}), \circ)$ şi elementele $a, b \in \mathrm{Fun}(\mathbb{N}, \mathbb{N})$ definite astfel: $a(n) = n/2$ dacă n este par şi $a(n) = 0$ dacă n este impar, respectiv $b(n) = 2n$ pentru orice $n \in \mathbb{N}$. Este evident că a, b nu sunt inversabile, dar $a \circ b = \mathrm{Id}_{\mathbb{N}}$ este element inversabil.

20. Fie $F(\mathbb{N}) = \{f \mid f : \mathbb{N} \to \mathbb{N}$ funcţie$\}$. Atunci $(F(\mathbb{N}), *)$ este

monoid, unde operaţia $*$ este definită prin $u * v = v \circ u$. Elementul neutru al acestui monoid este $1_{\mathbb{N}}$. Fixăm $k \in \mathbb{N}$. Fie $f \in F(\mathbb{N})$ definită prin $f(0) = f(1) = \ldots = f(k) = 0$ şi $f(k+i) = i$ pentru orice $i \in \mathbb{N}$, unde k este un număr natural nenul. Dacă $g \in F(\mathbb{N})$, atunci g este un invers la stânga pentru f dacă şi numai dacă $g * f = 1_{\mathbb{N}}$, adică $f \circ g = 1_{\mathbb{N}}$. Aceasta este echivalent cu $g(i) = k + i$ pentru orice $i \in \mathbb{N}^*$ şi $g(0) \in \{0, 1, \ldots, k\}$. Dar există exact $k+1$ astfel de funcţii g, deci f are $k+1$ inverşi la stânga.

21. (i) Fie G un grup cu n elemente, de exemplu $(\mathbb{Z}_n, +)$, şi H un monoid care are ca element inversabil doar elementul neutru, de exemplu $(\mathbb{N}, +)$. În produsul direct de monoizi $G \times H$ un element (g, h) este inversabil dacă şi numai dacă g şi h sunt inversabile în G, respectiv H. Rezultă că $G \times H$ are exact n elemente inversabile. (Precizăm că operaţia pe $G \times H$ este definită astfel: $(g, h)(g', h') = (gg', hh')$, pentru orice $g, g' \in G$, $h, h' \in H$).
(ii) Fie G un grup cu n elemente şi H un monoid cu două elemente, dintre care doar elementul neutru este inversabil (de exemplu $(\mathbb{Z}_2, \cdot)$). Atunci în produsul direct de monoizi $G \times H$ avem exact n elemente inversabile: toate perechile în care pe poziţia a doua se găseşte elementul neutru din H.

22. Începem prin a observa că dacă în semigrupul finit M considerăm un element x, iar (k_n) este un şir strict crescător de numere naturale, atunci putem alege un subşir (k_{n_i}) al său astfel încât elementele $x^{k_{n_i}}$, $i \geq 1$, să ia toate aceeaşi valoare. Aceasta este evident, deoarece elementele şirului x^{k_n} pot lua doar un număr finit de valori. Fie $M = \{x_1, \ldots, x_r\}$. Aplicăm observaţia de mai sus elementului x_1 şi şirului tuturor numerelor naturale. Obţinem un şir $(n_i)_{i \geq 1}$ de numere naturale pentru care toate puterile $x_1^{n_i}$ sunt egale. Aplicăm acum observaţia de mai sus elementului x_2 şi şirului $(n_i)_{i \geq 1}$. Renotând, obţinem un şir $(n_i)_{i \geq 1}$ pentru care toţi $x_1^{n_i}$ iau aceeaşi valoare şi toţi $x_2^{n_i}$ sunt egali. Continuând procedeul obţinem după r paşi şirul căutat.

23. Fie A mulţimea cu un singur element a. Din construcţia monoidului M liber generat de mulţimea A, acesta este format din mulţimea tuturor cuvintelor formate din alfabetul A, adică mulţimea cuvintelor de forma $aa \ldots a$ cu n apariţii ale lui a, unde $n \in \mathbb{N}^*$ şi din cuvântul vid λ. Multiplicarea este dată de alăturarea cuvintelor, elementul neutru fiind λ. Atunci aplicaţia $f : \mathbb{N} \to M$ definită astfel: $f(0) = \lambda$ şi $f(n) = aa \ldots a$ (cuvântul format cu n litere de a) este un izomorfism de monoizi.

24. Vom demonstra mai întâi următoarea

Lemă. Fie $n \geq 2$ un număr natural şi $a_1, \ldots, a_n \in \mathbb{N}^*$ cu proprietatea că $(a_1, \ldots, a_n) = 1$. Atunci există $n_0 \in \mathbb{N}^*$ cu proprietatea că pentru orice $x \in \mathbb{N}$, $x \geq n_0$, există $k_1, \ldots, k_n \in \mathbb{N}$ astfel încât $x = k_1a_1 + \ldots + k_na_n$.

Demonstraţie. Inducţie după n. Dacă $n = 2$, alegem $n_0 = a_1a_2$ şi considerăm şirul de numere $0 \cdot a_2, 1 \cdot a_2, \ldots, (a_1 - 1) \cdot a_2$. Să observăm că termenii şirului dau resturi distincte la împărţirea cu a_1 şi fiind în număr de a_1 vor apărea toate resturile posibile. Dacă $x \geq n_0$, scriem $x = qa_1 + r$ cu $0 \leq r < a_1$. Din cele de mai sus rezultă că există $l \in \{0, \ldots, a_1 - 1\}$ astfel încât $la_2 = q'a_1 + r$. Deci $x - la_2 = (q - q')a_1$. Dacă $q - q' < 0$, atunci $x < la_2$ şi rezultă $a_1a_2 < la_2$, adică $a_1 < l$, fals. Rezultă că $q - q' \geq 0$ şi $r = la_2 + (q - q')a_1$.

Dacă $n > 2$, notăm $b = (a_1, \ldots, a_{n-1})$ şi $c = a_n$. Atunci $(b, c) = 1$ şi din cele de mai sus rezultă că există $n_1 \in \mathbb{N}$ cu proprietatea că pentru orice $x \in \mathbb{N}$, $x \geq n_1$, există $k, l \in \mathbb{N}$ astfel încît $x = kb + lc$. Dar $(a_1/b, \ldots, a_{n-1}/b) = 1$ şi din ipoteza de inducţie rezultă că există $n_2 \in \mathbb{N}$ cu proprietatea că pentru orice $y \in \mathbb{N}$, $y \geq n_2$, există $l_1, \ldots, l_{n-1} \in \mathbb{N}$ astfel încît $y = l_1a_1/b + \ldots + l_{n-1}a_{n-1}/b \Rightarrow by = l_1a_1 + \ldots + l_{n-1}a_{n-1}$ pentru $y \geq n_2$. Considerăm $n_0 = n_2b(1 + c) + n_1$ şi arătăm că pentru orice $x \geq n_0$ există $k_1, \ldots, k_n \in \mathbb{N}$ astfel ca $x = k_1a_1 + \ldots + k_na_n$.

Cum $n_0 > n_1$, există $k, l \in \mathbb{N}$ astfel ca $x = kb + lc$. Putem presupune că $k \geq n_2$, altfel $k < n_2 \Rightarrow n_2b(1 + c) < x = kb + lc < n_2b + lc \Rightarrow n_2bc < lc \Rightarrow n_2b < l \Rightarrow x = (k + n_2c)b + (l - n_2b)c$, scriere în care coeficienţii lui b şi c sunt numere naturale iar coeficientul lui b este mai mare sau egal decât n_2. Deci $bk = l_1a_1 + \ldots + l_{n-1}a_{n-1}$, unde $l_1, \ldots, l_{n-1} \in \mathbb{N}$. În concluzie, $x = kb + lc = l_1a_1 + \ldots + l_{n-1}a_{n-1} + lc$ şi nu avem decât să alegem $k_1 = l_1, \ldots, k_{n-1} = l_{n-1}, k_n = l$ pentru a obţine scrierea dorită.

Să trecem acum la rezolvarea problemei. Fie d cel mai mare divizor comun al elementelor mulţimii $M - \{0\}$. Atunci $(1/d)M \subseteq \mathbb{N}$ este submonoid, deci putem presupune de la început că $d = 1$. Scriem $M - \{0\} = \{a_1, \ldots, a_n, \ldots\}$ şi notăm $q_n = (a_1, \ldots, a_n) \Rightarrow \ldots |q_n|q_{n-1}| \ldots |q_2|q_1 \Rightarrow \ldots \leq q_n \leq q_{n-1} \leq \ldots \leq q_2 \leq q_1$, deci există $t \in \mathbb{N}$ astfel încât $q_n = q_{n+1}$ pentru orice $n \geq t$. Notăm $q = q_n$ şi cum $q|a_n$ pentru orice $n \in \mathbb{N}^*$, avem că $q = 1$. Deci $(a_1, \ldots, a_n) = 1$, unde $n \geq t$ este fixat $\Rightarrow$ există $n_0 \in \mathbb{N}^*$ (conform lemei) cu proprietatea că pentru orice $x \in \mathbb{N}$, $x \geq n_0$, există $k_1, \ldots, k_n \in \mathbb{N}$ astfel încât $x = k_1a_1 + \ldots + k_na_n \Rightarrow \{x \in \mathbb{N} \mid x \geq n_0\} \subseteq M$, deci $M = A \cup \{x \in \mathbb{N} \mid x \geq n_0\}$, unde $A = \{x \in M \mid x < n_0\}$ este în mod evident o mulţime finită.

Observaţie. Din demonstraţie rezultă că elementele mulţimii A sunt şi ele multipli de d.

25. (i) Definim $f : \mathbb{N}^* \to M_2$ astfel: dacă $n = 2^k m$, $k \in \mathbb{N}$ şi m impar, atunci $f(2^k m) = m$. Este uşor de văzut că f este izomorfism de monoizi.
(ii) Este imediat că M_3 şi M_5 sunt monoizi în raport cu operaţia de înmulţire. Să presupunem că ar exista un izomorfism $f : \mathbb{N}^* \to M_3$. Fie $p \in \mathbb{N}^*$ un număr prim de forma $3k-1$. Atunci $p^2 \in M_3$ şi deci există $x \in \mathbb{N}^*$ astfel încât $f(x) = p^2$. Avem că x este număr prim, altfel x ar fi reductibil, deci ar exista $y, z \in \mathbb{N}^* - \{1\}$ astfel încât $x = yz$. De aici rezultă $f(x) = f(yz) = f(y)f(z)$, adică $f(y) = f(z) = p$ (deoarece $f(a) = 1 \Rightarrow a = 1$). În consecinţă, $p \in M_3$, contradicţie.
Fie acum $q \in \mathbb{N}^*$ încă un număr prim de forma $3k-1$, $q \neq p$. Rezultă că există $y, z \in \mathbb{N}^*$ numere prime astfel încât $f(y) = q^2$ şi $f(z) = pq$. Obţinem $f(x)f(y) = f(z)^2$ şi ţinând seama că f este izomorfism de monoizi rezultă că $xy = z^2$. Ţinând cont că x, y, z sunt numere prime, deducem că $x = y = z$, contradicţie. Deci monoizii $\mathbb{N}^*$ şi M_3 nu sunt izomorfi.

Analog se poate arăta că monoizii $\mathbb{N}^*$ şi M_5 nu sunt izomorfi, considerând numere prime de forma $5k-1$.

Presupunem acum că există un izomorfism $f : M_3 \to M_5$. Să arătăm mai întâi că dacă $x \in M_3$ şi x este ireductibil în M_3, atunci x este număr prim sau $x = p_1 p_2$ cu p_1, p_2 numere prime de forma $3k-1$. Presupunem că x nu este număr prim, deci există $a, b \in \mathbb{N}$, $a, b > 1$ astfel încât $x = ab$. Rezultă că a, b sunt de forma $3k-1$ (altfel ar trebui să fie de forma $3k+1$, ceea ce ar însemna că x este reductibil în M_3). Dacă a nu este număr prim, atunci $a = uv$ cu $u, v \in \mathbb{N}$, $u, v > 1$. Atunci u este de forma $3k+1$ şi v este de forma $3k-1$ (sau invers), deci $x = u(vb)$ cu $u, vb \in M_3 \Rightarrow x$ reductibil in M_3, contradicţie. Deci a şi b sunt numere prime.

Fie acum $q_1, q_2, q_3, q_4 \in \mathbb{N}$ numere prime distincte de forma $5k+2$. Atunci $(q_1q_2)^2$, $(q_1q_3)^2$, $(q_2q_4)^2$, $(q_3q_4)^2$, $q_1q_2q_3q_4 \in M_5$ şi există $x, y_1, y_2, z_1, z_2 \in M_3$ distincte şi ireductibile astfel încît $f(x) = q_1q_2q_3q_4$, $f(y_1) = (q_1q_2)^2$, $f(y_2) = (q_3q_4)^2$, $f(z_1) = (q_1q_3)^2$, $f(z_2) = (q_2q_4)^2$. De aici obţinem că $f(x)^2 = f(y_1)f(y_2) = f(z_1)f(z_2) \Rightarrow f(x^2) = f(y_1y_2) = f(z_1z_2) \Rightarrow x^2 = y_1y_2 = z_1z_2$, deci în monoidul M_3 elementul x^2 are trei descompuneri distincte în factori ireductibili, ceea ce este uşor de verificat că nu este posibil (ţinând cont de descrierea elementelor ireductibile din M_3).

26. Definim monoizii $T_m = \{k \in \mathbb{N}^* \mid (k, m) = 1\}$ şi $T_n = \{l \in \mathbb{N}^* \mid (l, n) = 1\}$. Vom arăta că fiecare dintre izomorfismele din enunţ furnizează un izomorfism de monoizi între T_m şi T_n.

Fie $f : M_m \to M_n$ izomorfism de monoizi. Să observăm mai întâi că dacă $r, s \in M_m$ astfel încât $(r, s) = 1$, atunci $(f(r), f(s)) = 1$. Dacă $(f(r), f(s)) = c > 1$, atunci $c \in T_n$ şi $\overline{c} \in U(\mathbb{Z}_n)$ (unde prin $\overline{c}$ s-a notat clasa lui c modulo n). Cum $c^{\phi(n)} \equiv 1 \pmod{n}$, rezultă că $c^{\varphi(n)} \in M_n$. Dar $(f(r)^{\varphi(n)}, f(s)^{\varphi(n)}) = c^{\varphi(n)}$ şi deoarece f este surjectivă există $u, v, w \in M_m$ astfel încât $f(u) = c^{\varphi(n)}$, $f(v) = d$ şi $f(w) = e$, unde $f(r^{\varphi(n)}) = dc^{\varphi(n)}$ şi $f(s^{\varphi(n)}) = ec^{\varphi(n)}$. Să observăm că $d, e \in M_n$. Deci $r^{\varphi(n)} = uv$ şi $s^{\varphi(n)} = uw$. De aici obţinem $1 = (r^{\varphi(n)}, s^{\varphi(n)}) \geq u$, adică $u = 1$. În consecinţă, $c^{\varphi(n)} = 1$, de unde $c = 1$, contradicţie.
Definim $g : T_m \to T_n$ astfel: $g(x) = (f(ax), f(bx))$, unde $a, b \in T_m$, $(a, b) = 1$ şi $ax, bx \in M_m$ ($x \in T_m \Rightarrow (x, m) = 1 \Rightarrow \hat{x} \in U(\mathbb{Z}_m)$, unde prin $\hat{x}$ am notat clasa lui x modulo $m \Rightarrow$ există $a \in T_m$ astfel încât $\hat{a}\hat{x} = \hat{1} \Rightarrow ax \in M_m$; pe b îl putem alege egal cu $a + m$). Să observăm că

$$\begin{aligned} g(x)^{\varphi(m)} &= (f(ax)^{\varphi(m)}, f(bx)^{\varphi(m)}) \\ &= (f(a^{\varphi(m)}), f(b^{\varphi(n)}))f(x^{\varphi(m)}) \\ &= f(x^{\varphi(m)}). \end{aligned}$$

Ultima egalitate rezultă din observaţia facută în paragraful anterior, care ne garantează că dacă $(a^{\varphi(m)}, b^{\varphi(m)}) = 1$, atunci $(f(a^{\varphi(m)}), f(b^{\varphi(n)})) = 1$. De aici rezultă imediat faptul că g este bine definită, multiplicativă (adică $g(xy) = g(x)g(y)$ pentru orice $x, y \in T_m$) şi injectivă. Arătăm acum că g este surjectivă: fie $y \in T_n$. Există $u, v \in T_n$, $(u, v) = 1$ astfel încât $uy, vy \in M_n$, deci există $x, x' \in M_m$ astfel încât $f(x) = uy$ şi $f(x') = vy$. Rezultă acum că $g((x, x')) = (f(x), f(x')) = (uy, vy) = y$. Deci g este un izomorfism de monoizi.
Să mai observăm că dacă $x, y \in T_m$ cu $x \equiv y \pmod{m}$, atunci $g(x) \equiv g(y) \pmod{n}$, deoarece $x \in T_m \Rightarrow$ există $c \in T_m$ astfel încât $cx \in M_m \Rightarrow cy \in M_m \Rightarrow f(cx) \equiv f(cy) \pmod{n} \Rightarrow n | f(cx) - f(cy) = g(cx) - g(cy)$ (deoarece $g(z) = f(z)$ pentru orice $z \in M_m$) $\Rightarrow n | g(c)[g(x) - g(y)] \Rightarrow n | g(x) - g(y)$, deoarece $(n, g(c)) = 1$.
Definim acum $h : U(\mathbb{Z}_m) \to U(\mathbb{Z}_n)$ prin $h(\hat{x}) = \overline{g(x)}$. Din cele de mai înainte rezultă că h este bine definită, este morfism de grupuri şi este surjectivă. Să arătăm că h este şi injectivă: $h(\hat{x}) = \overline{1} \Rightarrow \overline{g(x)} = \overline{1} \Rightarrow g(x) \in M_n \Rightarrow$ există $u \in M_m$ astfel încât $f(u) = g(x) \Rightarrow f(u)^{\varphi(m)} = g(x)^{\varphi(m)} \Rightarrow f(u^{\varphi(m)}) = f(x^{\varphi(m)}) \Rightarrow u = x \Rightarrow x \in M_m \Rightarrow \hat{x} = \hat{1}$. Deci h este izomorfism.

Fie $f : U(\mathbb{Z}_m) \to U(\mathbb{Z}_n)$ izomorfism de grupuri şi $r = \varphi(m) = \varphi(n)$. Dacă $U(\mathbb{Z}_m) = \{\hat{a}_1, \ldots, \hat{a}_r\}$, considerăm $\overline{b}_i = f(\hat{a}_i)$, $1 \leq i \leq r$, şi obţinem că

$U(\mathbb{Z}_n) = \{\overline{b}_1, \ldots, \overline{b}_r\}$. Fie

$$A_{m,a_i} = \{p \mid p \text{ număr prim pozitiv cu } p \equiv a_i \pmod{m}\}$$

şi

$$B_{n,b_i} = \{p \mid p \text{ număr prim pozitiv cu } p \equiv b_i \pmod{n}\}$$

pentru $1 \leq i \leq r$. Din teorema lui Dirichlet (o progresie aritmetică de numere naturale în care primul termen şi raţia sunt numere prime între ele, conţine o infinitate de numere prime) rezultă că mulţimile A_{m,a_i}, B_{n,b_i} sunt numărabile, deci elementele lor se pot scrie sub forma unui şir crescător.
Se observă că dacă $x \in T_m$, $x = p_1^{r_1} \cdots p_t^{r_t}$ cu $p_1, \ldots, p_t$ numere prime distincte, atunci $p_i \in A_{m,a_1} \cup \cdots \cup A_{m,a_r}$, pentru orice $1 \leq i \leq t$. Fie $g : T_m \to T_n$ definită astfel: $g(p) = q$, unde $p \in A_{m,a_i}$ şi este al s-lea element în ordine crescătoare al acesteia, iar $q \in B_{m,b_i}$ şi este al s-lea element în ordine crescătoare al acesteia, iar apoi considerăm că g este multiplicativă. Astfel am definit un izomorfism între monoizii T_m şi T_n.
Definim acum $h : M_m \to M_n$ prin $h(x) = g(x)$ $(x \in M_m \Rightarrow g(x) \in M_n)$. Acesta este izomorfismul căutat.

27. Considerăm mai întâi monoizii $M_p = \{pk + 1 \mid k \in \mathbb{N}\}$, cu $p \geq 3$ număr prim. Aceştia nu sunt izomorfi cu monoidul $\mathbb{N}^*$, fapt care se poate arăta la fel ca la problema precedentă, şi nu sunt izomorfi între ei.

Fie monoizii $T_p = \{k \in \mathbb{N}^* \mid (k, p) = 1\}$, cu $p \geq 3$ număr prim. Vom arăta că aceştia sunt izomorfi cu $\mathbb{N}^*$. Dacă $p_1, \ldots, p_n, \ldots$ este şirul numerelor naturale prime, atunci există $t \in \mathbb{N}^*$ astfel încât $p = p_t$. Definim $f : T_p \to \mathbb{N}^*$ astfel:

$$f(p_1^{k_1} \ldots p_{t-1}^{k_{t-1}} p_{t+1}^{k_{t+1}} \ldots p_r^{k_r}) = p_1^{k_1} \ldots p_{t-1}^{k_{t-1}} p_t^{k_{t+1}} \ldots p_{r-1}^{k_r}.$$

Este imediat că f este izomorfism de monoizi.

Capitolul 9

Soluţii: Grupuri

1. Fie $a \in S$, $a' \in S$ cu $a'a = e$ şi $a'' \in S$ astfel încât $a''a' = e$. Atunci $a = ea = a''a'a = a''e$ şi $ae = a''ee = a''e = a$, de unde rezultă că e este element neutru. În plus, $a = a''e = a''$, deci $aa' = e$ şi $aa' = a''a' = e$, deci a este inversabil. Prin urmare, S este grup.

Dacă înlocuim (ii) cu (ii)' nu mai rezultă că S este grup, după cum arată următorul exemplu: pe mulţimea $\mathbb{R}^*$ definim legea de compoziţie " $\star$ " prin $x \star y = |x|y$ pentru orice $x, y \in \mathbb{R}$. Evident $(\mathbb{R}^*, \star)$ este semigrup, $e = 1$ verifică (i), iar pentru $a \in \mathbb{R}$ elementul $a' = 1/|a|$ verifică $a \star a' = 1$. Totuşi $\mathbb{R}^*$ cu operaţia algebrică astfel definită nu este grup, deoarece e nu este element neutru şi la dreapta.

2. (ii) $\Rightarrow$ (i) Evident ecuaţiile $ax = b$ şi $ya = b$ au soluţiile $x = a^{-1}b$, respectiv $y = ba^{-1}$.
(i) $\Rightarrow$ (ii) Fie $a \in S$ şi $e \in S$ cu $ae = a$. Arătăm că e este element neutru la dreapta pentru S. Într-adevăr, dacă $c \in S$ există $y \in S$ cu $ya = c$. Atunci $ce = yae = ya = c$. Analog, considerând $e' \in S$ cu $e'a = a$ rezultă că $e'c = c$ pentru orice $c \in S$. Cum e' şi e sunt elemente neutre la stânga, respectiv la dreapta, rezultă $e' = e'e = e$, deci e este element neutru pentru S. Fie acum $a \in S$ şi $a', a'' \in S$ cu $a'a = e$ şi $aa'' = e$. Atunci $a' = a'e = a'aa'' = ea'' = a''$ şi acesta este un invers pentru a. Aşadar S este grup.

3. Fie $(S, \cdot)$ un semigrup finit cu simplificare. Atunci pentru orice $a \in S$ aplicaţia $f : S \to S$ definită prin $f(s) = as$ este injectivă şi cum S este finit, f este şi surjectivă. Aceasta înseamnă că pentru orice $a, b \in S$ ecuaţia $ax = b$ are soluţie în S. Analog ecuaţia $ya = b$ are soluţie în S şi atunci aplicând

problema 2 rezultă că S este grup.

4. Observăm mai întâi că dacă X şi Y sunt grupuri aditive, iar $f \in \mathrm{Hom}_{gr}(X,Y)$, atunci pentru orice $n \in \mathbb{N}^*$ şi orice $x_1, \ldots, x_n \in X$ are loc relaţia $f(x_1 + \cdots + x_n) = f(x_1) + \cdots + f(x_n)$, lucru care se demonstrează imediat prin inducţie după n. Atunci, dacă $f \in \mathrm{Hom}_{gr}(\mathbb{Z},\mathbb{Z})$ şi $f(1) = a \in \mathbb{Z}$, rezultă că pentru $n \in \mathbb{N}$ avem $f(n) = nf(1) = na$. Apoi pentru $n \in \mathbb{Z}$, $n < 0$, $f(n) = -f(-n) = -a(-n) = an$ şi $f(0) = 0 = a \cdot 0$, deci $f(n) = an$ pentru orice $n \in \mathbb{Z}$. Aşadar $\mathrm{Hom}_{gr}(\mathbb{Z},\mathbb{Z}) = \{f_a \mid a \in \mathbb{Z}\}$, unde $f_a : \mathbb{Z} \to \mathbb{Z}$ este definită prin $f_a(n) = an$. Deci $\mathrm{Hom}_{gr}(\mathbb{Z},\mathbb{Z}) \simeq \mathbb{Z}$.

În mod similar $\mathrm{Hom}_{gr}(\mathbb{Z},\mathbb{Q}) = \{g_a \mid a \in \mathbb{Q}\}$, unde $g_a : \mathbb{Z} \to \mathbb{Q}$ este definită prin $g_a(n) = an$ pentru orice $n \in \mathbb{Z}$. Deci $\mathrm{Hom}_{gr}(\mathbb{Z},\mathbb{Q}) \simeq \mathbb{Q}$.

Dacă $h \in \mathrm{Hom}_{gr}(\mathbb{Q},\mathbb{Q})$, atunci notând $h(1) = a \in \mathbb{Q}$ rezultă de mai sus că $h(n) = an$ pentru orice $n \in \mathbb{Z}$. Apoi dacă $x = p/q \in \mathbb{Q}$, cu $p, q \in \mathbb{Z}$, $q > 0$, atunci $h(p) = h(q(p/q)) = qh(p/q)$, deci $h(p/q) = h(p)/q = ap/q$. Aşadar $h(x) = ax$ pentru orice $x \in \mathbb{Q}$ şi $\mathrm{Hom}_{gr}(\mathbb{Q},\mathbb{Q}) = \{h_a \mid a \in \mathbb{Q}\}$, unde $h_a : \mathbb{Q} \to \mathbb{Q}$ este definită prin $h_a(x) = ax$. Deci $\mathrm{Hom}_{gr}(\mathbb{Q},\mathbb{Q}) \simeq \mathbb{Q}$.

Dacă $h \in \mathrm{Hom}_{gr}(\mathbb{Q},\mathbb{Z})$, atunci există $a \in \mathbb{Q}$ astfel încât $h(x) = ax$ pentru orice $x \in \mathbb{Q}$, deoarece îl putem privi pe h ca pe un morfism de la $\mathbb{Q}$ la $\mathbb{Q}$. Dacă $a \neq 0$, atunci $h(1/2a) = 1/2 \in \mathbb{Z}$, contradicţie. Rezultă că $a = 0$ şi deci $\mathrm{Hom}_{gr}(\mathbb{Q},\mathbb{Z}) = \{0\}$ (prin 0 am desemnat morfismul nul).

Pentru a calcula $\mathrm{Hom}_{gr}(\mathbb{Z}_n,\mathbb{Z}_n)$ procedăm ca şi în cazul lui $\mathrm{Hom}_{gr}(\mathbb{Z},\mathbb{Z})$ şi obţinem că morfismele cerute sunt aplicaţiile de forma $f_{\hat{a}} : \mathbb{Z}_n \to \mathbb{Z}_n$ definite prin $f_{\hat{a}}(\hat{x}) = \hat{a}\hat{x}$ pentru orice $x \in \mathbb{Z}$, unde $a \in \{0, 1, \ldots, n-1\}$. Deci $\mathrm{Hom}_{gr}(\mathbb{Z}_n,\mathbb{Z}_n) \simeq \mathbb{Z}_n$.

Vom arăta că $\mathrm{Hom}_{gr}(\mathbb{Z}_m,\mathbb{Z}_n) \simeq \mathbb{Z}_d$, unde $d = (m,n)$. Notăm cu $\hat{x}$ clasele din $\mathbb{Z}_m$, cu $\overline{x}$ clasele din $\mathbb{Z}_n$ şi cu cu $\tilde{x}$ clasele din $\mathbb{Z}_d$. Considerăm $f \in \mathrm{Hom}_{gr}(\mathbb{Z}_m,\mathbb{Z}_n)$. Atunci $f(\hat{x}) = \overline{ax}$ pentru orice $x \in \mathbb{Z}_m$, unde $\overline{a} = f(\hat{1})$. Dar $m\overline{a} = mf(\hat{1}) = f(m\hat{1}) = f(\hat{0}) = \overline{0}$ şi cum $(\underline{m/d}, n/d) = 1$, rezultă că $\frac{n}{d} | a \Rightarrow \overline{a} \in \{\overline{0}, \overline{n/d}, \ldots, \overline{(d-1)n/d}\}$, adică $\overline{a} \in < \overline{n/d} >$. Acum este clar că asocierea $f \mapsto f(\hat{1})$ defineşte un izomorfism de grupuri între $\mathrm{Hom}_{gr}(\mathbb{Z}_m,\mathbb{Z}_n)$ şi $< \overline{n/d} > \simeq \mathbb{Z}_d$.

5. Cum $\mathbb{Z}$ şi $\mathbb{Q}$ sunt mulţimi numărabile, iar $\mathbb{R}$ şi $\mathbb{C}$ sunt nenumărabile rămâne să determinăm perechile de grupuri izomorfe din clasele:
(i) $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{Q}^*,\cdot)$, $(\mathbb{Q}_+^*,\cdot)$;
(ii) $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{R}_+^*,\cdot)$, $(\mathbb{C}^*,\cdot)$.

În cazul (i), din problema precedentă $(\mathbb{Z},+)$ şi $(\mathbb{Q},+)$ nu sunt izomorfe. Apoi $(\mathbb{Q}^*,\cdot)$ nu este ciclic, deoarece dacă $a=p/q$, cu $p,q\in\mathbb{Z}$, $q\neq 0$, ar fi un generator, este suficient să alegem un număr prim h care nu divide nici p şi nici q, şi atunci evident $h\neq a^n$ pentru orice $n\in\mathbb{Z}$. Cu acelaşi argument $(\mathbb{Q}_+^*,\cdot)$ nu este ciclic. Rezultă că niciunul din aceste două grupuri nu este izomorf cu $(\mathbb{Z},+)$.

Observăm că grupul $(\mathbb{Q},+)$ este divizibil (adică pentru orice $a\in\mathbb{Q}$ şi $n\in\mathbb{N}^*$ ecuaţia $nx=a$ are soluţie în $\mathbb{Q}$), dar grupurile $(\mathbb{Q}^*,\cdot)$ şi $(\mathbb{Q}_+^*,\cdot)$ nu au această proprietate, ecuaţia $x^2=2$ neavând soluţie în niciunul dintre ele. Cum proprietatea de a fi grup divizibil se transferă între grupuri izomorfe, rezultă că $(\mathbb{Q},+)$ nu este izomorf cu niciunul dintre aceste două grupuri.

În sfârşit, în $(\mathbb{Q}^*,\cdot)$ ecuaţia $x^2=1$ are două soluţii, iar în $(\mathbb{Q}_+^*,\cdot)$ ecuaţia $x^2=a$ are cel mult o soluţie pentru orice a, de unde rezultă că nici aceste două grupuri nu sunt izomorfe. Aşadar orice două grupuri din prima clasă sunt neizomorfe.

În cazul (ii) vom arăta mai întâi că $(\mathbb{R},+)$ şi $(\mathbb{C},+)$ sunt izomorfe. Pentru aceasta privim pe $\mathbb{R}$ şi $\mathbb{C}$ ca $\mathbb{Q}$-spaţii vectoriale. Deoarece $\mathbb{Q}$ este mulţime numărabilă, un $\mathbb{Q}$-spaţiu vectorial de dimensiune cel mult numărabilă este cel mult numărabil. Cum $\mathbb{R}$ şi $\mathbb{C}$ sunt nenumărabile, rezultă că ambele au baze de acelaşi cardinal cu $\mathbb{R}$ (am folosit aici ipoteza continuului, că între $|\mathbb{N}|$ şi $|\mathbb{R}|$ nu mai există nici un număr cardinal). Dar două spaţii vectoriale cu baze de acelaşi cardinal sunt izomorfe, deci $\mathbb{R}$ şi $\mathbb{C}$ sunt izomorfe ca $\mathbb{Q}$-spaţii vectoriale, deci şi ca grupuri aditive.

De asemenea observăm că $f:(\mathbb{R},+)\to(\mathbb{R}_+^*,\cdot)$, $f(x)=e^x$, este un izomorfism de grupuri.

Grupurile $(\mathbb{R},+)$ şi $(\mathbb{C}^*,\cdot)$ sunt divizibile, iar grupul $(\mathbb{R}^*,\cdot)$ nu este divizibil, ecuaţia $x^2=-1$ neavând soluţii în $\mathbb{R}^*$, deci $(\mathbb{R}^*,\cdot)$ nu este izomorf cu niciunul dintre grupurile $(\mathbb{R},+)$ şi $(\mathbb{C}^*,\cdot)$.

În sfârşit, $(\mathbb{R},+)$ şi $(\mathbb{C}^*,\cdot)$ nu sunt izomorfe, deoarece ecuaţia $z^2=1$ are două soluţii în $\mathbb{C}^*$, iar ecuaţia $2x=0$ are o singură soluţie în $(\mathbb{R},+)$.

Aşadar din a doua listă sunt izomorfe grupurile $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{R}^*,\cdot)$.

6. (i) Fie $g\in G$. Atunci $A\cap gB^{-1}\neq\emptyset$, deoarece $|A|+|gB^{-1}|=|A|+|B|>|G|$ (am notat $B^{-1}=\{b^{-1}\mid b\in B\}$). Fie $a\in A\cap gB^{-1}$. Atunci există $b\in B$ cu $a=gb^{-1}$. Rezultă că $g=ab\in AB$, deci $G=AB$.
(ii) Aplicăm punctul (i) pentru mulţimile M şi M şi rezultă că $G=MM$. Fie atunci $g,h\in G$. Avem $g=ab$, $h=cd$ cu $a,b,c,d\in M$. Cum elementele lui M comută între ele rezultă că $gh=hg$.

7. Presupunem că submulţimea finită H a lui G este parte stabilă. Fie $h \in H$. Atunci $\{h^n \mid n \in \mathbb{N}\} \subseteq H$ şi cum H este finită rezultă că există $i < j$ cu $h^i = h^j$. Atunci $h^{j-i} = e$ (e elementul neutru al lui G), de unde $e \in H$. De asemenea, dacă $h \neq e$, atunci $j - i > 1$ şi $h^{-1} = h^{j-i-1} \in H$. Obţinem că H este subgrup.

8. Avem $D_4 = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\}$, unde $\text{ord}(r) = 4$, $\text{ord}(s) = 2$ şi $sr = r^3s$. Folosind aceste relaţii între generatori se obţine uşor prin calcul că D_4 are două elemente de ordin 4, r şi r^2, un element de ordin 1 (elementul neutru) şi cinci elemente de ordin 2: r^2, s, rs, r^2s, r^3s.
Un subgrup al lui D_4 poate avea $1, 2, 4$ sau 8 elemente. Avem un subgrup cu un element (subgrupul trivial), un subgrup cu 8 elemente (D_4) şi cinci subgrupuri cu 2 elemente: cele de forma $\{e, x\}$ cu $\text{ord}(x) = 2$. Rămân de descris subgrupurile cu 4 elemente. Unul dintre acestea este $< r > = \{e, r, r^2, r^3\}$. Dacă H este un alt subgrup cu 4 elemente, atunci el nu poate conţine pe r sau r^3 care au ordinul 4. Dacă $r^2 \notin H$, atunci H conţine trei dintre elementele s, rs, r^2s, r^3s, deci există $i \in \{0, 1, 2\}$ cu $r^is, r^{i+1}s \in H$. Atunci $r = (r^{i+1}s)(r^is)^{-1} \in H$, contradicţie. Aşadar $r^2 \in H$ şi obţinem două astfel de subgrupuri: $\{e, r^2, s, r^2s\}$ şi $\{e, r^2, rs, r^3s\}$.
Subgrupurile $\{e\}$ şi D_4 sunt normale. De asemenea subgrupurile cu 4 elemente sunt normale, având indice 2. Dintre subgrupurile cu 2 elemente se verifică prin calcul că doar $\{e, r^2\}$ este normal (ca intersecţie de două subgrupuri normale de ordin 4).

9. Vom arăta mai mult: dacă H şi K sunt subgrupuri ale unui grup G, atunci $H \cup K$ este subgrup dacă şi numai dacă $H \subseteq K$ sau $K \subseteq H$. Să presupunem că $H \not\subseteq K$ şi $K \not\subseteq H$. Fie $h \in H - K$ şi $k \in K - H \Rightarrow hk \notin H \cup K$ (dacă $hk \in H$, atunci $k \in H$, fals; dacă $hk \in K$, atunci $h \in K$, fals), deci $H \cup K$ nu este subgrup.

Grupul lui Klein şi grupul diedral D_4 se scriu ca reuniune de trei subgrupuri proprii. Într-adevăr, fie $K = \{e, a, b, ab\}$ un grup multiplicativ izomorf cu grupul lui Klein, deci e este element neutru, $a^2 = b^2 = e$ şi $ab = ba$. Atunci $K = \{e, a\} \cup \{e, b\} \cup \{e, ab\}$ este reuniune de trei subgrupuri proprii. De asemenea, ţinând cont de descrierea subgrupurilor lui D_4 din problema 8, păstrând notaţiile de la soluţia acelei probleme, avem că $D_4 = \{e, r, r^2, r^3\} \cup \{e, r^2, s, r^2s\} \cup \{e, r^2, rs, r^3s\}$.

10. Fie $x \in G$. Dacă $x \in H \cap K \cap L$, atunci este clar. Dacă $x \in H \cap K$, atunci arătăm că $x \in L$. Într-adevăr, dacă $x \notin L$, alegem $z \in L - (H \cup K)$ (dacă $L \subseteq H \cup K \Rightarrow G = H \cup K$, ceea ce nu se poate după cum rezultă din problema 9) si obţinem că $xz \notin H$ (altfel $z \in H$, fals), $xz \notin K$ (altfel $z \in K$, fals) şi $xz \notin L$ (altfel $x \in L$, fals), contradicţie. Deci un element care aparţine intersecţiei a două dintre subgrupurile H, K, L este şi în al treilea. Să presupunem acum că $x \in H$ şi $x \notin K \cup L$. Fie $z \in L - (H \cup K) \Rightarrow xz \notin H$ şi $xz \notin L \Rightarrow xz \in K - (H \cup L) \Rightarrow x(xz) \notin H \cup K \Rightarrow x(xz) \in L \Rightarrow x^2 z \in L \Rightarrow x^2 \in L$. Alegând acum $y \in K - (H \cup L)$, obţinem că $xy \notin H \cup K \Rightarrow xy \in L - (H \cup K) \Rightarrow x^2 y \notin H \cup L \Rightarrow x^2 y \in K \Rightarrow x^2 \in K$. În concluzie, $x^2 \in H \cap K \cap L$.

Observaţie. Se poate arăta chiar mai mult, că H, K, L sunt subgrupuri de indice 2. De aici rezultă că $x^2 \in H \cap K \cap L$ pentru orice $x \in G$.

11. Să presupunem că $G = H_1 \cup \cdots \cup H_m$, unde $H_1, \ldots, H_m$ sunt subgrupuri proprii ale lui G, $i = 1, \ldots, m$. Deoarece există $x_i \in H_i$ cu $\text{ord}(x_i) > m$, rezultă că $|H_i| > m$ pentru orice $i = 1, \ldots, m$. Fie $t_i = [G : H_i]$. Avem $t_i > 1$ pentru orice $i = 1, \ldots, m$. Pe de altă parte, $|G| < |H_1| + \cdots + |H_m|$ (deoarece $H_i \cap H_j \neq \emptyset$ oricare ar fi $i, j \in \{1, \ldots, m\}$). Fie $t = \min\{t_1, \ldots, t_m\}$. Rezultă că $t > 1$ şi fie p un divizor prim al lui $t \Rightarrow p||G| \Rightarrow$ există $g \in G$ cu $\text{ord}(g) = p$ (din teorema lui Chauchy) $\Rightarrow p > m \Rightarrow t_i > m$, pentru orice $i = 1, \ldots, m \Rightarrow 1 > \frac{1}{t_1} + \cdots + \frac{1}{t_m} = \frac{1}{|G|}(|H_1| + \cdots + |H_m|) > 1$, contradicţie.

12. Din teorema lui Lagrange rezultă că dacă G are elemente de ordin 2 atunci $|G|$ este par. Reciproc, presupunem că $|G|$ este par. Dacă G nu ar avea elemente de ordin 2, atunci pentru orice $x \neq e$ avem $x \neq x^{-1}$ şi atunci putem scrie $G = \{e\} \cup (\cup_{x \in G} \{x, x^{-1}\})$, deci G ar avea un număr impar de elemente (mulţimile cu câte două elemente care intră în reuniune sunt sau disjuncte sau egale). Obţinem astfel o contradicţie, deci G are elemente de ordin 2.

13. (i) Aplicaţia f este morfism de grupuri dacă şi numai dacă pentru orice $x, y \in G$ avem $f(xy) = f(x)f(y)$, adică $(xy)^2 = x^2 y^2$. Înmulţind cu x^{-1} la stânga şi cu y^{-1} la dreapta obţinem $xy = yx$, adică G este grup abelian. Reciproc este evident.
(ii) Ştim că f este morfism de grupuri. Cum G este grup finit, rezultă că f este izomorfism dacă şi numai dacă f este injectiv, deci dacă şi numai dacă $\text{Ker}(f) = \{e\}$. Aşadar f este izomorfism dacă şi numai dacă G nu are ele-

mente de ordin 2. Dar din problema 12 aceasta este echivalent cu $|G|$ impar.

14. (i) Fie $x, y \in G$. Atunci $(xy)^2 = e$, deci $xyxy = e$. Înmulţind cu x^{-1} la stânga şi cu y^{-1} la dreapta şi ţinând cont că $x^2 = y^2 = e$, obţinem $yx = xy$.
(ii) Observăm că grupul abelian $(G, \cdot)$ se poate înzestra cu o structură de $\mathbb{Z}_2$-spaţiu vectorial, înmulţirea cu scalari fiind definită astfel: $\hat{0} \cdot x = e$ şi $\hat{1} \cdot x = x$ pentru orice $x \in G$. Verificarea este imediată, observându-se că este esenţială condiţia $x^2 = e$ pentru orice $x \in G$ (trebuie, de exemplu, ca $(\hat{1}+\hat{1})x = (\hat{1}x)(\hat{1}x)$ ceea ce este echivalent cu $x^2 = e$). Cum G este grup finit, va avea dimensiune finită. Fie aceasta n. Atunci G este izomorf, ca $\mathbb{Z}_2$-spaţiu vectorial, cu $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (în produs intrând n factori). În particular, acesta este şi izomorfism de grupuri, deci G are 2^n elemente.

15. Dacă există $g \in G$ de ordin infinit, atunci subgrupul $< g >$ generat de g este izomorf cu $(\mathbb{Z}, +)$, deci are o infinitate de subgrupuri. Acestea fiind şi subgrupuri ale lui G obţinem rezultatul dorit.
Dacă toate elementele lui G au ordin finit, considerăm toate subgrupurile ciclice ale lui G. Dacă am avea doar un număr finit de astfel de subgrupuri ar rezulta că G este o reuniune finită de subgrupuri finite, deci G este grup finit, contradicţie. În concluzie G are o infinitate de subgrupuri distincte şi în acest caz.

16. Să observăm că din problema 15 rezultă că grupurile cu un număr finit de subgrupuri sunt finite.
(i) G are exact două subgrupuri. Atunci aceste subgrupuri sunt G şi $\{e\}$. Fie $g \in G - \{e\}$. Atunci $< g >$ este subgrup netrivial al lui G, deci $< g > = G$. Rezultă că G este grup ciclic finit şi deci există $n \in \mathbb{N}^*$ cu $G \simeq \mathbb{Z}_n$. Dacă n nu este număr prim, fie p prim cu $p|n$ şi atunci $\hat{p}\mathbb{Z}_n$ este un subgrup propriu şi netrivial al lui $\mathbb{Z}_n$, contradicţie. Aşadar n este număr prim. Rezultă că $|G| = p$ cu p număr prim. Evident orice astfel de grup verifică proprietatea cerută.
(ii) G are exact trei subgrupuri. Fie $\{e\}, H$ şi G cele trei subgrupuri. Deoarece $H \neq G$, există $g \in G - H \Rightarrow < g > \neq \{e\}, H \Rightarrow < g > = G$, deci G este grup ciclic finit. Rezultă că $G \simeq \mathbb{Z}_n$ cu $n \in \mathbb{N}^*$. Dacă n ar avea doi divizori primi distincţi, atunci fiecare dintre aceştia ar genera un subgrup propriu şi netrivial în $\mathbb{Z}_n$, deci G ar avea cel puţin patru subgrupuri. Rezultă că $n = p^2$ cu p număr prim şi $G \simeq \mathbb{Z}_{p^2}$. Evident aceste grupuri verifică proprietatea

cerută.
(iii) G are exact patru subgrupuri. Fie $\{e\}, H, K$ şi G cele patru subgrupuri. Deoarece $H \cup K \neq G$ (vezi problema 9), există $g \in G - (H \cup K) \Rightarrow < g > \neq \{e\}, H, K \Rightarrow < g > = G$, deci G este grup ciclic finit. Rezultă că $G \simeq \mathbb{Z}_n$ cu $n \in \mathbb{N}^*$. Cum numărul de subgrupuri ale lui $\mathbb{Z}_n$ este egal cu numărul divizorilor naturali ai lui n, obţinem că $n = p^3$, p număr prim, sau $n = pq$, unde p şi q sunt numere prime distincte.
(iv) G are exact cinci subgrupuri. Fie $\{e\}, H, K, L$ şi G cele cinci subgrupuri. Avem două cazuri: $G \neq H \cup K \cup L$ sau $G = H \cup K \cup L$.
Dacă $G \neq H \cup K \cup L$, atunci există $g \in G - (H \cup K \cup L) \Rightarrow < g > \neq \{e\}, H, K, L \Rightarrow < g > = G$, deci G este grup ciclic finit, $G \simeq \mathbb{Z}_n$. Astfel obţinem că $n = p^4$, unde p este număr prim.
Dacă $G = H \cup K \cup L$, atunci $x^2 \in H \cap K \cap L$ pentru orice $x \in G$ (vezi problema 10). Dar $H \cap K \cap L = \{e\}$, deoarece $H \cap K \cap L$ este subgrup al fiecăruia dintre cele trei subgrupuri şi dacă să zicem $H \cap K \cap L = H$, atunci $H \subseteq K \cap L$ şi vom avea că $G = K \cup L$, fals. Rezultă că $x^2 = e$ pentru orice $x \in G$, deci G este izomorf cu un produs direct finit de cópii ale lui $\mathbb{Z}_2$ (vezi problema 14) şi cum G are exact cinci subgrupuri rezultă imediat că doar cazul $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ convine.

17. Implicaţia directă este evidentă din definiţia subgrupului normal. Presupunem acum că pentru orice $i \in I$ avem $a_i g {a_i}^{-1} \in < g >$ şi ${a_i}^{-1} g a_i \in < g >$. Vrem să arătăm că $xg^p x^{-1} \in < g >$ pentru orice $p \in \mathbb{Z}$ şi $x \in G$. Cum $xg^p x^{-1} = (xgx^{-1})^p$, rezultă că $a_i u {a_i}^{-1} \in < g >$ şi ${a_i}^{-1} u a_i \in < g >$ pentru orice $i \in I$ şi $u \in < g >$. Acum orice $x \in G$ este de forma $x = b_1 \cdots b_r$ cu $b_i \in \{a_i \mid i \in I\} \cup \{a_i^{-1} \mid i \in I\}$ şi afirmaţia rezultă imediat prin inducţie după r.

18. (i) Prin calcul rezultă că $\text{ord}(\mathbf{j}) = \text{ord}(\mathbf{k}) = 4$, $\mathbf{j}^2 = \mathbf{k}^2$ şi că $J \cap K = \{I_2, \mathbf{j}^2\}$.
(ii) Avem $\mathbf{j}^{-1}\mathbf{jj} = \mathbf{jjj}^{-1} = \mathbf{j} \in J$, $\mathbf{kjk}^{-1} = \mathbf{k}^{-1}\mathbf{jk} = \mathbf{j}^2 \in J$ şi acum din problema 17 rezultă că J este subgrup normal în Q. În mod similar K este subgrup normal (folosind relaţiile $\mathbf{jkj}^{-1} = \mathbf{j}^{-1}\mathbf{kj} = \mathbf{k}^2$). Atunci JK este subgrup în Q şi cum $\mathbf{j}, \mathbf{k} \in JK$ rezultă că $JK = Q$. Din teorema a doua de izomorfism pentru grupuri obţinem $JK/J \simeq K/J \cap K$, deci $|Q| = |JK| = |J||K|/|J \cap K| = 8$.
(iii) Cum J este subgrup de indice 2 în Q şi $\mathbf{k} \in J$, rezultă că $Q = J \cup \mathbf{k}J$, deci $Q = \{I_2, \mathbf{j}, \mathbf{j}^2, \mathbf{j}^3, \mathbf{k}, \mathbf{kj}, \mathbf{kj}^2, \mathbf{kj}^3\}$. Folosind relaţiile de la (ii) rezultă prin

calcule că $\mathbf{j}^2 = \mathbf{k}^2$ este singurul element de ordin 2 din Q.
(iv) Fie H un subgrup al lui Q. Din teorema lui Lagrange rezultă că $|H| \in \{1, 2, 4, 8\}$. Dacă $|H|$ este 1 sau 8, evident H este subgrup normal. Dacă $|H| = 4$, atunci el are indice 2 şi deci este normal. Dacă $|H| = 2$, folosind (iii) rezultă că $H = \{I_2, \mathbf{j}^2\}$. Atunci $H =< \mathbf{j}^2 >$ şi cum $\mathbf{jj}^2\mathbf{j}^{-1} = \mathbf{j}^{-1}\mathbf{j}^2\mathbf{j} = \mathbf{j}^2 \in H$ şi $\mathbf{kj}^2\mathbf{k}^{-1} = \mathbf{k}^{-1}\mathbf{j}^2\mathbf{k} = \mathbf{k}^2 = \mathbf{j}^2 \in H$, din problema 17 rezultă că H este subgrup normal în Q. Cum $\mathbf{jk} \neq \mathbf{kj}$, Q nu este abelian.

19. (i) Fie $\text{ord}(x) = n$, $\text{ord}(y) = m$. Observăm mai întâi că $< x > \cap < y > = \{e\}$, deoarece din teorema lui Lagrange ordinul acestei intersecţii divide şi pe n şi pe m, deci este 1. Acum dacă $(xy)^p = e$, cum x şi y comută rezultă că $x^p y^p = e$, deci $x^p = y^{-p} \in < x > \cap < y > = \{e\}$, deci $x^p = y^{-p} = e$. Atunci n divide p şi m divide $-p$. Cum $(n, m) = 1$, rezultă că p se divide cu mn. Pe de altă parte $(xy)^{mn} = (x^n)^m (y^m)^n = e$ şi deci $\text{ord}(xy) = nm$.

Dacă n şi m nu sunt relativ prime rezultatul nu mai este adevărat. De exemplu, fie x un element de ordin $n > 1$ într-un grup şi $y = x^{-1}$. Avem că $\text{ord}(y) = n$, iar $xy = e$ are ordinul 1.
(ii) În grupul $GL(2, \mathbb{R})$ considerăm elementele:

$$x = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \quad \text{şi} \quad y = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$$

care au ordinul 2. În schimb

$$xy = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

are ordin infinit. În concluzie afirmaţia de la (i) nu mai este adevărată dacă x şi y nu comută.
(iii) Răspunsul este în general negativ. Pentru aceasta fie x un element de ordin infinit într-un grup G şi $y = x^{-1}$, care are tot ordin infinit. Atunci $xy = e$ are ordinul 1, dar nici unul dintre $\text{ord}(x)$ şi $\text{ord}(y)$ nu este finit.
(iv) Demonstrăm prin inducţie după n. Pentru $n = 1$ este clar. Presupunem adevărat pentru n şi fie G un grup abelian cu $p_1 \cdots p_{n+1}$ elemente, unde $p_1, \ldots, p_{n+1}$ sunt prime distincte. Fie $x \in G - \{e\}$. Dacă $\text{ord}(x) = p_1 \cdots p_{n+1}$, atunci evident G este grup ciclic. Altfel putem presupune (eventual renotând) că $\text{ord}(x) = p_k \cdots p_{n+1}$, cu $k > 1$. Atunci $x^{p_k \cdots p_n}$ are ordinul p_{n+1}. Aşadar putem găsi $y \in G$ cu $\text{ord}(y) = p_{n+1}$. Grupul factor $G/< y >$ are $p_1 \cdots p_n$

elemente şi din ipoteza de inducţie este ciclic. Fie $z< y >$ un generator al său, $z \in G$. Deci $z^{p_1 \cdots p_n} \in < y >$. Dacă $z^{p_1 \cdots p_n} = e$, atunci $\text{ord}(z) = p_1 \cdots p_n$ şi atunci din (i) rezultă că $\text{ord}(yz) = p_1 \cdots p_{n+1}$, deci G este grup ciclic. Dacă $z^{p_1 \cdots p_n} \neq e$, atunci el are ordin p_{n+1}, deci z are ordin $p_1 \cdots p_{n+1}$ şi din nou rezultă că G este grup ciclic.

20. (i) Fie G un grup cu 4 elemente. Dacă G are un element de ordin 4, atunci G este ciclic, deci izomorf cu $\mathbb{Z}_4$. Dacă G nu are elemente de ordin 4, atunci $x^2 = e$ pentru orice $x \in G$ şi atunci $G = \{e, a, b, ab\}$, unde a, b sunt elemente ale lui G diferite între ele şi diferite de e. Este clar că $ba \notin \{e, a, b\}$, deci $ba = ab$ şi atunci G este izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_2$, un izomorfism fiind dat de $f : G \to \mathbb{Z}_2 \times \mathbb{Z}_2$ $f(e) = (\hat{0}, \hat{0}), f(a) = (\hat{1}, \hat{0}), f(b) = (\hat{0}, \hat{1}), f(ab) = (\hat{1}, \hat{1})$.
(ii) Fie G un grup cu 6 elemente. Dacă G are un element de ordin 6, atunci G este ciclic, deci izomorf cu $\mathbb{Z}_6$. Presupunem că G nu este ciclic. Atunci $\text{ord}(x) \in \{1, 2, 3\}$ pentru orice $x \in G$. Dacă $\text{ord}(x) = 2$ pentru orice $x \neq e$, atunci dacă $a, b \in G - \{e\}, a \neq b$, rezultă ca la (i) că $\{e, a, b, ab\}$ este subgrup al lui G şi din teorema lui Lagrange rezultă că $4|6$, contradicţie. Aşadar există $x \in G$ cu $\text{ord}(x) = 3$. Fie $y \in G - < x >$. Atunci $G = < x > \cup y< x > = \{e, x, x^2, y, yx, yx^2\}$. Dacă $\text{ord}(y) = 3$, cum $y^2 \notin \{e, y, yx, yx^2\}$, rezultă $y^2 = x$, de unde $y = y^4 = x^2$, contradicţie, sau $y^2 = x^2$, de unde $y = y^4 = x^4 = x$, din nou contradicţie. Deci $\text{ord}(y) = 2$. Dacă $xy = yx$, cum $\text{ord}(x)$ şi $\text{ord}(y)$ sunt relativ prime rezultă $\text{ord}(xy) = 2 \cdot 3 = 6$ (vezi problema 19), deci G este ciclic, contradicţie. Mai departe obţinem $xy = yx^2$, deoarece xy nu poate fi niciunul dintre celelalte cinci elemente. Rezultă că G este izomorf cu S_3, un izomorfism fiind indus de asocierile $x \to \sigma$ şi $y \to \tau$ cu σ ciclu de lungime 3 şi τ transpoziţie.
(iii) Fie G un grup neabelian cu 8 elemente. Atunci G nu are elemente de ordin 8 şi nu se poate ca $x^2 = e$ pentru orice $x \in G$ (ar rezulta că G este abelian). Aşadar există $x \in G$ cu $\text{ord}(x) = 4$. Fie $y \in G - < x >$. Atunci $G = < x > \cup y< x > = \{e, x, x^2, x^3, y, yx, yx^2, yx^3\}$. Avem două posibilităţi: $\text{ord}(y) = 2$ sau $\text{ord}(y) = 4$.
Dacă $\text{ord}(y) = 2$, atunci evident $xy \notin \{e, x, x^2, x^3, y, yx\}$. Dacă $xy = yx^2$, atunci $x^2 = yxy$, deci $e = x^4 = (yxy)(yxy) = yx^2y$, deci $x^2 = y^2 = e$, contradicţie. Deci $xy = yx^3$ şi atunci $G = < x, y >$ cu $\text{ord}(x) = 4$, $ord(y) = 2$ şi $xy = yx^3$, aceasta determinând în mod unic operaţia pe G, de unde $G \simeq D_4$ (grupul diedral cu 8 elemente este definit prin aceleaşi relaţii ca şi G).
Dacă $\text{ord}(y) = 4$, atunci evident $y^2 \notin \{e, y, yx, yx^2, yx^3\}$. Dacă $y^2 = x$, rezultă $x^2 = y^4 = e$, contradicţie. Dacă $y^2 = x^3$, atunci $x^2 = x^6 = y^4 =$

e, din nou contradicţie. Aşadar $y^2 = x^2$. Mai departe este clar că $xy \notin \{e, x, x^2, x^3, yx\}$. Dacă $xy = yx^2$, atunci $xy = y^3$, deci $x = y^2$ şi $x^2 = y^4 = e$, contradicţie. Rezultă că $xy = yx^3$ şi deci $G = < x, y >$, unde $\text{ord}(x) = \text{ord}(y) = 4$, $xy = yx^3$, relaţii care determină în mod unic operaţia pe G. În consecinţă G este izomorf cu Q, grupul cuaternionilor, care satisface exact aceste relaţii.

Fie acum G un grup abelian cu 8 elemente. Dacă G este ciclic, atunci el este izomorf cu $\mathbb{Z}_8$. Presupunem că G nu are elemente de ordin 8. Dacă toate elementele lui G au ordin 2, atunci definim pe G o structură de $\mathbb{Z}_2$-spaţiu vectorial (ca în soluţia de la problema 14) şi rezultă că $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Dacă există un element de ordin 4, fie acesta x, atunci alegem $y \notin < x >$ şi avem $G = < x > \cup y < x > = \{e, x, x^2, x^3, y, yx, yx^2, yx^3\}$. Arătăm că există un element $z \notin < x >$ de ordin 2. Într-adevăr, dacă y are ordin 2 luăm $z = y$. Dacă nu, atunci $\text{ord}(y) = 4$, deci $\text{ord}(y^2) = 2$ şi deci $y \neq x, x^2$ care au ordin 4 şi evident $y^2 \notin \{e, y, yx, yx^2, yx^3\}$. Rezultă că $y^2 = x^2$ şi atunci $yx \neq e$, iar $(yx)^2 = y^2x^2 = x^4 = e$, de unde $\text{ord}(yx) = 2$ şi putem lua $z = yx$. Aşadar am găsit $x, z \in G$ cu $\text{ord}(x) = 4$, $\text{ord}(z) = 2$ şi $z \notin < x >$. Atunci aplicaţia $f : \mathbb{Z}_2 \times \mathbb{Z}_4 \to G$ definită prin $f(\hat{i}, \hat{j}) = z^i x^j$ este corect definită, este morfism de grupuri şi este surjectivă. Cum cele două grupuri au 8 elemente rezultă că f este izomorfism de grupuri.
(iv) Fie G un grup cu p elemente, p număr prim. Dacă $x \in G - \{e\}$, atunci $< x >$ este un subgrup netrivial al lui G şi din teorema lui Lagrange rezultă că are p elemente. Atunci $G = < x >$, deci este grup ciclic cu p elemente.

21. Fie $x = r/s \in X$, $x \neq 0$. Atunci $0 \neq sx \in X \cap \mathbb{Z}$ şi deci $X \cap \mathbb{Z}$ este un subgrup nenul al lui $\mathbb{Z}$. Fie $X \cap \mathbb{Z} = n\mathbb{Z}$ cu $n > 0$. Cum $X + \mathbb{Z} = \mathbb{Q}$, rezultă că există $a \in \mathbb{Z}$ şi $y \in X$ cu $1/n = a + y$. Atunci $1 = na + ny \in n\mathbb{Z} + X \subseteq X + X = X$, deci $1 \in X$. Rezultă că $\mathbb{Z} \subseteq X$ şi $\mathbb{Q} = \mathbb{Z} + X = X$.

Observaţie. Mai putem rezolva această problemă şi cu ajutorul problemei 35(v). Mai precis, din $X + \mathbb{Z} = \mathbb{Q}$ rezultă $\mathbb{Q}/X = (X + \mathbb{Z})/X \simeq \mathbb{Z}/X \cap \mathbb{Z}$, deci X este un subgrup de indice finit al lui $\mathbb{Q}$ care este un grup divizibil, aşadar $X = \mathbb{Q}$.

22. Fie $H = < p_1/q_1, \ldots, p_n/q_n >$ şi $q = q_1 \cdots q_n$. Atunci evident qH este un subgrup al lui $\mathbb{Z}$, deci există $m \in \mathbb{Z}$ cu $qH = m\mathbb{Z}$. Rezultă că $H = (m/q)\mathbb{Z}$, deci H este subgrup ciclic generat de m/q.

Dacă grupul $(\mathbb{Q}, +)$ ar fi finit generat, atunci ar fi ciclic. Fie atunci $x \in \mathbb{Q}$, $x = r/s$, $r \in \mathbb{Z}$, $s \in \mathbb{N}^*$, cu proprietatea că $< x > = \mathbb{Q}$. Dar $\frac{1}{s+1} \notin < \frac{r}{s} >$,

contradicţie.

23. Presupunem că S este un sistem de generatori pentru grupul $(\mathbb{Q}, +)$ şi fie $s \in S - \{0\}$. Fie H subgrupul generat de $S - \{s\}$. Avem $\mathbb{Q} = < S > = H + \mathbb{Z}s$, de unde $(1/s)H + \mathbb{Z} = (1/s)\mathbb{Q} = \mathbb{Q}$. Din problema 21 rezultă că $(1/s)H = \mathbb{Q}$, deci $H = s\mathbb{Q} = \mathbb{Q}$. Atunci şi $S - \{s\}$ este sistem de generatori pentru $\mathbb{Q}$. În particular $(\mathbb{Q}, +)$ nu are un sistem minimal de generatori.

24. Procedăm prin inducţie după $d(G)$. Dacă $d(G) = 1$, atunci evident $2^{d(G)} = 2 \leq |G|$. Presupunem afirmaţia adevărată pentru $d(G) \leq k$ şi fie G un grup cu $d(G) = k + 1$. Fie $\{x_1, \ldots, x_{k+1}\}$ un sistem minimal de generatori pentru G. Notăm cu G' subgrupul lui G generat de $x_1, \ldots, x_k$. Atunci $d(G') = k$ (deoarece G' are un sistem de generatori cu k elemente, iar dacă G' ar avea un sistem de generatori cu $r < k$ elemente, adăugându-l şi pe x_{k+1} am obţine un sistem de generatori pentru G cu $r + 1 < d(G)$ elemente, contradicţie) şi din ipoteza de inducţie rezultă că $|G'| \geq 2^{d(G')} = 2^k$. Cum $x_{k+1} \notin G'$, rezultă că mulţimile G' şi $x_{k+1}G'$ sunt disjuncte, de unde obţinem că $|G| \geq 2|G'| \geq 2^{d(G)}$, ceea ce trebuia demonstrat.

25. Fie σ un ciclu de lungime 3 şi τ o transpoziţie din S_3. Arătăm că $\{(\sigma, \hat{1}), (\tau, \hat{1})\}$ este un sistem minimal de generatori pentru $S_3 \times \mathbb{Z}_4$. Fie $(f, \hat{k}) \in S_3 \times \mathbb{Z}_4$. Cum σ şi τ generează pe S_3, rezultă că există $i, j \in \mathbb{Z}$ astfel încât $f = \sigma^i \tau^j$. Atunci $f = \sigma^s \tau^j$ pentru orice $s \in \mathbb{Z}$ cu $s \equiv i (\text{mod } 3)$. Arătăm că există s astfel încât $s + j \equiv k (\text{mod } 4)$ (va rezulta atunci că $(\sigma, \hat{1})^s (\tau, \hat{1})^j = (f, \hat{k})$). Aceasta este echivalent cu $s \equiv i (\text{mod } 3)$ şi $s \equiv k - j (\text{mod } 4)$. Dar un astfel de s există deoarece 4 şi 3 sunt relativ prime (se aplică Lema chineză a resturilor). Cum grupul $S_3 \times \mathbb{Z}_4$ nu este abelian, el nu este nici ciclic, deci nu are un sistem de generatori cu un singur element. Prin urmare un sistem minimal de generatori are două elemente.

Pentru $Q \times \mathbb{Z}_3$ se arată la fel ca mai sus că $\{(\mathbf{j}, \hat{1}), (\mathbf{k}, \hat{1})\}$ este sistem minimal de generatori (notaţiile sunt cele din problema 18).

26. (i) Fie $x, y \in H$ şi $i, j \in \mathbb{N}^*$ cu $x \in H_i$, $y \in H_j$. Presupunem de exemplu că $i \leq j$. Atunci $H_i \subseteq H_j$, deci $x, y \in H_j$ şi cum H_j este subgrup rezultă $xy^{-1} \in H_j$, deci $xy^{-1} \in H$.
(ii) Presupunem prin absurd că H ar fi finit generat, $H = < x_1, \ldots, x_p >$. Atunci există $n_1, \ldots, n_p \in \mathbb{N}^*$ cu $x_i \in H_{n_i}$ pentru orice $i = 1, \ldots, p$. Dacă n este cel mai mare dintre numerele $n_1, \ldots, n_p$, rezultă că $x_1, \ldots, x_p \in H_n$, de

unde $H = H_n$. Atunci $H_n = H_{n+1}$, contradicţie.

27. Prin calcul rezultă imediat că $g^n(x) = 2^n x$ şi $f_n(x) = x + 1/2^n$ pentru orice $n \in \mathbb{N}^*$ şi $x \in \mathbb{R}$. Atunci $f_{n+1}^2 = f_n$, de unde rezultă, notând $H_n = < f_n >$, că avem $H_n \subseteq H_{n+1}$. Mai mult, incluziunea este strictă deoarece dacă am avea egalitate ar exista $p \in \mathbb{Z}$ cu $f_{n+1} = f_n^p$. Aceasta ar însemna că $x + 1/2^{n+1} = x + p/2^n$, deci $1/2 = p \in \mathbb{Z}$, contradicţie. Aplicând acum rezultatul din problema 26 rezultă că $H = \bigcup_{n \leq 1} H_n$ nu este finit generat.

Observaţie. În cazul în care grupul G este abelian şi finit generat, orice subgrup al său este de asemenea finit generat.

28. Alegem un sistem de generatori $S = \{x_1, \ldots, x_n\}$ pentru G astfel ca dacă $x \in S$ atunci şi $x^{-1} \in S$ (aceasta se poate face considerând un sistem finit de generatori şi adăugând inversele tuturor acestor generatori). Atunci orice element din G se poate scrie ca un produs de elemente din S. Fie acum $g_1, \ldots, g_r$ un sistem de reprezentanţi pentru clasele la dreapta modulo H, deci $G = \bigcup_{i=1}^{r} Hg_i$. Mai mult, reprezentantul ales din clasa H va fi chiar e (elementul neutru al lui G) şi eventual renotând, $g_1 = e$. Cum pentru orice $j \in \{1, \ldots, r\}$ şi $t \in \{1, \ldots, n\}$ avem $g_j x_t \in G$, rezultă că există şi sunt unic determinate $i \in \{1, \ldots, r\}$ şi $h_{jt} \in H$ cu proprietatea că $g_j x_t = h_{jt} g_i$. Fie acum $h \in H$. Atunci $h = x_{i_1} \cdots x_{i_k}$ cu $x_{i_j} \in S$. Folosind relaţiile de mai sus obţinem $h = eh = g_1 h = g_1 x_{i_1} \cdots x_{i_k} = h_{1i_1} g_{j_1} x_{i_2} \cdots x_{i_k} = h_{1i_1} h_{j_1 i_2} g_{j_2} x_{i_3} \cdots x_{i_k} = \ldots = h_{1i_1} h_{j_1 i_2} \cdots h_{j_{k-1} i_k} g_{j_k}$, unde elementele $g_{j_1}, \ldots, g_{j_k}$ sunt unic determinate. Din ultima egalitate rezultă că $g_{j_k} \in H$ şi cum reprezentantul ales în H era chiar e, obţinem $g_{j_k} = e$. Rezultă că H este generat de toate elementele h_{jt}, deci H este finit generat.

29. (i) Definim pe $H \times K$ relaţia $\sim$ prin $(h, k) \sim (h', k')$ dacă şi numai dacă $hk = h'k'$. Deoarece $(h, k) \sim (h', k') \Leftrightarrow hk = h'k'$, avem $h'^{-1}h = k'k^{-1} \in H \cap K$, rezultă că clasa de echivalenţă a lui (h, k) este mulţimea $\{(hx^{-1}, xk) \mid x \in H \cap K\}$. Avem astfel $|HK|$ clase de echivalenţă, fiecare având $|H \cap K|$ elemente. Rezultă că $|H \times K| = |HK||H \cap K|$, deoarece clasele de echivalenţă formează o partiţie a mulţimii $H \times K$.
(ii) Definim $f : (G/H \cap K)_s \to (G/H)_s \times (G/K)_s$ prin $f(x(H \cap K)) = (xH, xK)$, unde prin $(G/H)_s$ am notat mulţimea claselor la stânga modulo subgrupul H. Aplicaţia f este corect definită, deoarece $x(H \cap K) = y(H \cap K)$

implică $x^{-1}y \in H \cap K$, deci $x^{-1}y \in H$ şi $x^{-1}y \in K$, adică $xH = yH$ şi $xK = yK$. Mai mult, f este injectivă, deoarece $xH = yH$ şi $xK = yK$ implică $x^{-1}y \in H$ şi $x^{-1}y \in K$, deci $x^{-1}y \in H \cap K$, adică $x(H \cap K) = y(H \cap K)$. Cum $|(G/H)_s| = [G : H]$, obţinem inegalitatea cerută din existenţa acestei injecţii.
Presupunem acum că $[G : H] = n$ şi $[G : K] = m$ sunt finite şi $(n, m) = 1$. De mai sus avem $[G : H \cap K] \leq nm$. Dar $[G : H \cap K] = [G : H][H : H \cap K]$, deci $n|[G : H \cap K]$. Analog $m|[G : H \cap K]$ şi atunci din faptul că $(n, m) = 1$ rezultă că $nm|[G : H \cap K]$. Prin urmare $[G : H \cap K] = nm$. Mai departe, în acest caz aplicaţia f este chiar bijectivă, deoarece este injectivă şi domeniul şi codomeniul său au acelaşi număr de elemente. Fie $g \in G$. Din surjectivitatea lui f rezultă că există $x \in G$ cu $f(x(H \cap K)) = (g^{-1}H, K)$, deci $xH = g^{-1}H$ şi $xK = K$. Atunci $x \in K$ şi $g^{-1} \in xH$, de unde $g \in H^{-1}x^{-1} = Hx^{-1} \subseteq HK$. Am obţinut deci că $G \subseteq HK$, de unde $G = HK$.
(iii) Definim aplicaţia $f : (L \cap H/L \cap K)_s \to (H/K)_s$ prin $f(x(L \cap K)) = xK$. În mod similar cu (i) se arată că f este corect definită şi este injectivă, de unde rezultă inegalitatea cerută.

30. (i) Să observăm că $(g, h)^p = (e_G, e_H)$ dacă şi numai dacă $g^p = e_G$ şi $h^p = e_H$, ceea ce este echivalent cu $\text{ord}(g)|p$ şi $\text{ord}(h)|p$, de unde rezultă imediat afirmaţia din problemă.
(ii) Cum ordinul lui $\mathbb{Z}_6 \times \mathbb{Z}_{10}$ este 60 şi 8 nu este divizor al acestuia, rezultă că nu există elemente de ordinul 8 în $\mathbb{Z}_6 \times \mathbb{Z}_{10}$.

Folosind (i) rezultă că $(g, h) \in \mathbb{Z}_{12} \times \mathbb{Z}_{15}$ are ordin 4 dacă şi numai dacă $[n, m] = 4$, unde $n = \text{ord}(g)$ şi $m = \text{ord}(h)$. Cum $n|12$ şi $m|15$ rezultă $n = 4$ şi $m = 1$. Singurele elemente de ordin 4 din $\mathbb{Z}_{12}$ sunt $\hat{3}$ şi $\hat{9}$, deci în grupul iniţial există două elemente de ordin 4, şi anume $(\hat{3}, \hat{0})$ şi $(\hat{9}, \hat{0})$.

În sfârşit, un element $(g, h) \in \mathbb{Z}_{12} \times \mathbb{Z}_{36}$ are ordin 6 dacă şi numai dacă $[n, m] = 6$. Aceasta este echivalent cu $(n, m) \in \{(6, 1), (6, 2), (6, 3), (6, 6), (3, 2), (3, 6), (2, 3), (2, 6), (1, 6)\}$. Dar în $\mathbb{Z}_{12}$ avem două elemente de ordin 6, două de ordin 3, unul de ordin 2 şi unul de ordin 1, iar în $\mathbb{Z}_{36}$ avem câte două elemente de ordin 6 şi 3 şi câte un element de ordin 2 şi 1. Corespunzător cu descrierea făcută obţinem 24 de elemente de ordin 6 în grupul dat.

31. (i) Presupunem că G este grup ciclic finit. Fără a micşora generalitatea putem considera $G = \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Din teorema de structură a subgrupurilor unui grup factor, orice subgrup al lui G este de forma $m\mathbb{Z}/n\mathbb{Z}$, unde m este un divizor natural al lui n. În plus, $|m\mathbb{Z}/n\mathbb{Z}| = n/m$. Aşadar

pentru orice divizor pozitiv d al lui n, grupul G are exact un subgrup cu d elemente şi anume $m\mathbb{Z}/n\mathbb{Z}$ cu $m = n/d$.

Presupunem acum că G este un grup finit cu proprietatea că pentru orice $d|n = |G|$ există cel mult un subgrup de ordin d. Fie $A_d = \{x \in G \mid \text{ord}(x) = d\}$. Atunci $|G| = \sum_{d|n} |A_d|$. Fie $d|n$. Dacă $A_d \neq \emptyset$, fie $x \in A_d$; atunci $< x >$ este unicul subgrup cu d elemente al lui G şi deci pentru orice $y \in A_d$ avem $< y > = < x >$. Atunci elementele de ordin d din G sunt chiar elementele de ordin d din grupul ciclic $< x >$ şi în acest caz $|A_d| = \varphi(d)$, unde φ este indicatorul lui Euler. Deci $|A_d| \in \{0, \varphi(d)\}$ pentru orice d. Fie acum $H = \mathbb{Z}_n$ şi $B_d = \{x \in H \mid \text{ord}(x) = d\}$. Din prima parte a problemei rezultă că $|B_d| = \varphi(d)$ pentru orice $d|n$ şi atunci din $\sum_{d|n} |A_d| = \sum_{d|n} |B_d|$ şi $|A_d| \leq |B_d|$ pentru orice d, rezultă că $|A_d| = |B_d|$ pentru orice d. În particular, pentru $d = n$ obţinem $A_n \neq \emptyset$, deci există un element de ordin n în G, ceea ce arată că G este grup ciclic.
(ii) Presupunem mai întâi că G este ciclic şi din nou putem considera $G = \mathbb{Z}_n$. Dacă $d|n$, atunci pentru $x \in \{0, \ldots, n-1\}$ ecuaţia $d\hat{x} = \hat{0}$ este echivalentă cu $\frac{n}{d}|x$. Dar există exact d astfel de elemente x, şi anume $0, \frac{n}{d}, 2\frac{n}{d}, \ldots, (d-1)\frac{n}{d}$.

Reciproc, presupunem că ecuaţia $x^d = 1$ are cel mult d soluţii pentru orice $d|n$. Fie $X_d = \{x \in G \mid x^d = 1\}$. Avem deci $|X_d| \leq d$. Acum dacă H este un subgrup cu d elemente al lui G rezultă că $H \subseteq X_d$. Prin urmare sau nu există subgrupuri de ordin d sau X_d este unicul subgrup de ordin d. Atunci pentru orice $d|n$ grupul G are cel mult un subgrup de ordin d şi atunci din (i) rezultă că G este ciclic.
(iii) Rezultă imediat din (ii) că în cazul în care G este ciclic ecuaţia $x^p = 1$ are cel mult p soluţii în G.

Reciproc, vom demonstra că ecuaţia $x^d = 1$ are cel mult d soluţii în G şi vom aplica din nou (ii). Presupunem că există $d|n$ astfel încât ecuaţia $x^d = 1$ să aibă cel puţin $d+1$ soluţii în G. Fie d minim cu această proprietate şi fie $p > 0$ un divizor prim al lui d. Scriem $d = pd_1$ si observăm că $d_1|n$. Vom arăta că ecuaţia $x^{d_1} = 1$ are cel puţin $d_1 + 1$ soluţii în G, contradicţie cu alegerea lui d. Fie $x_1, \ldots, x_{d+1} \in G$ soluţii ale ecuaţiei $x^d = 1$ şi fie $y_i = x_i^p$, $i = 1, \ldots, d+1$. Avem că $y_i^{d_1} = 1$, $i = 1, \ldots, d+1$. Dacă ecuaţia $x^{d_1} = 1$ ar avea cel mult d_1 soluţii, atunci ar exista cel puţin $p+1$ indici în mulţimea $\{1, \ldots, d+1\}$, să zicem $j_1, \ldots, j_{p+1}$, astfel încât $y_{j_1}^p = \cdots = y_{j_{p+1}}^p$. Rezultă că $(y_{j_1} y_{j_k}^{-1})^p = 1$, $k = 1, \ldots, p+1$, deci ecuaţia $x^p = 1$ are cel puţin $p+1$ soluţii în G, contradicţie.

Afirmaţia nu mai este adevărată dacă grupul G nu este comutativ. Dacă

$G = Q$ (grupul cuaternionilor), atunci ecuaţia $x^2 = 1$ are doar două soluţii în G.

32. Fie G un subgrup finit al grupului multiplicativ $(K^*, \cdot)$ şi fie d un divizor natural al lui $n = |G|$. Atunci ecuaţia $x^d = 1$ are cel mult d soluţii în G, deoarece polinomul $X^d - 1 \in K[X]$ are în corpul comutativ K cel mult tot atâtea rădăcini cât gradul său. Aplicând acum problema 31(ii), rezultă că G este grup ciclic. În particular, dacă K este corp finit, atunci $(K^*, \cdot)$ este grup ciclic.

Observaţie. Proprietatea din problemă rămâne adevărată şi în cazul mai general în care se consideră un inel comutativ integru în locul corpului K.

33. (i) Scriem $m = p_1^{a_1} \cdots p_r^{a_r}$ şi $n = p_1^{b_1} \cdots p_r^{b_r}$ cu p_i numere prime şi $a_i, b_i \in \mathbb{N}$. Atunci $[m, n] = p_1^{c_1} \cdots p_r^{c_r}$, $c_i = \max(a_i, b_i)$, $i = 1 \ldots, r$. Arătăm că există elementele $z_i \in G$ astfel încât $\text{ord}(z_i) = p_i^{c_i}$, $i = 1, \ldots, r$. De aici va rezulta că $\text{ord}(z_1 \cdots z_r) = p_1^{c_1} \cdots p_r^{c_r} = [m, n]$ (vezi problema 19(i)). Dacă $c_i = a_i$, alegem $z_i = x^{p_1^{a_1} \cdots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \cdots p_r^{a_r}}$, iar dacă $c_i = b_i$, alegem $z_i = x^{p_1^{b_1} \cdots p_{i-1}^{b_{i-1}} p_{i+1}^{b_{i+1}} \cdots p_r^{b_r}}$.
(ii) Fie $x \in G$, $x \neq e$ şi $x_0 \in G$ astfel încât $\text{ord}(x_0) = m_0$. Dacă $\text{ord}(x)$ nu divide m_0, atunci există $y \in G$ astfel încât $\text{ord}(y) = [m_0, \text{ord}(x)] > m_0$, contradicţie.
(iii) Din teorema lui Cauchy obţinem că există $x_i \in G$ cu $\text{ord}(x_i) = p_i$ pentru orice $i = 1, \ldots, n$. Aplicând (i) deducem că există în grupul G un element de ordin $p_1 \cdots p_n$, deci G este grup ciclic.
(iv) Fie $m_0 = \max\{\text{ord}(x) \mid x \in G\}$, unde G este un subgrup finit al grupului multiplicativ $(K^*, \cdot)$. Atunci $m_0 | n = |G|$. Fie $f = X^{m_0} - 1 \in K[X]$. Din (ii) rezultă că G este conţinut în mulţimea rădăcinilor lui f, deci $n \leq m_0$. Dar ştiam deja că $m_0 \leq n$, deci $m_0 = n$. Asta înseamnă în particular că grupul G conţine un element de ordin n, deci este grup ciclic.

34. (i) $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ este subgrup al lui $(\mathbb{C}^*, \cdot)$, deoarece pentru $x, y \in U_n$ avem $(xy^{-1})^n = x^n y^{-n} = 1$, deci $xy^{-1} \in U_n$. Dacă H este un subgrup cu n elemente al lui $(\mathbb{C}^*, \cdot)$, din teorema lui Lagrange rezultă că $z^n = 1$ pentru orice $z \in H$, deci $H \subseteq U_n$. Cum H şi U_n au acelaşi număr de elemente rezultă că $H = U_n$.
(ii) În grupul $(\mathbb{C}^*, \cdot)$ considerăm subgrupurile U_{p^n} cu $n \in \mathbb{N}$. Avem $U_{p^n} \subseteq U_{p^{n+1}}$, deoarece $z^{p^n} = 1$ implică $z^{p^{n+1}} = 1$ şi incluziunea este strictă, cele

două subgrupuri având cardinale diferite. Din problema 26 rezultă acum că C_{p^∞} nu este finit generat.
(iii) Fie H un subgrup al lui C_{p^∞}. Atunci orice element al lui H are ordinul de forma p^m, $m \in \mathbb{N}$. Avem două posibilităţi: mulţimea $\{m \in \mathbb{N} \mid \text{există } x \in H \text{ cu } \text{ord}(x) = p^m\}$ este mărginită sau nemărginită.
Dacă mulţimea $\{m \in \mathbb{N} \mid \text{există } x \in H \text{ cu } \text{ord}(x) = p^m\}$ este nemărginită, atunci vom avea $H = C_{p^\infty}$. Fie $g \in C_{p^\infty}$, $\text{ord}(g) = p^n$. $< g >$ este un subgrup cu p^n elemente al lui C_{p^∞} şi din (i) rezultă că $< g > = U_{p^n}$. Pe de altă parte, există $m \in \mathbb{N}$, $m > n$ şi $x \in H$ cu $\text{ord}(x) = p^m$. Atunci, ca mai sus, $< x > = U_{p^m} \supseteq U_{p^n}$, deci $g \in < x > \subseteq H$.
Dacă mulţimea $\{m \in \mathbb{N} \mid \text{există } x \in H \text{ cu } \text{ord}(x) = p^m\}$ este mărginită, atunci fie n cel mai mare element al său şi $x \in H$ cu $\text{ord}(x) = p^n$. Vom arăta că în acest caz $H = U_{p^n}$. Într-adevăr, dacă $g \in H$, atunci $\text{ord}(g) = p^m$ cu $m \leq n$ şi $< g > = U_{p^m} \subseteq U_{p^n}$, deci $H \subseteq U_{p^n}$. Pe de altă parte, $H \supseteq < x > = U_{p^n}$ şi de aici rezultă egalitatea dorită.
(iv) G nu este grup ciclic, altfel G ar fi izomorf cu $\mathbb{Z}$ şi nu are proprietatea din enunţ. Mai mult, rezultă că $\text{ord}(x) < \infty$ pentru orice $x \in G$, deoarece $< x >$ este un subgrup ciclic al lui G şi din aceleaşi motive ca mai sus nu poate fi infinit.
Arătăm acum că există un unic număr prim $p > 0$ cu proprietatea că $\text{ord}(x)$ este o putere a lui p pentru orice $x \in G$. Să presupunem că există $x_1, x_2 \in G$ cu $\text{ord}(x_1) = p_1^{a_1}$ şi $\text{ord}(x_2) = p_2^{a_2}$, unde p_1, p_2 sunt numere prime distincte. (Să observăm că întotdeauna există elemente în grupul G care au ordinul o putere a unui număr prim: dacă $\text{ord}(x) = q_1^{b_1} \cdots q_r^{b_r}$, q_i numere prime distincte, atunci $\text{ord}(x^{q_2^{b_2} \cdots q_r^{b_r}}) = q_1^{b_1}$.) Alegem a_1, a_2 maxime. (Dacă ar exista un număr prim p astfel încât mulţimea $\{k \in \mathbb{N} \mid \text{există } x \in G \text{ cu } \text{ord}(x) = p^k\}$ să fie infinită, atunci $C_{p^\infty} \subseteq G$, deci C_{p^∞} este un subgrup infinit al lui G, deci $C_{p^\infty} = G$.) Fie $x_3 \in G - < x_1, x_2 >$ (există un astfel de element, deoarece $< x_1, x_2 >$ este subgrup finit al lui G). Dacă $\text{ord}(x_3) = p_1^{k_1} p_2^{k_2}$, atunci $k_1 \leq a_1$ şi $k_2 \leq a_2$ (deoarece $\text{ord}(x_3^{p_2^{k_2}}) = p_1^{k_1}$ şi $\text{ord}(x_3^{p_1^{k_1}}) = p_2^{k_2}$). Rezultă că $x_3^{p_2^{k_2}} \in < x_1 > = U_{p_1^{a_1}}$ şi $x_3^{p_1^{k_1}} \in < x_2 > = U_{p_2^{a_2}}$, deci $x_3^{p_2^{k_2}} \in < x_1, x_2 >$ şi $x_3^{p_1^{k_1}} \in < x_1, x_2 >$. În particular, obţinem $x_3 \in < x_1, x_2 >$ (deoarece $(p_1^{k_1}, p_2^{k_2}) = 1$), contradicţie. Rezultă că există un număr prim p_3, diferit de p_1, p_2, astfel încât $p_3 | \text{ord}(x_3)$. Deci există în G elemente de ordin o putere a lui p_3. Notăm tot cu x_3 un element de ordin $p_3^{a_3}$ cu a_3 maxim. În acest fel se obţine un şir (x_n) de elemente din G, un şir de numere prime distincte (p_n)

şi un şir de numere naturale nenule (a_n) cu proprietatea că $\text{ord}(x_n) = p_n^{a_n}$ pentru orice $n \geq 1$. În mod clar $< x_2, \ldots, x_n, \ldots >$ este subgrup infinit al lui G şi diferit de G (infinit, deoarece $\text{ord}(x_2 \cdots x_n) = p_2^{a_2} \cdots p_n^{a_n}$ pentru orice $n \geq 2$ şi diferit de G, deoarece $x_1 \notin < x_2, \ldots, x_n, \ldots >$), contradicţie.
Deci există un unic număr prim p cu proprietatea că $\text{ord}(x)$ este o putere a lui p pentru orice $x \in G$. Dacă mulţimea $\{k \in \mathbb{N} \mid \text{există } x \in G \text{ cu } \text{ord}(x) = p^k\}$ ar fi finită, fie k_0 maximul său. Rezultă că $G \subseteq U_{p^{k_0}}$, fals. Deci mulţimea este infinită şi în acest caz obţinem că $G = C_{p^\infty}$.
(v) Fie $f : C_{p^\infty} \to C_{p^\infty}$ definită prin $f(z) = z^{p^n}$. Atunci f este morfism de grupuri, $\text{Ker}(f) = U_{p^n}$ şi f este surjectiv, deoarece dacă $z = \cos(2k\pi/p^j) + i\sin(2k\pi/p^j)$, atunci $z = f(y)$, unde $y = \cos(2k\pi/p^{n+j}) + i\sin(2k\pi/p^{n+j})$. Din teorema fundamentală de izomorfism obţinem acum izomorfismul cerut.

35. (i) Evident pentru orice $a \in \mathbb{Q}$ şi $n \in \mathbb{N}^*$ ecuaţia $nx = a$ are soluţie în $\mathbb{Q}$, deci $(\mathbb{Q}, +)$ este grup divizibil.

Fie $a \in C_{p^\infty}$, $\text{ord}(a) = p^h$ şi $n = p^r m \in \mathbb{N}^*$ cu $(m, p) = 1$. Arătăm că ecuaţia $x^n = a$ are soluţie în C_{p^∞}. Deoarece $(m, p^h) = 1$, există $u, v \in \mathbb{Z}$ cu $um + vp^h = 1$. Atunci $a = a^{um+vp^h} = (a^u)^m (a^{p^h})^v = (a^u)^m$, deci există $b \in C_{p^\infty}$, $b = a^u$, cu $b^m = a$. Fie $b = \cos(2k\pi/p^s) + i\sin(2k\pi/p^s)$. Atunci $x = \cos(2k\pi/p^{s+r}) + i\sin(2k\pi/p^{s+r})$ verifică $x^{p^r} = b$, deci $x^n = b^m = a$. Aşadar $(C_{p^\infty}, \cdot)$ este grup divizibil.
(ii) Fie G un grup divizibil netrivial. Dacă prin absurd G ar fi grup finit, fie $|G| = n$ şi $a \in G - \{e\}$. Atunci ecuaţia $x^n = a$ nu are soluţie în G, contradicţie.
(iii) Fie H un subgrup normal al grupului divizibil G. Fie $\hat{a} \in G/H$ şi $n \in \mathbb{N}^*$. Cum G este divizibil există $x \in G$ cu $x^n = a$. Atunci $\hat{x}^n = \hat{a}$, deci şi grupul G/H este divizibil.

Un subgrup al unui grup divizibil nu este în general divizibil. De exemplu $(\mathbb{Q}, +)$ este divizibil, dar $(\mathbb{Z}, +)$ nu este divizibil, ecuaţia $2x = 1$ neavând soluţie în $\mathbb{Z}$.
(iv) Pe $\mathbb{R}_+^* \times \mathbb{R}$ definim operaţia $(a_1, x_1) * (a_2, x_2) = (a_1 a_2, a_1 x_2 + x_1)$. Se verifică uşor că această operaţie defineşte o structură de grup. Acest grup nu este abelian, deoarece $(1,1)(2,1) = (2,2)$ şi $(2,1)(1,1) = (2,3)$. Arătăm că acest grup este divizibil. Fie $(a, b) \in \mathbb{R}_+^* \times \mathbb{R}$ şi $n \in \mathbb{N}^*$. Căutăm (c, x) cu $(c, x)^n = (a, b)$. Dar $(c, x)^n = (c^n, (c^{n-1} + \cdots + c + 1)x)$. Deci căutăm c şi x cu $c^n = a$ şi $(c^{n-1} + \cdots + c + 1)x = b$. Atunci luăm $c = \sqrt[n]{a}$ şi $x = b/(c^{n-1} + \cdots + c + 1)$ şi acestea verifică relaţiile cerute.

(v) Fie G grup divizibil şi H un subgrup al său de indice finit. Vom arăta că $H = G$. Să notăm $n = [G : H]$. Fie $x \in G$. Atunci clasele (la stânga modulo H) $H, xH, \ldots, x^nH$ nu pot fi distincte, deci există $i, j \in \{0, 1, \ldots, n\}$, $j > i$, cu $x^iH = x^jH$, adică $x^{j-i} \in H$. În particular, $x^{n!} \in H$ pentru orice $x \in G$. Fie acum $y \in G$. Deoarece grupul G este divizibil, va exista un $x \in G$ cu proprietatea că $y = x^{n!}$, deci $y \in H$. De aici rezultă că $H = G$.

Observaţie. O altă soluţie, mai puţin elementară, se poate obţine folosind problema 75. Deoarece indicele lui H este finit, atunci şi indicele lui H_G, interiorul normal al lui H în G, este finit (şi ordinul său divide pe $n!$). Cum H_G este subgrup normal, are sens să vorbim despre grupul factor G/H_G. Acesta este la rândul său un grup divizibil (ca grup factor al unui grup divizibil) şi va fi cu necesitate trivial, deci $H_G = G$. De aici rezultă că $H = G$.

(vi) Fie $(G, +)$ un grup divizibil şi să presupunem că există $H_1, \ldots, H_n$ subgrupuri proprii ale lui G cu proprietatea că $G = \bigcup_{i=1}^{n} H_i$ şi $H_i \nsubseteq \bigcup_{j \neq i} H_j$ pentru orice $i = 1, \ldots, n$. Alegem acum două elemente $x_1 \in H_1 - \bigcup_{i \neq 1} H_i$ şi $x_2 \in H_2 - \bigcup_{i \neq 2} H_i$. Să observăm că dacă $x_1 = ky_1$, cu $k \in \mathbb{N}^*$ şi $y_1 \in G$, atunci $y_1 \in H_1 - \bigcup_{i \neq 1} H_i$. În mod evident $y_1 \notin \bigcup_{i \neq 1} H_i$ şi atunci, deoarece $G = \bigcup_{i=1}^{n} H_i$, rămâne ca singură posibilitate $y_1 \in H_1$.

Fie acum $m = (n-1)!$ şi fie $y_1 \in G$ cu proprietatea că $x_1 = my_1$. Considerăm elementele $a_j = jy_1 + x_2$, $j = 1, \ldots, n-1$. Dacă $a_j \in H_1$, atunci $x_2 \in H_2$ (deoarece $jy_1 \in H_1$), fals. Dacă $a_j \in H_2$, atunci $jy_1 \in H_2$, deci şi $(m/j)jy_1 = my_1 = x_1 \in H_2$, fals. În concluzie, $a_j \in \bigcup_{i=3}^{n} H_i$ pentru orice $j = 1, \ldots, n-1$. Deci există $k \in \{3, \ldots, n\}$, $i, j \in \{1, \ldots, n-1\}$, $j > i$, cu proprietatea că $a_i, a_j \in H_k$. Rezultă că $a_j - a_i = (j-i)y_1 \in H_k$, deci şi $\frac{m}{j-i}(j-i)y_1 = my_1 = x_1 \in H_k$, contradicţie.

36 Fie $f : \mathbb{Q} \to G$ un morfism de grupuri. $H = \mathrm{Ker}(f)$ este subgrup al lui $(\mathbb{Q}, +)$ şi există $\overline{f} : \mathbb{Q}/H \to G$ morfism injectiv, deci $\mathbb{Q}/H$ este grup finit. Dar $\mathbb{Q}/H$ este grup divizibil (deoarece este grup factor al unui grup divizibil), deci $\mathbb{Q}/H = 0$ (dacă $\mathbb{Q}/H \neq 0$, atunci ar fi grup infinit după cum rezultă din problema 35(ii)). În concluzie $H = \mathbb{Q}$, adică f este morfismul nul şi astfel obţinem că $\mathrm{Hom}_{gr}(\mathbb{Q}, G) = \{0\}$.

37. (i) Considerăm mulţimea

$$\mathcal{F} = \{Y \mid Y \text{ este subgrup propriu în } G, X \subseteq Y\}$$

Aceasta este o mulţime nevidă, deoarece $X \in \mathcal{F}$, şi este ordonată în raport cu incluziunea. Arătăm că este inductiv ordonată. Pentru aceasta fie $(Y_i)_{i\in I}$ o submulţime total ordonată a lui $\mathcal{F}$ şi $Y = \bigcup_{i\in I} Y_i$. Atunci Y este subgrup al lui G. Într-adevăr, dacă $g, h \in Y$, atunci există $i, j \in I$ cu $g \in Y_i$ şi $h \in Y_j$. Avem $Y_i \subseteq Y_j$ sau $Y_j \subseteq Y_i$. Fără a micşora generalitatea presupunem $Y_i \subseteq Y_j$. Atunci $g, h \in Y_j$ şi cum acesta este subgrup obţinem $gh^{-1} \in Y_j$. Atunci $gh^{-1} \in Y$, de unde rezultă că Y este subgrup. Mai mult, arătăm că Y este subgrup propriu, deci $Y \in \mathcal{F}$. Dacă am presupune că $Y = G$, considerând un sistem de generatori $g_1, \ldots, g_p$ pentru G, rezultă că aceştia se găsesc în Y, deci există $i_1, \ldots, i_p \in I$ cu $g_j \in Y_{i_j}$. Din faptul că mulţimea aleasă este total ordonată rezultă că putem găsi un j cu $g_1, \ldots, g_p \in Y_{i_j}$. Atunci $Y_{i_j} = G$, contradicţie. Evident Y este un majorant pentru familia $(Y_i)_{i\in I}$ şi atunci $\mathcal{F}$ este inductiv ordonată. Din Lema lui Zorn rezultă că $\mathcal{F}$ are un element maximal H şi acesta este chiar un subgrup maximal în G care conţine pe X.
(ii) Fie G un grup abelian divizibil netrivial. Dacă H este un subgrup maximal al lui G, atunci grupul factor G/H este divizibil şi netrivial, deci este infinit. Dar un grup infinit are o infinitate de subgrupuri, în particular are un subgrup propriu netrivial, fie acesta K/H. Atunci K este un subgrup al lui G şi $H \subseteq K \subseteq G$. Dar $K \neq H$ şi $K \neq G$, deci H nu este maximal, contradicţie. Deci G nu are subgrupuri maximale.

38. Presupunem că G are un singur subgrup maximal, fie acesta H. Fie $x \in G - H$. Dacă $< x > \neq G$, din problema 37(i) rezultă că există un subgrup maximal al lui G care îl include pe $< x >$. Dar singurul subgrup maximal este H şi acesta nu îl include pe $< x >$, deoarece nu conţine elementul x. Rezultă că $< x > = G$, deci G este grup ciclic. Putem acum să considerăm că $G = \mathbb{Z}_m$, $m \in \mathbb{N}$, $m \geq 2$. Dacă p este un număr prim care divide pe m, atunci $< \hat{p} >$ este subgrup maximal al lui $\mathbb{Z}_m$ (vezi, de exemplu, problema 31(i)). Cum trebuie ca să avem un singur subgrup maximal, rezultă că există un singur divizor prim al lui m şi deci $m = p^n$ cu $n \geq 2$.
Reciproc, dacă $G = \mathbb{Z}_{p^n}$, rezultă din structura subgrupurilor acestui grup că $< \hat{p} >$ este unicul subgrup maximal, deci şi G are un unic subgrup maximal.

39. (i) Verificarea este imediată.
(ii) Observăm că $\varphi_g\varphi_h = \varphi_{gh}$ şi $\varphi_g^{-1} = \varphi_{g^{-1}}$. De aici rezultă că $\mathrm{Inn}(G)$ este subgrup al lui $\mathrm{Aut}(G)$. Dacă $f \in \mathrm{Aut}(G)$, atunci $f\varphi_g f^{-1} = \varphi_{f(g)} \in \mathrm{Inn}(G)$. Deci $\mathrm{Inn}(G)$ este subgrup normal al lui $\mathrm{Aut}(G)$.
(iii) Din prima relaţie de la (ii) rezultă că aplicaţia $F : G \to \mathrm{Inn}(G)$ definită prin $F(g) = \varphi_g$ este morfism de grupuri. Evident F este morfism surjectiv şi $g \in \mathrm{Ker}(F) \Leftrightarrow \varphi_g = \mathrm{Id}_G \Leftrightarrow g \in Z(G)$. Din teorema fundamentală de izomorfism rezultă izomorfismul dorit.

40. Scriem $G/Z(G) = < \hat{g} >$. Fie $x, y \in G$. Atunci $\hat{x}, \hat{y} \in G/Z(G)$ şi deci $\hat{x} = \hat{g}^m$, $\hat{y} = \hat{g}^n$, cu $m, n \in \mathbb{Z}$. Rezultă că $x = g^m x_1$, $y = g^n y_1$, cu $x_1, y_1 \in Z(G)$. Atunci $xy = g^m x_1 g^n y_1 = g^{m+n} x_1 y_1 = yx$.

41. Fie X un grup ciclic de ordin impar. Arătăm că X nu este izomorf cu $\mathrm{Aut}(G)$ pentru nici un grup G. Presupunem contrariul. Dacă G ar fi grup abelian, atunci $\mathrm{Aut}(G)$ ar conţine un element de ordin 2, şi anume $f : G \to G$, $f(x) = x^{-1}$. Dar X nu are elemente de ordin 2, contradicţie. Presupunem acum că G este neabelian şi că $X \simeq \mathrm{Aut}(G)$. Atunci $\mathrm{Inn}(G)$ este subgrup al unui grup ciclic, deci este ciclic şi din problema 39(iii) rezultă că $G/Z(G)$ este grup ciclic. Din problema 40 rezultă atunci că G este grup abelian, contradicţie. Aşadar X nu este izomorf cu $\mathrm{Aut}(G)$ pentru nici un grup G.

42. (i) Soluţia problemei 4 descrie endomorfismele grupului $(\mathbb{Z}, +)$. Este clar că dintre acestea sunt izomorfisme doar identitatea şi aplicaţia $g : \mathbb{Z} \to \mathbb{Z}$ definită prin $g(x) = -x$. Aşadar $\mathrm{Aut}(\mathbb{Z})$ este un grup cu două elemente, deci este izomorf cu $\mathbb{Z}_2$.
(ii) Tot în soluţia problemei 4 găsim descrise endomorfismele grupului $(\mathbb{Q}, +)$. Se observă că acestea sunt unic determinate de valoarea lor în 1. Aşadar putem defini o aplicaţie $F : \mathrm{Aut}(\mathbb{Q}) \to (\mathbb{Q}^*, \cdot)$ prin $F(f) = f(1)$. Se verifică uşor că F este izomorfism de grupuri.
(iii) Folosim descrierea endomorfismelor lui $\mathbb{Z}_n$ din soluţia problemei 4. Morfismul $f_{\hat{a}} : \mathbb{Z}_n \to \mathbb{Z}_n$ definit prin $f_{\hat{a}}(\hat{x}) = \hat{a}\hat{x}$ este automorfism dacă şi numai dacă este surjectiv (deoarece $\mathbb{Z}_n$ este mulţime finită). Aceasta este echivalent cu faptul că există $\hat{x} \in \mathbb{Z}_n$ cu $f(\hat{x}) = \hat{1} \Leftrightarrow \hat{a}\hat{x} = \hat{1} \Leftrightarrow \hat{a} \in U(\mathbb{Z}_n)$, unde cu $U(\mathbb{Z}_n)$ notăm grupul elementelor simetrizabile din monoidul $(\mathbb{Z}_n, \cdot)$. Este imediat atunci că aplicaţia $F : U(\mathbb{Z}_n) \to \mathrm{Aut}(\mathbb{Z}_n)$, $F(\hat{a}) = f_{\hat{a}}$ este izomorfism de grupuri.

(iv) Fie $G = \{e, x_1, x_2, x_3\}$ grupul lui Klein (care este izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_2$). Observăm că pentru orice $\sigma \in S_3$, aplicaţia $f_\sigma : G \to G$ definită prin $f_\sigma(e) = e$ şi $f_\sigma(x_i) = x_{\sigma(i)}$ este automorfism al lui G. Cum un automorfism duce pe e în e şi este bijectiv, rezultă că $\mathrm{Aut}(G) = \{f_\sigma \mid \sigma \in S_3\}$. Mai departe este clar că aplicaţia $F : S_3 \to \mathrm{Aut}(G)$, $F(\sigma) = f_\sigma$, este izomorfism de grupuri.

43. Ştim că grupul S_3 este generat de $\sigma = (123)$ şi $\tau = (12)$. Dacă $f \in \mathrm{Aut}(S_3)$, atunci $f(\sigma)$ este element de ordin 3, iar $f(\tau)$ este element de ordin 2. Cum S_3 are două elemente de ordin 3 şi trei elemente de ordin 2, rezultă că există cel mult şase automorfisme (un automorfism al lui S_3 este complet determinat de $f(\sigma)$ şi $f(\tau)$). Pe de altă parte, $\mathrm{Inn}(S_3) \simeq S_3/Z(S_3) \simeq S_3$ (centrul lui S_3 este trivial, vezi problema 56), deci există şase automorfisme interioare ale lui S_3 şi deci $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3) \simeq S_3$.

Pentru descrierea automorfismele grupului diedral D_4 să reamintim că $D_4 = < r, s >$, cu $\mathrm{ord}(r) = 4$, $\mathrm{ord}(s) = 2$ şi $sr = r^3 s$. De asemenea, D_4 are două elemente de ordin 4, r şi r^3, şi cinci elemente de ordin 2. Un automorfism h al lui D_4 duce pe r într-unul din cele două elemente de ordin 4, iar pe s într-unul din cele cinci elemente de ordin 2. Observăm că $h(s)$ nu poate fi r^2, în acest caz rezultând că $\mathrm{Im}(h) \subseteq < r >$, deci h nu ar fi surjectiv. Deci $h(s)$ poate lua doar patru valori. Se verifică uşor că orice h definit în acest mod (pe generatori) este într-adevăr un automorfism şi deci $|\mathrm{Aut}(D_4)| = 8$. Mai departe, dacă notăm cu h automorfismul pentru care $h(r) = r$ şi $h(s) = rs$, şi cu g automorfismul pentru care $g(r) = r^3$ şi $g(s) = s$, avem $\mathrm{ord}(h) = 4$, $\mathrm{ord}(g) = 2$ şi $gh = h^3 g$, de unde rezultă că $\mathrm{Aut}(D_4) = < g, h > \simeq D_4$.

44. (i) Grupul $\mathbb{Z} \times \mathbb{Z}$ nu este ciclic. Într-adevăr, dacă $\mathbb{Z} \times \mathbb{Z} = < (a, b) >$, atunci cum $(1, 0) \in \mathbb{Z} \times \mathbb{Z}$, există $n \in \mathbb{Z}$ cu $(1, 0) = (na, nb)$, deci $b = 0$, deoarece evident $n \neq 0$. Similar obţinem $a = 0$, deci $< (0, 0) > = \mathbb{Z} \times \mathbb{Z}$, contradicţie. Cum $\mathbb{Z}$ este grup ciclic, rezultă că cele două grupuri nu sunt izomorfe.
(ii) Grupul $\mathbb{Q} \times \mathbb{Q}$ are un subgrup care este finit generat şi nu este ciclic, şi anume $\mathbb{Z} \times \mathbb{Z}$. Acesta este generat de $(1, 0)$ şi $(0, 1)$ şi nu este ciclic după cum s-a arătat la (i). Conform problemei 22, în grupul $\mathbb{Q}$ orice subgrup finit generat este ciclic. Rezultă că $\mathbb{Q}$ şi $\mathbb{Q} \times \mathbb{Q}$ nu sunt izomorfe.
(iii) Aplicaţia $f : \mathbb{R} \times \mathbb{R} \to \mathbb{C}$, $f(a, b) = a + ib$, este un izomorfism de grupuri. Folosind acum rezultatul de la problema 5 care afirmă că $\mathbb{R}$ şi $\mathbb{C}$ sunt grupuri izomorfe, obţinem că $\mathbb{R}$ este izomorf cu $\mathbb{R} \times \mathbb{R}$.

45. (i) Fie $f : \mathbb{R} \to S^1$ definită prin $f(x) = \cos(2\pi x) + i \sin(2\pi x)$. Este imediat că f este morfism surjectiv de grupuri. Mai departe $\mathrm{Ker}(f) = \mathbb{Z}$ şi aplicând teorema fundamentală de izomorfism obţinem $\mathbb{R}/\mathbb{Z} \simeq S^1$.
(ii) Fie $g : \mathbb{Q} \to S^1$ definită prin $g(x) = \cos(2\pi x) + i \sin(2\pi x)$. Atunci g este morfism de grupuri, $\mathrm{Im}(g) = U_\infty$ şi $\mathrm{Ker}(g) = \mathbb{Z}$. Din nou aplicând teorema fundamentală de izomorfism obţinem $\mathbb{Q}/\mathbb{Z} \simeq U_\infty$.
(iii) Grupurile $(\mathbb{R}, +)$ şi $(\mathbb{R}/\mathbb{Q}, +)$ pot fi înzestrate cu structuri de $\mathbb{Q}$-spaţii vectoriale dacă definim înmulţirea cu scalari prin $q \cdot x = qx$, oricare ar fi $q \in \mathbb{Q}$ şi $x \in \mathbb{R}$, pentru primul grup şi $q \cdot (x + \mathbb{Q}) = qx + \mathbb{Q}$, oricare ar fi $q \in \mathbb{Q}$ şi $x \in \mathbb{R}$, pentru al doilea grup (se observă că definiţia nu depinde de reprezentantul x). Ca la problema 5, $\mathbb{Q}$-spaţiul vectorial $\mathbb{R}$ are o bază de cardinal $|\mathbb{R}|$. De asemenea, prin argumente standard, din faptul că $\mathbb{R}$ este nenumărabilă iar $\mathbb{Q}$ este numărabilă, rezultă că şi $\mathbb{R}/\mathbb{Q}$ are o bază de acelaşi cardinal. Atunci $\mathbb{R}$ şi $\mathbb{R}/\mathbb{Q}$ sunt $\mathbb{Q}$-spaţii vectoriale de aceeaşi dimensiune. Rezultă că ele sunt izomorfe şi în particular şi grupurile subiacente sunt izomorfe.
(iv) Din cele arătate la (i) avem un izomorfism de grupuri $F : \mathbb{R}/\mathbb{Z} \to S^1$ definit prin $F(x + \mathbb{Z}) = \cos(2\pi x) + i \sin(2\pi x)$. Mai mult, $\mathbb{Q}/\mathbb{Z}$ este subgrup (normal) al lui $\mathbb{R}/\mathbb{Z}$ şi $F(\mathbb{Q}/\mathbb{Z}) = U_\infty$. Obţinem atunci că $S^1/U_\infty = F(\mathbb{R}/\mathbb{Z})/F(\mathbb{Q}/\mathbb{Z}) \simeq (\mathbb{R}/\mathbb{Z})/(\mathbb{Q}/\mathbb{Z}) \simeq \mathbb{R}/\mathbb{Q} \simeq \mathbb{R}$.

46. Din (i) şi (iv) de la problema 45 rezultă că grupurile $\mathbb{R}$ şi S^1 sunt izomorfe fiecare cu un grup factor al celuilalt. Pe de altă parte aceste grupuri nu sunt izomorfe, deoarece există $z \in S^1$, $z \neq 1$, cu $z^2 = 1$ (şi anume $z = -1$), dar nu există $x \in \mathbb{R}$, $x \neq 0$, cu $2x = 0$ (adică S^1 este grup cu torsiune iar $\mathbb{R}$ este grup fără torsiune).

47. Aplicaţia $f : \mathbb{R}_+^* \times \mathbb{R} \to \mathbb{C}^*$ definită prin $f(r, a) = r(\cos a + i \sin a)$ este un morfism surjectiv de grupuri şi $\mathrm{Ker}(f) = \{1\} \times \mathbb{Z}$. Rezultă că $\mathbb{C}^* \simeq \mathbb{R}_+^* \times (\mathbb{R}/\mathbb{Z})$. Din problema 5 ştim că $(\mathbb{R}_+^*, \cdot) \simeq (\mathbb{R}, +)$, deci $\mathbb{C}^* \simeq \mathbb{R} \times (\mathbb{R}/\mathbb{Z})$. Pe de altă parte $\mathbb{Q}$-spaţiile vectoriale $\mathbb{R}$ şi $\mathbb{R} \times \mathbb{R}$ au aceeaşi dimensiune (care este egală cu $|\mathbb{R}|$) şi putem găsi astfel un izomorfism $f : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ cu $f(1) = (0, 1)$ (aceasta se poate face alegând în $\mathbb{R}$ o bază care îl conţine pe 1 şi în $\mathbb{R} \times \mathbb{R}$ o bază care îl conţine pe $(0, 1)$ şi construind pe f astfel încât aceste elemente ale bazelor să se corespundă). Atunci f este şi izomorfism de grupuri şi avem că $f(\mathbb{Z}) = \{0\} \times \mathbb{Z}$, de unde $\mathbb{R}/\mathbb{Z} \simeq (\mathbb{R} \times \mathbb{R})/(\{0\} \times \mathbb{Z}) \simeq \mathbb{R} \times (\mathbb{R}/\mathbb{Z})$. Dar $\mathbb{R}/\mathbb{Z} \simeq S^1$ din problema 44(i), şi de aici rezultă că $\mathbb{C}^* \simeq S^1$.

Deoarece $\mathbb{R} \times \mathbb{R} \simeq \mathbb{C}$ (prin $(a, b) \to a + ib$) şi imaginea lui $\mathbb{Z} \times \{0\}$ prin acest izomorfism este chiar $\mathbb{Z}$, obţinem $(\mathbb{R}/\mathbb{Z}) \times \mathbb{R} \simeq \mathbb{C}/\mathbb{Z}$ şi de aici rezultă că $\mathbb{C}/\mathbb{Z} \simeq \mathbb{R}/\mathbb{Z} \simeq S^1$.

48. Fie $G = D_4$, $K = \{e, s\}$, $H = \{e, r^2, s, r^2s\}$ (cu notaţiile din problema 8). Atunci $K \trianglelefteq H$ şi $H \trianglelefteq G$, deoarece în fiecare caz indicele subgrupului este 2. Însă $K \not\trianglelefteq G$, deoarece $rsr^{-1} = sr^2 \notin K$.

49. (i) Dacă $h \in H$ şi $k \in K$ avem $hk = k(k^{-1}hk) \in KH$, deci $HK \subseteq KH$. Similar $KH \subseteq HK$, deci are loc egalitatea. Acum faptul că HK este subgrup rezultă imediat.
(ii) Ştim că G/H este grup finit şi $HK/H \leq G/H$. Rezultă atunci că $(|HK/H|, |K|) = 1$. Dar $HK/H \simeq K/H \cap K$, deci $(|K/H \cap K|, |K|) = 1$. Acum $|K| = [K : H \cap K]|H \cap K|$ şi deci $[K : H \cap K] = 1$, de unde $K = H \cap K$, echivalent $K \subseteq H$.
(iii) Cum H este normal, rezultă că HK este subgrup în G. Mai departe, avem o bijecţie $f : (H/H \cap K)_s \to (HK/K)_s$ definită prin $f(x(H \cap K)) = xK$. Se verifică uşor că f este bine definită şi că este bijectivă. Atunci $[HK : K] = [H : H \cap K]$. Acum avem $[G : K] = [G : HK][HK : K] = [G : HK][H : H \cap K]$ şi înmulţind cu $|H \cap K|$ rezultă că $|H \cap K|[G : K] = [G : HK]|H|$. De aici avem că $|H|$ divide pe $|H \cap K|[G : K]$. Cum $(|H|, [G : K]) = 1$, rezultă că $|H|$ divide pe $|H \cap K|$. Dar $|H| \leq |H \cap K|$, deci avem egalitate $H = H \cap K$. De aici obţinem $H \subseteq K$.

50. (i) Luăm $G_1 = G_2 = \mathbb{Z}_2 \times \mathbb{Z}_4$, $H_1 = \mathbb{Z}_2 \times \{0\}$ şi $H_2 = \{0\} \times \hat{2}\mathbb{Z}_4$. Avem $G_1/H_1 \simeq \mathbb{Z}_4$ şi $G_2/H_2 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, deci cele două grupuri factor nu sunt izomorfe.
(ii) Fie $G_1 = G_2 = \mathbb{Z}_2 \times \mathbb{Z}_4$, $H_1 = \{0\} \times \mathbb{Z}_4$ şi $H_2 = \mathbb{Z}_2 \times \hat{2}\mathbb{Z}_4$ (observăm că H_1 şi H_2 nu sunt izomorfe, H_1 fiind ciclic, iar H_2 fiind izomorf cu grupul lui Klein). Avem $G_1/H_1 \simeq G_2/H_2 \simeq \mathbb{Z}_2$.
(iii) Fie $G = \mathbb{Z}_4$, $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$, $H_1 = \hat{2}\mathbb{Z}_4$, $H_2 = \{0\} \times \mathbb{Z}_2$. Atunci $G_1/H_1 \simeq G_2/H_2 \simeq \mathbb{Z}_2$.

51. Fie $G = \mathbb{Q}^{\mathbb{N}}$ şi $H = \mathbb{Z} \times \mathbb{Q}^{\mathbb{N}}$ cu structurile aditive de grupuri (prin $\mathbb{Q}^{\mathbb{N}}$ înţelegem aici mulţimea şirurilor de numere raţionale cu adunarea pe componente). Atunci G se poate scufunda în H, via morfismul care duce şirul $(a_0, a_1, \dots)$ în $(0, a_0, a_1, \dots)$, iar H se scufundă în G prin incluziune. Însă G şi H nu sunt izomorfe, deoarece G este grup divizibil iar H nu este divizibil.

52. (i) Fie $g \in I$ şi $A = g^{-1}I \cap I$. Avem $|A| = |I| + |g^{-1}I| - |g^{-1}I \cup I| > (3/4)|G| + (3/4)|G| - |G| > (1/2)|G|$. Dacă $a \in A$, atunci $a \in I$ şi $a = g^{-1}b$, cu $b \in I$. Avem atunci $ag = \alpha(a^{-1})\alpha(g^{-1}) = \alpha((ga)^{-1}) = \alpha(b^{-1}) = \alpha(b)^{-1} = b = ga$, deci $A \subseteq C(g)$ (centralizatorul elementului g). Cum $C(g)$ este subgrup al lui G şi are mai mult de $(1/2)|G|$ elemente, rezultă că $C(g) = G$, deci $g \in Z(G)$. Rezultă $I \subseteq Z(G)$ şi cum $|I| > (3/4)|G|$ obţinem $|Z(G)| > (3/4)|G|$, deci $Z(G) = G$.
(ii) Dacă pentru orice $g \in I$ avem $C(g) = G$, rezultă ca la (i) că $Z(G) = G$, deci G este grup abelian. Atunci I este chiar subgrup al lui G, deci $(3/4)|G|$ divide $|G|$, imposibil. Rezultă că există $g \in I$ astfel încât $C(g) \neq G$. Dar am văzut la (i) că $A \subseteq C(g)$. Cum $|A| \geq (1/2)|G|$ (cu aceleaşi calcule ca la (i), dar scriind peste tot "$\geq$" în loc de ">"), rezultă că $|C(g)| = (1/2)|G|$, deci $C(g)$ este subgrup de indice 2 în G.

53. Mai întâi arătăm că orice subgrup normal netrivial N al unui grup simetric $S(X)$ are proprietatea că $|N| \geq |X|$. Fie $\sigma \in N$, $\sigma \neq \mathrm{Id}_X$. Atunci există $x \in X$ astfel încât $\sigma(x) = x'$, $x' \neq x$. Fie $y \in X - \{x\}$. Îi asociem lui y permutarea $\sigma_y = \tau_{x',y}\sigma\tau_{x',y} \in N$, unde prin $\tau_{x',y}$ am notat transpoziţia definită de $\tau_{x',y}(x') = y$, $\tau_{x',y}(y) = x'$ şi $\tau_{x',y}(z) = z$ pentru orice $z \neq x', z \neq y$. Să observăm că această asociere este injectivă: dacă $\sigma_y = \sigma_{y'}$, atunci $\sigma_y(x) = \sigma_{y'}(x)$, deci $y = y'$. Mai mult, deoarece $\sigma \neq \mathrm{Id}_X$, avem că $\sigma_y \neq \mathrm{Id}_X$ pentru orice $y \in X$, $y \neq x$. În concluzie, $|X| \leq |N|$.
Revenim acum la rezolvarea problemei. Dacă una dintre mulţimile X, Y este finită, atunci şi cealaltă este finită şi în mod evident cele două mulţimi vor avea acelaşi număr de elemente.
Considerăm că X, Y sunt mulţimi infinite şi fie $f : S(X) \to S(Y)$ un izomorfism. Fie N mulţimea *permutărilor finite* ale lui X, adică permutările lui X care acţionează doar asupra unei submulţimi finite F a lui X lăsând neschimbate elementele din $X - F$. Este uşor de arătat că N este subgrup normal al lui $S(X)$. Mai mult, $|N| = |X|$, deoarece mulţimea părţilor finite ale unei mulţimi infinite are acelaşi cardinal cu mulţimea respectivă (vezi problema 31(c) din Capitolul 1). Deoarece $f(N)$ este subgrup normal netrivial al lui $S(Y)$, avem că $|N| = |f(N)| \geq |Y|$, deci $|X| \geq |Y|$. Analog se arată că $|Y| \geq |X|$ şi din Teorema Cantor-Schröder-Bernstein (vezi problema 26 din Capitolul 1) rezultă că $|X| = |Y|$.

54. (i) Verificare imediată.
(ii) Dacă $n = 2$, atunci S_2 este grup abelian şi deci orice subgrup al său este normal. Dacă $n \geq 3$, cum $(12) \in H$ şi $(1n)(12)(1n) = (2n) \notin H$, rezultă că H nu este subgrup normal.
(iii) Aplicaţia $f : H \to S_{n-1}$ definită prin $f(\sigma)(i) = \sigma(i)$ pentru orice $i \in \{1, \ldots, n-1\}$ este în mod evident un izomorfism de grupuri.
(iv) Se observă că pentru $\sigma, \tau \in S_n$, $\sigma \equiv \tau \pmod{H}$ dacă şi numai dacă $\sigma(n) = \tau(n)$. Fie $\sigma_1, \ldots, \sigma_n \in S_n$ cu proprietatea că $\sigma_i(n) = i$ pentru orice $i \in \{1, \ldots, n\}$. Mulţimea $\{\sigma_1, \ldots, \sigma_n\}$ este un sistem de reprezentanţi pentru clasele la stânga modulo H. Cum fiecare σ_i se poate alege în $(n-1)!$ moduri, obţinem $[(n-1)!]^n$ sisteme de reprezentanţi.

55. Fie $\sigma \in Z(S_n)$, $n \geq 3$. Presupunem prin absurd că $\sigma \neq e$, deci există $i \neq j$ cu $\sigma(i) = j$. Dacă $\sigma(j) = i$, fie $k \neq i, j$ şi $\tau = (ijk)$. Atunci $\sigma\tau(i) = i$ şi $\tau\sigma(i) = k$, deci $\sigma\tau \neq \tau\sigma$, contradicţie. Dacă $\sigma(j) = k \neq i$, atunci avem şi $k \neq j$. Fie acum $\tau = (ij)$. Avem $\sigma\tau(i) = k$ şi $\tau\sigma(i) = i$, deci $\sigma\tau \neq \tau\sigma$, contradicţie. Rezultă că $Z(S_n) = \{e\}$.

Fie acum $\sigma \in Z(A_n)$ şi din nou presupunem că $\sigma \neq e$, deci există $i \neq j$ cu $\sigma(i) = j$. Dacă $\sigma(j) = i$ luăm $\tau = (ijk) \in A_n$ şi avem ca la prima parte $\sigma\tau \neq \tau\sigma$. Dacă $\sigma(j) = k \neq i$, atunci fie $l \neq i, j, k$ (este posibil să alegem un astfel de element deoarece $n \geq 4$) şi $\tau = (ij)(kl) \in A_n$. Atunci $\sigma\tau(i) = k$ şi $\tau\sigma(i) = i$, deci $\sigma\tau \neq \tau\sigma$ şi din nou obţinem o contradicţie. Aşadar $Z(A_n) = \{e\}$.

56. Se ştie că orice grup finit se scufundă într-un S_n (teorema lui Cayley). Rezultă că este suficient să arătăm că pentru orice $n \in \mathbb{N}^*$ grupul S_n se scufundă într-un grup altern. Definim $f : S_n \to A_{n+2}$ astfel: dacă $\sigma \in S_n$ este permutare pară, atunci $f(\sigma)(i) = \sigma(i)$ pentru $1 \leq i \leq n$ şi $f(\sigma)(i) = i$ pentru $i \in \{n+1, n+2\}$. Dacă σ este permutare impară, definim $f(\sigma)(i) = \sigma(i)$ pentru $1 \leq i \leq n$, $f(\sigma)(n+1) = n+2$ şi $f(\sigma)(n+2) = n+1$. Este imediat că această aplicaţie este corect definită (adică are imaginea în A_{n+2}) şi este morfism injectiv de grupuri.

Observaţie. Se poate arăta că S_n nu se scufundă în A_{n+1}.

57. Scriem $k = dk_1$ şi $s = ds_1$ cu $(k_1, s_1) = 1$. Rezultă că $\tau^k = \tau^{dk_1} = (\tau^d)^{k_1}$. Să determinăm acum pe τ^d. Avem $\tau^d(i_1) = i_{d+1}, \tau^d(i_{d+1}) = i_{2d+1}, \ldots, \tau^d(i_{(s_1-1)d+1}) = i_{s+1} = i_1$. Rezultă că $\tau^d = \tau_1 \cdots \tau_d$, unde $\tau_j = (i_j, i_{d+j}, \ldots, i_{(s_1-1)d+j})$, $1 \leq j \leq d$, sunt cicli disjuncţi de lungime $s_1 =$

s/d. Obţinem că $\tau^k = \tau_1^{k_1} \cdots \tau_d^{k_1}$ şi cum $(k_1, s_1) = 1$ rămâne să arătăm că $\tau_1^{k_1}, \ldots, \tau_d^{k_1}$ sunt cicli disjuncţi de lungime s_1 şi cu aceeaşi orbită ca $\tau_1, \ldots, \tau_d$. Problema s-a redus astfel la cazul $d = 1$, adică $(k, s) = 1$.
Dacă $\tau^k = \pi_1 \cdots \pi_r$, descompunere în produs de cicli disjuncţi (cu $r \geq 2$), atunci să presupunem că i_1 aparţine orbitei ciclului π_1. Rezultă că $\pi_1^m(i_1) = i_1$, unde m este lungimea ciclului π_1. De aici obţinem $\tau^{km}(i_1) = i_1 \Rightarrow km \equiv 0 \pmod{s} \Rightarrow s|km \Rightarrow s|m$, deoarece $(s, k) = 1$, deci $m \geq s$, contradicţie. În concluzie $r = 1$.

58. Fie $n_i = \text{ord}(\pi_i)$ şi $m = [n_1, \ldots, n_r]$. Cum ciclii disjuncţi comută, avem $(\pi_1 \cdots \pi_r)^m = \pi_1^m \cdots \pi_r^m = e$, deoarece $\text{ord}(\pi_i)|m$ pentru orice $i = 1, \ldots, r$. Rezultă că $\text{ord}(\sigma)|m$.
Dacă $k \in \mathbb{N}^*$ şi $\sigma^k = e$, atunci $\pi_1^k \cdots \pi_r^k = e$. Din problema 57 avem că $\pi_i^k = \tau_{i1} \cdots \tau_{is_i}$, produs de cicli disjuncţi ale căror orbite sunt submulţimi ale orbitei ciclului π_i, $i = 1, \ldots, r$. Rezultă că τ_{ij}, $1 \leq j \leq s_i$, $1 \leq i \leq r$, sunt cicli disjuncţi al căror produs este permutarea identică, deci $\tau_{ij} = e$ pentru orice $1 \leq j \leq s_i$, $1 \leq i \leq r$. Rezultă că $\pi_i^k = e$ pentru orice $i \in \{1, \ldots, r\}$, de unde obţinem că $n_i|k$ pentru orice $i \in \{1, \ldots, r\}$, deci $m|k$. Aşadar $\text{ord}(\sigma) = m$.

59. Presupunem că $n \geq 6$ şi fie $\tau = (12)(3456) \in A_n$. Arătăm că nu există $\sigma \in S_n$ astfel încât $\sigma^2 = \tau$. Scriem $\sigma = \pi_1 \cdots \pi_r \pi$ descompunere în produs de cicli disjuncţi, unde primii r factori sunt cicli disjuncţi de lungime ≥ 3, iar π este produsul ciclilor de lungime 2. Atunci $\sigma^2 = \pi_1^2 \cdots \pi_r^2$ şi rezultă că nu putem avea cicli de lungime impară în scrierea lui σ, deoarece pătratul unui astfel de ciclu este tot ciclu de lungime impară. De asemenea, pătratul unui ciclu de lungime pară este produsul a doi cicli disjuncţi de lungime egală (vezi problema 57), iar τ conţine un singur ciclu de lungime 2, contradicţie. Dacă $n \leq 5$, se verifică uşor prin calcule că $A_n = \{\sigma^2 \mid \sigma \in S_n\}$.

60. Fie $\sigma = \pi_1 \cdots \pi_r$ descompunere în produs de cicli disjuncţi în care scriem şi ciclii de lungime 1. Dacă $\sigma = e$, afirmaţia este evidentă. Altfel avem $p = \text{ord}(\sigma) = [\text{ord}(\pi_1), \ldots, \text{ord}(\pi_r)]$, deci $\text{ord}(\pi_i) \in \{1, p\}$ pentru orice $i \in \{1, \ldots, r\}$. Dacă $\text{ord}(\pi_i) = p$ pentru orice $i \in \{1, \ldots, r\}$, atunci $n = \text{ord}(\pi_1) + \cdots + \text{ord}(\pi_r) = pr$, deci n se divide cu p, contradicţie. Rezultă că există un ciclu π_i de lungime 1 şi acesta ne dă un punct fix pentru σ.

61. (i) Deoarece orice permutare este un produs de transpoziţii, este suficient să arătăm că orice transpoziţie se află în subgrupul generat de familia

de transpoziţii dată. Într-adevăr, dacă $i \neq j$, avem $(ij) = (1i)(1j)(1i)$ şi afirmaţia este demonstrată.
(ii) Este suficient să arătăm că transpoziţiile de la (i) sunt în subgrupul generat de familia dată. Pentru aceasta folosim următoarea relaţie care are loc pentru orice $1 \leq i \leq n-1$:

$$(1, i+1) = (i, i+1)(1i)(i, i+1).$$

Faptul că $(1i)$ se află în subgrupul generat de transpoziţiile din enunţ rezultă prin inducţie după i. Pentru $i = 2$, transpoziţia (12) apare printre cele date. Presupunem că $(1i)$ este în subgrupul generat de familia de transpoziţii dată. Din formulă rezultă că şi $(1, i+1)$ se află acolo.
(iii) Să observăm că pentru orice $1 \leq i \leq n-2$ are loc următoarea relaţie:

$$(12\ldots n)^i(12)(12\ldots n)^{-i} = (i+1, i+2)$$

care rezultă imediat prin inducţie după i. Atunci transpoziţiile de la (ii) sunt în subgrupul generat de cele două permutări date şi deci şi acestea generează pe S_n.

62. Presupunem prin absurd că există $n-2$ transpoziţii care generează pe S_n. Fie acestea $\tau_1, \ldots, \tau_{n-2}$. Există printre acestea una care îl conţine pe 1 în orbită, altfel 1 ar fi fixat de toate aceste transpoziţii şi deci de toate permutările din S_n, contradicţie. Eventual renotând, putem presupune că $\tau_1 = (1, i_1), \ldots, \tau_p = (1, i_p)$ sunt toate cele care îl conţin pe 1 în orbită. Dacă $p = n-2$, atunci există $i \in \{1, \ldots, n\} - \{1, i_1, \ldots, i_p\}$ şi acest i este fixat de toate transpoziţiile date, deci de toate permutările din S_n, contradicţie. Deci $p < n-2$. Acum dacă există $\tau \in \{\tau_{p+1}, \ldots, \tau_{n-2}\}$ care conţine în orbită unul dintre elementele $i_1, \ldots, i_p$, să zicem $\tau = (i_p, j)$, atunci o putem înlocui pe aceasta în sistemul de generatori cu $(1j)$, deoarece $(i_p, j) = (1i_p)(1j)(1i_p)$. După un număr finit de astfel de înlocuiri putem presupune că nici una dintre transpoziţiile $\tau_{p+1}, \ldots, \tau_{n-2}$ nu are în orbită vreun element din mulţimea $\{1, i_1, \ldots, i_p\}$. Alegem $j \notin \{1, i_1, \ldots, i_p\}$ şi atunci transpoziţia $(1j)$ nu se poate scrie ca produs de transpoziţii din mulţimea $\{\tau_1, \ldots, \tau_{n-2}\}$, deoarece un astfel de produs duce pe 1 într-unul din elementele $1, i_1, \ldots, i_p$, contradicţie.

63. Orice permutare se poate scrie ca produs de transpoziţii. Dacă permutarea este în A_n, deci pară, în produs intră un număr par de transpoziţii. Afirmaţia din enunţ rezultă atunci imediat dacă arătăm produsul a două

transpoziţii este în subgrupul generat de ciclii de lungime 3. Pentru aceasta observăm că au loc formulele: $(ij)(kl) = (ijk)(ikl)$ şi $(ij)(il) = (ilj)$ şi demonstraţia este încheiată.

64. Arătăm mai întâi că dacă N este un subgrup normal netrivial al lui A_n care conţine un ciclu de lungime 3, atunci N contine toţi ciclii de lungime 3. Să presupunem că $(123) \in N$. Atunci pentru permutarea $\tau \in S_n$ cu $\tau(1) = i$, $\tau(2) = j$, $\tau(3) = k$ şi $\tau(l) = l$ pentru $l > 3$ avem $\tau(123)\tau^{-1} = (ijk)$. Dacă τ este permutare pară s-a terminat. Dacă nu, înlocuim pe τ cu $(rs)\tau$, unde r, s sunt distincte şi diferite de i, j, k.
Vom arăta acum că dacă N este un subgrup normal netrivial al lui A_n, atunci el conţine un ciclu de lungime 3. Fie $\sigma \in N$, $\sigma \neq e$. Notăm $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1} \in N$, unde $\tau \in A_n$. Dacă σ este un ciclu de lungime 3, s-a terminat. Dacă nu, considerăm următoarele trei cazuri:
a) σ conţine în descompunere un ciclu $(ijkl\dots)$ de lungime cel puţin 4. Luăm $\tau = (ijk)$ şi obţinem $\sigma\tau\sigma^{-1} = (jkl)$ şi deci $[\sigma, \tau] = (ilj) \in N$.
b) σ conţine în descompunere un ciclu (ijk) de lungime 3. Scriem $\sigma = (ijk)(lm\dots)\dots$, luăm $\tau = (ijl)$ şi obţinem $\sigma\tau\sigma^{-1} = (jkm)$ şi deci $[\sigma, \tau] = (ilkmj) \in N$. Aplicăm acum cazul a) cu $[\sigma, \tau]$ în loc de σ.
c) σ conţine în descompunere doar cicli de lungime 2. Scriem $\sigma = (ij)(kl)\dots$, alegem m diferit de i, j, k, l, luăm $\tau = (ikm)$ şi obţinem $\sigma\tau\sigma^{-1} = (jl\sigma(m))$. Avem următoarele posibilităţi pentru $[\sigma, \tau]$: dacă $\sigma(m) = m$, atunci $[\sigma, \tau] = (ijlmk)$ şi aplicăm din nou cazul a) cu $[\sigma, \tau]$ în loc de σ. Altfel $[\sigma, \tau] = (jl\sigma(m))(mki)$ şi din nou putem aplica cazul b) cu $[\sigma, \tau]$ în loc de σ.
De aici rezultă că N conţine toţi ciclii de lungime 3, deci conform problemei 63 obţinem $N = A_n$, contradicţie. Deci A_n este grup simplu.

65. Presupunem că H este un subgrup normal al lui S_n şi că $H \neq \{e\}, S_n$. Vom arăta că $H = A_n$. Cum $H \trianglelefteq S_n$, rezultă că $H \cap A_n \trianglelefteq A_n$. Dar pentru $n = 3$ sau $n \geq 5$ grupul A_n este simplu, adică nu are subgrupuri normale proprii (vezi problema 64). Deci $H \cap A_n = A_n$ sau $H \cap A_n = \{e\}$. Dacă $H \cap A_n = A_n$, atunci $A_n \subseteq H \subseteq S_n$ şi cum $[S_n : A_n] = 2$, rezultă că $H = S_n$ (caz imposibil) sau $H = A_n$. Presupunem acum că $H \cap A_n = \{e\}$. Cum $A_n \trianglelefteq S_n$, rezultă că $HA_n \leq S_n$. Dar H este netrivial şi conţine o permutare impară, deci $HA_n \neq A_n$. Obţinem $HA_n = S_n$ şi atunci $S_n/H = HA_n/H \simeq A_n/H \cap A_n \simeq A_n$, de unde $|H| = 2$. Atunci $H = \{e, \sigma\}$, unde σ este o permutare de ordin 2. Dar $H \trianglelefteq S_n$ implică $\sigma \in Z(S_n)$, deci $\sigma = e$, contradicţie. Rămâne deci că $H = A_n$.

66. (i) Fie $\sigma \in S_4$. Atunci $\sigma(12)(34)\sigma^{-1} = (\sigma(1)\sigma(2))(\sigma(3)\sigma(4)) \in K$. Analog şi pentru celelalte elemente din K, de unde obţinem $K \trianglelefteq S_4$.
(ii) Avem $|S_4/K| = 6$, deci S_4/K este izomorf cu $\mathbb{Z}_6$ sau cu S_3. Dacă $S_4/K \simeq \mathbb{Z}_6$, atunci este grup ciclic şi conţine un element de ordin 6, fie acesta $\hat{\sigma}$. Dar $\sigma \in S_4$ şi deci $\text{ord}(\sigma) \in \{1, 2, 3, 4\}$. Atunci $\hat{\sigma}$ nu poate avea ordin 6, contradicţie. Rezultă că $S_4/K \simeq S_3$.
(iii) Observăm că A_4 are un element de ordin 1, trei elemente de ordin 2 şi opt elemente de ordin 3. Dacă X este un subgrup cu 6 elemente al lui A_4, atunci X nu poate fi izomorf cu $\mathbb{Z}_6$ deoarece A_4 nu are elemente de ordin 6, deci $X \simeq S_3$. Atunci X are trei elemente de ordin 2 şi cum în A_4 există doar trei elemente de ordin 2, cele din $K - \{e\}$, rezultă că $K \subseteq X$ şi atunci, din teorema lui Lagrange, obţinem $4|6$, contradicţie. În concluzie, A_4 nu are subgrupuri cu 6 elemente.
(iv) Un subgrup propriu al lui A_4 are două, trei, patru sau şase elemente. Ştim din (iii) că subgrupuri cu şase elemente nu există. Singurul subgrup cu 4 elemente este K, deoarece un grup cu patru elemente nu are elemente de ordin 3 şi deci un subgrup cu patru elemente al lui A_4 este inclus în K, deci egal cu K. Subgrupurile cu trei sau două elemente sunt ciclice, deci generate de cicli de lungime 3 sau de produse de transpoziţii disjuncte. În ambele situaţii, un calcul simplu cu permutări arată că acestea nu pot fi normale.
(v) Fie $X \trianglelefteq S_4$. Analizăm două cazuri:
a) $X \subseteq A_4$. Deci $X \trianglelefteq A_4 \Rightarrow X = \{e\}, K$ sau A_4 (vezi (iv)).
b) $X \not\subseteq A_4$. Deci există $\sigma \in X$ permutare impară. Rezultă că σ este o transpoziţie sau ciclu de lungime 4. Dacă σ este transpoziţie, să zicem $\sigma = (ij)$, atunci $\tau\sigma\tau^{-1} = (\tau(i)\tau(j)) \in X$ pentru orice $\tau \in S_4$, deci X conţine toate transpoziţiile. De aici obţinem că $X = S_4$. Dacă σ este ciclu de lungime 4, $\sigma = (ijkl)$, atunci X va conţine toţi ciclii de lungime 4. Cum $\sigma^2 = (ik)(jl) \in X$, X va conţine şi toate produsele de câte două transpoziţii disjuncte, deci $K \subseteq X$. Dar $(ijkl)(iljk) = (jlk) \in X$, deci X conţine toţi ciclii de lungime 3. Rezultă că $A_4 \subsetneq X$, deci $X = S_4$.

67. (i) Dacă $f : S_n \to \mathbb{Z}$ este un morfism de grupuri, atunci $\text{Im}(f)$ este un subgrup finit al lui $\mathbb{Z}$, deci este $\{0\}$. Aşadar avem numai morfismul nul.
(ii) Fie $f : S_n \to \mathbb{Q}^*$ un morfism de grupuri. Discutăm mai întâi cazurile $n \geq 5$ sau $n = 3$. Din problema 65 rezultă că $\text{Ker}(f)$ este $\{e\}$, A_n sau S_n. Dacă $\text{Ker}(f) = \{e\}$, atunci f este morfism injectiv şi rezultă că $\mathbb{Q}^*$ are un subgrup neabelian (izomorf cu S_n), contradicţie. Dacă $\text{Ker}(f) = A_n$,

atunci pentru o transpoziţie $\tau \in S_n$ avem $1 = f(e) = f(\tau^2) = f(\tau)^2$, deci $f(\tau) \in \{-1, 1\}$. Cum $\tau \notin \mathrm{Ker}(f)$, rezultă că $f(\tau) = -1$. Atunci $f(\sigma) = -1$ pentru orice permutare impară $\sigma \in S_n$, deci f este morfismul signatură. Dacă $\mathrm{Ker}(f) = S_n$, atunci f este morfismul trivial. Deci există două morfisme, signatura şi morfismul trivial.
Discutăm acum cazul $n = 4$. În acest caz, pe lângă $\{e\}, A_4$ şi S_4, grupul S_4 mai are şi subgrupul normal K descris în problema 66. Dacă $\mathrm{Ker}(f)$ este unul dintre primele trei subgrupuri, soluţia decurge ca mai sus şi obţinem tot două morfisme, signatura şi morfismul trivial. Dacă însă $\mathrm{Ker}(f) = K$, atunci $f((ij)) = -1$ pentru orice $i \neq j$, deoarece $f((ij))^2 = 1$ şi $f((ij)) \neq 1$. Avem acum că $f((123)) = f((13))f((12)) = 1$, deci $(123) \in \mathrm{Ker}(f) = K$, contradicţie. În concluzie şi în acest caz avem tot două morfisme.
(iii) Soluţia este similară cu cea de la (ii) şi obţinem tot două morfisme, morfismul nul şi morfismul care duce permutările pare în $\hat{0}$ şi permutările impare în $\hat{3}$.

68. (i) Fie $f : S_n \to \mathbb{Z}_2 \times \mathbb{Z}_2$ un morfism de grupuri. Dacă $\sigma \in S_n$ este un ciclu de lungime 3, atunci $\sigma^3 = e$, deci $3f(\sigma) = (\hat{0}, \hat{0})$, adică $f(\sigma) = (\hat{0}, \hat{0})$. Cum ciclii de lungime 3 generează pe A_n (vezi problema 63), rezultă că $A_n \subseteq \mathrm{Ker}(f)$. Atunci $\mathrm{Ker}(f) = A_n$ sau $\mathrm{Ker}(f) = S_n$. Dacă este $\mathrm{Ker}(f) = S_n$, atunci f este morfismul nul. Dacă $\mathrm{Ker}(f) = A_n$, fie σ şi τ două permutări impare din S_n. Atunci $f(\sigma) \neq (\hat{0}, \hat{0})$, $f(\tau) \neq (\hat{0}, \hat{0})$ şi $f(\sigma) + f(\tau) = (\hat{0}, \hat{0})$, de unde $f(\sigma) = f(\tau)$. Aşadar există $a \in \mathbb{Z}_2 \times \mathbb{Z}_2$, nenul, cu $f(\sigma) = a$ pentru orice $\sigma \in S_n$ permutare impară. Este clar că pentru orice $a \in \mathbb{Z}_2 \times \mathbb{Z}_2$ aplicaţia $f : S_n \to \mathbb{Z}_2 \times \mathbb{Z}_2$ definită prin $f(\sigma) = 0$ pentru $\sigma \in A_n$ şi $f(\sigma) = a$ pentru $\sigma \in S_n - A_n$, este un morfism de grupuri. Avem deci patru astfel de morfisme.
(ii) Fie $f : S_3 \to \mathbb{Z}_3$ un morfism de grupuri. Atunci $\mathrm{Ker}(f)$ este subgrup normal al lui S_3, deci poate fi $\{e\}, A_3$ sau S_3. Dacă $\mathrm{Ker}(f) = \{e\}$, atunci f este morfism injectiv, imposibil. Dacă $\mathrm{Ker}(f) = A_3$, atunci $S_3/A_3 \simeq \mathrm{Im}(f) \leq \mathbb{Z}_3$, deci $\mathbb{Z}_3$ are un subgrup cu două elemente, imposibil. Rămâne ca singură posibilitate $\mathrm{Ker}(f) = S_3$ şi în acest caz f este morfismul nul.
(iii) Dacă $f : \mathbb{Z}_3 \to S_3$ este morfism de grupuri, atunci sau $\mathrm{Ker}(f) = \mathbb{Z}_3$ şi atunci f este morfismul nul, sau $\mathrm{Ker}(f) = \{\hat{0}\}$ şi atunci f este morfism injectiv. În acest caz f este de forma: $f(\hat{0}) = e$, $f(\hat{1}) = \sigma$ şi $f(\hat{2}) = \sigma^2$, unde σ este un ciclu de lungime 3, şi avem deci două astfel de morfisme.
Avem în total trei morfisme.

69. Fie $f : S_4 \to S_3$ un morfism de grupuri. Cum $\text{Ker}(f) \trianglelefteq S_4$, rezultă că $\text{Ker}(f)$ poate fi $\{e\}$, K (descris în problema 66), A_4 sau S_4. Nu se poate ca $\text{Ker}(f)$ să fie $\{e\}$, deoarece ar rezulta că f este morfism injectiv, contradicţie. Dacă $\text{Ker}(f) = S_4$, atunci f este morfismul trivial.
Dacă $\text{Ker}(f) = A_4$, atunci $f((12)(34)) = e$, de unde $f((12)) = f((34))$ şi sunt egale cu o transpoziţie din S_3. Mai departe $f((12))f((23)) = f((123)) = e$, deci $f((12)) = f((23))$. Procedând analog obţinem $f(\sigma) = \tau$ pentru orice $\sigma \in S_4 - A_4$, unde τ este o transpoziţie dată din S_3. Evident, pentru orice astfel de transpoziţie, aplicaţia f definită prin $f(\sigma) = e$ dacă $\sigma \in A_4$ şi $f(\sigma) = \tau$ dacă $\sigma \in S_4 - A_4$ este morfism de grupuri. Avem deci trei morfisme de această formă.
Dacă $\text{Ker}(f) = K$, procedând ca mai sus obţinem $f((12)) = f((34)) = \tau_1$, $f((13)) = f((24)) = \tau_2$ şi $f((14)) = f((23)) = \tau_3$, unde τ_1, τ_2, τ_3 sunt transpoziţii distincte din S_3 (dacă nu ar fi distincte am obţine o relaţie de tipul $(ij)(ik) = (jik) \in \text{Ker}(f) = K$, contradicţie). Este clar că pentru fiecare alegere a lui τ_1, τ_2, τ_3 distincte, relaţiile de mai sus definesc un morfism de grupuri (având f definit pe transpoziţii). Cum în S_3 avem exact trei transpoziţii, rezultă că avem 6 posibilităţi de alegere pentru τ_1, τ_2, τ_3, deci avem 6 morfisme de acest tip.
Avem în total zece morfisme.

70. Să observăm mai întâi că dacă τ este o transpoziţie, atunci $f(\tau) \in H$. Pentru (ijk), ciclu de lungime 3, avem $f((ijk)) = f((ikj)^2) = f((ikj))^2 = f((ik)(kj))^2 = (f((ik))f((kj)))^2 = e$, deoarece $f((ik))f((kj)) \in H$, fiind produsul a două elemente din H. Aşadar $f((ijk)) = f((ij))f((jk)) = e$, de unde $f((ij)) = f((jk))$, aceste elemente fiind egale cu inversele lor. Deci există $a \in H$ cu $f(\tau) = a$ pentru orice transpoziţie $\tau \in S_n$. Din scrierea unei permutări ca produs de transpoziţii rezultă acum imediat că permutările pare sunt duse în e, iar cele impare în a.

71. (i) Fie $G \leq S_n$ astfel încât G nu este inclus în A_n. Din problema 29(iii) rezultă că $[G : G \cap A_n] \leq [S_n : A_n] = 2$. Dar $G \neq G \cap A_n$, deci $[G : G \cap A_n] > 1$. Am obţinut că $[G : G \cap A_n] = 2$ şi deci $G \cap A_n$ este subgrup de indice 2 în G.
Se poate argumenta chiar mai simplu: deoarece $G \neq G \cap A_n$, G conţine o permutare impară, să o notăm cu σ. Rezultă imediat că $G \cap A_n$ şi $\sigma(G \cap A_n)$ formează o partiţie a lui A_n. Dacă $\tau \in G$, atunci τ poate fi pară, caz în care $\tau \in G \cap A_n$, sau poate fi impară, caz în care $\sigma^{-1}\tau \in G \cap A_n \Leftrightarrow \tau \in \sigma(G \cap A_n)$.

(ii) Cum $|G| = 4n + 2$, din teorema lui Cauchy rezultă că G are un element g de ordin 2. Din teorema lui Cayley ştim că există un morfism injectiv de grupuri $f : G \to S(G)$ definit prin $f(x)(y) = xy$ pentru orice $x, y \in G$. (Prin $S(G)$ am notat grupul simetric al mulţimii G, care în acest caz este izomorf cu S_{4n+2}). Să observăm că permutarea $f(g)$ nu are puncte fixe, deoarece $g \neq e$, şi că $(f(g))^2 = \mathrm{Id}_G$. Rezultă că descompunerea lui $f(g)$ în produs de cicli disjuncţi constă în produsul a $2n + 1$ transpoziţii. Aşadar $f(g)$ este o permutare impară şi aplicând (i) pentru grupul $\mathrm{Im}(f)$ obţinem că $\mathrm{Im}(f)$ are un subgrup de indice 2. Dar f este morfism injectiv, deci $G \simeq \mathrm{Im}(f)$, de unde rezultă că G are un subgrup de indice 2.
Presupunem acum că există două subgrupuri distincte H_1, H_2 de indice 2 în G. Acestea sunt subgrupuri normale şi deci $H_1H_2/H_1 \simeq H_2/H_1 \cap H_2$. Deoarece H_1 este subgrup propriu al lui H_1H_2, rezultă că $H_1H_2 = G$, deci $|H_1H_2/H_1| = 2 = |H_2/H_1 \cap H_2|$, ceea ce înseamnă că $H_1 \cap H_2$ are $\frac{|H_2|}{2} = \frac{2n+1}{2}$ elemente, ceea ce este absurd.

72. Avem $D_n = \{e, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$ cu $\mathrm{ord}(r) = n$, $\mathrm{ord}(s) = 2$ şi $sr = r^{n-1}s$. Fie $j \in \{1, \ldots, n-1\}$. Atunci $r^j \in Z(D_n)$ dacă şi numai dacă $r^j s = sr^j$, deoarece un element se găseşte în centrul unui grup dacă şi numai dacă el comută cu generatorii grupului. Această relaţie este echivalentă cu $r^j s = r^{(n-1)j}s$, care la rândul ei se poate scrie $r^{(n-2)j} = e$. Cum $\mathrm{ord}(r) = n$, rezultă că $n|(n-2)j$. Dacă n este impar acest lucru este imposibil, deoarece avem $(n, n-2) = 1$ şi ar trebui atunci ca $n|j$, fals. Dacă n este par, atunci este adevărat doar pentru $j = n/2$.
Considerăm acum un element de forma $r^j s \in Z(D_n)$ cu $1 \leq j \leq n-1$. Pentru că el comută cu r avem $r^j sr = r^{j+1}s \Rightarrow r^{j+n-1}s = r^{j+1}s \Rightarrow r^{n-2} = e$, ceea ce este imposibil.
Aşadar dacă n este impar avem $Z(D_n) = \{e\}$, iar dacă n este par avem $Z(D_n) = \{e, r^{n/2}\}$.

73. (i) Fie $A \in Z(GL(n, R))$. În particular, A comută cu toate matricele din $GL(n, R)$ de forma $I_n + E_{ij}$, $1 \leq i \neq j \leq n$, unde E_{ij} este matricea care are 1 pe poziţia (i, j) şi 0 în rest. Rezultă din calcule că matricea A trebuie să fie o matrice scalară, adică $A = aI_n$, $a \in R$. Cum $A \in GL(n, R)$, trebuie ca elementul $a \in R$ să fie inversabil. În concluzie $Z(GL(n, R)) = \{aI_n \mid a \in U(R)\}$, unde $U(R)$ reprezintă grupul elementelor inversabile ale inelului R, deci $Z(GL(n, R)) \simeq U(R)$.
(ii) Dacă vreuna dintre perechile de grupuri date în enunţ ar fi izomorfe,

atunci centrele lor ar fi izomorfe, adică ar exista o pereche de grupuri izomorfe printre $(\{-1,1\},\cdot)$, $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$, respectiv $(\mathbb{C}^*,\cdot)$, ceea ce este evident fals (vezi şi problema 5).

Observaţie. Dacă R este un inel (unitar) oarecare, atunci $Z(GL(n,R)) = \{aI_n \mid a \in C(R) \cap U(R)\}$, unde prin $C(R)$ s-a notat centrul inelului R, adică $C(R) = \{x \in R \mid xy = yx \text{ oricare ar fi } y \in R\}$.

74. Să presupunem că grupurile $GL(2,\mathbb{Z})$ şi $GL(3,\mathbb{Z})$ sunt izomorfe. Vom defini acum un morfism injectiv de grupuri $f : GL(2,\mathbb{Z}) \times \{\pm 1\} \to GL(3,\mathbb{Z})$ prin $f(A, \pm 1) = \begin{pmatrix} A & 0 \\ 0 & \pm 1 \end{pmatrix}$. Deoarece grupul $(\{\pm 1\},\cdot)$ este izomorf cu $\mathbb{Z}_2$ şi $GL(2,\mathbb{Z})$ este izomorf cu $GL(3,\mathbb{Z})$, rezultă că avem un morfism injectiv de la $GL(2,\mathbb{Z}) \times \mathbb{Z}_2$ la $GL(2,\mathbb{Z})$. Iterând obţinem că există un morfism injectiv de la $GL(2,\mathbb{Z}) \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (în produs se consideră n cópii ale lui $\mathbb{Z}_2$) la $GL(2,\mathbb{Z})$. În particular, aceasta înseamnă că pentru orice $n \in \mathbb{N}^*$ există $A_1, \ldots, A_n \in GL(2,\mathbb{Z})$ cu proprietatea că $\text{ord}(A_i) = 2$ şi $A_iA_j = A_jA_i$, oricare ar fi $i, j \in \{1, \ldots, n\}$.

Elementele de ordin 2 din $GL(2,\mathbb{Z})$ sunt matricele $-I_2$ şi $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$, cu $bc = 1 - a^2$. Să considerăm două matrice de această formă şi să vedem în ce condiţii acestea comută: fie $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ şi $A' = \begin{pmatrix} a' & b' \\ c' & -a' \end{pmatrix}$ astfel încât $AA' = A'A$. Din calcule se obţine că $ab' = a'b, ac' = a'c, bc' = b'c$. Ţinând cont de faptul că $bc = 1 - a^2$ şi $b'c' = 1 - a'^2$, rezultă că singurele matrice de ordin 2 cu care A comută sunt $-A$ şi $-I_2$, contradicţie.

Observaţie. Soluţia dată se bazează pe faptul că grupul $\mathbb{Z}_2^3$ nu se scufundă în $GL(2,\mathbb{Z})$, dar se scufundă în $GL(3,\mathbb{Z})$. Această observaţie se poate generaliza ducând la concluzia că grupurile $GL(m,\mathbb{Z})$ şi $GL(n,\mathbb{Z})$ nu sunt izomorfe pentru $m \neq n$.

75. (i) Este clar că $H_G \subseteq H$, deoarece $eHe^{-1} = H$ se află în intersecţie. Mai departe, dacă $g \in G$ avem

$$gH_Gg^{-1} = g(\bigcap_{x\in G} xHx^{-1})g^{-1} = \bigcap_{x\in G} gxHx^{-1}g^{-1} = \bigcap_{x\in G} (gx)H(gx)^{-1} = H_G$$

deci H_G este egal cu toţi conjugaţii săi. De aici rezultă că H_G este subgrup normal.

(ii) Fie $N \trianglelefteq G$ astfel încât $N \subseteq H$. Atunci pentru orice $x \in G$ avem

$N = x^{-1}Nx \subseteq H$, de unde $N \subseteq xHx^{-1}$. Rezultă că $N \subseteq H_G$.
(iii) Considerăm acţiunea prin translaţii la stânga a grupului G pe mulţimea $(G/H)_s$ a claselor la stânga modulo H, adică pentru $g \in G$ şi $xH \in (G/H)_s$ avem $g(xH) = gxH$. Această acţiune dă naştere unui morfism de grupuri $f : G \to S((G/H)_s)$ definit prin $f(g)(xH) = g(xH) = gxH$. Să observăm că $g \in \mathrm{Ker}(f)$ dacă şi numai dacă $gxH = xH$ pentru orice $x \in G \Leftrightarrow x^{-1}gx \in H$ pentru orice $x \in G \Leftrightarrow g \in xHx^{-1}$ pentru orice $x \in G \Leftrightarrow g \in H_G$. Deci $\mathrm{Ker}(f) = H_G$ şi atunci există un morfism injectiv de grupuri între G/H_G şi $S((G/H)_s)$. Cum $|(G/H)_s| = [G : H] = n$, rezultă că $S((G/H)_s) \simeq S_n$ şi de aici obţinem morfismul injectiv căutat. În particular, H_G are indice finit ($\leq n!$) şi este subgrup normal al lui G.

76. Vom arăta că $H_G = \{aI_n \mid a \in K^*\}$. Este evident că mulţimea matricelor scalare $\{aI_n \mid a \in K^*\}$ formează un subgrup normal al lui G conţinut în H, deci $\{aI_n : a \in K^*\} \subseteq H_G$. Fie acum $A \in H$ cu proprietatea că A nu este scalară. Scriem $A = \sum_{i=1}^{n} a_{kk}E_{kk}$, unde E_{ij} este matricea care are 1 pe poziţia (i, j) şi 0 în rest, şi există $1 \leq i \neq j \leq n$ astfel încât $a_{ii} \neq a_{jj}$. Avem $E_{ij}A = \sum_{k=1}^{n} a_{kk}E_{ij}E_{kk} = a_{jj}E_{ij}$ şi $AE_{ij} = \sum_{k=1}^{n} a_{kk}E_{kk}E_{ij} = a_{ii}E_{ij}$. Fie $B = I_n + E_{ij} \in G$. Vom arăta că $BAB^{-1} \notin H$, de unde rezultă că $A \notin H_G$. Într-adevăr

$$\begin{aligned} BAB^{-1} &= (I_n + E_{ij})A(I_n - E_{ij}) \\ &= (A + a_{jj}E_{ij})(I_n - E_{ij}) \\ &= A + a_{jj}E_{ij} - a_{ii}E_{ij} - a_{jj}E_{ij}E_{ij} \\ &= A + (a_{jj} - a_{ii})E_{ij} \notin H. \end{aligned}$$

77. Se arată uşor că H este subgrup. Cum o matrice $\begin{pmatrix} \hat{a} & \hat{b} \\ \hat{0} & \hat{c} \end{pmatrix}$ din H are $\hat{b} \in \mathbb{Z}_3$ şi $\hat{a}, \hat{c} \in \mathbb{Z}_3 - \{\hat{0}\}$, rezultă că H are 12 elemente. Ştim că $Z(G)$ este format din mulţimea matricelor scalare din G, deci $|Z(G)| = 2$. Avem că $Z(G) \leq H$ şi $Z(G) \trianglelefteq G$, deci $Z(G) \subseteq H_G$.
Fie acum $A \in H_G$, deci $BAB^{-1} \in H$ pentru orice $B \in G$. Scriem $A = \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{0} & \hat{c} \end{pmatrix}$, cu $\hat{a}\hat{c} \neq \hat{0}$. Considerăm $B = \begin{pmatrix} \hat{0} & -\hat{1} \\ \hat{1} & \hat{0} \end{pmatrix}$ şi avem că $BAB^{-1} = \begin{pmatrix} \hat{c} & \hat{0} \\ \hat{b} & \hat{a} \end{pmatrix}$, deci $\hat{b} = \hat{0}$. Acum pentru $B = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{1} & \hat{1} \end{pmatrix}$ obţinem $BAB^{-1} = \begin{pmatrix} \hat{a} & \hat{0} \\ \hat{a} - \hat{c} & \hat{c} \end{pmatrix}$, deci $\hat{a} = \hat{c}$. În concluzie, $A = \hat{a}I_2 \in Z(G)$.

78. Presupunem că G este un grup simplu infinit şi H un subgrup de indice finit al său. Din problema 75 rezultă că H_G este un subgrup normal de indice finit al lui G. Dar singurele subgrupuri normale ale lui G sunt $\{e\}$ (care are indicele infinit) şi G (de indice 1), contradicţie.

79. (i) Fie H un subgrup al lui G de indice p. Conform problemei 75, grupul G/H_G se scufundă în S_p. Rezultă că $[G : H_G]$ divide $p!$. Dar $[G : H_G] = [G : H][H : H_G] = p[H : H_G]$, de unde $[H : H_G]|(p-1)!$. Dacă $H \neq H_G$, atunci există q un divizor prim al lui $[H : H_G]$ şi cum $q|(p-1)!$ rezultă că $q < p$. Dar $|G| = [G : H_G]|H_G| = [G : H][H : H_G]|H_G|$, deci $q||G|$. Dar aceasta este o contradicţie cu faptul că p este cel mai mic număr prim care divide $|G|$. Deci $H = H_G \trianglelefteq G$.
(ii) Fie H un subgrup al lui G de ordin p. Presupunem că $H \not\subseteq Z(G)$. Atunci rezultă că $H \cap Z(G) = \{e\}$. Considerăm acum acţiunea prin conjugare a lui G pe H şi scriem ecuaţia claselor pentru această acţiune. Vom avea $|H| = |H \cap Z(G)| + \sum[G : C_G(x)]$, unde $C_G(x)$ este centralizatorul elementului $x \in H$, în acest caz cu $C_G(x) \neq G$. Deoarece $[G : C_G(x)]$ divide $|G|$ şi p este cel mai mic număr prim care divide $|G|$, rezultă că $[G : C_G(x)] \geq p$, de unde $p = |H| = 1 + \sum[G : C_G(x)] \geq 1 + p$, contradicţie.

80. Ştim din problema 75 că dacă H este un subgrup de indice n al lui G, atunci există un morfism injectiv de grupuri $f : G \to S_n$ cu $\mathrm{Ker}(f) = H_G$. Cum G este finit generat, rezultă că există un număr finit de astfel de morfisme. Într-adevăr, dacă $g_1, \ldots, g_m$ generează G şi $f_1, f_2 : G \to S_n$ sunt morfisme de grupuri cu $f_1(g_1) = f_2(g_1), \ldots, f_1(g_m) = f_2(g_m)$, atunci $f_1 = f_2$. Cum există doar un număr finit de posibilităţi pentru $f(g_1), \ldots, f(g_m)$, rezultă că există doar un număr finit de morfisme $f : G \to S_n$. Prin urmare există doar un număr finit de nuclee de astfel de morfisme. Dar cum H_G nu poate fi decât unul dintre aceste nuclee, rezultă că există doar un număr finit de posibilităţi pentru el.
Acum dacă X este un subgrup normal al lui G, există o corespondenţă bijectivă între subgrupurile lui G/X şi subgrupurile H ale lui G cu $H \supseteq X$. Deci dacă X are indice finit, cum G/X este grup finit, există doar un număr finit de astfel de subgrupuri intermediare H. Aşadar există doar un număr finit de posibilităţi pentru H_G şi fiecare dintre acestea determină un număr finit de subgrupuri de indice n în G. În concluzie G are doar un număr finit de subgrupuri de indice n.

Presupunem acum că există subgrupuri de indice n în G şi fie acestea $H_1, \ldots, H_r$. Dacă $\alpha \in \mathrm{Aut}(G)$ şi $H \leq G$ cu $[G : H] = n$, atunci şi $[G : \alpha(H)] = n$. Rezultă că $\alpha(H_1), \ldots, \alpha(H_r)$ sunt chiar $H_1, \ldots, H_r$, eventual într-o altă ordine. Atunci $\alpha(H) = \alpha(\bigcap_{i=1}^{r} H_i) = \bigcap_{i=1}^{r} \alpha(H_i) = \bigcap_{i=1}^{r} H_i = H$.

81. (i) Din ecuaţia claselor de conjugare pentru grupul G rezultă că $|Z(G)| \neq 1$, deci $|Z(G)| = p$ sau $|Z(G)| = p^2$. Dacă $|Z(G)| = p^2$, atunci $Z(G) = G$, deci G este abelian. Dacă însă $|Z(G)| = p$, atunci $|G/Z(G)| = p$, deci $G/Z(G)$ este grup ciclic. Din problema 40 obţinem că G este abelian, de unde $Z(G) = G$, contradicţie.
(ii) Dacă G are un element de ordin p^2, atunci este ciclic şi deci este izomorf cu $\mathbb{Z}_{p^2}$. Dacă toate elementele $\neq e$ ale lui G au ordinul p, atunci fie $x \in G$, $x \neq e$ şi $y \in G - < x >$. Evident $< x > \cap < y > = \{e\}$. Definim acum $f : G \to G/< x > \times G/< y >$ prin $f(a) = (\overline{a}, \overline{\overline{a}})$. Se verifică uşor că f este morfism de grupuri şi din faptul că $< x > \cap < y > = \{e\}$ rezultă că este injectiv. Cum G şi $G/< x > \times G/< y >$ au acelaşi număr de elemente, f va fi şi surjectiv, deci f este izomorfism de grupuri. În concluzie, în acest caz G este izomorf cu $\mathbb{Z}_p \times \mathbb{Z}_p$.

82. Ştim că $|S_4| = 24 = 2^3 \cdot 3$, $|A_4| = 12 = 2^2 \cdot 3$. Notăm cu n_p numărul p-subgrupurilor Sylow ale unui grup. Avem că $H_1 = \{e, (123), (132)\}$, $H_2 = \{e, (124), (142)\}$, $H_3 = \{e, (134), (143)\}$, $H_4 = \{e, (234), (243)\}$ sunt 3-subgrupuri Sylow ale lui A_4 şi ale lui S_4. Cum pentru A_4 avem $n_3|4$, rezultă că $n_3 = 4$ şi H_1, H_2, H_3, H_4 sunt toate 3-subgrupurile Sylow ale lui A_4. Pentru S_4 avem $n_3|8$ şi $n_3 \equiv 1 \pmod 3$. Cum $n_3 \geq 4$, rezultă că $n_3 = 4$, deci H_1, H_2, H_3, H_4 sunt toate 3-subgrupurile Sylow şi în S_4.

Pentru S_4 avem $n_2 = 3$, deoarece $D_4 = < (1234), (12) >$ este subgrup al lui S_4 care nu este normal (şi din problema 85 ar rezulta că dacă $n_2 = 1$, atunci unicul 2-subgrup Sylow ar fi normal). Pentru A_4 avem $n_2 = 1$, deoarece $K \trianglelefteq A_4$ şi $|K| = 2^2$.

83. (i) Este evident că dacă G este grup ciclic orice p-subgrup Sylow al său este ciclic. Reciproc, fie $|G| = p_1^{k_1} \cdots p_r^{k_r}$ cu p_i numere prime distincte şi $k_i \geq 1$. Fie G_i (singurul) p_i-subgrup Sylow al lui G. Cum G_i este ciclic, rezultă că există $x_i \in G_i$ astfel încât $G_i = < x_i >$, deci $\mathrm{ord}(x_i) = p_i^{k_i}$. Deoarece G este grup abelian şi numerele $p_i^{k_i}$ sunt oricare două prime între ele, obţinem că $\mathrm{ord}(x_1 \cdots x_r) = p_1^{k_1} \cdots p_r^{k_r}$, deci G este grup ciclic.

(ii) Pentru S_3 este evident, deoarece un grup cu un număr prim de elemente este grup ciclic.

Fie acum p un divizor prim al lui $|D_n| = 2n$. Dacă $p = 2$, atunci un 2-subgrup Sylow al lui D_n va avea 2 elemente, deci va fi ciclic. Dacă $p > 2$, scriem $n = p^k l$ cu $(l, p) = 1$. Deci un p-subgrup Sylow H al lui D_n va avea p^k elemente. În particular H nu conţine elemente de ordin 2, de unde rezultă că $H \subseteq < r >$, deci H este ciclic (ca subgrup al unui grup ciclic).

84. Fie $H \leq S_5$ astfel încât $H \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Cum $|S_5| = 2^3 \cdot 3 \cdot 5$, rezultă că H este un 2-subgrup Sylow al lui S_5. Dar orice 2-subgrupuri Sylow ale lui S_5 sunt conjugate, în particular izomorfe. Cum $< (1234), (12) >$ este un 2-subgrup Sylow al lui S_5 care este izomorf cu D_4 (prin morfismul care asociază (1234) lui r şi (12) lui s), ar rezulta că $D_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, contradicţie.

85. (i) Cum orice conjugat al lui H este tot un p-subgrup Sylow şi există un singur astfel de subgrup, rezultă că H este egal cu toţi conjugaţii săi, deci este normal.
(ii) Fie $H_1, \ldots, H_{n_p}$ toate p-subgrupurile Sylow ale lui G (care au fiecare câte p elemente). Din teorema lui Lagrange rezultă că $H_i \cap H_j = \{e\}$ pentru orice $i \neq j$. Mai departe, mulţimea elementelor de ordin p din G este chiar $(H_1 \cup \ldots \cup H_{n_p}) - \{e\}$, deoarece orice element de ordin p generează un p-subgrup Sylow, deci această mulţime are $n_p(p-1)$ elemente.

86. (i) Se verifică uşor că operaţia este asociativă, admite element neutru pe (e_N, e_H) şi orice element este inversabil, inversul unui element (n, h) fiind $(\varphi(h^{-1})(n^{-1}), h^{-1})$.
Fie $p : G \to H$ definită prin $p(n, h) = h$. Este imediat că p este morfism surjectiv de grupuri şi $\mathrm{Ker}(p) = N'$, deci $N' \trianglelefteq G$. Celelalte afirmaţii rezultă din calcule simple.
(ii) Să observăm mai întâi că orice element al lui G se scrie în mod unic sub forma nh, cu $n \in N$ şi $h \in H$. Dacă $nh = n'h'$, atunci $n'^{-1}n = h'h^{-1} \in N \cap H$, deci $n'^{-1}n = h'h^{-1} = e \Rightarrow n = n', h = h'$. Acum rezultă că aplicaţia $\alpha : N \rtimes_\varphi H \to G$ dată prin $\alpha(n, h) = nh$ este bijectivă. Rămâne să arătăm

că α este morfism de grupuri. Pentru $(n,h),(n',h') \in N \rtimes_\varphi H$ avem

$$\begin{aligned}\alpha((n,h)*(n',h')) &= \alpha(n\varphi(h)(n'),hh') \\ &= \alpha(nhn'h^{-1},hh') \\ &= nhn'h^{-1}hh' \\ &= nhn'h' \\ &= \alpha((n,h))\alpha((n',h')).\end{aligned}$$

Deci α este izomorfism.

87. (i) Fie G un grup cu pq elemente. Din teorema a treia a lui Sylow avem că $n_p|q$, deci $n_p \in \{1,q\}$ şi $n_p \equiv 1 \pmod p$. Cum p nu divide $q-1$, rezultă $n_p = 1$. Apoi $n_q|p$ şi $n_q \equiv 1 \pmod q$. Cum $p < q$, rezultă că $n_q = 1$. Aplicăm acum problema 85 şi obţinem că există $p-1$ elemente de ordin p şi $q-1$ elemente de ordin q în G. Cum $1+p-1+q-1 < pq$, rezultă că mai există şi alte elemente în G. Deoarece p,q sunt prime, divizorii lui pq sunt $1,p,q$ şi pq. Atunci acele elemente au ordin pq şi deci G este ciclic.
(ii) Să observăm că G admite un q-subgrup Sylow normal (notat în cele ce urmează cu N), deoarece şi în acest caz $n_q = 1$. Fie H un p-subgrup Sylow al lui G. Rezultă că $N \cap H = \{e\}$ şi deoarece NH are pq elemente avem $NH = G$. Deci G este produs semidirect intern al subgrupurilor N şi H. Dar $N \simeq \mathbb{Z}_q$, iar $H \simeq \mathbb{Z}_p$.
Un astfel de produs semidirect este unic definit de morfismul corespun-zător de la $\mathbb{Z}_p$ la $\mathrm{Aut}(\mathbb{Z}_q) \simeq \mathbb{Z}_{q-1}$. Se ştie din problema 4 că există e- xact p astfel de morfisme şi fiecare dintre ele duce pe $\hat{1} \in \mathbb{Z}_p$ în $\pi^{i(q-1)/p}$, unde π este un generator al grupului ciclic $\mathrm{Aut}(\mathbb{Z}_q)$, $i = 0,1,\ldots,p-1$. Produsul semidirect corespunzător G_i se poate descrie prin generatori şi relaţii astfel: fie x un generator al lui $\mathbb{Z}_q$ şi y un generator al lui $\mathbb{Z}_p$. Atunci $G_i = < x,y : x^q = y^p = e, yxy^{-1} = \pi^{i(q-1)/p}(x) >$. În particular, dacă $i = 0$, atunci G_0 este abelian şi deci ciclic de ordin pq. Dacă $i \neq 0$, atunci G_i este izomorf cu G_1. Într-adevăr aplicaţia $G_1 \to G_i$ care duce pe x în x şi pe y în y^i este un izomorfism.

88. Fie G un grup cu p^n elemente, p număr prim şi $n > 1$. Dacă G nu este abelian, atunci centrul său, care este netrivial (după cum rezultă din ecuaţia claselor de conjugare), este un subgrup normal propriu şi netrivial al lui G, deci G nu este grup simplu. Dacă G este abelian, atunci fie g un element de

ordin p al lui G. Subgrupul $< g >$ este propriu, netrivial şi normal (G fiind abelian), deci din nou G nu este simplu.

Considerăm acum $|G| = pq$, cu p, q numere prime, $p < q$. Ca la problema 87(i) obţinem că $n_q = 1$. Acum din problema 85(i) rezultă că G nu este simplu.

Fie acum G un grup cu p^2q elemente, unde p şi q sunt numere prime distincte. Presupunem prin absurd că G este grup simplu, deci $n_p, n_q > 1$. Cum $n_p|q$, rezultă că $n_p \in \{1, q\}$, deci $n_p = q$. Atunci $q \equiv 1 \pmod{p}$, deci $q > p$. Mai departe avem $n_q|p^2$, deci $n_q \in \{1, p, p^2\}$. Dar $n_q > 1$ şi de asemenea $n_q \neq p$, deoarece $n_q \equiv 1 \pmod{q}$. Rezultă că $n_q = p^2$. Din problema 85(ii) obţinem că numărul elementelor de ordin q din G este $n_q(q-1) = p^2(q-1)$. Atunci mulţimea $A = \{g \in G \mid g \text{ are ordinul diferit de } q\}$ are exact p^2 elemente. Cum orice p-subgrup Sylow al lui G este inclus în A şi are p^2 elemente, rezultă că orice p-subgrup Sylow este egal cu A. Aşadar $n_p = 1$, contradicţie. Deci G nu este grup simplu.

Fie acum G un grup cu pqr elemente, unde $p < q < r$ sunt numere prime distincte. Presupunem prin absurd că G este grup simplu. Atunci $n_p, n_q, n_r > 1$. Cum $n_r|pq$, rezultă $n_r \in \{1, p, q, pq\}$. Dar $n_r \equiv 1 \pmod{r}$, deci $n_r = pq$. De asemenea $n_q|pr$ implică $n_q \in \{1, p, r, pr\}$, de unde $n_q \geq r$ (p nu poate fi congruent cu 1 modulo q). Atunci numărul elementelor de ordin r din G este $pq(r-1)$, iar numărul elementelor de ordin q este cel puţin $r(q-1)$. În sfârşit, avem $n_p \in \{1, q, r, qr\}$, deci $n_p \geq q$ şi numărul elementelor de ordin p este cel puţin $q(p-1)$. Ţinând cont şi de elementul neutru, care are ordin 1, rezultă că $|G| = pqr \geq pq(r-1)+r(q-1)+q(p-1)+1 = pqr+rq-r-q+1$, deci $0 \geq (r-1)(q-1)$, contradicţie. Aşadar G nu este grup simplu.

89. (i) Fie p un număr prim cu proprietatea că $p||G|$ şi H un p-subgrup Sylow al lui G. Scriem $|G_i| = p^{k_i}m_i$ cu $(p, m_i) = 1$. Fie $\pi_i : G \to G_i$ proiecţia canonică şi $H_i = \pi_i(H)$. În mod evident H_i este subgrup al lui G_i şi deoarece este izomorf cu un grup factor al lui H (din teorema fundamentală de izomorfism pentru grupuri aplicată restricţiei lui π_i la H) rezultă că este un p-grup, adică are ordinul o putere a lui p. Notăm $|H_i| = p^{l_i}$ şi din cauză că H_i este subgrup al lui G_i rezultă că $p^{l_i}|p^{k_i}m_i \Rightarrow p^{l_i}|p^{k_i} \Rightarrow l_i \leq k_i$. Pe de altă parte, $H \subseteq H_1 \times \cdots \times H_n$, deci $|H| \leq |H_1| \cdots |H_n| \Rightarrow p^{k_1+\cdots+k_n} \leq p^{l_1+\cdots+l_n} \Rightarrow k_1 + \cdots + k_n \leq l_1 + \cdots + l_n$ şi cum $l_i \leq k_i$ pentru orice i, vom avea $l_i = k_i$ pentru orice i. În concluzie $H = H_1 \times \cdots \times H_n$ deoarece au acelaşi număr de elemente şi H_i este p-subgrup Sylow al lui G_i pentru orice i. Desigur, în cazul în care $k_i = 0$ vom avea $H_i = \{e\}$.

Reciproc este evident.
(ii) 2-subgrupurile Sylow sunt $\hat{3}\mathbb{Z}_6 \times < \tau >$, unde $\tau \in S_3$ este o transpoziţie, iar 3-subgrupurile Sylow sunt $\hat{2}\mathbb{Z}_6 \times < \sigma >$, unde $\sigma \in S_3$ este un ciclu de lungime 3.

90. Să începem prin a face următoarea remarcă: dacă G este un grup şi $H, K \subseteq G$ sunt subgrupuri normale cu proprietatea că $H \cap K = \{e\}$, atunci oricare ar fi $x \in H$ şi $y \in K$ rezultă că $xy = yx$. Aceasta rezultă imediat: se consideră elementul $xyx^{-1}y^{-1}$ şi se observă că datorită faptului că H şi K sunt subgrupuri normale $xyx^{-1}y^{-1} \in H \cap K \Rightarrow xyx^{-1}y^{-1} = e \Rightarrow xy = yx$.
Fie acum $H_i \leq G$ cu $|H_i| = p_i$ pentru orice $i = 1, \ldots, n$. Ştim că $H_i \trianglelefteq G$. Din remarca de mai sus rezultă că dacă $x \in H_i$ şi $y \in H_j$, atunci $xy = yx$, pentru orice $i, j \in \{1, \ldots, n\}$. Dacă $i = j$ este evident că cele două elemente comută deoarece $H_i \simeq \mathbb{Z}_{p_i}$, deci H_i este grup abelian. Dacă $i \neq j$, atunci $H_i \cap H_j = \{e\}$, deoarece $(|H_i|, |H_j|) = 1$.
Se arată inductiv că $H_1 \cdots H_n$ este subgrup al lui G cu $p_1 \cdots p_n$ elemente. Pentru $n = 1$ este evident. Să presupunem acum că $H_1 \cdots H_{n-1}$ este subgrup al lui G cu $p_1 \cdots p_{n-1}$ elemente. Cum H_n este subgrup normal, rezultă că $(H_1 \cdots H_{n-1})H_n$ este subgrup al lui G şi din teorema a doua de izomorfism pentru grupuri obţinem că

$$(H_1 \cdots H_{n-1})H_n/H_n \simeq H_1 \cdots H_{n-1}/(H_1 \cdots H_{n-1}) \cap H_n.$$

Dar $(H_1 \cdots H_{n-1}) \cap H_n = \{e\}$, deoarece $(|H_1 \cdots H_{n-1}|, |H_n|) = 1$. Deci

$$(H_1 \cdots H_{n-1})H_n/H_n \simeq H_1 \cdots H_{n-1},$$

de unde rezultă că $|H_1 \cdots H_n| = p_1 \cdots p_n$. Cum $H_1 \cdots H_n \subseteq G$ şi au acelaşi număr de elemente obţinem $H_1 \cdots H_n = G$, deci G este grup abelian. Acum rezultă imediat că G este izomorf cu $H_1 \times \cdots \times H_n$: definim $f : H_1 \times \cdots \times H_n \to G$ prin $f(h_1, \ldots, h_n) = h_1 \cdots h_n$ şi rezultă din cele de mai sus că f este izomorfism.

Observaţie. În condiţiile din problemă rezultă că G este grup ciclic.

Capitolul 10

Soluţii: Inele şi corpuri

1. Deoarece orice grup cu p elemente este izomorf cu $(\mathbb{Z}_p, +)$, este suficient să determinăm structurile de inel al căror grup abelian subiacent este $(\mathbb{Z}_p, +)$. Cum acest grup este generat de $\hat{1}$, înmulţirea "$*$" din inel este complet determinată de $\hat{1} * \hat{1}$. Într-adevăr, dacă $\hat{1} * \hat{1} = \hat{a}$, atunci $\hat{n} * \hat{m} = \widehat{nma}$ pentru orice $\hat{n}, \hat{m} \in \mathbb{Z}_p$. Pe de altă parte, o verificare simplă arată că pentru orice $\hat{a} \in \mathbb{Z}_p$ înmulţirea $\hat{n} * \hat{m} = \widehat{nma}$ defineşte o structură de inel $(\mathbb{Z}_p, +, *)$. Dacă $\hat{a} \neq \hat{0}$, atunci inelul $(\mathbb{Z}_p, +, *)$ este izomorf cu inelul $(\mathbb{Z}_p, +, \cdot)$ al claselor de resturi modulo p, un izomorfism fiind $f : (\mathbb{Z}_p, +, \cdot) \to (\mathbb{Z}_p, +, *)$, $f(\hat{n}) = \widehat{na}$.
Dacă $\hat{a} = \hat{0}$, atunci $(\mathbb{Z}_p, +, *)$ este inelul nul, în care $\hat{n} * \hat{m} = \hat{0}$ pentru orice $\hat{n}, \hat{m} \in \mathbb{Z}_p$, şi acesta este evident neizomorf cu $(\mathbb{Z}_p, +, \cdot)$.
Prin urmare există exact două structuri de inel neizomorfe pe o mulţime cu p elemente, şi anume inelul nul şi inelul $(\mathbb{Z}_p, +, \cdot)$ care este chiar corp comutativ.

2. O structură de inel pe $(\mathbb{Z}_n, +)$ este determinată de $\hat{1} * \hat{1} = \hat{a}$ (atunci $\hat{x} * \hat{y} = \widehat{xya}$ pentru orice $\hat{x}, \hat{y} \in \mathbb{Z}_n$ şi se verifică uşor axiomele inelului). Arătăm că $(\mathbb{Z}_n, +, *)$ este inel unitar dacă şi numai dacă $(a, n) = 1$. Într-adevăr, $\hat{e}$ este element unitate în raport cu "$*$" dacă şi numai dacă $\hat{x} * \hat{e} = \hat{e} * \hat{x} = \hat{x}$ pentru orice $\hat{x} \in \mathbb{Z}_n$, adică $\widehat{xea} = \hat{x}$ pentru orice $\hat{x} \in \mathbb{Z}_n$, ceea ce este echivalent cu $\widehat{ea} = \hat{1}$. Un astfel de $\hat{e}$ există dacă şi numai dacă $(a, n) = 1$. Aşadar, există $\phi(n)$ structuri de inel unitar pe $(\mathbb{Z}_n, +)$ şi, la fel ca la soluţia problemei 1, se arată că acestea sunt izomorfe cu $(\mathbb{Z}_n, +, \cdot)$.

3. Dacă grupul $(R, +)$ subiacent inelului este ciclic, fie a un generator al acestui grup şi $r, s \in R$ două elemente arbitrare. Atunci există $m, p \in \mathbb{N}^*$ cu

$r = ma$ şi $s = pa$. Rezultă $rs = (ma)(pa) = mpa^2 = pma^2 = (pa)(ma) = sr$ şi deci R este comutativ.
În particular, dacă R are $p_1 \cdots p_n$ elemente atunci, conform problemei 19(iv) din Capitolul 3, rezultă că grupul $(R, +)$ este ciclic.

4. Fie R un inel unitar cu p^2 elemente. Dacă $1 = 1_R$ are ordinul p^2 în $(R, +)$, atunci $(R, +)$ este ciclic şi din problema 3 rezultă că R este comutativ. Dacă 1 are ordinul p, fie K subinelul lui R generat de 1. Atunci K are p elemente, deci este corp comutativ (a se vedea rezultatul problemei 1). Mai mult, există $a \in R$ astfel încât $\{1, a\}$ este o bază a K-spaţiului vectorial R şi $K = \{n \cdot 1_R | \ n \in \mathbb{N}^*\}$ este inclus în centrul lui R. Dacă $r, s \in R$, atunci există $\alpha, \beta, \gamma, \delta$ în K astfel încât $r = \alpha + \beta a$ şi $s = \gamma + \delta a$. Efectuând înmulţirile obţinem $rs = sr$.

Dacă R nu este inel unitar afirmaţia nu mai este adevărată. Fie $R = \mathbb{Z}_p \times \mathbb{Z}_p$ cu adunarea pe componente şi înmulţirea dată de $(a, b)(c, d) = (ac + bc, ad + bd)$ pentru orice $a, b, c, d \in \mathbb{Z}_p$. Se arată prin calcul că sunt satisfăcute axiomele inelului. Avem $(1, 1)(1, 0) = (2, 0)$ şi $(1, 0)(1, 1) = (1, 1)$, deci R nu este comutativ. În particular, din prima parte a problemei rezultă că R nu este unitar.

5. Fie R subinelul lui $M_2(\mathbb{Z}_p)$ având ca elemente matricele care au 0 pe poziţia $(2, 1)$. Atunci R este inel unitar (cu I_2 element unitate), are p^3 elemente şi este evident necomutativ deoarece

$$\begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix} \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{0} & \hat{0} \end{pmatrix} \neq \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{0} & \hat{0} \end{pmatrix} \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}.$$

6. Fie $S = \mathbb{Z} \times R$. Definim pe S adunarea pe componente şi înmulţirea $(p, a) \cdot (m, b) = (pm, pb + ma + ab)$ pentru orice $p, m \in \mathbb{Z}$ şi $a, b \in R$. Se verifică uşor că S este inel unitar cu elementul identitate la înmulţire $(1, 0)$. Aplicaţia $\phi : R \to S$, $\phi(r) = (0, r)$ este un morfism injectiv de inele, deci $R \simeq \phi(R)$ care este subinel al lui S.

Dacă există $n \in \mathbb{N}^*$ cu $nr = 0$ pentru orice $r \in R$, luăm $S = \mathbb{Z}_n \times R$ cu adunarea pe componente şi înmulţirea $(\hat{p}, a) \cdot (\hat{m}, b) = (\hat{p}\hat{m}, pb + ma + ab)$ care este corect definită (se observă uşor că pentru $b \in R$ şi $p, q \in \mathbb{Z}$ cu $\hat{p} = \hat{q}$ avem $p = q + ns$ pentru un $s \in \mathbb{Z}$ şi cum $nb = 0$ rezultă $pb = qb$).

7. Vom arăta că perechea (S, ϕ) din soluţia problemei 6 satisface condiţia cerută. Fie $f : R \to A$ un morfism de inele, unde A este un inel unitar.

Definim $\bar{f} : S \to A$ prin $\bar{f}(p, a) = p \cdot 1_A + f(a)$. Atunci

$$\begin{aligned}
\bar{f}((p,a)(m,b)) &= \bar{f}(pm, pb + ma + ab) \\
&= pm \cdot 1_A + f(pb + ma + ab) \\
&= pm \cdot 1_A + pf(b) + mf(a) + f(a)f(b) \\
&= (p \cdot 1_A + f(a))(m \cdot 1_A + f(b)) \\
&= \bar{f}(p,a)\bar{f}(m,b)
\end{aligned}$$

şi $\bar{f}(1, 0) = 1_A$, deci $\bar{f}$ este morfism unitar de inele. Evident $f = \bar{f}\phi$. Dacă g este un morfism unitar de inele astfel încât $f = g\phi$ atunci $g(p, a) = g(p, 0) + g(0, a) = pg(1, 0) + g(\phi(a)) = p \cdot 1_A + f(a)$, deci $g = \bar{f}$.
Presupunem acum că (S', ϕ') este o altă pereche cu proprietatea din enunţ. Aplicând proprietatea din enunţ perechii (S, ϕ) şi morfismului de inele $\phi' : R \to S'$ obţinem un morfism unitar de inele $h : S \to S'$ cu $h\phi = \phi'$. Analog există un morfism unitar de inele $u : S' \to S$ cu $u\phi' = \phi$. Atunci $uh\phi = u\phi' = \phi$ şi aplicând partea de unicitate din proprietatea lui (S, ϕ) pentru morfismul de inele $\phi : R \to S$ rezultă că $uh = Id_S$. Analog $hu = Id_{S'}$, deci S şi S' sunt izomorfe.

8. (i) Arătăm că $\hat{a} \in U(\mathbb{Z}_n) \Leftrightarrow (a, n) = 1$. Într-adevăr, $\hat{a} \in U(\mathbb{Z}_n)$ $\Leftrightarrow$ există $\hat{b} \in \mathbb{Z}_n$ astfel încât $\hat{a}\hat{b} = \hat{1} \Leftrightarrow$ există $b \in \mathbb{Z}$ astfel încât $n|ab - 1$ $\Leftrightarrow$ există b şi k în $\mathbb{Z}$ cu proprietatea că $ab + nk = 1 \Leftrightarrow (a, n) = 1$. Deci $|U(\mathbb{Z}_n)| = |\{a \in \mathbb{N}^* \mid a < n \text{ şi } (a, n) = 1\}|$, iar cardinalul din membrul drept al acestei egalităţi este $\phi(n)$, unde ϕ este indicatorul lui Euler.

Deducem că $\hat{a} \in \mathbb{Z}_n$ este divizor al lui zero $\Leftrightarrow (a, n) \neq 1$. Într-adevăr, dacă $(a, n) = d \neq 1$, $d \in \mathbb{Z}$, rezultă $n = dc$ pentru un $c \in \mathbb{Z}$ şi atunci $\hat{a}\hat{c} = 0$, deci $\hat{a}$ este divizor al lui zero. Cealaltă implicaţie este evidentă. Astfel, numărul divizorilor lui zero ai lui $\mathbb{Z}_n$ este $n - \phi(n)$.

Arătăm acum că $\hat{a} \in N(\mathbb{Z}_n) \Leftrightarrow \hat{a} \in \widehat{p_1 \cdots p_r}\mathbb{Z}_n$, unde $p_1, \ldots, p_r$ sunt factorii primi ai lui n. Fie $\hat{a} \in N(\mathbb{Z}_n)$, deci există $k \in \mathbb{N}$ astfel încât $\hat{a}^k = \hat{0}$. Rezultă $n|a^k$, deci $p_i|a^k$ pentru orice $i \in \{1, 2, \ldots, r\}$, adică $p_i|a$ pentru orice $i \in \{1, 2, \ldots, r\}$, de unde rezultă $p_1 \cdots p_r|a$. Reciproc, fie $\hat{a} \in \widehat{p_1 \cdots p_r}\mathbb{Z}_n \Leftrightarrow$ există $\hat{b} \in \mathbb{Z}_n$ astfel încât $\hat{a} = \widehat{p_1 \cdots p_r}\hat{b} \Leftrightarrow n|a - p_1 \cdots p_r b \Rightarrow p_1 \cdots p_r|a$. Pentru fiecare $i \in \{1, 2, \ldots, r\}$ notăm cu α_i exponentul lui p_i din descompunerea lui n. Atunci, luând $k \in \mathbb{N}$ astfel încât $k \geq \alpha_i$ pentru orice $i \in \{1, 2, \ldots, r\}$ avem că $n|a^k$, deci $\hat{a}^k = \hat{0}$. Prin urmare $N(\mathbb{Z}_n) = \widehat{p_1 \cdots p_r}\mathbb{Z}_n$, de unde $|N(\mathbb{Z}_n)| = |p_1 \cdots p_r\mathbb{Z}/n\mathbb{Z}| = n/p_1 \cdots p_r$.

(ii) Se consideră $R = \mathbb{Z}_{216} \times \mathbb{Z}_2$ şi $S = \mathbb{Z}_{216} \times \mathbb{Q}$.

9. Fie $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Vom arăta că există o bijecţie între mulţimile $\mathrm{Idemp}(\mathbb{Z}_n)$ şi $\mathcal{P}(\{p_1, \ldots, p_r\})$ şi astfel va rezulta că $|\mathrm{Idemp}(\mathbb{Z}_n)| = 2^r$. Se observă că $\hat{x} = \hat{x}^2 \Leftrightarrow n|x(x-1)$ şi cum $(x, x-1) = 1$ rezultă că $p_i^{\alpha_i}|x$ sau $p_i^{\alpha_i}|x-1$ oricare ar fi $1 \leq i \leq r$ (deoarece $p_i^{\alpha_i}|x \Leftrightarrow p_i|x$). Dacă $\{i_1, \ldots, i_k\}$ este o submulţime a lui $\{1, \ldots, r\}$ cu proprietatea că $p_i^{\alpha_i}|x \Leftrightarrow i \in \{i_1, \ldots, i_k\}$, atunci vom defini $f : \mathrm{Idemp}(\mathbb{Z}_n) \to \mathcal{P}(\{p_1, \ldots, p_r\})$ prin $f(\hat{x}) = \{p_{i_1}, \ldots, p_{i_k}\}$.
• f este bine definită: dacă $\hat{x}, \hat{y} \in \mathrm{Idemp}(\mathbb{Z}_n)$ astfel încât $\hat{x} = \hat{y}$ rezultă $n|x-y$, deci $p_i|x-y$ pentru orice $1 \leq i \leq r$. Atunci pentru $j \in \{1, \ldots, r\}$ avem că $p_j|x \Leftrightarrow p_j|x-(x-y) = y$, deci f este bine definită.
• f este injectivă: dacă $f(\hat{x}) = f(\hat{y}) = \{i_1, \ldots i_k\}$ avem că $p_{i_1}^{\alpha_{i_1}} \cdots p_{i_k}^{\alpha_{i_k}}|x$ şi $p_{i_1}^{\alpha_{i_1}} \cdots p_{i_k}^{\alpha_{i_k}}|y$, deci $p_{i_1}^{\alpha_{i_1}} \cdots p_{i_k}^{\alpha_{i_k}}|x-y$. Dar $p_{j_1}^{\alpha_{j_1}} \cdots p_{j_l}^{\alpha_{j_l}}|x-1$ şi $p_{j_1}^{\alpha_{j_1}} \cdots p_{j_l}^{\alpha_{j_l}}|y-1$, unde $\{j_1, \ldots, j_l\} = \{1, \ldots, r\} \backslash \{i_1, \ldots, i_k\}$, de unde rezultă că $p_{j_1}^{\alpha_{j_1}} \cdots p_{j_l}^{\alpha_{j_l}}|(x-1)-(y-1) = x-y$. Aşadar, $n|x-y$, deci $\hat{x} = \hat{y}$.
• f este surjectivă: fie $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, r\}$ şi $\{j_1, \ldots, j_l\} = \{1, \ldots, r\} \setminus \{i_1, \ldots, i_k\}$. Cum $(p_{i_1}^{\alpha_{i_1}} \cdots p_{i_k}^{\alpha_{i_k}}, p_{j_1}^{\alpha_{j_1}} \cdots p_{j_l}^{\alpha_{j_l}}) = 1$ există $x', y' \in \mathbb{Z}$ astfel încât $p_{i_1}^{\alpha_{i_1}} \cdots p_{i_k}^{\alpha_{i_k}} x' + p_{j_1}^{\alpha_{j_1}} \cdots p_{j_l}^{\alpha_{j_l}} y' = 1$. Considerăm $x = p_{i_1}^{\alpha_{i_1}} \cdots p_{i_k}^{\alpha_{i_k}} x'$ şi se obţine că $n|x(x-1)$, de unde rezultă că $\hat{x} = \hat{x}^2$ şi $f(\hat{x}) = \{p_{i_1}, \ldots, p_{i_k}\}$.

Observăm că demonstraţia faptului că f este surjectivă oferă un algoritm de a găsi idempotenţii lui $\mathbb{Z}_n$. Vom determina în acest fel idempotenţii lui $\mathbb{Z}_{72}$. Avem $72 = 2^3 3^2$, deci vom avea patru idempotenţi, fiecare dintre ei fiind corespunzător unei submulţimi a mulţimii $\{2, 3\}$.
Mulţimii vide îi va corespunde $\hat{x} = \hat{1}$, deoarece în relaţia $1x' + 72y' = 1$ se poate lua $x' = 1, y' = 0$.
Pentru submulţimea $\{2\}$ avem $2^3 x' + 3^2 y' = 1$. Cum $x' = -1$ şi $y' = 1$ este o soluţie a ecuaţiei precedente, obţinem idempotentul $\hat{x} = \widehat{2^3 x'} = \hat{64}$.
Pentru submulţimea $\{3\}$ avem $3^2 x' + 2^3 y' = 1$ şi idempotentul corespunzător este $\hat{x} = \hat{9}$.
În final, submulţimii $\{2, 3\}$ îi corespunde $\hat{x} = \hat{0}$.

10. Fie $a \in R$ astfel încât există $a' \in R$ cu $a'a = 1$ şi $aa' \neq 1$. Considerăm mulţimea $M = \{b \in R \mid ba = 1\}$ a inverşilor la stânga ai lui a. Evident, M este nevidă deoarece $a' \in M$. Fie $f : M \to M$, $f(b) = ab + a' - 1$. Funcţia f este corect definită deoarece pentru $b \in M$, $(ab+a'-1)a = aba+a'a-a = a+1-a = 1$, deci şi $f(b) \in M$. Funcţia f este

injectivă deoarece $f(b) = f(c) \Rightarrow ab + a' - 1 = ac + a' - 1$, de unde $ab = ac$ şi înmulţind la stânga cu a' rezultă că $b = c$. Pe de altă parte, $a' \notin \mathrm{Im}(f)$, altfel ar rezulta că există $b \in R$ cu $ab = 1$ şi s-ar contrazice faptul că a nu este inversabil la dreapta. Existenţa funcţiei $f : M \to M$ injectivă şi nesurjectivă demonstrează că M este infinită (a se vedea problema 4 din Capitolul 1).
Partea a doua este o consecinţă a primei părţi, deoarece un element care are doi inverşi la stânga nu este inversabil.

11. Fie R un inel unitar finit şi $a \in R \setminus \{0\}$ un nondivizor al lui zero, adică a nu este divizor al lui zero nici la stânga şi nici la dreapta. Definim $f : R \to R$ prin $f(x) = xa$ pentru orice $x \in R$. Deoarece a nu este divizor al lui zero, rezultă că f este injectivă. Cum R este mulţime finită rezultă că f este şi surjectivă, deci este bijectivă. Rezultă că există $b \in R$ astfel încât $ba = 1$, deci a este inversabil la stânga. Analog se obţine că a este inversabil la dreapta. Rezultă că a este inversabil.
Dacă R este inel integru finit, atunci mulţimea divizorilor lui zero la stânga sau la dreapta din R este $\{0\}$. Rezultă că orice element nenul este inversabil, deci R este corp.

12. Fie $D = \{a_1, \ldots, a_n\}$ mulţimea divizorilor lui zero la stânga sau la dreapta din R. Presupunem prin absurd că R este infinit. Fie $a \in D \setminus \{0\}$ un divizor al lui zero la dreapta (se raţionează analog pentru un divizor al lui zero la stânga). Dacă $x \in R \setminus D$, atunci ax este un element nenul din D. Cum D este finită, rezultă că există o mulţime infinită de elemente din R, fie acestea $r_1, \ldots, r_n, \ldots$, astfel încât $ar_1 = \ldots = ar_n = \ldots$. Rezultă că $r_i - r_j \in D$ pentru orice $i, j \in \mathbb{N}^*$, deci $r_i - r_1 \in D$ pentru orice $i \in \mathbb{N}^*$ ceea ce contrazice finitudinea lui D. Prin urmare, R este finit.
Fie $x \in R \setminus \{0\}$ un divizor al lui zero la dreapta şi $\phi : R \to xR$ definită prin $\phi(a) = xa$. Avem că ϕ este morfism surjectiv de grupuri, deci $R/\operatorname{Ker}(\phi) \simeq xR$, de unde obţinem $|R| = |\operatorname{Ker}(\phi)||xR|$. Cum mulţimile $\operatorname{Ker}(\phi)$ şi xR sunt formate din divizori ai lui zero la dreapta, rezultă $|D|^2 \geq n$, deci $|D| \geq \sqrt{n} \geq [\sqrt{n}]$ (se poate raţiona analog pentru un divizor al lui zero la stânga, luând Rx în loc de xR). Conform problemei 11, într-un inel finit avem $U(R) = R \setminus D$, rezultă că $|U(R)| \leq n - [\sqrt{n}]$.

13. (i) Presupunem că $1 - ba$ are inversul la stânga u. Atunci $R(1-ab) \supseteq Rb(1-ab) = R(1-ba)b = Rb$. În particular, $ab \in R(1-ab)$. Cum şi $1 - ab \in R(1-ab)$, rezultă că $1 = ab + (1-ab) \in R(1-ab)$, deci $R(1-ab) = R$

şi $1-ab$ este inversabil la stânga.
Observăm că soluţia permite şi calculul efectiv al unui invers la stânga pentru $1-ab$. Într-adevăr

$$\begin{aligned} 1 &= 1-ab+ab \\ &= 1-ab+au(1-ba)b \\ &= 1-ab+aub(1-ab) \\ &= (1+aub)(1-ab) \end{aligned}$$

deci $1+aub$ este un invers la stânga pentru $1-ab$. Analog se arată că dacă u este un invers la dreapta pentru $1-ba$ atunci $1+aub$ este un invers la dreapta pentru $1-ab$.
(ii) Afirmaţia rezultă imediat din (i).

14. (i) Asociativitatea se verifică prin calcul direct. Evident, 0 (elementul neutru la adunare din R) este element neutru pentru $(R,\circ)$.
(ii) Presupunem că R este unitar, cu elementul neutru la înmulţire 1. Atunci aplicaţia $g: R\to R$ definită prin $g(r)=1-r$ este un izomorfism între monoizii $(R,\circ)$ şi $(R,\cdot)$. Într-adevăr, g este evident bijectivă, $g(0)=1$ şi cum

$$\begin{aligned} g(a\circ b) &= 1-a\circ b \\ &= 1-a-b+ab \\ &= (1-a)(1-b) \\ &= g(a)g(b) \end{aligned}$$

pentru orice $a,b\in R$, rezultă că g este morfism, deci este izomorfism.
(iii) Conform problemei 6, putem considera pe R ca un subinel al unui inel unitar S. Din (ii) rezultă că aplicaţia $g: S\to S$, $g(s)=1-s$ este un izomorfism de monoizi între $(S,\circ)$ şi $(S,\cdot)$, unde operaţia "$\circ$" a fost definită pe S prin aceeaşi formulă ca pe R.
Presupunem că $a,b\in R$ şi ba este quasi-regulat la stânga, deci există $v\in R$ cu $v\circ(ba)=0$. Atunci, gândind totul în S, avem $1=g(0)=g(v)g(ba)=(1-v)(1-ba)$, de unde rezultă că $1-ba$ are în S inversul la stânga $u=1-v$. Din demonstraţia problemei 13 rezultă că $1-ab$ este inversabil la stânga în S şi inversul său este $1+aub=w\in R$. Atunci $g(0)=1=w(1-ab)=g(1-w)g(ab)=g((1-w)\circ(ab))$, de unde se obţine $(1-w)\circ(ab)=0$, deci ab este quasi-regulat la stânga.

Afirmaţia similară la dreapta se demonstrează analog.
(iv) Fie $x \in R$ cu $x^n = 0$. Atunci pentru $a = -x - x^2 - \ldots - x^{n-1}$ se observă că $a + x = ax = xa$, deci $a \circ x = x \circ a = 0$.

15. (i) $\Rightarrow$ (ii) Dacă $a \in R \setminus \{1\}$, atunci $a-1$ este inversabil şi $b = (a-1)^{-1}a$ verifică relaţia $a + b = ab$.
(ii) $\Rightarrow$ (i) Fie $r \in R \setminus \{0\}$. Atunci, pentru $a = 1 - r$, există $b \in R$ astfel încât $a + b = ab$. Obţinem că $(1 - a)(1 - b) = 1$, deci r este inversabil la dreapta. Aşadar, orice element nenul din R este inversabil la dreapta. Fie $r \in R \setminus \{0\}$ şi $r', r'' \in R$ astfel încât $rr' = 1$, $r'r'' = 1$. Atunci $r'' = (rr')r'' = r(r'r'') = r$, de unde rezultă $rr' = r'r = 1$, deci r este inversabil.
Echivalenţa (i) $\Leftrightarrow$ (iii) se demonstrează similar.

16. Implicaţiile (i) $\Rightarrow$ (ii) şi (i) $\Rightarrow$ (iii) sunt clare.
(ii) $\Rightarrow$ (i) $vu^2v = 1 \Rightarrow uvu^2v = u \Rightarrow u^2v = u$. Atunci $1 = vu^2v = vu$ şi $1 = vu^2v = vuuv = uv$, deci u este inversabil şi are inversul v.
(iii) $\Rightarrow$ (i) $u(v + vu - 1)u = uvu + uvu^2 - u^2 = u + u^2 - u^2 = u$ şi din unicitatea lui v rezultă că $v + vu - 1 = v$, deci $vu = 1$. Apoi, similar, $u(v + uv - 1)u = uvu + u^2vu - u^2 = u + u^2 - u^2 = u \Rightarrow v + uv - 1 = v$, deci $uv = 1$. Aşadar u este inversabil şi $u^{-1} = v$.

17. Demonstrăm mai întâi următorul rezultat:
Dacă $f : \mathbb{R} \to \mathbb{R}$ este o funcţie care verifică relaţia $f(x + y) = f(x) + f(y)$ pentru orice $x, y \in \mathbb{R}$, atunci $f(x) = ax$ pentru orice $x \in \mathbb{Q}$, unde $a = f(1)$. Pentru aceasta se demonstrează mai întâi că $f(x_1 + \ldots + x_n) = f(x_1) + \ldots + f(x_n)$ pentru orice $n \in \mathbb{N}^*$, fapt care se obţine imediat prin inducţie. În particular, pentru $x_1 = \ldots = x_n = 1$ rezultă $f(n) = na$ pentru orice $n \in \mathbb{N}^*$. Pentru $x = y = 0$ rezultă $f(0) = 0$, iar pentru $y = -x$ rezultă $f(-x) = -f(x)$. Prin urmare, $f(x) = ax$ pentru orice $x \in \mathbb{Z}$.
Fie acum $x = p/q \in \mathbb{Q}$ cu $p, q \in \mathbb{Z}, q > 0$. Pentru $x_1 = \ldots = x_q = p/q$ se obţine $f(p) = qf(p/q)$, de unde $f(p/q) = f(p)/q = ap/q$. Aşadar $f(x) = ax$ pentru orice $x \in \mathbb{Q}$.

Din rezultatul de mai sus se obţine că dacă $f : A \to A$, unde $A = \mathbb{Z}$ sau $A = \mathbb{Q}$, verifică $f(x + y) = f(x) + f(y)$ pentru orice $x, y \in A$, atunci $f(x) = ax$ pentru orice $x \in A$, unde $a = f(1)$. În plus, dacă $f : A \to A$ este un morfism de inele, cum $f(1) = 1$ rezultă $f(x) = x$ pentru orice $x \in A$. Deci există câte un singur morfism de inele unitare $f : \mathbb{Z} \to \mathbb{Z}$, respectiv $f : \mathbb{Q} \to \mathbb{Q}$, şi anume aplicaţia identică.

Fie acum un morfism de inele $f : \mathbb{R} \to \mathbb{R}$. Avem $f(x) = x$ pentru orice $x \in \mathbb{Q}$. De asemenea, dacă $x < y$, atunci $f(y) - f(x) = f(y - x) = f(\sqrt{y-x})^2 \geq 0$, deci f este crescătoare. Fie $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Există $(x_n)_{n\in\mathbb{N}} \subseteq \mathbb{Q}$ şir crescător şi $(y_n)_{n\in\mathbb{N}} \subseteq \mathbb{Q}$ şir descrescător, ambele având limita α. Din $x_n \leq \alpha \leq y_n$ rezultă $x_n = f(x_n) \leq f(\alpha) \leq f(y_n) = y_n$. Trecând la limită obţinem $f(\alpha) = \alpha$ şi deci $f = 1_{\mathbb{R}}$. În concluzie, există un unic morfism de inele $f : \mathbb{R} \to \mathbb{R}$, şi anume morfismul identic.

18. (i) Notăm cu F mulţimea morfismelor de inele $f : \mathbb{Z} \to R$ şi definim $\phi : F \to \text{Idemp}(R)$ prin $\phi(f) = f(1)$. Cum $f(1) = f(1 \cdot 1) = f(1)f(1)$ rezultă $f(1) \in \text{Idemp}(R)$, deci ϕ este corect definită. Apoi, fie $\psi : \text{Idemp}(R) \to F$ definită prin $\psi(e)(n) = ne$ pentru orice $e \in \text{Idemp}(R)$ şi $n \in \mathbb{Z}$. Evident $\psi(e)(m + n) = \psi(e)(m) + \psi(e)(n)$ şi $\psi(e)(n)\psi(e)(m) = (ne)(me) = nme^2 = nme = \psi(e)(nm)$ pentru orice $n, m \in \mathbb{Z}$, deci $\psi(e)$ este morfism de inele. O verificare imediată arată că $\phi\psi$ şi $\psi\phi$ sunt aplicaţiile identice, deci ϕ este bijectivă.
(ii) Fie $f : \mathbb{Z}_m \to \mathbb{Z}_n$ un morfism de inele. Dacă $p : \mathbb{Z} \to \mathbb{Z}_m$ este proiecţia canonică, atunci $g = fp : \mathbb{Z} \to \mathbb{Z}_n$ este un morfism de inele pentru care, conform punctului (i), există $e \in \text{Idemp}(\mathbb{Z}_n)$ cu $g(b) = be$ pentru orice $b \in \mathbb{Z}$. Rezultă că $f(\bar{b}) = be$, unde prin $\bar{b}$ s-a notat clasa de resturi a lui b modulo m. Pentru ca f să fie corect definită este necesar ca $me = \hat{0}$, deoarece pentru $\bar{b} = \bar{c}$ (deci pentru $b - c$ divizibil cu m) trebuie ca $be = ce$, adică $(b-c)e = \hat{0}$. Am stabilit astfel o aplicaţie ϕ între mulţimea F, a morfismelor de inele între $\mathbb{Z}_m$ şi $\mathbb{Z}_n$, şi mulţimea $\text{Idemp}(\mathbb{Z}_n) \cap \{e \in \mathbb{Z}_n \mid me = \hat{0}\}$. Invers, definim $\psi : \text{Idemp}(\mathbb{Z}_n) \cap \{e \in \mathbb{Z}_n \mid me = \hat{0}\} \to F$ prin $\psi(e) = f$, unde $f : \mathbb{Z}_m \to \mathbb{Z}_n, f(\bar{b}) = be$ pentru orice $\bar{b} \in \mathbb{Z}_n$, este o funcţie corect definită şi morfism de inele. Se verifică uşor că ϕ şi ψ sunt inverse una celeilalte şi se obţine astfel bijecţia căutată.
Vom arăta că numărul morfismelor de inele $f : \mathbb{Z}_m \to \mathbb{Z}_n$ este $2^{\omega(n)-\omega(n/d)}$, unde $d = (m, n)$, iar $\omega(n)$ reprezintă numărul factorilor primi distincţi din descompunerea lui n. Pentru aceasta este suficient să calculăm $|\text{Idemp}(\mathbb{Z}_n) \cap \{e \in \mathbb{Z}_n \mid me = \hat{0}\}|$. Din $e \in \mathbb{Z}_n$ rezultă $e = \hat{a}$ pentru un $a \in \mathbb{Z}$, iar din $me = \hat{0}$ rezultă $\widehat{ma} = \hat{0}$, deci $n|ma$. Notând $m' = m/d$ şi $n' = n/d$ se obţine că $n'|m'a$, deci $n'|a$. Aşadar avem de calculat $|\text{Idemp}(\mathbb{Z}_n) \cap \{\hat{a} \in \mathbb{Z}_n \mid n'|a\}|$. Urmărind soluţia problemei 9 se obţine că numărul căutat este 2^t unde t este numărul factorilor primi din n care nu sunt în n', adică $\omega(n) - \omega(n/d)$.

19. (i) Evident, un morfism injectiv de inele este monomorfism. Re-

ciproc, fie $f : R \to S$ un monomorfism. Fie $A = \{(a, b) \mid a, b \in R$ şi $f(a) = f(b)\}$ care este un inel unitar cu adunarea şi înmulţirea pe componente. Aplicaţiile $u, v : A \to R$ definite prin $u(a, b) = a$ şi $v(a, b) = b$ sunt morfisme unitare de inele şi avem că $fu = fv$. Cum f este monomorfism rezultă că $u = v$. Aşadar, dacă $a, b \in R$ verifică $f(a) = f(b)$ atunci $(a, b) \in A$ şi $a = u(a, b) = v(a, b) = b$. Prin urmare, f este injectivă.
(ii) Evident, un morfism surjectiv de inele este epimorfism de inele, fiind chiar epimorfism de mulţimi.
Reciproc, arătăm că morfismul de inele $f : \mathbb{Z} \to \mathbb{Q}$ definit prin $f(x) = x$, $x \in \mathbb{Z}$, este epimorfism, dar în mod clar nu este surjectiv. Fie $u, v : \mathbb{Q} \to R$ morfisme unitare de inele (R fiind un inel unitar) astfel încât $uf = vf$. Conform problemei 4 din Capitolul 2, f este epimorfism de monoizi şi deci $u = v$. Rezultă că f este şi epimorfism de inele.

20. (i) Fie $e, f \in \text{Idemp}(R)$. Atunci

$$\begin{aligned}(e + f - 2ef)^2 &= e^2 + f^2 + 4e^2f^2 + 2ef - 4e^2f - 4ef^2 \\ &= e + f + 4ef + 2ef - 4ef - 4ef \\ &= e + f - 2ef,\end{aligned}$$

deci $e + f - 2ef$ este idempotent. Rezultă că $\text{Idemp}(R)$ este parte stabilă în raport cu "$*$".
• Pentru orice $e, f, g \in \text{Idemp}(R)$ avem

$$\begin{aligned}(e * f) * g &= (e + f - 2ef) * g \\ &= (e + f - 2ef) + g - 2(e + f - 2ef)g \\ &= e + f + g - 2ef - 2eg - 2fg + 4efg\end{aligned}$$

şi

$$\begin{aligned}e * (f * g) &= e + (f + g - 2fg) - 2e(f + g - 2fg) \\ &= e + f + g - 2fg - 2ef - 2eg + 4efg,\end{aligned}$$

deci "$*$" este asociativă.
• Pentru orice $e \in \text{Idemp}(R)$ avem $e * 0 = 0 * e = e$, deci 0 este element neutru pentru "$*$".
• Orice idempotent e are un invers $e * (1 - e) = (1 - e) * e = e$.
Prin urmare $(\text{Idemp}(R), *)$ este grup.

(ii) Observăm că $e * e = 0$ pentru orice $e \in \text{Idemp}(R)$, deci în acest grup orice element este de ordin 2. În ipoteza că $\text{Idemp}(R)$ este grup finit putem aplica rezultatul problemei 14(ii) din Capitolul 3 şi obţinem că există $n \in \mathbb{N}^*$ astfel încât $|\text{Idemp}(R)| = 2^n$.

21. (i) Avem $\phi_t(f+g) = (f+g)(t) = f(t) + g(t) = \phi_t(f) + \phi_t(g)$ şi $\phi_t(fg) = (fg)(t) = f(t)g(t) = \phi_t(f)\phi_t(g)$. Elementul identitate la înmulţire în inelul C este $u : [0,1] \to \mathbb{R}, u(t) = 1$ pentru orice $t \in [0,1]$. Atunci $\phi_t(u) = u(t) = 1$. Rezultă că ϕ_t este morfism de inele.
(ii) Fie $\phi : C \to \mathbb{R}$ un morfism unitar de inele. Presupunem prin absurd că $\phi \neq \phi_t$ pentru orice t. Atunci, pentru orice $t \in [0,1]$, există $f_t \in C$ cu $\phi(f_t) \neq \phi_t(f_t)$, deci $\phi(f_t) \neq f_t(t)$. Fie $g_t = f_t - \phi(f_t)u$. Avem $g_t \in C, \phi(g_t) = 0$ şi $g_t(t) \neq 0$. Cum g_t este continuă, există o vecinătate V_t a lui t astfel încât $g_t(x) \neq 0$ pentru orice $x \in V_t \cap [0,1]$. Dar $[0,1] \subseteq \bigcup_{t \in [0,1]} V_t$ şi cum [0,1] este compact, rezultă că există $t_1, \ldots, t_n$ astfel încât $[0,1] \subseteq V_{t_1} \cup \ldots \cup V_{t_n}$. Atunci avem $\sum_{i=1}^{n} g_{t_i}^2(x) \neq 0$ pentru orice $x \in [0,1]$, deoarece x aparţine unui V_{t_i}. Rezultă că $g = \sum_{i=1}^{n} g_{t_i}^2$ este inversabilă în C. Dar $\phi(g) = 0$, contradicţie.

22. (i) Fie $x, y \in u^{-1}(J)$. Atunci $u(x)$ şi $u(y)$ se găsesc în J, deci $u(x-y) = u(x) - u(y) \in J$, de unde $x - y \in u^{-1}(J)$.
Fie $a \in R, x \in u^{-1}(J)$. Atunci $u(x) \in J$, deci $u(ax) = u(a)u(x) \in J$. Prin urmare $ax \in u^{-1}(J)$.
(ii) Considerăm injecţia canonică $i : \mathbb{Z} \to \mathbb{Q}$, $i(x) = x$. Imaginea prin i a idealului $\mathbb{Z}$ este chiar $\mathbb{Z}$, care nu este însă ideal în $\mathbb{Q}$, pentru că, de exemplu, $\frac{1}{2} \cdot 1 \notin \mathbb{Z}$.
(iii) Evident.
(iv) Fie $x \in I$. Atunci $u(x) \in u(I) \subset I^e$, deci $x \in u^{-1}(I^e) = (I^e)^c$.
Considerând din nou injecţia canonică a lui $\mathbb{Z}$ în $\mathbb{Q}$ (vezi soluţia punctului (ii)), constatăm că $(\mathbb{Z}^e)^c = \mathbb{Q} \neq \mathbb{Z}$.
(v) Fie $y \in (J^c)^e$. Atunci, conform (iii), există $b_1, \ldots, b_n \in S$ şi $x_1, \ldots, x_n \in J^c$ astfel încât $y = \sum_{i=1}^{n} u(x_i)$. Cum $x_1, \ldots, x_n \in J^c$, $u(x_1), \ldots, u(x_n) \in J$, prin urmare, $y \in J$.
Considerăm acum injecţia canonică $j : \mathbb{Q} \to \mathbb{Q}[X]$,$j(a) = a$. Dacă punem $J = (X)$, atunci $J^c = (0)$, deci $(J^c)^e = (0) \neq J$.
(vi) Conform punctului (v), $((I^e)^c)^e \subset I^e$. Pentru incluziunea contrară să

considerăm $y \in I^e$. Atunci există $n \in \mathbb{N}^*$, $b_1, \ldots, b_n \in S$ şi $x_1, \ldots, x_n \in I$ astfel încât $y = \sum_{i=1}^{n} b_i u(x_i)$. Dar, conform punctului (iv), $I \subset (I^e)^c$, deci $x_1, \ldots, x_n \in (I^e)^c$. Prin urmare, $y \in ((I^e)^c)^e$.
(vii) Conform punctului (iv) avem că $J^c \subset ((J^c)^e)^c$. Fie acum $x \in ((J^c)^e)^c$. Atunci $u(x) \in (J^c)^e$, deci există $n \in \mathbb{N}^*$, $b_1, \ldots, b_n \in S$ şi $x_1, \ldots, x_n \in J^c$ astfel încât $u(x) = \sum_{i=1}^{n} b_i u(x_i)$. Cum însă $x_1, \ldots, x_n \in J^c$ implică $u(x_1), \ldots, u(x_n) \in J$, rezultă că $u(x) \in J$, deci $x \in J^c$.

23. (i) $\widehat{x} \in I^e$ dacă şi numai dacă există $\widehat{a_1}, \ldots, \widehat{a_n} \in \overline{R}$ şi $x_1, \ldots, x_n \in I$ astfel încât $\widehat{x} = \sum_{i=1}^{n} \widehat{a_i}\pi(x_i)$ (vezi problema 22(iii)). Această relaţie se rescrie $\widehat{x} = \sum_{i=1}^{n} \widehat{a_i}\widehat{x_i}$, iar această expresie este în mod evident în $\overline{I}\,\overline{R}$.
(ii) Dacă $\widehat{x} \in I^e$, atunci $\widehat{x}$ este de forma $\sum_{1=1}^{n} \widehat{\alpha_i}\pi(a_i) = \sum_{i=1}^{n} \widehat{\alpha_i a_i}$ (vezi problema 22(iii)), unde $\alpha_i \in R$, $a_i \in I$, pentru orice $i \in \{1, 2, 3, \ldots, n\}$. Cum $\alpha_i a_i \in I$ pentru orice $i \in \{1, 2, 3, \ldots, n\}$ şi $I \subset I + J$, avem $\widehat{x} \in (I + J)/J$.
Reciproc, fie $\widehat{x} \in (I + J)/J$. Atunci există $a \in I$ şi $b \in J$ astfel încât $\widehat{x} = \widehat{a + b} = \widehat{a} + \widehat{b}$. Cum $b \in J$, avem $\widehat{b} = \widehat{0}$, deci $\widehat{x} = \widehat{a} \in \overline{I} \subset I^e$.
(iii) Folosind (i) şi (ii),

$$\overline{R}/\overline{I}\,\overline{R} = \overline{R}/I^e = \frac{R/J}{(I + J)/J}.$$

Aplicând teorema a III-a de izomorfism pentru inele obţinem

$$\overline{R}/\overline{I}\,\overline{R} = \frac{R/J}{(I + J)/J} \simeq R/(I + J).$$

24. (i) Să presupunem că R este noetherian. Fie I un ideal al său. Considerăm un element $a_1 \in I$. Dacă $I = (a_1)$, atunci I este finit generat. Dacă $I \neq (a_1)$, fie $a_2 \in I \setminus (a_1)$. Dacă $I = (a_1, a_2)$, atunci I este finit generat. Dacă nu, putem găsi $a_3 \in I \setminus (a_1, a_2)$. Continuăm inductiv acest procedeu. Dacă la fiecare pas s-ar obţine $I \neq (a_1, \ldots, a_n)$, atunci am obţine şirul crescător de ideale $(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3) \subsetneq \cdots$ care nu este staţionar, contradicţie. Rămâne că există $n \in \mathbb{N}^*$ aşa încât $I = (a_1, \ldots, a_n)$. Prin urmare, I este finit generat.

Reciproc, fie un şir crescător $I_1 \subseteq I_2 \subseteq \cdots$ de ideale ale lui R. Considerăm $I = \bigcup_{k\in\mathbb{N}^*} I_k$. Dacă $x, y \in I$, atunci există $m, n \in \mathbb{N}^*$ aşa încât $x \in I_m$ şi $y \in I_n$. Atunci $x - y \in I_{\max\{m,n\}} \subseteq I$. Pentru $x \in I$ şi $a \in R$, dacă $x \in I_m$, atunci $ax \in I_m \subseteq I$. Prin urmare, I este ideal al lui R. Conform ipotezei, I trebuie să fie finit generat, să zicem $I = (a_1, \ldots, a_r)$. Există atunci $n_1, \ldots, n_r$ aşa încât $a_j \in I_{n_j}$. Dacă $n = \max\{n_1, \ldots, n_r\}$, atunci $I = (a_1, \ldots, a_r) \subseteq I_n \subseteq I_{n+1} \subseteq \cdots \subseteq I$, de unde $I_n = I_{n+1} = \cdots$ şi demonstraţia este încheiată.

(ii) "$\Rightarrow$" Se aplică punctul anterior.

"$\Leftarrow$" Presupunem că există ideale ale lui R care nu sunt finit generate. Notăm $\mathcal{M} = \{I \leq R \mid I \text{ nu este finit generat}\}$ şi observăm că $\mathcal{M} \neq \emptyset$. Considerăm pe $\mathcal{M}$ ordinea dată de incluziune. Fie $\mathcal{N}$ o parte total ordonată a lui $\mathcal{M}$. Definim $J = \bigcup_{I\in\mathcal{N}} I$. Dacă $x, y \in J$, atunci există $I_x, I_y \in \mathcal{N}$ aşa încât $x \in I_x$ şi $y \in I_y$. Presupunem $I_x \subset I_y$. Atunci $x - y \in I_y \subset J$. Pentru $x \in J$ şi $a \in R$, dacă $x \in I_x$, atunci $ax \in I_x \subset J$. Prin urmare, J este ideal al lui R. Idealul J nu poate fi finit generat, deoarece idealele din $\mathcal{N}$ care conţin toţi generatorii lui J ar fi şi ele finit generate. Prin urmare, $J \in \mathcal{N}$.

Aşadar, $\mathcal{N}$ este inductiv ordonată. Conform Lemei lui Zorn, $\mathcal{N}$ admite elemente maximale şi fie P unul dintre acestea. Presupunem că P nu este ideal prim. Atunci există $a, b \in R \setminus P$ astfel încât $ab \in P$. Notăm $P : a = \{x \in R \mid ax \in P\}$. Este imediat că $P : a$ este ideal al lui R. Observăm că $P \subseteq P : a$ şi că $b \in P : a$. Prin urmare, $P \subsetneq P : a$. Avem de asemenea $P \subsetneq P + (a)$. Deci $P : a$ şi $P + (a)$ sunt ideale finit generate ale lui R, să zicem $P : a = (c_1, \ldots, c_m)$ şi $P + (a) = (d_1, \ldots, d_n)$. Cum $d_j \in P + (a)$, există $u_j \in P$ şi $v_j \in R$, $j = \overline{1, n}$, astfel încât $d_j = u_j + av_j$.

Fie acum $x \in P$. Atunci $x \in P + (a)$, deci există $\lambda_1, \ldots, \lambda_n \in R$ astfel ca $x = \sum_{j=1}^{n} \lambda_j d_j = \sum_{j=1}^{n} \lambda_j u_j + a \sum_{j=1}^{n} \lambda_j v_j$. De aici rezultă că $a \sum_{j=1}^{n} \lambda_j v_j \in P$, deci $\sum_{j=1}^{n} \lambda_j v_j \in P : a$. Putem prin urmare găsi $\mu_1, \ldots, \mu_m \in R$ astfel ca $\sum_{j=1}^{n} \lambda_j v_j = \sum_{i=1}^{m} \mu_i c_i$. Înlocuind în expresia lui x, obţinem $x = \sum_{j=1}^{n} \lambda_j u_j + \sum_{i=1}^{m} \mu_i (ac_i)$. De aici rezultă că P este generat de $\{u_1, \ldots, u_n, ac_1, \ldots, ac_m\}$, contradicţie.

Rămâne că P este ideal prim în R. Dar $P \in \mathcal{N}$, deci P nu este finit generat, ceea ce contrazice ipoteza.

(iii) Fie R inel noetherian, I un ideal al său şi $\pi : R \to R/I$, $\pi(x) = \widehat{x}$

proiecţia canonică. Notăm $\overline{R} = R/I$. Fie J un ideal al lui $\overline{R}$. Atunci $\pi^{-1}(J)$ este ideal al lui R. Cum R este inel noetherian, $\pi^{-1}(J)$ este finit generat. Fie $x_1, \ldots, x_n$ un sistem de generatori al lui $\pi^{-1}(J)$. Să observăm că $\widehat{x_1}, \ldots, \widehat{x_n} \in J$, deci idealul generat de aceste elemente, pe care îl vom nota $(\widehat{x_1}, \ldots, \widehat{x_n})$, este inclus în J. Fie acum $\widehat{x} \in J$. Atunci, $x \in \pi^{-1}(J)$, deci există $a_1, \ldots, a_n \in R$ astfel încât $x = a_1x_1 + \cdots + a_nx_n$. De aici rezultă că $\widehat{x} = \widehat{a_1}\widehat{x_1} + \cdots + \widehat{a_n}\widehat{x_n}$. Prin urmare, $J \subseteq (\widehat{x_1}, \ldots, \widehat{x_n})$. Rezultă că $J = (\widehat{x_1}, \ldots, \widehat{x_n})$, deci J este ideal finit generat al lui $\overline{R}$. În concluzie, $\overline{R}$ este inel noetherian.

25. Se ţine seama de corespondenţa bijectivă dintre idealele lui R/I, unde R este un inel comutativ unitar şi I este un ideal al său, şi idealele lui R care conţin pe I, precum şi de corespondenţele bijective induse între mulţimea idealelor prime (respectiv maximale) ale lui R/I şi mulţimea idealelor prime (respectiv maximale) ale lui R care conţin pe I.
Fie $R = \mathbb{Z}_n$, unde $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ cu $p_1, \ldots, p_r$ numere prime diferite şi $\alpha_1, \ldots, \alpha_r \in \mathbb{N}^*$. Idealele lui $\mathbb{Z}_n$ sunt de forma $m\mathbb{Z}/n\mathbb{Z}$, unde m este un divizor natural al lui n. Rezultă că $\mathbb{Z}_n$ are $(1+\alpha_1)\cdots(1+\alpha_r)$ ideale. Cum în $\mathbb{Z}$ idealele prime nenule şi idealele maximale coincid, rezultă că idealele prime şi idealele maximale din $\mathbb{Z}_n$ coincid şi sunt de forma $p_i\mathbb{Z}/n\mathbb{Z}$, cu $i = 1, \ldots, r$, deci sunt în număr de r.

26. (i) Fie $p_i : R \to R_i$ proiecţia lui R pe componenta de pe poziţia i, pentru orice $i = 1, \ldots, n$. Dacă I este un ideal al lui R, notăm cu $I_i = p_i(I)$ care este un ideal în R_i (deoarece p_i este surjectivă). Evident $I \subseteq I_1 \times \cdots \times I_n$. Fie acum $\alpha = (a_1, \ldots, a_n) \in I_1 \times \cdots \times I_n$. Cum $a_i \in I_i$, rezultă că există $\beta_i \in I$ care are pe poziţia i chiar pe a_i. Notând cu e_i elementul lui R care are 1 pe poziţia i şi 0 în rest, se obţine că $e_i\beta_i \in I$ este elementul care are a_i pe poziţia i şi 0 în rest. Dar $\alpha = \sum_{i=1}^{n} \alpha_i\beta_i \in I$, deci $I = I_1 \times \cdots \times I_n$. Evident, orice mulţime de această formă este ideal al lui R.
(ii) Notăm cu $\pi_i : R_i \to R_i/I_i$ proiecţia canonică. Definim $f : R \to R_1/I_1 \times \cdots \times R_n/I_n$ prin $f(r_1, \ldots, r_n) = (\pi_1(r_1), \ldots, \pi_n(r_n))$. Evident f este morfism surjectiv de inele şi $\mathrm{Ker}(f) = I_1 \times \cdots \times I_n$. Aplicând teorema fundamentală de izomorfism se obţine izomorfismul cerut.
(iii) Fie $R = \prod_{j \in J} R_j$ un produs direct de inele unitare, unde J este o mulţime infinită. Fie I mulţimea tuturor elementelor lui R care au suportul finit

(adică doar un număr finit de componente nenule). Se verifică imediat că I este ideal al lui R. Dacă I ar fi produs direct de ideale, fie $I = \prod_{j\in J} I_j$, unde I_j este ideal în R_j pentru orice $j \in J$, atunci considerând elementul lui R care are 1 pe poziţia j şi 0 pe toate celelalte poziţii, acesta este în I, având suport finit, şi atunci ar rezulta că $1 \in I_j$, adică $I_j = R_j$. Obţinem $I = \prod_{j\in J} R_j = R$, ceea ce este o contradicţie, deoarece R conţine elemente de suport infinit.

27. (i) Fie $n, m \in \mathbb{N}^*$ astfel încât $I^n = 0$ şi $J^m = 0$. Arătăm că $(I + J)^{n+m} = 0$. Într-adevăr, dacă $x_1, \ldots, x_{n+m} \in I$ şi $y_1, \ldots, y_{n+m} \in J$ atunci $(x_1 + y_1) \cdots (x_{n+m} + y_{n+m})$ este o sumă de produse de câte $n + m$ elemente din $I \cup J$. Rezultă că în orice astfel de produs găsim n factori din I sau m factori din J. Cum R este inel comutativ, rezultă că orice astfel de produs este 0.
(ii) Dacă I este nilpotent, atunci evident orice element din I este nilpotent. Presupunem că orice element din I este nilpotent şi că I este generat de elementele $x_1, \ldots, x_p$. Fie $n \in \mathbb{N}$ astfel încât $x_i^n = 0$ pentru orice $i = 1, \ldots, p$. Dacă $r \in I$, atunci există $r_1, \ldots, r_p \in R$ cu $r = r_1x_1 + \ldots + r_px_p$. Atunci r^{np} este o sumă de produse de câte np factori de forma r_ix_i, deci în fiecare astfel de factor apare cel puţin un x_i la puterea n. Rezultă că orice astfel de produs este 0, deci $r^{np} = 0$.

Dacă I nu este finit generat afirmaţia nu mai este întotdeauna adevărată. De exemplu, în inelul $R = \prod_{n\geq 1} \mathbb{Z}_{p^n}$, p număr prim, idealul I, format din toate elementele de suport finit care pe orice poziţie au clasa unui multiplu de p (mod p^n), nu este nilpotent, dar orice element este nilpotent (explicaţia este că indicii de nilpotenţă ai elementelor din I pot fi oricât de mari).

28. Notând cu $p_1, \ldots, p_n$ proiecţiile canonice ale lui R pe $R/I_1, \ldots, R/I_n$ respectiv, morfismul ϕ se poate descrie prin $\phi(r) = (p_1(r), \ldots, p_n(r))$.
(i) Evident $\mathrm{Ker}(\phi) = \bigcap_{i=1}^{n} \mathrm{Ker}(p_i) = I_1 \cap \ldots \cap I_n$.
(ii) Presupunem că ϕ este surjectivă. Fie $j, k \in \{1, \ldots, n\}, j \neq k$. Pentru elementul $\alpha \in R/I_1 \times \cdots \times R/I_n$ care are $p_j(1)$ pe poziţia j şi $p_k(0)$ pe poziţia k există $r \in R$ astfel încât $\phi(r) = \alpha$, deci $p_j(r) = p_j(1)$ şi $p_k(r) = p_k(0)$. Rezultă că $r-1 \in I_j$ şi $r \in I_k$, de unde obţinem că $1 = r+(1-r) \in I_k+I_j$, deci I_k şi I_j sunt comaximale. Reciproc, presupunem că oricare două dintre idealele date sunt comaximale. Pentru a arăta că ϕ este surjectivă este suficient să arătăm că $(p_1(0), \ldots, p_i(1), \ldots, p_n(0)) \in \mathrm{Im}(\phi)$ pentru orice $i = 1, \ldots, n$.

Ţinând cont de faptul că pentru $j \neq i$ avem $I_i + I_j = R$, putem găsi $a_j \in I_i$ şi $b_j \in I_j$ astfel încât $a_j + b_j = 1$. Fie $r = \prod_{j \neq i} b_j = \prod_{j \neq i}(1 - a_j)$. Atunci $r \in I_j$ pentru $j \neq i$ şi $1 - r \in I_i$, deci $\phi(r) = (p_1(0), \ldots, p_i(1), \ldots, p_n(0))$.
(iii) Afirmaţia rezultă din (i), (ii) şi din teorema fundamentală de izomorfism.

29. (i) $\Rightarrow$ (ii) Fie M unicul ideal maximal al lui R. Atunci evident $M \subseteq R \setminus U(R)$. Dacă $a \in R \setminus U(R)$, atunci Ra este ideal propriu în R, deci este conţinut într-un ideal maximal, adică $Ra \subseteq M$. Rezultă că $R \setminus U(R) \subseteq M$ şi deci $R \setminus U(R) = M$ care este ideal.
(ii) $\Rightarrow$ (iii) Fie $a, b \in R$ cu $a + b \in U(R)$. Dacă $a, b \in R \setminus U(R)$, cum acesta este ideal rezultă că şi $a + b \in R \setminus U(R)$, contradicţie. Deci $a \in U(R)$ sau $b \in U(R)$.
(iii) $\Rightarrow$ (i) Arătăm că $R \setminus U(R)$ este ideal. Dacă $a, b \in R \setminus U(R)$, atunci conform (iii) rezultă că şi $a + b \in R \setminus U(R)$. Fie $a \in R \setminus U(R)$ şi $r \in R$. Dacă $ar \in U(R)$ rezultă $a, r \in U(R)$, contradicţie. Aşadar $ar \in R \setminus U(R)$.
Este evident că $R \setminus U(R)$ este ideal maximal şi că orice ideal propriu este conţinut în $R \setminus U(R)$, deci acesta este unicul ideal maximal.

30. Fie R un inel local şi e un idempotent în R. Din $e + (1 - e) = 1$ rezultă $e \in U(R)$ sau $1 - e \in U(R)$. Dar $e(1 - e) = 0$ şi unul dintre ele este inversabil, deci $e = 0$ sau $1 - e = 0$. Aşadar $e = 0$ sau $e = 1$.

31. Dacă $n = p^k$, p număr prim, conform problemei 25 inelul $\mathbb{Z}_n$ are un singur ideal maximal, deci este local. Reciproc, dacă $\mathbb{Z}_n$ este inel local, atunci nu are decât idempotenţii 0 şi 1. Dacă prin absurd n nu ar fi putere a unui număr prim, atunci ar exista $a, b \in R \setminus \{0, 1\}$ cu $n = ab$ şi $(a, b) = 1$. Fie $c, d \in \mathbb{Z}$ cu $ca + db = 1$ şi $e = \hat{c}\hat{a} \in \mathbb{Z}_n$. Atunci $e^2 = \hat{c}\hat{a}(1 - \hat{d}\hat{b}) = e - \hat{c}\hat{a}\hat{d}\hat{b} = e - \widehat{cdn} = e$, deci e este idempotent. Rezultă $e = \hat{0}$ sau $e = \hat{1}$. Dacă $e = \hat{0}$ atunci $n = ab | ac$, deci $b | c$ şi cum $ca + db = 1$ rezultă $b = 1$, contradicţie. Analog, dacă $e = \hat{1}$ rezultă $\hat{d}\hat{b} = \hat{0}$ şi apoi $a = 1$. Rezultă că n este putere a unui număr prim.

Observaţie. Putem da acum o altă demonstraţie problemei 9 observând că dacă $R = R_1 \times \cdots \times R_r$ este un produs direct de inele, atunci idempotenţii lui R sunt elementele de forma $(e_1, \ldots, e_r)$, unde fiecare e_i este idempotent în R_i. Fie $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Idealele $I_i = p_i^{\alpha_i}\mathbb{Z}$ sunt oricare două comaximale în $\mathbb{Z}$, iar $I_1 \cap \ldots \cap I_r = n\mathbb{Z}$. Folosind problema 28 obţinem $\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_r^{\alpha_r}}$. Fiecare dintre componentele acestui produs de inele este inel local, deci are

doar doi idempotenţi. Rezultă că $\mathbb{Z}_n$ are 2^r idempotenţi.

32. (i) Dacă $ab \in U(R)$, nu rezultă neapărat că $a, b \in U(R)$. De exemplu, fie V un spaţiu vectorial (peste un corp arbitrar) având o bază numărabilă $(e_n)_{n\geq 1}$ şi fie $R = \mathrm{End}_K(V)$ cu structura de inel dată de adunarea obişnuită a morfismelor de spaţii vectoriale şi compunerea morfismelor. Este imediat că R devine inel cu aceste operaţii. Fie $f, g \in R$ definite prin: $f(e_n) = e_{n+1}$ pentru orice $n \geq 1$, iar $g(e_n) = e_{n-1}$ pentru $n \geq 2$ şi $g(e_1) = 0$. Evident f nu este surjectivă iar g nu este injectivă, deci nu aparţin lui $U(R)$ care este format din toate automorfismele lui V. Pe de altă parte, $g \circ f$ este aplicaţia identică pe V, deci $g \circ f \in U(R)$.
(ii) Fie $a^n r = ra^n = 1$. Atunci $a(a^{n-1}r) = (ra^{n-1})a = 1$, deci a este inversabil la stânga şi la dreapta, de unde rezultă că a este inversabil.
(iii) Fie $ra = 1$ cu $r \in R$. Atunci $ara = a$, deci $(ar - 1)a = 0$ şi cum a nu este divizor al lui zero la dreapta rezultă $ar - 1 = 0$. Se obţine $ar = 1$ şi cum $ra = 1$ rezultă că a este inversabil.

33. Fie $R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a, b, c \in \mathbb{Z} \right\}$, inelul matricelor superior triunghiulare peste $\mathbb{Z}$ şi fie $x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Atunci $Rx = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| a \in \mathbb{Z} \right\}$, iar $xR = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a, b \in \mathbb{Z} \right\}$.

34. (i) Fie $R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a, b \in \mathbb{Z} \right\}$ care este un inel neunitar cu adunarea şi înmulţirea matricelor. Atunci $x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ este element identitate la stânga, dar nu este element identitate la dreapta în R.
(ii) Fie R un inel care are un unic element identitate la stânga, fie acesta $e \in R$. Atunci, dacă $a, b \in R$ avem $(e+ae-a)b = eb+aeb-ab = b+ab-ab = b$, deci $e + ae - a$ este element identitate la stânga. Rezultă $e + ae - a = e$, de unde se obţine $ae = a$ pentru orice $a \in R$, adică e este element identitate şi la dreapta.

35. (i) Dacă $r, s \in C_R(A)$ atunci $(r - s)a = ra - sa = ar - as = a(r - s)$

pentru orice $a \in A$, deci $r - s \in C_R(A)$. De asemenea, $(rs)a = rsa = ras = ars = a(rs)$ deci şi $rs \in C_R(A)$. Rezultă că $C_R(A)$ este subinel în R.
(ii) Evident, dacă $X \subseteq Y \subseteq R$ atunci $C_R(X) \supseteq C_R(Y)$. De asemenea, $X \subseteq C_R(C_R(X))$, deoarece pentru orice $x \in X$ şi $r \in C_R(X)$ avem $xr = rx$, deci $x \in C_R(C_R(X))$. Aplicând ultima relaţie pentru $X = C_R(A)$ rezultă $C_R(A) \subseteq C_R(C_R(C_R(A)))$. De asemenea $A \subseteq C_R(C_R(A))$ şi aplicând prima observaţie rezultă că $C_R(A) \supseteq C_R(C_R(C_R(A)))$, de unde se obţine egalitatea cerută.

36. Fie $a \in Z(R), a \neq 0$. Atunci RaR este ideal bilateral nenul al lui R, deci $RaR = R$. Rezultă că $Ra = aR = R$ (deoarece a comută cu toate elementele lui R), de unde se obţine că a este inversabil la stânga şi la dreapta, deci este inversabil. Mai mult, deoarece $a \in Z(R)$ rezultă că şi $a^{-1} \in Z(R)$, deci $Z(R)$ este corp.
Dacă R este comutativ, evident $Z(R) = R$.

37. Presupunem prin absurd că $y \notin Z(D)$. Atunci există $x \in D$ cu $yx \neq xy$. Are loc relaţia $x(xy) - (xy)x = x(xy - yx)$ şi cum $xy - yx$ este nenul, el este inversabil şi $x = [x(xy) - (xy)x](xy - yx)^{-1}$. Fie $C_R(y) = \{r \in R \mid ry = yr\}$. Cum y comută cu toţi comutatorii aditivi obţinem că $x(xy) - (xy)x, xy - yx \in C_R(y)$, de unde $(xy - yx)^{-1} \in C_R(y)$ şi deci $x \in C_R(y)$, contradicţie.

38. (i) Rezultă imediat prin calcul.
(ii) Fie $b \in K$. Arătăm că b comută cu toate elementele lui D. Fie $a \in D \setminus K$. Din relaţiile $\delta_a^2(b) = a^2b - 2aba + ba^2 \in K$ şi $\delta_{a^2}(b) = a^2b - ba^2 \in K$ se obţine prin adunare că $2(a^2b - aba) = 2a\delta_a(b) \in K$. Dacă $\delta_a(b) \neq 0$ rezultă $2\delta_a(b) \in K^*$ şi se obţine $a \in K$, contradicţie. Deci $\delta_a(b) = 0$, adică b comută cu elementele din $D \setminus K$.
Fie acum $c \in K^*$. Atunci a şi ac se găsesc în $D \setminus K$, deci din cele de mai sus ele comută cu b. Obţinem $(ac)b = b(ac) = (ba)c = abc$ şi înmulţind cu a^{-1} rezultă că $cb = bc$, deci b comută şi cu elementele din K. Rezultă $b \in Z(D)$, deci $K \subseteq Z(D)$.

39. Fie $c \in D$ un element care comută cu toţi comutatorii multiplicativi din D. Presupunem prin absurd că există $a \in D$ cu $ac \neq ca$ (echivalent, $a^{-1}cac^{-1} \neq 1$). Fie $b = a - 1 \in D^*$. Atunci $bc - cb = ac - ca \neq 0$, deci

$b^{-1}cbc^{-1} \neq 1$. Avem

$$\begin{aligned} a(a^{-1}cac^{-1} - b^{-1}cbc^{-1}) &= cac^{-1} - ab^{-1}cbc^{-1} \\ &= [c(b+1) - (b+1)b^{-1}cb]c^{-1} \\ &= (c - b^{-1}cb)c^{-1} \\ &= 1 - b^{-1}cbc^{-1} \\ &\neq 0. \end{aligned}$$

Din ipoteză c comută cu $a^{-1}cac^{-1}$ şi cu $b^{-1}cbc^{-1}$, de unde, folosind ultima relaţie, rezultă că c comută şi cu a, contradicţie.

40. Fie $c \in K$. Arătăm că c comută cu toate elementele lui D (putem considera $c \in K^*$). Fie $a \in D \setminus K$. Presupunem prin absurd că $ac \neq ca$, atunci notând $b = a - 1 \in D^*$ avem $bc - cb = ac - ca \neq 0$ ($\Leftrightarrow c \neq b^{-1}cb$). Avem $a(a^{-1}ca - b^{-1}cb) = ca - ab^{-1}cb = c(b+1) - (b+1)b^{-1}cb = c - b^{-1}cb \neq 0$ şi cum $a^{-1}ca, b^{-1}cb \in K^*$ rezultă că şi $a \in K^*$, ceea ce este o contradicţie. Deci c comută cu orice element $a \in D \setminus K$.
Fie acum $c' \in K^*$. Atunci $a, ac' \in D \setminus K$, deci c comută cu ele. Rezultă că c comută şi cu $a^{-1}ac' = c'$. Prin urmare, $c \in Z(D)$, deci $K \subseteq Z(D)$.

41. Cum $f \in R/I$, există $x \in R$ astfel încât $f = \hat{x}$. Din $\widehat{x^2} = \hat{x}$ rezultă $a = x^2 - x \in I \subseteq N(R)$, deci există $n \in \mathbb{N}^*$ astfel încât $a^n = 0$. Obţinem

$$\begin{aligned} 0 &= (x^2 - x)^n \\ &= \sum_{k=0}^{n} (-1)^k C_n^k x^{2k} x^{n-k} \\ &= \sum_{k=0}^{n} (-1)^k C_n^k x^{n+k} \\ &= x^n - x^{n+1} \sum_{k=1}^{n} (-1)^{k-1} C_n^k x^{k-1}. \end{aligned}$$

Notând $t = \sum_{k=1}^{n} (-1)^{k-1} C_n^k x^{k-1}$, avem că $x^n = x^{n+1}t$ şi $xt = tx$. Fie $e = x^n t^n$. Arătăm că e este idempotent şi că $f = \hat{e}$. Avem $e = x^n t^n = (x^{n+1}t)t^n = x^{n+1}t^{n+1} = (x^{n+2}t)t^{n+1} = x^{n+2}t^{n+2} = \ldots = x^{2n}t^{2n} = (x^n t^n)^2 = e^2$. De asemenea, $\hat{e} = (\hat{x}\hat{t})^n$ şi cum $\hat{x} = \widehat{x^{n+1}}$ se obţine $\hat{x}\hat{t} = \widehat{x^{n+1}}\hat{t} = \widehat{x^{n+1}t} = \widehat{x^n}$,

deci $\hat{e} = (\widehat{x^n})^n = \hat{x}^{n^2} = \hat{x} = f$, ceea ce era de demonstrat.

42. Fie $\hat{x} \in R/I$ cu $\hat{x}^2 = \hat{x}$. Rezultă $x^2 - x \in I$, deci $x^2 - x = a_1e_1 + \ldots + a_ne_n$ cu $a_i \in R$ şi $e_i \in P, e_i^2 = e_i$ pentru orice $1 \leq i \leq n$. Avem $(1-e_1)\cdots(1-e_n)(x^2-x) = 0$, deoarece pentru fiecare $i = 1, \ldots, n$, termenul a_ie_i este anulat de $1-e_i$. Acum o inducţie simplă după n ne conduce la concluzia că $(1-e_1)\ldots(1-e_n) = 1-e$ pentru un $e \in P, e^2 = e$ (pentru aceasta se observă că $(1-e_1)(1-e_2) = 1-e$ pentru $e = e_1 + e_2 - e_1e_2$ cu $e^2 = e$). Deci $(1-e)(x^2-x) = 0$. Pe de altă parte, $x^2 - x \in I \subseteq P \Rightarrow x \in P$ sau $1 - x \in P$.
Dacă $x \in P$, atunci $x - ex = x^2 - (ex)^2 = (x-ex)^2 \Rightarrow x - ex$ este un element idempotent al lui $P \Rightarrow x - ex \in I \Rightarrow \hat{x} = \hat{e}\hat{x} = \hat{0}$.
Dacă $1 - x \in P$, atunci se verifică uşor că $(1-x) - e(1-x) \in P$ este un element idempotent $\Rightarrow \hat{1} - \hat{x} = \hat{e}(\hat{1} - \hat{x}) = \hat{0} \Rightarrow \hat{x} = \hat{1}$.

43. (i) Vom arăta mai întâi că în inelul R avem $2 = 0$. Într-adevăr, $(-1)^2 = -1 \Rightarrow 1 = -1 \Rightarrow 1 + 1 = 0$. Deci $2x = 0$ pentru orice $x \in R$. Fie $x, y \in R$. Atunci $(x+y)^2 = x + y \Rightarrow x^2 + xy + yx + y^2 = x + y \Rightarrow xy + yx = 0 \Rightarrow xy = -yx \Rightarrow xy = yx$.
(ii) Fie $P \in \mathrm{Spec}(R)$. Există $M \in \mathrm{Max}(R)$ astfel încât $P \subseteq M$. Dacă $P \neq M$ atunci există $x \in M \setminus P$. Dar $x^2 = x \Rightarrow x(1-x) = 0 \in P \Rightarrow 1 - x \in P \Rightarrow 1 - x \in M \Rightarrow 1 \in M$, contradicţie. Deci $P = M \in \mathrm{Max}(R)$.
(iii) Pentru o mulţime X se verifică prin calcul că mulţimea părţilor sale $\mathcal{P}(X)$ are o structură de inel în raport cu diferenţa simetrică $A\Delta B = (A \setminus B) \cup (B \setminus A)$ (care joacă rolul adunării în $\mathcal{P}(X)$) şi intersecţia mulţimilor (care joacă rolul înmulţirii în $\mathcal{P}(X)$). Elementul nul al acestui inel este mulţimea vidă, iar elementul unitate este X. Mai mult, $A \cap A = A$ pentru orice $A \in \mathcal{P}(X)$, deci $(\mathcal{P}(X), \Delta, \cap)$ este inel Boole.
(iv) Fie R un inel Boole finit. Atunci $(R, +)$ este grup finit şi $2x = 0$ pentru orice $x \in R$. Aplicând problema 14(ii) din Capitolul 3, rezultă că există $n \in \mathbb{N}$ astfel încât $|R| = 2^n$. Dacă $n = 0$ sau $n = 1$, atunci este clar.
Dacă $n \geq 2$ vom arăta prin inducţie după n că există elementele $a_1, \ldots, a_n \in R \setminus \{0, 1\}$ cu proprietatea că $a_ia_j = 0$ pentru orice $i \neq j$.
Pentru $n = 2$ există $e \in R \setminus \{0, 1\}$ şi alegem $a_1 = e, a_2 = 1 - e$. Pentru $n > 2$ se consideră $e \in R \setminus \{0, 1\}$ şi se scrie $R = Re + R(1-e)$. Re şi $R(1-e)$ sunt inele Boole cu elementul unitate e, respectiv $1 - e$, iar $R \simeq Re \times R(1-e)$ deoarece $Re \cap R(1-e) = 0$. Dar $|Re| = 2^r$ şi $R(1-e) = 2^s$ cu $r + s = n$, iar din ipoteza de inducţie rezultă că există $b_1, \ldots, b_r \in Re$ astfel încât $b_ib_j = 0$ pen-

tru orice $i \neq j$ şi $c_1, \ldots, c_s \in R(1-e)$ astfel încât $c_k c_l = 0$ pentru orice $k \neq l$. Fie acum $a_1 = b_1, \ldots, a_r = b_r, a_{r+1} = c_1, \ldots, a_n = c_n$ şi cum $e(1-e) = 0$ vom avea $a_i a_j = 0$ pentru orice $i \neq j$.
Arătăm acum că mulţimea tuturor sumelor $a_{i_1} + \ldots + a_{i_k}$, cu $1 \leq i_1 < \ldots < i_k \leq n$, are 2^n elemente, deci coincide cu R, de unde rezultă că pentru orice $x \in R$ există şi sunt unice $1 \leq i_1 < \ldots < i_s \leq n$ cu proprietatea că $x = a_{i_1} + \ldots + a_{i_s}$. Este suficient să arătăm că dacă avem $1 \leq j_1 < \ldots < j_s \leq n$ şi $1 \leq k_1 < \ldots < k_t \leq n$, atunci $a_{j_1} + \ldots + a_{j_s} = a_{k_1} + \ldots + a_{k_t} \Leftrightarrow s = t$ şi $j_1 = k_1, \ldots, j_s = k_s$. Aceasta se demonstrează arătând că $j_1, \ldots, j_s \in \{k_1, \ldots, k_t\}$ şi $k_1, \ldots, k_t \in \{j_1, \ldots, j_s\}$. Dacă, de exemplu, $j_1 \notin \{k_1, \ldots, k_t\}$, atunci din $a_{j_1}(a_{j_1} + \ldots + a_{j_s}) = a_{j_1}(a_{k_1} + \ldots + a_{k_t})$ rezultă că $a_{j_1}^2 + \ldots + a_{j_1}a_{j_s} = a_{j_1}a_{k_1} + \ldots + a_{j_1}a_{k_t} \Rightarrow a_{j_1} = 0$, contradicţie.
Va fi suficient să considerăm acum aplicaţia $f : R \to (\mathcal{P}(\{1, \ldots, n\}), \Delta, \cap)$ definită prin $f(x) = \{i_1, \ldots, i_s\}$, unde $x = a_{i_1} + \ldots + a_{i_s}$, care este izomorfism.
(v) Fie $\mathcal{P}_f(X)$ mulţimea părţilor finite ale lui X şi $\mathcal{P}_{cf}(X)$ mulţimea părţilor lui X care au complementara finită. Este uşor de verificat că $\mathcal{P}_f(X) \cup \mathcal{P}_{cf}(X)$ este subinel unitar al inelului Boole $(\mathcal{P}(X), \Delta, \cap)$. Folosind problema 31(c) din Capitolul 1 rezultă că $|\mathcal{P}_f(X)| = |X|$. Este clar că aplicaţia care duce o mulţime în complementara ei defineşte o bijecţie între $\mathcal{P}_f(X)$ şi $\mathcal{P}_{cf}(X)$, de unde $|\mathcal{P}_{cf}(X)| = |\mathcal{P}_f(X)|$. Atunci $|\mathcal{P}_f(X) \cup \mathcal{P}_{cf}(X)| = |\mathcal{P}_{cf}(X)| + |\mathcal{P}_f(X)| = |X| + |X| = |X|$. Rezultă că există o bijecţie între $\mathcal{P}_f(X) \cup \mathcal{P}_{cf}(X)$ şi X. Transportând structura de inel Boole a lui $\mathcal{P}_f(X) \cup \mathcal{P}_{cf}(X)$ prin această bijecţie, obţinem că există o structură de inel Boole pe X.

44. (i) Este imediat că $N(R) \subseteq \bigcap\{P \mid P \text{ ideal prim}\}$, deoarece dacă $x \in N(R)$, există $n \in \mathbb{N}$ astfel încât $x^n = 0 \in P$ pentru orice ideal prim P, deci $x \in P$.
Reciproc, fie $x \in \bigcap\{P \mid P \text{ ideal prim}\}$. Să presupunem că $x \notin N(R)$. Considerăm $S = \{1, x, x^2, x^3, \ldots\}$ şi

$$\mathcal{F} = \{\ I \mid I \text{ ideal în } R \text{ şi } I \cap S = \emptyset\}.$$

Atunci $\mathcal{F}$ este inductiv ordonată deoarece orice parte total ordonată $(I_\alpha)_{\alpha \in A}$, cu $I_\alpha \cap S = \emptyset$ pentru orice $\alpha \in A$, are un majorant $\bigcup_{\alpha \in A} I_\alpha \in \mathcal{F}$. Atunci, conform lemei lui Zorn, $\mathcal{F}$ are elemente maximale. Fie $J \in \mathcal{F}$ element maximal. Atunci J este ideal prim deoarece, dacă nu ar fi prim ar exista $a, b \in R$ astfel încât $ab \in J$ şi $a \notin J, b \notin J \Rightarrow J \subset J + (a)$ şi $J \subset J + (b) \Rightarrow (J + (a)) \cap S \neq \emptyset$ şi $(J + (b)) \cap S \neq \emptyset \Rightarrow$ există $m, n \in \mathbb{N}$ astfel încât $x^m \in J + (a)$ şi $x^n \in J + (b)$

$\Rightarrow x^{m+n} \in (J+(a))(J+(b)) \subseteq J \Rightarrow x^{m+n} \in J \cap S \Rightarrow J \cap S \neq \emptyset$, contradicţie. Am arătat deci că există ideale prime P cu proprietatea că $P \cap S = \emptyset$, ceea ce contrazice alegerea lui x.
(ii) Să presupunem că $x + u$ nu ar fi element inversabil. Atunci există $P \in \mathrm{Spec}(R)$ astfel încât $x + u \in P$. Dar x este nilpotent $\Rightarrow x \in P \Rightarrow u = (x + u) - x \in P \Rightarrow u$ nu este inversabil, contradicţie.
(iii) Fie $x \in J(R)$ şi $a \in R$. Dacă $1 - ax \notin U(R)$ atunci există $M \in \mathrm{Max}(R)$ astfel încât $1 - ax \in M$. Dar $x \in J(R) \Rightarrow x \in M \Rightarrow ax \in M$ şi cum $1 - ax \in M$ rezultă $1 \in M$, contradicţie. Reciproc, fie $x \in R$ şi $1 - ax \in U(R)$ pentru orice $a \in R$ şi fie $M \in \mathrm{Max}(R)$. Dacă $x \notin M$ atunci $M \subset M + (x) \Rightarrow M + (x) = R \Rightarrow$ există $a \in R$ astfel încât $1 - ax \in M \Rightarrow 1 - ax \notin U(R)$, fals.
(iv) Pentru $R = \mathbb{Z}$ avem $N(R) = J(R) = 0$. Pe de altă parte, dacă R este un inel local cu proprietatea că $\mathrm{Spec}(R) \neq \mathrm{Max}(R)$ (de exemplu, pentru $R = K[[X]]$, după cum rezultă din descrierea idealelor lui R dată în problema 31 din Capitolul 5), atunci $N(R) \neq J(R)$.

45. Să observăm mai întâi că un produs direct finit de inele comutative unitare este inel integru dacă şi numai dacă are un singur termen nenul şi acela este inel integru.
(i) "$\Rightarrow$" Fie P ideal prim al lui R. Rezultă că există $I_1 \leq R_1, \ldots, I_n \leq R_n$ astfel încât $P = I_1 \times \cdots \times I_n$. Cum P este ideal prim, R/P este integru, prin urmare $R_1/I_1 \times \cdots \times R_n/I_n$ este inel integru, deci există un unic $1 \leq i \leq n$ astfel încât $R_i/I_i \neq 0$ şi acesta este inel integru. Rezultă $I_j = R_j$ pentru orice $j \neq i$ şi I_i este ideal prim în R_i.
"$\Leftarrow$" Dacă $P = R_1 \times \cdots \times R_{i-1} \times P_i \times R_{i+1} \times \cdots \times R_n$, atunci $R/P \simeq R_i/P_i$, de unde rezultă că R/P este inel integru, deci P este ideal prim.
(ii) Analog cu (i).
(iii) Rezultă din (i) şi (ii).

46. Idealele lui $\mathbb{Z}_{20}$ sunt $(0), \hat{2}\mathbb{Z}_{20}, \hat{4}\mathbb{Z}_{20}, \hat{5}\mathbb{Z}_{20}, \widehat{10}\mathbb{Z}_{20}, \mathbb{Z}_{20}$. Cum $\mathbb{Q}$ şi $\mathbb{Z}_{19}$ sunt corpuri, ele au ca ideale doar pe (0) şi pe ele însele. Deci R va avea 24 de ideale formate din produsele directe ale idealelor de mai sus. Cum $\mathrm{Spec}(\mathbb{Z}_{20}) = \mathrm{Max}(\mathbb{Z}_{20}) = \{\hat{2}\mathbb{Z}_{20}, \hat{5}\mathbb{Z}_{20}\}$ rezultă că $\mathrm{Spec}(R) = \mathrm{Max}(R) = \{\hat{2}\mathbb{Z}_{20} \times \mathbb{Q} \times \mathbb{Z}_{19}, \hat{5}\mathbb{Z}_{20} \times \mathbb{Q} \times \mathbb{Z}_{19}, \mathbb{Z}_{20} \times (0) \times \mathbb{Z}_{19}, \mathbb{Z}_{20} \times \mathbb{Q} \times (0)\}$. Inelele factor sunt izomorfe cu unul dintre inelele $0, \mathbb{Z}_{10}, \mathbb{Z}_5, \mathbb{Z}_4, \mathbb{Z}_2, \mathbb{Z}_{20}$ sau cu produsele directe dintre unul din acestea şi unul dintre inelele $\mathbb{Q}, \mathbb{Z}_{19}, \mathbb{Q} \times \mathbb{Z}_{19}$.
$J(R) = N(R) = N(\mathbb{Z}_{20}) \times N(\mathbb{Q}) \times N(\mathbb{Z}_{19}) = \widehat{10}\mathbb{Z}_{20} \times (0) \times (0)$ şi $\mathrm{Idemp}(R) =$

$\text{Idemp}(\mathbb{Z}_{20}) \times \text{Idemp}(\mathbb{Q}) \times \text{Idemp}(\mathbb{Z}_{19}) = \{\hat{0}, \hat{1}, \hat{5}, \widehat{16}\} \times \{0, 1\} \times \{\hat{0}, \hat{1}\}$.

47. (i) Fie $a, b \in \text{Rad}(I)$. Atunci există $m, n \in \mathbb{N}^*$ cu $a^m \in I$ şi $b^n \in I$. Atunci $(a+b)^{m+n} = \sum_{0 \leq i \leq m+n} C_{m+n}^i a^{m+n-i} b^i$ şi cum pentru orice $0 \leq i \leq m+n$ avem $i \geq n$ sau $m + n - i \geq m$, rezultă că toţi termenii sumei din membrul drept sunt în I, deci $(a+b)^{m+n} \in I$, de unde $a + b \in \text{Rad}(I)$.
Dacă $a \in \text{Rad}(I)$, să zicem că $a^m \in I$, şi $r \in R$, atunci $(ra)^m = r^m a^m \in I$, deci $ra \in \text{Rad}(I)$.
În concluzie $\text{Rad}(I)$ este ideal al lui R. Din definiţie este clar că $I \subseteq \text{Rad}(I)$.
(ii) $\hat{a} \in N(R/I) \Leftrightarrow$ există $n \in \mathbb{N}$ astfel încât $\hat{a}^n = \hat{0} \Leftrightarrow$ există $n \in \mathbb{N}$ astfel încât $a^n \in I \Leftrightarrow a \in \text{Rad}(I) \Leftrightarrow \hat{a} \in \text{Rad}(I)/I$.
(iii) Avem $N(R/I) = \bigcap\{Q \mid Q \in \text{Spec}(R/I)\}$. Pe de altă parte, $Q \in \text{Spec}(R/I) \Leftrightarrow$ există $P \in \text{Spec}(R), I \subseteq P$ astfel încât $Q = P/I$, deci $N(R/I) = \bigcap\{P/I \mid P \in \text{Spec}(R), I \subseteq P\}$. Aşadar, $\text{Rad}(I)/I = N(R/I) = (\bigcap\{P \mid P \in \text{Spec}(R), I \subseteq P\})/I$, de unde obţinem că $\text{Rad}(I) = \bigcap\{P \mid P \in \text{Spec}(R), I \subseteq P\}$.
(iv) Este clar din definiţie că dacă $I_1 \subseteq I_2$, atunci $\text{Rad}(I_1) \subseteq \text{Rad}(I_2)$.
Cum $I \subseteq \text{Rad}(I)$, obţinem că $\text{Rad}(I) \subseteq \text{Rad}(\text{Rad}(I))$. Pentru a demonstra incluziunea inversă, fie $a \in \text{Rad}(\text{Rad}(I))$. Atunci există $n > 0$ cu $a^n \in \text{Rad}(I)$, deci există $m > 0$ cu $(a^n)^m \in I$. Aceasta arată că $a^{mn} \in I$, de unde $a \in \text{Rad}(I)$.
(v) Cum $IJ \subseteq I \cap J$, este clar că avem $\text{Rad}(IJ) \subseteq \text{Rad}(I \cap J) \subseteq \text{Rad}(I) \cap \text{Rad}(J)$. Fie acum $a \in \text{Rad}(I) \cap \text{Rad}(J)$. Atunci există $m, n > 0$ cu $a^m \in I$ şi $a^n \in J$. Atunci $a^{m+n} = a^m a^n \in IJ$, deci $a \in \text{Rad}(IJ)$. Rezultă că $\text{Rad}(I) \cap \text{Rad}(J) \subseteq \text{Rad}(IJ)$, de unde $\text{Rad}(IJ) = \text{Rad}(I \cap J) = \text{Rad}(I) \cap \text{Rad}(J)$.
Cum $I + J \subseteq \text{Rad}(I) + \text{Rad}(J)$, rezultă că $\text{Rad}(I + J) \subseteq \text{Rad}(\text{Rad}(I) + \text{Rad}(J))$. Pentru incluziunea inversă, fie $a \in \text{Rad}(\text{Rad}(I) + \text{Rad}(J))$, deci există $n > 0$ cu $a^n \in \text{Rad}(I) + \text{Rad}(J)$. Există atunci $u \in \text{Rad}(I)$ şi $v \in \text{Rad}(J)$ cu $a^n = u + v$. Fie $m, p > 0$ cu $u^m \in I$ şi $v^p \in J$. Atunci $a^{n(m+p)} = (u+v)^{m+p} = \sum_{0 \leq i \leq m+p} C_{m+p}^i u^{m+p-i} v^i$, şi cum pentru orice $0 \leq i \leq m+p$ avem $m+p-i \geq m$ sau $i \geq p$, rezultă că orice termen al ultimei sume este sau în I sau în J, de unde $a^{n(m+p)} \in I+J$, ceea ce arată că $a \in \text{Rad}(I+J)$.

48. Presupunem că $|\text{Max}(R)| < \infty$. Rezultă că intersecţia tuturor idealelor maximale $J(R) \neq 0$, deoarece idealele maximale ale lui R sunt nenule (pentru că R nu este corp) şi produsul acestora (care este conţinut în $J(R)$)

este nenul pentru că R este inel integru.
Fie acum $x \in J(R), x \neq 0$ şi definim $f : R \to U(R)$ prin $f(a) = 1-ax$ pentru orice $a \in R$. Este clar că f este bine definită, deoarece $x \in J(R) \Rightarrow 1-ax \in U(R)$ pentru orice $a \in R$ (conform problemei 43). Arătăm că f este injectivă. Pentru $a, b \in R$ avem $f(a) = f(b) \Leftrightarrow 1-ax = 1-bx \Leftrightarrow (a-b)x = 0 \Rightarrow a = b$. Deci $|R| \leq |U(R)| \Rightarrow |R| \leq \infty$, contradicţie.

49. (i) Fie $I \leq R = d\mathbb{Z}/n\mathbb{Z} \Rightarrow I$ este subgrup al lui $(R, +) \Rightarrow$ există $k \in \mathbb{N}, k|m$ astfel încât $I = kd\mathbb{Z}/n\mathbb{Z}$. Reciproc, este imediat că dacă I este de forma din enunţ atunci I este ideal al lui R.
(ii) Fie $P \in \mathrm{Spec}(R)$. Atunci există $k \in \mathbb{N}, k|m$ cu proprietatea că $P = kd\mathbb{Z}/n\mathbb{Z}$. Avem $k \neq 0$ deoarece $(\hat{0})$ nu este ideal prim al lui R. Într-adevăr, dacă $(\hat{0})$ ar fi ideal prim, cum m nu este număr prim, avem $m = ab$, cu $a, b \in \mathbb{N} \setminus \{0, 1\}$, şi din $(\widehat{da})(\widehat{db}) = \widehat{dn} = \hat{0}$ ar rezulta $\widehat{da} = \hat{0}$ sau $\widehat{db} = \hat{0}$, fals. Presupunem, prin absurd, că numărul k nu este prim. Rezultă că există $r, s \in \mathbb{N} \setminus \{0, 1\}$ astfel încât $k = rs$. Atunci avem $(\widehat{dr})(\widehat{ds}) = \widehat{d^2k} \in P$, de unde rezultă $\widehat{dr} \in P$ sau $\widehat{ds} \in P$. Dacă $\widehat{dr} \in P$ atunci există $x \in \mathbb{Z}$ astfel încât $\widehat{dr} = \widehat{kdx}$. Rezultă $n|d(r - kx)$, deci $m|r - kx$, şi cum $k|m$ se obţine $k|r$, deci $r = 1$, contradicţie. În acelaşi mod se obţine o contradicţie în cazul în care $\widehat{ds} \in P$. Deci k este număr prim.
Să presupunem acum $k|d \Rightarrow d = kt$ pentru un $t \in \mathbb{Z} \Rightarrow \widehat{d^2} = \widehat{dkt} \in P \Rightarrow \hat{d} \in P \Rightarrow$ există $y \in \mathbb{Z}$ astfel încât $\hat{d} = \widehat{kdy} \Rightarrow n|d - kdy \Rightarrow m|1 - ky$, şi cum $k|m$ rezultă $k|1$, fals. Deci k nu divide pe d.
Reciproc, fie $P = pd\mathbb{Z}/n\mathbb{Z}$, cu p număr prim, $p|m$ şi p nu divide pe d. Fie $\hat{a}, \hat{b} \in R$ astfel încât $\hat{a}\hat{b} \in P$. Rezultă că există $x, y, z \in \mathbb{Z}$ astfel încât $\hat{a} = \widehat{dx}$, $\hat{b} = \widehat{dy}$ şi $\widehat{d^2xy} = \widehat{pdz}$. Obţinem $n|d^2xy - pdz$, deci $m|dxy - pz$, şi cum $p|m$ rezultă că $p|dxy \Rightarrow p|xy \Rightarrow p|x$ sau $p|y$, ceea ce înseamnă că $\hat{a} \in P$ sau $\hat{b} \in P$.
(iii) Fie $M \in \mathrm{Max}(R)$. Atunci există $k \in \mathbb{N}, k|m$ astfel încât $M = kd\mathbb{Z}/n\mathbb{Z}$. Dacă, prin absurd, k nu ar fi număr prim atunci există $r, s \in \mathbb{N} \setminus \{0, 1\}$ astfel încât $k = rs$; rezultă $kd\mathbb{Z} \subset rd\mathbb{Z} \subset d\mathbb{Z}$, deci $M \subset rd\mathbb{Z}/n\mathbb{Z} \subset d\mathbb{Z}/n\mathbb{Z} = R$, contradicţie.
Reciproc, să considerăm $M = pd\mathbb{Z}/n\mathbb{Z}$, cu p număr prim şi $p|m$. Fie $I \leq R, I \neq R$ astfel încât $M \subseteq I$; rezultă că există $k \in \mathbb{N} \setminus \{0, 1\}$ astfel încât $I = kd\mathbb{Z}/n\mathbb{Z}$ şi $pd\mathbb{Z} \subseteq kd\mathbb{Z} \Rightarrow k|p \Rightarrow k = p \Rightarrow I = M$. Deci $M \in \mathrm{Max}(R)$.

50. Se rezolvă asemănător cu problema 49.

51. Fie $R = (\mathbb{Q}, +, *)$, unde multiplicarea se defineşte astfel: $x * y = 0$ pentru orice $x, y \in \mathbb{Q}$. Se obţine astfel un inel neunitar. Idealele lui R coincid cu subgrupurile lui $(\mathbb{Q}, +)$ şi cum acest grup nu are subgrupuri maximale (a se vedea problema 37 din Capitolul 3), rezultă că inelul R nu are ideale maximale.

Observaţie. În problema 30 din Capitolul 5 vom da un exemplu de astfel de inel care va fi chiar integru.

52. Notăm $A = A_1 \times \cdots \times A_m$ şi $B = B_1 \times \cdots \times B_n$. Să observăm că $x = (x_1, \ldots, x_m) \in \text{Idemp}(A) \Leftrightarrow x_i \in \text{Idemp}(A_i)$ pentru orice $i = 1, \ldots, m$ $\Leftrightarrow x_i = 0$ sau $x_i = 1$ pentru orice $i = 1, \ldots, m$.
Presupunem $A \simeq B$. Atunci $|\text{Idemp}(A)| = |\text{Idemp}(B)| \Rightarrow 2^m = 2^n \Rightarrow m = n$.
Fie acum $f : A \to B$ izomorfism de inele. Pentru fiecare $i = 1, \ldots, n$ fie $e_i \in A$ (respectiv $f_i \in B$) elementul care are 1 (elementul unitate al inelului A_i, respectiv B_i) pe poziţia i şi 0 în rest. Observăm că $e_i \in \text{Idemp}(A)$ şi $e_i e_j = 0$ pentru orice $i \neq j$. Rezultă că $f(e_i) \in \text{Idemp}(B) \setminus \{0\}$ şi $f(e_i)f(e_j) = 0$ pentru orice $i \neq j$. Deci $f(e_i)$ are pe fiecare componentă 0 sau 1. Atunci $f(e_i)f(e_j) = 0 \Leftrightarrow \text{supp}(f(e_i)) \cap \text{supp}(f(e_j)) = \emptyset$, unde prin $\text{supp}(x)$ s-a notat suportul elementului $x = (x_1, \ldots, x_n)$, definit ca $\text{supp}(x) = \{i \mid 1 \leq i \leq n,\ x_i \neq 0\}$. Avem $|\text{supp}(f(e_i))| \geq 1$ pentru orice $i = 1, \ldots, n$. Rezultă $|\bigcup_{i=1}^{n} \text{supp}(f(e_i))| = \sum_{i=1}^{n} |\text{supp}(f(e_i))| \geq n$. Dar $\bigcup_{i=1}^{n} \text{supp}(f(e_i)) \subseteq \{1, \ldots, n\}$ implică $|\bigcup_{i=1}^{n} \text{supp}(f(e_i))| \leq n$. Deci $|\text{supp}(f(e_i))| = 1$ pentru orice $i = 1, \ldots, n$. Rezultă că există $\sigma \in S_n$ astfel încât $f(e_i) = f_{\sigma(i)}$ pentru orice $i = 1, \ldots, n$. Dar $e_i A \simeq A_i$ iar $f_{\sigma(i)} B \simeq B_{\sigma(i)}$ şi cum $f(e_i A) = f_{\sigma(i)} B$ rezultă că $A_i \simeq B_{\sigma(i)}$ pentru orice $i = 1, \ldots, n$.

53. Vom arăta că dacă $[K^* : k^*] = n$, atunci $|k| \leq n + 1$. Să presupunem $|k| > n + 1$. Atunci $|k^*| > n$. Fie $x \in K^* \setminus k^*$. Considerând elementele de forma $1 + \alpha x$, $\alpha \in k^*$, care sunt cel puţin în număr de $n + 1$, există două astfel de elemente care se află în aceeaşi clasă modulo k^*, deoarece în K^* există n clase modulo k^*. Deci există $\alpha, \beta \in k^*, \alpha \neq \beta$, astfel încât $1 + \alpha x, 1 + \beta x \in k^* y$ pentru un $y \in K^*$. Atunci $(\alpha - \beta)x \in k^* y \Rightarrow \alpha - \beta \in k^*(yx^{-1}) \cap k^* \Rightarrow yx^{-1} \in k^* \Rightarrow$ există $\gamma \in k^*$ astfel încât $y = \gamma x$. Cum $1 + \alpha x \in k^* y$ se obţine $1 + \alpha x \in k^* x$, de unde rezultă $1 \in k^* x$, deci $x \in k^*$,

contradicţie.

54. Presupunem $K = K_1 \cup \ldots \cup K_n$, unde $K_1, \ldots, K_n$ sunt subcorpuri proprii ale lui K, $n \geq 2$.
Dacă corpul K este finit, atunci $(K^*, \cdot)$ este grup ciclic, deci există $x \in K^*$ astfel încât $K^* = < x >$, de unde rezultă că există $1 \leq i \leq n$ astfel încât $K = K_i$, fals.
Deci putem presupune că corpul K este infinit. Vom arăta că $|\bigcap_{i=1}^{n} K_i| \leq n$. Presupunem prin absurd că $|\bigcap_{i=1}^{n} K_i| > n$. Atunci, considerând $x \in K_1 \setminus \bigcup_{i \neq 1} K_i$ şi $y \in K_2 \setminus \bigcup_{i \neq 2} K_i$ arbitrar fixate, mulţimea $\{x + ay \mid a \in \bigcap_{i=1}^{n} K_i, a \neq 0\} \subseteq K$ are cel puţin n elemente, deci există $1 \leq i \leq n$ şi $a, b \in \bigcap_{i=1}^{n} K_i, a \neq b$, astfel încât $x + ay, x + by \in K_i$. Rezultă $(a - b)y \in K_i$, deci $y \in K_i$, ceea ce înseamnă că $i = 2$, deci $x + ay \in K_2$, de unde obţinem $x \in K_2$, contradicţie cu alegerea lui x. Aşadar, $|\bigcap_{i=1}^{n} K_i| \leq n$.
Pe de altă parte, vom arăta că $|\bigcap_{i=1}^{n} K_i| = \infty$. Deoarece K este infinit, cel puţin unul dintre corpurile $K_1, \ldots, K_n$ este infinit, să presupunem (printr-o eventuală renumerotare) că corpul K_1 este infinit. Fie şirul $(a_n)_{n \geq 1} \subseteq K_1$ şi fie $\alpha \in K \setminus K_1$, atunci $\alpha + a_n \notin K_1$ pentru orice $n \in \mathbb{N}^*$. Rezultă că există $2 \leq i \leq n$ astfel încât K_i conţine o infinitate de termeni ai şirului $(\alpha + a_n)_{n \geq 1}$. Să presupunem $i = 2$, deci K_2 are această proprietate. Deci există un subşir $(a_{n_k})_{k \geq 1}$ al şirului $(a_n)_{n \geq 1}$ cu proprietatea că $a_{n_k} - a_{n_1} \in K_1 \cap K_2$ (deoarece $a_{n_k} - a_{n_1} = (a_{n_k} + \alpha) - (a_{n_1} + \alpha) \in K_2$) pentru orice $k \in \mathbb{N}^*$. Renotând, rezultă că există un şir $(b_n)_{n \geq 1}$ cu proprietatea că $b_n \in K_1 \cap K_2$ pentru orice $n \in \mathbb{N}^*$. Acum vom considera $\beta \in K \setminus (K_1 \cup K_2) \Rightarrow \beta + b_n \notin K_1 \cup K_2$ pentru orice $n \in \mathbb{N}^* \Rightarrow$ există $3 \leq i \leq n$ astfel încât K_i conţine o infinitate de termeni ai şirului $(\beta + b_n)_{n \geq 1}$. Să presupunem că $i = 3$, deci K_3 are această proprietate. Obţinem acum un şir $(c_n)_{n \geq 1}$ cu proprietatea că $c_n \in K_1 \cap K_2 \cap K_3$ pentru orice $n \in \mathbb{N}^*$. Procedând ca mai sus vom găsi în final un şir care are toţi termenii în $K_1 \cap \ldots \cap K_n$, deci $|K_1 \cap \ldots \cap K_n| = \infty$.
Astfel am obţinut o contradicţie.

55. Să presupunem, prin absurd, că pentru orice $x, y \in K$ există $a \in K$

astfel încât $x^2 + y^2 = a^2$ şi să considerăm $L = \{x^2 \mid x \in K\} \subseteq K$. Se observă că L este subcorp al lui K deoarece $x^2 - y^2 = x^2 + 2y^2 = x^2 + a^2y^2 = x^2 + (ay)^2 \in L$, unde $a \in K$ astfel încât $2 = a^2$. Deoarece K este corp finit de caracteristică 3, atunci există $n \in \mathbb{N}^*$ şi $x \in K^*$ cu proprietatea că $|K| = 3^n$ şi $K^* = < x >$. Cum $\text{ord}(x) = 3^n - 1$ rezultă că $\text{ord}(x^2) = (3^n - 1)/(2, 3^n - 1) = (3^n - 1)/2$. Este imediat că $L \neq K$ (deoarece aplicaţia $\phi : K \to K, \phi(x) = x^2$ pentru orice $x \in K$, nu este injectivă, deci nu poate fi nici surjectivă). Apoi, cum $x^2 = y^2 \Leftrightarrow x = y$ sau $x = -y$ rezultă că $[K^* : L^*] = 2$. Deci $|K^*| = 2|L^*|$ şi cum L este şi el corp finit de caracteristică 3, există $r \in \mathbb{N}^*$ astfel încât $|L| = 3^r$, deci $|L^*| = 3^r - 1$. Obţinem că $3^n - 1 = 2(3^r - 1)$, de unde $3^n + 1 = 2 \cdot 3^r$, deci $3|3^n + 1$, contradicţie.

Capitolul 11

Soluţii: Construcţii de inele: inele de matrice, inele de polinoame, inele de serii formale şi inele de fracţii

1. Dacă $n = 1$ şi R este inel comutativ, atunci $M_n(R) \simeq R$ este inel comutativ. Dacă $ab = 0$ pentru orice $a, b \in R$, atunci $AB = 0$ pentru orice $A, B \in M_n(R)$ şi evident $M_n(R)$ este comutativ.
Reciproc, presupunem că $M_n(R)$ este inel comutativ. Dacă $n = 1$, atunci $M_n(R) \simeq R$, deci condiţia (i) este satisfăcută. Dacă $n \geq 2$, fie $a, b \in R$. Considerăm matricele

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & . \\ a & 0 & \dots & 0 \end{pmatrix}, \quad B = \begin{pmatrix} b & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ . & \dots & \dots & . \\ 0 & 0 & \dots & 0 \end{pmatrix}.$$

Atunci $BA = 0$ şi

$$AB = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & . \\ ab & 0 & \dots & 0 \end{pmatrix}.$$

Deoarece $AB = BA$, este necesar ca $ab = 0$, deci condiţia (ii) este satisfăcută.

2. (i) Fie $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_p)$. Atunci $A^2 = A$ dacă şi numai dacă au loc relaţiile

$$a^2 + bc = a,\ b(a+d) = b,\ c(a+d) = c,\ d^2 + bc = d.$$

Dacă $a + d \neq 1$, rezultă că $b = c = 0$ şi $a = d = 0$ sau $a = d = 1$, şi obţinem matricele idempotente $A = 0$ şi $A = I_2$.
Dacă $a + d = 1$, avem următoarele posibilităţi:
• $a = 0$ şi atunci $d = 1$, $bc = 0$, de unde $b = 0$ sau $c = 0$. Obţinem matricele idempotente $A = \begin{pmatrix} 0 & b \\ 0 & 1 \end{pmatrix}$ cu $b \in \mathbb{Z}_p$ şi $A = \begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix}$ cu $c \in \mathbb{Z}_p - \{0\}$, în număr de $p + p - 1 = 2p - 1$.
• $a = 1$ şi atunci $d = 0$, $bc = 0$. Obţinem matricele idempotente $A = \begin{pmatrix} 1 & b \\ 0 & 0 \end{pmatrix}$ cu $b \in \mathbb{Z}_p$ şi $A = \begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix}$ cu $c \in \mathbb{Z}_p - \{0\}$, în număr de $p+p-1 = 2p - 1$.
• $a \notin \{0, 1\}$ şi atunci rezultă că $bc = a - a^2 \neq 0$, deci b poate fi orice element nenul din $\mathbb{Z}_p$ iar c este unic determinat de a şi b prin formula $c = b^{-1}(a - a^2)$ (unde b^{-1} este inversul lui b în $\mathbb{Z}_p$). Obţinem matricele idempotente

$$A = \begin{pmatrix} a & b \\ b^{-1}(a - a^2) & 1 - a \end{pmatrix}$$

cu $a \in \mathbb{Z}_p - \{0, 1\}$ şi $b \in \mathbb{Z}_p - \{0\}$, în număr de $(p - 2)(p - 1)$.
În total avem $2 + 2p - 1 + 2p - 1 + (p - 2)(p - 1) = p(p + 1) + 2$ matrice idempotente în $M_2(\mathbb{Z}_p)$.
(ii) Numărăm mai întâi câte matrice inversabile există în $M_2(\mathbb{Z}_p)$. Avem $(p - 1)^4 - (p - 1)^3$ matrice inversabile care au patru poziţii nenule (deoarece într-o matrice neinversabilă cu elemente nenule trei poziţii pot fi alese fără restricţii în $\mathbb{Z}_p - \{0\}$, iar a patra poziţie este determinată în mod unic de celelalte trei), $4(p - 1)^3$ matrice inversabile cu exact trei poziţii nenule şi $2(p - 1)^2$ matrice inversabile cu exact două poziţii nenule. În total avem $(p - 1)^4 - (p - 1)^3 + 4(p - 1)^3 + 2(p - 1)^2 = q$ matrice inversabile în $M_2(\mathbb{Z}_p)$. Atunci grupul multiplicativ al elementelor inversabile din $M_2(\mathbb{Z}_p)$ are q elemente şi din teorema lui Lagrange rezultă că $A^q = I_2$.
Dacă matricea B este inversabilă, atunci $B^q = I_2$, de unde $B^{q+2} = B^2$. Dacă B nu este inversabilă, atunci $\det(B) = 0$ şi relaţia $B^2 - \mathrm{tr}(B)B + \det(B)I_2 = 0$ devine $B^2 = \alpha B$, unde $\alpha = \mathrm{tr}(B)$. Rezultă mai departe că $B^{q+2} = \alpha^{q+1}B$.

Dacă $\alpha = 0$, atunci $B^2 = 0$ şi evident $B^{q+2} = B^2$. Dacă $\alpha \neq 0$, atunci $\alpha^{p-1} = 1$ (din teorema lui Lagrange în grupul multiplicativ $\mathbb{Z}_p - \{0\}$), de unde $\alpha^q = 1$ şi deci $\alpha^{q+1} = \alpha$, ceea ce arată că $\alpha^{q+1}B = \alpha B = B^2$.

3. Dacă A este inversabilă, atunci este clar că A nu este divizor al lui zero. Reciproc, presupunem că A nu este divizor al lui zero. Dacă prin absurd A nu ar fi inversabilă, atunci $\det(A) = 0$ şi sistemul de n ecuaţii cu n necunoscute

$$A \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix} = 0$$

are o soluţie nenulă $(x_1, x_2, \dots, x_n)$. Atunci $AB = 0$, unde

$$B = \begin{pmatrix} x_1 & x_1 & \dots & x_1 \\ x_2 & x_2 & \dots & x_2 \\ \dots & \dots & \dots & \dots \\ x_n & x_n & \dots & x_n \end{pmatrix} \neq 0$$

de unde rezultă că A este divizor al lui zero la stânga. Analog se arată că A este divizor al lui zero la dreapta, contradicţie. Prin urmare A trebuie să fie inversabilă.

4. Reamintim că pentru orice $1 \leq i, j \leq n$ notăm cu e_{ij} matricea $n \times n$ care are 1 pe poziţia (i, j) şi 0 în rest. Atunci $e_{ij}e_{pq} = \delta_{jp}e_{iq}$ pentru orice i, j, p, q, unde δ_{jp} este simbolul lui Kronecker. Fie $A = (a_{ij})_{1 \leq i,j \leq n}$. Atunci $A = \sum_{1 \leq i,j \leq n} a_{ij}e_{ij}$ şi avem $Ae_{pq} = \sum_{1 \leq i \leq n} a_{ip}e_{iq}$ şi $e_{pq}A = \sum_{1 \leq j \leq n} a_{qj}e_{pj}$. De aici obţinem că $Ae_{pq} = e_{pq}A$ dacă şi numai dacă $a_{ip} = a_{qj} = 0$ pentru orice $i \neq p$ şi $j \neq q$, şi $a_{pp} = a_{qq}$. Rezultă că dacă $A \in Z(M_n(R))$, deci $Ae_{pq} = e_{pq}A$ pentru orice p, q, atunci avem $a_{uv} = 0$ pentru orice $u \neq v$ şi $a_{11} = a_{22} = \dots = a_{nn}$, adică $A = aI_n$ pentru un $a \in R$. Reciproc, dacă $A = aI_n$, atunci este evident că A comută cu orice matrice din $M_n(R)$.
Este clar că aplicaţia $f : R \to Z(M_n(R))$, $f(a) = aI_n$, este izomorfism de inele.

5. Este uşor de verificat că dacă $f : A \to B$ este un izomorfism de inele şi $Z(A)$ este corp, atunci $Z(B)$ este un corp izomorf cu $Z(A)$, iar $Z(A)$-spaţiul vectorial A şi $Z(B)$-spaţiul vectorial B au aceeaşi dimensiune. Într-adevăr,

prima parte se probează printr-un calcul direct, iar pentru a doua se arată că dacă $(e_i)_{i\in I}$ este o bază în $Z(A)$-spaţiul vectorial A, atunci $(f(a_i))_{i\in I}$ este o bază în $Z(B)$-spaţiul vectorial B.
În cazul particular în care $A = M_m(K)$ şi $B = M_n(L)$, din problema 4 avem că $Z(A) \simeq K$, rezultă că $K \simeq Z(M_m(K)) \simeq Z(M_n(L)) \simeq L$ şi că $\dim_K(A) = \dim_L(B)$, deci $m^2 = n^2$, de unde $m = n$.

6. Fie X un ideal bilateral în inelul $M_n(R)$. Notăm cu I mulţimea tuturor elementelor care apar pe poziţia $(1,1)$ în matricele din X. Evident I este subgrup aditiv al lui R. Mai mult, I este ideal bilateral în R, deoarece dacă $a \in I$, atunci există $A \in X$ care are a pe poziţia $(1,1)$ şi pentru $r \in R$ matricele $(rI_n)A$ şi $A(rI_n)$ din X au pe poziţia $(1,1)$ elementele ra, respectiv ar, de unde $ar, ra \in I$.
Arătăm că $X = M_n(I)$. (Ca şi în soluţia problemei 4, notăm cu e_{ij} matricea care are 1 pe poziţia (i,j) şi 0 în rest). Fie $a \in I$ şi $A \in X$ care are elementul a pe poziţia $(1,1)$. Atunci $e_{i1}Ae_{1j} = ae_{ij}$, deci $ae_{ij} \in X$. Cum orice matrice din $M_n(I)$ este o sumă de matrice de forma ae_{ij} cu $a \in I$, rezultă că $M_n(I) \subseteq X$. Fie acum $A = (a_{ij})_{1\le i,j\le n} \in X$. Pentru orice i, j avem că $e_{1i}Ae_{j1} = a_{ij}e_{11}$ este o matrice din X, de unde $a_{ij} \in I$. Obţinem că $A \in M_n(I)$, adică $X \subseteq M_n(I)$, ceea ce probează egalitatea $X = M_n(I)$.
Dacă I este un ideal bilateral din R, fie $p : R \to R/I$ proiecţia canonică. Definim $f : M_n(R) \to M_n(R/I)$ astfel: dacă $A = (a_{ij})_{1\le i,j\le n} \in M_n(R)$, atunci $f(A) = (p(a_{ij}))_{1\le i,j\le n} \in M_n(R/I)$. Se verifică printr-un calcul simplu că f este morfism de inele. Este clar că f este surjectiv şi că $\mathrm{Ker}(f) = M_n(I)$. Din teorema fundamentală de izomorfism pentru inele obţinem că $M_n(R)/M_n(I) \simeq M_n(R/I)$.
În final, observăm că pentru $n > 1$, mulţimea matricelor din $M_n(R)$ care au 0 pe coloanele $2, 3, \ldots, n$ este ideal stâng în $M_n(R)$, dar nu este de forma $M_n(J)$ cu J ideal stâng din R.

7. Presupunem că ar exista un morfism de inele $f : M_n(K) \to K$. Atunci $\mathrm{Ker}(f)$ este ideal bilateral în $M_n(K)$, deci din problema 6 este de forma $M_n(I)$, cu I ideal bilateral în K. Singurele ideale în K sunt 0 şi K. Cum $f(I_n) = 1$, nu putem avea $\mathrm{Ker}(f) = M_n(K)$. Rămâne că $\mathrm{Ker}(f) = 0$, adică f este injectiv, şi atunci $M_n(K) \simeq \mathrm{Im}(f)$, care este un subinel al lui K. Dar $M_n(K)$ are divizori ai lui zero (pentru că $n \ge 2$) şi deci şi K are divizori ai lui zero, contradicţie.

8. (i) Pentru orice $u, v, z, w \in \mathbb{C}$ avem

$$\begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} - \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} = \begin{pmatrix} u-z & v-w \\ -\overline{v}+\overline{w} & \overline{u}-\overline{z} \end{pmatrix} \in \mathbb{H},$$

$$\begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix}\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} = \begin{pmatrix} uz-v\overline{w} & uw+v\overline{z} \\ -\overline{uw}-\overline{v}z & \overline{uz}-\overline{v}w \end{pmatrix} \in \mathbb{H}$$

şi $I_2 \in \mathbb{H}$, ceea ce arată că $\mathbb{H}$ este subinel al lui $M_2(\mathbb{C})$. Observăm că dacă $A = \begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} \in \mathbb{H}$, atunci $\det(A) = |u|^2 + |v|^2$, de unde $A = 0$ dacă şi numai dacă $\det(A) = 0$. Atunci pentru orice $A \neq 0$ din $\mathbb{H}$ avem că A este inversabilă în $M_2(\mathbb{C})$ şi inversa sa este matricea $\frac{1}{\det(A)}\begin{pmatrix} \overline{u} & -v \\ \overline{v} & u \end{pmatrix}$, care este în $\mathbb{H}$.
(ii) Aplicaţia $f : \mathbb{C} \to \mathbb{H}$, $f(u) = \begin{pmatrix} u & 0 \\ 0 & \overline{u} \end{pmatrix}$, este clar morfism (injectiv) de corpuri.
(iii) Dacă $A = \begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix}$ cu $u = a + ib$ şi $v = c + id$, cu $a, b, c, d \in \mathbb{R}$, atunci $A = aI_2 + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$. Această reprezentare este unică deoarece dacă $a_0I_2 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} = b_0I_2 + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k}$ obţinem $a_0 + a_1i = b_0 + b_1i$ şi $a_2 + a_3i = b_2 + b_3i$, de unde $a_t = b_t$ pentru orice $0 \leq t \leq 3$.
Fie $A = \begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix}$ cu $u = a + ib$ şi $v = c + id$. Atunci $T(A) = 2aI_2 = \mathrm{tr}(A)I_2$, unde $\mathrm{tr}(A)$ este urma matricei A. Folosind relaţiile $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -I_2$, $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$, $\mathbf{jk} = -\mathbf{kj} = \mathbf{i}$ şi $\mathbf{ki} = -\mathbf{ik} = \mathbf{j}$, obţinem printr-un calcul direct că

$$\begin{aligned} N(A) &= (aI_2 + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(aI_2 - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) \\ &= (a^2 + b^2 + c^2 + d^2)I_2 \\ &= (|u|^2 + |v|^2)I_2 \\ &= \det(A)I_2. \end{aligned}$$

Acum relaţia $A^2 - T(A)A + N(A) = 0$ nu este altceva decât cunoscuta formulă $A^2 - \mathrm{tr}(A)A + \det(A)I_2 = 0$ pentru matrice pătratice de ordin 2, formulă care rezultă uşor printr-un calcul direct. Formula $N(AB) = N(A)N(B) = N(BA)$ rezultă acum din faptul că $\det(AB) = \det(A)\det(B)$.
(iv) Fie $A = aI_2 + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in Z(\mathbb{H})$, cu $a, b, c, d \in \mathbb{R}$. Cum $A\mathbf{i} =$

$a\mathbf{i} - bI_2 - c\mathbf{k} + d\mathbf{j}$ şi $\mathbf{i}A = a\mathbf{i} - bI_2 + c\mathbf{k} - d\mathbf{j}$, rezultă că $c = d = 0$. Apoi $\mathbf{j}A = \mathbf{j}(aI_2 + b\mathbf{i}) = a\mathbf{j} - b\mathbf{k}$ şi $A\mathbf{j} = a\mathbf{j} + b\mathbf{k}$, ceea ce arată că $b = 0$, adică $A = aI_2$. Rezultă că $Z(\mathbb{H}) \subseteq \mathbb{R}I_2$. Este clar că are loc şi incluziunea inversă, de unde rezultă că $Z(\mathbb{H}) = \mathbb{R}I_2$.
(v) Fie A o soluţie a ecuaţiei $x^2 = -1$ în $\mathbb{H}$, adică $A = aI_2 + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ cu $a, b, c, d \in \mathbb{R}$ şi $A^2 = -I_2$. Atunci $\det(A)^2 = \det(-I_2) = 1$ şi cum $\det(A) = a^2 + b^2 + c^2 + d^2 \geq 0$ avem $\det(A) = 1$, adică $N(A) = I_2$. Apoi $A^2 = -I_2$ implică $A^2\overline{A} = -\overline{A}$, de unde $AN(A) = -\overline{A}$, sau $A = -\overline{A}$. Aceasta arată că $a = 0$, deci $A = b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ cu $b^2 + c^2 + d^2 = 1$. Arătăm că orice astfel de A este soluţie. Într-adevar, avem $N(A) = I_2$ şi $A = -\overline{A}$, de unde $AN(A) = -\overline{A}$, sau $A^2\overline{A} = -\overline{A}$. Cum $\mathbb{H}$ este corp şi $\overline{A} \neq 0$, rezultă că $A^2 = -I_2$.
Aşadar soluţiile ecuaţiei $x^2 = -1$ în $\mathbb{H}$ sunt matricele de forma $A = b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$ cu $b, c, d \in \mathbb{R}$ pentru care $b^2 + c^2 + d^2 = 1$. Este clar că există o infinitate de astfel de matrice.

9. (a) $\Rightarrow$ (b) Fie $E_{ij} \in M_n(R)$ matricea care are 1 pe poziţia (i, j) şi 0 în rest. Atunci $\sum_{1\leq i\leq n} E_{ii} = I_n$ şi $E_{ij}E_{kl} = \delta_{jk}E_{il}$ pentru orice $1 \leq i, j, k, l \leq n$. Dacă $f : M_n(R) \to S$ este un izomorfism de inele şi $e_{ij} = f(E_{ij})$, atunci familia $(e_{ij})_{1\leq i,j\leq n}$ satisface condiţiile cerute.
(b) $\Rightarrow$ (a) Fie $R = \{r \in S \mid re_{pl} = e_{pl}r \text{ pentru orice } 1 \leq p, l \leq n\}$. Se verifică imediat că R este subinel în S (sau rezultă direct din problema 35 din Capitolul 4).
Arătăm că dacă $(r_{ij})_{1\leq i,j\leq n}$ este o familie de elemente din R cu $\sum_{1\leq i,j\leq n} r_{ij}e_{ij} = 0$, atunci $r_{ij} = 0$ pentru orice i, j. Într-adevăr, pentru orice p, q, k, l avem

$$\begin{aligned} 0 &= e_{pq}\Big(\sum_{1\leq i,j\leq n} r_{ij}e_{ij}\Big)e_{kl} \\ &= \sum_{1\leq i,j\leq n} e_{pq}r_{ij}e_{ij}e_{kl} \\ &= \sum_{1\leq i,j\leq n} r_{ij}e_{pq}e_{ij}e_{kl} \\ &= r_{qk}e_{pl}. \end{aligned}$$

Atunci $r_{ij} = \sum_{1\leq p\leq n} r_{ij}e_{pp} = 0$.
Definim acum $f : M_n(R) \to S$ în modul următor. Dacă $A = (r_{ij})_{1\leq i,j\leq n} \in$

$M_n(R)$, definim $f(A) = \sum_{1\leq i,j\leq n} r_{ij}e_{ij}$. Evident f este morfism de grupuri aditive. De asemenea pentru $A = (r_{ij})_{1\leq i,j\leq n}, B = (s_{ij})_{1\leq i,j\leq n} \in M_n(R)$ avem că

$$\begin{aligned} f(A)f(B) &= \sum_{i,j,p,q} r_{ij}e_{ij}s_{pq}e_{pq} \\ &= \sum_{i,j,p,q} r_{ij}s_{pq}e_{ij}e_{pq} \\ &= \sum_{i,j,q} r_{ij}s_{jq}e_{iq} \\ &= \sum_{i,q}(\sum_{j} r_{ij}s_{jq})e_{iq} \\ &= f(AB) \end{aligned}$$

şi $f(I_n) = \sum_{1\leq i\leq n} e_{ii} = 1$, ceea ce arată că f este morfism de inele.
Dacă $f(A) = 0$, rezultă din cele de mai sus că $A = 0$, deci f este injectivă.
În sfârşit, fie $a \in S$. Arătăm că pentru orice $1 \leq i, j \leq n$, elementul $a_{ij} = \sum_{1\leq k\leq n} e_{ki}ae_{jk}$ este în R. Într-adevăr

$$\begin{aligned} a_{ij}e_{pl} &= \sum_{1\leq k\leq n} e_{ki}ae_{jk}e_{pl} \\ &= \sum_{1\leq k\leq n} \delta_{kp}e_{ki}ae_{jl} \\ &= e_{pi}ae_{jl} \end{aligned}$$

şi

$$\begin{aligned} e_{pl}a_{ij} &= \sum_{1\leq k\leq n} e_{pl}e_{ki}ae_{jk} \\ &= \sum_{1\leq k\leq n} \delta_{lk}e_{pi}ae_{jk} \\ &= e_{pi}ae_{jl}. \end{aligned}$$

Atunci $A = (a_{ij})_{1\leq i,j\leq n} \in M_n(R)$ şi

$$\begin{aligned} f(A) &= \sum_{1\leq i,j\leq n} a_{ij}e_{ij} \\ &= \sum_{1\leq i,j\leq n}\sum_{1\leq k\leq n} e_{ki}ae_{jk}e_{ij} \\ &= \sum_{1\leq i,j\leq n} e_{ii}ae_{jj} \\ &= (\sum_{1\leq i\leq n} e_{ii})a(\sum_{1\leq j\leq n} e_{jj}) \\ &= a \end{aligned}$$

ceea ce arată că f este şi surjectivă, deci izomorfism de inele.

10. Rezultă imediat din problema 9. Familia $(e_{ij})_{1\leq i,j\leq n}$ de elemente din S care satisface condiţiile din problema 9(b) este o familie cu aceleaşi proprietăţi şi în B. De asemenea familia $(p(e_{ij}))_{1\leq i,j\leq n}$ din A satisface proprietăţile din problema 9(b) pentru A, unde $p : S \to A$ este proiecţia canonică.

11. (i) Verificare imediată.
(ii) Folosind proprietatea de universalitate a inelelor de polinoame, există un morfism de inele $\phi : \mathbb{Z}[X] \to R_k$ astfel încât $f(a) = aI_2$ pentru orice $a \in \mathbb{Z}$ şi $\phi(X) = \begin{pmatrix} 0 & 1 \\ k & 0 \end{pmatrix}$. Atunci ϕ este surjectiv, deoarece $\phi(a+bX) = \begin{pmatrix} a & b \\ kb & a \end{pmatrix}$. Arătăm că $\mathrm{Ker}(\phi) = (X^2 - k)$. Este clar că $\phi(X^2 - k) = 0$, deci $(X^2 - k) \subseteq \mathrm{Ker}(\phi)$. Fie acum $f \in \mathrm{Ker}(\phi)$. Cum $X^2 - k$ are coeficientul dominant 1, putem aplica algoritmul de împărţire cu rest şi obţinem $f(X) = (X^2 - k)g(X) + r(X)$, unde $r(X) = a + bX$ cu $a, b \in \mathbb{Z}$. Aplicând ϕ obţinem că $\phi(r) = 0$, deci $\begin{pmatrix} a & b \\ kb & a \end{pmatrix} = 0$, de unde evident $a = b = 0$. Rezultă că $r = 0$ şi $f \in (X^2 - k)$.
(iii) Din (ii) avem că $R_k \simeq R_l$ dacă şi numai dacă există un izomorfism $\psi : \mathbb{Z}[X]/(X^2 - k) \to \mathbb{Z}[X]/(X^2 - l)$. Notăm cu $\hat{f}$ şi $\overline{f}$ clasele unui polinom f în inelele factor $\mathbb{Z}[X]/(X^2-k)$ şi $\mathbb{Z}[X]/(X^2-l)$, respectiv. Este clar că $\psi(\hat{a}) = \overline{a}$ pentru $a \in \mathbb{Z}$. Fie $\psi(\hat{X}) = \overline{a + bX}$. Atunci $\psi(\hat{X})^2 = \psi(\hat{X}^2) = \psi(\hat{k}) = \overline{k}$, de unde $\overline{(a + bX)}^2 = \overline{k}$, ceea ce implică $2abX + a^2 + b^2l - k \in (X^2 - l)$. De aici obţinem că $ab = 0$ şi $a^2 + b^2l = k$. Cum $b \neq 0$ (altfel ψ nu ar fi surjectivă),

rezultă că $a = 0$ şi apoi $b^2 l = k$. Rezultă că $l|k$ şi l, k au acelaşi semn. Din motive de simetrie (lucrând cu inversul lui ψ) obţinem şi $k|l$, de unde $k = l$.

12. **Soluţia 1.** Putem construi efectiv un izomorfism între cele două inele. Fie $A \in M_n(R[X])$, $A = (f_{ij})_{1 \leq i,j \leq n}$. Scriem $f_{ij}(X) = \sum_{0 \leq k \leq m} a_{ij}^{(k)} X^k$, unde putem alege m suficient de mare ca să fie bun pentru orice i, j. Definim $\phi : M_n(R[X]) \to M_n(R)[X]$ prin $\phi(A) = \sum_{0 \leq k \leq m} A_k X^k$, unde $A_k = (a_{ij}^{(k)})_{1 \leq i,j \leq n} \in M_n(R)$. Un calcul simplu arată că ϕ este izomorfism de inele.
Soluţia 2. Fie $S = M_n(R)[X]$. Vom arăta, folosind problema 9, că S este izomorf cu un inel de matrice $n \times n$ peste $R[X]$. Fie $e_{ij} \in M_n(R)$ matricea care are 1 pe poziţia (i, j) şi 0 în rest. Considerăm e_{ij} ca pe nişte polinoame de grad zero din S. Deoarece familia $(e_{ij})_{1 \leq i,j \leq n}$ verifică condiţiile din problema 9(b), rezultă că $S \simeq M_n(T)$, unde

$$T = \{s \in S \mid se_{ij} = e_{ij}s \text{ pentru orice } 1 \leq i, j \leq n\}.$$

Fie $f \in S$, $f(X) = A_0 + \ldots + A_h X^h$. Atunci $f \in T$ dacă şi numai dacă $e_{ij}A_k = A_k e_{ij}$ pentru orice $1 \leq i, j \leq n$ şi $0 \leq k \leq h$. Dar aceasta este echivalent cu $A_k \in Z(M_n(R)) = RI_n$ pentru orice k. Obţinem că $T = (RI_n)[X] \simeq R[X]$, ceea ce arată că $S \simeq M_n(R[X])$.

13. Folosind proprietatea de universalitate a inelelor de polinoame obţinem că există un unic morfism de inele $\phi : R[X_1, \ldots, X_n] \to R$ cu proprietatea că $\phi(r) = r$ pentru $r \in R$ şi $\phi(X_i) = a_i$ pentru $1 \leq i \leq n$. Este evident că ϕ este surjectiv. Arătăm prin inducţie după n că $\mathrm{Ker}(\phi) = (X_1 - a_1, \ldots, X_n - a_n)$. Pentru $n = 1$ rezultă din teorema lui Bézout. Presupunem că afirmaţia este adevărată pentru $n - 1$ şi o demonstrăm pentru n. Din teorema de împărţire cu rest pentru polinoame rezultă că $f(X_1, \ldots, X_n) = (X_n - a_n)g(X_1, \ldots, X_n) + r(X_1, \ldots, X_{n-1})$, deoarece restul r este un polinom de grad zero în X_n. Cum $f(a_1, \ldots, a_n) = 0$, rezultă că $r(a_1, \ldots, a_{n-1}) = 0$ şi din ipoteza de inducţie avem că $r \in (X_1 - a_1, \ldots, X_{n-1} - a_{n-1})$. De aici rezultă că $f \in (X_1 - a_1, \ldots, X_n - a_n)$. Reciproc este evident că dacă $f \in (X_1 - a_1, \ldots, X_n - a_n)$, atunci $f \in \mathrm{Ker}(\phi)$. Izomorfismul cerut rezultă acum din teorema fundamentală de izomorfism pentru inele.

14. Notăm cu A inelul $R[X_1, \ldots, X_n]$ şi cu I^e idealul extins al lui I în A.
(i) Este clar că $I \subset I[X_1, \ldots, X_n]$. De aici rezultă că idealul generat de I în

A, adică I^e, este inclus în $I[X_1, \ldots, X_n]$. Pentru incluziunea contrară folosim caracterizarea

$$I^e = \left\{ \sum_{i=1}^{n} a_i f_i \mid a_i \in I, f_i \in A \right\}.$$

Se observă că polinoamele $a_i f_i$ din suma de mai sus au toţi coeficienţii în I, deci suma lor va avea prin urmare aceeaşi proprietate. În consecinţă, $I^e \subset I[X_1, \ldots, X_n]$.
(ii) Considerăm proiecţia canonică $\pi : R \to R/I$ şi o extindem la un morfism $\overline{\pi} : R[X_1, \ldots, X_n] \to (R/I)[X_1, \ldots, X_n]$, conform proprietăţii de universalitate a inelelor de polinoame. Avem că

$$\overline{\pi}(\sum a_{i_1 \ldots i_n} X_1^{i_1} \cdots X_n^{i_n}) = \sum \pi(a_{i_1 \ldots i_n}) X_1^{i_1} \cdots X_n^{i_n}$$

şi morfismul $\overline{\pi}$ este în mod evident surjectiv. Pe de altă parte, un polinom $f = \sum a_{i_1 \ldots i_n} X_1^{i_1} \cdots X_n^{i_n}$ aparţine lui $\operatorname{Ker} \overline{\pi}$ dacă şi numai dacă $\sum \pi(a_{i_1 \ldots i_n}) X_1^{i_1} \cdots X_n^{i_n} = 0$, ceea ce este echivalent cu $\pi(a_{i_1 \ldots i_n}) = 0$ pentru orice multiindice $i_1 \ldots i_n$, adică $a_{i_1 \ldots i_n} \in I$ pentru orice multiindice $i_1 \ldots i_n$. În concluzie, $\operatorname{Ker} \overline{\pi} = I[X_1, \ldots, X_n]$ şi izomorfismul căutat rezultă acum din teorema fundamentală de izomorfism pentru inele.
(iii) Idealul $I[X_1, \ldots, X_n]$ este prim în A dacă şi numai dacă inelul factor $R[X_1, \ldots, X_n]/I[X_1, \ldots, X_n]$ este domeniu de integritate. Conform izomorfismului de la punctul (ii), aceasta se întâmplă dacă şi numai dacă inelul de polinoame $(R/I)[X_1, \ldots, X_n]$ este domeniu de integritate, echivalent cu faptul că R/I este domeniu. În fine, R/I este domeniu dacă şi numai dacă I este ideal prim al lui R.

15. (i) Folosind proprietatea de universalitate a inelelor de polinoame, deducem că există un morfism de inele $\phi : \mathbb{Z}[X] \to \mathbb{Z}[\sqrt{d}]$ cu proprietatea că $\phi(n) = n$ pentru orice $n \in \mathbb{Z}$ şi $\phi(X) = \sqrt{d}$. Acest morfism se poate descrie simplu prin $\phi(f) = f(\sqrt{d})$ pentru orice $f \in \mathbb{Z}[X]$. Este clar că ϕ este surjectiv, deoarece $\phi(a + bX) = a + b\sqrt{d}$. Pe de altă parte $\operatorname{Ker}(\phi) = (X^2 - d)$. Incluziunea "$\supseteq$" este evidentă. Invers, dacă $f \in \operatorname{Ker}(\phi)$, adică $f(\sqrt{d}) = 0$, împărţim cu rest pe f la $X^2 - d$ şi obţinem $f(X) = (X^2 - d)q(X) + r(X)$, $q(X), r(X) \in \mathbb{Z}[X]$ cu $\deg r < 2$. Fie deci $r(X) = a + bX$, $a, b \in \mathbb{Z}$. Evaluând $f(X) = (X^2 - d)q(X) + r(X)$ pentru $X = \sqrt{d}$ obţinem că $a + b\sqrt{d} = 0$, şi cum d este liber de pătrate, deci $\sqrt{d}$ este iraţional, trebuie să avem $a = b = 0$. Obţinem că $r = 0$, deci $f \in (X^2 - d)$.

Acum izomorfismul cerut rezultă aplicând teorema fundamentală de izomorfism pentru inele morfismului ϕ.
(ii) Similar cu (i), dacă se consideră morfismul de inele $\phi : \mathbb{Q}[X] \to \mathbb{Q}(\varepsilon)$, $\phi(f) = f(\varepsilon)$.
(iii) Similar cu (i), dacă se consideră morfismul de inele $\phi : \mathbb{R}[X] \to \mathbb{C}$, $\phi(f) = f(i)$.

16. Fie $d \in \mathbb{Z}$ liber de pătrate şi $a, b \in \mathbb{Z}$ cu $a \neq 0$ sau $b \neq 0$. Să notăm $I = (a + b\sqrt{d})$, ideal în $\mathbb{Z}[\sqrt{d}]$.
Dacă $b = 0$, atunci $\mathbb{Z}[\sqrt{d}]/(a + b\sqrt{d}) = \mathbb{Z}[\sqrt{d}]/(a) = \{\widehat{u + v\sqrt{d}} | u, v \in \{0, 1, \ldots, |a| - 1\}\}$ (conform teoremei de împărţire cu rest din $\mathbb{Z}$, pentru orice $x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ există $x', y' \in \mathbb{Z}$ şi $r, s \in \{0, 1, \ldots, |a| - 1\}$ astfel încât $x + y\sqrt{d} = (ax' + r) + (ay' + s\sqrt{d}) \equiv r + s\sqrt{d} \pmod{I}$). Cum aceste clase sunt distincte, obţinem că $\mathbb{Z}[d]/(a + b\sqrt{d})$ are $a^2 = |a^2 - db^2|$ elemente.
Pentru $b \neq 0$ să notăm $g = (a, b)$. Punem $a = ga'$ şi $b = gb'$, cu $a', b' \in \mathbb{Z}$, $(a', b') = 1$, şi $m = (a')^2 - d(b')^2$. Cum $(b', m) = 1$, există $b'' \in \mathbb{Z}$ pentru care $b'b'' \equiv 1 \pmod{m}$. Rezultă că $b'b'' - 1 \equiv 0 \pmod{m}$, de unde $b'b'' - 1 \equiv 0 \pmod{a' + b'\sqrt{d}}$, deci $b'b'' \equiv 1 \pmod{a' + b'\sqrt{d}}$. Avem şi $b'\sqrt{d} \equiv -a' \pmod{a' + b'\sqrt{d}}$, de unde $b'b''\sqrt{d} \equiv -a'b'' \pmod{a' + b'\sqrt{d}}$, adică $\sqrt{d} \equiv -a'b'' \pmod{a' + b'\sqrt{d}}$, ceea ce duce la $g\sqrt{d} \equiv -ga'b'' \pmod{g(a' + b'\sqrt{d})} \Leftrightarrow g\sqrt{d} \equiv -ga'b'' \pmod{I}$. Pe de altă parte este evident că $gm \equiv 0 \pmod{I}$. Prin urmare, orice element din $\mathbb{Z}[\sqrt{d}]/I$ este de forma $\widehat{j + k\sqrt{d}}$ cu $0 \leq j < g|m|$ şi $0 \leq k < g$. Rămâne de arătat că aceste clase sunt distincte. Este suficient să probăm că $j + k\sqrt{d} \equiv 0 \pmod{I}, |j| < g|m|, |k| < g \Rightarrow j = k = 0$. Fie un astfel de $j + k\sqrt{d}$. Vom avea o relaţie de forma $j + k\sqrt{d} = (a + b\sqrt{d})(a_1 + b_1\sqrt{d})$. De aici rezultă $k = ab_1 + ba_1 = g(a'b_1 + b'a_1) \Rightarrow a'b_1 + b'a_1 = 0$, deoarece $|k| < g$. Există deci $c \in \mathbb{Z}$ astfel încât $a_1 = a'c$ şi $b_1 = b'c$. De aici şi din $j + k\sqrt{d} = (a + b\sqrt{d})(a_1 + b_1\sqrt{d})$ obţinem $j = aa_1 + bb_1\sqrt{d} = gc((a')^2 - (b')^2 d)$, deci $j = \pm gmc \Rightarrow c = 0$, deoarece $|j| < g|m|$, de unde $a_1 = b_1 = 0$, ceea ce dă $k = j = 0$.
În concluzie, $\mathbb{Z}[\sqrt{d}]/I$ are $g|m| \cdot g = g^2|m| = |a^2 - bd^2|$ elemente.

17. (i) Dacă $\Delta > 0$, atunci polinomul $aX^2 + bX + c$ are două rădăcini reale distincte α şi β, şi atunci $(aX^2 + bX + c) = (a(X - \alpha)(X - \beta)) = ((X - \alpha)(X - \beta))$, de unde $\mathbb{R}[X]/(aX^2 + bX + c) \simeq \mathbb{R}[X]/((X - \alpha)(X - \beta))$. Aplicând Lema chineză a resturilor pentru $n = 2$ şi $I_1 = (X - \alpha)$, $I_2 = (X - \beta)$ (vezi problema 28 din Capitolul 4) obţinem că $R \simeq \mathbb{R}[X]/(X - \alpha) \times \mathbb{R}[X]/(X - \beta)$.

Acum $R \simeq \mathbb{R} \times \mathbb{R}$ din problema 13.
(ii) Fie θ una din rădăcinile complexe ale lui $aX^2 + bX + c$ (clar $\theta \notin \mathbb{R}$). Atunci ca în problema 15(iii) avem că $R \simeq \mathbb{R}[\theta]$. Dar evident $\mathbb{R}[\theta] = \mathbb{C}$, de unde rezultă izomorfismul cerut.
(iii) Dacă $\Delta = 0$, există $\alpha \in \mathbb{R}$ astfel încât $aX^2 + bX + c = a(X - \alpha)^2$, deci $R \simeq \mathbb{R}[X]/((X - \alpha)^2)$. Atunci $\overline{X - \alpha}$ este element nilpotent al lui R, deci R are divizori ai lui zero.
Fie $M \in \text{Max}(R)$. Atunci $M \in \text{Spec}(R)$, deci există $P \in \text{Spec}(\mathbb{R}[X])$ cu $((X - \alpha)^2) \subseteq P$ astfel încât $M = P/((X - \alpha)^2)$. Dar $(X - \alpha)^2 \in P$ şi P ideal prim implică $X - \alpha \in P$, de unde $(X - \alpha) \subseteq P$. Dar $(X - \alpha)$ este ideal maximal (pentru că $\mathbb{R}[X]/(X - \alpha) \simeq \mathbb{R}$ este corp), deci $P = (X - \alpha)$. Obţinem că $M = (X - \alpha)/((X - \alpha)^2)$, de unde rezultă că R este inel local.

18. Similar cu soluţia problemei 15(iii) există un izomorfism de inele $\psi : \mathbb{Z}[X]/(X^2 + 1) \simeq \mathbb{Z}[i]$. Cum $\psi((2, X^2 + 1)/(X^2 + 1)) = 2\mathbb{Z}[i]$, rezultă că $R \simeq \mathbb{Z}[i]/2\mathbb{Z}[i]$. Este clar că $\mathbb{Z}[i]/2\mathbb{Z}[i] = \{\overline{0}, \overline{1}, \overline{i}, \overline{1 + i}\}$, unde clasele sunt modulo $2\mathbb{Z}[i]$, şi acesta este un inel cu 4 elemente. Inelul R nu este izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_2$ deoarece $\overline{1 + i}^{\,2} = \overline{0}$, în timp ce $\mathbb{Z}_2 \times \mathbb{Z}_2$ nu are elemente nilpotente nenule.

19. Dacă I ar fi ideal principal, atunci ar exista $f \in \mathbb{Z}[X]$ cu $I = (f)$. Cum $3 \in (f)$, rezultă că $\deg(f) = 0$ şi $f \in \{1, -1, 3, -3\}$. Dacă $f = 1$ sau $f = -1$, atunci $I = \mathbb{Z}[X]$, deci există $g, h \in \mathbb{Z}[X]$ cu $1 = 3g + (X^3 - X^2 + 2X + 1)h$. Evaluând în $X = 1$ obţinem că $1 = 3(g(1) + h(1))$, contradicţie. Dacă $f = 3$ sau $f = -3$, atunci $I = 3\mathbb{Z}[X]$ şi deci $X^3 - X^2 + 2X + 1 \in 3\mathbb{Z}[X]$, din nou contradicţie. Aşadar I nu este ideal principal.
Pentru partea a doua avem $\mathbb{Z}[X]/I \simeq \mathbb{Z}_3[X]/(X^3 - X^2 + \hat{2}X + \hat{1})$, unde clasele sunt modulo 3. Dar în $\mathbb{Z}_3[X]$ avem $X^3 - X^2 + \hat{2}X + \hat{1} = X^3 - X^2 - X + \hat{1} = (X - \hat{1})^2(X + \hat{1})$. Rezultă că $\mathbb{Z}[X]/I \simeq \mathbb{Z}_3[X]/(X - \hat{1})^2(X + \hat{1}))$, care nu este domeniu de integritate, deci cu atât mai mult nu este corp.

20. Verificări simple arată că R este subinel al lui $\mathbb{R}[X]$ şi că I este ideal al lui R. Fie $\phi : R \to \mathbb{Q}$ definită prin $\phi(f) = f(0)$. Atunci ϕ este morfism surjectiv de inele şi $\text{Ker}(\phi) = I$, de unde rezultă că $R/I \simeq \mathbb{Q}$, care este corp, deci I este ideal maximal în R.
Presupunem prin absurd că I ar fi finit generat, fie $I = (f_1, \ldots, f_n)$, unde $f_i = a_1^{(i)}X + a_2^{(i)}X^2 + \ldots$ pentru $1 \leq i \leq n$. Atunci pentru orice $a \in \mathbb{R}$ există

$g_1, \ldots, g_n \in R$ cu $aX = g_1 f_1 + \cdots + g_n f_n$. În această relaţie putem simplifica prin X şi apoi, pentru $X = 0$ obţinem $a = g_1(0)a_1^{(1)} + \cdots + g_n(0)a_1^{(n)}$. Aceasta arată că $\{a_1^{(1)}, \ldots, a_1^{(n)}\}$ este sistem de generatori pentru $\mathbb{Q}$-spaţiul vectorial $\mathbb{R}$, ceea ce este o contradicţie cu faptul că $\mathbb{R}$ este mulţime nenumărabilă. Prin urmare I nu este finit generat.

21. Presupunem prin absurd că $I = (f_1, \ldots, f_n)$. Polinoamele $f_1, \ldots, f_n$ au în scrierea lor doar un număr finit de nedeterminate care apar efectiv iar pentru simplitate convenim că aceste nedeterminate sunt $X_1, \ldots, X_N$. Cum $X_{N+1} \in I$, există $g_1, \ldots, g_n \in R$ pentru care $X_{N+1} = g_1 f_1 + \cdots + g_n f_n$. Pentru $X_1 = \ldots = X_n = 0$ şi $X_{N+1} \neq 0$ obţinem o contradicţie.

22. Folosind problema 47(v) din Capitolul 4, avem

$$\begin{aligned} \mathrm{Rad}(I) &= \mathrm{Rad}((X^r) + (Y^s)) \\ &= \mathrm{Rad}(\mathrm{Rad}(X^r) + \mathrm{Rad}(Y^s)) \\ &= \mathrm{Rad}((X) + (Y)) \\ &= \mathrm{Rad}(X, Y) \\ &= (X, Y). \end{aligned}$$

Dacă $fg \in I$ şi $g \notin \mathrm{Rad}(I)$, vom arăta că $f \in I$. Cum $g \notin (X, Y)$, avem $a = g(0, 0) \neq 0$. Este clar că $f(0, 0) = 0$. Considerăm cel mai mic monom al lui f în ordinea lexicografică, să zicem $X^u Y^v$, cu coeficientul $a_{uv} \neq 0$. Acesta apare în produsul fg o singură dată, cu coeficientul $aa_{uv} \neq 0$. Dar în produsul fg monoamele au proprietatea că exponentul lui X este mai mare sau egal cu r sau exponentul lui Y este mai mare sau egal cu s, deci $u \geq r$ sau $v \geq s$. Aceasta înseamnă că $X^u Y^v \in I$. Considerăm acum polinomul $f_1 = f - a_{uv} X^u Y^v$. Avem că $f_1 g \in I$ şi folosind aceleaşi argumente ca mai înainte obţinem că toate monoamele lui f se află în idealul I, deci $f \in I$.

23. (i) Arătăm că idealul $(X^2 - Y^3)$ este prim, ceea ce este echivalent cu faptul că $X^2 - Y^3$ este ireductibil. Presupunem că $X^2 - Y^3 = fg$. Atunci $\deg_X(f) + \deg_X(g) = 2$. Dacă $\deg_X(f) = 2$, atunci egalăm coeficienţii lui X^2 în $X^2 - Y^3 = fg$ şi rezultă că $g \in K^*$, deci g este inversabil. Similar dacă $\deg_X(g) = 2$ rezultă că f este inversabil. Presupunem că $\deg_X(f) = \deg_X(g) = 1$ şi scriem $f = a(Y) + b(Y)X$, $g = c(Y) + d(Y)X$, cu $a, b, c, d \in K[Y]$. Relaţia $X^2 - Y^3 = fg$ revine la $b(Y)d(Y) = 1$, $a(Y)d(Y) + b(Y)c(Y) = 0$ şi $a(Y)c(Y) = -Y^3$. Prima relaţie arată că $b(Y)$

şi $d(Y)$ sunt constante nenule, deci $b(Y) = b$, $d(Y) = b^{-1}$, cu $b \in K^*$. A doua relaţie arată atunci că $c(Y) = b^{-2}a(Y)$, în particular că $a(Y)$ şi $c(Y)$ au acelaşi grad. Dar atunci $a(Y)c(Y)$ are grad par şi nu poate fi egal cu $-Y^3$. Prin urmare unul dintre f şi g este inversabil.
(ii) Folosim proprietatea de universalitate a inelelor de polinoame pentru a construi un morfism de inele $\phi : K[X, Y] \to k[T]$ pentru care $\phi(a) = a$ pentru orice $a \in K$, $\phi(X) = T^3$ şi $\phi(Y) = T^2$. Atunci $\mathrm{Im}(\phi) = B$. Într-adevăr, $\phi(X^iY^j) = T^{3i+2j} \in B$ pentru orice i, j, deoarece pentru $(i, j) \neq (0, 0)$ avem $3i + 2j \geq 2$. Pe de altă parte $T^m \in \mathrm{Im}(\phi)$ pentru orice $m \geq 2$, deoarece $T^{2i} = \phi(Y^i)$ şi $T^{2i+1} = \phi(XY^{i-1})$ pentru $i \geq 1$.
Arătăm acum că $\mathrm{Ker}(\phi) = (X^2 - Y^3)$. Incluziunea "$\supseteq$" este clară. Invers, fie $f \in K[X, Y]$ cu $f(T^3, T^2) = 0$. Îl privim pe f în $K[Y][X]$ şi folosind teorema de împărţire cu rest obţinem că $f = (X^2 - Y^3)g + r$, unde $r(X, Y) = a(Y) + b(Y)X$. În plus $r(T^3, T^2) = 0$, deci $a(T^2) = -b(T^2)T^3$. Aceasta implică $a(Y) = b(Y) = 0$, altfel gradul în T al lui $a(T^2)$ ar fi par, în timp ce gradul lui $-b(T^2)T^3$ ar fi impar. Rezultă că $r = 0$ şi $f \in (X^2 - Y^3)$. Izomorfismul cerut rezultă acum direct din teorema fundamentală de izomorfism. Să observăm că integritatea lui R rezultă direct din (ii), soluţia dată la (i) fiind o manieră directă de a demonstra integritatea lui R.

24. Faptul că R este integru rezultă din calcule similare celor de la problema 23(i). Arătăm acum că $(Y^2 - X^3 - X^2)$ nu este ideal prim în $K[[X, Y]]$. Pentru aceasta să observăm mai întâi că există $u \in K[[X]]$ cu $u^2 = 1 + X$. Într-adevăr, dacă $u = a_0 + a_1X + a_2X^2 + \ldots$, atunci $u^2 = 1 + X$ dacă şi numai dacă $a_0^2 = 1$, $2a_0a_1 = 1$, $2a_0a_2 + a_1^2 = 0$, $2a_0a_3 + 2a_1a_2 = 0$, ... Recurent putem găsi $a_0, a_1, a_2, \ldots$ care verifică relaţiile de mai sus (aici avem nevoie de caracteristică $\neq 2$) şi deci există u cu $u^2 = 1 + X$. Atunci $(Xu)^2 = X^2 + X^3$ şi $Y^2 - X^3 - X^2 = Y^2 - (Xu)^2 = (Y - Xu)(Y + Xu)$ nu este element ireductibil în $K[[X, Y]]$. Obţinem că $(Y^2 - X^3 - X^2)$ nu este ideal prim în $K[[X, Y]]$, de unde concluzia.

25. (i) Procedăm prin inducţie după $n = \deg(f)$. Pentru $n = 0$ este clar. Presupunem afirmaţia adevărată pentru toate polinoamele de grad mai mic strict decât n. Dacă $\deg(f) = n$, atunci din faptul că f este nilpotent obţinem că a_n este nilpotent (deoarece coeficientul dominant al lui f^p este a_n^p). Atunci polinomul a_nX^n este nilpotent, de unde $f - a_nX^n$ este nilpotent. Din ipoteza de inducţie rezultă acum că $a_0, a_1, \ldots, a_{n-1}$ sunt nilpotenţi.
(ii) "$\Leftarrow$" Avem că a_0 este inversabil şi $a_1X + \ldots + a_nX^n$ este nilpotent (ca

sumă de elemente nilpotente). Din problema 44(ii) din Capitolul 4 rezultă că f este inversabil, ca sumă dintre un element inversabil şi un element nilpotent.
"$\Rightarrow$" Procedăm prin inducţie după $\deg(f) = n$. Pentru $n = 0$ este clar. Presupunem afirmaţia adevărată pentru toate polinoamele de grad mai mic strict decât n şi fie f cu $\deg(f) = n$. Fie $g = b_0 + b_1X + \ldots + b_mX^m$ inversul lui f. Din $fg = 1$ rezultă că

$$a_nb_m = 0, a_nb_{m-1} + a_{n-1}b_m = 0, \ldots, a_0b_0 = 1.$$

Înmulţind a doua relaţie cu a_n obţinem că $a_n^2b_{m-1} = 0$, şi apoi prin recurenţă rezultă că $a_n^ib_{m-i+1} = 0$ pentru orice $1 \leq i \leq m+1$. Pentru $i = m+1$ aceasta înseamnă că $a_n^{m+1}b_0 = 0$. Cum b_0 este inversabil rezultă că $a_n^{m+1} = 0$, deci a_n este nilpotent. În continuare $g = f - a_nX^n$ este nilpotent ca sumă dintre un element inversabil şi un element nilpotent. Din ipoteza de inducţie rezultă acum că şi elementele $a_1, \ldots, a_{n-1}$ sunt nilpotente.
(iii) "$\Leftarrow$" Evident.
"$\Rightarrow$" Dacă f este divizor al lui zero, există $g \in R[X]$, $g \neq 0$ cu $fg = 0$. Alegem g de grad minim cu această proprietate. Fie $g(X) = b_0 + b_1X + \ldots + b_mX^m$. Din $fg = 0$ rezultă că $a_nb_m = 0$. Atunci a_ng are gradul mai mic ca m şi $(a_ng)f = 0$, de unde obţinem că $a_ng = 0$. În particular $a_nb_{m-1} = 0$ şi atunci egalând cu zero coeficientul lui X^{m+n-1} din fg rezultă că $a_{n-1}b_m = 0$. Atunci $a_{n-1}g$ are grad mai mic ca m şi $(a_{n-1}g)f = 0$, de unde $a_{n-1}g = 0$. Continuăm recurent şi obţinem că $a_ig = 0$ pentru orice $0 \leq i \leq n$. Aceasta implică $a_ib_m = 0$ pentru orice i, de unde $b_mf = 0$, ceea ce încheie demonstraţia.
(iv) Dacă f este idempotent, $f^2 = f$, atunci $a_0^2 = a_0$, $2a_0a_1 = a_1$, $2a_0a_2 + a_1^2 = a_2$, şi aşa mai departe. Înmulţind a doua relaţie cu a_0 şi folosind-o pe prima obţinem $2a_0a_1 = a_0a_1$, deci $a_0a_1 = 0$. Rezultă că şi $a_1 = 0$. Apoi înmulţind a treia relaţie cu a_0 şi folosind-o pe prima, obţinem că $2a_0a_2 = a_0a_2$, deci $a_0a_2 = 0$, ceea ce arată că şi $a_2 = 0$. Continuând recurent găsim $a_i = 0$ pentru $1 \leq i \leq n$, deci $f = a_0$.

26. (i) Reamintim că dacă într-un inel comutativ avem $u^m = v^n = 0$, atunci $(u + v)^{m+n} = 0$. Dacă $f^t = 0$, $t \in \mathbb{N}$, atunci $a_0^t = 0$, deci a_0 este nilpotent. Dar $f - a_0 = X(a_1 + a_2X + \ldots)$ şi cum $f^t = a_0^t = 0$, cu observaţia de mai sus avem că $(f - a_0)^{2t} = 0$, deci $f_1^{2t} = 0$, unde $f_1 = a_1 + a_2X + \ldots$. Obţinem că $a_1^{2t} = 0$, deci a_1 este nilpotent. Recurent obţinem că $a_i^{2^it} = 0$

pentru orice $i \geq 0$, deci toţi coeficienţii sunt nilpotenţi (chiar mai mult, avem nişte margini pentru indicii de nilpotenţă ai fiecărui coeficient).

Reciproc este fals. Fie $A = \mathbb{Z}[Y_0, Y_1, \ldots]$ inelul de polinoame cu coeficienţi întregi într-o infinitate de nedeterminate. Considerăm idealul

$$I = (Y_0, Y_1^{2^2}, \ldots, Y_n^{2^{2n}}, \ldots)$$

şi notăm $R = A/I$. Fie $f(X) = \sum_{i \geq 0} \hat{Y}_i X^i \in R[[X]]$. Dacă f ar fi nilpotent, atunci $f^t = 0$ pentru un $t \in \mathbb{N}^*$. Din prima parte rezultă că $\hat{Y}_i^{2^i t} = \hat{0}$ pentru orice $i \geq 0$. Rezultă că $Y_i^{2^i t} \in I$ pentru orice i, de unde $2^{2i} \leq 2^i t$ pentru orice $i \geq 0$. Aceasta nu este posibil, deoarece ar rezulta că $t \geq 2^i$ pentru orice i.
(ii) Dacă f este inversabil, fie $g = b_0 + b_1 X + \ldots$ inversul lui f. Atunci $fg = 1$ implică $a_0 b_0 = 1$, deci a_0 este inversabil în R.
Reciproc, presupunem că a_0 este inversabil şi construim un invers g pentru f. Cum $fg = 1$ este echivalent cu

$$a_0 b_0 = 1,\ a_0 b_1 + a_1 b_0 = 0, \ldots, a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0 = 0, \ldots,$$

putem construi pe g astfel: alegem mai întâi $b_0 = a_0^{-1}$. Apoi b_1 se obţine din $a_0 b_1 + a_1 b_0 = 0$, mai precis $b_1 = -a_0^{-1} a_1 b_0$. Recurent construim $b_0, b_1, \ldots$, unde $b_n = -a_0^{-1}(a_1 b_{n-1} + \ldots a_n b_0)$.
(iii) Se procedează la fel ca la soluţia problemei similare pentru polinoame, vezi problema 25(iv).

27. (i) Să observăm mai întâi că $X \in M$, altfel $M + XR[[X]] = R[[X]]$, deci există $f \in R[[X]]$ cu $1 - Xf \in M$. Dar seria formală $1 - Xf$ este inversabilă, deoarece are primul termen 1 (folosim problema 26(ii)), de unde rezultă că $M = R[[X]]$, contradicţie.
Fie $f = a_0 + a_1 X + \ldots \in M$. Atunci $f - a_0 \in XR[[X]] \subseteq M$, de unde $a_0 \in M \cap R$. Rezultă că $f \in (M \cap R)R[[X]] + XR[[X]]$. Prin urmare $M \subseteq (M \cap R)R[[X]] + XR[[X]]$. Incluziunea inversă este imediată. Atunci avem $R[[X]]/M \simeq R/M \cap R$, de unde $M \cap R$ este ideal maximal în R.
(ii) Fie R un inel local cu idealul maximal m şi fie M un ideal maximal al lui $R[[X]]$. Folosind (i) rezultă că $M \cap R = m$ şi $M = mR[[X]] + XR[[X]]$.
(iii) Să presupunem că $R[X]$ ar fi inel local cu idealul maximal M. Atunci X şi $1 - X$ sunt în M, altfel ar fi inversabile în $R[X]$ (din problema 28(ii)). Atunci $1 = X + (1 - X) \in M$, contradicţie.

28. Fie Q un ideal prim al lui $R[[X]]$. Notăm $P = \{a \in R \mid \text{există } f = a + a_1X + a_2X^2 + \cdots \in Q\}$. Cum P este ideal al lui R, rezultă că există $a_1, \ldots, a_r \in P$ astfel încât $P = (a_1, \ldots, a_r)$.
Dacă $X \in Q$, atunci $Q = (a_1, \ldots, a_r, X)$.
Dacă $X \notin Q$, fie $f_1, \ldots, f_r \in Q$ serii formale astfel încât termenul liber al lui f_j să fie a_j, $j = 1, \ldots, r$. Are loc relaţia $Q = (f_1, \ldots, f_r)$. Într-adevăr, fie $g \in Q$. Atunci termenul liber al lui g se poate scrie sub forma $b_{10}a_1 + \cdots + b_{1r}a_r$. Se obţine $g - (b_{10}f_1 + \cdots + b_{r0}f_r) = Xg_1 \in Q$. Cum $X \notin Q$, rezultă că $g_1 \in Q$, deci, procedînd ca mai sus, putem scrie $g_1 - (b_{11}f_1 + \cdots + b_{r1}f_r) = Xg_2 \in Q$. De aici, $g_2 \in Q$. Inductiv găsim $b_{1k}, \ldots, b_{rk}$ aşa încât $g_k - (b_{1k}f_1 + \cdots + b_{rk}f_r) = Xg_{k+1} \in Q$, de unde $g_{k+1} \in Q$. Este clar acum că $h_i = b_{10} + b_{i1}X + \cdots$ verifică relaţia $g = h_1f_1 + \cdots + h_rf_r$.
În concluzie, orice ideal prim al lui $R[[X]]$ este finit generat. Conform problemei 24(ii) din Capitolul 4, $R[[X]]$ este inel noetherian.

29. Presupunem prin absurd că $\mathbb{Z}[[X]]/(X-2) \simeq \mathbb{Z}$. Cum $J(\mathbb{Z}) = 0$ (pentru definiţia radicalului Jacobson a se vedea problema 44 din Capitolul 4), rezultă că $J(\mathbb{Z}[[X]]/(X-2)) = 0$. Dar idealele maximale ale lui $\mathbb{Z}[[X]]$ sunt de forma $p\mathbb{Z}[[X]] + X\mathbb{Z}[[X]]$, unde p este număr prim (din problema 27(i)), deci singurul ideal maximal al lui $\mathbb{Z}[[X]]$ care îl conţine pe $(X-2)$ este $2\mathbb{Z}[[X]] + X\mathbb{Z}[[X]]$ şi în mod evident incluziunea este strictă. Aşadar $\mathbb{Z}[[X]]/(X-2)$ este inel local cu idealul maximal nenul, ceea ce contrazice presupunerea făcută.

30. Din problema 27(i) rezultă imediat că $J(R[[X]]) = J(R)[[X]]$.
Dacă $f \in J(R[X])$, atunci $1 - Xf \in U(R[X])$ (din problema 42(iii) din Capitolul 4). Din problema 25(ii) rezultă că toţi coeficienţii lui f sunt nilpotenţi, deci $f \in N(R[X])$. Obţinem că $J(R[X]) \subseteq N(R[X])$. Incluziunea inversă este clară, de unde rezultă egalitatea.

31. (i) Este clar că $G_I \neq \emptyset$, deoarece $0 \in G_I$. De asemenea, dacă $a, b \in G_I$, atunci există $f, g \in I$, $f = aX^n + \alpha_{n+1}X^{n+1} + \ldots$, $g = bX^n + \beta_{n+1}X^{n+1} + \ldots$, şi cum $f - g = (a-b)X^n + (\alpha_{n+1} - \beta_{n+1})X^{n+1} + \ldots$, rezultă că $a - b \in G_I$, ceea ce arată că G_I este subgrup în $(K, +)$.
Presupunem că I este ideal maximal al lui R. Fie atunci $G_I \leq G \leq (K, +)$ cu $G \neq K$. Definim

$$J = \{f \in R \mid (\exists)\alpha \in G \text{ cu } f = \alpha X^n + \alpha_2 X^{n+1} + \ldots\}.$$

Este imediat că J este ideal al lui R şi $I \subseteq J$. În plus $J \neq R$, altfel am avea $n = 1$ şi $G = K$. Cum I este ideal maximal, rezultă că $J = I$. Atunci dacă $a \in G$, avem $aX^n \in J$, deci $aX^n \in I$, de unde $a \in G_I$. Am obţinut că $G_I = G$, ceea ce arată că G_I este subgrup maximal.
(ii) Evident $I_G \neq \emptyset$, deoarece $0 \in I_G$. De asemenea, dacă $f, g \in I_G$, $f = aX + \alpha_2 X^2 + \ldots$, $g = bX + \beta_2 X^2 + \ldots$ cu $a, b \in G$, atunci $f - g = (a-b)X + \ldots \in I_G$, şi $qf = q_1 a X^2 + \ldots \in I_G$ pentru orice $q = q_1 X + \ldots \in R$, deci I_G este ideal al lui R.
Presupunem acum că G este subgrup maximal în $(K, +)$. Fie J un ideal al lui R cu $I_G \subseteq J$ şi $J \neq R$. Atunci

$$G \subseteq H = \{a \in R \mid (\exists) f \in J \text{ cu } f = aX + \ldots\},$$

deoarece dacă $a \in G$, atunci $aX \in I_G$, deci $aX \in J$, de unde $a \in H$. Este clar că H este subgrup în $(K, +)$.
Arătăm că $H \neq K$. Într-adevăr, dacă $H = K$ avem $1 \in H$, deci există $f = X + a_2 X^2 + \ldots \in J$. Atunci $f = Xu$, unde u este un element inversabil în inelul seriilor formale $K[[X]]$ (conform problemei 26(ii)). Atunci pentru orice $g \in R$ de forma $g = b_2 X^2 + \ldots$ avem $g = X^2 q$ pentru un $q \in K[[X]]$, de unde $g = XuXu^{-1}q \in J$, pentru că $Xu = f \in J$ şi $Xu^{-1}q \in R$. Fie acum $h = c_1 X + c_2 X^2 + \ldots \in R$. Atunci $g = c_2 X^2 + \ldots \in J$. Pe de altă parte $c_1 \in K = H$, deci există $p = c_1 X + d_2 X^2 + \ldots \in J$. Cum $d_2 X^2 + \ldots \in J$, obţinem că $c_1 X \in J$. Atunci $h = c_1 X + g \in J$, ceea ce înseamnă că $J = R$, contradicţie. Prin urmare $H \neq K$.
Obţinem $H = G$, deoarece G este maximal. Dacă $f = aX + \ldots \in J$, atunci avem că $a \in H$, deci $a \in G$, şi deci $f \in I_G$. Obţinem $J = I_G$, ceea ce arată că I_G este maximal.
(iii) Rezultă direct din (i) şi (ii).
(iv) Dacă grupul $(K, +)$ este divizibil, atunci pentru orice $n \in \mathbb{Z} - \{0\}$ şi orice $a \in K$, ecuaţia $nx = a$ are soluţie $x \in K$. În particular, pentru orice p prim ecuaţia $px = 1$ are soluţie în K, de unde $\mathrm{char}(K) \neq p$. Rămâne că $\mathrm{char}(K) = 0$.
Reciproc, dacă $\mathrm{char}(K) = 0$, atunci orice $n \in \mathbb{Z} - \{0\}$ este inversabil în K şi atunci ecuaţia $nx = a$ are soluţia $x = n^{-1}a$.
(v) Dacă grupul $(K, +)$ are subgrupuri maximale, atunci, din problema 37(ii) din Capitolul 3, el nu este divizibil şi din (iv) rezultă $\mathrm{char}(K) \neq 0$.
Reciproc, dacă $\mathrm{char}(K) = p > 0$, atunci K are un subcorp izomorf cu corpul $\mathbb{Z}_p$, deci putem să privim pe K ca pe un $\mathbb{Z}_p$-spaţiu vectorial. Atunci K are un $\mathbb{Z}_p$-subspaţiu vectorial maximal (este suficient să luăm o bază B a lui K,

un element $b \in B$, şi atunci $\mathbb{Z}_p$-subspaţiul vectorial generat de $B - \{b\}$ este maximal), care este evident şi un subgrup maximal al lui $(K, +)$.
(vi) Rezultă direct din (iii) şi (vi).

32. (i) Fie I un ideal propriu al lui $K[[X]]$ şi fie $n = \inf\{\text{ord}(f) \mid f \in I\}$. Atunci $n \geq 1$, altfel există $f \in I$ cu $\text{ord}(f) = 0$ şi cum un astfel de f este inversabil, rezultă că $I = K[[X]]$, contradicţie.
Vom arăta că $I = (X^n)$. Dacă $f \in I$, atunci $\text{ord}(f) \geq n$, deci $f = a_nX^n + a_{n+1}X^{n+1} + \ldots = X^n(a_n + a_{n+1}X + \ldots) \in (X^n)$, de unde $I \subseteq (X^n)$. Pe de altă parte, există $f \in I$ cu $\text{ord}(f) = n$ şi atunci $f = X^n u$, cu $\text{ord}(u) = 0$, adică u este inversabil. Atunci $X^n = X^n uu^{-1} = fu^{-1} \in I$, de unde $(X^n) \subseteq I$. Obţinem că $I = (X^n)$.
În particular, singurul ideal maximal al lui $K[[X]]$ este (X), deci $K[[X]]$ este inel local.
(ii) Este uşor de văzut că dacă $f = a_0 + a_2X^2 + \ldots$ cu $a_0 \neq 0$, atunci f este inversabil în R (într-adevăr, inversul lui f din $K[[X]]$, calculat în soluţia problemei 26(ii), se găseşte în R). Fie I un ideal propriu nenul al lui R. Atunci $n = \inf\{\text{ord}(g) \mid g \in I\} \geq 2$ şi există $f = a_nX^n + a_{n+1}X^{n+1} + \ldots \in I$ cu $a_n \neq 0$. Cum $a_n \neq 0$, există $u \in K[[X]]$ cu $(a_n + a_{n+1}X + \ldots)u = 1$. Atunci $X^{n+2} = X^2fu \in I$ şi $X^{n+3} = X^3fu \in I$. De aici rezultă că $a_{n+2}X^{n+2} + a_{n+3}X^{n+3} + \ldots = X^{n+2}(a_{n+2} + a_{n+4}X^2 + \ldots) + a_{n+3}X^{n+3} \in I$, şi mai departe că $a_nX^n + a_{n+1}X^{n+1} \in I$. Avem două cazuri:
1. Există $g \in I$, $g = b_nX^n + b_{n+1}X^{n+1} + \ldots$ cu proprietatea că $a_nb_{n+1} \neq a_{n+1}b_n$.
Avem că $b_nX^n + b_{n+1}X^{n+1} \in I$. Într-adevăr, dacă $b_n \neq 0$ rezultă din cele arătate mai sus. Dacă $b_n = 0$, atunci $b_{n+1} \neq 0$ şi din nou ca mai sus avem că $b_{n+1}X^{n+1} + b_{n+2}X^{n+2} \in I$. Dar ştim deja că $X^{n+2} \in I$ şi obţinem că $b_{n+1}X^{n+1} \in I$.
Atunci avem că $a_n(b_nX^n + b_{n+1}X^{n+1}) \in I$ şi cum $b_n(a_nX^n + a_{n+1}X^{n+1}) \in I$, obţinem prin scădere că $(a_nb_{n+1} - a_{n+1}b_n)X^{n+1} \in I$, de unde $X^{n+1} \in I$. În continuare rezultă că $a_nX^n \in I$, deci $X^n \in I$, şi obţinem că $(X^n, X^{n+1}) \subseteq I$. Dar incluziunea inversă este evidentă din relaţia $c_nX^n + c_{n+1}X^{n+1} + \ldots = X^n(c_n + c_{n+2}X^2 + \ldots) + c_{n+1}X^{n+1}$. Rezultă că $I = (X^n, X^{n+1})$.
2. Pentru orice $g = b_nX^n + b_{n+1}X^{n+1} + \ldots \in I$ avem $a_nb_{n+1} = a_{n+1}b_n$.
Fie $a = a_n^{-1}a_{n+1}$. Arătăm că $I = (X^n + aX^{n+1})$. Deoarece $a_nX^n + a_{n+1}X^{n+1} \in I$ rezultă că $a_n^{-1}(a_nX^n + a_{n+1}X^{n+1}) \in I$, deci $X^n + aX^{n+1} \in I$. Invers, fie $h \in I$, $h = c_nX^n + c_{n+1}X^{n+1} + \ldots$. Atunci se verifică uşor că $g = (X^n + aX^{n+1})(d_0 + d_2X^2 + \ldots)$, unde $d_0 = c_n, d_2 = c_{n+2}, d_i = c_{n+i} - ad_{i-1}$

pentru orice $i \geq 3$ (notăm că relaţia $ad_0 = c_{n+1}$ este verificată deoarece $a_n c_{n+1} = a_{n+1} c_n$). Aşadar $g \in I$ şi rezultă că $I = (X^n + aX^{n+1})$.
Este clar acum că R este un inel local cu idealul maximal (X^2, X^3).

33. Este evident că $U_1(K[[X]])$ este grup cu înmulţirea seriilor formale. Fie $N > 0$. Se arată imediat prin inducţie după N că dacă $f = 1 + a_1X + a_2X^2 + \ldots$, atunci

$$f^N = 1 + Na_1X + (Na_2 + h_2(a_1))X^2 + (Na_3 + h_3(a_1, a_2))X^3 + \ldots$$

pentru nişte funcţii polinomiale $h_2, h_3, \ldots$ care nu depind de f. Fie $g = 1 + b_1X + b_2X^2 + \ldots \in U_1(K[[X]])$. Atunci

$$g^N = 1 + Nb_1X + (Nb_2 + h_2(b_1))X^2 + (Nb_3 + h_3(b_1, b_2))X^3 + \ldots$$

Dacă $\phi_N(f) = \phi_N(g)$, identificând coeficienţii rezultă că
• $Na_1 = Nb_1$ şi cum $N1_K \neq 0$, deci este inversabil, obţinem că $a_1 = b_1$.
• $Na_2 + h_2(a_1) = Nb_2 + h_2(b_1)$, şi cum $a_1 = b_1$, obţinem că $Na_2 = Nb_2$, deci $a_2 = b_2$.
• Recurent obţinem că $a_i = b_i$ pentru orice $i \geq 1$.
Rezultă că $f = g$, deci ϕ_N este injectivă.
Pentru surjectivitate, fie $u = 1 + u_1X + u_2X^2 + \ldots \in U_1(K[[X]])$. Căutăm $f = 1 + a_1X + a_2X^2 + \ldots$ cu $f^N = u$. Aceasta este echivalent cu

$$\begin{gathered} Na_1 = u_1 \\ Na_2 + h_2(a_1) = u_2 \\ \ldots\ldots\ldots\ldots\ldots \end{gathered}$$

sistem în $a_1, a_2, \ldots$ care se rezolvă ecuaţie cu ecuaţie (începând cu prima) şi rezultă soluţii pentru $a_1, a_2, \ldots$ (din nou folosim la fiecare ecuaţie faptul că $N1_K$ este inversabil).
Este clar că ϕ_N este morfism de grupuri deoarece $\phi_N(fg) = (fg)^N = f^N g^N = \phi_N(f)\phi_N(g)$. Aşadar ϕ_N este izomorfism de grupuri.
Considerăm aplicaţia $\psi : U_1(K[[X]]) \to U_1(K[[X]])$, $\psi(f) = f^{-1}$, care este evident izomorfism de grupuri. Atunci $\psi\phi_N = \phi_{-N}$, deci şi ϕ_{-N} este izomorfism de grupuri.

34. (i) Primele două formule rezultă uşor prin calcule directe, iar a treia se obţine din a doua prin inducţie după n.

(ii) Scriem $A = 1 + a_1X + a_2X^2 + \ldots$ şi $B = 1 + b_1X + b_2X^2 + \ldots$. Dacă egalăm coeficienţii în $A'B = AB'$, rezultă că $a_1 = b_1$, $a_1b_1 + 2a_2 = a_1b_1 + 2b_2$, $a_1b_2 + 2a_2b_1 + 3a_3 = a_2b_1 + 2a_1b_2 + 3b_3, \ldots$. De aici rezultă printr-o inducţie ale cărei detalii sunt uşoare că $a_1 = b_1$, $a_2 = b_2, a_3 = b_3, \ldots$, deci $A = B$.
(iii) Rezultă imediat din identificarea coeficienţilor.

35. (i) Avem $F_i' = \sum_{j\geq 1} ja_{ij}X^{j-1} = \sum_{j\geq 1}(j+1)a_{i,j+1}X^j$, şi cum pentru orice j şirul $((j+1)a_{i,j+1})_{i\geq 0}$ conţine doar un număr finit de elemente nenule, rezultă că familia $(F_i')_{i\geq 0}$ este sumabilă. Cum $\sum_{i\geq 0}(j+1)a_{i,j+1} = (j+1)b_{j+1}$, obţinem că $F' = \sum_{i\geq 0} F_i'$.
(ii) Deoarece familia $(F_i)_{i\geq 0}$ este sumabilă, pentru orice $j \geq 0$ doar un număr finit de serii formale din familie, fie acestea $F_{i_1}, \ldots, F_{i_s}$, au coeficientul vreunui X^r, cu $r \leq j$, nenul. Atunci pentru orice $i \neq i_1, \ldots, i_s$ seria formală GF_i are coeficienţii lui X^r cu $r \leq j$ nuli. Prin urmare familia $(F_iG)_{i\geq 0}$ este sumabilă şi egalitatea coeficienţilor lui X^j din $(\sum_{i\geq 0} F_i)G$ şi $\sum_{i\geq 0} F_iG$ rezultă din egalitatea $(F_{i_1} + \ldots + F_{i_s})G = F_{i_1}G + \ldots + F_{i_s}G$.

36. (i) Deoarece familia $(\frac{1}{n!}f^n)_{n>0}$ este sumabilă, rezultă din problema 35(ii) că şi familia $(\frac{1}{(n-1)!}f^{n-1}f')_{n>0}$, care constă din derivatele seriilor formale din prima familie, este sumabilă şi în plus $(\exp(f))' = \sum_{n>0} \frac{1}{(n-1)!}f^{n-1}f' = (\exp(f))f'$.
(ii) Fie $f = 1 - g \in XK[[X]]$. Atunci $\log(g) = -\sum_{n>0} \frac{1}{n}f^n$ şi aplicând problema 35(ii) obţinem că $(\log(g))' = -(1 + \sum_{n>0} f^n)f'$. Pe de altă parte arătăm că $(1-f)(1+\sum_{n>0} f^n) = 1$. Într-adevăr, pentru orice $j > 0$ coeficientul lui X^j din $(1-f)(1+\sum_{n>0} f^n)$ este egal cu coeficientul lui X^j din $(1-f)(1+\sum_{0<n\leq j} f^n) = 1 - f^{j+1}$ (deoarece în f^n coeficientul lui X^j este 0 pentru orice $n > j$). Dar coeficientul lui X^j din $1 - f^{j+1}$ este 0. Obţinem că $(1-f)(1+\sum_{n>0} f^n) = 1$.
Atunci

$$\begin{aligned} g(\log(g))' &= (1-f)(\log(g))' \\ &= -(1-f)(1+\sum_{n>0} f^n)f' \\ &= -f' \\ &= g'. \end{aligned}$$

(iii) Avem $(\exp(\log(g)))' = \exp(\log(g))(\log(g))'$ şi atunci

$$\begin{aligned} g(\exp(\log(g)))' &= \exp(\log(g)) \cdot g \cdot (\log(g))' \\ &= \exp(\log(g)) \cdot g' \end{aligned}$$

Aplicând problema 34(ii) rezultă că $\exp(\log(g)) = g$.
(iv) Folosind formula de la (iii) pentru $g = \exp(f)$ obţinem că

$$(\exp(f))(\log(\exp(f)))' = (\exp(f))'.$$

Folosind (i) rezultă că $(\exp(f))(\log(\exp(f)))' = \exp(f)f'$. Cum $\exp(f)$ este inversabil în $K[[X]]$, rezultă că $(\log(\exp(f)))' = f'$. Din problema 34(iii) rezultă că $\log(\exp(f)) = f$.
(v) Avem

$$\begin{aligned} \exp(f+h) &= 1 + \sum_{n>0} \frac{1}{n!}(f+h)^n \\ &= \sum_{n\geq 0} \frac{1}{n!}(f+h)^n \\ &= \sum_{n\geq 0} \sum_{0\leq i\leq n} \frac{1}{i!(n-i)!} f^i h^{n-i} \\ &= (\sum_{m\geq 0} \frac{1}{m!} f^m)(\sum_{p\geq 0} \frac{1}{p!} f^p) \\ &= \exp(f)\exp(h). \end{aligned}$$

(vi) Din (iii) şi (iv) rezultă că exp şi log sunt funcţii inverse una celeilalte, iar din (v) rezultă că exp (deci şi log) este morfism de grupuri.

37. (i) Fie $\alpha = \frac{a}{N} = \frac{b}{M}$. Fie $g = \phi_{NM}^{-1}(1+X)$, deci $g^{NM} = 1+X$. Rezultă că $(g^M)^N = 1+X$, deci $g^M = \phi_N^{-1}(1+X)$, şi atunci $(\phi_N^{-1}(1+X))^a = g^{Ma}$. De asemenea $(g^N)^M = 1+X$, deci $g^N = \phi_M^{-1}(1+X)$, de unde $(\phi_M^{-1}(1+X))^b = g^{Nb}$.
Dar $\frac{a}{N} = \frac{b}{M}$, de unde $Ma = Nb$ şi atunci $(\phi_N^{-1}(1+X))^a = g^{Ma} = g^{Nb} = (\phi_M^{-1}(1+X))^b$, adică definiţia lui $(1+X)^\alpha$ nu depinde de reprezentarea lui α ca fracţie raţională.
(ii) Fie $g \in U_1(K[[X]])$. Atunci $\log(g^N) = N\log(g)$ pentru orice N întreg, deoarece log este morfism de grupuri. Rezultă că $\log(g) = \frac{1}{N}\log(g^N)$. Pentru

$g = f^{\frac{1}{N}} = \phi_N^{-1}(f)$, cu $f \in U_1(K[[X]])$, obţinem că $\log(f^{\frac{1}{N}}) = \frac{1}{N}\log(f)$, de unde pentru orice a întreg avem $\frac{a}{N}\log(f) = \log(f^{\frac{a}{N}})$. Aşadar $\log(f^\alpha) = \alpha\log(f)$ pentru orice $\alpha \in \mathbb{Q}$. Atunci

$$\begin{aligned}\exp(\alpha\log(1+X)) &= \exp(\log((1+X)^\alpha)) \\ &= (1+X)^\alpha.\end{aligned}$$

(iii) Avem $\alpha\log(1+X) = -\sum_{m>0}\frac{\alpha}{m}(-X)^m$ şi

$$\begin{aligned}(1+X)^\alpha &= \exp(\alpha\log(1+X)) \\ &= 1 + \sum_{n>0}\frac{\alpha^n}{n!}\left(\sum_{m>0}\frac{(-X)^m}{m}\right)^n.\end{aligned}$$

Cum pentru un j fixat X^j apare cu coeficient nenul în $\left(\sum_{m>0}\frac{(-X)^m}{m}\right)^n$ doar pentru un număr finit de valori ale lui n (este necesar ca $n \leq j$), rezultă că orice coeficient în $(1+X)^\alpha$ este funcţie polinomială de α.
(iv) Din (iii) avem că există polinoame $P_1, P_2, \ldots \in K[T]$ astfel încât

$$(1+X)^\alpha = 1 + P_1(\alpha)X + P_2(\alpha)X^2 + \ldots$$

pentru orice $\alpha \in \mathbb{Q}$. Fixăm un $j > 0$ şi arătăm că $P_j(T) = \frac{1}{j!}T(T-1)\ldots(T-j+1)$. Deoarece pentru orice $n \geq j$ avem din binomul lui Newton că $(1+X)^n = 1 + C_n^1X + C_n^2X^2 + \ldots + C_n^nX^n$, privind coeficientul lui X^j obţinem că $P_j(n) = C_n^j = \frac{1}{j!}n(n-1)\ldots(n-j+1)$. Prin urmare dacă notăm $F(T) = \frac{1}{j!}T(T-1)\ldots(T-j+1)$, avem că $P_j(n) = F(n)$ pentru orice n întreg, $n \geq j$. Deoarece funcţiile polinomiale ataşate polinoamelor P_j şi F sunt egale pentru o infinitate de valori, rezultă că $P_j = F$, deci $P_j(\alpha) = \frac{\alpha(\alpha-1)\ldots(\alpha-n+1)}{n!} = \binom{\alpha}{n}$ pentru orice α raţional, ceea ce încheie soluţia.

38. (i) Avem

$$\begin{aligned}F^2 &= X^2 + (T_1T_2 + T_2T_1)X^3 + \ldots + (T_1T_{n-1} + \ldots + T_{n-1}T_1)X^n + \ldots \\ &= T_2X^2 + T_3X^3 + \ldots + T_nX^n + \ldots \\ &= F - X\end{aligned}$$

(ii) Cum $F^2 - F = -X$, avem că $(1-2F)^2 = 1-4X$. Cum $1-2F, 1-4X \in U_1(\mathbb{Q}[[X]])$, rezultă din problema 33 că $1-2F = \phi_2^{-1}(1-4X)$, deci

$$F = \frac{1}{2} - \frac{1}{2}\phi_2^{-1}(1-4X)$$

(iii) Folosim formula

$$(1+Y)^{1/2} = 1 + \binom{1/2}{1}Y + \ldots + \binom{1/2}{n}Y^n + \ldots$$

care rezultă din Problema 37(iv) pentru $\alpha = 1/2$ în inelul $\mathbb{Q}[[Y]]$ şi facem "schimbarea de variabilă" $Y = -4X$. Obţinem formula

$$\phi_2^{-1}(1-4X) = 1 + (-4)\binom{1/2}{1}X + \ldots + (-4)^n\binom{1/2}{n}X^n + \ldots \qquad (11.1)$$

Riguros, această "schimbare de variabilă" se poate explica astfel. Rezultă printr-o verificare imediată că aplicaţia $\Psi : \mathbb{Q}[[Y]] \to \mathbb{Q}[[X]]$ definită prin

$$\Psi(a_0 + a_1Y + \ldots + a_nY^n + \ldots) = a_0 + (-4)a_1X + \ldots + (-4)^n a_n X^n + \ldots$$

este un izomorfism de inele. Avem că

$$1 - 4X = \Psi(1+Y) = \Psi(((1+Y)^{1/2})^2) = (\Psi((1+Y)^{1/2}))^2$$

de unde $\phi_2^{-1}(1-4X) = \Psi((1+Y)^{1/2})$. Ţinând cont de formula pentru $(1+Y)^{1/2}$ din Problema 37(iv) şi de definiţia lui Ψ, obţinem formula (11.1). Atunci coeficientul lui X^n din $\phi_2^{-1}(1-4X)$ este

$$\begin{aligned}
(-4)^n\binom{1/2}{n} &= \frac{\frac{1}{2}(\frac{1}{2}-1)\ldots(\frac{1}{2}-n+1)}{n!}\cdot(-4)^n \\
&= \frac{1\cdot(-1)\cdot(-3)\cdot\ldots\cdot(-(2n-3))}{2^n\cdot n!}\cdot(-4)^n \\
&= \frac{(-1)^{n-1}\cdot 1\cdot 3\cdot\ldots\cdot(2n-3)}{n!}\cdot(-1)^n\cdot 2^n \\
&= -\frac{1\cdot 2\cdot 3\cdot 4\cdot\ldots\cdot(2n-3)\cdot(2n-2)}{n!\cdot 2\cdot 4\cdot\ldots\cdot(2n-2)}\cdot 2^n \\
&= -\frac{(2n-2)!}{n!\cdot 2^{n-1}\cdot(n-1)!}\cdot 2^n \\
&= -\frac{2}{n}C_{2n-2}^{n-1}
\end{aligned}$$

ceea ce demonstrează formula dorită.
(iv) Rezultă imediat prin identificarea coeficienţilor lui X^n în $F = \frac{1}{2} -$

$\frac{1}{2}\phi_2^{-1}(1-4X)$, dacă ţinem cont de formula pentru $\phi_2^{-1}(1-4X)$ din (iii).

39. (i) Notăm $K = k[X]/(f)$.
"$\Rightarrow$" Să presupunem că f este reductibil. Fie $f = gh$ o descompunere a lui f în $k[X]$. Reducând această relaţie modulo (f), obţinem $\widehat{0} = \widehat{g}\widehat{h}$. Inelul K fiind corp, rezultă că $\widehat{g} = \widehat{0}$ sau $\widehat{h} = \widehat{0}$, adică $f|g$ (şi h este inversabil) sau $f|h$ (şi g este inversabil). Prin urmare, f este ireductibil în $k[X]$.
"$\Leftarrow$" Este suficient să probăm că orice element nenul din K este inversabil. Fie aşadar $\widehat{g} \in K \setminus \{\widehat{0}\}$. Rezultă că $f \nmid g$, deci $(f, g) = 1$ în $k[X]$. Cum $k[X]$ este inel principal, rezultă că există $F, G \in k[X]$ astfel încât $fF + gG = 1$. Trecând la clase se obţine $\widehat{g}\widehat{G} = \widehat{1}$, deci $\widehat{g} \in U(K)$.
(ii) Fie g un factor al lui f ireductibil peste Q. Atunci, conform punctului (i), $L = Q[X]/(g)$ este corp. Remarcăm că aplicaţia $j : Q \to L$, $j(a) = \widehat{a}$ pentru orice $a \in Q$, este morfism de corpuri. Considerăm acum o mulţime M disjunctă de L şi pentru care există o bijecţie $u : M \to L \setminus j(Q)$ (există astfel de mulţimi, de exemplu $(L \setminus j(Q)) \times \{L\}$). Definim $v : Q \cup M \to L$,

$$v(x) = \begin{cases} u(x), & x \in M \\ j(x), & x \in Q \end{cases}$$

Din definiţia lui v şi din proprietăţile funcţiilor u şi j rezultă imediat că v este bijectivă. Pe mulţimea $k = Q \cup M$ definim operaţiile $x \bigoplus y = v^{-1}(v(x)+v(y))$ şi $x \bigotimes y = v^{-1}(v(x)v(y))$. Se arată fără dificultate că aceste operaţii definesc pe k o structură de corp comutativ.
Prezentăm ca exemplu verificarea distributivităţii. Fie $x, y, z \in k$. Atunci

$$\begin{aligned} x \bigotimes (y \bigoplus z) &= v^{-1}(v(x)v(y \bigoplus z)) \\ &= v^{-1}(v(x)v(v^{-1}(v(y) + v(z)))) \\ &= v^{-1}(v(x)(v(y) + v(z))) \\ &= v^{-1}(v(x)v(y) + v(x)v(z)) \\ &= v^{-1}(v(v^{-1}(v(x)v(y))) + v(v^{-1}(v(x)v(z)))) \\ &= v^{-1}(v(x \bigotimes y) + v(x \bigotimes z)) \\ &= (x \bigotimes y) \bigoplus (x \bigotimes z). \end{aligned}$$

Să observăm acum că v este izomorfism de corpuri. Într-adevăr, pentru orice $x, y \in k$ avem $v(x \bigoplus y) = v(v^{-1}(v(x) + v(y))) = v(x) + v(y)$ şi $v(x \bigotimes y) =$

$v(v^{-1}(v(x)v(y))) = v(x)v(y)$. În plus, $v(1) = j(1) = 1$.
Prin urmare, v este morfism de corpuri. Cum v este şi bijecţie, rezultă că v este izomorfism. În consecinţă, $(k, \bigoplus, \bigotimes)$ este un corp comutativ. Cum pentru orice $x, y \in Q$ avem $x \bigoplus y = x + y$ şi $x \bigotimes y = xy$, rezultă că Q este subcorp al lui k. Dacă punem acum $g = a_0 + a_1X + \cdots + a_rX^r$, atunci

$$\begin{aligned} g(v^{-1}(\widehat{X})) &= a_0 \bigoplus a_1 \bigotimes v^{-1}(\widehat{X}) \bigoplus \cdots \bigoplus a_r \bigotimes v^{-1}(\widehat{X})^r \\ &= v^{-1}(j(a_0) + j(a_1)\widehat{X} + \cdots + j(a_r)\widehat{X}^r) \\ &= v^{-1}(\widehat{a_0} + \widehat{a_1}\widehat{X} + \cdots + \widehat{a_r}\widehat{X}^r) \\ &= v^{-1}(\widehat{a_0 + a_1X + \cdots + a_rX^r}) \\ &= 0. \end{aligned}$$

În concluzie, $v^{-1}(\widehat{X}) \in k$ este rădăcină pentru g (deci şi pentru f).
(iii) Procedăm prin inducţie după $n = \operatorname{grad} f$. Dacă $n = 1$, atunci putem lua $K = Q$. Fie acum $n > 1$. Presupunem afirmaţia adevărată pentru toate polinoamele de grad mai mic decât n. Conform punctului (ii), există un corp K_1 care conţine Q ca subcorp şi în care f are cel puţin o rădăcină, fie aceasta a. Atunci putem scrie $f = (X - a)f_1$, unde $f_1 \in K_1[X]$ are gradul $n - 1$. Conform ipotezei de inducţie, există un corp K în care f_1 are toate rădăcinile şi care conţine pe K_1 ca subcorp. Deci K conţine pe Q ca subcorp şi întrucât f are drept rădăcini exact pe a şi rădăcinile lui f_1, atunci f are toate rădăcinile în K.

40. Vom arăta că exponentul oricărui divizor prim al lui a este multiplu de n, ceea ce garantează că a este putere a n-a a unui număr întreg, deci f are o rădăcină întreagă.
Fie p un divizor prim al lui a, deci $a = p^t a'$, $t \in \mathbb{N}^*$, $a' \in \mathbb{Z}$ şi $(a', p) = 1$. Dacă t nu este multiplu al lui n, atunci există $h \in \mathbb{N}$ astfel încât $hn < t < (h+1)n$. Fie $m = p^{(h+1)n}$. Polinomul $X^n - \hat{a}$ are o rădăcină în $\mathbb{Z}_m$, deci există $x \in \mathbb{Z}$ cu $p^{(h+1)n} | x^n - a$. Cum $p|a$, avem $p|x$ şi fie $x = p^s y$, cu $y \in \mathbb{Z}$ şi $(p, y) = 1$. Cum $p^t | m$, avem şi $p^t | x^n - a = p^{ns}y^n - p^t a'$, de unde $p^t | p^{ns}y^n$, ceea ce garantează că $t \leq ns$. Atunci avem şi $hn < ns$, de unde deducem că $h < s$. Deci $h + 1 \leq s$. Dar $p^{ns} | x^n$, deci şi $p^{n(h+1)} | x^n$, adică $m | x^n$. Cum $m | x^n - a$, obţinem că $m|a$, adică $(h + 1)n < t$, contradicţie. Aşadar t trebuie să fie multiplu de n.

41. Procedăm prin inducţie după n. Dacă $n = 1$, se ştie că un polinom nenul într-o nedeterminată peste un domeniu de integritate are un număr de

rădăcini $\leq \deg(f)$, deci funcţia polinomială asociată are doar un număr finit de zerouri.
Presupunem adevărat pentru $n-1$ şi demonstrăm pentru n. Scriem

$$f(X_1, \ldots, X_n) = \sum_{0 \leq i \leq m} f_i(X_1, \ldots, X_{n-1}) X_n^i$$

unde $f_i(X_1, \ldots, X_{n-1}) \in K[X_1, \ldots, X_{n-1}]$ pentru orice $0 \leq i \leq m$. Rezultă că pentru orice $a_1 \in A_1, \ldots, a_{n-1} \in A_{n-1}$, funcţia polinomială asociată polinomului

$$f(a_1, \ldots, a_{n-1}, X_n) = \sum_{0 \leq i \leq m} \tilde{f}_i(a_1, \ldots, a_{n-1}) X_n^i \in R[X_n]$$

se anulează pentru orice $a_n \in A_n$. Cum mulţimea A_n este infinită, rezultă că polinomul $f(a_1, \ldots, a_{n-1}, X_n)$ este nul, deci $\tilde{f}_i(a_1, \ldots, a_{n-1}) = 0$ pentru orice $0 \leq i \leq m$. Din ipoteza de inducţie rezultă că $f_i(X_1, \ldots, X_{n-1}) = 0$ pentru orice $0 \leq i \leq m$. Atunci evident $f = 0$.

Dacă $\tilde{f}$ se anulează într-o mulţime infinită care nu mai este de forma $A_1 \times \ldots \times A_n$ cu A_i infinite, atunci concluzia nu mai rămâne adevărată. Pentru aceasta considerăm polinomul $f(X, Y) = XY \in \mathbb{Z}[X, Y]$. Atunci $\tilde{f}(0, y) = 0$ pentru orice $y \in \mathbb{Z}$, dar $f \neq 0$.

Dacă R nu este inel comutativ, rezultatul nu mai este adevărat. De exemplu dacă $\mathbb{H}$ este corpul cuaternionilor, atunci polinomul nenul $f(X) = X^2 + 1 \in \mathbb{H}[X]$ are o infinitate de rădăcini în $\mathbb{H}$, conform problemei 8(v).

42. Este clar că este suficient să demonstrăm afirmaţia în cazul în care f constă dintr-un singur monom (prin sumare se obţine apoi rezultatul pentru un polinom arbitrar). Fie $X_1^{k_1} \cdots X_n^{k_n}$ un monom care apare în scrierea lui f. Pentru fiecare $1 \leq i \leq n$ folosim teorema de împărţire cu rest şi obţinem $X_i^{k_i} = (X_i^q - X_i) q_i(X_i) + r_i(X_i)$, unde $q_i, r_i \in K[X_i]$ cu $\operatorname{grad} r_i < q$. Înmulţind aceste relaţii obţinem $f = \sum_{1 \leq i \leq n} (X_i^q - X_i) g_i + r_1 \cdots r_n$, şi notând $g_0 = r_1 \cdots r_n$, toate condiţiile dorite sunt satisfăcute.

43. Procedăm prin inducţie după n la fel ca la problema 41.

44. Rezultă imediat din problemele 41 şi 42 dacă ţinem cont de faptul că $x^q = x$ pentru orice $x \in K$.

45. Fie $|K| = q$. Numărul funcţiilor de la K^n la K este q^{q^n}. Pe de altă parte orice funcţie polinomială este de forma $\tilde{f}$, unde f este un polinom pentru care $\deg_{X_i}(f) < q$ pentru orice $1 \leq i \leq n$, deoarece $x^q = x$ pentru orice $x \in K$. În scrierea unui astfel de f apar numai monoame de forma $X_1^{k_1} \cdots X_n^{k_n}$, cu $k_i < q$ pentru orice $1 \leq i \leq n$. Numărul acestor monoame este q^n şi cu ele putem forma q^{q^n} polinoame cu coeficienţi în K. Dar funcţiile polinomiale asociate acestor polinoame sunt distincte din problema 42, de unde rezultă că avem exact q^{q^n} funcţii polinomiale de la K^n la K. De aici rezultă că orice funcţie $\phi : K^n \to K$ este polinomială.

46. (i) Presupunem că $\tilde{f}(a) \neq 0$ pentru orice $a \neq (0, \ldots, 0)$. Fie polinoamele $g = 1 - f^{q-1}$ şi $h = (1 - X_1^{q-1}) \cdots (1 - X_n^{q-1})$. Atunci, pentru orice $a \neq (0, \ldots, 0)$ avem $\tilde{h}(a) = 0$ (deoarece $x^{q-1} = 1$ pentru orice $x \in K$, $x \neq 0$) şi $\tilde{g}(a) = 1 - (\tilde{f}(a))^{q-1} = 0$ (deoarece $\tilde{f}(a) \in K - \{0\}$). Pentru $a = (0, \ldots, 0)$ avem $\tilde{g}(a) = \tilde{h}(a) = 1$. Rezultă că $\tilde{g} = \tilde{h}$. În plus, avem că $\deg(g) = d(q-1) < n(q-1) = \deg(h)$.
Din problema 41 rezultă că $g = \sum_{1 \leq i \leq n} (X_i^q - X_i) g_i + g_0$, cu $g_i \in K[X_1, \ldots, X_n]$ pentru orice $0 \leq i \leq n$, $\deg_{X_i}(g_0) < q$ pentru orice $1 \leq i \leq n$, şi $\deg(g_0) \leq \deg(g) = d(q-1)$. Este clar că $\tilde{g_0} = \tilde{g}$, de unde $\tilde{g_0} = \tilde{h}$. Aplicând problema 42 (observăm că g_0 şi h satisfac condiţiile impuse asupra gradelor, căci şi $\deg_{X_i}(h) < q$), rezultă că $g_0 = h$. Dar $\deg(g_0) \leq \deg(g) < \deg(h)$, contradicţie. Aşadar presupunerea făcută este falsă.
(ii) Am văzut în soluţia punctului (i) că $\tilde{g}(a) = 1$ dacă $\tilde{f}(a) = 0$ iar $\tilde{g}(a) = 0$ dacă $\tilde{f}(a) \neq 0$. Aşadar $N1_K = \sum_{a \in K^n} \tilde{g}(a)$. Dar $\tilde{g} = \tilde{g_0}$ şi din soluţia problemei 41 ştim că $g_0 = r_1 \cdots r_n$, unde $r_1 \in K[X_1], \ldots, r_n \in K[X_n]$, toate de grad mai mic decât q. Rezultă că g_0 se poate scrie sub forma

$$g_0 = \sum_{0 \leq i_1, \ldots, i_n < q} c_{i_1} \cdots c_{i_n} X_1^{i_1} \cdots X_n^{i_n}$$

şi de aici rezultă că

$$\begin{aligned} N1_K &= \sum_{(a_1, \ldots, a_n) \in K^n} \Big(\sum_{0 \leq i_1, \ldots, i_n < q} c_{i_1} \cdots c_{i_n} a_1^{i_1} \cdots a_n^{i_n} \Big) \\ &= \sum_{0 \leq i_1, \ldots, i_n < q} c_{i_1} \cdots c_{i_n} \Big(\sum_{(a_1, \ldots, a_n) \in K^n} a_1^{i_1} \cdots a_n^{i_n} \Big). \end{aligned}$$

Dar $\sum_{(a_1, \ldots, a_n) \in K^n} a_1^{i_1} \cdots a_n^{i_n} = \big(\sum_{a_1 \in K} a_1^{i_1} \big) \cdots \big(\sum_{a_n \in K} a_n^{i_n} \big)$ şi cum $\deg(g_0) \leq \deg(g) =$

$d(q-1) < n(q-1)$, rezultă că nu toţi indicii $i_1, \ldots, i_n$ sunt egali cu $q-1$. Pe de altă parte, dacă $1 \leq i < q-1$, atunci $\sum_{x \in K} x^i = 0$. Într-adevăr, cum $(K^*, \cdot)$ este grup ciclic (vezi problema 32 din Capitolul 3), există $\alpha \in K$ astfel încât $K^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$. Avem $\alpha^i - 1 \neq 0$ pentru orice $i \geq 0$ şi

$$\begin{aligned} \sum_{x \in K} x^i &= \sum_{0 \leq j \leq q-2} \alpha^{ij} \\ &= (\alpha^{(q-1)i} - 1)(\alpha^i - 1)^{-1} \\ &= ((\alpha^{(q-1)})^i - 1)(\alpha^i - 1)^{-1} \\ &= 0. \end{aligned}$$

Rezultă că $\sum_{(a_1,\ldots,a_n) \in K^n} a_1^{i_1} \cdots a_n^{i_n} = 0$ pentru orice $i_1, \ldots, i_n$. Obţinem că $N1_K = 0$, deci $p|N$.

47. Fie $K^* = \{b_1, \ldots, b_{q-1}\}$. Avem că $b_i^{q-1} = 1$ pentru orice i. Considerăm matricea

$$B = \begin{pmatrix} 1 & b_1 & \ldots & b_1^{q-2} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & b_{q-1} & \ldots & b_{q-1}^{q-2} \end{pmatrix} \in M_{q-1}(K).$$

Atunci avem

$$BA = \begin{pmatrix} f(b_1) & b_1^{-1} f(b_1) & \ldots & b_1^{-(q-2)} f(b_1) \\ \ldots & \ldots & \ldots & \ldots \\ f(b_{q-1}) & b_{q-1}^{-1} f(b_{q-1}) & \ldots & b_{q-1}^{-(q-2)} f(b_{q-1}) \end{pmatrix}.$$

$N = |\{a \in K^* \mid \tilde{f}(a) = 0\}|$ este numărul de zerouri din şirul $f(b_1), \ldots, f(b_{q-1})$. Să presupunem de exemplu că ultimii N termeni ai acestui şir sunt nuli. Atunci ultimele N linii ale matricei BA sunt nule, de unde $\text{rang}(BA) \leq q-1-N$. Pe de altă parte minorul lui BA format de primele $(q-1-N)$ linii şi primele $(q-1-N)$ coloane este nenul (determinantul este un determinant de tip Vandermonde înmulţit cu elementele nenule $f(b_1), \ldots, f(b_{q-1-N})$), deci $\text{rang}(BA) = q-1-N$. Cum B este inversabilă, rezultă că $\text{rang}(A) = q-1-N$. De aici obţinem că $N = q-1-\text{rang}(A)$.

48. (i) "$\Rightarrow$" Fie $s \in S$ şi să presupunem că s ar fi divizor al lui zero, deci $sa = 0$ pentru un $a \in R$, $a \neq 0$. Atunci $a/1 = 0/1$, deci $\phi(a) = 0/1$, ceea ce

arată că ϕ nu este injectivă, contradicţie.
"$\Leftarrow$" Dacă $\phi(a) = 0$, atunci $a/1 = 0/1$, deci există $s \in S$ cu $sa = 0$. Cum s nu este divizor al lui zero, obţinem că $a = 0$.
(ii) "$\Rightarrow$" Din (i) avem că S este format din nondivizori ai lui zero. Fie $s \in S$. Atunci există $a \in R$ cu $\phi(a) = 1/s$ (deoarece ϕ este surjectivă). De aici rezultă că $sa = 1$, deci $s \in U(R)$.
"$\Leftarrow$" Dacă $S \subseteq U(R)$, atunci clar S este format din nondivizori ai lui zero, de unde ϕ este injectivă. Fie acum $a/s \in S^{-1}R$. Atunci $a/s = \phi(as^{-1})$, deci ϕ este şi surjectivă.

49. (i) Se verifică imediat că $S^{-1}I$ este ideal în $S^{-1}R$. Fie $\phi : R \to S^{-1}R$, $\phi(a) = a/1$, morfismul canonic, şi fie J un ideal în $S^{-1}R$. Atunci $I = \phi^{-1}(J)$ este ideal în R. Arătăm că $J = S^{-1}I$. Într-adevăr, dacă $a/s \in J$, atunci $a/1 = (a/s)(s/1) \in J$, de unde $a \in I$, şi atunci $a/s \in S^{-1}I$. Invers, dacă $a \in I$ şi $s \in S$, atunci $a/1 = \phi(a) \in J$ şi $a/s = (1/s)(a/1) \in J$.
(ii) Dacă $S^{-1}I = S^{-1}R$, atunci $1/1 \in S^{-1}I$, deci există $a \in I$ şi $s \in S$ cu $a/s = 1/1$. De aici rezultă că există $t \in S$ cu $t(a-s) = 0$, deci $ta = ts \in I \cap S$ şi obţinem că $I \cap S \neq \emptyset$.
Reciproc, dacă $a \in I \cap S$, atunci $1/1 = a/a \in S^{-1}I$, deci $S^{-1}I = S^{-1}R$.
(iii) O verificare imediată arată că T este sistem multiplicativ în R/I. Fie $\pi : R \to R/I$ proiecţia canonică şi $\psi : R/I \to T^{-1}(R/I)$ morfismul canonic. Dacă $u = \psi\pi$, este imediat că $u(S) \subseteq U(T^{-1}(R/I))$ (adică pentru orice $s \in S$ avem că $u(s) = \hat{s}/\hat{1}$ este inversabil în $T^{-1}(R/I)$), şi aplicând proprietatea de universalitate a inelelor de fracţii obţinem un morfism $v : S^{-1}R \to T^{-1}(R/I)$ astfel încât $v(a/s) = \hat{a}/\hat{s}$. Este clar că v este surjectiv şi

$$\begin{aligned} \mathrm{Ker}(v) &= \{a/s \mid \hat{a}/\hat{s} = \hat{0}/\hat{1}\} \\ &= \{a/s \mid \text{există } t \in S \text{ cu } \hat{t}\hat{a} = \hat{0}\} \\ &= \{a/s \mid \text{există } t \in S \text{ cu } ta \in I\} \\ &= S^{-1}I. \end{aligned}$$

Rezultă că v induce un izomorfism de inele între $S^{-1}R/S^{-1}I$ şi $T^{-1}(R/I)$.
(iv) Verificare imediată.

50. (i) Din problema 48(ii) obţinem că $S^{-1}p \neq S^{-1}R$, iar din punctul (iii) al aceleiaşi probleme avem că $S^{-1}R/S^{-1}p \simeq T^{-1}(R/p)$. Dar R/p este inel integru, deci orice inel de fracţii al lui R/p este integru. În particular, $T^{-1}(R/p)$ este integru, de unde $S^{-1}p$ este ideal prim al lui $S^{-1}R$.

(ii) Fie $P \in \mathrm{Spec}(S^{-1}R)$. Din problema 48(i) rezultă că există un ideal p al lui R cu $P = S^{-1}p$. Deoarece $P \neq S^{-1}R$ avem $p \cap S = \emptyset$. Arătăm că p este ideal prim. Fie $a, b \in R$ cu $ab \in p$. Atunci $(a/1)(b/1) \in S^{-1}p = P$, de unde $a/1 \in P$ sau $b/1 \in P$. Fie, de exemplu, $a/1 \in P$. Atunci există $c \in p$ şi $s \in S$ cu $a/1 = c/s$, deci există $t \in S$ cu $tsa = tc \in p$. Cum $ts \in S$, avem că $ts \notin p$, deci $a \in p$.
Acum este imediat că aplicaţia $p \mapsto S^{-1}p$ este o corespondenţă bijectivă între $\mathrm{Spec}(R) \cap \Sigma$ şi $\mathrm{Spec}(S^{-1}R)$.
(iii) Fie $P \in \mathrm{Spec}(S^{-1}R)$. Atunci există $q \in \mathrm{Spec}(R)$, $q \cap S = \emptyset$, cu $P = S^{-1}q$. Deoarece $S = R - p$ şi $q \cap S = \emptyset$, rezultă că $q \subseteq p$. Atunci $P = S^{-1}q \subseteq S^{-1}p$. Dar $S^{-1}R/S^{-1}p \simeq T^{-1}(R/p)$, unde $T = \{\hat{s} \mid s \in S\} = \{\hat{s} \mid s \notin p\} = \{\hat{s} \mid \hat{s} \neq \hat{0}\} = R/p - \{\hat{0}\}$, deci $S^{-1}R/S^{-1}p$ este izomorf cu corpul de fracţii al inelului R/p. În particular $S^{-1}p \in \mathrm{Max}(S^{-1}R)$. În consecinţă $S^{-1}p$ este unicul ideal maximal al lui $S^{-1}R$.

51. Fie R inel noetherian, S un sistem multiplicativ al său şi J un ideal al lui $S^{-1}R$. Conform problemei 49, există un ideal I al lui R astfel încât $J = S^{-1}I$. Cum R este noetherian, I este ideal finit generat, să zicem $I = (a_1, \ldots, a_n)$. Evident, $(\frac{a_1}{1}, \ldots, \frac{a_n}{1}) \subseteq J$. Dacă $y \in J$, atunci există $a \in I$ şi $s \in S$ astfel ca $y = \frac{a}{s}$. Dar x fiind în I se poate scrie sub forma $\alpha_1 a_1 + \cdots + \alpha_n a_n$, unde $\alpha_1, \ldots, \alpha_n \in R$. De aici rezultă că $y = \frac{\alpha_1}{s} \cdot \frac{a_1}{1} + \cdots + \frac{\alpha_n}{s} \cdot \frac{a_n}{s}$. Prin urmare, $J = (\frac{a_1}{1}, \ldots, \frac{a_n}{1})$, deci J este ideal finit generat al lui $S^{-1}R$. Cum J a fost arbitrar, rezultă că $S^{-1}R$ este inel noetherian.

52. Este evident că $S = \mathbb{Z} - 2\mathbb{Z}$. Cum $2\mathbb{Z}$ este ideal prim al lui $\mathbb{Z}$, totul rezultă din problema 49. Idealul maximal al lui $S^{-1}\mathbb{Z}$ este $S^{-1}(2\mathbb{Z}) = \{2a/(2k+1) \mid a, k \in \mathbb{Z}\}$.

53. Un calcul simplu arată că S este sistem multiplicativ. Avem că $S^{-1}\mathbb{Z} \subseteq \mathbb{Q}$. Arătăm că această incluziune este de fapt egalitate. Fie $x \in \mathbb{Q}$, $x = a/b$, cu $a, b \in \mathbb{Z}$, $b \neq 0$. Atunci $x = 3a/3b \in S^{-1}\mathbb{Z}$.

54. Deoarece $R \subseteq R_m$ pentru orice $m \in \mathrm{Max}(R)$, avem $R \subseteq \bigcap_{m \in \mathrm{Max}(R)} R_m$. Reciproc, fie $x \in \bigcap_{m \in \mathrm{Max}(R)} R_m$. Atunci pentru orice $m \in \mathrm{Max}(R)$ există $a_m \in R$, $b_m \in R - m$, cu $x = a_m/b_m$. Pe de altă parte, idealul I generat de

mulţimea $\{b_m \mid m \in \mathrm{Max}(R)\}$ este egal cu R, altfel ar exista $n \in \mathrm{Max}(R)$ cu $I \subseteq n$, şi atunci $b_n \in n$, contradicţie. Obţinem că $1 = \sum_{1 \leq i \leq s} c_i b_{m_i}$, unde $m_1, \ldots, m_s \in \mathrm{Max}(R)$ şi $c_1, \ldots, c_s \in R$. Rezultă că $x = \sum_{1 \leq i \leq s} c_i b_{m_i} x = \sum_{1 \leq i \leq s} c_i a_{m_i} \in R$.

55. Este evident că S este sistem multiplicativ al lui R.
Notăm cu $u : R \to R[X]/(aX-1)$ morfismul obţinut prin compunerea proiecţiei canonice $R[X] \to R[X]/(aX-1)$ cu incluziunea canonică $R \to R[X]$. În inelul $R[X]/(aX-1)$ avem $\hat{a}\hat{X} = \hat{1}$, deci $\hat{a}$ este un element inversabil şi inversul său este $\hat{X}$. Rezultă că $u(S) \subseteq U(R[X]/(aX-1))$. Din proprietatea de universalitate a inelelor de fracţii există un morfism de inele $\overline{u} : S^{-1}R \to R[X]/(aX-1)$ cu $\overline{u}(r/a^n) = \hat{r}\hat{X}^n$.
Din proprietatea de universalitate a inelelor de polinoame rezultă că există un morfism de inele $v : R[X] \to S^{-1}R$ cu $v(X) = 1/a$. Este evident că $(aX-1) \subseteq \mathrm{Ker}(v)$, deci există un morfism de inele $\overline{v} : R[X]/(aX-1) \to S^{-1}R$ cu $\overline{v}(\hat{X}) = 1/a$.
Un calcul simplu arată că $\overline{u} \circ \overline{v}$ şi $\overline{v} \circ \overline{u}$ sunt aplicaţiile identice, deci $\overline{u}$ este izomorfism între $S^{-1}R$ şi $R[X]/(aX-1)$.

56. Fie $\pi : R \to R/\mathrm{Ker}(\phi)$ proiecţia canonică. Atunci avem $\pi(S) \subseteq U(R/\mathrm{Ker}(\phi))$, altfel ar exista $s \in S$ cu $\hat{s} \notin U(R/\mathrm{Ker}(\phi))$, şi atunci $\hat{s}$ este divizor al lui zero în $R/\mathrm{Ker}(\phi)$ (deoarece într-un inel comutativ finit orice element este sau inversabil sau divizor al lui zero), deci ar exista $a \in R - \mathrm{Ker}(\phi)$ cu $\hat{s}\hat{a} = 0$. Aceasta înseamnă că $sa \in \mathrm{Ker}(\phi)$, deci există $t \in S$ cu $tsa = 0$. Cum $ts \in S$, obţinem că $a \in \mathrm{Ker}(\phi)$, contradicţie.
Acum folosind proprietatea de universalitate a inelelor de fracţii găsim un morfism $\psi : S^{-1}R \to R/\mathrm{Ker}(\phi)$. Este clar că $\overline{\phi}\psi = \mathrm{Id}$, unde $\overline{\phi} : R/\mathrm{Ker}(\phi) \to S^{-1}R$ este morfismul canonic care se obţine din ϕ. Deci $\overline{\phi}$ este un morfism surjectiv (chiar izomorfism), de unde $\phi = \overline{\phi}\pi$ este surjectiv.

Considerăm acum $R = \mathbb{Z}_{12}$ şi $d = 2$. Presupunem că ar exista un sistem multiplicativ S al lui R cu $S^{-1}R \simeq \mathbb{Z}_2$. Cum $S^{-1}R \simeq R/\mathrm{Ker}(\phi)$, unde $\phi : R \to S^{-1}R$ este morfismul canonic, rezultă că $\mathrm{Ker}(\phi) = \hat{2}\mathbb{Z}_{12}$. Atunci $\hat{2} \in \mathrm{Ker}(\phi)$, deci există $s \in S$ cu $\hat{2}\hat{s} = \hat{0}$. Aceasta arată că $2s \in 12\mathbb{Z}$, adică $s \in 6\mathbb{Z}$, şi atunci $\hat{0} = \hat{s}^2 \in S$, contradicţie.

57. Fie $S = \{a \in R \mid a \neq 0 \text{ şi } 1/a \in A\}$. Este clar că S este sistem

multiplicativ al lui R şi că $S^{-1}R \subseteq A$. Arătăm acum că $A \subseteq S^{-1}R$. Fie $x \in A$. Atunci $x = a/b$ pentru nişte $a, b \in R$, $b \neq 0$. Cum idealul (a, b) este principal, există $c \in R$ cu $(a, b) = (c)$. Atunci există $a', b', \alpha, \beta \in R$ cu $a = ca'$, $b = cb'$ şi $c = a\alpha + b\beta$. Obţinem că $x = a'/b'$ şi $1a'\alpha + b'\beta$, de unde $1/b' = (a'\alpha + b'\beta)/b' = x\alpha + \beta \in A$. Rezultă că $b' \in S$, de unde $x \in S^{-1}R$.

Considerăm $R = \mathbb{Z}[i\sqrt{3}]$ şi $A = \mathbb{Z}[(1 + i\sqrt{3})/2]$. Calcule directe arată că $U(R) = \{-1, 1\}$ şi $U(A) = \{-1, 1, \frac{1}{2} + i\sqrt{3}, -\frac{1}{2} + i\sqrt{3}, \frac{1}{2} - i\sqrt{3}, -\frac{1}{2} - i\sqrt{3}\}$. Dacă ar exista S sistem multiplicativ în R cu $S^{-1}R = A$, atunci $S \subseteq U(A)$, deci $S \subseteq \{-1, 1\} = U(R)$. Dar atunci $S^{-1}R = R$, de unde $A = R$, contradicţie.

58. Folosind proprietatea de universalitate a inelelor de polinoame găsim un morfism de inele $u : R[X] \to (S^{-1}R)[X]$ astfel încât $u(a) = a/1$ pentru orice $a \in R$ şi $u(X) = X$. Deoarece $u(S) \subseteq U((S^{-1}R)[X])$, din proprietatea de universalitate a inelelor de fracţii deducem că există un morfism de inele $\overline{u} : S^{-1}(R[X]) \to (S^{-1}R)[X]$ care extinde pe u.
Fie $q : R \to R[X]$ morfismul canonic şi $v : S^{-1}R \to S^{-1}(R[X])$ morfismul definit prin $v(a/s) = q(a)/s$. Folosind proprietatea de universalitate a inelelor de polinoame obţinem că există un morfism de inele $\overline{v} : (S^{-1}R)[X] \to S^{-1}(R[X])$ care extinde pe v şi pentru care $\overline{v}(X) = X$.
Este imediat că $\overline{u} \circ \overline{v} = \mathrm{Id}$ şi $\overline{v} \circ \overline{u} = \mathrm{Id}$, ceea ce arată că $S^{-1}(R[X])$ şi $(S^{-1}R)[X]$ sunt izomorfe canonic.

Pentru serii formale putem defini un morfism canonic $\psi : S^{-1}(R[[X]]) \to (S^{-1}R)[[X]]$ prin $\psi(f/s) = \sum_{n\geq 0}(a_n/s)X^n$, unde $f = \sum_{n\geq 0} a_n X^n$. Se observă că ψ este injectiv dacă S este format din nondivizori ai lui zero. În general, ψ nu este nici injectiv, nici surjectiv. Aceasta rezultă din următoarele exemple.
• Fie K un corp, $R = K[Y_0, Y_1, \ldots, Y_n, \ldots]/(Y_0Y_1, Y_0^2Y_2, \ldots, Y_0^nY_n, \ldots)$, $S = \{\hat{Y_0}^n \mid n \in \mathbb{N}\}$ şi $f = \sum_{n\geq 0} \hat{Y}_n X^n$. Atunci $\psi(f/1) = 0$, dar $f/1 \neq 0$, deci ψ nu este injectiv.
• Fie $R = \mathbb{Z}$, $S = \mathbb{Z} - \{0\}$, p un număr prim şi $g = \sum_{n\geq 0}(1/p^n)X^n \in \mathbb{Q}[[X]]$. Dacă ar exista $f \in \mathbb{Z}[[X]]$, $f = \sum_{n\geq 0} a_n X^n$, şi $s \in S$ cu $\psi(f/s) = g$, atunci am avea $a_n/s = 1/p^n$ pentru orice n. Atunci $p^n a_n = s$, deci $p^n | s$ pentru orice n. Aceasta implică $s = 0$, contradicţie. Rezultă că ψ nu este surjectiv.

59. Este evident că S este sistem multiplicativ al lui R. Fie $\phi_i : R_i \to$

$S_i^{-1}R_i$, $i \in I$, morfismele canonice şi fie $\phi = \prod_{i\in I}\phi_i : R \to \prod_{i\in I}(S_i^{-1}R_i)$. Deoarece $\phi(S) \subseteq U(\prod_{i\in I}(S_i^{-1}R_i))$, putem folosi proprietatea de universalitate a inelelor de fracţii şi obţinem că există un morfism $u : S^{-1}R \to \prod_{i\in I}(S_i^{-1}R_i)$ care extinde pe ϕ, dat prin $u((a_i)_{i\in I}/(s_i)_{i\in I}) = (a_i/s_i)_{i\in I}$. Este o verificare simplă că u este izomorfism.

60. Presupunem că R este redus. Arătăm mai general, că $S^{-1}R$ este redus pentru orice sistem multiplicativ S al lui R. Fie $a/s \in N(S^{-1}R)$. Atunci $a^n/s^n = 0$ pentru un $n \in \mathbb{N}^*$, deci există $t \in S$ cu $ta^n = 0$. Atunci $(ta)^n = 0$, de unde $ta = 0$, ceea ce arată că $a/s = 0$.
Presupunem acum că R_m este redus pentru orice ideal maximal m. Fie $a \in N(R)$, deci $a^n = 0$ pentru un $n \in \mathbb{N}^*$. Atunci, pentru orice $m \in \mathrm{Max}(R)$ avem $(a/1)^n = 0$ în R_m, şi cum $N(R_m) = 0$ rezultă că $a/1 = 0$ în R_m. Aceasta arată că există $b_m \in R - m$ cu $b_m a = 0$. Acum un raţionament similar cu cel de la problema 53 arată că $a = 0$.

Proprietatea nu mai rămâne adevărată dacă în loc de redus considerăm integru. Fie K un corp comutativ şi $R = K \times K$. Idealele maximale ale lui R sunt $K \times \{0\}$ şi $\{0\} \times K$. Pentru $m = K \times \{0\}$ avem $S = R - m = K^* \times K$. Atunci este uşor de văzut că pentru $(a, b), (c, d) \in R$ şi $(\alpha, \beta), (\gamma, \delta) \in S$ avem că $(a, b)/(\alpha, \beta) = (c, d)/(\gamma, \delta)$ dacă şi numai dacă $a\gamma - c\alpha = 0$, adică $a/\alpha = c/\gamma$. Aceasta arată că asocierea $(a, b)/(\alpha, \beta) \mapsto a/\alpha$ defineşte un izomorfism de inele între $R_m = S^{-1}R$ şi K, în particular R_m este inel integru. La fel, dacă $m = \{0\} \times K$, rezultă că $R_m \simeq K$, care este inel integru. Este clar însă că R nu este inel integru.

61. (i) Din definiţie rezultă că $D_n(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$ este produs după toate perechile (i, j) cu $1 \le i < j \le n$ de nişte factori care sunt $X_i - X_j$ sau $X_j - X_i$ pentru fiecare astfel de pereche (i, j). În plus, numărul factorilor $X_j - X_i$ (cu $j > i$) este egal cu numărul inversiunilor lui σ. De aici rezultă formula cerută.
(ii) Avem că

$$\begin{aligned}\Delta_n(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) &= (D_n(X_{\sigma(1)}, \ldots, X_{\sigma(n)}))^2\\ &= (\varepsilon(\sigma)D_n(X_1, \ldots, X_n))^2\\ &= (D_n(X_1, \ldots, X_n))^2\\ &= \Delta_n(X_1, \ldots, X_n).\end{aligned}$$

(iii) Cum $f(X_1,\ldots,X_i,\ldots,X_j,\ldots,X_n) = -f(X_1,\ldots,X_j,\ldots,X_i,\ldots,X_n)$, rezultă că $2f(X_1,\ldots,X_i,\ldots,X_i,\ldots,X_n) = 0$ şi cum $\mathrm{char}(K) \neq 2$ obţinem că $f(X_1,\ldots,X_i,\ldots,X_i,\ldots,X_n) = 0$. Atunci $X_i - X_j | f$ pentru orice $i < j$, de unde $D_n | f$. Rezultă că există $g \in K[X_1,\ldots,X_n]$ cu $f = gD_n$. Este imediat că g este polinom simetric.
(iv) Fie $\tau \in S_n - A_n$. Definim

$$f_1(X_1,\ldots,X_n) = 2^{-1}(f(X_1,\ldots,X_n) + f(X_{\tau(1)},\ldots,X_{\tau(n)})).$$

Atunci pentru orice $\sigma \in S_n$ avem

$$f_1(X_{\sigma(1)},\ldots,X_{\sigma(n)}) = 2^{-1}(f(X_{\sigma(1)},\ldots,X_{\sigma(n)}) + f(X_{\tau\sigma(1)},\ldots,X_{\tau\sigma(n)})).$$

Dacă $\sigma \in A_n$, avem $\tau\sigma = (\tau\sigma\tau^{-1})\tau$ şi $\tau\sigma\tau^{-1} \in A_n$, de unde

$$f_1(X_{\sigma(1)},\ldots,X_{\sigma(n)}) = 2^{-1}(f(X_1,\ldots,X_n) + f(X_{\tau(1)},\ldots,X_{\tau(n)})).$$

Dacă $\sigma \in S_n - A_n$, atunci $\sigma = (\sigma\tau^{-1})\tau$, cu $\sigma\tau^{-1} \in A_n$, şi $\tau\sigma \in A_n$, de unde

$$f_1(X_{\sigma(1)},\ldots,X_{\sigma(n)}) = 2^{-1}(f(X_{\tau(1)},\ldots,X_{\tau(n)}) + f(X_1,\ldots,X_n)).$$

În ambele situaţii rezultă că $f_1(X_{\sigma(1)},\ldots,X_{\sigma(n)}) = f_1(X_1,\ldots,X_n)$, deci f_1 este polinom simetric. Acum se arată printr-un calcul similar că polinomul $f - f_1$ satisface proprietatea de la (iii), deci există un polinom simetric f_2 cu $f - f_1 = f_2 D_n$.

62. (i) Urmăm algoritmul din demonstraţia teoremei fundamentale a polinoamelor simetrice. Polinomul dat este simetric şi omogen de grad 6, şi scăzând din el polinoame simetrice omogene de grad 6 vom obţine tot polinoame simetrice omogene de grad 6 sau polinomul nul. Termenii principali care pot apărea sunt de forma $X_1^{k_1}X_2^{k_2}X_3^{k_3}$ cu $k_1 \geq k_2 \geq k_3$ şi $k_1 + k_2 + k_3 = 6$, deci (k_1, k_2, k_3) poate fi unul dintre $(4,2,0)$, $(4,1,1)$, $(3,3,0)$, $(3,2,1)$, $(2,2,2)$, deoarece gradul maxim al fiecărei nedeterminate în polinom este 4. Aşadar polinomul se scrie ca $s_1^2s_2^2 + as_1^3s_3 + bs_2^3 + cs_1s_2s_3 = ds_3^2$, şi dând valori particulare nedeterminatelor obţinem că $a = -4, b = -4, c = 18, d = -27$.
(ii) Se obţine $(X_1^2+X_2^2)(X_1^2+X_3^2)(X_2^2+X_3^2) = s_1^2s_2^2 - 2s_1^3s_3 - 2s_2^3 + 4s_1s_2s_3 - s_3^2$.
(iii) Notând cu f polinomul din enunţ avem că

$$\begin{aligned} f &= (s_1 - 2X_1)\cdots(s_n - 2X_n) \\ &= s_1^n - (2s_1)s_1^{n-1} + \cdots + (-1)^{n-1}(2^{n-1}s_{n-1})s_1 + (-1)^n(2^n s_n) \\ &= -s_1^n + (4s_2)s_1^{n-2} - \cdots + (-1)^{n-1}(2^{n-1}s_{n-1})s_1 + (-1)^n(2^n s_n) \end{aligned}$$

(iv) Avem $X_1^3 + \cdots + X_n^3 = s_1^3 + as_1s_2 + bs_3$ şi dând valori particulare nedeterminatelor găsim că $a = -3$, $b = 3$.

63. (i) Din relaţiile $X_i^n - s_1X_i^{n-1} + \cdots + (-1)^{n-1}s_{n-1}X_i + (-1)^n s_n = 0$, $1 \leq i \leq n$, obţinem că $X_i^k - s_1X_i^{k-1} + \cdots + (-1)^{n-1}s_{n-1}X_i^{k-n+1} + (-1)^n s_n X_i^{k-n} = 0$ pentru orice $k \geq n$. Sumând aceste relaţii obţinem relaţia dorită.
(ii) Arătăm mai întâi că dacă un polinom $f \in K[X_1, \ldots, X_n]$ este omogen de grad $q < n$ şi are proprietatea că atunci când dăm valoarea zero la oricare $n - q$ dintre nedeterminatele $X_1, \ldots, X_n$, polinomul (în celelalte q nedeterminate rămase) care rezultă se anulează, atunci $f = 0$. Într-adevăr, dacă f ar fi nenul, el s-ar scrie ca o sumă de termeni nenuli de forma $aX_{i_1}^{k_1} \cdots X_{i_s}^{k_s}$ cu $k_j \geq 1$ pentru orice $1 \leq j \leq s$ şi $k_1 + \ldots + k_s = q$. De aici rezultă în particular că $s \leq q$. Făcând X_i zero pentru orice $i \notin \{i_1, \ldots, i_s\}$, obţinem un polinom nenul, contradicţie.
Considerăm acum polinomul simetric $f(X_1, \ldots, X_n) = p_k - s_1p_{k-1} + \cdots + (-1)^{k-1}s_{k-1}p_1 + (-1)^k k s_k$ pentru $k < n$. Avem că f este polinom omogen de grad k. Dar $f(X_1, \ldots, X_k, 0, \ldots 0) = p'_k - s'_1p'_{k-1} + \cdots + (-1)^{k-1}s'_{k-1}p'_1 + (-1)^k k s'_k$, unde $s'_j = s_j(X_1, \ldots, X_k, 0, \ldots 0)$ şi $p'_j = p_j(X_1, \ldots, X_k, 0, \ldots 0)$. Cum $s'_1, \ldots, s'_k$ sunt polinoamele simetrice fundamentale în nedeterminatele $X_1, \ldots, X_k$, rezultă din punctul (i), aplicat pentru $n = k$, că avem $f(X_1, \ldots, X_k, 0, \ldots 0) = 0$. Cum f este polinom simetric, obţinem că polinomul care rezultă atunci când dăm valoarea zero la oricare $n - k$ dintre nedeterminatele $X_1, \ldots, X_n$ este nul. Aceasta arată că $f = 0$.

64. Avem că polinoamele $p_1, \ldots, p_n$ evaluate pentru $X_1 = x_1, \ldots, X_n = x_n$ sunt zero. Din formulele lui Newton rezultă că şi polinoamele $s_1, \ldots, s_n$ evaluate pentru $X_1 = x_1, \ldots, X_n = x_n$ sunt zero (de fapt, obţinem că ks_k este zero când este evaluat pentru $X_1 = x_1, \ldots, X_n = x_n$, şi cum K are caracteristică zero rezultă că $s_k = 0$ pentru aceste valori). Aceasta înseamnă că $x_1, \ldots, x_n$ sunt rădăcini ale polinomului $X^n = 0$, deci $x_1 = \ldots = x_n = 0$.

Concluzia nu mai este adevărată dacă $x_1^k + \cdots + x_n^k = 0$ pentru n valori ale lui k care nu sunt neapărat consecutive. De exemplu, luăm $n = 2$, $x_1 = 1$, $x_2 = -1$ şi atunci $x_1 + x_2 = 0$ şi $x_1^3 + x_2^3 = 0$.

Concluzia nu mai este adevărată pentru caracteristică diferită de zero. De exemplu, în $K = \mathbb{Z}_2$, dacă $x_1 = x_2 = \hat{1}$, avem $x_1 + x_2 = \hat{0}$ şi $x_1^2 + x_2^2 = \hat{0}$, dar $x_1, x_2 \neq \hat{0}$.

65. Folosim formulele lui Newton şi obţinem că, evaluat în x_1, x_2, x_3,

$p_{10} = 621$.

66. (i) Folosim formulele lui Newton şi obţinem că $x_1^i + \cdots + x_n^i = -(a^i + b^i)$ pentru i impar şi $x_1^i + \cdots + x_n^i = -(a^{i/2} + b^{i/2})$ pentru i par.
(ii) Înmulţim polinomul cu $(X - a)(X - b)$ şi folosim formulele lui Newton pentru rădăcinile acestuia. Obţinem că $x_1^i + \cdots + x_n^i = -(a^i + b^i)$.

Capitolul 12

Soluţii: Aritmetică în inele integre

1. Fracţiile pe care le vom scrie sunt elemente din corpul de fracţii al domeniului în care lucrăm.
(i) Notăm $R = \mathbb{Z}[i]$, $a = 1 + i$, $b = 2 + i$, $c = 1 - i$, $d = 1 + 2i$, $e = 1 - 2i$ şi $f = -2 + i$. Vom studia relaţiile între elementele a şi b.
Metoda I. $\frac{a}{b} = \frac{(1+i)(2-i)}{5} = \frac{3}{5} + \frac{1}{5}i \notin R$. Prin urmare, $b \nmid a$ şi $b \nsim a$.
$\frac{b}{a} = \frac{5}{3+i} = \frac{3}{2} - \frac{1}{2}i \notin R$, deci $a \nmid b$.
Metoda II. Avem (vezi problema 2) $N(a) = 2 \nmid_{\mathbb{Z}} 5 = N(b)$, deci conform problemei 3(i), $a \nmid b$ (şi, evident, $a \nsim b$). De asemenea, $N(b) \nmid_{\mathbb{Z}} N(a)$, deci $b \nmid a$.
Cu consideraţii similare obţinem $a \sim c$, $a \nmid d$, $b \nmid d$, $b \sim e$, $d \nmid a$, $d \nmid b$, $d \sim f$. Celelalte relaţii între elementele date se deduc imediat din cele deja menţionate.
(ii) Procedând ca la punctul (i) obţinem că nu există nicio pereche de elemente diferite a, b din mulţimea dată astfel încât $a|b$.
(iii) Notăm $R = \mathbb{Z}[\rho]$, $a = 5$, $b = 5\rho$, $c = 5\rho + 5$, $d = 5\rho - 5$, $e = 5 - 5\rho$, $f = 3 + 2\rho$, $g = 3 - 2\rho$. Să considerăm de exemplu elementele b şi c. Avem: $\frac{b}{c} = \frac{\rho}{\rho+1} = \frac{\rho(1+\overline{\rho})}{(1+\rho)(1+\overline{\rho})} = \rho(1 - 1 - \rho) = -\rho^2 = 1 + \rho$.
Metoda I. $\frac{b}{c} = 1+\rho \in R$, deci $c|b$; $\frac{c}{b} = \frac{1}{1+\rho} = \frac{1+\overline{\rho}}{(1+\rho)(1+\overline{\rho})} = 1-1-\rho = -\rho \in R$, deci $b|c$. Prin urmare avem $b \sim c$.
Metoda II. $\frac{b}{c} = 1 + \rho \in U(R)$ (vezi problema 5), deci $b \sim c$.
Metoda III. Ca la metoda I, $c|b$. Dar $N(c) = 25 = N(b)$, deci, conform problemei 3(iii), $c \sim b$.

Cu consideraţii de acelaşi tip obţinem $a \sim b \sim c | d \sim e$ şi $d \nmid c$. Procedând ca la metoda I de la acest punct sau ca la metoda II de la punctul (i) deducem că f nu divide niciun element din listă şi nici nu se divide cu vreunul (cu excepţia lui însuşi). O afirmaţie similară este valabilă şi pentru g.
(iv) Notăm $R = \mathbb{Z}[\sqrt{2}]$, $a = 1 + 2\sqrt{2}$, $b = 1 - 2\sqrt{2}$, $c = 3 + \sqrt{2}$, $d = 3 - \sqrt{2}$, $e = 2 + \sqrt{2}$. Folosind metodele deja ilustrate la punctele anterioare, obţinem $a \sim d$, $b \sim c$, şi nu există nicio altă pereche de elemente diferite α, β din listă cu $\alpha | \beta$.
(v) Notăm $R = \mathbb{Q}[[X]]$. Se ştie (vezi problema 26 din Capitolul 5) că elementele inversabile din R sunt seriile formale cu termen liber nenul.
Vom studia cazul elementelor $f = a_r X^r + a_{r+1} X^{r+1} + \ldots$ şi $g = b_s X^s + b_{s+1} X^{s+1} + \ldots$. Avem $f = X^r \overline{f}$, unde $\overline{f} = a_r + a_{r+1} X + \cdots \in U(R)$ şi $g = X^s \overline{g}$, unde $\overline{g} = b_s + b_{s+1} X + \cdots \in U(R)$. Dacă $r \leq s$, atunci $g = (X^{s-r} \overline{f}^{-1} \overline{g}) f$, deci $f | g$. Dacă $r > s$, $f = (X^{r-s} \overline{g}^{-1} \overline{f}) g$, deci $g | f$.
Prin urmare $f | g$ dacă şi numai dacă $r \leq s$, iar $f \sim g$ dacă şi numai dacă $r = s$. Toate relaţiile care trebuie studiate se deduc de aici.
(vi) Notăm $R = \mathbb{Q} + X\mathbb{R}[X]$, $a = 2 + X$, $b = \frac{3}{7} + \frac{3}{14} X$, $c = 2\pi X + \pi X^2$, $d = \frac{\pi}{5} X + \frac{\pi}{10} X^2$, $e = 3\pi^2 X + \frac{3\pi^2}{2} X^2$ şi $f = 2 + 3X + X^2$.
Avem $b = \frac{3}{14} a$ şi $a = \frac{14}{3} b$, deci $a \sim b$. $c = \pi X \cdot a$, deci $a | c$. Presupunând $c | a$, ar exista $g \in R$ cu $a = cg$, relaţie valabilă şi în $\mathbb{R}[X]$, unde este însă contradictorie din motive de grad. Rămâne deci că $c \nmid a$. $e = \frac{3\pi^2}{2} X \cdot a$, deci $a | e$; $e \nmid a$ din motive de grad. $f = (1 + X) \cdot a$, deci $a | f$. Din motive de grad, $f \nmid a$. Cum $b \sim a$, comportarea lui b din punctul de vedere al divizibilităţii coincide cu cea a lui a. $d = \frac{1}{10} c$ şi $c = 10 \cdot d$, deci c este asociat cu d. Dacă $c | e$, atunci există $g \in R$ cu $e = gc$. Rezultă că termenul liber al lui g este $\frac{3\pi}{2} \notin \mathbb{Q}$, contradiţie. Rămâne deci că $c \nmid e$. Analog se arată că $e \nmid c$. Dacă presupunem $c | f$, atunci există $g \in R$ cu $f = gc$. Privind relaţia în $\mathbb{R}[X]$, constatăm că grad $g = 0$, deci $g \in \mathbb{R} \cap R = \mathbb{Q}$. Pe de altă parte, comparând coeficienţii dominanţi din relaţia $f = gc$, obţinem $g = \frac{1}{\pi}$, contradicţie. Rămâne deci că $c \nmid f$. Analog se arată relaţiile $f \nmid c$, $e \nmid f$ şi $f \nmid e$. Cum $d \sim c$, comportarea lui d din punctul de vedere al divizibilităţii coincide cu cea a lui c.

2. (i) Evident.
(ii) Fie $z_1, z_2 \in \mathbb{Q}[\sqrt{d}]$, $z_1 = a_1 + b_1\sqrt{d}$, $z_2 = a_2 + b_2\sqrt{d}$. Avem

$$\begin{aligned} N(z_1z_2) &= N(a_1a_2+db_1b_2+(a_1b_2+a_2b_1)\sqrt{d}) \\ &= |(a_1a_2+db_1b_2)^2-d(a_1b_2+a_2b_1)^2| \\ &= |a_1^2a_2^2+d^2b_1^2b_2^2-da_1^2b_2^2-da_2^2b_1^2| \\ &= |(a_1^2-db_1^2)(a_2^2-db_2^2)| \\ &= N(z_1)N(z_2). \end{aligned}$$

Mai simplu, $N(z_1z_2)=|z_1z_2\overline{z_1z_2}|=|z_1z_2\overline{z_1}\ \overline{z_2}|=|z_1\overline{z_1}||z_2\overline{z_2}|=N(z_1)N(z_2)$.
(iii) Evident.
(iv) Dacă $z\in U(\mathbb{Z}[\sqrt{d}])$, atunci există $z'\in\mathbb{Z}[\sqrt{d}]$ cu $zz'=1$. Rezultă $N(z)N(z')=1$, deci $N(z)=1$. Reciproc, dacă z are norma 1, atunci $1=N(z)=|z\overline{z}|$, deci unul dintre elementele $\overline{z}$, $-\overline{z}$ este inversul lui z în $\mathbb{Z}[\sqrt{d}]$.
(v) Fie $z\in\mathbb{Z}[\sqrt{d}]$ cu norma p, p prim număr prim, şi $z_1,z_2\in\mathbb{Z}[\sqrt{d}]$ cu $z=z_1z_2$. Atunci $p=N(z)=N(z_1)N(z_2)$, deci $N(z_1)=1$ sau $N(z_2)=1$. Aplicând (iv) rezultă că z_1 este inversabil sau z_2 este inversabil. Aşadar z este ireductibil.
Pentru exemplul cerut, să considerăm elementul $3\in\mathbb{Z}[i]$. El are norma 9. Dacă s-ar descompune în produs de doi factori neinversabili, fiecare dintre aceştia ar trebui să aibă norma 3. Este însă imediat că în $\mathbb{Z}[i]$ nu există elemente de normă 3.
(vi) Dacă d este de forma $4k+1$, atunci pentru orice $z=a+b\frac{1+\sqrt{d}}{2}\in\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ avem $N(z)=|z\overline{z}|=\left|\left(a+b\frac{1+\sqrt{d}}{2}\right)\left(a+b\frac{1-\sqrt{d}}{2}\right)\right|=\left|a^2+ab+\frac{1-d}{4}b^2\right|\in\mathbb{N}$.
Demonstraţiile date la punctele (iv) şi (v) rămân valabile şi în $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.
(vii) Fie $z\in\mathbb{Z}[i\sqrt{3}]$, $z=a+bi\sqrt{3}$, cu $N(z)=112$. Avem $a^2+3b^2=112$. Pot apărea cazurile:
$b=0$, care duce la $a^2=112$, imposibil, pentru că $a\in\mathbb{Z}$;
$b=\pm1$, care duce la $a^2=109$, imposibil, pentru că $a\in\mathbb{Z}$;
$b=\pm2$, care duce la $a^2=100$, de unde $z=\pm10\pm2\sqrt{3}$;
$b=\pm3$, care duce la $a^2=85$, imposibil, pentru că $a\in\mathbb{Z}$;
$b=\pm4$, care duce la $a^2=64$, de unde $z=\pm8\pm4\sqrt{3}$;
$b=\pm5$, care duce la $a^2=37$, imposibil, pentru că $a\in\mathbb{Z}$;
$b=\pm6$, care duce la $a^2=4$, de unde $z=\pm2\pm6\sqrt{3}$, şi
$|b|>6$, care duce la $a^2<0$, imposibil.
Prin urmare, elementele de ordin 112 din $\mathbb{Z}[i\sqrt{3}]$ sunt $\pm10\pm2\sqrt{3}$, $\pm8\pm4\sqrt{3}$ şi $\pm2\pm6\sqrt{3}$.

Fie $z \in \mathbb{Z}[i\sqrt{5}]$, $z = a + bi\sqrt{5}$, cu $N(z) = 112$. Avem $a^2 + 5b^2 = 112$. Rezultă de aici că $a^2 \equiv 2 \pmod 5$, lucru imposibil. Prin urmare, în $\mathbb{Z}[\sqrt{5}]$ nu există elemente de normă 112.

Fie $z \in \mathbb{Z}[i\sqrt{11}]$, $z = a + bi\sqrt{11}$, cu $N(z) = 112$. Avem $a^2 + 11b^2 = 112$. Pot apărea cazurile:
$b = 0$, care duce la $a^2 = 112$, imposibil, pentru că $a \in \mathbb{Z}$;
$b = \pm 1$, care duce la $a^2 = 101$, imposibil, pentru că $a \in \mathbb{Z}$;
$b = \pm 2$, care duce la $a^2 = 68$, imposibil, pentru că $a \in \mathbb{Z}$;
$b = \pm 3$, care duce la $a^2 = 13$, imposibil, pentru că $a \in \mathbb{Z}$ şi
$|b| > 4$, care duce la $a^2 < 0$, imposibil.
Prin urmare, în $\mathbb{Z}[i\sqrt{11}]$ nu există elemente de normă 112.

Fie $z = a + b\frac{1+i\sqrt{7}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{7}}{2}\right]$ cu $N(z) = 112$. Rezultă că $\left(a + \frac{b}{2}\right)^2 + \frac{7b^2}{4} = 112$, adică $(2a+b)^2 + 7b^2 = 448$. Rezultă că există $k \in \mathbb{Z}$ astfel ca $2a + b = 7k$. Relaţia anterioară devine $7k^2 + b^2 = 64$. Pot apărea cazurile:
$k = 0$, care duce la $b = \pm 8$;
$k = \pm 1$, care duce la $a^2 = 57$, imposibil, pentru că $b \in \mathbb{Z}$;
$k = \pm 2$, care duce la $b^2 = 36$ şi $2a + b = \pm 14$;
$k = \pm 3$, care duce la $b^2 = 1$ şi $2a + b = \pm 21$.
Înlocuind, deducem că elementele de normă 112 din inelul $\mathbb{Z}\left[\frac{1+\sqrt{7}}{2}\right]$ sunt $\pm 4i\sqrt{7}, \pm 7 \pm 3i\sqrt{7}$ şi $\frac{\pm 21 \pm i\sqrt{7}}{2}$.

3. (i) Fie $a, b \in \mathbb{Z}[\sqrt{d}]$ astfel încât $a|b$. Rezultă că există $c \in \mathbb{Z}[\sqrt{d}]$ astfel încât $b = ac$. Trecând la norme (vezi problema 2(ii)) obţinem $N(b) = N(a)N(c)$, deci $N(a)|N(b)$.
(ii) Notăm $R = \mathbb{Z}[i\sqrt{2}]$ şi considerăm elementele $a = 3$ şi $b = 1 + 2i\sqrt{2}$ din R. Avem $N(a) = 9|9 = N(b)$, dar $\frac{b}{a} = \frac{1}{3} + \frac{2}{3}i\sqrt{2} \notin R$, deci $a \nmid b$ în R.
(iii) Fie $a, b \in R$ cu $a|_R b$ şi $N(a) = N(b)$; există $c \in R$ astfel încât $b = ac$. Trecând la norme obţinem $N(b) = N(a)N(c)$. Cum $N(a) = N(b)$, rezultă că $N(c) = 1$, deci $c \in U(R)$. Prin urmare, $a \sim_R b$.
(iv) Evident, $1|a$ şi $1|b$. Fie acum $f \in \mathbb{Z}[\sqrt{d}]$ cu proprietatea că $f|a$ şi $f|b$. Trecând la norme, obţinem (conform (i)) $N(f)|N(a)$ şi $N(f)|N(b)$, deci $N(f)|(N(a), N(b)) = 1$. Prin urmare, $N(f) = 1$, de unde, conform problemei 2(iv), f este element inversabil, adică $f|1$. În concluzie, 1 este c.m.m.d.c pentru a şi b în $\mathbb{Z}[\sqrt{d}]$.
(v) Nu neapărat. Să considerăm, de exemplu, elementele $a = 2$ şi $b = 1 + i\sqrt{5}$ din inelul $R = \mathbb{Z}[i\sqrt{5}]$. Dacă $d \in R$ divide a şi b, atunci, conform (i),

$N(d)|N(a)$ şi $N(d)|N(b)$, deci $N(d)|(N(a), N(b)) = (4, 6) = 2$ în $\mathbb{Z}$. Prin urmare, $N(d) \in \{1, 2\}$. Cum însă R nu are elemente de normă 2, rezultă că $N(d) = 1$, deci $d|_R 1$. Cum $1|_R a$ şi $1|_R b$, rezultă că 1 e un c.m.m.d.c. pentru a şi b în R. Avem însă $N(1) = 1 \neq 2 = (N(a), N(b))$.
(vi) Demonstraţiile de la punctele (i),(iii) şi (iv) rămân valabile şi dacă înlocuim inelul $\mathbb{Z}[\sqrt{d}]$ cu $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

4. (i) Conform problemei 2(iv), un element $z \in \mathbb{Z}[\sqrt{d}]$, $z = a + b\sqrt{d}$, este inversabil dacă şi numai dacă $N(z) = 1$, condiţie care se rescrie $a^2 - db^2 = 1$. Procedând ca la problema 2(vii), constatăm că pentru $d = -1$ se obţin valorile $a = \pm 1, b = 0$ şi $a = 0, b = \pm 1$, în timp ce pentru $d < -1$ relaţia de mai sus e posibilă numai pentru $a = \pm 1, b = 0$. În concluzie, pentru $d \in \mathbb{Z}$, $d < 0$ şi d liber de pătrate

$$U(\mathbb{Z}[\sqrt{d}]) = \begin{cases} \{1, -1, i, -i\} & \text{dacă} \quad d = -1 \\ \{1, -1\} & \text{dacă} \quad d < -1 \end{cases} .$$

(ii) Să notăm $R = \mathbb{Z}[\sqrt{2}]$, $G = U(R)$, $u = 1 + \sqrt{2} \in G$ şi $\mathcal{N} = \{a + b\sqrt{2} \mid a, b \in \mathbb{N}\} \cap G$. Fie $x = a + b\sqrt{2} \in \mathcal{N}$. Atunci există $n \in \mathbb{N}$ astfel încât $x \in [u^n, u^{n+1})$. Datorită multiplicativităţii normei pe $\mathbb{Q}[\sqrt{2}]$ (vezi problema 2(ii)) avem $N(xu^{-n}) = 1$. Prin urmare, $xu^{-n} \in G \subset R$; să punem $xu^{-n} = r + s\sqrt{2}, r, s \in \mathbb{Z}$. Dacă $rs > 0$, cum $xu^{-n} > 0$, obţinem $r > 0$ şi $s > 0$. Deci $r \geq 1$ şi $s \geq 1$. Rezultă $x = (r + s\sqrt{2})u^n \geq u^{n+1}$, contradicţie. Dacă $rs = 0$, atunci $xu^{-n} \in \mathcal{N}$ implică $r = 1$ şi $s = 0$, prin urmare $x = u^n$. Dacă $rs < 0$, atunci

$$\frac{x}{u^n} = \frac{r^2 - 2s^2}{r - s\sqrt{2}} ,$$

deci $x(r - s\sqrt{2}) = \pm u^n$. Rezultă $x(|r| + |s|\sqrt{2}) = u^n$. Cum $|r| + |s|\sqrt{2} \geq u$, obţinem $x \leq u^{n-1}$, din nou contradicţie.
În concluzie, $\mathcal{N} = \{u^n \mid n \in \mathbb{N}\}$.
Să constatăm în continuare că dacă $x = a + b\sqrt{2} \in G$ şi $x > 0$, avem posibilităţile:
1) $a, b \in \mathbb{N}$, caz în care $x \in \mathcal{N}$.
2) $ab < 0$, situaţie în care

$$x = a + b\sqrt{2} = \frac{a^2 - 2b^2}{a - b\sqrt{2}} = \frac{1}{|a| + |b|\sqrt{2}} .$$

Cum $|a| + |b|\sqrt{2} \in \mathcal{N}$, rezultă că există $n \in \mathbb{N}^*$ astfel încât $x = u^{-n}$. Prin urmare, $G_+ = \{x \in G \mid x > 0\} \subset \{u^n \mid n \in \mathbb{Z}\}$. Incluziunea contrară fiind evidentă, obţinem $G_+ = \{u^n \mid n \in \mathbb{Z}\}$. Cum $x \in G_- = \{x \in G \mid x < 0\} \Leftrightarrow -x \in G_+$, se obţine $G = \{\pm u^n \mid n \in \mathbb{Z}\}$.

Acum este clar că funcţia $f : \mathbb{Z}_2 \times \mathbb{Z} \to G, f(\widehat{a}, n) = (-1)^a u^n$ este corect definită şi izomorfism de grupuri.

5. Să notăm $\varepsilon = \frac{1+i\sqrt{3}}{2}$ şi $R = \mathbb{Z}[\varepsilon]$. Deoarece $\varepsilon^2 - \varepsilon + 1 = 0$, avem $R = \{a + b\varepsilon \mid a, b \in \mathbb{Z}\}$. Pentru $z \in \mathbb{Z}[\varepsilon]$, $z = a + b\varepsilon$, definim $N(z) = z\overline{z} = \left(a + \frac{1}{2}b\right)^2 + \frac{3b^2}{4} = a^2 + ab + b^2 \in \mathbb{N}$. Procedând ca la soluţia problemei 2, se arată că N este multiplicativă şi că $z \in R$ este inversabil dacă şi numai dacă $N(z) = 1$, condiţie care se rescrie $\left(a + \frac{1}{2}b\right)^2 + \frac{3b^2}{4} = 1$. Pot apărea cazurile:
$b = 0$, caz în care obţinem $a = \pm 1$;
$b = 1$, caz în care $\left(a + \frac{1}{2}\right)^2 = \frac{1}{4}$, deci $a \in \{-1, 0\}$;
$b = -1$, caz în care $\left(a - \frac{1}{2}\right)^2 = \frac{1}{4}$, deci $a \in \{0, 1\}$.
Prin urmare, $U(\mathbb{Z}[\varepsilon]) = \{1, -1, \varepsilon, -1 + \varepsilon, -\varepsilon, 1 - \varepsilon\}$. Constatăm că $\varepsilon^2 = -1 + \varepsilon \neq 1$, $\varepsilon^3 = -1 \neq 1$, $\varepsilon^4 = -\varepsilon \neq 1$, $\varepsilon^5 = 1 - \varepsilon \neq 1$ şi $\varepsilon^6 = 1$. Prin urmare, ordinul lui ε în $U(\mathbb{Z}[\varepsilon])$ este 6. În consecinţă, $U(\mathbb{Z}[\varepsilon]) = < \varepsilon >$. Aşadar $U(\mathbb{Z}[\varepsilon])$ este grup ciclic cu 6 elemente, deci izomorf cu $\mathbb{Z}_6$.

6. Din problema 11(ii) din Capitolul 4 rezultă că R_k este domeniu de integritate $\Leftrightarrow (X^2 - k)$ este ideal prim în $\mathbb{Z}[X] \Leftrightarrow X^2 - k$ este element prim în $\mathbb{Z}[X] \Leftrightarrow X^2 - k$ este element ireductibil în $\mathbb{Z}[X] \Leftrightarrow X^2 - k$ nu are rădăcini în $\mathbb{Z} \Leftrightarrow k$ nu este pătrat perfect.

7. Să considerăm $R = \mathbb{Z} + X\mathbb{R}[X]$. Notăm $a = X^2$ şi $b = \sqrt{2}X^2$, $a, b \in R$. Fie d un divizor comun pentru a şi b. Atunci, $\text{grad}(d) \leq 2$. Scriind $a = d\alpha$, $\alpha \in R$, obţinem, după identificarea coeficienţilor, că d e fie număr întreg, fie de forma AX, $A \in \mathbb{R}$, fie de forma $\frac{1}{n}X^2$, $n \in \mathbb{Z}^*$. Observăm că elementele de ultimul tip dintre cele de mai înainte nu divid pe $b = \sqrt{2}X^2$, dar celelalte îl divid. Elementele din $\mathbb{Z} \subset R$ nu se divid însă prin divizorul comun X al elementelor a şi b. Prin urmare, un eventual c.m.m.d.c. în R al elementelor a şi b trebuie să fie de forma AX, $A \in \mathbb{R}$ şi să se dividă în R cu X şi cu $\sqrt{2}X$. Însă R nu conţine astfel de elemente. Rămâne deci că a şi b nu admit c.m.m.d.c. în R, prin urmare R nu are proprietatea c.m.m.d.c.

Să observăm acum că dacă $f \in R$ este ireductibil, atunci f fie este număr prim din $\mathbb{Z} \subset R$, fie este ireductibil în $\mathbb{R}[X]$ şi are în plus proprietatea

$f(0) \in \{-1, 1\}$. (În cazul unui element $f \in R$ de grad mai mare decât zero, dacă $f(0) = 0$, atunci $f = 2 \cdot (\frac{1}{2}f)$ este o descompunere relevantă a lui f, iar dacă un număr prim $p \in \mathbb{Z}$ ar divide pe $f(0) \neq 0$, atunci $f = p \cdot (\frac{1}{p}f)$ este o descompunere relevantă a lui f; în oricare dintre aceste situaţii f este reductibil. Dacă $f \in R$, nenul şi neinversabil, are gradul 0 şi nu e număr prim, atunci pentru orice număr prim $p \in \mathbb{Z}$ care divide pe f obţinem descompunerea relevantă $f = p \cdot \frac{f}{p}$, deci f este reductibil în R.)
Fie acum $f \in R$ ireductibil şi $g, h \in R$ astfel ca $f|_R gh$. Considerăm cele două cazuri:
1. f este număr prim din $\mathbb{Z} \subset R$. Avem $f|_{\mathbb{Z}} g(0)h(0)$, deci $f|_{\mathbb{Z}} g(0)$ sau $f|_{\mathbb{Z}} h(0)$, de unde $f|_R g$ sau $f|_R h$, respectiv.
2. f este ireductibil în $\mathbb{R}[X]$ şi $f(0) \in \{-1, 1\}$. Cum $f|_R gh$, rezultă $f|_{\mathbb{R}[X]} gh$, deci (f fiind prim în inelul euclidian $\mathbb{R}[X]$) $f|_{\mathbb{R}[X]} g$ sau $f|_{\mathbb{R}[X]} h$. Dacă, de exemplu, $f|_{\mathbb{R}[X]} g$, atunci există $F \in \mathbb{R}[X]$ astfel încât $g = fF$. Rezultă că $g(0) = f(0)F(0)$, deci $F(0) = \pm g(0) \in \mathbb{Z}$. Prin urmare, $F \in R$, deci $f|_R g$. Cazul $f|_{\mathbb{R}[X]} h$ se tratează analog. În concluzie, f este prim în R şi demonstraţia e încheiată.

8. Notăm $R = \mathbb{Z}[i\sqrt{n}]$, $n \geq 3$ impar. În R avem relaţia $2 \cdot \frac{n+1}{2} = n + 1 = (1 + i\sqrt{n})(1 - i\sqrt{n})$. Aceasta ne arată că $2|_R(1 + i\sqrt{n})(1 - i\sqrt{n})$. În mod evident însă 2 nu divide în R niciunul dintre cei doi factori. Prin urmare, 2 nu este prim în R. Pe de altă parte, $N(2) = 4$. Presupunând 2 reductibil în R, ar rezulta că el este produs de două elemente de normă 2. Dar (procedând ca la soluţia problemei 2(vii)) în R nu există elemente de normă 2, contradicţie. Rămâne deci că 2 e ireductibil în R. Cum în inelele cu proprietatea c.m.m.d.c. orice element ireductibil e prim, rezultă că R nu este un inel cu proprietatea c.m.m.d.c..

9. (i) Notăm $R = \mathbb{Z}[i\sqrt{5}]$. Să presupunem că $a = 2(1 + i\sqrt{5})$ şi $b = 6$ au un c.m.m.d.c. în R, fie el d. Atunci, $d|_R a$ şi $d|_R b$, deci $N(d)|_{\mathbb{Z}} N(a) = 24$ şi $N(d)|_{\mathbb{Z}} N(b) = 36$. Prin urmare, $N(d)|_{\mathbb{Z}} 12$. Pe de altă parte, 2 şi $1 + i\sqrt{5}$ divid a şi b în R, deci ele divid d. Rezultă că $4 = N(2)|_{\mathbb{Z}} N(d)$ şi $6 = N(1 + i\sqrt{5})|_{\mathbb{Z}} N(d)$, deci $12|_{\mathbb{Z}} N(d)$. Prin urmare, $N(d) = 12$. Procedând ca în soluţia problemei 2(vii), obţinem că în R nu există elemente de normă 12, contradicţie. Rămâne că $2(1 + i\sqrt{5})$ şi 6 nu au un c.m.m.d.c. în R.

În ceea ce priveşte elementele $1 + i\sqrt{5}$ şi 3, norma oricărui divizor comun al lor trebuie să dividă $3 = (N(1 + i\sqrt{5}), N(3)) = (6, 9)_{\mathbb{Z}}$. Cum în R nu

există elemente de normă 3, rezultă că orice divizor comun al elementelor considerate are norma 1, deci, conform problemei 2(iv), este inversabil, adică divide 1. Cum în mod evident 1 divide $1+i\sqrt{5}$ şi 3, rezultă că acestea au ca c.m.m.d.c. pe 1.
(ii) Dacă în R avem $6 = xy$, atunci $N(6) = N(x)N(y)$. Putem considera, fără a restrânge generalitatea, că $N(x) \leq N(y)$. Trebuie cercetate situaţiile:
$N(x) = 1, N(y) = 36$. Atunci $x \in U(R)$, deci în acest caz nu avem de-a face cu o descompunere relevantă.
$N(x) = 2$, $N(y) = 18$. Imposibil, căci R nu are elemente de normă 2 (se arată ca în soluţia problemei 2(vii)).
$N(x) = 3$, $N(y) = 12$. Imposibil, căci R nu are elemente de normă 3.
$N(x) = 4$, $N(y) = 9$. Obţinem $x \sim_R 2$ şi $y \sim_R 3$ (vezi problema 2(vii)).
$N(x) = 6$, $N(y) = 6$. Obţinem $x \sim_R 1 + i\sqrt{5}$ şi $y \sim_R 1 - i\sqrt{5}$ sau invers.

Să constatăm că $2 \cdot 3 = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$. Această relaţie arată că $2|_R(1 + i\sqrt{5})(1 - i\sqrt{5})$. Este clar însă că 2 nu divide niciunul din factorii acestui produs, deci 2 nu e prim în R. În mod similar se arată că niciunul dintre elementele 3, $1 + i\sqrt{5}$ şi $1 - i\sqrt{5}$ nu este prim în R. Pe de altă parte, aceste elemente sunt ireductibile în R. Vom arăta acest lucru pentru 2, pentru celelalte elemente procedându-se similar. Presupunem că 2 e reductibil în R. Rezultă că există $x, y \in R \setminus U(R)$ cu $2 = xy$. Rezultă că $4 = N(2) = N(x)N(y)$, deci $N(x) = N(y) = 2$. Dar în R nu există elemente de normă 2, contradicţie.
În concluzie, 6 se descompune în factori ireductibili în R ca $2 \cdot 3$ şi $(1 + i\sqrt{5})(1 - i\sqrt{5})$, dar nu admite nici o descompunere în factori primi în R.

10. Notăm $R = \mathbb{Z}[i\sqrt{3}]$. Presupunem că 2 e reductibil în R. Rezultă că există $x, y \in R \setminus U(R)$ cu $2 = xy$. Deducem că $4 = N(2) = N(x)N(y)$, deci $N(x) = N(y) = 2$. Dar în R nu există elemente de normă 2, contradicţie. Analog se arată că $1 + i\sqrt{3}$ e ireductibil în R.
Cum $N(2) = 4 = N(1+i\sqrt{3})$, norma oricărui divizor comun d al elementelor 2 şi $1 + i\sqrt{3}$ trebuie să dividă 4. Dacă această normă ar fi 4, ar rezulta (conform problemei 3(iii)) că $d \sim_R 2$ şi $d \sim_R 1 + i\sqrt{3}$, deci $2 \sim_R 1 + i\sqrt{3}$, contradicţie (vezi problema 1). Cum în R nu există elemente de normă 2, rezultă că orice divizor comun al elementelor considerate are norma 1, deci, conform problemei 2(iv), este inversabil, adică divide pe 1. Cum 1 divide $1 + i\sqrt{3}$ şi 2, rezultă că 2 şi $1 + i\sqrt{3}$ au c.m.m.d.c. în R pe 1.
Elementul 2 nu e prim în R deoarece divide $4 = (1 + i\sqrt{3})(1 - i\sqrt{3})$, dar nu divide niciunul din factori. Analog se arată că $1 + i\sqrt{3}$ nu e prim în R.

Să presupunem că $a = 2(1 + i\sqrt{3})$ şi $b = 4$ au un c.m.m.d.c. în R, fie el d. Atunci, $d|_R a$ şi $d|_R b$, deci $N(d)|_{\mathbb{Z}} N(a)$ şi $N(d)|_{\mathbb{Z}} N(b)$. Cum $N(a) = N(b) = 16$, rezultă că $N(d)|_{\mathbb{Z}} 16$. Pe de altă parte, 2 divide a şi b în R, deci el divide d. Rezultă că $4 = N(2)|_{\mathbb{Z}} N(d)$. Dar cum în R nu există elemente de normă 8 (se procedează la fel ca la soluţia problemei 2(vii)), rezultă că $N(d) \in \{4, 16\}$. Dacă $N(d) = 4$, obţinem $d = \pm 2$ sau $d = \pm 2 \pm i\sqrt{3}$.
Dacă $N(d) = 16$, procedând ca la problema 2(vii), obţinem $d = \pm 4$ sau $d = \pm 2 \pm 2i\sqrt{3}$.
Se observă (ca la soluţia problemei 1) că $\pm 4 \nmid_R a$, iar $\pm 2 \pm 2i\sqrt{3} \nmid_R b$.
Pe de altă parte, $1 + i\sqrt{3}|_R a$ şi $1 + i\sqrt{3}|_R b$, dar $1 + i\sqrt{3} \nmid_R \pm 2$; $2|_R a$ şi $2|_R b$, dar $2 \nmid_R \pm 1 \pm i\sqrt{3}$. Prin urmare, niciunul dintre elementele din lista de mai sus nu este c.m.m.d.c. pentru a şi b. Rămâne că $2(1 + i\sqrt{3})$ şi 4 nu au un c.m.m.d.c. în R.

11. Notăm $R = \mathbb{Z}[i\sqrt{5}]$.
(i) Fie d un divizor comun în R pentru $a = 4 + i\sqrt{5}$ şi $b = 1 + 3i\sqrt{5}$. Atunci, $N(d)|N(a) = 21$ şi $N(d)|N(b) = 46$. Prin urmare, $N(d)|(21, 46)_{\mathbb{Z}} = 1$, deci $N(d) = 1$. Rezultă că $d \in U(R)$, deci $d|_R 1$. Cum 1 divide în R pe a şi pe b, rezultă că $1 = (a, b)_R$.
(ii) Fie d un divizor comun în R pentru $a = 6 + 2i\sqrt{5}$ şi $b = 14$. Atunci, $N(d)|N(a) = 56$ şi $N(d)|N(b) = 196$. Prin urmare, $N(d)|(56, 196)_{\mathbb{Z}} = 28$. Presupunem că d este chiar un c.m.m.d.c. pentru a şi b în R. Cum $2|_R a$ şi $2|_R b$, rezultă $2|_R d$, de unde $4 = N(2)|_{\mathbb{Z}} N(d)$. Avem şi $3+i\sqrt{5}|_R a$ şi $3+i\sqrt{5}|_R b$, deci $3 + i\sqrt{5}|_R d$, de unde $14 = N(3 + i\sqrt{5})|_{\mathbb{Z}} N(d)$. Prin urmare, $N(d)$ se va divide prin $[4, 14]_{\mathbb{Z}} = 28$. Deci $N(d) = 28$. Notând $d = u+vi\sqrt{5}$, cu $u, v \in \mathbb{Z}$, obţinem $u^2 + 5v^2 = 28$, de unde $u^2 \equiv 3 \pmod 5$, contradicţie. Aşadar a şi b nu au un c.m.m.d.c. în R.
(iii) Fie d un divizor comun în R pentru $a = 4+i\sqrt{5}$ şi $b = 1+2i\sqrt{5}$. Atunci $N(d)|_{\mathbb{Z}} N(a) = N(b) = 21$. Vom avea deci $N(d) \in \{1, 3, 7, 21\}$. Procedând ca la soluţia problemei 2(vii) se constată că în R nu există elemente de normă 3 sau 7. Dacă $N(d) = 21$, atunci se obţine (vezi problema 2(vii)) $d \sim_R a$ sau $d \sim_R \overline{a}$ sau $d \sim_R b$ sau $d \sim_R \overline{b}$. Dar $a \nmid_R b$, $\overline{a} \nmid_R a$, $b \nmid_R a$ şi $\overline{b} \nmid_R b$. Rămâne prin urmare că $N(d) = 1$. Rezultă că $d \in U(R)$, deci $d|_R 1$. Cum 1 divide în R pe a şi pe b, rezultă că $1 = (a, b)_R$.
(iv) Fie d un divizor comun în R pentru $a = 6 + 3i\sqrt{5}$ şi $b = 9$. Cum $N(a) = N(b) = 81$, rezultă $N(d)|81$. Presupunem acum că $d = (a, b)_R$; constatăm că $3|_R a$ şi $3|_R b$, de unde $3|_R d$, deci $9 = N(3)|_{\mathbb{Z}} N(d)$. Prin urmare, $N(d) \in \{9, 27, 81\}$. Cum în R nu există elemente de normă 27, mai rămân

de analizat situaţiile $N(d) = 9$ şi $N(d) = 81$.
Dacă $N(d) = 9$, atunci $d \sim 3$ sau $d \sim 2 \pm i\sqrt{5}$. Dar (ca la soluţia problemei 1) $2 - i\sqrt{5} \nmid_R a$. Rămâne deci că (până la o asociere în divizibilitate) $d = 3$ sau $d = 2 + i\sqrt{5}$. Însă $2 + i\sqrt{5}$ şi 3 sunt divizori comuni în R pentru a şi b şi în plus $3 \nmid_R 2 + i\sqrt{5}$, iar $2 + i\sqrt{5} \nmid_R 3$. Prin urmare, niciunul dintre elementele de normă 9 din R nu poate fi c.m.m.d.c. pentru a şi b.
Dacă $N(d) = 81$, atunci $d \sim 9$, $d \sim 6 \pm 3i\sqrt{5}$, sau $d \sim 1 \pm 4i\sqrt{5}$. Dar $9 \nmid_R a$, $6 \pm 3i\sqrt{5} \nmid_R b$, iar $1 \pm 4i\sqrt{5} \nmid_R b$. Prin urmare, a şi b nu admit un c.m.m.d.c. în R.
(v) Fie d un divizor comun în R pentru $a = 2 + 8i\sqrt{5}$ şi $b = 18$. Atunci, $N(d)|N(a) = N(b) = 324$. Presupunem că d este chiar un c.m.m.d.c. pentru a şi b în R. Cum $2|_R a$ şi $2|_R b$, rezultă $2|_R d$, de unde $4 = N(2)|_{\mathbb{Z}} N(d)$. Prin urmare, $N(d) \in \{4, 12, 36, 108, 324\}$. În R nu există însă elemente de normă 12 sau 108.
Dacă $N(d) = 4$, atunci $d \sim_R 2$.
Dacă $N(d) = 36$, atunci $d \sim_R 6$ sau $d \sim_R 4 \pm 2i\sqrt{5}$. Dar $6 \nmid_R a$, iar $4 + 2i\sqrt{5} \nmid_R a$. Pe de altă parte, $4 - 2i\sqrt{5}$ este divizor comun pentru a şi b (şi se divide şi prin divizorul comun 2 de la cazul precedent).
Dacă $N(d) = 324$, atunci, din $d|_R a$ şi $N(d) = N(a)$ rezultă (vezi problema 3(iii)) $d \sim_R a$; analog obţinem $d \sim_R b$, deci $a \sim_R b$, contradicţie.
Prin urmare, singurul (până la o asociere în divizibilitate) element care poate fi c.m.m.d.c. în R pentru a şi b este $4 - 2i\sqrt{5}$.
Rămâne să verificăm dacă $4 - 2i\sqrt{5}$ se divide într-adevăr prin toţi divizorii comuni ai elementelor a şi b. Fie c un astfel de divizor. S-a arătat mai sus că $N(c)|_{\mathbb{Z}} 324$. Ţinând cont de consideraţiile anterioare, mai avem de studiat cazurile $N(c) \in \{1, 2, 3, 6, 9, 18, 27, 54, 81, 162\}$.
Să observăm că în R nu există elemente de normă $2, 3, 18, 27$ sau 162.
Dacă $N(c) = 1$, atunci c este inversabil, deci divide pe $4 - 2i\sqrt{5}$.
Dacă $N(c) = 6$, atunci $c \sim_R 1 + i\sqrt{5}|_R 4 - 2i\sqrt{5}$ sau $c \sim_R 1 - i\sqrt{5} \nmid_R a$.
Dacă $N(c) = 9$, atunci $c \sim_R 3$ sau $c \sim_R 2 \pm i\sqrt{5}$. Dar 3 şi $2 + i\sqrt{5}$ nu divid în R pe a, iar $2 - i\sqrt{5}$, care este divizor comun pentru a şi b, divide în mod clar pe $4 - 2i\sqrt{5}$.
Dacă $N(c) = 54$, atunci $c \sim_R 7 \pm i\sqrt{5} \nmid_R b$ sau $c \sim_R 3(1 \pm i\sqrt{5}) \nmid_R a$.
În sfârşit, dacă $N(c) = 81$, atunci fie $c \sim_R 9 \nmid_R a$, fie $c \sim_R 6 \pm 3i\sqrt{5} \nmid_R a$, fie $c \sim_R 1 \pm 4i\sqrt{5} \nmid_R b$.
În concluzie, $4 - 2i\sqrt{5}$ este c.m.m.d.c. în R pentru a şi b.

12. (i) Cum $\{X^2, X^3\} \subset R$, avem $\mathbb{Z}[X^2, X^3] \subset R$. Pentru incluziunea

inversă, fie $f = a_0 + \sum_{k=2}^{n} a_k X^k \in R$. Detaliem scrierea lui f astfel:

$$f = \sum_{k=0}^{\left[\frac{n}{3}\right]} a_{3k} X^{3k} + \sum_{k=1}^{\left[\frac{n-1}{3}\right]} a_{3k+1} X^{3k+1} + \sum_{k=0}^{\left[\frac{n-2}{3}\right]} a_{3k+2} X^{3k+2}.$$

Dacă punem

$$F(U,V) = \sum_{k=0}^{\left[\frac{n}{3}\right]} a_{3k} V^k + \sum_{k=1}^{\left[\frac{n-1}{3}\right]} a_{3k+1} V^{k-1} U^2 + \sum_{k=0}^{\left[\frac{n-2}{3}\right]} a_{3k+2} V^k U \in \mathbb{Z}[U,V],$$

atunci $f = F(X^2, X^3)$, deci $f \in \mathbb{Z}[X^2, X^3]$.
(ii) Dacă $d|_R X^2$ şi $d|_R X^3$, atunci aceste divizibilităţi au loc şi în $\mathbb{Z}[X]$. Prin urmare, $d \in \{\pm 1, \pm X, \pm X^2\} \cap R = \{\pm 1, \pm X^2\}$. Dar $X^2 \nmid_R X^3$, deci $d \sim_R 1$. Evident, 1 divide X^2 şi X^3 în R, deci $1 = (X^2, X^3)_R$.
Presupunem acum că X^2 şi X^3 admit un c.m.m.m.c. în R, fie el m. Cum X^2 şi X^3 divid în R pe X^5, rezultă că $m|_R X^5$, deci $m|_{\mathbb{Z}[X]} X^5$. Avem şi $X^3|_R m$, deci $X^3|_{\mathbb{Z}[X]} m$. Prin urmare, $m \in \{\pm X^3, \pm X^4, \pm X^5\}$. Dar $X^2 \nmid_R \pm X^3$ şi $X^3 \nmid_R \pm X^4$. A rămas de investigat numai cazul $m = \pm X^5$; nici acesta nu este însă c.m.m.m.c. pentru X^2 şi X^3 în R, căci $X^2|_R X^6$ şi $X^3|_R X^6$, dar $X^5 \nmid_R X^6$. Rămâne aşadar că X^2 şi X^3 nu admit c.m.m.m.c. în R.
(iii) Presupunem că X^5 şi X^6 admit un c.m.m.d.c. în R, fie el d. Atunci, $d|_R X^5$, deci $d|_{\mathbb{Z}[X]} X^5$. Pe de altă parte, $X^3|_R X^5$ şi $X^3|_R X^6$, deci $X^3|_R d$, prin urmare $X^3|_{\mathbb{Z}[X]} d$. În consecinţă, $d \in \{\pm X^3, \pm X^4, \pm X^5\}$. Dar $X^5 \nmid_R \pm X^6$ şi $X^4 \nmid_R \pm X^5$. A rămas de investigat numai cazul $d = \pm X^3$; nici acesta nu este însă c.m.m.d.c. pentru X^5 şi X^6 în R, căci $X^2|_R X^5$ şi $X^2|_R X^6$, dar $X^2 \nmid_R \pm X^3$.
Presupunem acum că X^5 şi X^6 admit un c.m.m.m.c. în R, fie el m. Cum X^5 şi X^6 divid în R pe X^8, rezultă că $m|_R X^8$, deci $m|_{\mathbb{Z}[X]} X^8$. Avem şi $X^6|_R m$, deci $X^6|_{\mathbb{Z}[X]} m$. Prin urmare, $m \in \{\pm X^6, \pm X^7, \pm X^8\}$. Dar $X^5 \nmid_R \pm X^6$ şi $X^6 \nmid_R \pm X^7$. A rămas de investigat numai $m = \pm X^8$; nici acesta nu este însă c.m.m.m.c. pentru X^5 şi X^6 în R, căci $X^5|_R X^9$ şi $X^6|_R X^9$, dar $\pm X^8 \nmid_R X^9$. Rămâne aşadar că X^5 şi X^6 nu admit c.m.m.m.c. în R.
(iv) Dacă $X^2 = fg$ în R, atunci această relaţie are loc şi în $\mathbb{Z}[X]$. Prin urmare, $f = \pm 1$ şi $g = \pm X^2$ (sau viceversa), sau $f = g = \pm X$. Cum acest din urmă caz este imposibil în R, rămâne că singurele descompuneri posibile ale lui X^2 în R au factori inversabili, deci sunt irelevante. Prin urmare, X^2

este ireductibil în R. Pe de altă parte, $X^2|_R X^6 = X^3 \cdot X^3$, dar $X^2 \nmid_R X^3$. Prin urmare, X^2 nu este prim în R.

13. (i) Fie $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$. Pentru orice $i \in \{0, 1, \ldots n\}$ punem $a_i = \alpha_i c(f)$. Notăm $\overline{f} = \alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n$. Dacă un element $d \in R$ divide toţi coeficienţii lui $\overline{f}$, atunci $dc(f)$ divide toţi coeficienţii lui f. Prin urmare, $dc(f)$ va divide şi c.m.m.d.c. al acestora, adică pe $c(f)$. Rezultă că $d \in U(R)$. Prin urmare, $c(\overline{f}) = 1$.
(ii) Fie $f, g \in R$, $f = \sum_{i=0}^{m} a_i X^i$, $g = \sum_{j=0}^{n} b_j X^j$. Atunci avem că $fg = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) X^k$. Cum fiecare a_i se divide prin $c(f)$ şi fiecare b_j se divide prin $c(g)$, rezultă că $\sum_{i+j=k} a_i b_j$ se divide prin $c(f)c(g)$ pentru orice k. În consecinţă, $c(f)c(g)|c(fg)$. Scriem $c(fg) = ac(f)c(g)$, $a \in R$. Cum $c(f)c(g)\overline{f}\,\overline{g} = fg = c(fg)\overline{fg}$, rezultă $\overline{f}\,\overline{g} = a\overline{fg}$.
Notăm $I = aR$, $S = R/I$, $\pi : R \to S$ proiecţia canonică şi $\overline{\pi} : R[X] \to S[X]$, $\overline{\pi}(c_0 + \cdots + c_tX^t) = \pi(c_0) + \cdots + \pi(c_t)X^t$ extinsul lui π la inelele de polinoame corespunzătoare. Atunci $\overline{\pi}(\overline{f})\overline{\pi}(\overline{g}) = 0$.
• Dacă $\overline{\pi}(\overline{f}) = 0$, atunci toţi coeficienţii lui $\overline{f}$ sunt în I, deci se divid cu a. Cum $c(\overline{f}) = 1$, rezultă $a \in U(R)$, deci $c(f)c(g) = c(fg)$.
• Dacă $\overline{\pi}(\overline{f}) \neq 0$, atunci $\overline{\pi}(\overline{g})$ este divizor al lui zero în $S[X]$. Conform problemei 25 din Capitolul 5, există $\widehat{b} \in S \setminus \{0\}$ astfel ca $\widehat{b}\overline{\pi}(\overline{g}) = 0$. Notând $d = (a, b)$, $a = \alpha d$ şi $b = \beta d$, din consideraţiile anterioare rezultă că $\alpha \notin U(R)$ şi $\alpha | \beta\overline{g}$. Dar $(\alpha, \beta) = 1$, deci α divide toţi coeficienţii lui $\overline{g}$. Prin urmare, $\alpha | c(\overline{g})$, contradicţie. Aşadar acest caz este imposibil.
(iii) Rezultă din relaţia $c(f)c(g)\overline{f}\,\overline{g} = fg = c(fg)\overline{fg}$ şi din punctul (ii).
(iv) Este clar că dacă $f|g$ în $R[X]$, atunci $f|g$ şi în $Q[X]$. Pentru reciprocă să presupunem că $f|_{Q[X]}g$. Atunci există $h_1 \in Q[X]$ astfel încât $g = h_1 f$. Aducând coeficienţii lui h_1 la acelaşi numitor, găsim $h \in R[X]$ şi $s \in R \setminus \{0\}$ astfel ca $h_1 = \frac{h}{s}$. Obţinem $sg = fh$, de unde $sc(g) = c(f)c(h)$ şi $s = c(h)$. Atunci $g = f\frac{h}{s} = f\overline{h}$. Prin urmare, $f|_{R[X]}g$.
(v) Dacă $f|_{R[X]}g$, atunci există $h \in R[X]$ cu proprietatea $g = fh$. Conform punctului (ii) obţinem $c(g) = c(f)c(h)$, deci $c(f)|_R c(g)$. Conform punctului (iii), $\overline{g} = u\overline{f} \cdot \overline{h}$, $u \in U(R)$. Prin urmare, $\overline{f}|_{R[X]}\overline{g}$.
Reciproc, dacă $c(g) = c(f)\gamma$, $\gamma \in R$, şi $\overline{g} = \overline{f}h$, $h \in R[X]$, atunci $g = c(g)\overline{g} = c(f)\gamma\overline{f}h = (\gamma h)f$, deci $f|_{R[X]}g$.

(vi) Este echivalent cu (v) conform (iv).

14. Vom folosi în soluţia acestei probleme notaţiile din problema 13. Desemnăm prin Q corpul de fracţii al lui R. Fie $f, g \in R[X]$. Cum $Q[X]$ este inel euclidian, f şi g admit un c.m.m.d.c. în $Q[X]$, fie el d''. Aducând coeficienţii lui d'' la acelaşi numitor, putem scrie $d'' = \frac{d'}{\delta}$ cu $d' \in R[X]$, $\delta \in R$ şi $(c(d'), \delta)_R = 1$. Să considerăm acum $a = (c(f), c(g))_R$ şi $d = a\overline{d'}$. Avem $\frac{f}{d} = \frac{c(f)}{c(d)}\frac{\overline{f}}{\overline{d}} = \frac{c(f)}{a}\frac{\overline{f}}{\overline{d'}}$. Dar $d''|_{Q[X]}f \Rightarrow d'|_{Q[X]}f \Rightarrow \overline{d'}|_{Q[X]}\overline{f}$. Cum $\overline{d'}, \overline{f} \in R[X]$ şi $c(\overline{d'}) = c(\overline{f}) = 1$, rezultă din problema 13(iv) că $\overline{d'}|_{R[X]}\overline{f}$, adică $\frac{\overline{f}}{\overline{d'}} \in R[X]$. Cum $a|c(f)$, obţinem că $\frac{f}{d} \in R[X]$, deci $d|_{R[X]}f$; analog, $d|_{R[X]}g$.
Fie acum $D \in R[X]$ care divide atât pe f cât şi pe g. Conform problemei 13(v), $c(D)|_R c(f)$, $c(D)|_R c(g)$, $\overline{D}|_{R[X]}\overline{f}$ şi $\overline{D}|_{R[X]}\overline{g}$. De aici rezultă că $c(D)|_R(c(f), c(g))_R$ şi $\overline{D}|_{Q[X]}(\overline{f}, \overline{g})_{Q[X]}$; această ultimă relaţie dă imediat şi $\overline{D}|_{Q[X]}\overline{d'}$. Conform problemei 13(vi), obţinem $D|_{R[X]}d$. Prin urmare, d este un c.m.m.d.c. în $R[X]$ pentru f şi g.

15. Să începem cu observaţia că pentru orice $f \in R \setminus \{0\}$ există şi sunt unice $a_f \in \mathbb{Q}$, $r_f \in \mathbb{N}$ şi $\overline{f} \in R$ cu $\overline{f}(0) = 1$ astfel încât $f = a_f X^{r_f}\overline{f}$. Să constatăm că dacă $r_f = 0$, atunci $a_f \in \mathbb{Z}$. Evident, dacă $f|_R g$, atunci $r_f \leq r_g$. În situaţia în care $r_f \leq r_g$, $f|_R g \Rightarrow f|_{\mathbb{Q}[X]}g$. Cum $\frac{g}{f} = \frac{a_g}{a_f}X^{r_g - r_f}\frac{\overline{g}}{\overline{f}}$, obţinem $\overline{f}|_{\mathbb{Q}[X]}\overline{g}$, deci există $h \in \mathbb{Q}[X]$ astfel ca $\overline{g} = \overline{f}h$. Rezultă $h(0) = \overline{f}(0)h(0) = \overline{g}(0) = 1 \in \mathbb{Z}$, deci $h \in R$. Prin urmare, $\overline{f}|_R\overline{g}$. În concluzie, în cazul în care $r_f < r_g$, avem $f|_R g \Leftrightarrow \overline{f}|_R\overline{g}$.
În cazul $r_f = r_g$ avem

$$f|_R g \Leftrightarrow \frac{g}{f} \in R \Leftrightarrow \frac{a_g}{a_f} \cdot \frac{\overline{g}}{\overline{f}} \in R \Leftrightarrow \overline{f}|_R\overline{g} \text{ şi } \frac{a_g}{a_f} \in \mathbb{Z}.$$

Aceste preliminarii fiind încheiate, să arătăm că inelul R are proprietatea c.m.m.d.c. Fie $f, g \in R \setminus \{0\}$. Notăm $h = (\overline{f}, \overline{g})_{\mathbb{Q}[X]}$ şi $\overline{h} = \frac{1}{h(0)}h$.
Dacă $r_f < r_g$, punem $d = a_f X^{r_f}\overline{h}$. Avem $\frac{f}{d} = \frac{\overline{f}}{\overline{h}} \in R$, deci $d|_R f$, şi $\frac{g}{d} = \frac{a_g}{a_f}X^{r_g - r_f}\frac{\overline{g}}{\overline{h}} \in R$, deci $d|_R g$.
Fie acum $d' \in R$ astfel încât $d'|_R f$ şi $d'|_R g$. Pot apărea cazurile:
1. $r_{d'} < r_f$. Atunci $d'|_R f \Rightarrow \overline{d'}|_R\overline{f}$; $d'|_R g \Rightarrow \overline{d'}|_R\overline{g}$. Urmează că $d'|_R\overline{h} = \overline{d}$. Prin urmare, $d'|_R d$.
2. $r_{d'} = r_f$. Atunci $d'|_R f \Rightarrow \overline{d'}|_R\overline{f}$ şi $\frac{a_f}{a_{d'}} \in \mathbb{Z}$; $d'|_R g \Rightarrow \overline{d'}|_R\overline{g}$. Urmează că

$d'|_R\overline{h} = \overline{d}$ şi $\frac{a_d}{a_{d'}} = \frac{a_f}{a_{d'}} \in \mathbb{Z}$. Prin urmare, $d'|_R d$.
Dacă $r_f = r_g$, pot apărea situaţiile:
1. $r_f = r_g = 0$. Punem $d = (a_f, a_g)_{\mathbb{Z}}\overline{h}$. Avem

$$\frac{f}{d} = \frac{a_f\overline{f}}{(a_f, a_g)_{\mathbb{Z}}\overline{h}} \in R \Rightarrow d|_R f;\ \frac{g}{d} = \frac{a_g\overline{g}}{(a_f, a_g)_{\mathbb{Z}}\overline{h}} \in R \Rightarrow d|_R g.$$

Fie acum $d' \in R$ astfel încât $d'|_R f$ şi $d'|_R g$. Atunci $r_{d'} = 0$. Avem

$$d'|_R f \Rightarrow \frac{a_f}{a_{d'}} \cdot \frac{\overline{f}}{\overline{d'}} \in R \Rightarrow a_{d'}|_{\mathbb{Z}} a_f \text{ şi } \overline{d'}|_R\overline{f}$$

şi

$$d'|_R g \Rightarrow \frac{a_g}{a_{d'}} \cdot \frac{\overline{g}}{\overline{d'}} \in R \Rightarrow a_{d'}|_{\mathbb{Z}} a_g \text{ şi } \overline{d'}|_R\overline{g},$$

de unde obţinem $a_{d'}|_{\mathbb{Z}}(a_f, a_g) = a_d$ şi $\overline{d'}|_R(\overline{f}, \overline{g})_{\mathbb{Q}[X]} = \overline{h} = \overline{d}$. De aici rezultă $d'|_R d$.
2. $r_f = r_g > 0$. Punem $a_f = \frac{s_f}{t}$ şi $a_g = \frac{s_g}{t}$ cu $(s_f, s_g, t) = 1$ şi considerăm $d = \frac{(s_f, s_g)}{t} X^{r_f}\overline{h}$. Avem

$$\frac{f}{d} = \frac{\frac{s_f}{t} X^{r_f}\overline{f}}{\frac{(s_f, s_g)}{t} X^{r_f}\overline{h}} = \frac{s_f}{(s_f, s_g)}\frac{\overline{f}}{\overline{h}} \in R \Rightarrow d|_R f$$

şi

$$\frac{g}{d} = \frac{\frac{s_g}{t} X^{r_g}\overline{g}}{\frac{(s_f, s_g)}{t} X^{r_g}\overline{h}} = \frac{s_g}{(s_f, s_g)}\frac{\overline{g}}{\overline{h}} \in R \Rightarrow d|_R g.$$

Fie acum $d' \in R$ astfel încât $d'|_R f$ şi $d'|_R g$. Dacă $r_{d'} < r_f$, atunci, cum $d'|_R f \Rightarrow \overline{d'}|_R\overline{f}$ şi $d'|_R g \Rightarrow \overline{d'}|_R\overline{g}$, obţinem $\overline{d'}|_R\overline{h}$, deci $d'|_R d$. Dacă $r_{d'} = r_f$, atunci $d'|_R f \Rightarrow \overline{d'}|_R\overline{f}$ şi $\frac{a_f}{a_{d'}} \in \mathbb{Z}$ şi $d'|_R g \Rightarrow \overline{d'}|_R\overline{g}$ şi $\frac{a_g}{a_{d'}} \in \mathbb{Z}$. Din aceste relaţii rezultă că $\overline{d'}|_R\overline{h} = \overline{d}$ şi că există $c_f, c_g \in \mathbb{Z}$ cu proprietăţile

$$(**)\quad c_f a_{d'} = \frac{s_f}{t} \text{ şi } c_g a_{d'} = \frac{s_g}{t}.$$

Din ultimele relaţii obţinem $\frac{s_g}{c_g t} = \frac{s_f}{c_f t}$, de unde $c_f s_g = c_g s_f$. Punând $s_f = (s_f, s_g)u_f$ şi $s_g = (s_f, s_g)u_g$, ajungem la $c_f u_g = c_g u_f$. Cum $(u_f, u_g) = 1$, deducem existenţa unor numere întregi c'_f, c'_g pentru care $c_f = c'_f u_f$ şi $c_g =$

$c'_g u_g$. Introducând în $(**)$ obţinem $c'_f a_{d'} = \frac{(s_f, s_g)}{t}$, de unde $\frac{a_d}{a_{d'}} = \frac{(s_f,s_g)/t}{(s_f,s_g)/(c'_f t)} \in \mathbb{Z}$. Cum anterior obţinuserăm $\overline{d'}|_R\overline{d}$, rezultă $d'|_R d$.
Dacă $f = 0$, atunci este clar că $c.m.m.d.c.(f,g)_R = g$, iar dacă $g = 0$, atunci $c.m.m.d.c.(f,g)_R = f$.
În concluzie, R are proprietatea c.m.m.d.c.

Să presupunem acum că R este inel factorial. Cum X e nenul şi neinversabil în R, vor exista $n \in \mathbb{N}^*$ şi elementele $p_1, \ldots, p_n$ prime în R astfel ca $X = p_1 \cdots p_n$.
Dacă ar exista $a, b \in R \setminus U(R)$ astfel încât $2 = ab$, atunci, privind această relaţie în $\mathbb{Q}[X]$, rezultă $a, b \in \mathbb{Q}^*$. Dar $a, b \in R$, deci $a, b \in \mathbb{Z}$. Din $2 = ab$ obţinem că unul dintre elementele a şi b este inversabil, contradicţie. Prin urmare, 2 este ireductibil în R. Cum R are proprietatea c.m.m.d.c., rezultă că 2 este prim în R.
Considerând acum în R relaţia $X = 2^{n+1}\left(\frac{1}{2^{n+1}}X\right)$, deducem că $2^{n+1}|_R X = p_1 \cdots p_n$. De aici rezultă că $p_1 = \ldots = p_n = 2$ şi $2|_R 1$, contradicţie. Rămâne că R nu este factorial.

16. Să notăm $S = \{\frac{r}{s} | r \in \mathbb{Z}, s \in 2\mathbb{Z}+1, (r,s) = 1\} \subset \mathbb{Q}$. Pentru fiecare $f \in \mathbb{Q}[[X]]$ vom nota termenul său liber cu $\widetilde{f}$. Observăm că pentru orice $f \in R \setminus \{0\}$ există şi sunt unice $r_f \in \mathbb{N}$ şi $u_f \in \mathbb{Q}[[X]]$ astfel încât $f = X^{r_f} u_f$ şi $\widetilde{u_f} \neq 0$. În plus, $r_f = 0$ impune $\widetilde{u_f} \in S$.
Pentru elementele $f, g \in R \setminus \{0\}$, $f|g$ implică în mod clar $r_f \leq r_g$. În situaţia $r_f < r_g$ avem $g = X^{r_g} u_g = (X^{r_g - r_f} u_g u_f^{-1}) X^{r_f} u_f$, de unde $f|g$. Dacă $r_f = r_g$, atunci este evident că $f|g$ dacă şi numai dacă $\frac{\widetilde{u_g}}{\widetilde{u_f}} \in S$.
Am arătat deci că $f|g$ în R dacă şi numai dacă sunt într-una din următoarele două situaţii:
a) $r_f < r_g$ sau
b) $r_f = r_g$ şi $\frac{\widetilde{u_g}}{\widetilde{u_f}} \in S$.

Trecem acum la demonstraţia faptului că R are proprietatea c.m.m.d.c. Este evident că orice $f \in R$ este c.m.m.d.c. între el însuşi şi 0.
Fie acum $f, g \in R \setminus \{0\}$. Dacă $r_f < r_g$, atunci $f|g$, deci $f = (f,g)$. Dacă $r_f = r_g$, să notăm $\widetilde{u_f} = \frac{a_f}{s_f} \cdot 2^{v_f}$ şi $\widetilde{u_g} = \frac{a_g}{s_g} \cdot 2^{v_g}$, unde $a_f, s_f, a_g, s_g \in 2\mathbb{Z}+1$, iar $v_f, v_g \in \mathbb{Z}$. Notăm $v = \min\{v_f, v_g\}$ şi punem $d = 2^v X^{r_f}$.
Avem $f = X^{r_f} u_f = u_f \cdot 2^{-v} d = \frac{2^{v_f - v} a_f}{s_f}\left(\frac{s_f}{a_f} u_f\right) d$, deci $d|f$. Analog obţinem $d|g$.

Fie acum $d' \in R$ cu $d'|f$ şi $d'|g$. Dacă $r_{d'} < r_f$, atunci $d'|d$. Dacă $r_{d'} = r_f$, din $d'|f$ şi $d'|g$ deducem $\frac{\widetilde{u_f}}{\widetilde{u_{d'}}}, \frac{\widetilde{u_g}}{\widetilde{u_{d'}}} \in S$, deci există $\lambda_f, \lambda_g \in \mathbb{N}$ şi $\alpha_f, \alpha_g, \sigma \in 2\mathbb{Z}+1$, $(\alpha_f, \alpha_g, \sigma) = 1$, astfel încât $\frac{\widetilde{u_f}}{\widetilde{u_{d'}}} = 2^{\lambda_f}\frac{\alpha_f}{\sigma}$ şi $\frac{\widetilde{u_g}}{\widetilde{u_{d'}}} = 2^{\lambda_g}\frac{\alpha_g}{\sigma}$. Deducem $\frac{a_f}{s_f} \cdot 2^{v_f} = 2^{\lambda_f}\frac{\alpha_f}{\sigma}\widetilde{u_{d'}}$ şi $\frac{a_g}{s_g} \cdot 2^{v_g} = 2^{\lambda_g}\frac{\alpha_g}{\sigma}\widetilde{u_{d'}}$. De aici urmează $\widetilde{u_{d'}} = 2^{v_f-\lambda_f}\frac{a_f\sigma}{s_f\alpha_f} = 2^{v_g-\lambda_g}\frac{a_g\sigma}{s_g\alpha_g}$. În consecinţă, $2^{v_f-\lambda_f}a_fs_g\alpha_g = 2^{v_g-\lambda_g}a_gs_f\alpha_f$. Obţinem de aici $v_f - \lambda_f = v_g - \lambda_g$, deci $v_f - \lambda_f \leq v_g$. Atunci $d = 2^vX^{r_f} \sim_R 2^{\min\{v_f,v_g\}}\frac{s_f\alpha_f}{a_f\sigma\cdot 2^{v_f-\lambda_f}}d' = 2^{\min\{v_f,v_g\}-(v_f-\lambda_f)}\frac{s_f\alpha_f}{a_f\sigma} \cdot d'$. De aici rezultă că $d'|d$. Prin urmare, R are proprietatea c.m.m.d.c.

Să presupunem acum că 2 se scrie în R sub forma fg. Atunci, f şi g vor avea ordin zero. Dacă notăm $\widetilde{u_f} = \frac{a_f}{s_f}$ şi $\widetilde{u_g} = \frac{a_g}{s_g}$, cu $s_f, s_g \in 2\mathbb{Z}+1$ şi $(a_f, s_f) = (a_g, s_g) = 1$, avem $2 = \frac{a_fa_g}{s_fs_g}$, deci $2|a_f$ şi $2 \nmid a_g$ sau invers. Prin urmare, $\widetilde{u_f} \in U(S)$ sau $\widetilde{u_g} \in U(S)$, deci $f \in U(R)$ sau $g \in U(R)$. Cum R are proprietatea c.m.m.d.c., rezultă că 2 este prim în R.

Presupunem acum că R este factorial. Atunci există $n \in \mathbb{N}^*$, unic determinat, şi există elementele prime $p_1, \ldots, p_n \in R$ astfel încât $X = p_1 \cdots p_n$. Dar $X = 2^{n+1} \cdot \left(\frac{1}{2^{n+1}}X\right)$, de unde $2^{n+1}|p_1 \cdots p_n$. De aici deducem $p_1 = \ldots = p_n = 2$ şi $2|1$, contradicţie. Rămâne aşadar că R nu este inel factorial.

17. Notăm $R = \mathbb{Z}[\sqrt{2}]$ şi definim $N : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}$, $N(a+b\sqrt{2}) = |a^2-2b^2|$. Conform problemei 2(ii),(iii), N este multiplicativă şi $N(\mathbb{Z}[\sqrt{2}]) \subset \mathbb{N}$. Fie $x = a + b\sqrt{2}$ şi $y = c + d\sqrt{2}$, $y \neq 0$, elemente din R. Avem în $\mathbb{R}$

$$\frac{x}{y} = \frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{ac-2bd}{c^2-2d^2} + \frac{bc-ad}{c^2-2d^2}\sqrt{2}.$$

Prin urmare, $\frac{x}{y} \in \mathbb{Q}[\sqrt{2}]$. Notăm

$$\alpha = \frac{ac-2bd}{c^2-2d^2} \text{ şi } \beta = \frac{bc-ad}{c^2-2d^2},$$

iar cu A şi B întregii cei mai apropiaţi de α, respectiv de β. Prin urmare, $|A-\alpha| \leq \frac{1}{2}$ şi $|B-\beta| \leq \frac{1}{2}$. Cu aceste notaţii se obţine

$$\frac{x}{y} = A + B\sqrt{2} + (\alpha - A) + (\beta - B)\sqrt{2},$$

deci $x = (A + B\sqrt{2})y + [(\alpha - A) + (\beta - B)\sqrt{2}]y$. Cum x, y şi $q = A + B\sqrt{2}$ sunt în R, din relaţia anterioară rezultă că $r = [(\alpha - A) + (\beta - B)\sqrt{2}]y \in R$.

Avem deci în R scrierea $x = qy + r$. În plus, datorită multiplicativităţii lui N, $N(r) = N((\alpha - A) + (\beta - B)\sqrt{2})N(y) = N(y)|(\alpha - A)^2 - 2(\beta - B)^2|$. Avem însă $0 \leq (\alpha - A)^2 \leq \frac{1}{4}$ şi $-\frac{1}{2} \leq -2(\beta - B)^2 \leq 0$. Adunând membru cu membru aceste relaţii, obţinem $-\frac{1}{2} \leq (\alpha - A)^2 - 2(\beta - B)^2 \leq \frac{1}{4}$, de unde $|(\alpha - A)^2 - 2(\beta - B)^2| \leq \frac{1}{2}$. Prin urmare, $N(r) = N(y)|(\alpha - A)^2 - 2(\beta - B)^2| \leq \frac{1}{2}N(y) < N(y)$. În concluzie, R este inel euclidian în raport cu N.

Notăm $R = \mathbb{Z}[\omega]$, unde $\omega = \frac{1+\sqrt{5}}{2}$. Observăm că $\mathbb{Q}[\omega] = \{a + b\omega | a, b \in \mathbb{Q}\} = \{u + v\sqrt{5} | u, v \in \mathbb{Q}\} = \mathbb{Q}[\sqrt{5}]$. Considerăm $N : \mathbb{Q}[\sqrt{5}] \to \mathbb{Q}$, $N(u + v\sqrt{5}) = |a^2 - 5b^2|$. Conform problemei 2(ii), N este multiplicativă. Observăm şi că $N(a + b\omega) = |a^2 + ab - b^2|$, de unde $N(R) \subset \mathbb{N}$. Se constată imediat prin dublă incluziune că $R = \{\frac{a+b\sqrt{5}}{2} \mid a, b \in \mathbb{Z} \text{ au aceeaşi paritate}\}$. Fie $x = \frac{a+b\sqrt{5}}{2}$ şi $y = \frac{c+d\sqrt{5}}{2} \neq 0$ elemente din R. Avem în $\mathbb{R}$

$$\frac{x}{y} = \frac{a + b\sqrt{5}}{c + d\sqrt{5}} = \frac{ac - 5bd}{c^2 - 5d^2} + \frac{bc - ad}{c^2 - 5d^2}\sqrt{5}.$$

Prin urmare, $\frac{x}{y} \in \mathbb{Q}[\sqrt{5}]$. Notăm

$$\alpha = \frac{ac - 5bd}{c^2 - 5d^2} \text{ şi } \beta = \frac{bc - ad}{c^2 - 5d^2}$$

şi alegem B cel mai apropiat întreg de 2β (deci, $|\beta - \frac{B}{2}| \leq \frac{1}{4}$) şi A cel mai apropiat întreg de aceeaşi paritate cu B de 2α (deci, $|\alpha - \frac{A}{2}| \leq \frac{1}{2}$). Cu aceste notaţii se obţine

$$\frac{x}{y} = \frac{A + B\sqrt{5}}{2} + (\alpha - \frac{A}{2}) + (\beta - \frac{B}{2})\sqrt{5},$$

deci $x = (\frac{A+B\sqrt{5}}{2})y + [(\alpha - \frac{A}{2}) + (\beta - \frac{B}{2})\sqrt{5}]y$. Cum x, y şi $q = \frac{A+B\sqrt{5}}{2}$ sunt în R, din relaţia anterioară rezultă că $r = [(\alpha - \frac{A}{2}) + (\beta - \frac{B}{2})\sqrt{5}]y \in R$. Avem deci în R scrierea $x = qy + r$. În plus, datorită multiplicativităţii lui N, $N(r) = N((\alpha - \frac{A}{2}) + (\beta - \frac{B}{2})\sqrt{5})N(y) = N(y)|(\alpha - \frac{A}{2})^2 - 5(\beta - \frac{B}{2})^2| \leq \frac{5}{16}N(y) < N(y)$. Prin urmare, R este inel euclidian în raport cu N.

18. Notăm $R = \mathbb{Z}[\frac{1+i\sqrt{d}}{2}]$.

"$\Rightarrow$" Să presupunem că $d \geq 15$. Cum R este inel euclidian, există $\varphi : R \setminus \{0\} \longrightarrow \mathbb{N}$ astfel încât oricare ar fi $a, b \in R$, $b \neq 0$, există $q, r \in R$ cu proprietăţile $a = bq + r$ şi $r = 0$ sau $\varphi(r) < \varphi(b)$. Considerăm şi norma

$N : R \longrightarrow \mathbb{N}$, $N(x + y\frac{1+i\sqrt{d}}{2}) = x^2 + xy + \frac{1+d}{4}y^2$. Conform problemei 2, N este multiplicativă, iar $U(R) = \{a \in R \mid N(a) = 1\}$.
Procedând ca la soluţia problemei 4, obţinem $U(R) = \{-1, 1\}$. Fie $\alpha \in R \setminus \{-1, 0, 1\}$ astfel că $\varphi(\alpha) = \min\{\varphi(a) \mid a \in R \setminus \{-1, 0, 1\}\}$. (Remarcăm că acest minim este atins, întrucât $\mathbb{N}$ este bine ordonată.) Dacă z este un element arbitrar din R, atunci, conform proprietăţilor lui φ, există $q, r \in R$ cu proprietăţile $z = q\alpha + r$ şi $r = 0$ sau $\varphi(r) < \varphi(\alpha)$. Conform definiţiei lui α, ultima inegalitate nu este posibilă decât dacă $r \in \{-1, 0, 1\}$.
În consecinţă, orice element din R este congruent cu $-1, 0$ sau 1 modulo α. În particular 2 este congruent cu $-1, 0$ sau 1 modulo α, de unde $\alpha|3$ sau $\alpha|2$ sau $\alpha|1$. Ultimul caz este însă imposibil deoarece $\alpha \notin U(R)$. Trecând la norme în celelalte două relaţii obţinem (vezi problema 3(i)) că $N(\alpha)|9$ sau $N(\alpha)|4$. Cum α nu este inversabil, el nu poate avea norma 1. Prin urmare, $N(\alpha) \in \{2, 3, 4, 9\}$. Reamintind că $R = \left\{\alpha + \beta\frac{1+i\sqrt{d}}{2} \mid \alpha, \beta \in \mathbb{Z}\right\} = \left\{\frac{a+bi\sqrt{d}}{2} \mid a, b \in \mathbb{Z} \text{ au aceeaşi paritate}\right\}$, notăm $\alpha = \frac{a+bi\sqrt{d}}{2}$, unde $a, b \in \mathbb{Z}$ au aceeaşi paritate.
Dacă $N(\alpha) \in \{2, 3\}$, rezultă $a^2 + db^2 \in \{8, 12\}$. Dacă $b = 0$, obţinem $a^2 \in \{8, 12\}$, iar dacă $|b| \geq 1$ găsim $a^2 < 0$, contradicţie.
Dacă $N(\alpha) = 4$, vom avea $a^2 + db^2 = 16$; dacă $b = 0$ obţinem $\alpha = \pm 2 \sim 2$. Constatăm însă că dacă $\frac{1+i\sqrt{d}}{2}$ ar da rest $-1, 0$ sau 1 modulo 2, atunci ar avea loc în R o relaţie de forma $\frac{1+i\sqrt{d}}{2} = 2 \cdot \frac{u+vi\sqrt{d}}{2} + \varepsilon$, de unde $1 + i\sqrt{d} = 2(u + vi\sqrt{d}) + 2\varepsilon$ cu $\varepsilon \in \{-1, 0, 1\}$. Rezultă $1 = 2v$, contradicţie.
Dacă $|b| = 1$, avem variantele $d > 15$ (în care obţinem $a^2 = 4 - db^2 < 0$, contradicţie) şi $d = 15$ (în care vom avea $\alpha \sim \frac{1\pm i\sqrt{15}}{2}$. Atunci 2 trebuie să admită în R o scriere de forma $2 = \frac{1\pm i\sqrt{15}}{2} \cdot q + \varepsilon$, $\varepsilon \in \{-1, 0, 1\}$. Rezultă că $\frac{1\pm i\sqrt{15}}{2}$ divide 1,2 sau 3. Cum el are normă 4, rezultă că îl divide pe 2. Conform problemei 3(iii), rezultă că $\frac{1\pm i\sqrt{15}}{2} \sim 2$, contradicţie.) Dacă $|b| > 1$, obţinem $a^2 = 4 - db^2 < 0$, contradicţie.
Dacă $N(\alpha) = 9$, vom avea $a^2 + db^2 = 36$; pentru $b = 0$ obţinem $\alpha = \pm 3 \sim 3$; constatăm însă că dacă $i\sqrt{d}$ ar da rest $-1, 0$ sau 1 modulo 3, atunci ar avea loc în R o relaţie de tipul $\frac{1+i\sqrt{d}}{2} = 3\frac{u+vi\sqrt{d}}{2} + \varepsilon$ cu $\varepsilon \in \{-1, 0, 1\}$, de unde $1 = 3v$, contradicţie.
Dacă $|b| = 1$, distingem cazurile:
$d = 15$, în care obţinem $a^2 = 21$, contradicţie;
$d = 19$, în care obţinem $a^2 = 17$, contradicţie;

$d = 23$, în care obţinem $a^2 = 13$, contradicţie;
$d = 31$, în care obţinem $a^2 = 5$, contradicţie;
$d = 35$, în care obţinem $a^2 = 1$, deci $\alpha \sim \frac{1\pm i\sqrt{35}}{2}$. Va exista atunci $q \in R$ astfel ca $2 = \frac{1\pm i\sqrt{35}}{2} \cdot q + \varepsilon$, $\varepsilon \in \{-1, 0, 1\}$, de unde $\frac{1\pm i\sqrt{35}}{2}$ divide 1,2 sau 3. Având norma 9, $\frac{1\pm i\sqrt{35}}{2}$ va trebui să îl dividă pe 3. Conform problemei 3(iii), rezultă că $\frac{1\pm i\sqrt{35}}{2} \sim 3$, contradicţie.
$d \geq 39$, în care obţinem $a^2 < 0$, contradicţie.
Dacă $|b| > 1$, obţinem $a^2 = 36 - db^2 < 0$, contradicţie.
Rămâne aşadar că inelul R nu este euclidian.
"$\Leftarrow$" Fie $d \in \{3, 7, 11\}$. Definim $N : \mathbb{Q}[i\sqrt{d}] \to \mathbb{Q}$, $N(a + bi\sqrt{d}) = a^2 + db^2$. Conform problemei 2, N este multiplicativă şi $N(R) \subset \mathbb{N}$. Fie $x = \frac{a+bi\sqrt{d}}{2}$ şi $y = \frac{c+ei\sqrt{d}}{2} \neq 0$ elemente din R. Avem în $\mathbb{C}$

$$\frac{x}{y} = \frac{a + bi\sqrt{d}}{c + ei\sqrt{d}} = \frac{ac + dbe}{c^2 + de^2} + \frac{bc - ae}{c^2 + de^2} i\sqrt{d}.$$

Prin urmare, $\frac{x}{y} \in \mathbb{Q}[i\sqrt{d}]$. Notăm

$$\alpha = \frac{ac + dbe}{c^2 + de^2} \text{ şi } \beta = \frac{bc - ae}{c^2 + de^2}$$

şi alegem B cel mai apropiat întreg de 2β (deci, $|\beta - \frac{B}{2}| \leq \frac{1}{4}$) şi A cel mai apropiat întreg de aceeaşi paritate cu B de 2α (deci, $|\alpha - \frac{A}{2}| \leq \frac{1}{2}$). Cu aceste notaţii, se obţine

$$\frac{x}{y} = \frac{A + Bi\sqrt{d}}{2} + (\alpha - \frac{A}{2}) + (\beta - \frac{B}{2})i\sqrt{d},$$

deci $x = (\frac{A+Bi\sqrt{d}}{2})y + \left[(\alpha - \frac{A}{2}) + (\beta - \frac{B}{2})i\sqrt{d}\right] y$. Cum x, y şi $q = \frac{A+B\sqrt{d}}{2}$ sunt în R, din relaţia anterioară rezultă că $r = \left[(\alpha - \frac{A}{2}) + (\beta - \frac{B}{2})i\sqrt{d}\right] y \in R$. Avem deci în R scrierea $x = qy + r$. În plus, datorită multiplicativităţii lui N, $N(r) = N((\alpha - \frac{A}{2}) + (\beta - \frac{B}{2})i\sqrt{d})N(y) = N(y)\left(\alpha - \frac{A}{2})^2 + d(\beta - \frac{B}{2})^2\right) \leq \frac{4+d}{16}N(y) \leq \frac{15}{16}N(y) < N(y)$. Prin urmare, R este euclidian în raport cu N.

19. (i) $\Rightarrow$ (ii) Fie $\mathfrak{p}$ un ideal prim nenul al lui R şi $a \in \mathfrak{p} \setminus \{0\}$. Elementul a fiind în $\mathfrak{p}$, rezultă că este neinversabil, deci se scrie ca produs de elemente prime din R, să zicem $a = p_1 \cdots p_n$, $n \geq 1$. Cum $\mathfrak{p}$ este ideal prim, el conţine

măcar unul dintre factorii acestui produs.
(ii) $\Rightarrow$ (i) Notăm $S = \{a \in R \mid \ a \text{ se scrie ca produs de elemente prime}\}$. S este în mod evident un sistem multiplicativ. Presupunem că există $a \in R \setminus S$ nenul şi neinversabil. Dacă $(a) \cap S \neq \emptyset$, atunci ar exista $\alpha \in R$ astfel ca $a\alpha = p_1 \cdots p_n$ cu $p_1, \ldots, p_n$ prime şi $n \geq 1$ minim. Dacă $n = 1$, atunci $\alpha \in U(R)$, iar relaţia $a = \alpha^{-1} p_1$ arată că $a \in S$, contradicţie. Pentru $n \geq 2$, dacă nici unul dintre factorii din membrul drept nu divide pe α, atunci $p_1 \cdots p_n | a$; punând $a = b p_1 \cdots p_n$, obţinem $b\alpha = 1$, deci $b \in U(R)$. Prin urmare, $a = (bp_1)p_2 \cdots p_n$ este o scriere a lui a ca produs de elemente prime, contradicţie. Dacă pe de altă parte vreunul dintre elementele $p_1, \ldots, p_n$, să zicem p_n, divide pe α, atunci, punând $\alpha = \beta p_n$, am avea scrierea $a\beta = p_1 \cdots p_{n-1}$, contradicţie cu minimalitatea lui n. Rămâne aşadar că $(a) \cap S = \emptyset$. Prin urmare, mulţimea idealelor lui R care conţin pe (a) şi nu intersectează S este nevidă. Această mulţime este inductiv ordonată în raport cu incluziunea. Aplicând lema lui Zorn, deducem că admite un element maximal pe care îl notăm cu $\mathfrak{p}$.
Presupunem că $\mathfrak{p}$ nu este ideal prim. Atunci există $x, y \in R$ astfel încât $xy \in \mathfrak{p}$, dar $x, y \notin \mathfrak{p}$. Atunci, idealele $\mathfrak{p} + (x)$ şi $\mathfrak{p} + (y)$ conţin strict pe $\mathfrak{p}$, deci ele trebuie să intersecteze pe S. Fie $u = \pi + \alpha x \in (\mathfrak{p} + (x)) \cap S$ şi $v = \rho + \beta y \in (\mathfrak{p} + (y)) \cap S$, unde $\pi, \rho \in \mathfrak{p}$, $\alpha, \beta \in R$. Atunci $uv = \pi\rho + \pi\beta y + \rho\alpha x + \alpha\beta xy \in \mathfrak{p} \cap S$, contradicţie.
Rămâne deci că $\mathfrak{p}$ este ideal prim. Atunci, conform ipotezei, el trebuie să conţină un element prim, care se va afla însă şi în S. Prin urmare, $\mathfrak{p} \cap S \neq \emptyset$, contradicţie.
Presupunerea că există elemente nenule şi neinversabile în afara lui S este deci incorectă. Prin urmare, toate elementele nenule şi neinversabile ale lui R se scriu ca produs de elemente prime. În consecinţă, R este inel factorial.

20. Se ştie că orice inel de fracţii al unui domeniu de integritate este de asemenea domeniu de integritate.
Considerăm pentru început că R este inel euclidian în raport cu φ. Definim

$$\overline{\varphi} : S^{-1}R \setminus \{0\} \to \mathbb{N},\ \overline{\varphi}\left(\frac{a}{s}\right) = \min\left\{\varphi(\alpha) \mid \exists \sigma \in S \text{ cu } \frac{a}{s} = \frac{\alpha}{\sigma}\right\}.$$

Fie $\frac{a}{s}$ şi $\frac{b}{t} \neq 0$ din $S^{-1}R$ şi $\frac{\beta}{\tau} = \frac{b}{t}$ astfel ca $\overline{\varphi}\left(\frac{b}{t}\right) = \varphi(\beta)$. Cum R e euclidian, există $q, r \in R$ astfel ca $a = \beta q + r$ şi $r = 0$ sau $\varphi(r) < \varphi(\beta)$. Rezultă că

$\frac{a}{s} = \frac{q\tau}{s}\frac{\beta}{\tau} + \frac{r}{s}$ în $S^{-1}R$. Dacă $r \neq 0$, atunci

$$\overline{\varphi}\left(\frac{r}{s}\right) = \min\left\{\varphi(\rho) \mid \exists \sigma \in S \text{ cu } \frac{r}{s} = \frac{\rho}{\sigma}\right\} \leq \varphi(r) < \varphi(\beta) = \overline{\varphi}\left(\frac{b}{t}\right).$$

Prin urmare, $S^{-1}R$ este inel euclidian în raport cu $\overline{\varphi}$.

Dacă R este inel principal, fie J un ideal al lui $S^{-1}R$. Atunci (vezi problema 49 din Capitolul 5) există un ideal I al lui R astfel încât $J = S^{-1}I = \left\{\frac{a}{s} \mid a \in I,\ s \in S\right\}$. Fie b un generator al idealului (principal) I al lui R şi fie $\frac{a}{s} \in J$. Există atunci $\alpha \in R$ astfel încât $a = b\alpha$. Este clar atunci că $\frac{a}{s} = \frac{b}{1} \cdot \frac{\alpha}{s}$. Rezultă că J este ideal principal al lui $S^{-1}R$. Cum J a fost luat arbitrar, deducem că $S^{-1}R$ este inel principal.

Dacă R este inel factorial, să considerăm un element prim $p \in R$ care nu divide nici un element din S. Atunci p este nenul şi neinversabil ($\frac{p}{1} \cdot \frac{a}{s} = \frac{1}{1}$ înseamnă $pa = s$, adică $p|_R s$, contradicţie) în $S^{-1}R$. Dacă $p|_{S^{-1}R}\frac{a}{s} \cdot \frac{b}{t}$, atunci există $\frac{c}{u} \in S^{-1}R$ astfel ca $\frac{p}{1}\frac{c}{u} = \frac{a}{s}\frac{b}{t}$, de unde $pcst = abu$. Rezultă că $p|_R abu$. Dar p e prim în R şi nu divide $u \in S$, deci $p|_R a$ sau $p|_R b$. Dacă, de exemplu, $p|_R a$, atunci există $\alpha \in R$ pentru care $a = p\alpha$, de unde $\frac{a}{s} = \frac{p}{1}\frac{\alpha}{s}$, deci $p|_{S^{-1}R}\frac{a}{s}$. În acelaşi mod se arată că $p|_R b$ conduce la $p|_{S^{-1}R}\frac{b}{t}$. În concluzie, orice element prim din R care nu divide nici un element din S este prim şi în $S^{-1}R$. Fie acum un element nenul şi neinversabil $x = \frac{a}{s} \in S^{-1}R$. Atunci a este şi el nenul şi neinversabil în R, deci se poate scrie sub forma $a = p_1 \cdots p_n$, $n \geq 1$, unde $p_1, \ldots, p_n$ sunt elemente prime din R. După o eventuală renumerotare, putem considera că $p_1, \ldots, p_r$ $(0 \leq r < n)$ divid elemente din S, iar $p_{r+1}, p_{r+2}, \ldots, p_n$ nu divid elemente din S. Putem scrie atunci

$$x = \left(\frac{p_1 \cdots p_r}{s} \cdot \frac{p_{r+1}}{1}\right) \cdot \frac{p_{r+2}}{1} \cdots \frac{p_n}{1}.$$

În concluzie (observând că elementul $\frac{p_1 \cdots p_r}{s} \in S^{-1}R$ este inversabil), x se scrie ca produs de elemente prime din $S^{-1}R$. Prin urmare, $S^{-1}R$ este inel factorial.

21. Fie $\mathfrak{p}$ un ideal prim nenul al lui R. Dacă $\mathfrak{p} \cap S \neq \emptyset$, atunci există în $\mathfrak{p}$ un element de forma $p_1 \cdots p_n$, $n \geq 1$, unde $p_1, \ldots p_n$ sunt elemente prime din R. Cum $\mathfrak{p}$ este ideal prim, cel puţin unul dintre factorii acestui produs se va afla în $\mathfrak{p}$.

Dacă pe de altă parte $\mathfrak{p} \cap S = \emptyset$, atunci, conform problemei 50 din Capitolul 5, $S^{-1}\mathfrak{p} = \left\{\frac{a}{s} \mid a \in \mathfrak{p},\ b \in S\right\}$ este un ideal prim (nenul) al lui $S^{-1}R$. Cum $S^{-1}R$ este un inel factorial, deducem, în virtutea problemei 19, că $S^{-1}\mathfrak{p}$

conţine un element prim, fie el $\frac{q}{s}$. Dar $\frac{q}{s} = \frac{1}{s}\frac{q}{1}$, iar $\frac{1}{s}$ e inversabil în $S^{-1}R$, prin urmare putem considera că elementul prim din $S^{-1}\mathfrak{p}$ este chiar $\frac{q}{1}$. Să presupunem că q se divide în R prin elementul p_{i_1}, $i_1 \in I$. Atunci, există $q_1 \in R$ cu $q = p_{i_1}q_1$. Cum $p_{i_1} \in S$, rezultă că $p_{i_1} \notin \mathfrak{p}$ şi $p_{i_1} \in U(S^{-1}R)$, deci $q_1 \in \mathfrak{p}$ şi $\frac{q}{1} \sim_{S^{-1}R} \frac{q_1}{1}$. Dacă există p_{i_2}, $i_2 \in I$, care să dividă în R pe q_1, atunci există $q_2 \in R$ cu $q_1 = p_{i_2}q_2$. Cum $p_{i_2} \in S$, rezultă că $p_{i_2} \notin \mathfrak{p}$ şi $p_{i_2} \in U(S^{-1}R)$, deci $q_2 \in \mathfrak{p}$ şi $\frac{q_1}{1} \sim_{S^{-1}R} \frac{q_2}{1}$. Continuând în acest mod, obţinem şirul $q, q_1, q_2, \ldots$ de elemente din $\mathfrak{p}$, cu $q_1|_R q$, $q_2|_R q_1$, ş.a.m.d. În termeni de ideale aceasta înseamnă că $qR \subset q_1R \subset q_2R \subset \ldots$. Conform ipotezei, acest şir ascendent de ideale principale este staţionar; prin urmare, există un rang n pentru care $q_n \sim_R q_{n+1}$. Deci $\frac{q_n}{1} \sim_{S^{-1}R} \frac{q}{1}$, aşadar $\frac{q_n}{1}$ este prim în $S^{-1}R$, şi q_n nu se divide prin p_i pentru nici un $i \in I$.
Presupunem acum că $q_n|ab$ în R. Atunci, $\frac{q_n}{1}|_{S^{-1}R}\frac{a}{1} \cdot \frac{b}{1}$; prin urmare, $\frac{q_n}{1}|_{S^{-1}R}\frac{a}{1}$ sau $\frac{q_n}{1}|_{S^{-1}R}\frac{b}{1}$. Dacă $\frac{q_n}{1}|_{S^{-1}R}\frac{a}{1}$, atunci $\frac{a}{1} = \frac{q_n}{1} \cdot \frac{c}{s}$, $c \in R$, $s = p_{i_1} \cdots p_{i_r} \in S$. Deducem $p_{i_1} \cdots p_{i_r}a = q_nc$. Cum q_n nu se divide prin p_i pentru nici un $i \in I$, rezultă că $p_{i_1} \cdots p_{i_r}|_R c$. Scriem $c = p_{i_1} \cdots p_{i_r}d$, $d \in R$. Obţinem $a = q_nd$, deci $q_n|_R a$. Pentru $\frac{q_n}{1}|_{S^{-1}R}\frac{b}{1}$ se procedează analog şi se obţine $q_n|_R b$. Prin urmare, $q_n \in \mathfrak{p}$ este element prim.
În concluzie, orice ideal prim nenul al lui R conţine un element prim. Conform problemei 19, R este inel factorial.

22. (i) Conform problemei 55 din Capitolul 5, $K[X,Y]/(XY-1) \simeq S^{-1}K[X]$, unde S este sistemul multiplicativ al lui $K[X]$ format din puterile lui X. Cum $K[X]$ este inel euclidian, deducem, folosind problema 20, că $S^{-1}K[X]$ este inel euclidian. Izomorfismul de mai sus ne arată că inelul $K[X,Y]/(XY-1)$ este la rândul său inel euclidian.
(ii) Considerăm morfismele de inele $\Phi : \mathbb{C}[X,Y] \to \mathbb{C}[U,V]$ cu proprietăţile $\Phi(a) = a$ pentru orice $a \in \mathbb{C}$, $\Phi(X) = \frac{1}{2}(U+V)$, $\Phi(Y) = \frac{1}{2}i(V-U)$ şi $\Psi : \mathbb{C}[U,V] \to \mathbb{C}[X,Y]$ cu proprietăţile $\Psi(a) = a$ pentru orice $a \in \mathbb{C}$, $\Psi(U) = X + iY$ şi $\Psi(V) = X - iY$ (existenţa morfismelor Φ şi Ψ e asigurată de proprietatea de universalitate a inelelor de polinoame).
Se constată imediat că Φ şi Ψ sunt inverse unul celuilalt, deci sunt izomorfisme. Dacă notăm cu π proiecţia canonică a lui $\mathbb{C}[U,V]$ pe $\mathbb{C}[U,V]/(UV-1)$, constatăm imediat că $w = \pi \circ \Phi$ este morfism surjectiv şi $\operatorname{Ker} w = (X^2+Y^2-1)$. Aplicând teorema fundamentală de izomorfism pentru inele, obţinem

$$\frac{\mathbb{C}[X,Y]}{(X^2+Y^2-1)} \simeq \frac{\mathbb{C}[U,V]}{(UV-1)}.$$

Cum inelul din membrul drept al relaţiei anterioare este inel euclidian conform punctului (i), demonstraţia este încheiată.

23. Să notăm $A = R[X_1, \ldots, X_n]$.
„⇒": Presupunem pentru început că R nu este corp. Atunci există un element $a \in R$ nenul şi neinversabil. Presupunem că idealul $I = (a, X_1)$ este principal. Există atunci $f \in A$ astfel încât $I = (f)$. Cum $X_1 \in I$, rezultă că există $g \in A$ aşa încât $X_1 = fg$. De aici, $\text{grad}_{X_1}(f) + \text{grad}_{X_1}(g) = \text{grad}_{X_1}(X_1) = 1$, deci unul din aceste grade este 1, iar celălalt 0. Dacă $\text{grad}_{X_1}(f) = 1$, atunci, cum $a \in I$, rezultă că $\text{grad}_{X_1}(a) \geq 1$, contradicţie. Dacă $\text{grad}_{X_1}(f) = 0$ şi $\text{grad}_{X_1}(g) = 1$, avem că $f \in R[X_2, \ldots, X_n]$ şi $g = P_0 + P_1X_1$, $P_0, P_1 \in R[X_2, \ldots, X_n]$. Rezultă $P_0f = 0$ şi $P_1f = 1$, de unde $P_0 = 0$ şi (constatând că P_1 şi f au gradul 0 în raport cu toate nedeterminatele) $P_1, f \in U(R)$. Dar $f \in U(R)$ conduce la $1 \in I$, deci există $F, G \in A$ astfel încât $1 = aF + X_1G$. Făcând $X_1 = 0$ în această relaţie, obţinem $a \in U(R)$, contradicţie. Prin urmare, pentru ca A să fie principal, este necesar ca R să fie corp.
Presupunând că $n \geq 2$, considerăm $A = R[X_n][X_1, \ldots, X_{n-1}]$. Cum $R[X_n]$ nu este corp, A nu este inel principal conform cazului deja discutat, contradicţie. Rămâne aşadar că $n = 1$.
„⇐": Dacă R este corp şi $n = 1$, se ştie că A este inel euclidian, deci şi principal.

24. (i) "$\subseteq$" Fie $x \in P$. Există $\alpha = s + ti\sqrt{3}$ şi $\beta = u + vi\sqrt{3}$ astfel încât $x = 2\alpha + (1 + i\sqrt{3})\beta$. După efectuarea calculelor, se obţine $x = 2s + u - 3v + (2t + u + v)i\sqrt{3}$. Dacă punem $a = 2s + u - 3v$ şi $b = 2t + u + v$, avem $a, b \in \mathbb{Z}$ şi $2|2s - 2t - 4v = a - b$.
"$\supseteq$" Dacă $x \in R$ se scrie sub forma $a + bi\sqrt{3}$ cu $a, b \in \mathbb{Z}$ de aceeaşi paritate, atunci $x = 2 \cdot \frac{a-b}{2} + b(1 + i\sqrt{3}) \in P$.
(ii) Conform problemei 15 din Capitolul 5, $R \simeq \mathbb{Z}[X]/(X^2 + 3)$ iar prin acest izomorfism lui $i\sqrt{3}$ îi corespunde $\widehat{X}$, unde prin $\hat{f}$ notăm clasa lui $f \in \mathbb{Z}[X]$ modulo idealul $(X^2 + 3)$. Prin urmare,

$$\frac{R}{P} \simeq \frac{\mathbb{Z}[X]/(X^2 + 3)}{(2, X + 1)}.$$

Cum în $\mathbb{Z}[X]$ avem $(X^2 + 3) \subset (2, X + 1)$, obţinem

$$\frac{R}{P} \simeq \frac{\mathbb{Z}[X]/(X^2 + 3)}{(2, X + 1)/(X^2 + 3)}.$$

Aplicând de două ori teorema a III-a de izomorfism pentru inele deducem

$$\frac{R}{P} \simeq \frac{\mathbb{Z}[X]}{(2, X+1)} \simeq \frac{\mathbb{Z}[X]/(2)}{(2, X+1)/(2)} \overset{(*)}{\simeq} \frac{\mathbb{Z}[X]/2\mathbb{Z}[X]}{(0, X+1)} \overset{(**)}{\simeq} \frac{\mathbb{Z}_2[X]}{(X+1)} \overset{(***)}{\simeq} \mathbb{Z}_2,$$

unde izomorfismele $(*)$ şi $(**)$ sunt consecinţe ale problemei 14 din Capitolul 5, iar $(***)$ rezultă din problema 13, Capitolul 5. În consecinţă, R/P este inel integru (chiar corp), deci P este ideal prim (chiar maximal).
Să presupunem acum că P ar fi ideal principal şi fie x un generator al său. Atunci $x|_R 2$, deci $N(x)|_{\mathbb{Z}} 4$. Dar $N(x) \neq 1$, altfel ar rezulta că $x \in U(R)$, deci $P = R$; acest lucru este însă imposibil, întrucât, conform punctului (i), 1 nu este de forma necesară pentru a fi element al lui P. $N(x)$ nu poate fi nici 2, deoarece R nu conţine elemente de normă 2. Rămâne că $N(x) = 4$. Cum avem $x|_R 2$, $x|_R 1 + i\sqrt{3}$ şi $N(x) = 4 = N(2) = N(1 + i\sqrt{3})$, deducem, conform problemei 3(iii), că $x \sim_R 2$ şi $x \sim_R 1 + i\sqrt{3}$. De aici rezultă însă că $2 \sim_R 1 + i\sqrt{3}$, deci $2|_R 1 + i\sqrt{3}$, contradicţie. Rămâne aşadar că P nu este ideal principal.
(iii) Să presupunem că idealul $PR_P = \{\frac{a}{s} \mid a \in P, s \in R \setminus P\}$ al lui R_P (vezi problema 50(iii) din Capitolul 5) ar fi principal şi fie $\frac{x}{s}$ un generator al său. Cum s este inversabil în R_P, putem înlocui acest generator cu $\frac{x}{1} = \frac{s}{1}\frac{x}{s} \sim \frac{x}{s}$. Să notăm $x = a + bi\sqrt{3}$, unde $a, b \in \mathbb{Z}$ au aceeaşi paritate. Cum 2 şi $1 + i\sqrt{3}$ sunt în PR_P, rezultă că există $c, d, e, f, s, t, u, v \in \mathbb{Z}$ astfel încât

$$2 = \frac{c + di\sqrt{3}}{s + ti\sqrt{3}}(a + bi\sqrt{3}),\ 1 + i\sqrt{3} = \frac{e + fi\sqrt{3}}{u + vi\sqrt{3}}(a + bi\sqrt{3}),$$

unde c, d au aceeaşi paritate, e, f au aceeaşi paritate, s, t au parităţi diferite, u, v au parităţi diferite. Dacă a şi b ar fi pare, cum din a doua relaţie de mai sus rezultă că $u + v = af + be$, ar rezulta că $u + v$ e par, contradicţie. Trebuie deci ca a şi b să fie impare. Cum relaţia $2 = \frac{c+di\sqrt{3}}{s+ti\sqrt{3}}(a + bi\sqrt{3})$ conduce la $ac - 3bd = 2s$ şi $ad + bc = 2t$, c şi d trebuie să fie impare (altfel, din cele două relaţii anterioare am obţine că s şi t au aceeaşi paritate, absurd). Tot din relaţia $2 = \frac{c+di\sqrt{3}}{s+ti\sqrt{3}}(a + bi\sqrt{3})$ obţinem prin trecere la norme $4(s^2 + 3t^2) = (a^2 + 3b^2)(c^2 + 3d^2)$. Cum $a^2 + 3b^2 \equiv c^2 + 3d^2 \equiv 0 \pmod 4$, deducem că $s^2 + 3t^2$ e divizibil prin 4, ceea ce (ţinând cont că s şi t au parităţi diferite) este imposibil.
Rămâne aşadar că PR_P nu este ideal principal în R_P. În consecinţă, R_P nu este inel principal.
(iv) Presupunem că R_P admite cel puţin un element prim, fie el π. Cum R_P

e un inel local (vezi problema 50 din Capitolul 5) iar π nu este inversabil, rezultă că $\pi \in PR_P$ (vezi problema 29 din Capitolul 4). Făcând eventual uz de o asociere în divizibilitate în inelul R_P, putem considera că $\pi \in P$; notăm $\pi = a + bi\sqrt{3}$ cu $a, b \in \mathbb{Z}$ de aceeaşi paritate.
Dacă a şi b sunt pare, atunci 2 divide π în R, deci şi în R_P. Rezultă că $\pi = 2x$, cu $x \in R_P$, şi singura variantă pentru ca π să fie prim ar fi $\pi \sim_{R_P} 2$.
Dacă a şi b sunt impare şi dau acelaşi rest modulo 4, atunci $\pi = a + bi\sqrt{3} = (1 + i\sqrt{3})(\frac{a+3b}{4} + \frac{b-a}{4}i\sqrt{3})$. Prin urmare, $1 + i\sqrt{3}$ divide π în R, deci şi în R_P. Rezultă că $\pi = (1 + i\sqrt{3})x$, cu $x \in R_P$, şi singura variantă pentru ca π să fie prim ar fi $\pi \sim_{R_P} 1 + i\sqrt{3}$.
În mod similar se constată că, în situaţia în care a şi b sunt impare şi dau resturi diferite modulo 4, singura variantă pentru ca π să fie prim ar fi $\pi \sim_{R_P} 1 - i\sqrt{3}$.
Pe de altă parte, cum $2 \cdot 2 = 4 = (1 + i\sqrt{3})(1 - i\sqrt{3})$, dacă 2 ar fi prim în R_P, atunci el ar trebui să dividă pe $1 + i\sqrt{3}$ (şi atunci ar exista $c, d \in \mathbb{Z}$ de aceeaşi paritate şi $s, t \in \mathbb{Z}$ de parităţi diferite astfel ca $2 \cdot \frac{c+di\sqrt{3}}{s+ti\sqrt{3}} = 1 + i\sqrt{3}$, de unde $s + t = 2d$, contradicţie) sau pe $1 - i\sqrt{3}$ (şi atunci ar exista $c, d \in \mathbb{Z}$ de aceeaşi paritate şi $s, t \in \mathbb{Z}$ de parităţi diferite astfel ca $2 \cdot \frac{c+di\sqrt{3}}{s+ti\sqrt{3}} = 1 - i\sqrt{3}$, de unde $t - s = 2d$, contradicţie). Rămâne că 2 nu este prim în R_P, deci varianta $\pi \sim_{R_P} 2$ este contradictorie.
În mod similar se arată că nici unul dintre elementele $1 + i\sqrt{3}$ şi $1 - i\sqrt{3}$ nu este prim în R_P. Prin urmare, presupunerea că există elemente prime în R_P este contradictorie.
Rămâne că inelul R_P nu are nici un element prim.

25. Fie I un ideal al lui R. Dacă $I = (0)$, atunci I este generat de 0, deci este ideal principal. Dacă $I \neq (0)$, fie $y \in I \setminus \{0\}$ astfel încât $\varphi(y) = \min\{\varphi(z) | z \in I \setminus \{0\}\}$. Mulţimea $\mathbb{N}$ fiind bine ordonată, minimul de mai sus există şi este număr natural nenul. Fie x un element arbitrar nenul al lui I. Să presupunem că $y \nmid x$. Conform proprietăţii (ii) rezultă că există $u, v \in R$ astfel încât $0 < \varphi(xu - yv) < \varphi(y)$. Deoarece I este ideal, $xu - yv \in I$. În plus, $xu - yv \neq 0$ conform proprietăţii (i) şi inegalităţii $\varphi(xu - yv) > 0$. Contrazicem însă în acest mod minimalitatea lui $\varphi(y)$. Rămâne deci că $y \mid x$. Cum y a fost luat arbitrar în I, deducem că $I \subset Ry$; incluziunea $Ry \subset I$ este evidentă. Am arătat aşadar că $I = Ry$. Prin urmare, R este inel principal.

26. Pentru a demonstra că inelele din enunţ sunt principale, vom aplica criteriul din problema 25.

Notăm $R = \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ şi $N : R \to \mathbb{N}$, $N(z) = z\overline{z}$. Este evident că, pentru $a \in R$, $N(a) = 0$ dacă şi numai dacă $a = 0$. Fie acum $x, y \in R$, $y \neq 0$, $y \nmid x$. Conform problemei 25, demonstraţia se încheie dacă arătăm că există $u, v \in R$ astfel ca $0 < N(xu - yv) < N(y)$. Conform problemei 2, N se prelungeşte la funcţia multiplicativă $N : \mathbb{Q}[i\sqrt{19}] \to \mathbb{Q}$, $N(z) = z\overline{z}$. Relaţia anterioară se rescrie atunci $0 < N(\frac{x}{y}u - v) < 1$. Prin urmare, este suficient să demonstrăm că pentru orice $z \in \mathbb{Q}[i\sqrt{19}] \setminus R$ există $u, v \in R$ astfel încât $N(zu - v) \in (0, 1)$.

Fie deci $z \in \mathbb{Q}[i\sqrt{19}] \setminus R$. Există $a, b \in \mathbb{Z}$ şi $c \in \mathbb{N}$ astfel încât $z = \frac{a+bi\sqrt{19}}{c}$. Cum $z \notin R$, avem $c \geq 2$. Simplificând eventual prin (a, b, c), putem presupune că $(a, b, c) = 1$. Există atunci $\alpha, \beta, \delta \in \mathbb{Z}$ astfel ca $a\beta + b\alpha - c\delta = 1$. Din teorema împărţirii cu rest deducem existenţa întregilor γ şi r cu proprietăţile $a\alpha - 19b\beta = c\gamma + r$ şi $|r| \leq \frac{c}{2}$.

Dacă $c \geq 6$, alegem $u = \alpha + \beta i\sqrt{19}$ şi $v = \gamma + \delta i\sqrt{19}$. Obţinem $zu - v = \frac{r+i\sqrt{19}}{c}$, de unde $N(zu - v) = \frac{r^2+19}{c^2} \leq \frac{1}{4} + \frac{19}{c^2} \leq \frac{7}{9} < 1$. Pe de altă parte, $N(zu - v) = \frac{r^2+19}{c^2} \geq \frac{19}{c^2} > 0$.

Dacă $c = 5$, facem aceleaşi alegeri, constatând însă că de această dată $|r| \leq 2$. Prin urmare, $0 < \frac{r^2+19}{5^2} \leq \frac{23}{25} < 1$, deci $N(zu - v) \in (0, 1)$.

Dacă $c = 4$, observăm că a şi b nu pot fi simultan pare. Avem prin urmare de studiat următoarele două cazuri:

1. Dacă a şi b sunt de parităţi diferite, constatăm că $a^2 + 19b^2 \equiv s \pmod 4$, $s \in \{1, 3\}$. Scriem $a^2 + 19b^2 = 4q + s$ şi alegem $u = a - bi\sqrt{19}$ şi $v = q$. Rezultă $zu - v = \frac{s}{4}$, deci $N(zu - v) \in (0, 1)$.

2. Dacă a şi b sunt impare, atunci $a^2 + 19b^2 \equiv 4 \pmod 8$. Scriem $a^2 + 19b^2 = 8q + 4$ şi alegem $u = \frac{a-bi\sqrt{19}}{2}$ şi $v = q$. Rezultă $zu - v = \frac{1}{2}$, deci $N(zu - v) = \frac{1}{4} \in (0, 1)$.

Dacă $c = 3$, să presupunem că $3|a^2 + 19b^2$. Dacă 3 divide unul dintre numerele a şi b, rezultă că îl divide şi pe celălalt, contradicţie cu $(a, b, c) = 1$. Prin urmare, $3 \nmid a$ şi $3 \nmid b$. De aici obţinem însă $a^2 + 19b^2 \equiv 2 \pmod 3$, contradicţie. Rămâne aşadar că $3 \nmid a^2 + 19b^2$. Scriem $a^2 + 19b^2 = 3q + r$, $r \in \{1, 2\}$ şi alegem $u = a - bi\sqrt{19}$ şi $v = q$. Rezultă $zu - v = \frac{r}{3}$, deci $N(zu - v) \in (0, 1)$.

Dacă $c = 2$, atunci numerele a şi b trebuie să aibă parităţi diferite (altfel am avea $z \in R$). Atunci $a^2 + 19b^2 \equiv 1 \pmod 4$. Scriem $a^2 + 19b^2 = 4q + 1$ şi

alegem $u = a - bi\sqrt{19}$ şi $v = q$. Rezultă $zu - v = \frac{1}{2}$, deci $N(zu - v) = \frac{1}{4} \in (0, 1)$.

Notăm $R = \mathbb{Z}\left[\frac{1+i\sqrt{43}}{2}\right]$ şi $N : R \to \mathbb{N}$, $N(z) = z\overline{z}$. Este evident că, pentru $a \in R$, $N(a) = 0$ dacă şi numai dacă $a = 0$; Fie acum $x, y \in R$, $y \neq 0$, $y \nmid x$. Conform problemei 25, demonstraţia se încheie dacă arătăm că există $u, v \in R$ astfel ca $0 < N(xu - yv) < N(y)$. Conform problemei 2, N se prelungeşte la funcţia multiplicativă $N : \mathbb{Q}[i\sqrt{43}] \to \mathbb{Q}$, $N(z) = z\overline{z}$. Relaţia anterioară se rescrie atunci $0 < N(\frac{x}{y}u - v) < 1$. Prin urmare, este suficient să demonstrăm că pentru orice $z \in \mathbb{Q}[i\sqrt{43}] \setminus R$ există $u, v \in R$ astfel încât $N(zu - v) \in (0, 1)$.

Fie deci $z \in \mathbb{Q}[i\sqrt{43}] \setminus R$. Există $a, b \in \mathbb{Z}$ şi $c \in \mathbb{N}$ astfel încât $z = \frac{a+bi\sqrt{43}}{c}$. Cum $z \notin R$, avem $c \geq 2$. Simplificând eventual prin (a, b, c), putem presupune că $(a, b, c) = 1$. Există atunci $\alpha, \beta, \delta \in \mathbb{Z}$ astfel ca $a\beta + b\alpha - c\delta = 1$. Din teorema împărţirii cu rest deducem existenţa întregilor γ şi r cu proprietăţile $a\alpha - 43b\beta = c\gamma + r$ şi $|r| \leq \frac{c}{2}$.

Dacă $c \geq 8$, alegem $u = \alpha + \beta i\sqrt{43}$ şi $v = \gamma + \delta i\sqrt{43}$. Obţinem $zu - v = \frac{r+i\sqrt{43}}{c}$, de unde $N(zu - v) = \frac{r^2+43}{c^2} \leq \frac{1}{4} + \frac{43}{c^2} \leq \frac{59}{64} < 1$. Pe de altă parte, $N(zu - v) = \frac{r^2+43}{c^2} \geq \frac{43}{c^2} > 0$.

Dacă $c \in \{3, 5, 7\}$, să presupunem că $c | a^2 + 43b^2$. Dacă c divide unul dintre numerele a şi b, rezultă că îl divide şi pe celălalt, contradicţie cu $(a, b, c) = 1$. Prin urmare, $c \nmid a$ şi $c \nmid b$. De aici obţinem însă $\widehat{-43} = \left(\widehat{ab^{-1}}\right)^2$ în $\mathbb{Z}_c$. Cum $\widehat{-43}$ este egal cu $\widehat{6}$ în $\mathbb{Z}_7$, cu $\widehat{2}$ în $\mathbb{Z}_5$ respectiv cu $\widehat{2}$ în $\mathbb{Z}_3$, rezultă că el nu este pătratul nici unui element din $\mathbb{Z}_c$ şi am obţinut astfel o contradicţie.

Rămâne aşadar că $c \nmid a^2 + 43b^2$. Scriem $a^2 + 43b^2 = cq + r$, $r \in \{1, \ldots, c-1\}$ şi alegem $u = a - bi\sqrt{43}$ şi $v = q$. Rezultă $zu - v = \frac{r}{c}$, deci $N(zu - v) \in (0, 1)$.

Dacă $c = 6$, putem face aceleaşi alegeri de la cazul precedent. Faptul că $6 \nmid a^2 + 43b^2$ rezultă din relaţia $3 \nmid a^2 + 43b^2$ demonstrată în cazul anterior.

Dacă $c = 4$, observăm că a şi b nu pot fi simultan pare. Avem prin urmare de studiat următoarele două cazuri:

1. Dacă a şi b sunt de parităţi diferite, constatăm că $a^2 + 43b^2 \equiv s \pmod 4$, $s \in \{1, 3\}$. Scriem $a^2 + 43b^2 = 4q + s$ şi alegem $u = a - bi\sqrt{43}$ şi $v = q$. Rezultă $zu - v = \frac{s}{4}$, deci $N(zu - v) \in (0, 1)$.

2. Dacă a şi b sunt impare, atunci $a^2 + 43b^2 \equiv 4 \pmod 8$. Scriem $a^2 + 43b^2 = 8q + 4$ şi alegem $u = \frac{a-bi\sqrt{43}}{2}$ şi $v = q$. Rezultă $zu - v = \frac{1}{2}$, deci $N(zu - v) = \frac{1}{4} \in (0, 1)$.

Dacă $c = 2$, atunci numerele a şi b trebuie să aibă parităţi diferite (altfel am avea $z \in R$). Atunci $a^2 + 43b^2 \equiv 1 \pmod 4$. Scriem $a^2 + 43b^2 = 4q + 1$ şi alegem $u = a - bi\sqrt{43}$ şi $v = q$. Rezultă $zu - v = \frac{1}{2}$, deci $N(zu - v) = \frac{1}{4} \in (0, 1)$.

Notăm $R = \mathbb{Z}\left[\frac{1+i\sqrt{67}}{2}\right]$ şi $N : R \to \mathbb{N}$, $N(z) = z\overline{z}$. Este evident că, pentru $a \in R$, $N(a) = 0$ dacă şi numai dacă $a = 0$; Fie acum $x, y \in R$, $y \neq 0$, $y \nmid x$. Conform problemei 25, demonstraţia se încheie dacă arătăm că există $u, v \in R$ astfel ca $0 < N(xu - yv) < N(y)$. Conform problemei 2, N se prelungeşte la funcţia multiplicativă $N : \mathbb{Q}[i\sqrt{67}] \to \mathbb{Q}$, $N(z) = z\overline{z}$. Relaţia anterioară se rescrie atunci $0 < N(\frac{x}{y}u - v) < 1$. Prin urmare, este suficient să demonstrăm că pentru orice $z \in \mathbb{Q}[i\sqrt{67}] \setminus R$ există $u, v \in R$ astfel încât $N(zu - v) \in (0, 1)$.

Fie deci $z \in \mathbb{Q}[i\sqrt{67}] \setminus R$. Există $a, b \in \mathbb{Z}$ şi $c \in \mathbb{N}$ astfel încât $z = \frac{a+bi\sqrt{67}}{c}$. Cum $z \notin R$, avem $c \geq 2$. Simplificând eventual prin (a, b, c), putem presupune că $(a, b, c) = 1$. Există atunci $\alpha, \beta, \delta \in \mathbb{Z}$ astfel ca $a\beta + b\alpha - c\delta = 1$. Din teorema împărţirii cu rest deducem existenţa întregilor γ şi r cu proprietăţile $a\alpha - 67b\beta = c\gamma + r$ şi $|r| \leq \frac{c}{2}$.

Dacă $c \geq 10$, alegem $u = \alpha + \beta i\sqrt{67}$ şi $v = \gamma + \delta i\sqrt{67}$. Obţinem $zu - v = \frac{r+i\sqrt{67}}{c}$, de unde $N(zu - v) = \frac{r^2+67}{c^2} \leq \frac{1}{4} + \frac{67}{c^2} \leq \frac{23}{25} < 1$. Pe de altă parte, $N(zu - v) = \frac{r^2+67}{c^2} \geq \frac{67}{c^2} > 0$.

Dacă $c \in \{9, 6, 3\}$, să presupunem că $3|a^2 + 67b^2$.

Dacă 3 divide unul dintre numerele a şi b, rezultă că îl divide şi pe celălalt, contradicţie cu $(a, b, c) = 1$. Prin urmare, $3 \nmid a$ şi $3 \nmid b$. De aici obţinem însă $a^2 + 67b^2 \equiv 2 \pmod 3$, contradicţie.

Rămâne aşadar că $3 \nmid a^2+67b^2$, de unde obţinem şi $6 \nmid a^2+67b^2$ şi $9 \nmid a^2+67b^2$. Putem deci scrie $a^2+67b^2 = cq+r$ cu $r \in \{1, \ldots, c-1\}$. Alegem $u = a-bi\sqrt{67}$ şi $v = q$. Rezultă $zu - v = \frac{r}{c}$, deci $N(zu - v) \in (0, 1)$.

Dacă $c = 8$, observăm că a şi b nu pot fi simultan pare (altfel am avea $2|(a, b, c) = 1$). Prin urmare, $a^2 + 67b^2$ este congruent cu $s \in \{1, 3, 4\}$ modulo 8. Scriem $a^2 + 67b^2 = 8q + s$ şi alegem $u = a - bi\sqrt{67}$ şi $v = q$. Obţinem $zu - v = \frac{s}{8}$, de unde $N(zu - v) \in [\frac{1}{8}, \frac{1}{4}] \subset (0, 1)$.

Dacă $c \in \{5, 7\}$, să presupunem că $c|a^2 + 67b^2$. Dacă c divide unul dintre numerele a şi b, rezultă că îl divide şi pe celălalt, contradicţie cu $(a, b, c) = 1$. Prin urmare, $c \nmid a$ şi $c \nmid b$; de aici obţinem însă $\widehat{-67} = \left(\widehat{ab^{-1}}\right)^2$ în $\mathbb{Z}_c$. Cum $\widehat{-67}$ este egal cu $\widehat{6}$ în $\mathbb{Z}_7$, respectiv cu $\widehat{3}$ în $\mathbb{Z}_5$, rezultă că el nu este pătratul nici unui element din $\mathbb{Z}_c$ şi am obţinut astfel o contradicţie.

Rămâne aşadar că $c \nmid a^2+67b^2$. Scriem $a^2+67b^2 = cq+r$, $r \in \{1,\ldots,c-1\}$ şi alegem $u = a-bi\sqrt{67}$ şi $v = q$. Rezultă $zu-v = \frac{r}{c}$, deci $N(zu-v) \in (0,1)$.
Dacă $c = 4$, observăm că a şi b nu pot fi simultan pare. Avem prin urmare de studiat următoarele două cazuri:
1. Dacă a şi b sunt de parităţi diferite, constatăm că $a^2+67b^2 \equiv s \pmod 4$, $s \in \{1,3\}$. Scriem $a^2+67b^2 = 4q+s$ şi alegem $u = a-bi\sqrt{67}$ şi $v = q$. Rezultă $zu-v = \frac{s}{4}$, deci $N(zu-v) \in (0,1)$.
2. Dacă a şi b sunt impare, atunci $a^2+67b^2 \equiv 4 \pmod 8$. Scriem $a^2+67b^2 = 8q+4$ şi alegem $u = \frac{a-bi\sqrt{67}}{2}$ şi $v = q$. Rezultă $zu-v = \frac{1}{2}$, deci $N(zu-v) = \frac{1}{4} \in (0,1)$.
Dacă $c = 2$, atunci numerele a şi b trebuie să aibă parităţi diferite (altfel am avea $z \in R$). Atunci $a^2+67b^2 \equiv 1 \pmod 4$. Scriem $a^2+67b^2 = 4q+1$ şi alegem $u = a-bi\sqrt{67}$ şi $v = q$. Rezultă $zu-v = \frac{1}{2}$, deci $N(zu-v) = \frac{1}{4} \in (0,1)$.

Notăm $R = \mathbb{Z}\left[\frac{1+i\sqrt{163}}{2}\right]$ şi $N : R \to \mathbb{N}$, $N(z) = z\overline{z}$. Este evident că, pentru $a \in R$, $N(a) = 0$ dacă şi numai dacă $a = 0$. Fie acum $x, y \in R$, $y \neq 0$, $y \nmid x$. Conform problemei 25, demonstraţia se încheie dacă arătăm că există $u, v \in R$ astfel ca $0 < N(xu-yv) < N(y)$. Conform problemei 2, N se prelungeşte la funcţia multiplicativă $N : \mathbb{Q}[i\sqrt{163}] \to \mathbb{Q}$, $N(z) = z\overline{z}$. Relaţia anterioară se rescrie atunci $0 < N(\frac{x}{y}u - v) < 1$. Prin urmare, este suficient să demonstrăm că pentru orice $z \in \mathbb{Q}[i\sqrt{163}] \setminus R$ există $u, v \in R$ astfel încât $N(zu-v) \in (0,1)$.
Fie deci $z \in \mathbb{Q}[i\sqrt{163}] \setminus R$. Există $a, b \in \mathbb{Z}$ şi $c \in \mathbb{N}$ astfel încât $z = \frac{a+bi\sqrt{163}}{c}$. Cum $z \notin R$, avem $c \geq 2$. Simplificând eventual prin (a,b,c), putem presupune că $(a,b,c) = 1$. Există atunci $\alpha, \beta, \delta \in \mathbb{Z}$ astfel ca $a\beta + b\alpha - c\delta = 1$. Din teorema împărţirii cu rest deducem existenţa întregilor γ şi r cu proprietăţile $a\alpha - 163b\beta = c\gamma + r$ şi $|r| \leq \frac{c}{2}$.
Dacă $c \geq 15$, alegem $u = \alpha + \beta i\sqrt{163}$ şi $v = \gamma + \delta i\sqrt{163}$. Obţinem $zu-v = \frac{r+i\sqrt{163}}{c}$, de unde $N(zu-v) = \frac{r^2+163}{c^2} \leq \frac{1}{4} + \frac{163}{c^2} \leq \frac{877}{900} < 1$. Pe de altă parte, $N(zu-v) = \frac{r^2+163}{c^2} \geq \frac{163}{c^2} > 0$.
Dacă $c \in \{5,7,11,13\}$, să presupunem că $c|a^2+163b^2$. Dacă c divide unul dintre numerele a şi b, rezultă că îl divide şi pe celălalt, contradicţie cu $(a,b,c) = 1$. Prin urmare, $c \nmid a$ şi $c \nmid b$. De aici obţinem însă $\widehat{-163} = \left(\widehat{ab^{-1}}\right)^2$ în $\mathbb{Z}_c$. Cum $\widehat{-163}$ este egal cu $\widehat{6}$ în $\mathbb{Z}_{13}$, cu $\widehat{2}$ în $\mathbb{Z}_{11}$, cu $\widehat{5}$ în $\mathbb{Z}_7$, respectiv cu $\widehat{2}$ în $\mathbb{Z}_5$, rezultă că el nu este pătratul nici unui element din $\mathbb{Z}_c$ şi am obţinut astfel o contradicţie.

Rămâne aşadar că $c \nmid a^2+163b^2$. Scriem $a^2+163b^2 = cq+r$, $r \in \{1,\ldots,c-1\}$ şi alegem $u = a-bi\sqrt{163}$ şi $v = q$. Rezultă $zu-v = \frac{r}{c}$, deci $N(zu-v) \in (0,1)$.
Dacă $c = 14$, din afirmaţia $7 \nmid a^2+163b^2$ demonstrată la cazul anterior rezultă $14 \nmid a^2+163b^2$. Scriem $a^2+163b^2 = 14q+r$, $r \in \{1,\ldots,13\}$ şi alegem $u = a-bi\sqrt{163}$ şi $v = q$. Rezultă $zu-v = \frac{r}{14}$, deci $N(zu-v) \in (0,1)$.
Dacă $c = 10$, din afirmaţia $5 \nmid a^2+163b^2$ demonstrată anterior rezultă $10 \nmid a^2+163b^2$. Scriem $a^2+163b^2 = 10q+r$, $r \in \{1,\ldots,9\}$ şi alegem $u = a-bi\sqrt{163}$ şi $v = q$. Rezultă $zu-v = \frac{r}{10}$, deci $N(zu-v) \in (0,1)$.
Dacă $c \in \{3,6,9,12\}$, să presupunem că $3|a^2+163b^2$.
Dacă 3 divide unul dintre numerele a şi b, rezultă că îl divide şi pe celălalt, contradicţie cu $(a,b,c) = 1$. Prin urmare, $3 \nmid a$ şi $3 \nmid b$. De aici obţinem însă $a^2+163b^2 \equiv 2 \pmod 3$, contradicţie.
Rămâne aşadar că $3 \nmid a^2+163b^2$, de unde obţinem şi relaţiile $6 \nmid a^2+163b^2$, $9 \nmid a^2+163b^2$ şi $12 \nmid a^2+163b^2$. Putem deci scrie $a^2+163b^2 = cq+r$ cu $r \in \{1,\ldots,c-1\}$. Alegem $u = a-bi\sqrt{163}$ şi $v = q$. Rezultă $zu-v = \frac{r}{c}$, deci $N(zu-v) \in (0,1)$.
Dacă $c = 8$, observăm că a şi b nu pot fi simultan pare (altfel am avea $2|(a,b,c) = 1$). Prin urmare, a^2+163b^2 aste congruent cu $s \in \{1,3,4\}$ modulo 8. Scriem $a^2+163b^2 = 8q+s$ şi alegem $u = a-bi\sqrt{163}$ şi $v = q$. Obţinem $zu-v = \frac{s}{8}$, de unde $N(zu-v) \in [\frac{1}{8},\frac{1}{4}] \subset (0,1)$.
Dacă $c = 4$, observăm că a şi b nu pot fi simultan pare. Avem prin urmare de studiat următoarele două cazuri:
1. Dacă a şi b sunt de parităţi diferite, constatăm că $a^2+163b^2 \equiv s \pmod 4$, $s \in \{1,3\}$. Scriem $a^2+163b^2 = 4q+s$ şi alegem $u = a-bi\sqrt{163}$ şi $v = q$. Rezultă $zu-v = \frac{s}{4}$, deci $N(zu-v) \in (0,1)$.
2. Dacă a şi b sunt impare, atunci $a^2+163b^2 \equiv 4 \pmod 8$. Scriem $a^2+163b^2 = 8q+4$ şi alegem $u = \frac{a-bi\sqrt{163}}{2}$ şi $v = q$. Rezultă $zu-v = \frac{1}{2}$, deci $N(zu-v) = \frac{1}{4} \in (0,1)$.
Dacă $c = 2$, atunci numerele a şi b trebuie să aibă parităţi diferite (altfel am avea $z \in R$). Atunci $a^2+163b^2 \equiv 1 \pmod 4$. Scriem $a^2+163b^2 = 4q+1$ şi alegem $u = a-bi\sqrt{163}$ şi $v = q$. Rezultă $zu-v = \frac{1}{2}$, deci $N(zu-v) = \frac{1}{4} \in (0,1)$.
Faptul că inelele din enunţ nu sunt euclidiene rezultă din problema 18.

Observaţie. În anul 1952, K. Heegner a arătat că singurele inele principale de forma $\mathbb{Z}[i\sqrt{d}]$, $d \in \mathbb{N}$ liber de pătrate, sunt cele corespunzătoare valorilor $d \in \{1,2\}$ şi că singurele inele principale de forma $\mathbb{Z}\left[\frac{1+i\sqrt{d}}{2}\right]$, $d \in \mathbb{N}$ de forma $4k+3$ şi liber de pătrate, sunt cele corespunzătoare valorilor

$d \in \{3, 7, 11, 19, 43, 67, 163\}$.

27. Notăm $A = R[[X]]$ şi definim $u : R[[X]] \to R$ prin $u(f)$ =termenul liber al lui f. Este clar că u este morfism surjectiv de inele. Conform problemei 19, este suficient să aratăm că orice ideal prim nenul al lui A conţine un element prim.
Fie P un ideal prim nenul al lui A. X fiind element prim în A, afirmaţia e clară dacă $X \in P$. Dacă $X \notin P$ să notăm cu Q idealul $u(P)$ al lui R. Cum R este inel principal, există $a \in R$ astfel încât $Q = Ra$. Cum u e surjectiv există $f \in P$ astfel încât $a = u(f)$. Să notăm $f = a + a_1X + a_2X^2 + \cdots$. Cum $f \in P$, $Af \subset P$. Fie acum $g = b_0 + b_1X + \cdots \in P$. Atunci $b_0 = u(g) \in Q$, deci există $c_0 \in R$ astfel încât $b_0 = c_0a$. În concluzie, $g - c_0f$ nu are termen liber şi prin urmare există $g_1 \in A$ astfel încât $g - c_0f = Xg_1$. Cum $g, c_0f \in P$, rezultă $Xg_1 \in P$. Dar $X \notin P$, deci $g_1 \in P$.
Construim inductiv şirurile $(g_n)_{n\geq 1}$, $g_n \in P$ şi $(c_n)_{n\geq 0}$, $c_n \in A$, astfel: g_1 şi c_0 sunt cele de mai sus. Presupunem construiţi $c_0, c_1, \ldots, c_{k-1}$ şi g_k astfel încât $g = (c_0 + c_1X + \cdots + c_{k-1}X^{k-1})f + X^kg_k$. Atunci există $c_k \in R$ astfel încât $u(g_k) = c_ka$. Deci $g_k - c_kf$ nu are termen liber. Definim g_{k+1} astfel încât $g_k - c_kf = Xg_{k+1}$; cum $g_k, c_kf \in P$, obţinem $Xg_{k+1} \in P$; dar $X \notin P$, deci $g_{k+1} \in P$. În plus, $g = (c_0 + c_1X + \cdots + c_{k-1}X^{k-1})f + X^k(c_kf + Xg_{k+1}) = (c_0 + \cdots + c_kX^k)f + X^{k+1}g_{k+1}$.
Dacă notăm acum $h = c_0 + c_1X + c_2X^2 + \cdots \in A$, atunci g şi hf vor avea aceiaşi coeficienţi pentru $1, X, X^2, \ldots, X^k$, pentru orice $k \in \mathbb{N}$ şi prin urmare $g = hf$.
În concluzie, $P = Af$. Cum P este ideal prim, rezultă că f este element prim şi demonstaţia este încheiată.

28. Vom nota clasele elementelor X, Y şi Z modulo $(X^r + Y^s + Z^t)$ cu x, y, respectiv z.
(i) Dacă t este impar, considerăm morfismul $\varphi : k[X, Y, Z] \to k[X, Y, Z]$, $\varphi(f) = f(X, Y, -Z)$, a cărui existenţă rezultă din proprietatea de universalitate a inelelor de polinoame. Este evident că $\varphi \circ \varphi = 1_{k[X,Y,Z]}$, deci φ este izomorfism. Dar $\varphi(X^r + Y^s - Z^t) = X^r + Y^s + Z^t$, iar polinomul din membrul drept este ireductibil conform problemei 46. Prin urmare, $X^r + Y^s - Z^t$ este de asemenea ireductibil.
Dacă t este par, cum $t \equiv 1 \pmod{rs}$, vom avea r şi s impare. Reluăm atunci raţionamentul anterior folosind $\psi : k[X, Y, Z] \to k[X, Y, Z]$, $\psi(f) = f(-X, -Y, Z)$ şi ajungem din nou la concluzia că polinomul $X^r + Y^s - Z^t$

este ireductibil.
Cum $k[X,Y,Z]$ este inel factorial, elementul ireductibil $X^r+Y^s-Z^t$ este prim, deci $(X^r+Y^s-Z^t)$ este ideal prim. De aici rezultă că R este domeniu de integritate.
Notăm $w=\frac{1}{z}\in Q(R)$. Atunci, $z=x^rw^{t-1}+y^sw^{t-1}$, deci $z\in k[x,y,w]$, de unde rezultă $R[w]\subset k[x,y,w]$. Cum $t\equiv 1 \pmod{rs}$, există $\alpha\in\mathbb{N}$ astfel încât $t=\alpha rs+1$. Considerăm în $R[w]$ elementele $u=w^{\alpha s}x$ şi $v=w^{\alpha r}y$. Atunci $u^r+v^s=w^{\alpha rs}(x^r+y^s)=z$, de unde $(u^r+v^s)^{-1}=w$. Deducem incluziunea $k[u,v,(u^r+v^s)^{-1}]\subset R[w]$. Pe de altă parte, $x=uz^{\alpha s}=u(u^r+v^s)^{\alpha s}\in k[u,v,(u^r+v^s)^{-1}]$, $y=vz^{\alpha r}=v(u^r+v^s)^{\alpha r}\in k[u,v,(u^r+v^s)^{-1}]$, iar $w=(u^r+v^s)^{-1}\in k[u,v,(u^r+v^s)^{-1}]$. Obţinem şi incluziunea $R[w]\subset k[x,y,w]\subset k[u,v,(u^r+v^s)^{-1}]$, deci $R[w]=k[u,v,(u^r+v^s)^{-1}]$.
Fie $P=\sum_{i,j}a_{ij}U^iV^j\in k[U,V]$. Să presupunem că are loc egalitatea $P(u,v)=0$, adică $P(\frac{x}{z^{\alpha s}},\frac{y}{z^{\alpha r}})=0$. Aducem la acelaşi numitor şi obţinem o relaţie de tipul $\sum_{i,j}a_{ij}x^iy^jz^{n-\alpha(si+rj)}=0$, ceea ce înseamnă că există $F\in k[X,Y,Z]$ astfel ca $\sum_{i,j}a_{ij}X^iY^jZ^{n-\alpha(si+rj)}=(X^r+Y^s-Z^t)F$. Conform proprietăţii de universalitate a inelelor de polinoame, există un morfism de inele $\chi: k[X,Y,Z]\to k[C,D,Z]$, $\chi(f)=f(C^{\alpha s},D^{\alpha r},Z)$. Aplicând χ în relaţia de mai sus, obţinem $\sum_{i,j}a_{ij}C^{\alpha is}D^{\alpha jr}Z^{n-\alpha(si+rj)}=(C^{t-1}+D^{t-1}-Z^t)\chi(F)$.
Cum polinomul din membrul stâng al relaţiei anterioare este omogen, iar $C^{t-1}+D^{t-1}-Z^t$ are două componente omogene, rezultă că $\chi(F)=0$. Dar χ este în mod evident injectiv, de unde $F=0$, ceea ce conduce la $\sum_{i,j}a_{ij}X^iY^jZ^{n-\alpha(si+rj)}=0$, de unde $P=0$. În consecinţă, morfismul $\phi: k[U,V]\to k[u,v]$, $\phi(P)=P(u,v)$, are nucleul nul, deci este injectiv. Cum ϕ este în mod evident surjectiv, avem $k[u,v]\simeq k[U,V]$. Prin urmare, $k[u,v]$ este inel factorial.
Datorită izomorfismului evident $k[u,v,(u^r+v^s)^{-1}]\simeq S^{-1}k[u,v]$, unde S este sistemul multiplicativ al lui $k[u,v]$ format din toate puterile lui u^r+v^s, obţinem, conform problemei 20, că şi inelul $k[u,v,(u^r+v^s)^{-1}]$ este factorial. Am arătat însă mai sus că $R[w]\simeq k[u,v,(u^r+v^s)^{-1}]$, deci $R[w]$ este de asemenea inel factorial.
Folosind problema 23 din capitolul 4 şi teorema a III-a de izomorfism pentru

inele, obţinem izomorfismele

$$\frac{R}{zR} \simeq \frac{\frac{k[X,Y,Z]}{(X^r+Y^s-Z^t)}}{\frac{(Z,X^r+Y^s-Z^t)}{(X^r+Y^s-Z^t)}} \simeq \frac{k[X,Y,Z]}{(X^r+Y^s,Z)} \simeq \frac{\frac{k[X,Y,Z]}{(Z)}}{\frac{(X^r+Y^s,Z)}{(Z)}} \simeq \frac{k[X,Y]}{(X^r+Y^s)}.$$

Conform problemei 46, polinomul $X^r + Y^s \in k[X,Y]$ este ireductibil. prin urmare, $\frac{R}{zR} \simeq \frac{k[X,Y]}{(X^r+Y^s)}$ este domeniu, deci z este element prim al lui R. Cum $R[w] = R[\frac{1}{z}]$, deducem izomorfismul $R[w] \simeq T^{-1}R$, unde T este sistemul multiplicativ al lui R format din toate puterile lui z. Observăm că T este generat de elementul prim z. Pe de altă parte, inelul $k[X,Y,Z]$ fiind noetherian, obţinem (vezi problema 24 din capitolul 4) că R este şi el noetherian, deci orice lanţ ascendent de ideale principale este staţionar. Conform criteriului lui Nagata (vezi problema 21), R este inel factorial.

(ii) Considerăm în R sistemul multiplicativ $S = \{1, x, x^2 \ldots\}$. Notăm $S' = \{a_0 + a_1X + \ldots \in R[[X]] \mid a_0 \in S\}$. S' este în mod clar un sistem multiplicativ al lui R. Notăm $A = R[[X]]$, $B = S^{-1}A$, $B' = (S')^{-1}A$ şi $\widehat{B} = (S^{-1}R)[[X]]$. Incluzilunile $A \subset B \subset B'$ sunt evidente. Pe de altă parte, dacă $a_0 + a_1X + \ldots \in S'$, atunci există $n_0 \in \mathbb{N}$ astfel încât $a_0 = x^{n_0}$. Dacă considerăm sistemul de relaţii $c_0^{n_0}b_0 = 1$ şi $\sum\limits_{i+j=n} a_ib_j = 0$ pentru fiecare $n \in \mathbb{N}^*$, atunci $b_0 = \frac{1}{c_0^{n_0}}$, iar dacă presupunem pentru $n \geq 1$ că toţi b_j, $j \in \{0, 1, \ldots, m-1\}$, sunt de forma $\frac{\alpha_j}{c_0^{nj}}$, din relaţia $\sum\limits_{i+j=m} a_ib_j = 0$ deducem $b_m = -\sum\limits_{\substack{i+j=m \\ j \neq m}} \frac{a_i\alpha_j}{c_0^{nj}}$. Aducând fracţile din suma din membrul drept la acelaşi numitor rezultă că există $n_m \in N$şi $\alpha_m \in R$ aşa încât $b_m = \frac{\alpha_m}{C_0^{nm}}$. Am demonstrat deci prin inducţie că există un şir $(b_n)_{n\in\mathbb{N}}$ de elemente din $S^{-1}R$ cu proprietatea că $(a_0 + a_1X + \cdots)(b_0 + b_1X + \cdots) = 1$. De aici rezultă, folosind proprietatea de universalitate a inelelor de fracţii, că există un morfism canonic ξ de inele de la B' la $\widehat{B}$. Cum A este un inel integru, sistemul multiplicativ S' este format numai din nondivizori ai lui zero, de unde rezultă imediat că morfismul ξ este injectiv. În cele ce urmează, vom identifica uneori pe B' cu subinelul $\xi(B')$ al lui $\widehat{B}$.

Considerăm acum seria formală $v = xy - z^{t-1}X \in R[X] \subset A \subset B \subset B' \subset \widehat{B}$.

Pasul I: Arătăm că elementul v nu este asociat în inelul $\widehat{B}$ cu nici o serie formală de tipul $y + a_1X + a_2X^2 + \cdots$ cu $a_i \in R$ pentru fiecare $i \in \mathbb{N}^*$.

Într-adevăr, să presupunem contrariul. Atunci putem scrie o relaţie de tipul

$(xy-z^{t-1}X)\left(\frac{c_0}{x^{n_0}}+\frac{c_1}{x^{n_1}}X+\cdots\right)=y+a_1X+a_2X^2+\cdots$, unde pentru fiecare $i\in\mathbb{N}$ $c_i\in R$ şi $n_i\in\mathbb{N}$. Rezultă $\frac{c_0}{x^{n_0}}=\frac{1}{x}$ şi $c_1yx^{1-n_1}-z^{t-1}x^{-1}=a_1\in R$, de unde $c_1y-x^{n_1-2}z^{t-1}\in Rx^{n_1-1}$. Deducem de aici $c_1y\in Rx^{n_1-2}$, deci există $d\in R$ astfel încât $c_1y=dx^{n_1-2}$. Folosind problema 23 din capitolul 4 şi teorema a III-a de izomorfism pentru inele, obţinem

$$\frac{R}{yR}\simeq\frac{k[X,Y,Z]}{(Y,X^r+Y^s-Z^t)}\simeq\frac{\frac{k[X,Y,Z]}{(Y)}}{\frac{(Y,X^r+Y^s-Z^t)}{(Y)}}\simeq\frac{k[X,Z]}{(X^r-Z^t)}.$$

Dacă t este impar, considerăm morfismul $\varphi:k[X,Z]\to k[X,Z]$, $\varphi(f)=f(X,-Z)$, a cărui existenţă rezultă din proprietatea de universalitate a inelelor de polinoame. Este evident că $\varphi\circ\varphi=1_{k[X,Z]}$, deci φ este izomorfism. Dar $\varphi(X^r-Z^t)=X^r+Z^t$, iar polinomul din membrul drept este ireductibil conform problemei 46. Prin urmare, X^r-Z^t este de asemenea ireductibil.
Dacă t este par, cum $(r,t)=1$, vom avea r impar. Reluăm atunci raţionamentul anterior folosind $\psi:k[X,Z]\to k[X,Z]$, $\psi(f)=f(-X,Z)$ şi ajungem din nou la concluzia că polinomul X^r-Z^t este ireductibil.
Cum $k[X,Z]$ este inel factorial, elementul ireductibil X^r-Z^t este prim, deci (X^r-Z^t) este ideal prim. De aici rezultă că $\frac{R}{yR}\simeq\frac{k[X,Z]}{(X^r-Z^t)}$ este domeniu de integritate, prin urmare yR este ideal prim al lui R. Cum $x\notin yR$, relaţia $dx^{n_1-2}\in Ry$ ne dă $d\in Ry$. Există deci $e\in R$ astfel ca $d=ey$. Înlocuind în $c_1y-x^{n_1-2}z^{t-1}\in Rx^{n_1-1}$, obţinem $eyx^{n_1-2}-x^{n_1-2}z^{t-1}\in Rx^{n_1-1}$, de unde $ey-z^{t-1}\in Rx$. Există deci $f\in R$ astfel ca $z^{t-1}=fx+ey$, de unde deducem că există $E,F\in R[X,Y,Z]$ astfel încât $Z^t-X^r-Y^s|Z^{t-1}-XF-YE$. Dând în această relaţie nedeterminatelor X şi Y valoarea 0, obţinem contradicţia $Z^t|Z^{t-1}E(0,0,Z)$ şi demonstraţia afirmaţiei pasului I este încheiată.
Pasul II: Demonstrăm că există un număr natural a şi o serie formală $v'=y^ax^{-1}+b_1x^{-2}X+\cdots+b_mX^{-m-1}X^m+\cdots\in\widehat{B}$, cu $b_i\in R$ pentru fiecare $i\in\mathbb{N}^*$, astfel încât $u=v'v\in R$.
În acest scop, trebuie să determinăm elementele $b_1,b_2,\ldots$ ale lui R astfel încât coeficienţii lui u să fie în R. În scrierea lui u avem termenul liber $y^{t+1}\in R$, coeficientul lui X egal cu $b_1yx^{-1}-z^{t-1}y^ax^{-1}$, iar pentru $l\geq 2$ coeficientul lui X^l egal cu $b_lyx^{-l}-b_{l-1}z^{t-1}x^{-l}$. Pentru ca aceşti coeficienţi să se afle în R, este necesar şi suficient ca $b_1y-z^{t-1}y^a\in Rx$ şi $b_ly-z^{t-1}b_{l-1}\in Rx^l$ pentru orice $l\geq 2$. Realizăm acum construcţia inductivă a şirului $(b_m)_{m\geq 1}$:
Alegem $b_1=z^{t-1}y^{a-1},b_2=z^{2(t-1)}y^{a-2},\ldots,b_{rt-1}=z^{(rt-1)(t-1)}y^{a-rt+1}$ şi numărul natural $a\geq rt$ şi constatăm că $b_1,\ldots,b_{rt-1}\in R$. Pentru alegerea lui b_{rt}, vom ţine cont că trebuie îndeplinită relaţia $b_{rt}y-z^{rt(t-1)}y^{a-rt+1}=b_{rt}y-z^{t-1}b_{rt-1}\in$

Rx^{rt}. Cum $z^t = x^r + y^s$, trebuie să avem $b_{rt}y - (x^r + y^s)^{r(t-1)}y^{a-rt+1} \in Rx^{rt}$. Dacă dezvoltăm $(x^r + y^s)^{r(t-1)}$ folosind binomul lui Newton, termenii în care x apare la puterea cel mult rt vor avea suma

$$\sum_{k=0}^{t} C_{n(t-1)}^{k} y^{s(r(t-1)-k)} x^{rk} = y^{s(rt-r-t)} f_1(x^r, y^s),$$

unde $f_1(U,V) = \sum\limits_{k=0}^{t} C_{n(t-1)}^{k} U^k V^{t-k} \in R[U,V]$ este evident un polinom omogen de grad t. Relaţia anterioară se scrie atunci $b_{rt}y - y^{s(rt-r-t)-rt+a+1} f_1(x^r, y^s) \in Rx^{rt}$ şi se vede că putem alege $b_{rt} = y^{rst-rs-rt-st+a} f_1(x^r, y^s)$. Cum $r, s \geq 2$ şi $r \neq s$, avem $t(rs - r - s) \geq t$. În plus, din $t \equiv 1 \pmod{rs}$ se obţine $t > rs$. În consecinţă, exponentul lui y din scrierea lui b_{rt} este mai mare decât a.
Să presupunem acum că am construit $b_1, b_2, \ldots, b_{(l-1)rt}$, $l \geq 2$, în aşa fel încât $b_{(l-1)rt} = y^{\varphi(l-1)} f_{l-1}(x^r, y^s)$, unde f_{l-1} este un polinom omogen de grad $(l-1)t$ cu coeficienţi în R, iar $\varphi(l-1)$ este un număr natural cu proprietatea $\varphi(l-1) \geq a \geq rt$. Pentru fiecare $j \in \{1, \ldots, rt-1\}$ alegem $b_{(l-1)rt+j} = z^{j(t-1)} y^{\varphi(l-1)-j} f_{l-1}(x^r, y^s)$ şi constatăm că aceste valori verifică relaţiile $b_{(l-1)rt+j} - z^{t-1} b_{(l-1)rt+j-1} \in Rx^{(l-1)rt+j}$. Pentru alegerea lui b_{lrt}, vom ţine cont că trebuie îndeplinită relaţia $b_{lrt}y - z^{t-1} b_{lrt-1} \in Rx^{lrt}$, adică $b_{lrt}y - z^{rt(t-1)} y^{\varphi(l-1)-rt+1} f_{l-1}(x^r, y^s) \in Rx^{lrt}$. Dar $z^t = x^r + y^s$, deci relaţia pe care dorim să o obţinem se rescrie $b_{lrt}y - (x^r + y^s)^{r(t-1)} y^{\varphi(l-1)-rt+1} f_{l-1}(x^r, y^s) \in Rx^{lrt}$. Expresia $(x^r + y^s)^{r(t-1)} f_{l-1}(x^r, y^s)$ este un polinom omogen de grad $r(t-1) + (l-1)t$ în x^r şi y^s. Termenii din această expresie în care x apare la putere cel mult lrt vor avea exponentul lui y^s cel puţin $r(t-1) + (l-1)t - lt$, deci suma lor va avea forma $y^{s(r(t-1)+(l-1)t-lt)} f_l(x^r, y^s)$, unde f_l este un polinom omogen de grad lt cu coeficienţii în R. În consecinţă, putem alege $b_{lrt} = y^{\varphi(l-1)+rst-rs-st-tr} f_l(x^r, y^s)$. S-a arătat mai sus că $rst - rs - st - tr > 0$, deci, dacă definim $\varphi(l) = \varphi(l-1) + rst - rs - st - tr$, avem $\varphi(l) \geq \varphi(l-1) \geq a$, ceea ce încheie pasul de inducţie şi demonstraţia afirmaţiei de la pasul II.
Pasul III: $v\widehat{B} \cap B' = vB'$.
„$\supset$": Relativ la morfismul ξ, avem $v\widehat{B} \cap B' = ((vB')^e)^c$ (vezi problema 22), deci $vB' \subset v\widehat{B} \cap B'$.
„$\subset$": Pentru $F \in B'$ şi $m, n \in \mathbb{N}$ avem relaţia $(F + (X)^m) \cap (F + (X)^n) = F + (X)^{\max\{m,n\}}$. Prin urmare, există o topologie τ pe B' în care pentru fiecare $F \in B'$ familia $(F + (X)^n)_{n \in \mathbb{N}}$ reprezintă un sistem fundamental de vecinătăţi.
Fie acum $F \in v\widehat{B} \cap B'$. Există atunci $G = \frac{a_0}{x^{n_0}} + \frac{a_1}{x^{n_1}} X + \cdots \in \widehat{B}$ aşa încât

$F = vG$. Pentru fiecare $m \in \mathbb{N}^*$ notăm $G_n = \frac{a_0}{x^{n_0}} + \cdots + \frac{a_m}{x^{n_m}} X^m$. Atunci $v(G - G_m) = X^{m-1} v(\frac{a_{m+1}}{x^{m+1}} + \frac{a_{m+2}}{x^{m+2}} X + \cdots)$. Cum $G_m \in B \subset B'$, rezultă că fiecare vG_m este în vB', deci $v(G - G_m) \in v\widehat{B} \cap B'$ pentru orice $m \in \mathbb{N}$. Observînd că pentru $F = \frac{f}{g} \in B'$ $X^\alpha|_{\widehat{B}} F \Leftrightarrow X^\alpha|_A f$, tragem concluzia că pentru orice $m \in \mathbb{N}$ avem $vG - vG_m \in X^{m+1}B'$. Cum în spaţiul topologic (B', τ) fiecare punct admite un sistem fundamental de vecinătăţi numărabil, din cele de mai sus rezultă că $v\widehat{B} \cap B'$ este conţinut în aderenţa $\overline{vB'}$ a lui vB' (în raport cu topologia τ).
Fie acum $F \in \overline{vB'}$. Atunci trebuie ca pentru orice $n \in \mathbb{N}$ să existe $F_n \in vB'$ aşa încât $F_n \in F + (X)^n$, altfel spus, $F \in vB' \cap (X)^n$ pentru fiecare $n \in \mathbb{N}$. Deducem că $\overline{vB'} \subset \bigcap_{n \in \mathbb{N}} (vB' + (X)^n)$.
Considerăm proiecţia canonică $\pi : B' \to \frac{B'}{vB'}$. Pentru $F \in B'$, vom nota $\pi(F) = \widetilde{F}$. Dacă $n \in \mathbb{N}$, $\pi^{-1}((\widetilde{X})^n) = \{F \in B' |$ există $G \in B'$ aşa încât $\widetilde{F} = \widetilde{X}^n \widetilde{G}\}$. Dar $\widetilde{F} = \widetilde{X}^n \widetilde{G} \Leftrightarrow F - X^n G \in vB' \Leftrightarrow F \in vB' + X^n G$. În concluzie, $\pi^{-1}((\widetilde{X})^n) = vB' + (X)^n$. Cum luarea preimaginii comută cu intersecţiile arbitrare, obţinem $\pi^{-1}(\bigcap_{n \in \mathbb{N}} (\widetilde{X})^n) = \bigcap_{n \in \mathbb{N}} (vB' + (X)^n)$. Notăm $I = \bigcap_{n \in \mathbb{N}} (\widetilde{X})^n$. Dacă $\widetilde{F} \in I$, atunci $\widetilde{F} \in (\widetilde{X})$, deci există $G \in B'$ astfel încât $\widetilde{F} = \widetilde{X}\widetilde{G}$. Fie $n \in \mathbb{N}^*$. Atunci există $F_n \in B'$ astfel ca $\widetilde{F} = \widetilde{X}^n \widetilde{F_n}$, de unde $XG - X^n F_n \in vB'$. Scriind $XG - X^n F_n = vH$, $H \in B'$, constatăm folosind o observaţie anterioară că X divide în A numărătorul lui H, de unde $X|_{B'} H$. Punînd $H = XH'$, $H' \in B'$, rezultă $G - X^{n-1} F_n = vH' \in vB'$, deci $\widetilde{G} = \widetilde{X}^{n-1} \widetilde{F_n}$. Am obţinut deci $\widetilde{G} \in I$. În consecinţă, $I \subset (X)I$. Incluziunea contrară fiind evidentă, obţinem $I = (X)I$.
Conform problemei 24 din capitolul 4, R este inel noetherian. Folosind problema 28 din capitolul 5, deducem că A este noetherian. Din problema 51 din capitolul 5 deducem că B' este noetherian, iar din problema 24 din capitolul 4 deducem că $\frac{B'}{vB'}$ este inel noetherian. Prin urmare, idealul I este finit generat. Să presupunem că $I = (\widetilde{F_1}, \ldots, \widetilde{F_k})$. Cum $I = (X)I$, există $G_{ij} \in B'$, $i, j \in \{1, \ldots, k\}$, astfel ca $\widetilde{F_i} = \widetilde{X}\widetilde{G_{i1}}\widetilde{F_1} + \cdots + \widetilde{X}\widetilde{G_{ik}}\widetilde{F_k}$ pentru fiecare $i = \overline{1, k}$. Rescriem aceste relaţii sub forma

$$\begin{aligned}
&(1 - \widetilde{X}\widetilde{G_{11}})\widetilde{F_1} - \widetilde{G_{12}}\widetilde{F_2} - \cdots - \widetilde{G_{1k}}\widetilde{F_k} = 0 \\
&-\widetilde{G_{21}}\widetilde{F_1} + (1 - \widetilde{X}\widetilde{G_{22}})\widetilde{F_2} - \cdots - \widetilde{G_{1k}}\widetilde{F_k} = 0 \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&-\widetilde{G_{k1}}\widetilde{F_1} - \widetilde{G_{k2}}\widetilde{F_2} - \cdots + (1 - \widetilde{X}\widetilde{G_{kk}})\widetilde{F_k} = 0
\end{aligned}$$

Considerăm aceste relaţii ca fiind un sistem de ecuaţii cu necunoscutele $\widetilde{F_1}, \ldots, \widetilde{F_k}$. Matricea acestui sistem este

$$M = \begin{pmatrix} (1 - \widetilde{X}\widetilde{G_{11}}) & -\widetilde{G_{12}} & \ldots & -\widetilde{G_{1k}} \\ -\widetilde{G_{21}} & (1 - \widetilde{X}\widetilde{G_{22}}) & \ldots & -\widetilde{G_{2k}} \\ \ldots & \ldots & \ldots & \ldots \\ -\widetilde{G_{k1}} & -\widetilde{G_{k2}} & \ldots & (1 - \widetilde{X}\widetilde{G_{kk}}) \end{pmatrix}$$

Să observăm că $\det M$ este de forma $1 + \widetilde{X}\widetilde{H}$ cu $H \in B'$. Dacă considerăm elementul $1 + XH \in B'$, scriem H sub formă de fracţie şi aducem la acelaşi numitor, constatăm că numărătorul obţinut este în S'. Prin urmare, $1 + XH \in U(B')$, de unde $\det M \in U(\frac{B'}{vB'})$. Scriind sistemul sub formă matriceală şi înmulţind cu adjuncta lui M, obţinem $(\det M) \cdot \widetilde{F_i} = 0$ pentru fiecare $i = \overline{1,k}$. De aici rezultă că toţi generatorii lui I sunt nuli, deci $I = (0)$. Rezultă $\bigcap\limits_{n \in \mathbb{N}} (vB' + (X)^n) = \pi^{-1}(I) = vB'$. Folosind şi relaţiile obţinute anterior, obţinem $v\widehat{B} \cap B' \subset vB'$ şi relaţia $v\widehat{B} \cap B' = vB'$ este demonstrată.

Pasul IV: Finalizare.

Presupunem că inelul A este factorial. Conform rezultatului de la pasul II, seria formală $u = v'v$ se poate scrie sub forma $u = y^{a+1} + a_1X + a_2X^2 + \cdots$ cu $a_i \in R$ pentru orice $i \in \mathbb{N}^*$. Fie $u = u_1u_2 \cdots u_m$ descompunerea lui u în factori primi în inelul A. Din faptul că yR este ideal prim al lui R (vezi pasul I) rezultă că y este element prim al lui R. Prin urmare, R fiind inel factorial, fiecare factor prim u_j al lui u are termenul liber egal cu o putere a lui y. Considerăm morfismul surjectiv de inele $\theta : A \to \frac{R}{yR}[[X]]$, $\theta(a_0 + a_1X + \cdots) = \overline{a_0} + \overline{a_1}X + \cdots$, şi constatăm că nucleul său este yA. Prin urmare, $A/yA \simeq \frac{R}{yR}[[X]]$, iar inelul din membrul drept este integru. Se obţine că yA este ideal prim al lui A, deci y este prim şi în inelul A. Cum $(x, y) = 1$, rezultă că nici un element u_j nu se divide în A cu nici un element din S'. Conform soluţiei problemei 20, elementele $u_j, j = \overline{1,m}$ sunt prime şi în B'. Cum $v' \in \widehat{B}$, obţinem că $u = vv' \in v\widehat{B}$. Dar $u \in A \subset B'$, deci $u \in v\widehat{B} \cap B' = vB'$ (ultima egalitate rezultând din pasul III). Putem atunci scrie $u = vv''$ cu $v'' \in B'$. Se obţine $v(v' - v'') = 0$, de unde, $\widehat{B}$ fiind domeniu, $v' = v'' \in B'$. Observăm că v este element ireductibil al lui B' (dacă $v = \frac{a_0 + a_1X + \cdots}{x^p + b_1X + \cdots} \cdot \frac{c_0 + c_1X + \cdots}{x^q + d_1X + \cdots}$, atunci $x^{p+q+1}y = a_0c_0$, de unde, ţinând cont de factorialitatea lui R, unul dintre elememntele a_0 şi c_0 este putere de x, iar factorul corespunzător este inversabil în B'). Din relaţia $vv' = u_1 \cdots u_m$ şi din factorialitatea lui B' rezultă că v este asociat în B' cu

unul dintre $u_1, \ldots, u_m$, fie el u_j. Dacă ţinem cont de aspectul lui u_j privit ca element al lui $\widehat{B}$, constatăm că v este asociat în B' cu o serie formală de tipul $y + a_1X + a_2X^2 + \cdots$ cu $a_i \in R$ pentru fiecare $i \in \mathbb{N}^*$, ceea ce contrazice pasul I şi încheie demonstraţia.

29. Notăm $R = \mathbb{Z}[i\sqrt{6}]$. Relaţia $-i\sqrt{6} \cdot i\sqrt{6} = 6 = 2 \cdot 3$ ne arată că $i\sqrt{6}|_R 2 \cdot 3$; este clar însă (vezi problema 1) că $i\sqrt{6}$ nu divide în R nici unul din aceşti factori. Prin urmare, $i\sqrt{6}$ nu este prim în R. Pe de altă parte, dacă $i\sqrt{6}$ ar fi reductibil în R, ar rezulta că se scrie sub forma ab cu $a, b \in R \setminus U(R)$. Trecând la norme, se obţine $6 = N(a)N(b)$, de unde $N(a) = 2$ şi $N(b) = 3$ (sau viceversa). Dar în R nu există elemente de normă 2 (şi nici de normă 3), contradicţie. Aşadar $i\sqrt{6}$ este ireductibil în R, dar nu este prim. De aici rezultă că R nu este inel factorial.

Notăm $R = \mathbb{Z}[\sqrt{10}]$. Relaţia $(\sqrt{10})^2 = 10 = 2 \cdot 5$ ne arată că $2|_R(\sqrt{10})^2$; este clar însă (vezi problema 1) că 2 nu divide în R pe $\sqrt{10}$. Prin urmare, 2 nu este prim în R. Pe de altă parte, dacă 2 ar fi reductibil în R, ar rezulta că se scrie sub forma ab cu $a, b \in R \setminus U(R)$. Trecând la norme, se obţine $4 = N(a)N(b)$, de unde $N(a) = N(b) = 2$. Cum însă niciun pătrat perfect nu se termină în 2 sau în 8, relaţia $|x^2 - 10y^2| = 2$ este imposibilă în numere întregi, prin urmare în R nu există elemente de normă 2, contradicţie. Aşadar, 2 este ireductibil în R, dar nu este prim. De aici rezultă că R nu este inel factorial.

Notăm $R = \mathbb{Z}[\sqrt{26}]$. Relaţia $(\sqrt{26} - 1)(\sqrt{26} + 1) = 25 = 5 \cdot 5$ ne arată că $5|_R(\sqrt{26} - 1)(\sqrt{26} + 1)$; este clar însă (vezi problema 1) că 5 nu divide în R nici unul din aceşti factori. Prin urmare, 5 nu este prim în R. Pe de altă parte, dacă 5 ar fi reductibil în R, ar rezulta că se scrie sub forma ab cu $a, b \in R \setminus U(R)$. Trecând la norme, se obţine $5 = N(a)N(b)$, de unde $N(a) = N(b) = 5$. Dar în R nu există elemente de normă 5 (deoarece în caz contrar ar trebui să existe numere întregi x, y aşa încât $|x^2 - 26y^2| = 5$, deci $x^2 \equiv \pm 5 \pmod{13}$, ceea ce ar însemna că unul dintre elementele $\widehat{5}$ şi $\widehat{8}$ este pătrat în $\mathbb{Z}_{13}$, absurd) şi ajungem astfel la o contradicţie. Prin urmare, 5 este ireductibil în R, dar nu este prim. De aici rezultă că R nu este inel factorial.

Notăm $R = K[X, Y, Z, T]/(XT - YZ)$ şi $x = \hat{X}$, $y = \hat{Y}$, $z = \hat{Z}$, $t = \hat{T}$. Avem că $R = K[x, y, z, t]$ şi $xt = yz$. Polinomul $XT - YZ \in K[X, Y, Z, T] \simeq K[Y, Z, T][X]$ este de gradul întâi şi primitiv, deci este ireductibil. Inelul $K[X, Y, Z, T]$ fiind factorial, $XT - YZ$ este chiar prim. Rezultă de aici că

idealul $(XT - YZ)$ este prim şi prin urmare R este inel integru.
Vom prezenta două soluţii pentru faptul că R nu este inel factorial.
Soluţia 1. Polinoamele din $K[X, Y]$ se scriu în mod unic ca sumă de polinoame omogene. Această proprietate se transmite şi inelului R. Într-adevăr, este clar că orice element din R se scrie ca sumă de polinoame omogene de x, y, z, t. În ceea ce priveşte unicitatea, este suficient să demonstrăm că dacă $f_0(x, y, z, t) + f_1(x, y, z, t) + \cdots + f_n(x, y, z, t) = 0$ (unde f_j este polinom omogen de grad j pentru fiecare $j \in \{0, 1, \ldots, n\}$), atunci $f_0(x, y, z, t) = f_1(x, y, z, t) = \cdots = f_n(x, y, z, t) = 0$. Dar $f_0(x, y, z, t) + \cdots + f_n(x, y, z, t) = 0$ înseamnă $XT - YZ|_{K[X,Y,Z,T]} f_0(X, Y, Z, T) + f_1(X, Y, Z, T) + \cdots + f_n(X, Y, Z, T)$. Există deci $g = g_0 + g_1 + \cdots + g_m \in K[X, Y, Z, T]$, g_i omogen de grad i pentru orice $i \in \{0, 1, \ldots, m\}$, astfel ca $f_0(X, Y, Z, T) + f_1(X, Y, Z, T) + \cdots + f_n(X, Y, Z, T) = (XT - YZ)g$. Identificând componentele omogene din cei doi membri obţinem $m = n - 2$, $f_0(X, Y, Z, T) = 0$, $f_1(X, Y, Z, T) = 0$ şi $f_j(X, Y, Z, T) = (XT - YZ)g_{j-2}(X, Y, Z, T)$ pentru orice $j \in \{2, 3, \ldots, n\}$. Deci $XT - YZ|_{K[X,Y,Z,T]} f_j(X, Y, Z, T)$, de unde $f_j(x, y, z, t) = 0$ pentru orice $j \in \{0, 1, \ldots, n\}$.
Fie acum $x = fg$ o scriere a lui x ca produs de elemente din R. Constatăm că f şi g trebuie să fie omogene, deoarece dacă unul din ele ar avea cel puţin două componente omogene, produsul lor (şi deci şi x) ar avea aceeaşi proprietate, absurd. În plus, $\operatorname{grad} f = 0$ şi $\operatorname{grad} g = 1$ sau invers. Rezultă aşadar că unul din factorii produsului considerat este inversabil. Prin urmare, x este ireductibil în R.
Relaţia $xt = yz$ ne arată că $x|_R yz$. Dacă $x|_R z$, atunci există un polinom omogen u de grad 0 cu $z = ux$. De aici rezultă că $XT - YZ|_{K[X,Y,T,Z]} uX - Z$, absurd, deoarece dacă dăm valorile $X = T = 0$, $XT - YZ$ se anulează, iar $uX - Z$ nu se anulează. Rămâne că $x \nmid_R z$. Analog se arată că $x \nmid_R y$. Prin urmare, x nu este prim în R. Cum el este ireductibil în acest inel, rezultă că R nu este factorial.
Soluţia 2. Să demonstrăm pentru început că orice element din R se scrie în mod unic sub forma $\overline{F_1(X)} + \overline{T}\overline{F_2(T)}$ cu $F_1, F_2 \in K[Y, Z][U]$. Cum $K[X, Y, Z, T] \simeq K[Y, Z][X, T]$, orice element $\overline{f}$ din R se poate scrie sub forma $\overline{\sum a_{ij} X^i T^j}$ cu $a_{ij} \in K[Y, Z]$. Cum $\overline{XT} = \overline{YZ}$, $\overline{f}$ se rescrie $\overline{\sum\limits_{i \geq j} a_{ij} Y^j Z^j X^{i-j}} + \overline{\sum\limits_{i<j} a_{ij} Y^i Z^i T^{j-i}} = \overline{\sum\limits_{i \geq j} a_{ij} Y^j Z^j X^{i-j}} + \overline{T \sum\limits_{i<j} a_{ij} Y^i Z^i T^{j-i-1}}$ şi am probat astfel existenţa unei scrieri de tipul menţionat. Pentru a proba unicitatea acestui tip de scriere, considerăm egalitatea $\overline{F_1(X)} + \overline{TF_2(T)} = \overline{F_1'(X)} +$

$\overline{T\overline{F_2'(T)}}$. Aceasta înseamnă că $(F_1 - F_1')(X) + T(F_2 - F_2')(T) = (XT - YZ)\Phi$, unde $\Phi \in K[X,Y,Z,T]$. Presupunem că $F_1 \neq F_1'$. Notăm cu D c.m.m.d.c. al coeficienţilor polinoamelor $F_1 - F_1', F_2 - F_2' \in K[Y,Z][U]$ şi $\Phi \in K[Y,Z][X,T]$; punem $F_1 - F_1' = DG_1$, $F_2 - F_2' = DG_2$ şi $\Phi = D\Psi$ şi obţinem $G_1(X) + TG_2(T) = (XT - YZ)\Psi$. Făcând $T = 0$, obţinem $G_1(X) = YZ\Psi(X,Y,Z,0)$, de unde $YZ|G_1(X)$. Făcând $X = 0$, obţinem $G_1(0) + TG_2(T) = YZ\Psi(0,Y,Z,T)$. Cum din relaţia anterioară avem $YZ|G_1(0)$, obţinem şi $YZ|G_2(T)$. Urmează că $YZ|\Phi$, contradicţie. Rămâne deci că $F_1 = F_1'$, ceea ce duce imediat şi la $F_2 = F_2'$.
Să observăm acum că $\operatorname{grad}_X(\overline{F_1(X)} + \overline{T\overline{F_2(T)}})(\overline{F_1'(X)} + \overline{T\overline{F_2'(T)}}) =$
$= \operatorname{grad}_X(\overline{F_1(X)F_1'(X)} + \overline{TF_1(X)F_2'(T)} + \overline{TF_1'(X)F_2(T)} + \overline{T^2F_2(T)F_2'(T)})$
$= \operatorname{grad}_X \overline{F_1(X)} + \operatorname{grad}_X \overline{F_1'(X)}$
$= \operatorname{grad}_X(\overline{F_1(X)} + \overline{T\overline{F_2(T)}}) + \operatorname{grad}_X(\overline{\overline{F_1'(X)} + \overline{T\overline{F_2'(T)}})}$
Analog se arată că $\operatorname{grad}_T(\overline{F_1(X)} + \overline{T\overline{F_2(T)}})(\overline{F_1'(X)} + \overline{T\overline{F_2'(T)}}) =$
$= \operatorname{grad}_T(\overline{F_1(X)} + \overline{T\overline{F_2(T)}}) + \operatorname{grad}_T(\overline{\overline{F_1'(X)} + \overline{T\overline{F_2'(T)}})}$.
Considerăm acum o descompunere $\overline{X} = fg$, cu $f = \overline{F_1(X)} + \overline{T\overline{F_2(T)}}$ şi $g = \overline{F_1'(X)} + \overline{T\overline{F_2'(T)}}$, a lui $\overline{X}$ în R. Conform proprietăţii demonstrate mai sus vom avea $\operatorname{grad}_X f = 1$ şi $\operatorname{grad}_X g = 0$ (sau viceversa) şi $\operatorname{grad}_T f = \operatorname{grad}_T g = 0$. Prin urmare, $f = a\overline{X} + b$ cu $a, b \in K[Y,Z]$ şi $g \in K[Y,Z]$. Din relaţia $\overline{X} = fg$ rezultă acum $ag = 1$, deci g este inversabil în R. Aceste consideraţii ne arată că $\overline{X}$ nu admite descompuneri relevante în R, deci $\overline{X}$ este ireductibil în R.
Pe de altă parte, $\overline{X}|_R\overline{YZ}$. Dacă $\overline{X}|\overline{Y}$, aceasta ar însemna că $\overline{X}(\overline{F(X)} + \overline{T\overline{G(T)}}) = \overline{Y}$, deci $\overline{XF(X)} + \overline{YZG(T)} = \overline{Y}$. Considerând mai întâi gradele în X, rezultă $F(X) = 0$. Considerând apoi gradele în T, constatăm că $G(T)$ trebuie să fie constant. Prin urmare, $\overline{Y} = \alpha\overline{YZ}$ cu $\alpha \in K$, adică $YZ - XT|_{K[X,Y,Z,T]}Y(\alpha Z - 1)$, contradicţie. Rămâne că $\overline{X} \nmid_R \overline{Y}$. Analog se arată că $\overline{X} \nmid_R \overline{Z}$. Prin urmare, $\overline{X}$ este element ireductibil în R, dar nu este element prim. În consecinţă, R nu este inel factorial.

30. Notăm $R = \mathbb{Z}[i\sqrt{d}]$.
"$\Rightarrow$" Să presupunem că $d \geq 3$. Dacă $d = 4$, respectiv 8, folosind relaţiile $-2i \cdot 2i = 2 \cdot 2$, respectiv $-2i\sqrt{2} \cdot 2i\sqrt{2} = 2 \cdot 4$, deducem că 2 nu e prim în R. El este însă ireductibil, deci R nu are proprietatea c.m.m.d.c.. Conform problemei 24, dacă $d = 3$, inelul R nu este principal. Conform problemei 8, dacă $d \in \{5,7,9\}$, R nu are proprietatea c.m.m.d.c., iar dacă $d = 6$, conform problemei 29, R nu este factorial. În nici una din aceste situaţii R nu este euclidian, deci putem considera $d \geq 10$.

Cum R este inel euclidian, există $\varphi : R \setminus \{0\} \longrightarrow \mathbb{N}$ astfel încât oricare ar fi $a, b \in R$, $b \neq 0$, există $q, r \in R$ cu proprietăţile $a = bq + r$ şi $r = 0$ sau $\varphi(r) < \varphi(b)$. Considerăm şi norma $N : R \longrightarrow \mathbb{N}$, $N(x + yi\sqrt{d}) = x^2 + dy^2$. Conform problemei 2, N este multiplicativă, iar $U(R) = \{a \in R \mid N(a) = 1\}$. Conform problemei 4, $U(R) = \{-1, 1\}$. Fie $\alpha \in R \setminus \{-1, 0, 1\}$ astfel că $\varphi(\alpha) = \min\{\varphi(a) | a \in R \setminus \{-1, 0, 1\}\}$. (Remarcăm că acest minim este atins, întrucât $\mathbb{N}$ este bine ordonată.) Dacă z este un element arbitrar din R, atunci, conform proprietăţilor lui φ, există $q, r \in R$ cu proprietăţile $z = q\alpha + r$ şi $r = 0$ sau $\varphi(r) < \varphi(\alpha)$. Conform definiţiei lui α, ultima inegalitate nu este posibilă decât dacă $r \in \{-1, 0, 1\}$.
În consecinţă, orice element din R este congruent cu $-1, 0$ sau 1 modulo α. În particular 2 este congruent cu $-1, 0$ sau 1 modulo α, de unde $\alpha|3$ sau $\alpha|2$ sau $\alpha|1$. Ultimul caz este însă imposibil deoarece $\alpha \notin U(R)$. Trecând la norme în celelalte două relaţii obţinem (vezi problema 3(i)) că $N(\alpha)|9$ sau $N(\alpha)|4$. Cum α nu este inversabil, el nu poate avea norma 1. Prin urmare, $N(\alpha) \in \{2, 3, 4, 9\}$. Să notăm $\alpha = a + bi\sqrt{d}$.
Dacă $N(\alpha) \in \{2, 3\}$, rezultă $a^2 + db^2 \in \{2, 3\}$. Dacă $b = 0$, obţinem $a^2 \in \{2, 3\}$, iar dacă $|b| \geq 1$ găsim $a^2 < 0$, contradicţie.
Dacă $N(\alpha) = 4$, vom avea $a^2 + db^2 = 4$; dacă $b = 0$ obţinem $\alpha = \pm 2 \sim 2$. Constatăm însă că dacă $i\sqrt{d}$ ar da rest $-1, 0$ sau 1 modulo 2, atunci ar avea loc în R o relaţie de forma $i\sqrt{d} = 2(u + vi\sqrt{d}) + \varepsilon$ cu $\varepsilon \in \{-1, 0, 1\}$, de unde $1 = 2v$, contradicţie. Dacă $|b| \geq 1$, obţinem $a^2 = 4 - db^2 < 0$, contradicţie.
Dacă $N(\alpha) = 9$, vom avea $a^2 + db^2 = 9$; pentru $b = 0$ obţinem $\alpha = \pm 3 \sim 3$. Constatăm însă că dacă $i\sqrt{d}$ ar da rest $-1, 0$ sau 1 modulo 3, atunci ar avea loc în R o relaţie de tipul $i\sqrt{d} = 3(u + vi\sqrt{d}) + \varepsilon$ cu $\varepsilon \in \{-1, 0, 1\}$, de unde $1 = 3v$, contradicţie. Dacă $|b| \geq 1$, obţinem $a^2 = 9 - db^2 < 0$, contradicţie.
Rămâne aşadar că inelul R nu este euclidian.
"$\Leftarrow$" Fie $d \in \{1, 2\}$. Definim $N : \mathbb{Q}[i\sqrt{d}] \to \mathbb{Q}$, $N(a + bi\sqrt{d}) = a^2 + db^2$. Conform problemei 2(ii),(iii), N este multiplicativă şi $N(\mathbb{Z}[i\sqrt{d}]) \subset \mathbb{N}$. Fie $x = a + bi\sqrt{d}$ şi $y = c + ei\sqrt{d} \neq 0$ elemente din R. Avem în $\mathbb{C}$

$$\frac{x}{y} = \frac{ac + dbe}{c^2 + de^2} + \frac{bc - ae}{c^2 + de^2} i\sqrt{d} \in \mathbb{Q}[i\sqrt{d}]. \text{ Notăm } \alpha = \frac{ac + dbe}{c^2 + de^2} \text{ şi } \beta = \frac{bc - ae}{c^2 + de^2},$$

iar cu A şi B întregii cei mai apropiaţi de α, respectiv de β. Prin urmare, $|A - \alpha| \leq \frac{1}{2}$ şi $|B - \beta| \leq \frac{1}{2}$. Cu aceste notaţii se obţine

$$\frac{x}{y} = A + Bi\sqrt{d} + (\alpha - A) + (\beta - B)i\sqrt{d},$$

deci $x = (A+Bi\sqrt{d})y+\left[(\alpha - A) + (\beta - B)i\sqrt{d}\right] y$. Cum x, y şi $q = A+Bi\sqrt{d}$ sunt în R, din relaţia anterioară rezultă că $r = \left[(\alpha - A) + (\beta - B)i\sqrt{d}\right] y \in R$. Avem deci în R scrierea $x = qy + r$. În plus, datorită multiplicativităţii lui N, $N(r) = N((\alpha - A) + (\beta - B)i\sqrt{d})N(y) = N(y)|(\alpha - A)^2 + d(\beta - B)^2|$. Avem însă $0 \leq (\alpha - A)^2 \leq \frac{1}{4}$ şi $0 \leq (\beta - B)^2 \leq \frac{1}{4}$. Prin urmare, $N(r) = N(y)((\alpha - A)^2 + d(\beta - B)^2) \leq \frac{1+d}{4}N(y) \leq \frac{3}{4}N(y) < N(y)$. În concluzie, R este euclidian în raport cu N.

31. (i) Fie R un inel factorial care nu este corp şi care are doar un număr finit de elemente inversabile. Presupunem că R are doar un număr finit de elemente prime neasociate şi considerăm un sistem $p_1, \ldots p_n$ de reprezentanţi ai acestora (în raport cu relaţia de asociere în divizibilitate). Avem $n > 0$ deoarece R conţine elemente nenule şi neinversabile. Pentru fiecare $k \in \mathbb{N}^*$ considerăm elementul (nenul) $x_k = (p_1 \cdots p_n)^k + 1$. Remarcăm că $x_i = x_j$ conduce la $(p_1 \cdots p_n)^i = (p_1 \cdots p_n)^j$. Din unicitatea (până la asociere în divizibilitate) descompunerii în factori primi pentru elementele lui R deducem că $i = j$. Prin urmare, elementele mulţimii $\mathcal{X} = \{x_n | n \in \mathbb{N}^*\}$ sunt distincte două câte două, ceea ce arată că $\mathcal{X}$ e infinită, deci $\mathcal{X}$ conţine cel puţin un element neinversabil, fie el x_m. Presupunerea că elementul prim $p \in R$ ar divide x_m ne-ar conduce la contradicţia $p|1$. Rezultă că x_m nu are divizori primi, contradicţie. Rămâne aşadar că R are o infinitate de elemente prime neasociate.
(ii) Considerăm un domeniu de integritate R şi notăm $A = R[X]$. Să remarcăm că X este prim în A (dacă $X|fg$, atunci $f(0)g(0) = (fg)(0) = 0$, de unde $f(0) = 0$ sau $g(0) = 0$, adică $X|f$ sau $X|g$). Presupunem că A are doar un număr finit de elemente prime neasociate şi fie $p_1, \ldots p_n$ un sistem de reprezentanţi ai acestora (în raport cu relaţia de asociere în divizibilitate). Avem $n > 0$ deoarece X este prim în A. Elementul $f = p_1 \cdots p_n + 1$ (care are gradul cel putin 1 deoarece unul din factorii $p_1, \ldots, p_n$ este asociat cu X) nu se divide cu nici un element prim din A (vezi punctul (i)), de unde deducem că este inversabil. Conform problemei 25 din Capitolul 5, coeficienţii lui f diferiţi de $f(0)$ trebuie să fie nilpotenţi; cum R este domeniu, înseamnă că aceşti coeficienţi sunt nuli. Prin urmare, f este constant, contradicţie.

32. (i) Elementul $p = Y - 1 \in K[Y]$ este prim, deoarece dacă $p|_{K[Y]}fg$ rezultă, conform teoremei lui Bézout, $(fg)(1) = 0$, de unde $f(1) = 0$ sau

$g(1) = 0$, adică $p|_{K[Y]}f$ sau $p|_{K[Y]}g$. Polinomul primitiv $X^2 + Y^2 - 1 \in K[Y][X] \simeq K[X,Y]$ este prin urmare ireductibil conform criteriului lui Eisenstein (cu $p = Y - 1$). Cum $K[X,Y]$ este inel factorial, polinomul X^2+Y^2-1 chiar prim. Rezultă că $(X^2 + Y^2 - 1)$ este ideal prim în $K[X,Y]$, deci $K[X,Y]/(X^2 + Y^2 - 1)$ este inel integru.
(ii) Notăm $x = \widehat{X}, y = \widehat{Y}$. Fie $\widehat{f} = \sum a_{ij}x^iy^j \in R$. Punând $P(T) = \sum a_{i,2j}T^i(1-T^2)^j$ şi $Q(T) = \sum a_{i,2j+1}T^i(1-T^2)^j$, avem $\widehat{f} = P(x)+yQ(x)$. În plus, $P_1(x)+yQ_1(x) = P_2(x)+yQ_2(x)$ înseamnă $Y^2+X^2-1|_{K[X,Y]}(Q_2(X)-Q_1(X))Y + (P_2(X) - P_1(X))$, de unde rezultă că $P_1 = P_2$ şi $Q_1 = Q_2$. Prin urmare, elementele lui R se scriu în mod unic sub forma $P + yQ$, cu $P, Q \in K[x]$.
Definim $\mathcal{N} : R \to K[X]$, $\mathcal{N}(P + yQ) = P^2(X) + (X^2 - 1)Q^2(X)$. Avem $\mathcal{N}((P_1 + yQ_1)(P_2 + yQ_2)) = \mathcal{N}(P_1P_2 - (x^2 - 1)Q_1Q_2 + y(P_1Q_2 + P_2Q_1)) = (P_1P_2-(X^2-1)Q_1Q_2)^2+(X^2-1)(P_1Q_2+P_2Q_1)^2 = P_1^2P_2^2+(X^2-1)P_1^2Q_2^2+(X^2-1)P_2^2Q_1^2 + (X^2-1)^2Q_1^2Q_2^2 = \mathcal{N}(P_1 + yQ_1)\mathcal{N}(P_2 + yQ_2)$, deci $\mathcal{N}$ este multiplicativă.
Acum fie $P+yQ \in U(R)$ şi $P'+yQ'$ inversul său. Atunci $1 = \mathcal{N}((P+yQ)(P'+yQ')) = \mathcal{N}(P + yQ)\mathcal{N}(P' + yQ')$, deci $\mathcal{N}(P + yQ)$ este inversabil în $K[X]$, adică este o constantă nenulă din K. Reciproc, $\mathcal{N}(P + yQ) = \alpha \in K \setminus \{0\}$ înseamnă $(P + yQ)(P - yQ) = \alpha$, deci $(P + yQ)[\alpha^{-1}(P - yQ)] = 1$, adică $P + yQ \in U(R)$. Aşadar $P + yQ \in R$ e inversabil dacă şi numai dacă $\mathcal{N}(P + yQ)$ este un element din $K \setminus \{0\}$.
Ipoteza că $x = \widehat{X}$ este element reductibil înseamnă că există $a = P_1 + yQ_1$ şi $b = P_2 + yQ_2$ în $R \setminus U(R)$ astfel încât $x = ab$. Rezultă că $X^2 = \mathcal{N}(x) = \mathcal{N}(a)\mathcal{N}(b)$. Cum $a, b \notin U(R)$, $\mathcal{N}(a)$ şi $\mathcal{N}(b)$ trebuie să aibă gradul cel puţin 1. Din condiţia ca produsul lor să fie X^2 deducem că există $\alpha \in R \setminus \{0\}$ astfel încât $\mathcal{N}(a) = \alpha X$ şi $\mathcal{N}(b) = \alpha^{-1}X$. Aceste condiţii se rescriu $P_1^2 + (X^2 - 1)Q_1^2 = \alpha X$, respectiv $P_2^2 + (X^2 - 1)Q_2^2 = \alpha^{-1}X$. De aici deducem $[P_1(-1)P_2(1)]^2 = \alpha \cdot (-1) \cdot \alpha^{-1} \cdot 1 = -1$.
(iii) "$\Rightarrow$" Dacă $Z^2 + 1$ nu ar avea rădăcini în K, atunci, conform punctului precedent, $x \in R$ ar fi ireductibil. Pe de altă parte, $x|_R x^2 = 1 - y^2 = (1 - y)(1 + y)$. Dacă x ar fi element prim în R, atunci el ar trebui să dividă măcar unul dintre aceşti factori. Dar $x|_R 1 \pm y$ înseamnă că există $P+yQ \in R$ astfel ca $(P+yQ)x = 1\pm y$, adică $Y^2+X^2-1|_{K[X,Y]}(P(X)+YQ(X))X-1\mp Y$, de unde, făcând $X = 0$, obţinem că $Y^2 - 1|_{K[Y]}Y \pm 1$, contradicţie. Rămâne că x nu e prim în R, ceea ce, amintindu-ne că x este ireductibil, înseamnă că R nu este inel factorial, contradicţie.

"$\Leftarrow$" Să notăm cu i o rădăcină din K a lui $Z^2+1 \in K[Z]$. Conform proprietăţii de universalitate a inelelor de polinoame, există morfisme de K-algebre $\Phi, \Psi : K[X,Y] \to K[X,Y]$ astfel încât $\Phi(X) = X + iY, \Phi(Y) = X - iY, \Psi(X) = 2^{-1}(X+Y)$ şi $\Psi(Y) = (2i)^{-1}(X-Y)$. Se constată imediat că $\Phi = \Psi^{-1}$, deci Φ şi Ψ sunt izomorfisme. Avem relaţia $\Psi((X^2+Y^2-1)) = \Psi(((X+iY)(X-iY)-1)) = (XY-1)$. Rezultă că $R \simeq K[X,Y]/(XY-1)$, care, conform problemei 22, este inel euclidian, deci R este inel euclidian. În consecinţă, R este inel factorial.

33. (i) Deoarece polinomul $Z^2+1 \in \mathbb{R}[X]$ nu are rădăcini în $\mathbb{R}$, din problema 32(iii) rezultă că $\mathbb{R}[X,Y]/(X^2+Y^2-1)$ nu este inel factorial.
(ii) Notăm $R = \mathbb{R}[X,Y]/(X^2+Y^2+1)$, $x = \widehat{X}$ şi $y = \widehat{Y}$.
Cum polinomul X^2+Y^2+1 este ireductibil în $\mathbb{R}[X,Y] \simeq \mathbb{R}[Y][X]$ (aplicăm criteriul lui Eisenstein cu $p = Y^2+1$) şi $\mathbb{R}[X,Y]$ este factorial, rezultă că idealul (X^2+Y^2+1) al lui $\mathbb{R}[X,Y]$ este prim, deci R este domeniu.
Fie $\mathfrak{p}$ un ideal prim nenul al lui R. Atunci există un element $f(x,y) \in \mathfrak{p}$, $f(x,y) \neq 0$, cu $f \in \mathbb{R}[X,Y]$. Să notăm cu ξ şi η imaginile lui x, respectiv y, prin proiecţia canonică $R \to R/\mathfrak{p}$. Cum $f(x,y) \in \mathfrak{p}$, rezultă $f(\xi,\eta) = 0$. Pe de altă parte, relaţia $x^2+y^2+1 = 0$ implică $\xi^2+\eta^2+1 = 0$.
Sistemul de condiţii $\xi^2+\eta^2+1 = 0$ şi $f(\xi,\eta) = 0$ este echivalent cu un sistem de forma $\xi^2+\eta^2+1 = 0$ şi $P(\xi)+Q(\xi)\eta = 0$, $P, Q \in \mathbb{R}[T]$. Într-adevăr, afirmaţia este evidentă în situaţia în care $n = \operatorname{grad}_Y f \in \{0,1\}$. Dacă $n \geq 2$, să presupunem afirmaţia adevărată pentru polinoamele de grad mai mic decât n. Punând $f(X,Y) = a_0(X) + a_1(X)Y + \cdots + a_n(X)Y^n$, sistemul dat este echivalent cu $\xi^2+\eta^2+1 = 0$ şi $g(\xi,\eta) = 0$, unde $g(X,Y) = a_0(X)+a_1(X)Y+\cdots+a_{n-1}(X)Y^{n-1}-a_n(X)Y^{n-2}(X^2+1) = f(X,Y)-a_n(X)Y^{n-2}(X^2+Y^2+1)$. Gradul în Y al lui g fiind cel mult $n-1$, putem aplica ipoteza de inducţie şi afirmaţia este demonstrată. Remarcăm în plus că în pasul de inducţie prezentat mai sus avem $f \equiv g \pmod{X^2+Y^2+1}$. Prin urmare, ecuaţia $P(\xi)+Q(\xi)\eta = 0$ se realizează pentru P şi Q nu simultan nule. Evident, ξ şi η vor satisface şi relaţia $(P(\xi)+Q(\xi)\eta)(P(\xi)-Q(\xi)\eta) = 0$, adică $P^2(\xi) - Q^2(\xi)\eta^2 = 0$. Polinomul $P^2(X)-Q^2(X)Y^2$ nu se divide prin X^2+Y^2+1 (altfel am avea că $P(X)-Q(X)Y$ sau $P(X)+Q(X)Y$ se divid prin X^2+Y^2+1, de unde $P = Q = 0$, contradicţie). Aceeaşi proprietate o va avea deci şi polinomul $P^2(X)+Q^2(X)(X^2+1) = P^2(X)-Q^2(X)Y^2+Q^2(X)(X^2+Y^2+1)$. În concluzie, polinomul $P^2(X)+Q^2(X)(X^2+1) \in \mathbb{R}[X]$ este nenul şi are rădăcina ξ.

Prin urmare, există polinoame nenule cu coeficienţi reali care au ca rădăcină pe ξ. Considerăm un astfel de polinom P monic de grad minim. Este imediat că P este ireductibil, deci are grad 1 sau 2. Dacă $\operatorname{grad} P = 1$, atunci, deoarece $R/\mathfrak{p}$ este domeniu, P are exact o rădăcină în $R/\mathfrak{p}$, de unde rezultă că $\xi \in \mathbb{R} \subset R/\mathfrak{p}$. (Pentru ultima incluziune, să constatăm că dacă morfismul canonic $\mathbb{R} \to R/\mathfrak{p}$, $a \mapsto \widehat{a} + \mathfrak{p}$, n-ar fi injectiv atunci ar exista $a \in \mathbb{R}^*$ cu $\widehat{a} \in \mathfrak{p}$. Cum $\widehat{a} + \mathfrak{p}$ e inversabil în R, ar rezulta $\mathfrak{p} = R$, contradicţie.)
Prin urmare, $\xi \in \mathbb{R}$ sau ξ este rădăcină a unui polinom (monic) de grad 2 cu coeficienţi reali.
În mod analog se demonstrează că $\eta \in \mathbb{R}$ sau η este rădăcină a unui polinom (monic) de grad 2 cu coeficienţi reali.
Să mai observăm că ξ şi η nu pot fi simultan reale, deoarece $\xi^2 + \eta^2 + 1 = 0$.
Dacă ξ este o rădăcină a polinomului ireductibil $T^2 + AT + B$, iar η a polinomului $T^2 + CT + D$ $(A, B, C, D \in \mathbb{R})$, atunci $T^2 + AT + B$ se divide prin $T - \xi$ în $Q(R)$ (corpul de fracţii al lui R). Scriem $T^2 + AT + B = (\sigma T + \tau)(T - \xi)$, dezvoltăm şi identificăm coeficienţii. Obţinem $\sigma = 1$ şi $\tau - \xi = A$, de unde $\tau = A + \xi \in R/\mathfrak{p}$. Prin urmare, $\sigma T + \tau = T + (A + \xi) \in (R/\mathfrak{p})[T]$ şi a doua rădăcină a lui $T^2 + AT + B$ este $-(A + \xi) \in R/\mathfrak{p}$; notăm $\overline{\xi} = -(A + \xi)$. În mod similar a doua rădăcină lui $T^2 + CT + D$ este tot în $R/\mathfrak{p}$ şi o notăm cu $\overline{\eta}$.
Să constatăm acum că $A^2 - 4B < 0$ (altfel $T^2 + AT + B$ ar fi reductibil peste $\mathbb{R}$) şi să punem $i = \frac{1}{\sqrt{4B - A^2}}(\xi - \overline{\xi})$. Observăm că $i^2 = \frac{1}{4B - A^2}(\xi - \overline{\xi})^2 = \frac{1}{4B - A^2}[(\xi + \overline{\xi})^2 - 4\xi\overline{\xi}] = \frac{1}{4B - A^2}(A^2 - 4B) = -1$ şi din această relaţie deducem că $i \in U(R/\mathfrak{p})$, deci şi $\xi - \overline{\xi} \in U(R/\mathfrak{p})$.
Dacă notăm $\alpha = \frac{1}{2}(\xi - \overline{\xi})$, $\beta = \frac{1}{2}i^{-1}(\xi - \overline{\xi})$, $\gamma = \frac{1}{2}(\eta + \overline{\eta})$, $\delta = \frac{1}{2}i^{-1}(\eta - \overline{\eta})$, atunci $\alpha = -\frac{1}{2}A \in \mathbb{R} \subset R/\mathfrak{p}$ şi $\beta = \frac{1}{2}i^{-1}(\xi - \overline{\xi}) = \frac{1}{2}\left(\frac{1}{\sqrt{4B - A^2}}(\xi - \overline{\xi})\right) = \frac{\sqrt{4B - A^2}}{2} \in \mathbb{R} \subset R/\mathfrak{p}$. Analog $C, D \in R/\mathfrak{p}$.
Avem $\alpha + i\beta = \frac{1}{2}(\xi - \overline{\xi}) + i\frac{1}{2}i^{-1}(\xi\overline{\xi}) = \xi$ şi analog $\eta = \gamma + i\delta$.
Punând acum $a = \delta$, $b = -\beta$ şi $c = \beta\gamma - \alpha\delta$, obţinem $a\xi + b\eta + c = 0$, cu $a, b, c \in \mathbb{R}$ şi a şi b nu simultan nuli. Relaţia $a\xi + b\eta + c = 0$ conduce la $ax + by + c \in \mathfrak{p}$. Dacă $\xi \in \mathbb{R}$, iar $\eta \in R/\mathfrak{p} - \mathbb{R}$, atunci considerăm $a = 1$, $b = 0$, $c = -\xi$. Cazul $\eta \in \mathbb{R}$, $\xi \in R/\mathfrak{p} - \mathbb{R}$ se tratează analaog.
Prin urmare există întotdeauna $a, b, c \in \mathbb{R}$, cu a, b nu simultan nuli, astfel ca $ax + by + c \in \mathfrak{p}$.
Fie acum un astfel de element $ax + by + c \in R$ cu a, b nu simultan nuli. Conform problemei 23(iii) din Capitolul 4 şi teoremei III de izomorfism pentru

inele avem

$$\begin{aligned}\frac{R}{(ax+by+c)} &\simeq \frac{\mathbb{R}[X,Y]}{(X^2+Y^2+1, aX+bY+c)} \\ &\simeq \frac{\mathbb{R}[X,Y]/(aX+bY+c)}{(X^2+Y^2+1, aX+bY+c)/(aX+bY+c)}.\end{aligned}$$

Dar a şi b nu sunt simultan nuli. Să presupunem de exemplu $b \neq 0$ (cazul $a \neq 0$ se tratează analog). Atunci, $(aX+bY+c) = (Y + \frac{a}{b}X + \frac{c}{b})$. Notăm $a' = -\frac{a}{b}$ şi $b' = -\frac{c}{b}$ şi ţinând cont de izomorfismele de mai sus, putem scrie

$$\frac{R}{(ax+by+c)} \simeq \frac{\mathbb{R}[X,Y]/(Y-(a'X+b'))}{(X^2+Y^2+1, Y-(a'X+b'))/(Y-(a'X+b'))}.$$

Conform problemei 13 din Capitolul 5, avem că $\frac{\mathbb{R}[X,Y]}{(Y-(a'X+b'))} \simeq \mathbb{R}[X]$, acest izomorfism ducând $\widehat{Y}$ în $a'X+b'$. Prin urmare, $\frac{R}{(ax+by+c)} \simeq \frac{\mathbb{R}[X]}{(X^2+(a'X+b')^2+1)}$, acesta din urmă fiind inel integru deoarece idealul $(X^2+(a'X+b')^2+1)$ este prim, fiind generat de un polinom ireductibil (deci prim) din inelul euclidian $\mathbb{R}[X]$.
Să notăm cu S sistemul multiplicativ al lui R generat de elementele de forma $ax+by+c$ cu $(a,b) \neq (0,0)$. Conform consideraţiilor anterioare, orice ideal prim nenul al lui R intersectează pe S. Cum idealele prime ale lui $S^{-1}R$ sunt în corespondenţă bijectivă cu idealele prime ale lui R care nu intersectează pe S (vezi problema 50(ii) din Capitolul 5), rezultă că singurul ideal prim al lui $S^{-1}R$ este (0). Cum idealele maximale sunt prime, rezultă că singurul ideal maximal al lui $S^{-1}R$ este (0), deci $S^{-1}R$ este corp. Prin urmare, $S^{-1}R$ este inel factorial.

Pentru a aplica teorema lui Nagata (vezi problema 21), mai trebuie probat faptul că orice şir ascendent de ideale principale ale lui R este staţionar. Să observăm pentru început că fiecare element din R se reprezintă în mod unic sub forma $P(x)+Q(x)y$ cu $P,Q \in \mathbb{R}[X]$. Într-adevăr, să considerăm un element arbitrar $w \in R$. Atunci există un polinom $f \in \mathbb{R}[X,Y]$ astfel încât $w = f(x,y)$. Dacă $\text{grad}_Y f \in \{0,1\}$, afirmaţia este evidentă. Dacă $\text{grad}_Y f = n \geq 2$, să presupunem afirmaţia adevărată pentru toate elementele $g(x,y) \in R$ cu $\text{grad}_Y g < n$. Dacă scriem $f = a_n(X)Y^n + \cdots + a_0(X)$, atunci, notând $g = a_0(X) + a_1(X)Y + \cdots + a_{n-1}(X)Y^{n-1} - a_n(X)Y^{n-2}(X^2+1) \in \mathbb{R}[X,Y]$, avem în mod clar $\text{grad}_Y g \leq n-1 < n$. Conform ipotezei de inducţie, există $P,Q \in \mathbb{R}[X]$ astfel încât $g(x,y) = P(x)+Q(x)y$. Cum însă

$y^2 = -x^2 - 1$, rezultă că $f(x,y) = a_0(x) + \cdots + a_n(x)y^n = a_0(x) + a_1(x)y + \cdots + a_{n-1}(x)y^{n-1} - a_n(x)y^{n-2}(x^2+1) = g(x,y) = P(x) + Q(x)y$ şi existenţa scrierii este demonstrată. În ceea ce priveşte unicitatea, să remarcăm că pentru $P_1, P_2, Q_1, Q_2 \in \mathbb{R}[X]$, relaţia $P_1(x) + Q_1(x)y = P_2(x) + Q_2(x)y$ înseamnă $Y^2 + X^2 + 1 | (P_1 - P_2) + Y(Q_1 - Q_2)$, de unde deducem $P_1 = P_2$ şi $Q_1 = Q_2$.
Definim acum $N : R \to \mathbb{R}[X]$, $N(P(x) + Q(x)y) = P^2 + (X^2+1)Q^2$. Remarcăm că pentru elementele arbitrare $w_1 = P_1(x) + Q_1(x)y$ şi $w_2 = P_2(x) + Q_2(x)y$ ale lui R avem $N(w_1w_2) = N(P_1(x)P_2(x) - (x^2+1)Q_1(x)Q_2(x) + y(P_1(x)Q_2(x) + P_2(x)Q_1(x))) = P_1^2P_2^2 + (X^2+1)^2Q_1^2Q_2^2 + (X^2+1)P_1Q_2 + (X^2+1)P_2Q_1 = (P_1^2 + (X^2+1)Q_1^2)(P_2^2 + (X^2+1)Q_2^2) = N(w_1)N(w_2)$.
Fie acum $w \in U(R)$. Atunci există $w' \in R$ cu $ww' = 1$. Aplicând N acestei relaţii, obţinem $N(w)N(w') = 1$, deci $N(w) \in U(\mathbb{R}[X]) = \mathbb{R}^*$. Reciproc, dacă avem un element $w = P(x) + Q(x)y \in R$ cu $N(w) = \alpha \in \mathbb{R}^*$, atunci $1 = \frac{1}{\alpha}N(w) = \frac{1}{\alpha}(P^2 + (X^2+1)Q^2)$. Dând lui X valoarea x, obţinem $1 = \frac{1}{\alpha}(P^2(x) + (x^2+1)Q^2(x)) = P^2(x) - y^2Q^2(x) = w\frac{1}{\alpha}(P(x) - yQ(x))$, prin urmare $w \in U(R)$. În concluzie, un element $w \in R$ este inversabil dacă şi numai dacă $N(w) \in \mathbb{R}^*$.
Dacă $w_1|_R w_2$, atunci există $\lambda \in R$ astfel ca $w_2 = \lambda w_1$. Utilizând multiplicativitatea lui N, obţinem $N(w_2) = N(\lambda)N(w_1)$, de unde $N(w_1)|_{\mathbb{R}[X]}N(w_2)$. Dacă în plus $w_2 \sim_R w_1$, atunci $\lambda \in U(R)$, deci $N(\lambda) \in \mathbb{R}^*$, de unde $N(w_1) \sim_{\mathbb{R}[X]} N(w_2)$. Pe de altă parte, dacă $w_1|_R w_2$, $w_2 = \lambda w_1$, şi avem că $N(w_1) \sim_{\mathbb{R}[X]} N(w_2)$, atunci rezultă $N(\lambda) \in U(\mathbb{R}[X]) = \mathbb{R}^*$. Urmează $\lambda \in U(R)$, deci $w_1 \sim_R w_2$.
În concluzie, dacă pentru elementele $w_1, w_2 \in R$ avem $w_2R \subset w_1R$, atunci $N(w_2)\mathbb{R}[X] \subset N(w_1)\mathbb{R}[X]$, iar aceste incluziuni sunt fie ambele stricte, fie ambele egalităţi.
Fie acum $w_1R \subset w_2R \subset \cdots$ un lanţ ascendent de ideale principale ale lui R. Conform celor de mai sus, el induce lanţul ascendent de ideale principale $N(w_1)\mathbb{R}[X] \subset N(w_2)\mathbb{R}[X] \subset \cdots$ din $\mathbb{R}[X]$. Acest din urmă lanţ este însă staţionar deoarece $\mathbb{R}[X]$ este inel principal. Prin urmare, lanţul $w_1R \subset w_2R \subset \cdots$ este de asemenea staţionar.
Inelul R verifică aşadar condiţiile teoremei lui Nagata (vezi problema 21). Prin urmare, R este inel factorial.

34. (i) Notăm $R = \mathbb{Z}[\sqrt{d}]$. Fie π un element prim al lui R. Atunci π nu este inversabil în R, deci (vezi problema 2(iv)) $N(\pi) \neq 1$. Prin urmare, $N(\pi)$ se poate scrie ca produs de factori primi; fie $N(\pi) = p_1 \cdots p_n$ această

scriere. Rezultă $\pi\overline{\pi} = p_1 \cdots p_n$, deci π divide măcar unul din aceşti factori; după o eventuală renumerotare putem presupune că $\pi | p_1$. Există prin urmare $x \in R$ astfel încât $p_1 = \pi x$. Trecând la norme, obţinem $p_1^2 = N(\pi)N(x)$, de unde $p_1^2 = p_1 \cdots p_n N(x)$. Această relaţie nu este posibilă decât într-unul din următoarele două cazuri:
$n = 2$, $p_2 = p_1$ şi $N(x) = 1$. Atunci (vezi problema 2(iv)) x este inversabil în R. În consecinţă, $\pi \sim p_1$.
$n = 1$ şi $N(x) = p_1$. Atunci $\pi\overline{\pi} = N(\pi) = p_1$.
(ii) Demonstraţia este similară celei de la punctul (i).

35. Să notăm $R = \mathbb{Z}[\sqrt{d}]$.
"$\Rightarrow$" Dacă x este prim în R, atunci, conform problemei 34, $N(x)$ este număr prim sau x este asociat în R cu un număr prim $p \in \mathbb{Z}$. Acest din urmă caz ar duce însă la $p|_{\mathbb{Z}} a$ şi $p|_{\mathbb{Z}} b$, deci $p|_{\mathbb{Z}}(a, b) = 1$, contradicţie.
"$\Leftarrow$" Conform problemei 16 din Capitolul 5, inelul $R/(x)$ are $|a^2 - b^2 d| = N(x)$ elemente. Folosind problema 2 din Capitolul 4 (pe o mulţime cu un număr prim p de elemente există un singur tip de structură de inel unitar, cea a lui $\mathbb{Z}_p$), rezultă că $R/(x) \simeq \mathbb{Z}_p$. Cum $\mathbb{Z}_p$ este corp, deci cu atât mai mult inel integru, rezultă că (x) este ideal prim în R. De aici rezultă că x este element prim în R.

36. Notăm $R = \mathbb{Z}[i]$, care este inel euclidian. Prin urmare, un element din R este prim dacă şi numai dacă este ireductibil. Fie $\pi \in R$ prim. Conform problemei 34, π este asociat cu un prim din $\mathbb{Z}$ sau $N(\pi)$ este prim în $\mathbb{Z}$. Cum orice $p \in \mathbb{Z}_-$ este asociat cu $-p$, trebuie să considerăm elementele prime din $\mathbb{N}$ şi să decidem care rămân prime în R şi care sunt norme de prime din R.
Să remarcăm pentru început că $2 = (1 + i)(1 - i)$ şi $N(1 + i) = N(1 - i) = 2$, deci $2 \in R$ nu este prim. Pe de altă parte, $1 + i$ şi $1 - i$ sunt ireductibile (vezi problema 2(v)), deci, cum R este euclidian, ele sunt prime. Observăm şi că $1 - i = -i(1 + i)$, deci $1 - i \sim_R 1 + i$.
Pentru ca un prim p din $\mathbb{N}$ să fie reductibil în R, el trebuie să se scrie $p = xy$ cu $x, y \in R$ pentru care $N(x) = N(y) = p$. Punând $x = a + bi$, deducem $a^2 + b^2 = p$. Cum membrul stâng al acestei relaţii nu poate fi congruent cu 3 modulo 4, rezultă că primele de forma $4k + 3$ din $\mathbb{N}$ rămân prime şi în R.

Fie acum un prim $p \in \mathbb{N}$ de forma $4k+1$. Considerăm relaţiile:

$$\begin{array}{l} p-1 \equiv -1 \pmod p \\ p-2 \equiv -2 \pmod p \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \frac{p+1}{2} \equiv -\frac{p-1}{2} \pmod p, \end{array}$$

din care deducem (folosind teorema lui Wilson, i.e. $(p-1)! \equiv -1 \pmod p$) că $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod p$. Prin urmare, pentru $a = \left(\frac{p-1}{2}\right)!$ avem $a^2 \equiv -1 \pmod p$. Avem $p|a^2+1$, deci $p|_R(a-i)(a+i)$. Dar este clar că p nu divide în R niciunul din factorii acestui produs, prin urmare p nu este prim în R. Pe de altă parte, dacă p se descompune în R ca $(a+bi)(c+di)$, obţinem $N(a+bi) = N(c+di) = p$, deci $(a+bi)(a-bi) = p$; în plus, conform problemei 2(v), $a \pm bi$ sunt prime în R şi demonstraţia este completă.

37. Notăm $R = \mathbb{Z}[i\sqrt{2}]$, care este inel euclidian. Prin urmare, un element din R este prim dacă şi numai dacă este ireductibil. Fie $\pi \in R$ prim. Conform problemei 34, π este asociat cu un prim din $\mathbb{Z}$ sau $N(\pi)$ este prim în $\mathbb{Z}$. Cum orice $p \in \mathbb{Z}_-$ este asociat cu $-p$, trebuie să considerăm elementele prime din $\mathbb{N}$ şi să decidem care rămân prime în R şi care sunt norme de prime din R. Să remarcăm pentru început că $2 = (-i\sqrt{2}) \cdot i\sqrt{2}$ şi $N(i\sqrt{2}) = 2$, deci $2 \in R$ nu este prim. Pe de altă parte, $i\sqrt{2}$ este ireductibil (vezi problema 2(v)), prin urmare, cum R este euclidian, el este prim.
Pentru ca un prim p din $\mathbb{N}$ să fie reductibil în R, el trebuie să se scrie $p = xy$ cu $x, y \in R$ pentru care $N(x) = N(y) = p$. Punând $x = a + bi\sqrt{2}$, deducem $a^2 + 2b^2 = p$. Cum membrul stâng al acestei relaţii nu poate fi congruent cu 5 sau 7 modulo 8, rezultă că primele de forma $8k+5$ şi cele de forma $8k+7$ din $\mathbb{N}$ rămân prime şi în R.

În cele ce urmează vom avea nevoie de următorul rezultat:
Lemă Fie $p \in \mathbb{N}$ un număr prim impar şi $a \in \mathbb{Z}$ cu $(a,p) = 1$. Următoarele afirmaţii sunt echivalente:
1. Există $x \in \mathbb{Z}$ astfel încât $x^2 \equiv a \pmod p$.
2. $a^{\frac{p-1}{2}} \equiv 1 \pmod p$.
Demonstraţie Considerăm polinomul $F \in \mathbb{Z}_p[X]$, $F = X^{p-1} - 1$. Este evident că rădăcinile sale sunt exact elementele nenule din $\mathbb{Z}_p$. Putem scrie $F = GH$, unde $G = (X^{\frac{p-1}{2}} - 1)$, $H = (X^{\frac{p-1}{2}} + 1)$. Dacă $a = x^2$ în $\mathbb{Z}_p$, atunci a nu poate fi rădăcină a lui H, deoarece ar rezulta $x^{p-1} = a^{\frac{p-1}{2}} = -1$, ceea ce nu e posibil în grupul multiplicativ $\mathbb{Z}_p \setminus \{0\}$ de ordin $p-1$. Aşadar pătratele din $\mathbb{Z}_p \setminus \{0\}$

sunt rădăcini pentru G. Pe de altă parte, pentru $i, j \in \{\widehat{1}, \widehat{2}, \ldots, \widehat{\frac{p-1}{2}}\}$ avem $i^2 = j^2 \Leftrightarrow p|(i-j)(i+j)$. Este clar că $p \nmid i+j$ şi $p|i-j$ doar dacă $i = j$; prin urmare $i^2 = j^2 \Leftrightarrow i = j$. Aşadar în $\mathbb{Z}_p \setminus \{0\}$ avem exact $\frac{p-1}{2}$ pătrate distincte (evident, $\widehat{p-1}^2 = \widehat{1}^2, \widehat{p-2}^2 = \widehat{2}^2$, etc). Prin urmare, $\widehat{a} \in \mathbb{Z}_p \setminus \{0\}$ este pătrat dacă şi numai dacă este rădăcină a lui G, deci dacă şi numai dacă $\widehat{a}^{\frac{p-1}{2}} = \widehat{1}$, adică ceea ce era de demonstrat.

Fie acum un prim $p \in \mathbb{N}$ de forma $8k+1$ sau $8k+3$. Notăm $k = \left[\frac{p-1}{4}\right]$, $a_j = 2j$ pentru fiecare $j = \overline{1,k}$ şi $b_j = 2j$ pentru fiecare $j = \overline{k+1, \frac{p-1}{2}}$. Să observăm că $0 \leq a_1, a_2, \ldots, a_k \leq \frac{p-1}{2}$, $\frac{p-1}{2} < b_{k+1}, \ldots, b_{\frac{p-1}{2}} \leq p-1$ şi elementele $a_1, a_2, \ldots, a_k, p-b_{k+1}, \ldots, p-b_{\frac{p-1}{2}}$ sunt distincte două câte două ($a_i = a_j \Rightarrow p|2(i-j) \Rightarrow i = j$, deoarece $0 \leq i, j \leq \frac{p-1}{2}$; analog $b_i = b_j \Rightarrow i = j$; $a_i = b_j \Rightarrow p|2(i+j) \Rightarrow i = j$, deoarece $0 \leq i, j \leq \frac{p-1}{2}$). Prin urmare, $\{a_1, a_2, \ldots, a_k, p-b_{k+1}, \ldots, p-b_{\frac{p-1}{2}}\} = \{1, 2, \ldots, \frac{p-1}{2}\}$. Considerăm relaţiile:

$$\begin{aligned}
&2 \cdot 1 \equiv a_1 \pmod{p},\\
&2 \cdot 2 \equiv a_2 \pmod{p},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&2 \cdot k \equiv a_k \pmod{p},\\
&2 \cdot (k+1) \equiv b_{k+1} \pmod{p},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&2 \cdot \tfrac{p-1}{2} \equiv b_{\frac{p-1}{2}} \pmod{p}.
\end{aligned}$$

Înmulţindu-le membru cu membru obţinem $2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{p-1}{2}-k} \left(\frac{p-1}{2}\right)!$ (mod p) de unde deducem că $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}-\left[\frac{p-1}{4}\right]} \pmod{p}$, deci $(-2)^{\frac{p-1}{2}} \equiv (-1)^{p-1-\left[\frac{p-1}{4}\right]} \pmod{p}$. Dar pentru p de forma $8k+1$ sau $8k+3$ numărul $p-1-\left[\frac{p-1}{4}\right]$ este par, deci, conform lemei, există $a \in \mathbb{Z}$ cu proprietatea $a^2 \equiv -2 \pmod{p}$. Avem $p|a^2+2$, deci $p|_R(a-i\sqrt{2})(a+i\sqrt{2})$. Dar este clar că p nu divide în R niciunul din factorii acestui produs, prin urmare p nu este prim în R.
Scriind $p = (a+bi\sqrt{2})(c+di\sqrt{2})$ în R, obţinem $N(a+bi\sqrt{2}) = N(c+di\sqrt{2}) = p$, deci $(a+bi\sqrt{2})(a-bi\sqrt{2}) = p$; conform problemei 2(v), $a \pm bi\sqrt{2} \in R$ sunt prime (fiindcă sunt ireductibile) şi demonstraţia e completă.

38. Notăm $R = \mathbb{Z}[\sqrt{2}]$, care este inel euclidian. Prin urmare, un element din R este prim dacă şi numai dacă este ireductibil. Fie $\pi \in R$ prim. Conform problemei 34, π este asociat cu un prim din $\mathbb{Z}$ sau $N(\pi)$ este prim în $\mathbb{Z}$. Cum

orice $p \in \mathbb{Z}_-$ este asociat cu $-p$, trebuie să considerăm elementele prime din $\mathbb{N}$ şi să decidem care rămân prime în R şi care sunt norme de prime din R. Să remarcăm pentru început că $2 = \sqrt{2}^2$ şi $N(\sqrt{2}) = 2$, deci $2 \in R$ nu este prim. Pe de altă parte, $\sqrt{2}$ este ireductibil (vezi problema 2(v)), prin urmare, cum R este euclidian, el este prim.
Pentru ca un prim p din $\mathbb{N}$ să fie reductibil în R, el trebuie să se scrie $p = xy$ cu $x, y \in R$ pentru care $N(x) = N(y) = p$. Punând $x = a + b\sqrt{2}$, deducem $|a^2 - 2b^2| = p$. Cum membrul stâng al acestei relaţii nu poate fi congruent cu 3 sau 5 modulo 8, rezultă că primele de forma $8k + 3$ şi cele de forma $8k + 5$ din $\mathbb{N}$ rămân prime şi în R. Fie acum un prim $p \in \mathbb{N}$ de forma $8k + 1$ sau $8k + 7$. Notăm $k = \left[\frac{p-1}{4}\right]$, $a_j = 2j$ pentru fiecare $j = \overline{1, k}$ şi $b_j = 2j$ pentru fiecare $j = \overline{k+1, \frac{p-1}{2}}$. Să observăm că $0 \leq a_1, a_2, \ldots, a_k \leq \frac{p-1}{2}$, $\frac{p-1}{2} < b_{k+1}, \ldots, b_{\frac{p-1}{2}} \leq p-1$ şi elementele $a_1, a_2, \ldots, a_k, p - b_{k+1}, \ldots, p - b_{\frac{p-1}{2}}$ sunt distincte două câte două ($a_i = a_j \Rightarrow p|2(i-j) \Rightarrow i = j$, deoarece $0 \leq i, j \leq \frac{p-1}{2}$; analog $b_i = b_j \Rightarrow i = j$; $a_i = b_j \Rightarrow p|2(i+j) \Rightarrow i = j$, deoarece $0 \leq i, j \leq \frac{p-1}{2}$). Prin urmare, $\{a_1, a_2, \ldots, a_k, p - b_{k+1}, \ldots, p - b_{\frac{p-1}{2}}\} = \{1, 2, \ldots, \frac{p-1}{2}\}$. Considerăm relaţiile:

$$\begin{aligned}
&2 \cdot 1 \equiv a_1 \pmod{p},\\
&2 \cdot 2 \equiv a_2 \pmod{p},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&2 \cdot k \equiv a_k \pmod{p},\\
&2 \cdot (k+1) \equiv b_{k+1} \pmod{p},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&2 \cdot \tfrac{p-1}{2} \equiv b_{\frac{p-1}{2}} \pmod{p}.
\end{aligned}$$

Înmulţindu-le membru cu membru, obţinem $2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{p-1}{2}-k} \left(\frac{p-1}{2}\right)!$ (mod p) de unde deducem că $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}-\left[\frac{p-1}{4}\right]}$ (mod p). Dar pentru p de forma $8k + 1$ sau $8k + 7$ numărul $\frac{p-1}{2} - \left[\frac{p-1}{4}\right]$ este par, deci, conform lemei din soluţia problemei 37, există $a \in \mathbb{Z}$ cu proprietatea $a^2 \equiv 2 \pmod{p}$. Avem deci $p|a^2 - 2$, prin urmare $p|_R(a - \sqrt{2})(a + \sqrt{2})$. Dar este clar că p nu divide în R niciunul din factorii acestui produs, prin urmare p nu e prim în R.
Scriind $p = (a+b\sqrt{2})(c+d\sqrt{2})$ în R, obţinem $N(a+b\sqrt{2}) = N(c+d\sqrt{2}) = p$, deci $|(a + b\sqrt{2})(a - b\sqrt{2})| = p$; conform problemei 2(v), $a \pm b\sqrt{2} \in R$ sunt prime (fiindcă sunt ireductibile) şi demonstraţia este completă.

39. Notăm $R = \mathbb{Z}[\sqrt{3}]$, care este inel euclidian. Prin urmare, un element din R este prim dacă şi numai dacă este ireductibil. Fie $\pi \in R$ prim. Conform problemei 34, π este asociat cu un prim din $\mathbb{Z}$ sau $N(\pi)$ este prim în $\mathbb{Z}$. Cum orice $p \in \mathbb{Z}_-$ este asociat cu $-p$, trebuie să considerăm elementele prime din $\mathbb{N}$ şi să decidem care rămân prime în R şi care sunt norme de prime din R. Să remarcăm pentru început că $2 = (\sqrt{3}-1)(\sqrt{3}+1)$, iar $3 = \sqrt{3}^2$. $N(\sqrt{3}\pm 1) = 2$, iar $N(\sqrt{3}) = 3$, deci 2 şi 3 nu sunt prime în R, iar $\sqrt{3}\pm 1$ şi $\sqrt{3}$ sunt ireductibile (vezi problema 2(v)), prin urmare, cum R este euclidian, ele sunt prime. În plus, $\sqrt{3}-1 \sim_R 1+\sqrt{3}$.
Pentru ca un prim p din $\mathbb{N}$ să fie reductibil în R, el trebuie să se scrie $p = xy$ cu $x, y \in R$ pentru care $N(x) = N(y) = p$. Punând $x = a + b\sqrt{3}$, deducem $|a^2 - 3b^2| = p$. Cum membrul stâng al acestei relaţii nu poate fi congruent cu 5 sau 7 modulo 12, rezultă că primele din $\mathbb{N}$ de forma $12k+5$ şi cele de forma $12k+7$ rămân prime şi în R. Fie acum un prim $p \in \mathbb{N}$ de forma $12k+1$ sau $12k+11$. Notăm $k = \left[\frac{p-1}{6}\right]$ şi $l = \left[\frac{p-1}{3}\right]$. Considerăm relaţiile:

$$
\begin{aligned}
&3 \cdot 1 \equiv 3 \overset{not}{=} a_1 \pmod p,\\
&3 \cdot 2 \equiv 6 \overset{not}{=} a_2 \pmod p,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&3 \cdot k \equiv 3k \overset{not}{=} a_k \pmod p,\\
&3 \cdot (k+1) \equiv 3(k+1) \overset{not}{=} b_{k+1} \pmod p,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&3 \cdot l \equiv 3l \overset{not}{=} b_l \pmod p,\\
&3 \cdot (l+1) \equiv 3(l+1) \overset{not}{=} c_{l+1} \pmod p,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&3 \cdot \tfrac{p-1}{2} \equiv \tfrac{3(p-1)}{2} \overset{not}{=} c_{\frac{p-1}{2}} \pmod p.
\end{aligned}
$$

Să observăm că $0 \le a_1, a_2, \ldots, a_k \le \frac{p-1}{2}$, $\frac{p-1}{2} < b_{k+1}, \ldots, b_l \le p-1$, $p+1 \le c_{l+1}, c_{l+2}, \ldots, c_{\frac{p-1}{2}} \le \frac{3(p-1)}{2}$ şi elementele $a_1, a_2, \ldots, a_k, p-b_{k+1}, \ldots, p-b_l, c_{l+1}-p, \ldots, c_{\frac{p-1}{2}} - p$ sunt distincte două câte două (procedând ca în soluţia problemei 37). Prin urmare, $\{a_1, a_2, \ldots, a_k, p-b_{k+1}, \ldots, p-b_l, c_{l+1}-p, \ldots, c_{\frac{p-1}{2}}\} = \{1, 2, \ldots, \frac{p-1}{2}\}$. Înmulţind membru cu membru relaţiile anterioare, obţinem $3^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{l-k} \left(\frac{p-1}{2}\right)! \pmod p$ de unde deducem că $3^{\frac{p-1}{2}} \equiv (-1)^{\left[\frac{p-1}{3}\right]-\left[\frac{p-1}{6}\right]} \pmod p$. Dar pentru p de forma $12k+1$ sau $12k+11$ numărul $\left[\frac{p-1}{3}\right] - \left[\frac{p-1}{6}\right]$ este par, deci, conform lemei din soluţia problemei 37, există $a \in \mathbb{Z}$ cu proprietatea $a^2 \equiv 3 \pmod p$. Avem deci $p | a^2 - 3$, prin

urmare $p|_R(a-\sqrt{3})(a+\sqrt{3})$. Dar este clar că p nu divide în R niciunul din factorii acestui produs, prin urmare p nu este prim în R.
Pe de altă parte, dacă p se descompune în R ca $(a+b\sqrt{3})(c+d\sqrt{3})$, obţinem $N(a+b\sqrt{3}) = N(c+d\sqrt{3}) = p$, deci $|(a+b\sqrt{3})(a-b\sqrt{3})| = p$. În plus, conform problemei 2(v), $a \pm b\sqrt{3}$ sunt prime (fiindcă sunt ireductibile) în R şi demonstraţia este completă.

40. Notăm $R = \mathbb{Z}[\rho]$, $\rho = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, care este inel euclidian. Fie π un element prim al lui R. Conform problemei 34, π este asociat cu un element prim din $\mathbb{Z}$ sau $N(\pi)$ este prim în $\mathbb{Z}$. Prin urmare, orice element prim din R e asociat într-unul din aceste moduri cu un număr prim p din $\mathbb{N}$. Vom trece în revistă numerele prime din $\mathbb{N}$ pentru a stabili dacă le sunt asociate elemente prime din R şi, dacă da, în ce mod.
Dacă $p = 3$, atunci $p = (1-\rho)\overline{(1-\rho)} = (1-\rho)(2+\rho)$; cum $N(1-\rho) = N(2+\rho) = 3$, elementele $1-\rho$ şi $2+\rho$ sunt neinversabile în R, deci 3 este reductibil (prin urmare, nu este prim) în R.
Avem $N(1-\rho) = 3$. Conform problemei 2(v), $1-\rho$ este ireductibil în R şi cum R este inel euclidian (vezi problema 18) rezultă că $1-\rho$ este prim.
Fie acum un element $a+b\rho \in R$ cu $N(a+b\rho) = 3$. Atunci, $a^2 - ab + b^2 = \left(a - \frac{b}{2}\right)^2 + \frac{3b^2}{4} = 3$. Dacă $b = 0$, obţinem $a^2 = 3$, imposibil. Dacă $b = 1$ rezultă $\left(a - \frac{1}{2}\right)^2 = \frac{9}{4}$, deci $a \in \{-1, 2\}$. Dacă $b = -1$ rezultă $\left(a + \frac{1}{2}\right) = \frac{9}{4}$, deci $a \in \{-2, 1\}$. Dacă $b = 2$ obţinem $(a-1)^2 = 0$, deci $a = 1$, iar dacă $|b| > 2$, atunci $N(a+b\rho)$ nu poate fi 3. Prin urmare, elementele de normă 3 din R sunt $-1+\rho$, $-1-2\rho$, $1-\rho$, $1+2\rho$, $2+\rho$ şi $-2-\rho$.
Cum $|\{(1-\rho)a | a \in U(R)\}| \subset |\{x \in R | N(x) = 3\}|$ şi aceste mulţimi au câte 6 elemente (vezi problema 5 pentru prima dintre ele), rezultă că ele sunt egale, deci orice element de normă 3 din R este asociat cu $1-\rho$. Prin urmare, numărului prim 3 îi corespund elemente prime din R şi oricare dintre acestea este asociat în divizibilitate cu $1-\rho$.
Dacă numărul prim p este de forma $3k+1$, $k \in \mathbb{N}^*$, utilizăm relaţia

$$3^{\frac{p-1}{2}} \equiv (-1)^{\left[\frac{p-1}{3}\right] - \left[\frac{p-1}{6}\right]} \pmod{p},$$

pe care am demonstrat-o în soluţia problemei 39. Din această relaţie deducem

$$(-3)^{\frac{p-1}{2}} \equiv (-1)^{\left[\frac{p-1}{3}\right] - \left[\frac{p-1}{6}\right] + \left(\frac{p-1}{2}\right)} \pmod{p}.$$

Numărul p fiind prim şi de forma $3k+1$, el nu poate da prin împărţire la 12 decât resturile 1 sau 7.

Dacă $p = 12l + 1$, atunci

$$(-1)^{\left[\frac{p-1}{3}\right]-\left[\frac{p-1}{6}\right]+\left(\frac{p-1}{2}\right)} = (-1)^{4l-2l+6l} = 1.$$

Dacă $p = 12l + 7$, atunci

$$(-1)^{\left[\frac{p-1}{3}\right]-\left[\frac{p-1}{6}\right]+\left(\frac{p-1}{2}\right)} = (-1)^{4l+2-2l-1+6l+3} = 1.$$

Prin urmare, conform lemei din soluţia problemei 37, există $a \in \mathbb{Z}$ astfel ca $a^2 \equiv -3 \pmod{p}$. Atunci $p|_{\mathbb{Z}} a^2 + 3$, de unde $p|_R a^2 + 3 = (a - i\sqrt{3})(a + i\sqrt{3})$; este însă evident că p nu divide în R niciunul dintre aceşti factori. Prin urmare, p nu este prim în R, deci nu există elemente prime din R asociate cu el. Există în schimb, conform consideraţiilor de mai sus, elemente $\pi \in R$ pentru care $N(\pi) = \pi\overline{\pi} = p$ şi orice astfel de element este, conform problemei 2(v), ireductibil. Prin urmare, orice astfel de element este şi prim, căci ştim că R este inel euclidian.
Dacă numărul prim p este de forma $3k + 2$, $k \in \mathbb{N}$, vom presupune că p este reductibil în R. Atunci el se scrie sub forma $p = xy$ cu $x, y \in R \setminus U(R)$. Obţinem $p^2 = N(p) = N(x)N(y)$, de unde $N(x) = N(y) = p$. Punând $x = a + b\rho$, $a, b \in \mathbb{Z}$, obţinem $(2a - b)^2 + 3b^2 = 4p$, deci $(2a - b)^2 \equiv p \pmod{3}$, de unde $(2a - b)^2 \equiv 2 \pmod{3}$, contradicţie. Rămâne aşadar că p este ireductibil în R. Cum R este inel euclidian, obţinem că p este element prim în R.

41. Să observăm pentru început că dacă (x, y, z) este o soluţie pentru ecuaţia din enunţ cu $d = (x, y, z) \neq 1$, atunci $\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$ este şi ea soluţie. E suficient prin urmare să găsim soluţiile (x, y, z) cu $(x, y, z) = 1$ pentru ecuaţia considerată, celelalte obţinându-se apoi prin multiplicarea acestora cu constante. Apoi, singurele soluţii cu componentă nulă sunt cele din $\{(0, k, \pm k) | k \in \mathbb{Z}\}$ şi $\{(k, 0, \pm k) | k \in \mathbb{Z}\}$. În al treilea rând, să constatăm că, dată fiind soluţia (x, y, z), $(|x|, |y|, |z|)$ este la rându-i soluţie, deci soluţiile cu componente întregi se obţin din cele cu componente naturale luând toate combinaţiile posibile de semne.
Rămâne prin urmare să rezolvăm ecuaţia dată în numere naturale nenule cu cel mai mare divizor comun 1. Privim ecuaţia în $R = \mathbb{Z}[i]$ (care este inel euclidian), unde ea se poate rescrie $(x + iy)(x - iy) = z^2$. Dacă un element prim $\pi \in R$ divide în R pe $x + iy$ şi $x - iy$, atunci el divide şi suma şi diferenţa acestora, deci $\pi|_R(2x, 2iy)$. Dar $(x, y) = 1$, căci dacă ar exista un număr prim p care să dividă şi pe x şi pe y, atunci din ecuaţie ar rezulta că p îl divide şi

pe z, contradicţie cu faptul că $(x, y, z) = 1$. Prin urmare, $\pi|_R(2x, 2iy) = 2$. Rezultă că $\pi = 1 + i$. Dar $1 + i|_R x + iy$ conduce, conform problemei 3(i), la $2 = N(1+i)|N(x+iy) = x^2 + y^2$. Pe de altă parte, x şi y nu pot fi simultan pare, căci ar rezulta şi z par, deci $2|(x, y, z)$, contradicţie, şi nici simultan impare, căci s-ar obţine contradicţia $z^2 = x^2 + y^2 \equiv 2 \pmod 4$. Faptul că $1 + i|x + iy$ este aşadar contradictoriu. Prin urmare, $x + iy$ şi $x - iy$ nu au divizori primi comuni, deci sunt prime între ele în R.
Relaţia $(x + iy)(x - iy) = z^2$ împreună cu faptul că $x + iy$ şi $x - iy$ nu au divizori primi comuni conduce la concluzia că $x + iy$ şi $x - iy$ sunt asociate cu pătrate din R. avem de considerat cazurile:
1. Există $a, b \in \mathbb{Z}$ astfel ca $x + iy = (a + bi)^2$. Obţinem $x = a^2 - b^2$, $y = 2ab$ iar din ecuaţie deducem $z = a^2 + b^2$. Să observăm că această soluţie convine doar dacă $a^2 - b^2 > 0$, a şi b sunt de acelaşi semn (căci $y = 2ab \in \mathbb{N}$), situaţie în care ele pot fi luate numere naturale cu $a > b$, iar a şi b sunt prime între ele, căci altfel $(x, y, z) \neq 1$.
2. Există $a, b \in \mathbb{Z}$ astfel ca $x + iy = -(a + bi)^2$. Obţinem $x = |b|^2 - |a|^2$, $y = 2|a||b|$ iar din ecuaţie deducem $z = |a|^2 + |b|^2$. Pentru $|b| \leq |a|$, acest caz nu dă soluţii.
3. Există $a, b \in \mathbb{Z}$ astfel ca $x + iy = i(a + bi)^2$. Obţinem $x = 2|a||b|$, $y = |a|^2 - |b|^2$, $y = 2ab$ iar din ecuaţie deducem $z = |a|^2 + |b|^2$. Pentru $|a| \leq |b|$, acest caz nu dă soluţii.
4. Există $a, b \in \mathbb{Z}$ astfel ca $x + iy = -i(a + bi)^2$. Obţinem $x = 2|a||b|$, $y = |b|^2 - |a|^2$, $y = 2ab$ iar din ecuaţie deducem $z = |a|^2 + |b|^2$. Pentru $|b| \leq |a|$, acest caz nu dă soluţii.
Prin urmare, soluţiile netriviale ale ecuaţiei date, numită şi *ecuaţia lui Pitagora*, sunt $(\pm d(a^2 - b^2), \pm 2dab, \pm d(a^2 + b^2))$ şi $(\pm 2dab, \pm d(a^2 - b^2), \pm d(a^2 + b^2))$, unde $a > b$ sunt numere naturale prime între ele, $d \in \mathbb{N}^*$, iar alegerea semnelor $\pm$ poate fi făcută în toate combinaţiile posibile.

42. Să constatăm pentru început că singura soluţie care are componente nule este $(0, 0, 0)$. În continuare, pentru orice soluţie (x, y, z) cu componentele nenule, notând $d = c.m.m.d.c.(x, y, z)$, avem $d^4|x^2$, deci $d^2|x$. Deducem că (x, y, z) e soluţie dacă şi numai dacă $(\frac{x}{d^2}, \frac{y}{d}, \frac{z}{d})$ e soluţie. Prin urmare, este suficient să găsim soluţiile cu componentele prime între ele. Fie $(x, y, z) \in (\mathbb{Z}^*)^3$ o astfel de soluţie. Notăm $R = \mathbb{Z}[i\sqrt{2}]$ (care, conform problemei 17, este un inel euclidian) şi căutăm pentru ecuaţia dată soluţii din R^3. Ecuaţia devine $(x + y^2 i\sqrt{2})(x - y^2 i\sqrt{2}) = 17z^4$. Fie δ un divizor prim (în R!) comun pentru $x + y^2\sqrt{2}$ şi $x - y^2 i\sqrt{2}$. Atunci $\delta|2x$ şi $\delta|2y^2 i\sqrt{2}$. Rezultă (vezi

problema 31) că $\delta = i\sqrt{2}$. Există deci un element $a + bi\sqrt{2} \in R$ astfel ca $x + y^2 i\sqrt{2} = i\sqrt{2}(a + bi\sqrt{2})$, de unde $x = -2b$. Rezultă imediat din ecuaţia iniţială că z e par, şi apoi că y e par, contradicţie. Rămâne deci că $x + y^2 i\sqrt{2}$ şi $x - y^2 i\sqrt{2}$ sunt prime între ele în R. Acum, în R are loc relaţia $17 = (3 + 2i\sqrt{2})(3 - 2i\sqrt{2})$. Cum (vezi problema 31) $3 \pm 2i\sqrt{2}$ sunt prime în R, rezultă că $3+2i\sqrt{2}$ divide $x+y^2 i\sqrt{2}$ sau $x-y^2 i\sqrt{2}$. Să presupunem pentru a fixa ideile că $3+2i\sqrt{2}|_R x+y^2 i\sqrt{2}$. Rezultă imediat că $3-2i\sqrt{2}|_R x-y^2 i\sqrt{2}$; avem

$$\frac{x + y^2 i\sqrt{2}}{3 + 2i\sqrt{2}} \cdot \frac{x - y^2 i\sqrt{2}}{3 - 2i\sqrt{2}} = z^4;$$

cum cei doi factori din membrul stâng sunt primi între ei, rezultă că fiecare din ei este asociat cu puterea a patra a unui element din R. Prin urmare, există $c, d \in \mathbb{Z}$ astfel încât $\pm(x+y^2 i\sqrt{2}) = (3+2i\sqrt{2})(c+di\sqrt{2})^4$. Dezvoltând şi identificând coeficienţii, obţinem

$$\pm x = 3c^4 - 36c^2d^2 + 12d^4 - 16c^3d + 32cd^3 \tag{12.1}$$

şi

$$\pm y^2 = 2c^4 - 24c^2d^2 + 8d^4 + 12c^3d - 24cd^3.$$

Din ultima relaţie rezultă că y e par; punem $y = 2y_1$ şi obţinem

$$\pm 2y_1^2 = c^4 - 12c^2d^2 + 4d^4 + 6c^3d - 12cd^3,$$

de unde obţinem c par; din relaţia (12.1) rezultă acum că x e par, contradicţie cu faptul că x şi y sunt prime între ele. Prin urmare, ecuaţia considerată admite numai soluţia $(0, 0, 0)$.

43. Vom începe cu câţiva paşi preliminari şi apoi vom trece la rezolvarea problemei. Notăm $\rho = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $R = \mathbb{Z}[\rho]$ şi $\lambda = 1 - \rho$ (conform problemei 40, λ este prim în R). Toate literele greceşti din demonstraţie vor desemna elemente din R; $\alpha|\beta$ va avea semnificaţia "α divide β în R", iar $\alpha \equiv \beta \pmod{\gamma}$ va însemna $\gamma|\alpha - \beta$.

1. Orice element din R este congruent cu $0, 1$ sau -1 modulo λ:
Fie $\omega = a + b\rho \in R$. Atunci $\omega = a + b - b(1 - \rho) \equiv a + b \pmod{\lambda}$. Se ştie că $a + b$ este de forma $3k + r$, cu $k \in \mathbb{Z}$ şi $r \in \{-1, 0, 1\}$. Cum $3 \sim_R \lambda^2$, rezultă că $\omega \equiv 0$ sau $\pm 1 \pmod{\lambda^2}$, deci $\omega \equiv 0$ sau $\pm 1 \pmod{\lambda}$. În plus, 0 şi ± 1 sunt resturi distincte modulo λ deoarece (vezi problema 1) λ nu divide în R elementele ± 1 şi ± 2.

2. Dacă $\omega \in R$ şi $\lambda \nmid_R \omega$, atunci $\omega \equiv \pm 1 \pmod{\lambda^4}$:
Fie $\omega \in R$, $\lambda \nmid_R \omega$. Conform cu pasul 1, $\omega \equiv \pm 1 \pmod{\lambda}$. Notăm cu α acel element din mulţimea $\{-\omega, \omega\}$ care este congruent cu $1 \pmod{\lambda}$. Există aşadar $\beta \in R$ astfel încât $\alpha = 1 + \beta\lambda$. Ţinând cont şi de $1 - \rho^2 = \lambda(1 + \rho) = -\lambda\rho^2$, putem scrie $\pm(\omega^3 \pm 1) = \alpha^3 - 1 = (\alpha - 1)(\alpha - \rho)(\alpha - \rho^2) = \beta\lambda(\beta\lambda + 1 - \rho)(\beta\lambda + 1 - \rho^2) = \lambda^3\beta(\beta + 1)(\beta - \rho^2)$. Dar $\rho^2 \equiv 1 \pmod{\lambda}$, deci $\beta - \rho^2 \equiv \beta - 1 \pmod{\lambda}$. Conform pasului 1, unul dintre elementele $\beta - 1, \beta$ şi $\beta + 1$ este divizibil cu λ. Prin urmare, $\pm(\omega^3 \pm 1) \equiv 0 \pmod{\lambda^4}$, deci $\omega^3 \equiv \pm 1 \pmod{\lambda^4}$.

3. Dacă $\xi^3 + \eta^3 + \zeta^3 = 0$, atunci unul dintre elementele ξ, η, ζ se divide cu λ:
Dacă presupunem că nici unul dintre aceste elemente nu se divide cu λ, atunci, conform pasului 2, cuburile lor sunt congruente cu $\pm 1 \pmod{\lambda^4}$. Astfel ar rezulta $\pm 1 \pm 1 \pm 1 \equiv 0 \pmod{\lambda^4}$, deci $\lambda^4|1$ sau $\lambda^4|3 \sim_R \lambda^2$, contradicţie.

Trecem acum la rezolvarea problemei. Să remarcăm că tripletele de forma $(k, 0, k)$ şi $(k, k, 0)$, $k \in \mathbb{Z}$, reprezintă soluţii ale ecuaţiei din enunţ (ele sunt aşa-numitele "soluţii triviale" ale ecuaţiei considerate).
Ne propunem în continuare să arătăm că nu mai există şi alte soluţii. Aceasta este o consecinţă a faptului că ecuaţia $\xi^3 + \eta^3 + \zeta^3 = 0$ nu are soluţii netriviale (adică cu toate componentele nenule) în inelul R, afirmaţie pe care o vom demonstra în cele ce urmează. Fie (ξ, η, ζ) o soluţie netrivială a acestei ecuaţii. Putem considera că ξ, η şi ζ sunt prime două câte două în R (altfel, simplificăm relaţia prin cubul c.m.m.d.c.-ului lor). Conform pasului

3, λ trebuie să dividă unul dintre elementele ξ, η, ζ. Să presupunem că $\lambda|\zeta$. Atunci, există $n \in \mathbb{N}^*$ şi $\gamma \in R$ astfel încât $\zeta = \lambda^n\gamma$, $\lambda \nmid \gamma$. În plus, $\lambda \nmid \xi$ şi $\lambda \nmid \eta$. Ţinând cont de aceste constatări, avem practic de demonstrat că relaţia $\xi^3 + \eta^3 + \lambda^{3n}\gamma^3 = 0$ este imposibilă în condiţiile în care ξ, η, γ nu se divid prin λ, iar $(\xi, \eta) = 1$. Vom arăta ceva mai mult, şi anume că relaţia $\xi^3 + \eta^3 + \varepsilon\lambda^{3n}\gamma^3 = 0$ este imposibilă în condiţiile în care ξ, η, γ nu se divid prin λ, $\varepsilon \in U(R)$, iar $(\xi, \eta) = 1$. Presupunem că relaţia $\xi^3 + \eta^3 + \varepsilon\lambda^{3n}\gamma^3 = 0$, $\varepsilon \in U(R)$, este satisfăcută de ξ, η, γ care îndeplinesc condiţiile de mai sus.
Constatăm pentru început că $n \geq 2$: Relaţia considerată duce la $-\varepsilon\lambda^{3n}\gamma^3 \equiv \xi^3 + \eta^3 \equiv \pm 1 \pm 1 \pmod{\lambda^4}$. Dar $\lambda \nmid \pm 2$, deci $-\varepsilon\lambda^{3n}\gamma^3 \equiv 0 \pmod{\lambda^4}$ şi cum $\lambda \nmid \gamma$, obţinem $n \geq 2$.
Revenim la relaţia $\xi^3 + \eta^3 + \varepsilon\lambda^{3n}\gamma^3 = 0$, pe care o rescriem $-\varepsilon\lambda^{3n}\gamma^3 = (\xi + \eta)(\xi + \rho\eta)(\xi + \rho^2\eta)$. Diferenţele dintre factorii din membrul drept al acestei relaţii sunt $\eta\lambda$, $\rho\eta\lambda$ şi $\rho^2\eta\lambda$, toate asociate cu $\eta\lambda$. Cum $\lambda \nmid \eta$, aceste diferenţe nu se divid prin λ^2. Deoarece $n \geq 2$, avem $3n > 3$, deci măcar unul dintre factori trebuie să se dividă cu λ^2; ceilalţi se vor divide cu λ (căci diferenţele se divid cu λ), dar nu se vor divide cu λ^2 (căci diferenţele nu se divid cu λ^2). Înlocuind eventual η cu $\rho\eta$ sau cu $\rho^2\eta$, putem presupune că $\lambda^2|\xi+\eta$. Există deci $\kappa_1, \kappa_2, \kappa_3 \in R$, nedivizibile cu λ, astfel ca $\xi+\eta = \lambda^{3n-2}\kappa_1$, $\xi + \rho\eta = \lambda\kappa_2$ şi $\xi + \rho^2\eta = \lambda\kappa_3$. Dacă $\delta \in R$ ar divide κ_2 şi κ_3, atunci δ ar divide $\rho\eta = \kappa_2 - \kappa_3$ şi $\rho\xi = \rho\kappa_3 - \rho^2\kappa_2$, deci δ ar divide η şi ξ, ceea ce (dat fiind că η şi ξ sunt prime între ele în R) conduce la $\delta \in U(R)$. Prin urmare, $(\kappa_2, \kappa_3) = 1$. În mod similar se arată că $(\kappa_1, \kappa_2) = (\kappa_1, \kappa_3) = 1$.
Cu aceste observaţii, relaţia $-\varepsilon\lambda^{3n}\gamma^3 = (\xi + \eta)(\xi + \rho\eta)(\xi + \rho^2\eta)$ conduce la $-\varepsilon\gamma^3 = \kappa_1\kappa_2\kappa_3$. Prin urmare, κ_1, κ_2 şi κ_3 sunt asociate cu cuburi din R. Există deci $\theta, \phi, \psi \in R$ şi $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in U(R)$ astfel încât $\kappa_1 = \varepsilon_1\theta^3$, $\kappa_2 = \varepsilon_2\phi^3$ şi $\kappa_3 = \varepsilon_3\psi^3$. În plus, $(\theta, \phi) = (\phi, \psi) = (\psi, \theta) = 1$, deoarece $\kappa_1, \kappa_2, \kappa_3$ sunt prime două câte două. Urmează că $0 = (1 - \rho^3)\lambda^{3n-3}\kappa_1 = (1 + \rho + \rho^2)\lambda^{3n-2}\kappa_1 = (1 + \rho + \rho^2)(\xi + \eta) = (\xi + \eta) + \rho(\xi + \rho\eta) + \rho^2(\xi + \rho^2\eta) = \varepsilon_1\lambda^{3n-2}\theta^3 + \varepsilon_2\rho\lambda\phi^3 + \varepsilon_3\rho^2\lambda\psi^3$. Prin urmare, $\phi^3 + \varepsilon_4\psi^3 + \varepsilon_5\lambda^{3n-3}\theta^3 = 0$, unde $\varepsilon_4 = \varepsilon_3\varepsilon_2^{-1}\rho$ şi $\varepsilon_5 = \varepsilon_1(\varepsilon_2\rho)^{-1}$ sunt evident unităţi ale lui R.
Dar $n \geq 2$, deci $\phi^3 + \varepsilon_4\psi^3 \equiv 0 \pmod{\lambda^3}$; cu atât mai mult $\phi^3 + \varepsilon_4\psi^3 \equiv 0 \pmod{\lambda^2}$. Pe de altă parte, cum $\lambda \nmid \phi$ şi $\lambda \nmid \psi$, avem, conform pasului 2, $\phi^3 \equiv \pm 1 \pmod{\lambda^4}$ şi $\psi^3 \equiv \pm 1 \pmod{\lambda^4}$; cu atât mai mult $\phi^3 \equiv \pm 1 \pmod{\lambda^2}$ şi $\psi^3 \equiv \pm 1 \pmod{\lambda^2}$. Prin urmare, $\pm 1 \pm \varepsilon_4 \equiv 0 \pmod{\lambda^2}$. Dar elementele $\pm 1 \pm \rho$ şi $\pm 1 \pm \rho^2$ sunt asociate fie cu 1, fie cu λ, prin urmare nu sunt divizibile cu λ^2. Rămâne deci că $\varepsilon_4 = \pm 1$.
Obţinem prin urmare $\phi^3 + (\pm\psi)^3 + \varepsilon_5\lambda^{3(n-1)}\theta^3 = 0$, adică o nouă relaţie de

tipul considerat, dar în care însă exponentul lui λ a scăzut cu 3. Aplicând acest procedeu de încă $n-2$ ori, vom obţine o relaţie de acelaşi tip, dar în care exponentul lui λ este 3, contradicţie cu observaţia făcută mai devreme că în orice astfel de relaţie exponentul lui λ este cel puţin 6. Prin urmare, presupunerea că ecuaţia considerată are soluţii netriviale în R este falsă.
În concluzie, ecuaţia $x^3+y^3=z^3$ nu are soluţii netriviale în R^3 (şi cu atât mai puţin în numere întregi).

44. Notaţiile pe care le vom folosi sunt cele din soluţia problemei 43.
Să observăm mai întâi că dacă în R are loc o relaţie de forma $\xi^3+\eta^3+5\zeta^3=0$ cu ξ,η şi ζ prime două câte două, atunci ζ se divide prin λ:
Să presupunem că ζ nu se divide prin λ. Atunci avem fie că $\lambda\nmid\xi$ şi $\lambda\nmid\eta$, deci (vezi soluţia problemei 43) cuburile acestora sunt congruente cu ±1 (mod λ^4) şi rezultă $\pm1\pm1\pm5\equiv0 \pmod{\lambda^4}$, deci $\lambda^4|5$ sau $\lambda^4|7$, de unde $81=N(\lambda^4)|N(5)=25$ sau $81=N(\lambda^4)|N(7)=49$, contradicţie, fie că unul dintre elementele ξ şi η, să zicem ξ, se divide cu λ, iar celălalt nu. În acest caz, vom avea $0\equiv\eta^3+5\zeta^3 \pmod{\lambda^3}$, deci $\pm1\pm5\equiv0 \pmod{\lambda^3}$. Se obţine $\lambda^3|4$ sau $\lambda^3|6$, ceea ce constatăm prin trecere la normă că este imposibil.
Să remarcăm acum că tripletele de forma $(k,-k,0)$ cu $k\in\mathbb{Z}$ reprezintă soluţii ale ecuaţiei din enunţ (ele sunt aşa-numitele "soluţii triviale" ale ecuaţiei considerate). Ne propunem în continuare să arătăm că nu există alte soluţii. Aceasta este o consecinţă a faptului că ecuaţia $\xi^3+\eta^3+5\zeta^3=0$ nu are soluţii netriviale (adică cu toate componentele nenule) în inelul R, afirmaţie pe care o vom demonstra în cele ce urmează. Fie (ξ,η,ζ) o soluţie netrivială a acestei ecuaţii. Putem considera că ξ,η şi ζ sunt prime două câte două în R (altfel, simplificăm relaţia prin cubul c.m.m.d.c.-ului lor). Conform celor de mai sus, λ trebuie să dividă ζ. Atunci, există $n\in\mathbb{N}^*$ şi $\gamma\in R$ astfel încât $\zeta=\lambda^n\gamma$, $\lambda\nmid\gamma$. În plus, $\lambda\nmid\xi$ şi $\lambda\nmid\eta$. Ţinând cont de aceste constatări, avem practic de demonstrat că relaţia $\xi^3+\eta^3+5\lambda^{3n}\gamma^3=0$ este imposibilă în condiţiile în care ξ,η,γ nu se divid prin λ, iar $(\xi,\eta)=1$. Vom arăta ceva mai mult, şi anume că relaţia $\xi^3+\eta^3+5\varepsilon\lambda^{3n}\gamma^3=0$ este imposibilă în condiţiile în care ξ,η,γ nu se divid prin λ, $\varepsilon\in U(R)$, iar $(\xi,\eta)=1$. Presupunem că relaţia $\xi^3+\eta^3+5\varepsilon\lambda^{3n}\gamma^3=0$, $\varepsilon\in U(R)$, este satisfăcută de ξ,η,γ care îndeplinesc condiţiile de mai sus.
Constatăm pentru început că $n\geq2$: Relaţia considerată duce la $-5\varepsilon\lambda^{3n}\gamma^3=\xi^3+\eta^3\equiv\pm1\pm1 \pmod{\lambda^4}$. Dar $\lambda\nmid\pm2$, deci $-5\varepsilon\lambda^{3n}\gamma^3\equiv0 \pmod{\lambda^4}$ şi cum $\lambda\nmid\gamma$, obţinem $n\geq2$.
Revenim la relaţia $\xi^3+\eta^3+5\varepsilon\lambda^{3n}\gamma^3=0$, pe care o rescriem $-5\varepsilon\lambda^{3n}\gamma^3=$

$(\xi+\eta)(\xi+\rho\eta)(\xi+\rho^2\eta)$. Diferenţele dintre factorii din membrul drept al acestei relaţii sunt $\eta\lambda$, $\rho\eta\lambda$ şi $\rho^2\eta\lambda$, toate asociate cu $\eta\lambda$. Cum $\lambda \nmid \eta$, aceste diferenţe nu se divid prin λ^2. Deoarece $n \geq 2$, avem $3n > 3$, deci măcar unul dintre factori trebuie să se dividă cu λ^2; ceilalţi se vor divide cu λ (căci diferenţele se divid cu λ), dar nu se vor divide cu λ^2 (căci diferenţele nu se divid cu λ^2). Înlocuind eventual η cu $\rho\eta$ sau cu $\rho^2\eta$, putem presupune că $\lambda^2|\xi+\eta$. Există prin urmare $\kappa_1, \kappa_2, \kappa_3 \in R$, nedivizibile cu λ, astfel ca $\xi+\eta = \lambda^{3n-2}\kappa_1$, $\xi+\rho\eta = \lambda\kappa_2$ şi $\xi+\rho^2\eta = \lambda\kappa_3$. Dacă $\delta \in R$ ar divide κ_2 şi κ_3, atunci δ ar divide $\rho\eta = \kappa_2 - \kappa_3$ şi $\rho\xi = \rho\kappa_3 - \rho^2\kappa_2$, deci δ ar divide η şi ξ, ceea ce (dat fiind că η şi ξ sunt prime între ele în R) duce la $\delta \in U(R)$. Prin urmare, $(\kappa_2, \kappa_3) = 1$. În mod similar se arată că $(\kappa_1, \kappa_2) = (\kappa_1, \kappa_3) = 1$.
Cu aceste observaţii, relaţia $-5\varepsilon\lambda^{3n}\gamma^3 = (\xi+\eta)(\xi+\rho\eta)(\xi+\rho^2\eta)$ ne conduce la $-5\varepsilon\gamma^3 = \kappa_1\kappa_2\kappa_3$. Prin urmare, există $\theta, \phi, \psi \in R$ şi $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in U(R)$ astfel încât să aibă loc una dintre următoarele situaţii:
1. $\kappa_1 = 5\varepsilon_1\theta^3$,$\kappa_2 = \varepsilon_2\phi^3$ şi $\kappa_3 = \varepsilon_3\psi^3$,
2. $\kappa_1 = \varepsilon_1\theta^3$, $\kappa_2 = 5\varepsilon_2\phi^3$ şi $\kappa_3 = \varepsilon_3\psi^3$,
3. $\kappa_1 = \varepsilon_1\theta^3$, $\kappa_2 = \varepsilon_2\phi^3$ şi $\kappa_3 = 5\varepsilon_3\psi^3$.
În plus, $(\theta, \phi) = (\phi, \psi) = (\psi, \theta) = 1$, deoarece $\kappa_1, \kappa_2, \kappa_3$ sunt prime două câte două.
Pe de altă parte, $0 = (1-\rho^3)\lambda^{3n-3}\kappa_1 = (1+\rho+\rho^2)\lambda^{3n-2}\kappa_1 = (1+\rho+\rho^2)(\xi+\eta) = (\xi+\eta) + \rho(\xi+\rho\eta) + \rho^2(\xi+\rho^2\eta)$. Studiem ce se obţine din această relaţie în fiecare din cazurile de mai sus.
În cazul 1 se obţine $5\varepsilon_1\lambda^{3n-2}\theta^3 + \varepsilon_2\rho\lambda\phi^3 + \varepsilon_3\rho^2\lambda\psi^3 = 0$. Prin urmare, $\phi^3 + \varepsilon_4\psi^3 + 5\varepsilon_5\lambda^{3n-3}\theta^3 = 0$, unde $\varepsilon_4 = \varepsilon_3\varepsilon_2^{-1}\rho$ şi $\varepsilon_5 = \varepsilon_1(\varepsilon_2\rho)^{-1}$ sunt evident unităţi ale lui R. Dar $n \geq 2$, deci $\phi^3 + \varepsilon_4\psi^3 \equiv 0 \pmod{\lambda^3}$; cu atât mai mult $\phi^3 + \varepsilon_4\psi^3 \equiv 0 \pmod{\lambda^2}$. Pe de altă parte, cum $\lambda \nmid \phi$ şi $\lambda \nmid \psi$, avem (vezi soluţia problemei 43) $\phi^3 \equiv \pm 1 \pmod{\lambda^4}$ şi $\psi^3 \equiv \pm 1 \pmod{\lambda^4}$; cu atât mai mult $\phi^3 \equiv \pm 1 \pmod{\lambda^2}$ şi $\psi^3 \equiv \pm 1 \pmod{\lambda^2}$. Prin urmare, $\pm 1 \pm \varepsilon_4 \equiv 0 \pmod{\lambda^2}$. Dar elementele $\pm 1 \pm \rho$ şi $\pm 1 \pm \rho^2$ sunt asociate fie cu 1, fie cu λ, prin urmare nu sunt divizibile cu λ^2. Rămâne deci că $\varepsilon_4 = \pm 1$.
În cazul 3 se obţine $\varepsilon_1\lambda^{3n-2}\theta^3 + 5\varepsilon_2\rho\lambda\phi^3 + \varepsilon_3\rho^2\lambda\psi^3 = 0$ şi prin urmare, $\phi^3 + 5\varepsilon_4\psi^3 + \varepsilon_5\lambda^{3n-3}\theta^3 = 0$, unde $\varepsilon_4 = \varepsilon_3\varepsilon_2^{-1}\rho$ şi $\varepsilon_5 = \varepsilon_1(\varepsilon_2\rho)^{-1}$ sunt evident unităţi ale lui R. Dar $n \geq 2$, deci $\phi^3 + 5\varepsilon_4\psi^3 \equiv 0 \pmod{\lambda^3}$. Pe de altă parte, cum $\lambda \nmid \phi$ şi $\lambda \nmid \psi$, avem (vezi soluţia problemei 43) $\phi^3 \equiv \pm 1 \pmod{\lambda^4}$ şi $\psi^3 \equiv \pm 1 \pmod{\lambda^4}$; cu atât mai mult $\phi^3 \equiv \pm 1 \pmod{\lambda^3}$ şi $\psi^3 \equiv \pm 1 \pmod{\lambda^3}$. Prin urmare, $\pm 1 \pm 5\varepsilon_4 \equiv 0 \pmod{\lambda^3}$. Dar elementele $\pm 1 \pm 5$, $\pm 1 \pm 5\rho$ şi $\pm 1 \pm 5\rho^2$ au norme nedivizibile prin 27, deci nu sunt divizibile cu λ^3. Acest caz este deci imposibil.

În cazul 2 se procedează în mod similar şi se trage concluzia că nici acest caz nu este posibil.
Singura variantă rămasă în discuţie este prin urmare cea obţinută în cazul 1. Ea conduce la relaţia $\phi^3 + (\pm\psi)^3 + 5\varepsilon_5\lambda^{3(n-1)}\theta^3 = 0$, adică o nouă relaţie de tipul considerat, în care însă exponentul lui λ a scăzut cu 3. Aplicând acest procedeu de încă $n-2$ ori, vom obţine o relaţie de acelaşi tip, dar în care exponentul lui λ este 3, contradicţie cu observaţia făcută mai sus că în orice astfel de relaţie exponentul lui λ este cel puţin 6. Prin urmare, presupunerea că ecuaţia considerată are soluţii netriviale în R este falsă.
În concluzie, ecuaţia $x^3 + y^3 = z^3$ nu are soluţii netriviale în R^3 (şi cu atât mai puţin în numere întregi).

45. (i) Considerăm polinoamele în $K[Y,Z][X]$. Ele sunt monice, deci primitive. Pentru $X^2 - Y$ şi $X^2 - YZ^2$ aplicăm criteriul lui Eisenstein cu $p = Y$. Avem că Y este element prim deoarece (vezi problema 13 din Capitolul 5) $K[X,Y,Z]/(Y) \simeq K[X,Z]$ care este inel integru. Pentru $X^2 - Y^2Z$ aplicăm criteriul lui Eisenstein cu $p = Z$.
(ii) Gândim $K[X,Y] \simeq K[Y][X]$ şi aplicăm criteriul lui Eisenstein cu $p = Y - 1$, care se arată că este prim la fel ca la (i). În plus, $X^2 + Y^2 - 1$ este primitiv deoarece coeficientul lui X^2 este 1.

46. (i) Notăm $f = X^r + Y^s$. Să presupunem că $f = gh$ cu $g, h \in K[X,Y]$ neinversabile. Scriem $g = g_0 + g_1X + \cdots + g_kX^k$ şi $h = h_0 + h_1X + \cdots + h_lX^l$, unde $g_i \in K[Y]$ pentru orice $i \in \{1,\ldots,k\}$, $h_j \in K[Y]$ pentru orice $j \in \{1,\ldots,l\}$ şi constatăm că $l = \text{grad}_X(h) \leq r$ şi $k = \text{grad}_X(g) \leq r$. Cu consideraţii similare găsim $m = \text{grad}_Y(g) \leq s$ şi $n = \text{grad}_Y(h) \leq s$. De fapt, inegalităţile apărute sunt chiar stricte, căci dacă, de exemplu $f = g(X)h(X,Y)$, rezultă că $\text{grad}_Y(h) = s$ şi, dacă notăm coeficientul dominant al lui $h \in K[X][Y]$ cu $\overline{h}(X)$, $g(X)\overline{h}(X) = 1$, ceea ce arată că $g(X)$ este inversabil, contradicţie.
Acum scriem $g = \sum_{0\leq i\leq k, 0\leq j\leq l} g_{ij}X^iY^j$ şi $h = \sum_{0\leq i\leq m, 0\leq j\leq n} h_{ij}X^iY^j$, $g_{ij}, h_{ij} \in K$. Cum r şi s sunt prime între ele, unul dintre ele este impar, să zicem s. Atunci, în inelul de polinoame $K[U]$ avem relaţia $g(U^s, -U^r)h(U^s, -U^r) = f(U^s, -U^r) = 0$. Pe de altă parte, $g(U^s, -U^r) = \sum_{0\leq i\leq k, 0\leq j\leq l} (-1)^j g_{ij}U^{is+jr}$ iar $h(U^r, -U^s) = \sum_{0\leq i\leq m, 0\leq j\leq n} (-1)^j h_{ij}U^{is+jr}$. Dar $i_1s + j_1r = i_2s + j_2r \Leftrightarrow (i_1 - i_2)s = (j_2 - j_1)r$, de unde $i_1 \equiv i_2 \pmod r$ şi $j_1 \equiv j_2 \pmod s$. Dar

$i_1, i_2 \in \{0, 1, \ldots, r-1\}$ şi $j_1, j_2 \in \{0, 1, \ldots, s-1\}$, deci în situaţia dată $i_1 s + j_1 r = i_2 s + j_2 r \Leftrightarrow i_1 = i_2$ şi $j_1 = j_2$. În concluzie, la termeni diferiţi din g şi h corespund termeni diferiţi în $g(U^s, -U^r)$ şi $h(U^s, -U^r)$. Prin urmare, termenii din g, respectiv h nu se pot reduce când facem $X = U^r$ şi $Y = -U^s$. Atunci $g(U^s, -U^r) \neq 0 \neq h(U^s, -U^r)$, contradicţie cu $g(U^s, -U^r)h(U^s, -U^r) = f(U^s, -U^r) = 0$.
(ii) Notăm $f = X^r + Y^s + Z^t$. Aplicăm criteriul reducerii: considerăm $\varphi : K[Y, Z] \to K[Y], \varphi(g) = g(Y, 0)$. Extindem pe φ la un morfism $\overline{\varphi} : K[Y, Z][X] \to K[Y][X]$ cu proprietatea $\overline{\varphi}(X) = X$ şi observăm că $\overline{\varphi}(f) = X^r + Y^s$. Din $r \equiv 1 \pmod{st}$ rezultă că $(r, s) = 1$, deci, conform (i), $\overline{\varphi}(f) \in K[Y][X]$ este ireductibil. În plus, $\text{grad}_X(\overline{\varphi}(f)) = r = \text{grad}_X(f)$, deci conform criteriului reducerii f este ireductibil în $K(Y, Z)[X]$. Cum f este în mod clar primitiv, rezultă că el este ireductibil în $K[Y, Z][X] \simeq K[X, Y, Z]$.

47. (i) Conform problemei 39, 5 este element prim în $\mathbb{Z}[\sqrt{3}]$. Aplicăm criteriul lui Eisenstein cu $p = 5$ şi obţinem ireductibilitatea lui f în $\mathbb{Q}[\sqrt{3}][X]$. Cum $(\sqrt{3}, 25) = 1$, f este şi primitiv, deci este ireductibil şi în $\mathbb{Z}[\sqrt{3}][\text{X}]$.
(ii) Începem prin a observa că polinomul $X^3 + 6X + 2$ este ireductibil în $\mathbb{Q}[X]$ (are gradul 3 şi nu are rădăcini raţionale) şi primitiv peste $\mathbb{Z}$, deci este ireductibil în $\mathbb{Z}[X]$. Cum $\mathbb{Z}[X]$ este factorial, $X^3 + 6X + 2$ este chiar prim în acest inel. Atunci, constatând că $f \in \mathbb{Z}[X, Y]$ se poate scrie sub forma $(X+1)Y^4 - 2(X^3 + 6X + 2)Y^3 + X(X^3 + 6X + 2)Y^2 + X^2(X^3 + 6X + 2)$, îi aplicăm criteriul lui Eisenstein cu $p = X^3 + 6X + 2$. Rezultă că f este ireductibil peste $\mathbb{Q}[X]$. Cum însă coeficienţii $X + 1$ şi $-2(X^3 + 6X + 2)$ sunt primi între ei, f este şi primitiv. Prin urmare, f este ireductibil în $\mathbb{Z}[X, Y]$.

48. (i) f este ireductibil în $\mathbb{Q}[X]$ conform criteriului lui Eisenstein (aplicat pentru inelul factorial $\mathbb{Z}$ şi elementul prim $p = 2$). Cum în plus f este primitiv, rezultă că el este ireductibil şi în $\mathbb{Z}[X]$.
(ii) Aplicaţia $\Phi : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $\Phi(h) = h(X + 1)$ este evident un morfism de inele unitare. Analog $\Psi : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $\Psi(h) = h(X - 1)$ este morfism de inele unitare şi este inversul lui Φ, deci Φ este izomorfism. Prin urmare, f este ireductibil dacă şi numai dacă $\Phi(f) = f(X + 1)$ este ireductibil. Avem însă

$$f(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = \sum_{k=1}^{p} C_p^k X^{k-1}.$$

Din scrierea

$$C_p^j = \frac{p!}{j!(p-j)!} = \frac{p(p-1)\cdots(p-j+1)}{j(j-1)\cdots 1},$$

se obţine $j(j-1)\cdots 1 \cdot C_p^j = p(p-1)\cdots(p-j+1)$ şi deci p divide unul din factorii produsului din membrul stâng al egalităţii iar singurul posibil este C_p^j. În concluzie, $p|C_p^j$ pentru orice $j \in \{1,\ldots,p-1\}$. Prin urmare, $f(X+1) \in \mathbb{Z}[X]$ verifică condiţiile pentru aplicarea criteriului lui Eisenstein (în raport cu elementul prim $p \in \mathbb{Z}$). Se obţine că $f(X+1)$ este ireductibil peste $\mathbb{Q}$. Fiind monic este şi primitiv, deci este ireductibil peste $\mathbb{Z}$. Conform celor de mai sus, $f \in \mathbb{Z}[X]$ este la rândul său ireductibil.

(iii) Cu notaţiile de la punctul (ii), $\Phi(f) = \sum_{k=1}^{p^n} C_{p^n}^k X^k + p$. Pentru $j \in \{1,2,\ldots,p^n-1\}$ avem

$$C_{p^n}^j = \frac{p^n(p^n-1)\cdots(p^n-j+1)}{j!} = \frac{p^n}{j}\cdot\frac{p^n-1}{1}\cdot\frac{p^n-2}{2}\cdots\frac{p^n-(j-1)}{j-1}.$$

Fiecare $i \in \{1,2,\ldots,j\}$ se poate reprezenta sub forma $p^{t_i}h_i$, unde $t_i \in \mathbb{N}$, $t_i < n$ iar h_i nu se divide cu p. Atunci

$$C_{p^n}^j = \frac{p^n}{j}\prod_{i=1}^{j-1}\frac{p^n-i}{i} = \frac{p^n}{p^{t_j}h_j}\prod_{i=1}^{j-1}\frac{p^{n-t_i}-h_i}{h_i}.$$

Membrul drept al relaţiei de mai sus, fiind egal cu $C_{p^n}^j$, trebuie să fie întreg. Pe de altă parte, singurele numere divizibile cu p care apar în el sunt p^n şi p^{t_j}. Prin urmare, după ce facem toate simplificările posibile, obţinem un număr întreg divizibil prin p^{n-t_j}. Cum $t_j < n$, tragem concluzia că fiecare coeficient binomial $C_{p^n}^j$, $j \in \{1,\ldots,p^n-1\}$, este divizibil cu p. În consecinţă, lui $f(X+1) \in \mathbb{Z}[X]$ i se poate aplica criteriul lui Eisenstein (în raport cu elementul prim $p \in \mathbb{Z}$). Se deduce că $f(X+1)$ este ireductibil în $\mathbb{Q}[X]$. Fiind monic, este şi primitiv, deci este ireductibil şi peste $\mathbb{Z}$. Rezultă aşadar că $f \in \mathbb{Z}[X]$ este la rândul său ireductibil.

(iv) Aplicăm criteriul reducerii. Considerăm morfismul canonic $\pi : \mathbb{Z} \to \mathbb{Z}_p$, $\pi(x) = \widehat{x}$ şi extinsul său $\overline{\pi} : \mathbb{Z}[X] \to \mathbb{Z}_p[X]$. Este suficient să demonstrăm că polinomul $\overline{f} = \overline{\pi}(f)$, $\overline{f} = X^p - X + \widehat{a}$ este ireductibil în $\mathbb{Z}_p[X]$. Fie K o extindere a lui $\mathbb{Z}_p$ în care $\overline{f}$ are o rădăcină (vezi problema 39 din Capitolul 5) şi fie $\alpha \in K$ o rădăcină a lui $\overline{f}$. În grupul multiplicativ $\mathbb{Z}_p \setminus \{0\}$ (de ordin $p-1$) orice element $\widehat{x}$ are proprietatea $\widehat{x}^{p-1} = 1$, deci pentru orice $\widehat{k} \in \mathbb{Z}_p$

avem relaţia $\widehat{k}^p = \widehat{k}$. De aici rezultă că $\alpha, \alpha+\widehat{1}, \ldots, \alpha+\widehat{p-1}$ sunt şi ele rădăcini pentru $\overline{f}$. Fiind în număr de p, ele sunt de fapt toate rădăcinile polinomului $\overline{f}$. Presupunem acum că $\overline{f}$ este reductibil în $\mathbb{Z}_p[X]$. Există atunci două polinoame neconstante $g, h \in \mathbb{Z}_p[X]$ pentru care $\overline{f} = gh$. De aici obţinem $(X-\alpha)(X-\alpha-\widehat{1})\cdots(X-\alpha-\widehat{(p-1)}) = gh$, adică g este de forma $(X-\alpha-\widehat{k_1})(X-\alpha-\widehat{k_2})\cdots(X-\alpha-\widehat{k_s})$, $1 \leq s < p$. Atunci elementul $(\alpha+\widehat{k_1})+(\alpha+\widehat{k_2})+\cdots+(\alpha+\widehat{k_s})$, care este coeficientul lui X^{s-1} din scrierea lui g, aparţine lui $\mathbb{Z}_p$. Urmează $s\alpha \in \mathbb{Z}_p$, de unde, cum $p \nmid s$, $\alpha \in \mathbb{Z}_p$. Acum, pe de o parte $\overline{f}(\alpha) = \widehat{0}$, deci $\alpha^p - \alpha + \widehat{a} = \widehat{0}$, iar pe de alta, $\alpha^p - \alpha = \widehat{0}$. Rezultă $\widehat{a} = \widehat{0}$, adică $p|a$, contradicţie.

49. (i) Considerăm morfismul canonic $\pi : \mathbb{Z} \to \mathbb{Z}_2$, $\pi(a) = \widehat{a}$, şi extinsul său $\overline{\pi} : \mathbb{Z}[X] \to \mathbb{Z}_2[X]$ (pentru orice $h \in \mathbb{Z}[X]$ vom nota $\overline{\pi}(h)$ cu $\overline{h}$). Atunci $\overline{f} = (X^4+X^3+1)^n$. Dacă presupunem că f admite o descompunere relevantă peste $\mathbb{Z}$, fie ea $f = gh$, atunci (cum gradul lui f nu scade când îi reducem coeficienţii modulo 2 iar g sau h nu pot fi constante căci f este polinom primitiv) există $p, q \in \mathbb{N}^*$ cu $p+q = n$ astfel ca $\overline{g} = (X^4+X^3+1)^p$ şi $\overline{h} = (X^4+X^3+1)^q$. Rezultă că $f = [(X^4+X^3+1)^p+2g_1][(X^4+X^3+1)^q+2h_1]$. Înmulţim şi obţinem $(X^4+X^3+1)^n+4(X^4+X^3+1)^m+2 = (X^4+X^3+1)^{p+q}+2(X^4+X^3+1)^p h_1+2(X^4+X^3+1)^q g_1+4g_1h_1$, de unde $2(X^4+X^3+1)^m+1 = (X^4+X^3+1)^p h_1+(X^4+X^3+1)^q g_1+2g_1h_1$. Aplicând din nou $\overline{\pi}$, obţinem în $\mathbb{Z}_2[X]$ relaţia contradictorie $1 = (X^4+X^3+1)^p\overline{h_1}+(X^4+X^3+1)^q\overline{g_1}$. Rămâne aşadar că f este ireductibil peste $\mathbb{Z}$ (deci şi peste $\mathbb{Q}$).
(ii) Polinomul $f = X^4+3X^3+3X^2-5$ nu are rădăcini raţionale, deoarece nici unul dintre divizorii lui 5 nu este rădăcină. Prin urmare, el fiind şi primitiv, singurul mod în care s-ar putea descompune este ca produs de două polinoame (ireductibile) de gradul al doilea. Fie $f = gh$ o astfel de descompunere a lui f în $\mathbb{Z}[X]$. Reducem această relaţie modulo 2 şi obţinem în $\mathbb{Z}_2[X]$ relaţia $X^4+X^3+X^2+1 = \overline{f} = \overline{g}\,\overline{h}$. Cum $4 = \mathrm{grad}\overline{g}+\mathrm{grad}\overline{h} \leq \mathrm{grad}g+\mathrm{grad}h = 4$, obţinem $\mathrm{grad}\overline{g} = \mathrm{grad}\overline{h} = 2$. Pe de altă parte, în inelul euclidian $\mathbb{Z}_2[X]$ polinomul $\overline{f}$ are descompunerea unică în factori primi $\overline{f} = (X+1)(X^3+X+1)$, contradicţie. Rămâne deci că f este ireductibil.

50. Dacă $n = 1$, $f = X_1^2$, care este în mod evident reductibil. Dacă $n = 2$, atunci $f = (X_1+iX_2)(X_1-iX_2)$, deci este reductibil. Pentru $n = 3$, considerăm $f \in K[X_1, X_2][X_3]$ şi, constatând că f este primitiv, aplicăm criteriul lui Eisenstein cu $p = X_2+iX_3$ (care este prim în $K[X_2, X_3]$

deoarece, conform problemei 13 din Capitolul 5, $K[X_2, X_3]/(X_2 + iX_3) \simeq K[X_3][X_2]/(X_2 + iX_3) \simeq K[X_3]$, care este inel integru).
Fie acum $k \geq 3$. Să presupunem că $X_1^2 + \cdots + X_k^2$ este ireductibil în $K[X_1, \ldots, X_k]$. Atunci, lui $X_1^2 + \cdots + X_{k+1}^2 = X_{k+1}^2 + (X_1^2 + \cdots + X_k^2) \in K[X_1, X_2, \ldots, X_{k+1}] \simeq K[X_1, X_2, \ldots, X_k][X_{k+1}]$, care constatăm că este primitiv deoarece este monic, îi aplicăm criteriul lui Eisenstein cu $p = X_1^2 + \cdots + X_k^2$ şi constatăm că este ireductibil, ceea ce încheie pasul de inducţie şi demonstraţia.

51. Să notăm $f = X^4 + 1 \in \mathbb{Z}[X]$. Este evident că funcţia $\Phi : \mathbb{Z}[X] \to \mathbb{Z}[X], \Phi(g) = g(X + 1)$ este un automorfism al inelului $\mathbb{Z}[X]$. Prin urmare, un polinom g este ireductibil dacă şi numai dacă $g(X + 1) = \Phi(g)$ este ireductibil. Pentru polinomul dat avem $f(X + 1) = X^4 + 4X^3 + 6X^2 + 4X + 2$, care este ireductibil peste $\mathbb{Q}$ conform criteriului lui Eisenstein (pentru $p = 2$). Prin urmare, $f(X+1)$ fiind primitiv, este ireductibil şi peste $\mathbb{Z}$. În concluzie, f este la rândul său ireductibil peste $\mathbb{Z}$.
Dacă $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, atunci, conform lemei din soluţia problemei 37, există $a \in \mathbb{Z}$ astfel încât $a^2 \equiv -1 \pmod{p}$. În acest caz, în $\mathbb{Z}_p[X]$ avem descompunerea $X^4 + 1 = (X^2 - a)(X^2 + a)$. Dacă $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, atunci, conform lemei din soluţia problemei 37, există $b \in \mathbb{Z}$ astfel încât $b^2 \equiv 2 \pmod{p}$. În acest caz în $\mathbb{Z}_p[X]$ avem $X^4 + 1 = X^4 + 2X^2 + 1 - 2X^2 = (X^2 - bX + 1)(X^2 + bX + 1)$. În fine, dacă nu suntem în nici una din situaţiile de mai sus, atunci (vezi demonstraţia lemei din soluţia problemei 37) $(-1)^{\frac{p-1}{2}} \equiv 2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ şi atunci $(-2)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, deci există $c \in \mathbb{Z}$ astfel ca $c^2 \equiv -2 \pmod{p}$. Peste $\mathbb{Z}_p$ avem atunci descompunerea $X^4+1 = X^4-2X^2+1-(-2X^2) = (X^2+cX+1)(X^2-cX+1)$ şi demonstraţia este încheiată.

52. Procedăm prin inducţie după n. Pentru $n = 1$, $f_1 = X_{11}$, care este în mod evident ireductibil. Presupunem acum că f_k este ireductibil. Avem relaţia $f_{k+1} = X_{k+1,1}A_{k+1,1} + \cdots + X_{k+1,k+1}A_{k+1,k+1}$, unde A_{ij} desemnează complementul algebric al lui X_{ij} din matricea

$$\begin{pmatrix} X_{11} & X_{12} & \ldots & X_{1,k+1} \\ X_{21} & X_{22} & \ldots & X_{2,k+1} \\ \vdots & \vdots & & \vdots \\ X_{k+1,1} & X_{k+1,2} & \ldots & X_{k+1,k+1} \end{pmatrix}.$$

Să observăm că $A_{k+1,k+1} = f_k$. Cum f_{k+1} are gradul unu în $X_{k+1,k+1}$, rezultă că este ireductibil în $Q(\mathbb{Z}[\{X_{ij}|i,j \in \{1,\ldots,k+1\}\} \setminus \{X_{k+1,k+1}\}])[X_{k+1,k+1}]$. Este suficient deci să arătăm că este primitiv în $\mathbb{Z}[\{X_{ij}|i,j \in \{1,\ldots,k+1\}\} \setminus \{X_{k+1,k+1}\}][X_{k+1,k+1}]$. Presupunând că nu este primitiv, rezultă (ţinând cont că f_k este ireductibil din ipoteza de inducţie) că $f_k | X_{k+1,1}A_{k+1,1} + \cdots + X_{k+1,k}A_{k+1,k}$, ceea ce revine la $f_k | A_{k+1,j}$ pentru orice $j \in \{1,\ldots,k\}$. Dar aceste relaţii sunt contradictorii, deoarece dacă facem $X_{1j} = \cdots = X_{kj} = 0$, f_k se anulează, iar $A_{k+1,j}$ nu se anulează. Rămâne că f_{k+1} este primitiv în $\mathbb{Z}[\{X_{ij}|i,j \in \{1,\ldots,k+1\}\} \setminus \{X_{k+1,k+1}\}][X_{k+1,k+1}]$ şi demonstraţia este încheiată.

53. Procedăm prin inducţie după n. Pentru $n = 1, f_1 = X_{11}$, care este în mod evident ireductibil. Presupunem acum că f_k este ireductibil. Avem relaţia $f_{k+1} = X_{1,k+1}A_{k+1,1} + \cdots + X_{k+1,k+1}A_{k+1,k+1}$, unde A_{ij} desemnează complementul algebric al elementului de pe poziţia i,j din matricea

$$\begin{pmatrix} X_{11} & X_{12} & \ldots & X_{1,k+1} \\ X_{12} & X_{22} & \ldots & X_{2,k+1} \\ \vdots & \vdots & & \vdots \\ X_{1,k+1} & X_{2,k+1} & \ldots & X_{k+1,k+1} \end{pmatrix}.$$

Să observăm că $A_{k+1,k+1} = f_k$. Cum f_{k+1} are gradul unu în $X_{k+1,k+1}$, el este ireductibil în $Q(\mathbb{Z}[\{X_{ij}|i,j \in \{1,\ldots,k+1\}, i \leq j\} \setminus \{X_{k+1,k+1}\}])[X_{k+1,k+1}]$. Este deci suficient să arătăm că este primitiv în $\mathbb{Z}[\{X_{ij}|i,j \in \{1,\ldots,k+1\}, i \leq j\} \setminus \{X_{k+1,k+1}\}][X_{k+1,k+1}]$. Presupunând că nu este primitiv, rezultă (ţinând cont că f_k este ireductibil din ipoteza de inducţie) că $f_k | X_{1,k+1}A_{k+1,1} + \cdots + X_{k,k+1}A_{k+1,k}$, ceea ce revine la $f_k | A_{j,k+1}$ pentru orice $j \in \{1,\ldots,k\}$. Dar aceste relaţii sunt contradictorii, deoarece, dacă facem $X_{1j} = \cdots = X_{jj} = X_{j,j+1} = \cdots = X_{jk} = 0$, f_k se anulează, iar $A_{k+1,j}$ nu se anulează. Rămâne că f_{k+1} este primitiv în $\mathbb{Z}[\{X_{ij}|i,j \in \{1,\ldots,k+1\}, i \leq j\} \setminus \{X_{k+1,k+1}\}][X_{k+1,k+1}]$ şi demonstraţia este încheiată.

54. Procedăm prin inducţie după n. Pentru $n = 1, f_1 = X_1$, care este în mod evident ireductibil. Presupunem acum că f_k este ireductibil. Avem relaţia $f_{k+1} = X_{k+1}A_{k+1,1} + \cdots + X_{2k}A_{k+1,k+1} + X_{2k+1}A_{k+1,k+1}$, unde A_{ij} desemnează complementul algebric al elementului de pe poziţia i,j din ma-

tricea

$$\begin{pmatrix} X_1 & X_2 & \dots & X_{k+1} \\ X_2 & X_3 & \dots & X_{k+2} \\ \vdots & \vdots & & \vdots \\ X_{k+1} & X_{k+2} & \dots & X_{2k+1} \end{pmatrix}.$$

Să observăm că $A_{k+1,k+1} = f_k$. Cum f_{k+1} are gradul unu în X_{2k+1}, rezultă că este ireductibil în $Q(\mathbb{Z}[X_1, \dots, X_{2k}])[X_{2k+1}]$. Este deci suficient să arătăm că este primitiv în $\mathbb{Z}[X_1, \dots, X_{2k}][X_{2k+1}]$. Presupunând că nu este primitiv, rezultă (ţinând cont că f_k este ireductibil din ipoteza de inducţie) că $f_k | X_{k+1}A_{k+1,1} + \dots + X_{2k}A_{k+1,k}$, ceea ce revine la $f_k | A_{j,k+1}$ pentru orice $j \in \{1, \dots, k\}$. Dar aceste relaţii sunt contradictorii, deoarece, dacă facem $X_j = X_{j+1} = \dots = X_{j+k-1} = 0$, f_k se anulează, iar $A_{k+1,j}$ nu se anulează. Rămâne că f_{k+1} este primitiv în $\mathbb{Z}[X_1, \dots, X_{2k}][X_{2k+1}]$ şi demonstraţia este încheiată.

55. Notăm $g_n = \sum_{i=1}^{n} T_i f_i$. Vom demonstra afirmaţia prin inducţie după n. Pentru $n = 2$, polinomul $T_1 f_1 + T_2 f_2 \in R[T_1, T_2] \simeq k[X_1, \dots, X_q, T_1][T_2]$ este primitiv deoarece $(T_1 f_1, f_2) = 1$ şi este ireductibil în $k(X_1, \dots, X_q, T_1)[T_2]$ deoarece are gradul unu. Dar $k[X_1, \dots, X_q, T_1]$ este inel factorial. Prin urmare, conform lemei lui Gauss, $g_2 = T_1 f_1 + T_2 f_2$ este ireductibil în $R[T_1, T_2]$. Fie acum $n \geq 2$. Presupunem că g_n este ireductibil. Considerăm $g_{n+1} = f_{n+1}T_{n+1} + g_n \in k[X_1, \dots, X_q][T_1, \dots, T_n][T_{n+1}]$, ţinem seama de faptul că are loc izomorfismul

$$k[X_1, \dots, X_q][T_1, \dots, T_n][T_{n+1}] \simeq k[X_1, \dots, X_q, T_1, \dots, T_n][T_{n+1}]$$

şi constatăm că g_{n+1} este primitiv (avem $(T_{n+1}f_{n+1}, g_n) = 1$ deoarece T_{n+1} nu apare în g_n iar orice divizor comun între f_{n+1} şi g_n trebuie să dividă $(f_1, \dots, f_{n+1}) = 1$) şi ireductibil în $k(X_1, \dots, X_q, T_1, \dots, T_n)[T_{n+1}]$ deoarece are gradul unu.
Dar $k[X_1, \dots, X_q, T_1, \dots, T_n]$ este inel factorial. Prin urmare, conform lemei lui Gauss, g_{n+1} este ireductibil în $R[T_1, \dots, T_{n+1}]$, ceea ce încheie pasul de inducţie şi demonstraţia.

Bibliografie

[1] T. Albu, I. D. Ion, *Capitole de teoria algebrică a numerelor*, Editura Academiei R. S. R., 1984.

[2] T. Albu, Ş. Raianu, *Lecţii de algebră comutativă*, Tipografia Universităţii din Bucureşti, 1984.

[3] M. Becheanu, C. Vraciu, *Probleme de teoria grupurilor*, Tipografia Universităţii din Bucureşti, 1982.

[4] R. Brewer, *Power series over commutative rings*, Marcel Dekker Publishers, New York, 1981.

[5] A. H. Clifford, G. B. Preston, *The algebraic theory of semigroups*, Mathematical Surveys 7, A. M. S., 1961.

[6] T. Dumitrescu, *Algebră*, Editura Universităţii din Bucureşti, 2006.

[7] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*, fifth edition, Oxford University Press, 1978.

[8] T. W. Hungerford, *Algebra*, Springer Verlag, 1974.

[9] I. D. Ion, N. Radu, *Algebra*, Editura didactică şi pedagogică, Bucureşti, 1981.

[10] I. D. Ion, C. Niţă, N. Radu, D. Popescu, *Probleme de algebră*, Editura didactică şi pedagogică, Bucureşti, 1981.

[11] N. Jacobson, *Basic Algebra 1*, San Francisco, Freeman, 1974.

[12] T. Y. Lam, *A first course in noncommutative rings*, Springer Verlag, 1991.

[13] T. Y. Lam, *Exercises in classical ring theory*, Springer Verlag, 1995.

[14] C. Năstăsescu, *Introducere în teoria mulţimilor*, Editura didactică şi pedagogică, Bucureşti, 1974.

[15] C. Năstăsescu, *Inele. Module. Categorii*, Editura Academiei R. S. R., 1976.

[16] C. Năstăsescu, C. Niţă, C. Vraciu, *Bazele Algebrei*, Editura Academiei R. S. R., 1986.

[17] L. Panaitopol, A. Gica, *O introducere în aritmetică şi teoria numerelor*, Editura Universităţii din Bucureşti, 2001.

[18] P. Samuel, *Anneaux factoriels*, Publicaçao do instituto de pesquisas matematicas da Universidade de Sao Paolo e da sociedade matematica de Sao Paolo, 1963.

[19] I. Tomescu, *Probleme de combinatorică şi teoria grafurilor* , Editura didactică şi pedagogică, Bucureşti, 1981.