

Probleme de algebră

Cornel Băețica, Crina Boboc, Sorin Dăscălescu, Gabriel Mincu

PREFAȚĂ

Lucrarea de față își propune să vină în sprijinul studenților de la secțiile de matematică și informatică pentru o mai bună aprofundare a unor noțiuni fundamentale din algebra modernă. De asemenea culegerea conține chestiuni mai complicate care sunt de interes pentru studenții care urmează un program de Master în matematică. Ea este o ediție revizuită și completată a culegerii publicate de primul și al treilea autor în 1993 la Editura Universității București.

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

Dorim să mulțumim colegilor și studenților care ne-au ajutat la scrierea acestei culegeri prin furnizarea de probleme sau soluții. Mulțumiri speciale adresăm lui Tiberiu Dumitrescu pentru discuțiile matematice care ne-au fost de mare ajutor.

17 Martie 2008

Cornel Băețica, Crina Boboc, Sorin Dăscălescu și Gabriel Mincu

Cuprins

| | | |
|----|---|-----|
| 1 | Mulțimi | 3 |
| 2 | Legi de compoziție. Semigrupuri și monoizi | 11 |
| 3 | Grupuri | 16 |
| 4 | Inele și corpuri | 29 |
| 5 | Construcții de inele: inele de matrice, inele de polinoame, inele de serii formale și inele de fracții | 40 |
| 6 | Aritmetică în inele integrale | 53 |
| 7 | Soluții: Mulțimi | 64 |
| 8 | Soluții: Legi de compoziție. Semigrupuri și monoizi | 83 |
| 9 | Soluții: Grupuri | 96 |
| 10 | Soluții: Inele și corpuri | 136 |
| 11 | Soluții: Construcții de inele: inele de matrice, inele de polinoame, inele de serii formale și inele de fracții | 162 |
| 12 | Soluții: Aritmetică în inele integrale | 199 |

Capitolul 1

Mulțimi

- Dacă A și B sunt mulțimi, notăm cu $A - B$ (sau cu $A \setminus B$) *diferența* celor două mulțimi, adică $A - B = \{x \mid x \in A \text{ și } x \notin B\}$.
- Dacă $B \subseteq A$, atunci $A - B$ se mai notează $C_A B$ și se numește *complementara* lui B în A .
- Vom nota cu \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} , respectiv, mulțimile numerelor naturale, întregi, raționale, reale, complexe, respectiv. Dacă M este una din aceste mulțimi, vom nota $M^* = M - \{0\}$.
- Dacă A este o mulțime, atunci mulțimea tuturor submulțimilor lui A se notează cu $\mathcal{P}(A)$ și se numește *mulțimea părților* lui A .
- O mulțime A se numește *finită* dacă $A = \emptyset$ sau dacă există o bijecție între A și mulțimea $\{1, \dots, n\}$ 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 mulțime nevidă, notăm cu 1_X (sau cu Id_X) *funcția identică* a mulțimii X , unde $1_X : X \rightarrow X$ și este definită prin $1_X(x) = x$ pentru orice $x \in X$.
- Un element $x \in M$ se numește *punct fix* pentru funcția $f : M \rightarrow M$ dacă $f(x) = x$.
- Compunerea a două funcții $f : A \rightarrow B$ și $g : B \rightarrow C$ se notează $g \circ f$ sau gf .
- Dacă $f : A \rightarrow B$ este o funcție, $X \subseteq A$ și $Y \subseteq B$, notăm $f(X) = \{f(x) \mid x \in X\}$, care este o submulțime a lui B și $f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}$, care este o submulțime a lui A . Mulțimea $f(X)$ se numește *imaginea* lui X prin f , iar mulțimea $f^{-1}(Y)$ se numește *preimagea* sau *imaginea inversă* a lui Y prin f .
- Dacă $f : A \rightarrow B$ este o funcție și A' este o submulțime nevidă a lui A ,

notăm cu $f|_{A'}$ restricția lui f la A' , unde $f|_{A'} : A' \rightarrow B$ și este definită prin $f|_{A'}(x) = f(x)$ pentru orice $x \in A'$.

- Dacă X și Y sunt mulțimi nevide, notăm cu $\text{Fun}(X, Y)$ sau cu Y^X mulțimea tuturor funcțiilor definite pe X cu valori în Y .

- Spunem că mulțimile A și B sunt *echipotente* (și notăm aceasta prin $A \sim B$) dacă există o bijecție între A și B .

- Dacă A este o mulțime care este în bijecție 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 numește *nenumărabilă*.

- Dacă \sim este o relație de echivalență pe mulțimea A , notăm cu A/\sim mulțimea factor, iar aceasta este mulțimea tuturor claselor de echivalență relativ la \sim . *Proiecția canonică* $p : A \rightarrow A/\sim$ asociază unui element $a \in A$ clasa sa de echivalență în raport cu \sim .

- Dacă $f : A \rightarrow B$ este o funcție, atunci notăm cu ρ_f relația de echivalență definită de f pe mulțimea A astfel: $x \rho_f y$ dacă și numai dacă $f(x) = f(y)$.

- Mulțimile factor au următoarea *proprietate de universalitate*: fie A, B două mulțimi, \sim o relație de echivalență pe A și $f : A \rightarrow B$ o funcție cu proprietatea că $\sim \subseteq \rho_f$. Atunci există și este unică o funcție $\bar{f} : A/\sim \rightarrow B$ care satisface condiția $\bar{f}p = f$.

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

2. Fie A o mulțime finită cu n elemente. Să se arate că ecuația

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

are $(2^m - 1)^n$ soluții.

3. (*Principiul includerii și excluderii*) Fie A_1, \dots, A_s mulțimi finite. Să se arate că

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

4. Fie A o mulțime finită și $f : A \rightarrow A$ o funcție. Să se arate că următoarele afirmații sunt echivalente:

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

5. Fie M și N două mulțimi finite astfel încât $|M| = m$ și $|N| = n$. Să se determine:

- (a) Numărul funcțiilor definite pe M cu valori în N .
- (b) Numărul funcțiilor injective definite pe M cu valori în N .
- (c) Numărul funcțiilor surjective definite pe M cu valori în N .

6. Să se determine numărul permutărilor unei mulțimi cu n elemente care au cel puțin un punct fix și al celor care au exact un punct fix.

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

8. Fie $f : \mathbb{N} \rightarrow \mathbb{N}$ o funcție cu următoarele proprietăți:

- (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 $f, g : \mathbb{N} \rightarrow \mathbb{N}$ astfel încât $\max(f, g)$ este surjectivă și $\min(f, g)$ este injectivă. Să se arate că $f = g$.

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

11. Fie M o mulțime și A, B două submulțimi ale sale. Definim $f : \mathcal{P}(M) \rightarrow \mathcal{P}(A) \times \mathcal{P}(B)$ prin $f(X) = (X \cap A, X \cap B)$. Să se arate că :

- (a) f este injectivă dacă și numai dacă $A \cup B = M$.
- (b) f este surjectivă dacă și numai dacă $A \cap B = \emptyset$.
- (c) f este bijectivă dacă și numai dacă $A = C_M B$. În acest caz să se calculeze f^{-1} .

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

13. Fie $f : M \rightarrow N$ o funcție. Să se arate că următoarele afirmații sunt echivalente:

- (a) f este injectivă.
- (b) f este *monomorfism*, adică pentru orice mulțime X și orice funcții $u, v : X \rightarrow M$ astfel încât $fu = fv$, rezultă că $u = v$.
- (c) Există o funcție $g : N \rightarrow M$ astfel încât $gf = 1_M$.

14. Fie $f : M \rightarrow N$ o funcție. Să se arate că următoarele afirmații sunt echivalente:

- (a) f este injectivă.
- (b) Pentru orice familie $(M_i)_{i \in I}$ de submulțimi ale lui M are loc egalitatea $f(\bigcap_{i \in I} M_i) = \bigcap_{i \in I} f(M_i)$.

15. Fie $f : M \rightarrow N$ o funcție. Să se arate că următoarele afirmații sunt echivalente:

- (a) f este surjectivă.
- (b) f este *epimorfism*, adică pentru orice mulțime Y și orice funcții $u, v : N \rightarrow Y$ astfel încât $uf = vf$, rezultă că $u = v$.
- (c) Există o funcție $g : N \rightarrow M$ astfel încât $fg = 1_N$.

16. Fie $f : M \rightarrow N$ o funcție. Definim aplicațiile $f_* : \mathcal{P}(M) \rightarrow \mathcal{P}(N)$ și $f^* : \mathcal{P}(N) \rightarrow \mathcal{P}(M)$ prin $f_*(X) = f(X)$ și $f^*(Y) = f^{-1}(Y)$.

(i) Să se arate că următoarele afirmații 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 afirmații 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 mulțimi nevide. Să se arate că există o bijecție între:

- (a) $\text{Fun}(A, \text{Fun}(B, C))$ și $\text{Fun}(A \times B, C)$.
- (b) $\text{Fun}(A, B \times C)$ și $\text{Fun}(A, B) \times \text{Fun}(A, C)$.

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

18. Pe \mathbb{R} definim relația \sim astfel: $x \sim y$ dacă și numai dacă $x - y \in \mathbb{Z}$. Să se arate că \sim este relație de echivalență și că există o bijecție între mulțimea factor \mathbb{R}/\sim și intervalul $[0, 1)$.

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

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

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

Să se arate că relația

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

este cea mai mică relație de echivalență pe M care include pe ρ .

21. Fie M_1, \dots, M_n mulțimi nevide și ρ_1, \dots, ρ_n , respectiv, relații de echivalență pe acestea. Fie $M = M_1 \times \dots \times M_n$ și relația ρ definită pe M astfel: $(x_1, \dots, x_n)\rho(y_1, \dots, y_n)$ dacă și numai dacă $x_i\rho_i y_i$ pentru orice $i = 1, \dots, n$. Să se arate că ρ este relație de echivalență pe M și că M/ρ este în bijecție cu $M_1/\rho_1 \times \dots \times M_n/\rho_n$.

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

23. Fie A o mulțime nevidă, B o submulțime nevidă a sa și ρ o relație pe $\mathcal{P}(A)$ definită astfel: $X\rho Y$ dacă și numai dacă $X \cap B = Y \cap B$. Să se arate că ρ este o relație de echivalență și că $\mathcal{P}(A)/\rho$ este în bijecție cu $\mathcal{P}(B)$.

24. Fie A, B două mulțimi nevide și A' o submulțime nevidă a lui A . Pe mulțimea $B^A = \{f \mid f : A \rightarrow B \text{ funcție}\}$ considerăm relația binară ρ definită astfel: $f\rho g$ dacă și numai dacă $f|_{A'} = g|_{A'}$. Să se arate că ρ este o relație de echivalență și că B^A/ρ este în bijecție cu $B^{A'}$.

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

pentru orice mulțimi A, B, C au loc:

- (a) $A \sim A$.
- (b) Dacă $A \sim B$, atunci $B \sim A$.
- (c) Dacă $A \sim B$ și $B \sim C$, atunci $A \sim C$.

Vom numi *număr cardinal* o clasă formată din toate mulțimile echipotente cu o mulțime dată A și vom nota acest număr cardinal cu $|A|$.

Dacă A este o mulțime finită, identificăm numărul cardinal $|A|$ cu numărul elementelor lui A (care a fost notat tot cu $|A|$). Dacă A este mulțime infinită, spunem că numărul cardinal $|A|$ este *infinit*.

26. (a) (*Teorema Cantor-Schröder-Bernstein*) Fie $X_2 \subseteq X_1 \subseteq X_0$ mulțimi astfel încât $X_0 \sim X_2$. Să se arate că $X_0 \sim X_1$.

(b) Dacă $\alpha = |A|$ și $\beta = |B|$ sunt numere cardinale, spunem că $\alpha \leq \beta$ dacă există o funcție injectivă $f : A \rightarrow B$. Să se arate că definiția relației " \leq " nu depinde de reprezentanții A și B aleși în cele două clase.

(c) Dacă α și β sunt două numere cardinale astfel încât $\alpha \leq \beta$ și $\beta \leq \alpha$, să se arate că $\alpha = \beta$.

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

28. Fie X o mulțime infinită. Să se arate că:

- (a) $|\mathbb{N}| \leq |X|$, adică orice mulțime infinită are o submulțime numărabilă.
- (b) Dacă F este o submulțime finită a lui X , atunci $|X - F| = |X|$.

29. Fie $\alpha = |A|$ și $\beta = |B|$ numere cardinale, reprezentanții A și B fiind aleși astfel încât $A \cap B = \emptyset$. Definim *suma numerelor cardinale* α și β prin $\alpha + \beta = |A \cup B|$. Să se arate că:

- (a) Definiția nu depinde de reprezentanții aleși.
- (b) Dacă α, β, γ sunt numere cardinale, atunci $\alpha + \beta = \beta + \alpha$ și $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.
- (c) Dacă α și β sunt numere cardinale cu α infinit și $\beta \leq \alpha$, atunci $\alpha + \beta = \alpha$.

30. Fie $\alpha = |A|$ și $\beta = |B|$ două numere cardinale. Definim *produsul numerelor cardinale* α și β prin $\alpha\beta = |A \times B|$. Să se arate că:

- (a) Definiția lui $\alpha\beta$ nu depinde de reprezentanții A și B aleși.
- (b) Dacă α, β, γ sunt numere cardinale, atunci $\alpha\beta = \beta\alpha$, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ și $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

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

31. (a) Fie α un număr cardinal și $(A_i)_{i \in I}$ o familie de mulțimi 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 mulțimi cel mult numărabile este cel mult numărabilă.

(c) Dacă A este o mulțime infinită și $\mathcal{P}_f(A)$ mulțimea tuturor submulțimilor finite ale lui A , atunci $|\mathcal{P}_f(A)| = |A|$.

32. Fie $\alpha = |A|$ și $\beta = |B|$ două numere cardinale. Definim $\alpha^\beta = |\text{Fun}(B, A)|$. Să se arate că:

(a) Definiția lui α^β nu depinde de reprezentanții A și B aleși.

(b) Dacă α, β, γ sunt numere cardinale, atunci $\alpha^{\beta+\gamma} = \alpha^\beta \alpha^\gamma$, $(\alpha\beta)^\gamma = \alpha^\gamma \beta^\gamma$ și $(\alpha^\beta)^\gamma = \alpha^{\beta\gamma}$.

(c) Pentru orice mulțime A are loc $|\mathcal{P}(A)| = 2^{|A|}$ (prin 2 înțelegem aici numărul cardinal asociat unei mulțimi cu două elemente).

33. Să se arate că $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| < |\mathbb{R}| = |\mathbb{C}|$ și 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 funcții $f : \mathbb{R} \rightarrow \mathbb{R}$ cu proprietatea că $|f(x) - f(y)| > 1$ pentru orice $x, y \in \mathbb{R}$, $x \neq y$.

35. Fie $f : \mathbb{R} \rightarrow (0, \infty)$ o funcție. Să se arate că există $k \in \mathbb{N}^*$ și $a_1, \dots, a_k \in \mathbb{R}$ distincte astfel încât $f(a_1) + \dots + f(a_k) > 1$.

36. Pentru o funcție $f : \mathbb{R} \rightarrow \mathbb{R}$ un element $x_0 \in \mathbb{R}$ se numește *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 definește și noțiunea de *punct de maxim local strict*. Un element al lui \mathbb{R} care este punct de minim sau de maxim local strict se numește *punct de extrem local strict*.

Să se arate că mulțimea punctelor de extrem local strict ale unei funcții $f : \mathbb{R} \rightarrow \mathbb{R}$ este cel mult numărabilă.

37. Pe \mathbb{R} definim relația \sim astfel: $x \sim y$ dacă și numai dacă $x - y \in \mathbb{Q}$. Să se arate că \sim este relație de echivalență și că există o bijecție între mulțimea factor \mathbb{R}/\sim și \mathbb{R} .

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

Capitolul 2

Legi de compoziție. Semigrupuri și monoizi

- Fie M o mulțime nevidă. O funcție $\varphi : M \times M \rightarrow M$ se numește *lege de compoziție* pe M . Dacă nu menționăm altfel, legea de compoziție va fi notată multiplicativ, adică $\varphi(x, y) = xy$. Dacă legea de compoziție este asociativă, adică $(xy)z = x(yz)$ pentru orice $x, y, z \in M$, atunci (M, φ) se numește 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 numește monoid. Dacă nu există nici un pericol de confuzie, în loc de (M, φ) vom scrie simplu M .
- Dacă M este monoid, atunci mulțimea $U(M) = \{x \in M \mid x \text{ este simetrizabil}\}$ este grup cu legea de compoziție indusă din cea a lui M și se numește *grupul unităților* 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 și noțiunea de *semigrup cu simplificare la dreapta*. Un semigrup cu simplificare atât la stânga cât și la dreapta se numește *semigrup cu simplificare*.
- Fie S un semigrup. Un element $e \in S$ cu proprietatea că $e^2 = e$ se numește element *idempotent*.
- Fie S un semigrup și S' o submulțime 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 numește *subsemigrup* al lui S . Dacă X este o submulțime a lui S , atunci intersecția tuturor subsemigrupurilor lui S care conțin pe X se numește *subsemigrupul generat de X* .
- Fie M un monoid și M' o submulțime nevidă a sa. Dacă M' este monoid

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

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

1. Fie M o mulțime cu n elemente, $n \in \mathbb{N}^*$. Să se determine:

- (i) Numărul legilor de compoziție ce pot fi definite pe M ;
- (ii) Numărul legilor de compoziție comutative ce pot fi definite pe M ;
- (iii) Numărul legilor de compoziție cu element neutru ce pot fi definite pe M .

2. Fie M o mulțime înzestrată cu o lege de compoziție (nu neapărat asociativă). Să se arate că dacă $x_1, \dots, x_n \in M$, atunci numărul de moduri în care se pot aranja corect parantezele în produsul $x_1x_2 \dots x_n$ 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 $f : A \rightarrow B$ un morfism de monoizi. Să se arate că următoarele afirmații sunt echivalente:

- (i) f este injectiv;
- (ii) f este *monomorfism* de monoizi, adică pentru orice monoid X și pentru orice morfisme de monoizi $u, v : X \rightarrow A$ astfel încât $fu = fv$, rezultă că $u = v$.

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

Să se arate că morfismul incluziune $i : \mathbb{Z} \rightarrow \mathbb{Q}$, unde \mathbb{Z} și \mathbb{Q} sunt considerate cu structurile de monoizi date de înmulțire, 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 și un morfism injectiv de semigrupuri $f : S \rightarrow M$.

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

7. Fie S un semigrup finit și $a \in S$. 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 mulțime finită este finit. Să se arate că orice subsemigrup al lui G este subgrup.

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

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

Să se arate că:

(i) (H_e, \cdot) este grup;

(ii) Dacă $H \subseteq S$, $e \in H$ și (H, \cdot) este grup, atunci $H \subseteq H_e$.

11. (i) Să se arate că un semigrup S conține un grup (cu operația indusă) dacă și numai dacă S are cel puțin un element idempotent.

(ii) Să se dea exemplu de semigrup care nu conține niciun grup.

12. Fie S un semigrup și $e \in S$ element idempotent.

(i) Să se arate că mulțimea $eSe = \{ese \mid s \in S\}$ este subsemigrup. Mai mult, aceasta este un monoid.

(ii) Notând cu H_e mulțimea elementelor inversabile din monoidul eSe , să se arate că H_e este grup și 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 operația indusă sunt grupuri), atunci orice subgrup este conținut într-un subgrup maximal.

(ii) Dacă G și 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 și se scrie ca o reuniune de subgrupuri.

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

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

18. (i) Dacă X este o mulțime nevidă notăm cu $I(X)$ mulțimea funcțiilor injective $f : X \rightarrow X$. 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 și numai dacă S este semigrup cu simplificare la stânga.

19. (i) Să se arate că un monoid M se poate scufunda în monoidul $(\text{Fun}(M, M), \circ)$.

(ii) Fie M un monoid finit. Dacă $a, b \in M \setminus U(M)$, atunci $ab \in M \setminus U(M)$. Arătați 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 inverși 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 și care are exact n elemente inversabile.

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

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

24. Fie $(M, +)$ un submonoid al lui $(\mathbb{N}, +)$. Să se arate că există o submulțime finită A a lui \mathbb{N} și $d, n_0 \in \mathbb{N}$ 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 $M_3 = \{3n + 1 \mid n \geq 0\}$ și $M_5 = \{5n + 1 \mid n \geq 0\}$. Să se arate că (M_3, \cdot) și (M_5, \cdot) sunt monoizi și că oricare doi dintre monoizii (\mathbb{N}^*, \cdot) , (M_3, \cdot) și (M_5, \cdot) sunt neizomorfi.
26. Fie $m, n \in \mathbb{N}$, $m, n \geq 2$ și $M_m = \{mk + 1 \mid k \in \mathbb{N}\}$, $M_n = \{nk + 1 \mid k \in \mathbb{N}\}$ monoizi multiplicativi. Să se arate că aceștia sunt izomorfi dacă și numai dacă grupurile $U(\mathbb{Z}_m)$ și $U(\mathbb{Z}_n)$ sunt izomorfe.
27. Să se arate că există o infinitate de submonoizi ai lui (\mathbb{N}^*, \cdot) care sunt izomorfi cu el și 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 și B sunt grupuri, mulțimea morfismelor de grupuri de la A la B o notăm cu $\text{Hom}_{gr}(A, B)$.
- Ordinul unui element g al unui grup se notează $\text{ord}(g)$.
- 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*. Aplicația $p : G \rightarrow G/H$, $p(a) = \hat{a}$ pentru orice $a \in G$, este morfism de grupuri și se numește *proiecția canonică*.
- Grupurile factor au următoarea *proprietate de universalitate*: fie G , G' două grupuri, H subgrup normal al lui G și $f : G \rightarrow G'$ morfism de grupuri cu proprietatea că $H \subseteq \text{Ker}(f)$. Atunci există și este unic un morfism de grupuri $\bar{f} : G/H \rightarrow G'$ care satisface condiția $\bar{f}p = f$, unde $p : G \rightarrow G/H$ este proiecția canonică.
- Un subgrup propriu H al lui G se numește subgrup *maximal* dacă pentru orice $K \leq G$ cu $H \subseteq K$, rezultă că $K = H$ sau $K = G$.
- Fie $Z(G) = \{x \in G \mid xg = gx \text{ pentru orice } g \in G\}$. Mulțimea $Z(G)$ se numește *centrul* grupului G și este subgrup normal al lui G .
- Fie $g \in G$ și $C(g) = \{x \in G \mid xg = gx\}$. Mulțimea $C(g)$ se numește *centralizatorul* elementului g și este subgrup al lui G .
- Un grup G se numește *simplu* dacă singurele subgrupuri normale ale lui G sunt G și $\{e\}$.
- Fie G un grup, $H \leq G$ și $H_G = \bigcap_{x \in G} xHx^{-1}$. H_G se numește *interiorul*

normal al lui H în G .

- Spunem că un grup (G, \cdot) este *divizibil* dacă pentru orice $a \in G$ și orice $n \in \mathbb{N}^*$ ecuația $x^n = a$ are soluții în G .
- Dacă X este o mulțime nevidă, mulțimea bijectiilor de la X la X este grup cu compunerea funcțiilor. Acest grup se numește *grupul simetric* al mulțimii X și se notează cu $S(X)$. Elementele lui $S(X)$ se numesc *permutări*. Dacă $X = \{1, \dots, n\}$, atunci $S(X)$ se mai notează cu S_n . Subgrupul lui S_n care constă din toate permutările pare se notează cu A_n și se numește *grupul altern* de grad n .
- Grupul izometriilor unui poligon regulat cu n laturi se numește *grupul diedral* de grad n și se notează cu D_n . Acesta are $2n$ elemente și poate fi prezentat prin doi generatori r și s , $D_n = \langle r, s \rangle$, care satisfac relațiile $s^2 = e, r^n = e, sr = r^{n-1}s$. Geometric, s corespunde unei simetrii a poligonului regulat față de o axă de simetrie și r corespunde unei rotații 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 și se numește *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.

Arătați 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. Arătați că următoarele afirmații sunt echivalente:

- (i) S este grup;
- (ii) Pentru orice $a, b \in S$ ecuațiile $ax = b$ și $ya = b$ au soluții în S .

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

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

$\text{Hom}_{gr}(\mathbb{Q}, \mathbb{Z})$, $\text{Hom}_{gr}(\mathbb{Q}, \mathbb{Q})$, $\text{Hom}_{gr}(\mathbb{Z}_n, \mathbb{Z}_n)$ și $\text{Hom}_{gr}(\mathbb{Z}_m, \mathbb{Z}_n)$, unde \mathbb{Z} , \mathbb{Q} , \mathbb{Z}_m și \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 și $A, B \subset G$, notăm cu $AB = \{ab \mid a \in A \text{ și } b \in B\}$. Presupunem că G este finit. Să se arate că:

(i) Dacă $A, B \subset G$ și $|A| + |B| > |G|$, atunci $AB = G$;

(ii) Dacă există $M \subset G$ astfel încât $|M| > (1/2)|G|$ și $ab = ba$ pentru orice $a, b \in M$, atunci G este comutativ.

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

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

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

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

11. Fie $m \in \mathbb{N}$, $m > 2$ și G un grup finit cu proprietatea că $\text{ord}(x) > m$, oricare ar fi $x \in G - \{e\}$. Arătați 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 și numai dacă $|G|$ este par.

13. Fie (G, \cdot) un grup și $f : G \rightarrow G$ definită prin $f(x) = x^2$. Atunci:

(i) f este morfism de grupuri dacă și numai dacă G este grup abelian;

(ii) Dacă G este grup abelian finit, atunci f este izomorfism dacă și 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

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

produsul direct conținând 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 $(a_i)_{i \in I}$ și fie $g \in G$. Să se arate că $\langle g \rangle$ este subgrup normal în G dacă și numai dacă $a_i g a_i^{-1} \in \langle g \rangle$ și $a_i^{-1} g a_i \in \langle g \rangle$, pentru orice $i \in I$.

18. Fie elementele

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

și

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

în $GL(2, \mathbb{C})$. Notăm $J = \langle \mathbf{j} \rangle$, $K = \langle \mathbf{k} \rangle$ și $Q = \langle \mathbf{j}, \mathbf{k} \rangle$. Să se arate că:

- (i) $|J| = 4$, $|K| = 4$ și $|J \cap K| = 2$;
 - (ii) J și K sunt subgrupuri normale în Q și $|Q| = 8$;
 - (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 numește *grupul cuaternionilor*).

19. Fie (G, \cdot) un grup și $x, y \in G$.

- (i) Dacă $xy = yx$, $\text{ord}(x)$ și $\text{ord}(y)$ sunt finite și $(\text{ord}(x), \text{ord}(y)) = 1$, atunci $\text{ord}(xy) = \text{ord}(x) \text{ord}(y)$. Dacă cele două ordine nu sunt relativ prime, mai este adevărat rezultatul?
- (ii) Dacă $\text{ord}(x)$ și $\text{ord}(y)$ sunt finite, rezultă că $\text{ord}(xy)$ este finit?
- (iii) Dacă $\text{ord}(xy)$ este finit, rezultă că $\text{ord}(x)$ și $\text{ord}(y)$ sunt finite?
- (iv) Dacă G este grup abelian și $|G| = p_1 \cdots p_n$, unde p_1, \dots, 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 $X + \mathbb{Z} = \mathbb{Q}$. Arătați că $X = \mathbb{Q}$.

22. Să se arate că dacă H este un subgrup finit generat al lui $(\mathbb{Q}, +)$, atunci H este ciclic. Deduceți 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 și orice $s \in S$ mulțimea $S - \{s\}$ este un sistem de generatori.

24. Fie G un grup finit cu $|G| > 1$ și 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 $S_3 \times \mathbb{Z}_4$ și $Q \times \mathbb{Z}_3$, unde Q este grupul cuaternionilor.

26. Fie (G, \cdot) un grup și $H_1 \subset H_2 \subset \dots \subset H_n \subset \dots$ un șir 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 mulțimii numerelor reale. Considerăm funcțiile $f, g \in S(\mathbb{R})$ definite prin $f(x) = x + 1$, $g(x) = 2x$ pentru orice $x \in \mathbb{R}$. Notăm $f_n = g^{-n} f g^n$, $G = \langle f, g \rangle$ și $H_n = \langle f_n \rangle$. 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 și H este un subgrup de indice finit al lui G , atunci H este finit generat.

29. Fie (G, \cdot) un grup și 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 $[G : H]$ și $[G : K]$ sunt finite și prime între ele, atunci are loc chiar egalitate și, în plus, $G = HK$;
- (iii) Dacă $K \subset H$, atunci $[L \cap H : L \cap K] \leq [H : K]$.

30. (i) Fie G și H două grupuri și $x = (g, h) \in G \times H$ astfel încât $\text{ord}(g)$ și $\text{ord}(h)$ 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 $\mathbb{Z}_{12} \times \mathbb{Z}_{15}$ și 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 și 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 și numai dacă pentru orice divizor pozitiv d al lui n ecuația $x^d = 1$ are cel mult d soluții în G ;
- (iii) Dacă G este comutativ, atunci G este ciclic dacă și numai dacă pentru orice divizor prim p al lui n ecuația $x^p = 1$ are cel mult p soluții în G .
Afirmația (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 $\text{ord}(x) = m$ și $\text{ord}(y) = n$, atunci există $z \in G$ astfel încât $\text{ord}(z) = [m, n]$.
- (ii) Fie $m_0 = \max\{\text{ord}(x) \mid x \in G\}$. Arătați că $\text{ord}(x)$ divide pe m_0 , oricare ar fi $x \in G$.
- (iii) Deduceți din (i) o altă soluție pentru exercițiul 19(iv).
- (iv) Deduceți din (ii) o altă soluție pentru exercițiul 32.

34. (i) Să se arate că pentru orice $n \in \mathbb{N}^*$, grupul (\mathbb{C}^*, \cdot) are exact un subgrup cu n elemente și anume $U_n = \{z \in \mathbb{C}^* \mid z^n = 1\}$.

(ii) Dacă p este un număr prim, arătați 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) Arătați 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 $(\mathbb{Q}, +)$ și (C_{p^∞}, \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 $\text{Hom}_{gr}(\mathbb{Q}, G)$.

37. (i) Să se arate că dacă G este un grup finit generat și 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 și numai dacă există un număr prim p și $n \in \mathbb{N}$, $n \geq 2$, astfel încât $G \simeq \mathbb{Z}_{p^n}$.

39. Fie G un grup. Pentru $g \in G$ definim $\varphi_g : G \rightarrow G$ 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) $\text{Inn}(G) = \{\varphi_g \mid g \in G\}$ este un subgrup normal al lui $\text{Aut}(G)$, numit *grupul automorfismelor interioare* ale lui G ;

(iii) $\text{Inn}(G) \simeq G/Z(G)$.

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 $\text{Aut}(G)$ pentru niciun grup G .

42. Să se arate că:
- (i) $\text{Aut}(\mathbb{Z})$ este izomorf cu $(\mathbb{Z}_2, +)$;
 - (ii) $\text{Aut}(\mathbb{Q})$ este izomorf cu (\mathbb{Q}^*, \cdot) ;
 - (iii) $\text{Aut}(\mathbb{Z}_n)$ este izomorf cu $(U(\mathbb{Z}_n), \cdot)$;
 - (iv) $\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ este izomorf cu grupul de permutări S_3 .
43. Să se arate că $\text{Aut}(S_3)$ este izomorf cu S_3 și $\text{Aut}(D_4)$ este izomorf cu D_4 .
44. Să se arate că:
- (i) Grupurile \mathbb{Z} și $\mathbb{Z} \times \mathbb{Z}$ nu sunt izomorfe;
 - (ii) Grupurile \mathbb{Q} și $\mathbb{Q} \times \mathbb{Q}$ nu sunt izomorfe;
 - (iii) Grupurile \mathbb{R} și $\mathbb{R} \times \mathbb{R}$ sunt izomorfe.
45. Considerăm grupurile multiplicative $S^1 = \{z \in \mathbb{C}^* \mid |z| = 1\}$ și $U_\infty = \{z \in \mathbb{C}^* \mid \text{există } n \in \mathbb{N}^* \text{ cu } z^n = 1\}$. 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) și $(\mathbb{C}/\mathbb{Z}, +)$ sunt izomorfe.
48. Să se dea un exemplu de grup G care are două subgrupuri H și K astfel încât K este subgrup normal în H și H este subgrup normal în G , dar K nu este subgrup normal în G .
49. Fie G un grup și H, K două subgrupuri. Să se arate că:
- (i) Dacă $H \trianglelefteq G$, atunci $HK = KH$ și HK este subgrup în G ;
 - (ii) Dacă $H \trianglelefteq G$, $[G : H] < \infty$, $|K| < \infty$ și $([G : H], |K|) = 1$, atunci $K \subseteq H$;
 - (iii) Dacă $H \trianglelefteq G$, $|H| < \infty$, $[G : K] < \infty$ și $([G : K], |H|) = 1$, atunci $H \subseteq K$.
50. Să se dea un exemplu de două grupuri G_1, G_2 și 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 exemplul de două grupuri neizomorfe astfel încât fiecare să fie izomorf cu un subgrup al celuilalt.

52. Fie G un grup finit, $\alpha \in \text{Aut}(G)$ și $I = \{x \in G \mid \alpha(x) = x^{-1}\}$. 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 mulțimi. Să se arate că dacă grupurile simetrice $S(X)$ și $S(Y)$ sunt izomorfe, atunci X și Y sunt echipotente.

54. Fie $n > 1$ și $H = \{\sigma \in S_n \mid \sigma(n) = n\}$. 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 și numai dacă $n = 2$;
- (iii) H este izomorf cu S_{n-1} ;
- (iv) Se pot alege $[(n-1)!]^n$ sisteme de reprezentanți pentru clasele la stânga (dreapta) modulo H .

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

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

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 disjuncți de lungime s/d .

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

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

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

61. Să se arate că S_n este generat de fiecare din următoarele mulțimi de permutări:

- (i) $(12), (13), \dots, (1n)$;
- (ii) $(12), (23), \dots, (n-1, n)$;
- (iii) $(12), (12 \dots n)$.

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

63. Să se arate că A_n este generat de mulțimea ciclor 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 și 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 și 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 și S_4 .

67. Fie $n \in \mathbb{N}^*$. Să se determine:

- (i) $\text{Hom}_{gr}(S_n, \mathbb{Z})$;
- (ii) $\text{Hom}_{gr}(S_n, \mathbb{Q}^*)$;
- (iii) $\text{Hom}_{gr}(S_n, \mathbb{Z}_6)$.

68. Să se determine:

- (i) $\text{Hom}_{gr}(S_n, \mathbb{Z}_2 \times \mathbb{Z}_2)$;
- (ii) $\text{Hom}_{gr}(S_3, \mathbb{Z}_3)$;
- (iii) $\text{Hom}_{gr}(\mathbb{Z}_3, S_3)$.

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

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

71. (i) Dacă G este un subgrup al lui S_n care nu este conținut în A_n , atunci G conține un subgrup de indice 2.

(ii) Dacă G este un grup finit și $|G| = 4n + 2$, atunci G conține 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 și 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 $GL(2, \mathbb{Z})$ și $GL(3, \mathbb{Z})$ nu sunt izomorfe.

75. Fie G un grup și H un subgrup al său. Să se arate că:

(i) $H_G = \bigcap_{x \in G} xHx^{-1}$ este subgrup normal al lui G conținut în H ;

(ii) Dacă N este un subgrup normal al lui G conținut în H , atunci N este conținut în H_G ;

(iii) Dacă $[G : H] = n$, să se arate că există un morfism injectiv de grupuri $f : G/H_G \rightarrow S_n$. În particular, dacă un grup are un subgrup de indice finit, atunci are un subgrup normal de indice finit.

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

77. Fie $G = GL(2, \mathbb{Z}_3)$ și

$$H = \left\{ \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{0} & \hat{c} \end{pmatrix} \mid \hat{a}\hat{c} \neq \hat{0} \right\}$$

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

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 și 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 conținut 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, \dots, H_r și $H = \bigcap_{i=1}^r H_i$. Să se arate că pentru orice $\alpha \in \text{Aut}(G)$ avem $\alpha(H) = H$.

81. Fie p un număr prim și G un grup finit cu p^2 elemente. Arătați 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. Determinați subgrupurile Sylow ale lui S_4 , respectiv A_4 .

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

84. Arătați că S_5 nu conține 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 $|G|$ și 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 și H două grupuri și $\varphi : H \rightarrow \text{Aut}(N)$ un morfism de grupuri. Să se arate că $G = N \rtimes H$ este grup în raport cu operația

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

Acest grup se notează cu $N \rtimes_{\varphi} H$ și se numește *produsul semidirect extern* al lui N cu H .

Dacă $N' = \{(n, e_H) \mid n \in N\}$ și $H' = \{(e_N, h) \mid h \in H\}$, atunci $N' \trianglelefteq G$, $H' \leq G$, $G = N'H'$ și $N' \cap H' = \{(e_N, e_H)\}$.

(ii) Fie G un grup și H, N subgrupuri ale lui G , $N \trianglelefteq G$, cu proprietatea că $G = NH$ și $N \cap H = \{e\}$. (Se spune că G este *produsul semidirect intern* al lui N cu H .)

Să se arate că $G \simeq N \rtimes_{\varphi} H$, unde $\varphi : H \rightarrow \text{Aut}(N)$ este dată prin $\varphi(h)(n) = hnh^{-1}$.

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

(ii) Fie p și q numere prime astfel încât $p < q$ și 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 și \mathbb{Z}_p . Deduceți că există exact două tipuri de izomorfism de grupuri cu pq elemente.

88. Fie p, q, r trei numere prime distincte și 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, \dots, G_n grupuri finite, $G = G_1 \times \dots \times G_n$ produsul lor direct și p un divizor prim al lui $|G|$. Să se arate că un subgrup H al lui G este p -subgrup Sylow dacă și numai dacă $H = H_1 \times \dots \times H_n$, unde H_i este p -subgrup Sylow al lui G_i sau $H_i = \{e\}$, $i = 1, \dots, n$.

(ii) Determinați 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, \dots, p_n sunt numere prime distincte. Fie H_1, \dots, 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 $H_1 \times \dots \times H_n$.

Capitolul 4

Inele și corpuri

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

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

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

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

- Dacă I este ideal bilateral în inelul R , notăm cu R/I *inelul factor*. Aplicația $p : R \rightarrow R/I$, $p(a) = \bar{a}$ pentru orice $a \in R$, este morfism de inele și se numește *proiecția canonică*.

- Inelele factor au următoarea *proprietate de universalitate*: fie R, R' două inele, I ideal bilateral al lui R și $f : R \rightarrow R'$ morfism de inele cu proprietatea că $I \subseteq \text{Ker}(f)$. Atunci există și este unic un morfism de inele $\bar{f} : R/I \rightarrow R'$ care satisface condiția $\bar{f}p = f$, unde $p : R \rightarrow R/I$ este proiecția canonică.

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

- Fie $u : R \rightarrow S$ 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 numește *extensia* lui I prin morfismul u .

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

- Fie R un inel comutativ și $P \subseteq R$ un ideal.

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

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

- Pentru un inel R se vor folosi următoarele notații:

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

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

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

$\text{Idemp}(R)$ = mulțimea elementelor idempotente din R ,

$\text{Spec}(R)$ = mulțimea idealelor prime ale lui R ,

$\text{Max}(R)$ = mulțimea idealelor maxime ale lui R .

- Dacă I și J sunt ideale în inelul comutativ R , notăm cu IJ mulțimea elementelor lui R de forma $x_1y_1 + \dots + x_ny_n$, cu $n \in \mathbb{N}^*$, $x_1, \dots, x_n \in I$ și $y_1, \dots, y_n \in J$, iar cu $I + J$ mulțimea elementelor lui R de forma $x + y$, cu $x \in I$ și $y \in J$. Atunci IJ (respectiv $I + J$) este ideal al lui R și se numește *produsul* (respectiv *suma*) idealelor I și J . Puterile I^n ale idealului I se definesc recurent prin $I^1 = I$ și $I^n = II^{n-1}$ pentru $n \geq 2$.

- Fie R un inel comutativ unitar. R se numește *inel noetherian* dacă orice șir crescător de ideale ale lui R este staționar, adică dacă $I_0 \subseteq I_1 \subseteq \dots \subseteq I_n \subseteq \dots$ 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 mulțime cu p elemente, unde p este un număr prim.

2. Să se determine numărul structurilor de inel unitar ce pot fi definite pe $(\mathbb{Z}_n, +)$ și 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, \dots, 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 și un morfism de inele $\phi : R \rightarrow S$ cu proprietatea că pentru orice inel unitar A și orice morfism

de inele $\alpha : R \rightarrow A$ există un morfism unitar de inele $\bar{\alpha} : S \rightarrow A$ 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 și 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 distincți în descompunerea sa. Să se arate că numărul idempotenților lui \mathbb{Z}_n este 2^r . Să se determine idempotenții inelului \mathbb{Z}_{72} .

10. Fie R un inel unitar. Dacă există un element în R care este inversabil la stânga și nu este inversabil la dreapta, atunci acesta are o infinitate de inverși la stânga. În particular, dacă un element din R are cel puțin doi inverși la stânga, atunci el are o infinitate de inverși 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 $|U(R)| \leq n - \lfloor \sqrt{n} \rfloor$.

13. Fie R un inel unitar și $a, b \in R$. Să se arate că:

- (i) Dacă $1 - ba$ are un invers la stânga (dreapta), atunci și $1 - ab$ are un invers la stânga (dreapta).
(ii) $1 - ba$ este inversabil dacă și numai dacă $1 - ab$ este inversabil.

14. Fie R un inel. Definim pe R legea de compoziție "o" 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) și (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 și numai dacă ba este quasi-regulat la stânga (dreapta).
(iv) Orice element nilpotent din R este quasi-regulat la stânga și la dreapta.

15. Fie R un inel unitar. Să se demonstreze echivalența următoarelor afirmații:

- (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 și $u, v \in R$. Să se arate că următoarele afirmații sunt echivalente:

- (i) u este inversabil și $v = u^{-1}$;
- (ii) $uvu = u$ și $vu^2v = 1$;
- (iii) $uvu = u$ și 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 corespondență bijectivă între mulțimea morfismelor de inele (nu neapărat unitare, chiar dacă R este unitar) $f : \mathbb{Z} \rightarrow R$ și mulțimea $\text{Idemp}(R)$.

(ii) Să se arate că există o corespondență bijectivă între mulțimea morfismelor de inele $f : \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ și $\text{Idemp}(\mathbb{Z}_n) \cap \{\hat{a} \in \mathbb{Z}_n \mid m\hat{a} = 0\}$. Să se determine numărul de elemente al acestei mulțimi.

19. Fie R, S inele unitare și $f : R \rightarrow S$ un morfism de inele unitare.

(i) Să se arate că f este injectiv dacă și numai dacă f este *monomorfism* de inele unitare, adică pentru orice inel unitar A și pentru orice morfisme unitare de inele $u, v : A \rightarrow R$ 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 și pentru orice morfisme unitare de inele $u, v : S \rightarrow A$ 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) $\text{Idemp}(R)$ are o structură de grup în raport cu legea de compoziție "*" definită prin: $e * f = e + f - 2ef$ pentru orice $e, f \in \text{Idemp}(R)$.

(ii) Dacă R are un număr finit de idempotenți, atunci există $n \in \mathbb{N}^*$ astfel încât $|\text{Idemp}(R)| = 2^n$.

21. Fie $C = \{f \mid f : [0, 1] \rightarrow \mathbb{R}, f \text{ funcție continuă}\}$ cu structura de inel unitar dată de adunarea și înmulțirea funcțiilor. Dacă $t \in [0, 1]$ notăm cu $\phi_t : C \rightarrow \mathbb{R}$ aplicația dată de $\phi_t(f) = f(t)$. Să se arate că:

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

22. Fie $u : R \rightarrow S$ un morfism de inele comutative.

- (i) Arătați că dacă J este ideal al lui S , atunci $u^{-1}(J)$ este ideal al lui R .
- (ii) Arătați că dacă I este ideal al lui R , atunci $u(I)$ nu este neapărat ideal al lui S .
- (iii) Arătați că $I^e = \left\{ \sum_{i=1}^n u(x_i) \mid n \in \mathbb{N}, i \in S, x_i \in I \right\}$.
- (iv) Arătați că pentru orice ideal I al lui R avem $I \subset (I^e)^e$; dați exemple de situații când această incluziune este strictă.
- (v) Arătați că pentru orice ideal J al lui S avem $(J^e)^e \subset J$; dați exemple de situații când această incluziune este strictă.
- (vi) Arătați că pentru orice ideal I al lui R avem $((I^e)^e)^e = I^e$.
- (vii) Arătați că pentru orice ideal J al lui S avem $((J^e)^e)^e = J^e$.

23. Fie R un inel comutativ și I, J ideale ale lui R . Să se arate că:

- (i) Dacă se consideră I^e , extinsul lui I via proiecția canonică $\pi : R \rightarrow R/J$, atunci $I^e = \overline{I} \overline{R}$, unde $\overline{I} = \pi(I)$ și $\overline{R} = R/J$.
- (ii) $I^e = (I + J)/J$.
- (iii) $\overline{R}/\overline{I} \overline{R} \simeq R/(I + J)$.

24. (i) Arătați că un inel R este noetherian dacă și numai dacă orice ideal al său este finit generat.

(ii) (*Cohen*) Arătați că R este noetherian dacă și numai dacă orice ideal prim al său este finit generat.

(iii) Arătați că orice inel factor al unui inel noetherian este noetherian.

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

26. (i) Fie R_1, \dots, R_n inele unitare și $R = R_1 \times \dots \times R_n$. Să se arate că idealele lui R sunt de forma $I = I_1 \times \dots \times I_n$, unde I_1, \dots, I_n sunt ideale în R_1, \dots, R_n , respectiv.

(ii) Cu notațiile de la punctul (i) să se arate că inelele R/I și $R_1/I_1 \times \dots \times R_n/I_n$ 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 numește *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 și numai dacă orice element al său este nilpotent.

Dacă I nu este finit generat mai rămâne adevărată afirmația?

28. Fie R un inel comutativ și unitar și I_1, \dots, I_n ideale în R . Considerăm morfismul de inele $\phi : R \rightarrow R/I_1 \times \dots \times R/I_n$ definit astfel: $\phi(x) = (x \pmod{I_1}, \dots, x \pmod{I_n})$. Să se arate că:

- (i) $\text{Ker}(\phi) = I_1 \cap \dots \cap I_n$.
- (ii) ϕ este surjectiv dacă și numai dacă idealele I_1, \dots, 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 $R/I_1 \cap \dots \cap I_n$ și $R/I_1 \times \dots \times R/I_n$.

29. Fie R un inel comutativ și unitar. Să se arate că următoarele afirmații sunt echivalente:

- (i) R are un singur ideal maximal;
- (ii) $R \setminus U(R)$ este ideal în R ;
- (iii) Dacă $a, b \in R$ și $a + b \in U(R)$ atunci $a \in U(R)$ sau $b \in U(R)$.

Un inel care verifică una dintre condițiile echivalente de mai sus se numește *inel local*.

30. Să se arate că un inel local are doar idempotenții 0 și 1.

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

32. Fie R un inel unitar.

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

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

34. Fie R un inel. Un element $e \in R$ se numește *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 și element identitate la dreapta.

(ii) Dacă $e \in R$ este unicul element identitate la stânga, atunci e este și element identitate la dreapta.

35. Fie R un inel și A o submulțime 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) și 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) și R este corp.

37. Fie D un corp. Se numește *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 toți comutatorii aditivi ai lui D , atunci $y \in Z(D)$.

38. Fie D un corp. Pentru orice $a \in D$ fie aplicația $\delta_a : D \rightarrow D$ definită prin $\delta_a(x) = ax - xa$. Să se arate că:

(i) $\delta_a(x + y) = \delta_a(x) + \delta_a(y)$ și $\delta_a(xy) = x\delta_a(y) + \delta_a(x)y$ pentru orice $a, x, y \in D$.

(ii) Dacă D are caracteristica diferită de 2 și 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 numește *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 toți comutatorii multiplicativi din D , atunci $c \in Z(D)$.

40. Fie D un corp și 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 și 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 și unitar, P un ideal prim al său și I idealul generat de elementele idempotente din P . Să se arate că R/I nu are idempotenți netriviali (adică diferiți de 0 și 1).

43. Fie R un inel unitar. R se numește *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 și $2x = 0$ pentru orice $x \in R$.
- (ii) $\text{Spec}(R) = \text{Max}(R)$.
- (iii) Dacă X este o mulțime, atunci $(\mathcal{P}(X), \Delta, \cap)$ este inel Boole.
- (iv) Dacă R este inel Boole finit, atunci există o mulțime 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 mulțime infinită X se poate defini o structură de inel Boole.

44. Fie R un inel comutativ și unitar.

- (i) Să se arate că $N(R)$ coincide cu intersecția idealelor prime ale lui R . În particular, $N(R)$ este ideal.
- (ii) Dacă $x \in N(R)$ și $u \in U(R)$, atunci $x + u \in U(R)$.
- (iii) Dacă $J(R)$ este *radicalul Jacobson* al lui R , definit ca fiind intersecția 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 $N(R) \neq J(R)$ și de inele R pentru care $N(R) = J(R)$.

45. Fie R_1, \dots, R_n inele comutative unitare și $R = R_1 \times \dots \times R_n$. Atunci:

- (i) P este ideal prim al lui R dacă și numai dacă există $1 \leq i \leq n$ și P_i ideal prim al lui R_i astfel încât $P = R_1 \times \dots \times R_{i-1} \times P_i \times R_{i+1} \times \dots \times R_n$.
- (ii) M este ideal maximal al lui R dacă și numai dacă există $1 \leq i \leq n$ și M_i ideal maximal al lui R_i astfel încât $M = R_1 \times \dots \times R_{i-1} \times M_i \times R_{i+1} \times \dots \times R_n$.
- (iii) $N(R) = N(R_1) \times \dots \times N(R_n)$ și $J(R) = J(R_1) \times \dots \times J(R_n)$.

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

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

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

Să se arate că:

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

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, $p|m$ și 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 și $p|m$.

Deci $\text{Spec}(R) \subset \text{Max}(R)$ și $\text{Spec}(R) \neq \text{Max}(R)$.

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 $\text{Spec}(R) \setminus \{0\} \subset \text{Max}(R)$ și $\text{Spec}(R) \setminus \{0\} \neq \text{Max}(R)$.

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

52. Fie $A_1, \dots, A_m, B_1, \dots, B_n$ inele comutative unitare care nu au idempotenți netriviali (adică diferiți de 0 și 1). Atunci $A_1 \times \dots \times A_m \simeq B_1 \times \dots \times B_n$ dacă și numai dacă $m = n$ și 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. Arătați că există $x, y \in K$ cu proprietatea că $x^2 + y^2 \neq a^2$ pentru orice $a \in K$.

Capitolul 5

Construcții de inele: inele de matrice, inele de polinoame, inele de serii formale și inele de fracții

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

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

infinitate numărabilă de nedeterminate peste R .

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

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

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

notăm mulțimea polinoamelor din $R[X_1, \dots, X_n]$ cu toți coeficienții în I . Se observă că $I[X_1, \dots, X_n]$ este ideal (stâng, drept, bilateral) al inelului $R[X_1, \dots, X_n]$.

Pentru un polinom $f \in R[X_1, \dots, X_n]$ vom nota cu \tilde{f} funcția polinomială atașată lui f . Deci $\tilde{f}: R^n \rightarrow R$ 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 $R[X_1, \dots, X_n]$ este noetherian.

- Un polinom $f \in R[X_1, \dots, X_n]$ se numește *simetric* dacă pentru orice permutare $\sigma \in S_n$ avem $f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = f(X_1, \dots, X_n)$. Polinoamele simetrice fundamentale din $R[X_1, \dots, X_n]$ se notează cu s_1, \dots, s_n și sunt date de formulele

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

- Prin $M_n(R)$, $n \in \mathbb{N}^*$, notăm inelul matricelor pătratice de ordin n cu coeficienți într-un inel R .

Dacă I este un ideal (stâng, drept, bilateral) al lui R , atunci se notează cu $M_n(I)$ mulțimea matricelor cu toate elementele în I . Se observă că $M_n(I)$ este ideal (stâng, drept, bilateral) al lui $M_n(R)$.

Pentru $1 \leq i, j \leq n$ fixați se notează cu E_{ij} (sau e_{ij}) matricea care are 1 pe poziția (i, j) și 0 în rest.

- Fie R un inel comutativ și unitar. Prin $R[[X]]$ vom nota inelul de serii formale în nedeterminata X cu coeficienți în R . Dacă $f = a_0 + a_1 X + \dots$ este o serie formală nenulă, atunci *ordinul* lui f se notează cu $\text{ord}(f)$ și este cel mai mic n cu proprietatea că $a_n \neq 0$.

Dacă I este ideal al lui R , atunci prin $I[[X]]$ notăm mulțimea seriilor formale din $R[[X]]$ cu toți coeficienții în I . Se observă că $I[[X]]$ este ideal al lui $R[[X]]$.

- Fie R un inel comutativ și unitar iar $S \subset R$ un *sistem multiplicativ* (adică $1 \in S$ și pentru orice $s, t \in S$ avem $st \in S$). Inelul de fracții 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 $a, b \in R$ și $s, t \in S$ avem $a/s = b/t$ dacă și numai dacă există $u \in S$ astfel încât $u(at - bs) = 0$.

Inelele de fracții au următoarea *proprietate de universalitate*: pentru orice

morfism de inele comutative $f : R \rightarrow R'$ și pentru orice sistem multiplicativ $S \subset R$ cu proprietatea că $f(S) \subset U(R')$ există și este unic un morfism $\bar{f} : S^{-1}R \rightarrow R'$ astfel încât $\bar{f}\phi = f$, unde $\phi : R \rightarrow S^{-1}R$, $\phi(a) = a/1$ pentru orice $a \in R$, este morfismul canonic.

Dacă R este un domeniu de integritate și $S = R \setminus \{0\}$, atunci inelul de fracții $S^{-1}R$ este corp, se notează cu $Q(R)$ și se numește *corpul de fracții* al lui R . Dacă I este ideal al lui R , atunci se notează cu $S^{-1}I$ mulțimea fracțiilor 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 $i \neq j$ și cu 1 dacă $i = j$.

1. Fie R un inel. Să se arate că inelul de matrice $M_n(R)$ este comutativ dacă și numai dacă este satisfăcută una din următoarele două condiții:

- (i) $n = 1$ și 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 $M_2(\mathbb{Z}_p)$ și numărul acestora.
- (ii) Dacă $A, B \in M_2(\mathbb{Z}_p)$ și A este inversabilă, să se arate că $A^q = I_2$ și $B^{q+2} = B^2$, unde $q = (p^2 - 1)(p^2 - p)$.

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

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

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

6. Fie R un inel și $n \in \mathbb{N}^*$. 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 , și 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 și $n > 1$. Să se arate că nu există morfisme de inele $f : M_n(K) \rightarrow K$.

8. Fie $\mathbb{H} = \left\{ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \mid u, v \in \mathbb{C} \right\}$.

(i) Să se arate că \mathbb{H} este un corp necomutativ cu adunarea și înmulțirea 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 $\bar{x} = a_0 I_2 - a_1 \mathbf{i} - a_2 \mathbf{j} - a_3 \mathbf{k}$, $N(x) = x\bar{x}$ și $T(x) = x + \bar{x}$, să se arate că $x^2 - T(x)x + N(x) = 0$ și că $N(xy) = N(yx)$ pentru orice $x, y \in \mathbb{H}$.

(iv) Să se determine $Z(\mathbb{H})$.

(v) Să se arate că ecuația $x^2 = -1$ are o infinitate de soluții în \mathbb{H} .

9. Fie S un inel și $n \in \mathbb{N}^*$. Să se arate că următoarele afirmații 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 $\sum_{1 \leq i \leq n} e_{ii} = 1$ și $e_{ij}e_{kl} = \delta_{jk}e_{il}$ 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 $n \in \mathbb{N}^*$ și un inel R . Fie A un inel factor al lui S și B un inel pentru care S este subinel în B . Să se arate că A și B sunt și ele izomorfe cu inele de matrice $n \times n$ peste anumite inele.

11. Fie $k \in \mathbb{Z}$ și $R_k = \left\{ \begin{pmatrix} a & b \\ kb & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$. 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 și 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 și $a_1, \dots, a_n \in R$. Să se arate că

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

14. Fie R un inel comutativ și I un ideal al lui R . Arătați că:

- (i) $I[X_1, \dots, X_n]$ este ideal al lui $R[X_1, \dots, X_n]$ și coincide cu extinsul lui I via injecția canonică $\epsilon : R \rightarrow R[X_1, \dots, X_n]$.
- (ii) $R[X_1, \dots, X_n]/I[X_1, \dots, X_n] \simeq (R/I)[X_1, \dots, X_n]$.
- (iii) I este ideal prim în R dacă și numai dacă $I[X_1, \dots, X_n]$ este ideal prim în $R[X_1, \dots, X_n]$.

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 și înmulțirea numerelor reale.
- (ii) $\mathbb{Q}[X]/(X^2 + X + 1) \simeq \mathbb{Q}(\varepsilon)$, unde ε este o rădăcină primitivă de ordinul 3 a unității și $\mathbb{Q}(\varepsilon) = \{a + b\varepsilon \mid a, b \in \mathbb{Q}\}$ este inel cu adunarea și înmulțirea numerelor complexe.
- (iii) $\mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}$.

16. Fie $d \in \mathbb{Z}$ care nu este pătrat perfect. Arătați 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 $a, b, c \in \mathbb{R}$, $a \neq 0$ și $\Delta = b^2 - 4ac$. 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 și că $\mathbb{Z}[X]/I$ nu este corp.

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

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

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

23. Fie K un corp comutativ și $R = K[X, Y]/(X^2 - Y^3)$. 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 $n \in \mathbb{N}$ și $a_0, a_2, \dots, a_n \in K$.

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 și $f = a_0 + a_1X + \dots + a_nX^n \in R[X]$. Să se arate că:

- (i) f este nilpotent dacă și numai dacă a_i este nilpotent pentru orice $0 \leq i \leq n$.
- (ii) f este inversabil dacă și numai dacă a_0 este inversabil și a_i este nilpotent pentru orice $1 \leq i \leq n$.
- (iii) f este divizor al lui zero dacă și numai dacă există $a \in R$, $a \neq 0$, cu $af = 0$.
- (iv) f este idempotent dacă și numai dacă $f = a_0$ și $a_0^2 = a_0$.

26. Fie R un inel comutativ și $f = a_0 + a_1X + \dots \in R[[X]]$. 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 și numai dacă a_0 este inversabil.
- (iii) f este idempotent dacă și numai dacă $f = a_0$ și $a_0^2 = a_0$.

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 și $M = (M \cap R)R[[X]] + XR[[X]]$.
- (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. Arătați 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 $J(R[X]) = N(R[X])$ și $J(R[[X]]) = J(R)[[X]]$.

31. Fie K un corp comutativ și considerăm inelul neunitar $R = XK[[X]]$.
(i) Fie I un ideal al lui R și 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) Deduceți că R are ideale maximale dacă și numai dacă grupul $(K, +)$ are subgrupuri maximale.

(iv) Să se arate că grupul $(K, +)$ este divizibil dacă și numai dacă $\text{char}(K) = 0$.

(v) Deduceți că grupul $(K, +)$ are subgrupuri maximale dacă și numai dacă $\text{char}(K) \neq 0$.

(vi) Să se arate că R are ideale maximale dacă și 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 $n \in \mathbb{N}$, $n \geq 2$ și $a \in K$.

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

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

34. Dacă $F = \sum_{n \geq 0} a_n X^n$ este o serie formală cu coeficienți 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 $(F + G)' = F' + G'$, $(FG)' = F'G + FG'$ și $(F^n)' = nF^{n-1}F'$ pentru orice $n \in \mathbb{N}^*$.
- (ii) Pentru $\text{char } K = 0$, dacă $A, B \in U_1(K[[X]])$ și $A'B = AB'$, atunci $A = B$.
- (iii) Pentru $\text{char } K = 0$, dacă $A, B \in XK[[X]]$ și $A' = B'$, 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 $r \geq 0$ șirul $(a_{ir})_{i \geq 0}$ 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 înțelegem 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 și $F' = \sum_{i \geq 0} F'_i$.
- (ii) Dacă $G \in K[[X]]$, atunci familia $(F_i G)_{i \geq 0}$ este sumabilă și $(\sum_{i \geq 0} F_i)G = \sum_{i \geq 0} F_i G$.

36. Fie K un corp de caracteristică zero. Identificăm mulțimea numerelor raționale 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 și atunci suma din membrul drept se definește ca în problema 35.)

De asemenea, pentru orice $g \in U_1(K[[X]])$ definim

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

(Și 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) Deduceți că funcțiile \exp și \log sunt izomorfisme inverse unul celuilalt între grupurile $(XK[[X]], +)$ și $(U_1(K[[X]]), \cdot)$.

37. Fie K un corp de caracteristică zero. Identificăm mulțimea numerelor raționale cu cel mai mic subcorp al lui K . Fie $\alpha = \frac{a}{N}$ un număr rațional, 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) Definiția lui $(1 + X)^\alpha$ nu depinde de reprezentarea lui α ca fracție rațională.
- (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 funcție polinomială de α .
- (iv) $(1 + X)^\alpha = 1 + \sum_{n>0} \binom{\alpha}{n} X^n$, unde $\binom{\alpha}{n} = \frac{\alpha(\alpha-1)\dots(\alpha-n+1)}{n!}$ pentru orice $n > 0$.

38. Pentru $n \geq 2$ notăm cu T_n numărul de moduri în care se pot pune parantezele în produsul $x_1 x_2 \dots x_n$, unde x_1, \dots, x_n sunt elemente ale unei mulțimi pe care s-a definit o operație notată multiplicativ. Notăm $T_1 = 1$. Știm din soluția problemei 2 din Capitolul 2 că $T_n = \sum_{k=1, n-1} T_k T_{n-k}$. Considerăm seria formală $F = T_1 X + T_2 X^2 + \dots + T_n X^n + \dots \in \mathbb{Q}[[X]]$.

- (i) Să se arate că $F^2 = F - X$.
- (ii) Deduceți că $F = \frac{1}{2} - \frac{1}{2} \phi_2^{-1}(1 - 4X)$ (unde ϕ_2 are semnificația 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) și (iii) că $T_n = \frac{1}{n} C_{2n-2}^{n-1}$.

39. (i) Fie k un corp comutativ și $f \in k[X]$. Arătați că inelul factor $k[X]/(f)$ este corp dacă și numai dacă f este ireductibil.
(ii) Fie R un domeniu de integritate și Q corpul său de fracții. Arătați că pentru orice polinom neconstant $f \in R[X]$ există un corp care conține Q ca subcorp și în care f are cel puțin o rădăcină.
(iii) Cu notațiile de la (ii), demonstrați că pentru orice polinom $f \in R[X]$ cu grad $f \geq 1$ există un corp K care conține pe Q ca subcorp și în care f are toate rădăcinile.

40. Fie $a \in \mathbb{Z}$, $n \in \mathbb{N}^*$ și $f(X) = X^n - a \in \mathbb{Z}[X]$. 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 și $f \in R[X_1, \dots, X_n]$. Dacă există o submulțime $A = A_1 \times \dots \times A_n$ 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 funcția polinomială atașată polinomului f).

Mai rămâne adevărată afirmația dacă știm 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, $q \in \mathbb{N}$, $q > 1$ și $f \in K[X_1, \dots, X_n]$. 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 $g_i \in K[X_1, \dots, X_n]$ pentru orice $0 \leq i \leq n$, $\deg_{X_i}(g_0) < q$ pentru orice $1 \leq i \leq n$, și $\deg(g_0) \leq \deg(f)$.

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

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

46. Fie K un corp finit, $|K| = q$, și fie $f \in K[X_1, \dots, X_n]$ astfel încât $\deg(f) = d < n$ și $f(0, \dots, 0) = 0$. Să se arate că:

(i) Există $a \in K^n$, $a \neq (0, \dots, 0)$, cu $\tilde{f}(a) = 0$.

(ii) Dacă $|\{a \in K^n \mid \tilde{f}(a) = 0\}| = N$ și $p = \text{char}(K)$, atunci $p \mid N$.

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

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

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

(i) ϕ este injectiv dacă și numai dacă S este inclus în mulțimea nondivizorilor lui zero din R .

(ii) ϕ este bijectiv dacă și numai dacă $S \subseteq U(R)$.

49. Fie R un inel comutativ, $S \subseteq R$ un sistem multiplicativ și 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 și numai dacă $I \cap S \neq \emptyset$.

(iii) Mulțimea $T = \{\hat{s} \mid s \in S\}$ este sistem multiplicativ în R/I și avem $S^{-1}R/S^{-1}I \simeq T^{-1}(R/I)$.

(iv) $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$, $S^{-1}(I + J) = S^{-1}I + S^{-1}J$ și $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$ pentru orice ideale I și J .

50. Fie R un inel comutativ și 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 corespondență bijectivă între $\text{Spec}(R) \cap \Sigma$ și $\text{Spec}(S^{-1}R)$, 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 și $S = R - p$, atunci $S^{-1}R$ este inel local cu idealul maximal $S^{-1}p$ și $S^{-1}R/S^{-1}p$ este izomorf cu $Q(R/p)$, corpul de fracții al domeniului de integritate R/p . (În acest caz $S^{-1}R$ se notează cu R_p și se numește *localizatul* lui R în idealul prim p).

51. Fie R inel noetherian. Arătați că orice inel de fracții 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} și 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} și că $S^{-1}\mathbb{Z} = \mathbb{Q}$.

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

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

56. Fie R un inel comutativ finit și S un sistem multiplicativ al lui R . Să se arate că morfismul canonic $\phi : R \rightarrow S^{-1}R$ este surjectiv. În particular, orice inel de fracții al lui \mathbb{Z}_n este izomorf cu un \mathbb{Z}_d , $d|n$. Este adevărat și reciproc: pentru orice $n \in \mathbb{N}^*$ și 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 fracții al lui R și 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 și S un sistem multiplicativ al lui R . Să se arate că există un izomorfism canonic între $S^{-1}(R[X])$ și $(S^{-1}R)[X]$. Mai rămâne adevărată proprietatea pentru inele de serii formale?

59. Fie $(R_i)_{i \in I}$ o familie de inele comutative și 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 și că există un izomorfism canonic între $S^{-1}R$ și $\prod_{i \in I} (S_i^{-1}R_i)$.

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

61. Fie K un corp comutativ, $\text{char}(K) \neq 2$ și fie $D_n, \Delta_n \in K[X_1, \dots, X_n]$, $D_n = \prod_{1 \leq i, j \leq n} (X_i - X_j)$, $\Delta_n = D_n^2$. Să se arate că:

- (i) $D_n(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = \varepsilon(\sigma)D_n(X_1, \dots, X_n)$ pentru orice $\sigma \in S_n$.
- (ii) Δ_n este polinom simetric.
- (iii) Dacă $f \in K[X_1, \dots, X_n]$ are proprietatea că

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

pentru orice $\sigma \in S_n$, atunci există $g \in K[X_1, \dots, X_n]$ polinom simetric cu $f = gD_n$.

(iv) Dacă $f \in K[X_1, \dots, X_n]$ are proprietatea că

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

pentru orice $\sigma \in A_n$, atunci există $f_1, f_2 \in K[X_1, \dots, X_n]$ polinoame simetrice cu $f = f_1 + f_2D_n$.

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) $(-X_1 + X_2 + \dots + X_n)(X_1 - X_2 + \dots + X_n) \cdots (X_1 + X_2 + \dots + X_{n-1} - X_n)$.
- (iv) $X_1^3 + \dots + X_n^3$.

63. (*Formulele lui Newton*) Fie K un corp comutativ. Pentru fiecare $i \in \mathbb{N}$, $i > 0$, considerăm polinoamele $p_i = X_1^i + \dots + X_n^i \in K[X_1, \dots, X_n]$. De asemenea considerăm $p_0 = n$. Să se arate că:

- (i) $p_k - s_1p_{k-1} + \dots + (-1)^n s_n p_{k-n} = 0$ pentru orice $k \geq n$.
- (ii) $p_k - s_1p_{k-1} + \dots + (-1)^{k-1} s_{k-1} p_1 + (-1)^k k s_k = 0$ pentru orice $1 \leq k \leq n-1$.

64. Fie K un corp comutativ de caracteristică zero. Considerăm elementele $x_1, \dots, x_n \in K$ cu proprietatea că $x_1^k + \dots + x_n^k = 0$ pentru orice $1 \leq k \leq n$. Să se arate că $x_1 = \dots = x_n = 0$.

Mai rămâne adevărată concluzia dacă $x_1^k + \dots + x_n^k = 0$ 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 $x_1^i + \dots + x_n^i$, $1 \leq i \leq n$, unde x_1, \dots, x_n sunt rădăcinile polinomului:

- (i) $X^n + (a + b)X^{n-1} + (a^2 + b^2)X^{n-2} + \dots + (a^n + b^n)$, unde $a, b \in K$, K corp.
- (ii) $X^n + (a + b)X^{n-1} + (a^2 + ab + b^2) + \dots + (a^n + a^{n-1}b + \dots + ab^{n-1} + b^n)$, unde $a, b \in K$, K corp.

Capitolul 6

Aritmetică în inele integrale

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

- Fie R un inel comutativ unitar și $a, b \in R$. Spunem că a *divide* pe b în R (și 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 (și notăm $a \sim_R b$ sau $a \sim b$) dacă $a|_R b$ și $b|_R a$. Relația de asociere în divizibilitate este o relație de echivalență. În cazul în care R este domeniu, $a \sim_R b$ dacă și 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 și b din R dacă sunt îndeplinite următoarele condiții:

(i) $d|a$ și $d|b$.

(ii) Pentru orice $d' \in R$ care divide a și 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 și b din R dacă sunt îndeplinite următoarele condiții:

(i) $a|m$ și $b|m$.

(ii) Pentru orice $m' \in R$ care se divide prin a și 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. și $a, b, c \in R$. Atunci:

- (i) pentru $a, b \neq 0$ cu $(a, b) = d$ există a', b' cu $a = da', b = db'$ și $(a', b') = 1$;
- (ii) $(ac, bc) = (a, b)c$;
- (iii) există $[a, b]$ și $(a, b)[a, b] = ab$;
- (iv) $(a, b) = 1$ și $(a, c) = 1$ implică $(a, bc) = 1$;
- (v) $a|bc$ și $(a, b) = 1$ implică $a|c$;
- (vi) $a|c, b|c$ și $(a, b) = 1$ implică $ab|c$.

• Un element nenul și neinvertibil a al unui domeniu de integritate R se numește element *irreductibil* 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 și neinvertibil p al unui domeniu de integritate R se numește element *prim* dacă din $p|ab$ rezultă $p|a$ sau $p|b$.

Orice element prim este irreductibil.

Dacă inelul R are proprietatea c.m.m.d.c., atunci orice element irreductibil al lui R este element prim.

• Un domeniu de integritate R se numește *inel euclidian* dacă există o aplicație $\varphi : R \setminus \{0\} \rightarrow \mathbb{N}$ astfel încât pentru orice $a \in R$ și orice $b \in R \setminus \{0\}$ există $q, r \in R$ cu proprietățile:

- (i) $a = bq + r$.
- (ii) $r = 0$ sau $\varphi(r) < \varphi(b)$.

Un domeniu de integritate R se numește *inel principal* dacă orice ideal al său este principal.

Un domeniu de integritate R se numește *inel factorial* dacă orice element nenul și neinvertibil 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 șir ascendent de ideale ale sale este staționar.

• Fie R un domeniu. Următoarele afirmații sunt echivalente:

- (i) R este inel factorial.
- (ii) Orice element nenul și neinvertibil din R se scrie ca produs de elemente irreductibile și orice element irreductibil este prim.
- (iii) Orice element nenul și neinvertibil din R se scrie ca produs de elemente irreductibile și această scriere este unică abstractie făcând de asocierea în divizibilitate și de ordinea factorilor.
- (iv) Orice element nenul și neinvertibil din R se scrie ca produs de elemente irreductibile și 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. și $f \in R[X]$, atunci c.m.m.d.c al coeficienților lui f se numește *conținutul* polinomului f și 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 numește *primitiv* dacă $c(f) = 1$.

- Dacă R este un inel factorial cu corpul de fracții Q , atunci pentru $f \in R[X]$ sunt echivalente afirmațiile:

(i) f este ireductibil.

(ii) f este primitiv și ireductibil în $Q[X]$.

- *Criteriul lui Eisenstein*: Fie R un inel factorial cu corpul de fracții Q , $f = a_0 + a_1X + \dots + a_nX^n \in R[X]$ și p un element prim al lui R cu proprietățile:

(i) $p|a_0, p|a_1, \dots, p|a_{n-1}$.

(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 fracții Q , S un domeniu, $u : R \rightarrow S$ un morfism unitar de inele și $\bar{u} : R[X] \rightarrow S[X]$ extinsul acestuia (adică $\bar{u}(a_0 + a_1X + \dots + a_nX^n) = u(a_0) + u(a_1)X + \dots + u(a_n)X^n$). Dacă pentru $f \in R[X]$ avem că $\bar{u}(f)$ este ireductibil în $S[X]$ și $\text{grad } \bar{u}(f) = \text{grad } f$, atunci f este ireductibil în $Q[X]$.

- Dacă S este un inel, R un subinel al său iar $a, b \in R$, vom folosi notațiile $R[a] = \{\tilde{f}(a) \mid f \in R[X]\}$ și $R[a, b] = \{\tilde{f}(a, b) \mid f \in R[X, Y]\}$, unde \tilde{f} este funcția polinomială asociată polinomului f .

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

2. Fie $d \in \mathbb{Z}$ care nu e pătrat perfect și $N : \mathbb{Q}[\sqrt{d}] \rightarrow \mathbb{Q}$ 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) $N(\mathbb{Z}[\sqrt{d}]) \subset \mathbb{N}$. (Aplicația $N : \mathbb{Z}[\sqrt{d}] \rightarrow \mathbb{N}$ se numește *normă* pe inelul $\mathbb{Z}[\sqrt{d}]$.)

(iv) $z \in \mathbb{Z}[\sqrt{d}]$ este inversabil dacă și numai dacă $N(z) = 1$.

(v) Dacă $N(z)$ este număr prim, atunci z este element ireductibil. Dați exemple în care reciproca acestei afirmații nu este adevărată.

(vi) Dacă d este de forma $4k + 1$, atunci afirmațiile de la punctele (iii), (iv) și (v) sunt adevărate și pentru inelul $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

(vii) Determinați elementele de normă 112 din $\mathbb{Z}[i\sqrt{3}]$, $\mathbb{Z}[i\sqrt{5}]$, $\mathbb{Z}[i\sqrt{11}]$ și $\mathbb{Z}\left[\frac{1+i\sqrt{7}}{2}\right]$.

3. Fie $d \in \mathbb{Z}$ care nu e pătrat perfect și $a, b \in \mathbb{Z}[\sqrt{d}]$.

(i) Arătați că dacă $a|b$ în $\mathbb{Z}[\sqrt{d}]$, atunci $N(a)|N(b)$.

(ii) Dați exemple de situații în care reciproca afirmației de la (i) nu este adevărată.

(iii) Dacă $a|_{\mathbb{Z}\sqrt{d}} b$ și $N(a) = N(b)$, atunci $a \sim_{\mathbb{Z}\sqrt{d}} b$.

(iv) Arătați că dacă $(N(a), N(b)) = 1$, atunci 1 este c.m.m.d.c. pentru a și b .

(v) Este adevărat că dacă a și b admit c.m.m.d.c. în $\mathbb{Z}[\sqrt{d}]$, atunci norma acestuia este egală cu $(N(a), N(b))$?

(vi) Arătați că dacă d este de forma $4k + 1$, atunci afirmațiile de la punctele (i), (iii) și (iv) sunt adevărate și pentru inelul $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

4. (i) Determinați elementele inversabile ale inelului $\mathbb{Z}[\sqrt{d}]$, unde $d \in \mathbb{Z}$ și $d < 0$.

(ii) Arătați că grupul $U(\mathbb{Z}[\sqrt{2}])$ este izomorf cu grupul $\mathbb{Z}_2 \times \mathbb{Z}$.

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

6. Fie $k \in \mathbb{Z}$ și $R_k = \left\{ \begin{pmatrix} a & b \\ kb & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$. Să se arate că R_k are

divizori ai lui zero dacă și numai dacă k este pătrat perfect.

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

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

9. (i) Arătați că în inelul $\mathbb{Z}[i\sqrt{5}]$ elementele $2(1 + i\sqrt{5})$ și 6 nu au un c.m.m.d.c., dar elementele $1 + i\sqrt{5}$ și 3 au un c.m.m.d.c..

(ii) Găsiți toate descompunerile lui 6 în factori ireductibili, respectiv primi în $\mathbb{Z}[i\sqrt{5}]$.

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

11. Decideți dacă elementele

(i) $4 + i\sqrt{5}$ și $1 + 3i\sqrt{5}$

(ii) $6 + 2i\sqrt{5}$ și 14

(iii) $4 + i\sqrt{5}$ și $1 + 2i\sqrt{5}$

(iv) $6 + 3i\sqrt{5}$ și 9

(v) $2 + 8i\sqrt{5}$ și 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 $R = \{f \in \mathbb{Z}[X] \mid f = a_0 + a_2X^2 + \dots + a_nX^n, a_i \in \mathbb{Z}, n \in \mathbb{N}, n \neq 1\}$. Să se arate că:

(i) $R = \mathbb{Z}[X^2, X^3]$;

(ii) $\text{c.m.m.d.c.}(X^2, X^3) = 1$ și $\text{c.m.m.m.c.}(X^2, X^3)$ nu există;

(iii) $\text{c.m.m.d.c.}(X^5, X^6)$ și $\text{c.m.m.m.c.}(X^5, X^6)$ 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. și Q corpul său de fracții.

(i) Arătați că pentru orice $f \in R[X]$ există $\bar{f} \in R[X]$ cu $c(\bar{f}) = 1$ astfel încât $f = c(f)\bar{f}$.

Fie acum $f, g \in R[X]$. Arătați că:

(ii) $c(fg) = c(f)c(g)$.

(iii) $\bar{f}g = u\bar{f}\bar{g}$, $u \in U(R)$.

(iv) Dacă $c(f) = c(g) = 1$, atunci $f|_{Q[X]}g$ dacă și numai dacă $f|_{R[X]}g$.

- (v) $f|_{R[X]}g$ dacă și numai dacă $c(f)|_{R^c}(g)$ și $\bar{f}|_{R[X]}\bar{g}$.
 (vi) $f|_{R[X]}g$ dacă și numai dacă $c(f)|_{R^c}(g)$ și $\bar{f}|_{Q[X]}\bar{g}$.

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

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

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

17. Să se arate că inelele $\mathbb{Z}[\sqrt{2}]$ și $\mathbb{Z}[(1 + \sqrt{5})/2]$ 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 și numai dacă $d \in \{3, 7, 11\}$.

19. Fie R un domeniu de integritate. Următoarele afirmații sunt echivalente:

- (i) R este factorial.
- (ii) Orice ideal prim nenul al lui R conține un element prim.

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

21. (*Nagata*) Fie R un domeniu de integritate cu proprietatea că orice șir ascendent de ideale principale este staționar. Fie $(p_i)_{i \in I}$ o mulțime de elemente prime din R și S sistemul multiplicativ generat de această mulțime. 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. Arătați că inelul de polinoame $R[X_1, \dots, X_n]$ este inel principal dacă și numai dacă R este corp și $n = 1$.

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

- (i) $P = \{a + bi\sqrt{3} \mid a, b \in \mathbb{Z} \text{ și } a \equiv b \pmod{2}\}$;
- (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 funcție $\varphi : R \rightarrow \mathbb{N}$ cu următoarele proprietăți:

- (i) $\varphi(a) = 0$ dacă și 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. Arătați că inelele $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$, $\mathbb{Z}\left[\frac{1+i\sqrt{43}}{2}\right]$, $\mathbb{Z}\left[\frac{1+i\sqrt{67}}{2}\right]$ și $\mathbb{Z}\left[\frac{1+i\sqrt{163}}{2}\right]$ sunt principale, dar nu sunt euclidiene.

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

28. (*Samuel*) Fie k corp comutativ și $r, s, t \in \mathbb{N}^* \setminus \{1\}$ cu $(r, s) = 1$ și $t \equiv 1 \pmod{rs}$. Notăm $R = k[X, Y, Z]/(X^r + Y^s - Z^t)$.

- (i) Arătați că R este inel factorial.
- (ii) Arătați 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 $\text{char } K \neq 2$.

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

31. (i) Fie R un inel factorial care nu este corp și 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 $\text{char } K \neq 2$. Arătați 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 și numai dacă polinomul $Z^2 + 1 \in K[Z]$ are rădăcini în K .

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

(ii) Arătați 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. Arătați că dacă $\pi \in \mathbb{Z}[\sqrt{d}]$ este prim, atunci π este asociat în R cu un element prim din \mathbb{Z} sau $\pi\bar{\pi}$ este prim în \mathbb{Z} .

(ii) Fie $d \in \mathbb{Z}$ care nu e pătrat perfect, $d \equiv 1 \pmod{4}$. Arătați 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 $\pi\bar{\pi}$ este prim în \mathbb{Z} .

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

36. (*Aritmetica inelului $\mathbb{Z}[i]$*) Arătați că un element din inelul $\mathbb{Z}[i]$ este prim dacă și 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 $\mathbb{Z}[i\sqrt{2}]$*) Arătați că un element din inelul $\mathbb{Z}[i\sqrt{2}]$ este prim dacă și 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 $\mathbb{Z}[\sqrt{2}]$*) Arătați că un element din inelul $\mathbb{Z}[\sqrt{2}]$ este prim dacă și 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 $\mathbb{Z}[\sqrt{3}]$*) Arătați că un element din inelul $\mathbb{Z}[\sqrt{3}]$ este prim dacă și 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 $\mathbb{Z}[(-1 + i\sqrt{3})/2]$*) Arătați că un element din inelul $\mathbb{Z}[\rho]$, $\rho = (-1 + i\sqrt{3})/2$, este prim dacă și 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 ecuația $x^2 + y^2 = z^2$.

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

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

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

45. Fie K un corp. Să se arate că:

- (i) polinoamele $X^2 - Y$, $X^2 - Y^2Z$ și $X^2 - YZ^2$ sunt ireductibile în $K[X, Y, Z]$;
- (ii) dacă $\text{char } K \neq 2$, 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) Arătați 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) Arătați 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) $f \in \mathbb{Q}[X], f = X^{p-1} + \dots + X + 1$, unde $p \in \mathbb{N}$ este număr prim;
 (iii) $f \in \mathbb{Q}[X], f = X^{p^n} + p - 1$, unde $n, p \in \mathbb{N}$ și 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 și $(a, p) = 1$.

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 $\text{char } K \neq 2$ și $f \in K[X_1, \dots, X_n]$, $f = X_1^2 + \dots + X_n^2$. Să se arate că f este polinom ireductibil dacă și numai dacă $n \geq 3$.

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

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

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

este ireductibil.

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

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

este ireductibil.

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

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

este ireductibil.

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

Capitolul 7

Soluții: Mulțimi

1. **Soluția 1.** Presupunem prin absurd că $\bigcap_{i=1,s} A_i = \emptyset$. Fie $A_1 = \{x_1, \dots, x_r\}$. Atunci există $i_1, \dots, i_r \in \{1, \dots, s\}$ astfel încât $x_1 \notin A_{i_1}, \dots, x_r \notin A_{i_r}$. Rezultă că $A_1 \cap A_{i_1} \cap \dots \cap A_{i_r} = \emptyset$, deoarece dacă intersecția ar fi nevidă ea ar conține unul din elementele x_1, \dots, x_r ale lui A_1 , ceea ce este în contradicție cu alegerea mulțimilor A_{i_j} .

Așadar am găsit o familie constând din cel mult $r + 1$ dintre mulțimile date care au intersecția vidă, aceasta contrazicând ipoteza.

Soluția 2. Demonstrăm afirmația prin inducție după $s \geq r + 1$. Dacă $s = r + 1$ este clar. Fie acum $A'_1, A'_2, \dots, A'_{s+1}$ mulțimi finite având fiecare r elemente. Din ipoteza de inducție rezultă că intersecția 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 $1 \leq i \leq s + 1$ și observăm că $B_i \neq \emptyset$ pentru orice i , iar $B_k \cap B_l = \emptyset$ 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 obținem că

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

adică $s \leq r$, contradicție.

2. Demonstrăm afirmația prin inducție după $m \geq 1$. Pentru $m = 1$ este clar. Dacă $m > 1$, atunci presupunem că $A' = X_1 \cup \dots \cup X_{m-1}$ este o submulțime fixată a lui A . Atunci ecuația $A' \cup X_m = A$ are 2^t soluții, unde $t = |A'|$. Dar din ipoteza de inducție ecuația $X_1 \cup \dots \cup X_{m-1} = A'$ are

$(2^{m-1} - 1)^t$ soluții. Cum există C_n^t submulțimi distincte cu t elemente ale lui A , numărul soluțiilor ecuației 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 afirmația prin inducție după $n \geq 2$. Pentru $n = 2$ este evident. Dacă $n > 2$, atunci $\bigcup_{i=1,n} A_i = (\bigcup_{i=1,n-1} A_i) \cup A_n$ și aplicând formula din cazul $n = 2$ și apoi ipoteza de inducție, obținem

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

4. Fie $A = \{x_1, \dots, x_r\}$. Dacă f este injectivă, atunci $f(x_1), \dots, f(x_r)$ sunt distincte și cum $\{f(x_1), \dots, f(x_r)\} \subseteq A$ rezultă că avem egalitate în ultima incluziune, deci $f(A) = A$, adică f este surjectivă.

Dacă f este surjectivă, atunci $f(A) = A$ și deci mulțimea $f(A)$ are r elemente. Rezultă că $f(x_1), \dots, f(x_r)$ sunt distincte, deci f este injectivă.

Am demonstrat așadar că (a) și (b) sunt echivalente. Aceasta arată și că oricare dintre ele implică (c) (pentru că dacă f este injectivă și surjectivă rezultă că f este bijectivă). Faptul că (c) implică atât (a), cât și (b) este evident.

5. (a) Numărul funcțiilor definite pe M cu valori în N este n^m , după cum se poate verifica ușor prin inducție după m .

(b) Pentru ca să existe funcții injective trebuie ca $m \leq n$. În acest caz, numărul funcțiilor injective este $(n - m + 1) \cdots (n - 1)n$, după cum se poate

verifica simplu prin inducție după m .

(c) Pentru ca să existe funcții surjective trebuie ca $m \geq n$. În acest caz, fie $N = \{a_1, \dots, a_n\}$ și pentru fiecare $1 \leq i \leq n$ considerăm mulțimea

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

Atunci mulțimea funcțiilor nesurjective de la M la N este $\bigcup_{1 \leq i \leq n} A_i$, deci numărul funcțiilor surjective de la M la N este $n^m - \left| \bigcup_{1 \leq i \leq n} A_i \right|$.

Folosind principiul includerii și excluderii (vezi problema 3), avem

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

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 $|A_{i_1} \cap \dots \cap A_{i_r}| = (n-r)^m$ pentru orice $1 \leq i_1 < \dots < i_r \leq n$ (acest număr fiind de fapt numărul funcțiilor definite pe o mulțime cu m elemente cu valori într-o mulțime cu $n-r$ elemente) și atunci obținem că

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

Rezultă că numărul funcțiilor 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 mulțimea permutărilor mulțimii $\{1, 2, \dots, n\}$. Pentru fiecare $1 \leq i \leq n$ considerăm mulțimea $A_i = \{\sigma \in S_n \mid \sigma(i) = i\}$. Atunci mulțimea permutărilor care au cel puțin un punct fix este $\bigcup_{1 \leq i \leq n} A_i$ și folosind principiul includerii și excluderii (vezi problema 3) acest număr este

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

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

$\bigcup_{1 \leq i \leq n} (A_i - (\bigcup_{j \neq i} A_j))$, deci numărul lor este

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

7. Presupunem că B ar fi finită și 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 $g(x_1) < g(x_0)$ și $x_1 > x_0$. Fie $x_2 = f(x_1)$. Atunci $x_2 > x_1$ și $g(x_2) < g(x_1)$. Continuând procedeul, obținem un șir strict crescător de numere naturale $(x_n)_{n \geq 0}$ și unul strict descrescător $(g(x_n))_{n \geq 0}$ tot de numere naturale, contradicție.

8. Din (a) și (b) rezultă că $f(0) < f(1) < f(2) = 2$, deci $f(0) = 0$ și $f(1) = 1$. 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 $n \leq 6$.

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 inducție după $n \geq 1$ că $f(n(n+1)) = n(n+1)$. Pentru $n = 1$ și $n = 2$ este adevărat. Fie $n > 2$ și presupunem că afirmația este adevărată pentru $n-1$. Cum $f(n(n-1)) = n(n-1)$, rezultă că $f(k) = k$ pentru $k \leq n(n-1)$. Cum $f(n(n+1)) = f(n)f(n+1)$ și $n \leq n(n-1)$, $n+1 \leq n(n-1)$, iar $(n, n+1) = 1$, obținem că $f(n(n+1)) = f(n)f(n+1) = n(n+1)$, ceea ce trebuia demonstrat.

Observație. P. Erdős a demonstrat următorul rezultat mai general: dacă $f : \mathbb{N}^* \rightarrow \mathbb{R}$ este o funcție strict crescătoare și $f(mn) = f(m)f(n)$ 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. **Soluția 1.** Demonstrăm că dacă $u, v : \mathbb{N} \rightarrow \mathbb{N}$ sunt funcții astfel încât u este injectivă, v este surjectivă și $u \leq v$, atunci $u = v$. Presupunem prin absurd că mulțimea $A = \{n \in \mathbb{N} \mid u(n) < v(n)\}$ este nevidă. Fie atunci $B = \{u(n) \mid n \in A\}$, care este o mulțime 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 $u(x) \in B$ și este mai mic decât b , contradicție. Dacă $x \notin A$, atunci $u(x) = v(x) = b = u(a)$ și cum u este injectivă, rezultă că $a = x \notin A$, contradicție. Așadar $A = \emptyset$ și $u = v$.

Soluția 2. Notăm $u = \max(f, g)$ și $v = \min(f, g)$. 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 $u(x_0) = f(x_0)$ și $v(x_0) = g(x_0)$. 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 $u(x_1) = v(x_1)$ și $v(x_0) = v(x_1)$, contradicție. Așadar $v(x_1) > v(x_2)$. Continuând similar găsim două șiruri de numere naturale $(x_n)_{n \geq 0}$ și $(v(x_n))_{n \geq 0}$, cel din urmă strict descrescător, ceea ce este imposibil.

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

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

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

Funcția $f : \mathbb{C} \rightarrow \mathbb{C}$ definită prin $f(a + bi) = e^a + bi$ pentru orice $a, b \in \mathbb{R}$, este injectivă și nu este surjectivă. Funcția $g : \mathbb{C} \rightarrow \mathbb{C}$, $g(z) = z^2$, este surjectivă și 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 $X = \emptyset$, contradicție. Așadar $A \cup B = M$.

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

$X \cap A = Y \cap A$ și $X \cap B = Y \cap B$. 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 $X \cap A = \{x\}$ și $X \cap B = B - \{x\}$. Atunci $x \in X$ și deci $x \in X \cap B$, de unde $x \in B - \{x\}$, contradicție. Așadar $A \cap B = \emptyset$.

" \Leftarrow " Presupunem că $A \cap B = \emptyset$. Fie $(X, Y) \in \mathcal{P}(A) \times \mathcal{P}(B)$. Arătăm că $f(X \cup Y) = (X, Y)$ și de aici va rezulta că f este surjectivă. Într-adevăr, $(X \cup Y) \cap A = (X \cap A) \cup (Y \cap A) = X$ deoarece $X \subseteq A$ și $Y \cap A \subseteq B \cap A = \emptyset$ și $(X \cup Y) \cap B = (X \cap B) \cup (Y \cap B) = Y$ deoarece $Y \subseteq B$ și $X \cap B \subseteq A \cap B = \emptyset$.

(c) Echivalența rezultă din (a) și (b). În situația în care $A = C_M B$, deci f este bijectivă, inversa ei este $f^{-1} : \mathcal{P}(A) \times \mathcal{P}(B) \rightarrow \mathcal{P}(M)$, $f^{-1}(X, Y) = X \cup Y$, după cum rezultă din soluția punctului (b).

12. Dacă ar exista o funcție surjectivă $f : A \rightarrow \mathcal{P}(A)$, considerăm mulțimea $M = \{a \in A \mid a \notin f(a)\}$. Din surjectivitatea lui f rezultă că există $b \in A$ cu $f(b) = M$. Dacă $b \in M$, atunci din definiția lui M rezultă că $b \notin f(b) = M$, contradicție. Dacă $b \notin M$, atunci $b \in f(b) = M$, din nou contradicție.

13. (a) \Rightarrow (b) Fie $u, v : X \rightarrow M$ funcții astfel încât $fu = fv$. Dacă $x \in X$ avem $fu(x) = fv(x)$, deci $f(u(x)) = f(v(x))$, și cum f este injectivă rezultă că $u(x) = v(x)$. Obținem 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 $x_1, x_2 \in M$ și $f(x_1) = f(x_2) = y$, atunci fie $u, v : \{0\} \rightarrow M$ 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 $a \in M$ și definim $g : N \rightarrow M$ 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 $f(x) = f(y)$. Știm că există o funcție $g : N \rightarrow M$ 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 $f(\bigcap_{i \in I} M_i) \subseteq f(M_j)$, și 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 și fie $x, y \in M$, $x \neq y$, cu $f(x) = f(y)$. Fie $M_1 = \{x\}$ și $M_2 = \{y\}$. Atunci $f(M_1) \cap f(M_2) = \{f(x)\}$, dar $f(M_1 \cap M_2) = f(\emptyset) = \emptyset$, contradicție.

15. (a) \Rightarrow (c) Pentru fiecare $n \in N$ alegem un element $x_n \in M$ astfel încât $f(x_n) = n$. Definim $g : N \rightarrow M$ prin $g(n) = x_n$ pentru orice $n \in N$. Evident are loc $fg = 1_N$.

(c) \Rightarrow (b) Fie $u, v : N \rightarrow Y$ 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 $Y = \{0, 1\}$ și funcțiile $u, v : N \rightarrow Y$ definite prin $u(n) = 0$ dacă $n \neq n_0$, $u(n_0) = 1$ și $v(n) = 0$ pentru orice $n \in N$. Atunci $uf = vf$, dar $u \neq v$, contradicție.

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 $x = y \in Y$. Așadar $X \subseteq Y$ și 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 $f_*(\{a\}) = f_*(\{x\})$ și cum f_* este injectivă rezultă că $\{a\} = \{x\}$, deci $a = x \in X$. Așadar $f^{-1}(f(X)) \subseteq X$, ceea ce arată egalitatea.

(c) \Rightarrow (d) Cum $f^* \circ f_*$ este surjectivă, rezultă că și f^* este surjectivă.

(d) \Rightarrow (e) Presupunem prin absurd că există $X \subseteq M$ și $y \in N$ cu $y \in f(C_M X)$ și $y \notin C_N f(X)$. Atunci $y = f(a)$ cu $a \notin X$ și $y \in f(X)$, 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 și $x \in f^{-1}(Y) = \{a\}$, contradicție.

(e) \Rightarrow (a) Presupunem prin absurd că f nu este injectivă. Fie $a, b \in M$ cu $a \neq b$ și $f(a) = f(b)$. 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 $f(a) \notin C_N f(X)$, contradicție.

(ii) Se demonstrează similar cu (i).

17. (a) Definim aplicațiile $f : \text{Fun}(A, \text{Fun}(B, C)) \rightarrow \text{Fun}(A \times B, C)$ și $g : \text{Fun}(A \times B, C) \rightarrow \text{Fun}(A, \text{Fun}(B, C))$ prin $f(u)(a, b) = u(a)(b)$ și $g(v)(a)(b) = v(a, b)$ pentru orice $u \in \text{Fun}(A, \text{Fun}(B, C))$, $v \in \text{Fun}(A \times B, C)$, $a \in A, b \in B$. Atunci

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

și

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

ceea ce arată că $f \circ g$ și $g \circ f$ sunt aplicațiile identice, deci f și g sunt inverse una celeilalte.

(b) Notăm cu $p_B : B \times C \rightarrow B$ și $p_C : B \times C \rightarrow C$ proiecțiile canonice.

Definim aplicația $f : \text{Fun}(A, B \times C) \rightarrow \text{Fun}(A, B) \times \text{Fun}(A, C)$ prin $f(u) = (p_B u, p_C u)$.

Dacă $f(u) = f(v)$, atunci $p_B u = p_B v$ și $p_C u = p_C v$, de unde $u(a) = (p_B u(a), p_C u(a)) = (p_B v(a), p_C v(a)) = v(a)$, deci $u = v$. Obținem că f este injectivă.

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

18. Este imediat că \sim este reflexivă, simetrică și tranzitivă. Fie $f : \mathbb{R} \rightarrow [0, 1)$, $f(x) = \{x\}$, unde prin $\{x\}$ notăm partea fracționară 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 relația de echivalență asociată funcției f . Din proprietatea de universalitate a mulțimii factor rezultă că există o funcție $f' : \mathbb{R}/\sim \rightarrow [0, 1)$ astfel încât $f'p = f$, unde $p : \mathbb{R} \rightarrow \mathbb{R}/\sim$ este proiecția canonică. Cum $\sim = \rho_f$, avem că f' este injectivă, iar surjectivitatea lui f arată că f' este surjectivă. Prin urmare f' este o bijecție.

19. Se verifică imediat că ρ este reflexivă, antisimetrică și tranzitivă, deci este relație de ordine. Dacă $x = 1$ și $y = 3/2$, atunci nici una din relațiile xpy și $y\rho x$ 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 $n \geq 1$ și $s_1, \dots, s_{n-1} \in M$ cu $x(\rho \cup \rho^{-1})s_1, \dots, s_{n-1}(\rho \cup \rho^{-1})y$. Este ușor de văzut că relația $\rho \cup \rho^{-1}$ este simetrică și atunci obținem că $y\Delta_M x$ și $y(\rho \cup \rho^{-1})s_{n-1}, \dots, s_1(\rho \cup \rho^{-1})x$, 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 $x\rho'y$ și $y\rho'z$. Dacă $x = y$ sau $y = z$ este clar că $x\rho'z$. Altfel, există $m, n \geq 1$ cu $x(\rho \cup \rho^{-1})^m y$ și $y(\rho \cup \rho^{-1})^n z$. Aceasta arată că $x(\rho \cup \rho^{-1})^{m+n} z$, de unde $x\rho'z$.

Arătăm că ρ' este cea mai mică relație de echivalență care include pe ρ . Fie ρ'' o altă relație de echivalență cu $\rho \subseteq \rho''$. Este clar că $\rho \cup \rho^{-1} \subseteq \rho''$ și $\Delta_M \subseteq \rho''$. Dacă $x(\rho \cup \rho^{-1})^n y$, atunci există $s_1, \dots, s_{n-1} \in M$ cu $x(\rho \cup \rho^{-1})s_1, \dots, s_{n-1}(\rho \cup \rho^{-1})y$. Cum $\rho \cup \rho^{-1} \subseteq \rho''$, avem și $x\rho''s_1, \dots, s_{n-1}\rho''y$, deci cum ρ'' este tranzitivă avem și $x\rho''y$. Obținem că $(\rho \cup \rho^{-1})^n \subseteq \rho''$ pentru orice n , și de aici rezultă că $\rho' \subseteq \rho''$.

21. Verificăm mai întâi că ρ este relație de echivalență.

- ρ este reflexivă: avem $(x_1, \dots, x_n)\rho(x_1, \dots, x_n)$ deoarece $x_i\rho_i x_i$ pentru orice $1 \leq i \leq n$, ρ_i fiind reflexivă.
- ρ este simetrică: dacă $(x_1, \dots, x_n)\rho(y_1, \dots, y_n)$, 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 $(y_1, \dots, y_n)\rho(x_1, \dots, x_n)$.
- ρ este tranzitivă: dacă $(x_1, \dots, x_n)\rho(y_1, \dots, y_n)$ și $(y_1, \dots, y_n)\rho(z_1, \dots, z_n)$, atunci pentru orice i avem $x_i\rho_i y_i$ și $y_i\rho_i z_i$, și din tranzitivitatea lui ρ_i rezultă că $x_i\rho_i z_i$, ceea ce arată că $(x_1, \dots, x_n)\rho(z_1, \dots, z_n)$.

Vom construi o bijecție de la M/ρ la $M_1/\rho_1 \times \dots \times M_n/\rho_n$ folosind proprietatea de universalitate a mulțimii factor. Fie $f : M \rightarrow M_1/\rho_1 \times \dots \times M_n/\rho_n$ funcția definită prin $f(x_1, \dots, x_n) = (\widehat{x_1}, \dots, \widehat{x_n})$, unde pe poziția i am notat prin $\widehat{x_i}$ clasa de echivalență a lui x_i în mulțimea factor M_i/ρ_i . Notăm cu ρ_f relația de echivalență pe M asociată funcției f . Avem $(x_1, \dots, x_n)\rho_f(y_1, \dots, y_n) \Leftrightarrow f(x_1, \dots, x_n) = f(y_1, \dots, y_n) \Leftrightarrow \widehat{x_i} = \widehat{y_i}$ pentru orice $i \Leftrightarrow x_i\rho_i y_i$ pentru orice $i \Leftrightarrow (x_1, \dots, x_n)\rho(y_1, \dots, y_n)$, deci $\rho = \rho_f$. Atunci există $f' : M/\rho \rightarrow M_1/\rho_1 \times \dots \times M_n/\rho_n$ astfel încât $f'p = f$, unde $p : M \rightarrow M/\rho$ este proiecția canonică. Cum $\rho = \rho_f$, avem că f' este injectivă. Este evident că f este surjectivă, de unde și f' este surjectivă. Prin urmare f' este bijectivă.

22. Fie R_k mulțimea relațiilor de echivalență ρ pe M cu proprietatea că mulțimea factor M/ρ are k elemente. Notăm cu $N_{m,k} = |R_k|$. Numărul relațiilor de echivalență pe M este $N_{m,1} + \dots + N_{m,m}$.

Pentru a calcula $N_{m,k}$ să observăm că oricărui $\rho \in R_k$ îi putem asocia o surjecție de la M la mulțimea $\{1, \dots, k\}$ în modul următor: compunem o bijecție de la M/ρ la $\{1, \dots, k\}$ cu proiecția canonică $p : M \rightarrow M/\rho$. Invers, oricărei surjecții $f : M \rightarrow \{1, \dots, k\}$ îi asociem relația de echivalență ρ_f , care se află în R_k , deoarece din proprietatea de universalitate a mulțimii factor

există $f' : M/\rho_f \rightarrow \{1, \dots, k\}$ cu $f'p = f$, și atunci f' este bijectivă, deci $|M/\rho_f| = k$.

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

Așadar, la $k!$ surjecții corespunde aceeași relație de echivalență în corespondența descrisă mai sus, deci $N_{m,k} = S_{m,k}/k!$, unde $S_{m,k}$ este numărul surjecțiilor definite pe o mulțime cu m elemente cu valori într-o mulțime cu k elemente, care a fost calculat în problema 5.

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

24. Este imediat că ρ este relație de echivalență. Fie $F : B^A \rightarrow B^{A'}$ definită prin $F(f) = f|_{A'}$. Atunci $f\rho g \Leftrightarrow f|_{A'} = g|_{A'} \Leftrightarrow F(f) = F(g)$, deci $\rho = \rho_F$ și din proprietatea de universalitate a mulțimii factor există $F' : B^A/\rho \rightarrow B^{A'}$ injectivă cu $F'p = F$, unde $p : B^A \rightarrow B^A/\rho$ este proiecția canonică. Pentru a arăta că F' este și surjectivă este suficient să arătăm că F este surjectivă. Pentru aceasta fie $g \in B^{A'}$ și fie $b \in B$. Definim $f : A \rightarrow B$ prin $f(a) = g(a)$ dacă $a \in A'$ și $f(a) = b$ 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 $1_A : A \rightarrow A$ este bijectivă.
(b) Cum $A \sim B$, există o bijecție $f : A \rightarrow B$. Atunci $f^{-1} : B \rightarrow A$ este bijecție, deci $B \sim A$.
(c) Dacă $f : A \rightarrow B$ și $g : B \rightarrow C$ sunt bijecții, atunci $gf : A \rightarrow C$ este bijecție, deci $A \sim C$.

26. (a) Fie $f : X_0 \rightarrow X_2$ o bijecție. Definim prin recurență șirul de mulțimi $(X_n)_{n \geq 3}$ prin $X_n = f(X_{n-2})$ pentru orice $n \geq 3$. Se demonstrează imediat prin inducție că $X_n \supseteq X_{n+1}$ pentru orice $n \geq 0$. Notăm $A = \bigcap_{n \geq 0} X_n$

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

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

Pentru prima egalitate, fie $a \in X_0$. Dacă $a \in A$, atunci evident a aparține membrului drept. Dacă $a \notin A$, fie n cel mai mic număr natural pentru care $a \notin X_n$. Evident $n > 0$. Atunci $a \in X_{n-1}$ și $a \notin X_n$, deci $a \in B_{n-1}$, așadar a aparține și membrului drept. Incluziunea inversă este clară, toate mulțimile din reuniune fiind submulțimi ale lui X_0 . A doua egalitate se demonstrează similar.

În plus, observăm că în fiecare din cele două relații demonstrate în membrul drept avem o reuniune disjunctă de mulțimi (adică intersecția oricăror două mulțimi 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 funcția $g_n : B_n \rightarrow B_{n+2}$ prin $g_n(x) = f(x)$ pentru orice $x \in B_n$. Este clar că g_n este bijectivă. Definim acum $g : X_0 \rightarrow X_1$ astfel:

- $g(x) = x$ pentru orice $x \in A \cup \left(\bigcup_{n \geq 0} B_{2n+1} \right)$.
- $g(x) = g_{2n}(x)$ dacă $x \in B_{2n}$, $n \in \mathbb{N}$.

Atunci g este bijectivă, și aceasta arată că există o bijecție între X_0 și X_1 .

(b) Fie $\alpha = |A| = |A'|$ și $\beta = |B| = |B'|$ numere cardinale. Considerăm bijecțiile $u : A \rightarrow A'$ și $v : B \rightarrow B'$ și presupunem că există o funcție injectivă $f : A \rightarrow B$. Atunci $vf u^{-1} : A' \rightarrow B'$ este injectivă, deci definiția nu depinde de reprezentanții A și B .

(c) Fie $\alpha = |A|$ și $\beta = |B|$. Cum $\alpha \leq \beta$ și $\beta \leq \alpha$, rezultă că există funcții injective $f : A \rightarrow B$ și $g : B \rightarrow A$. Atunci $f(A) \subseteq B$ și $gf(A) \subseteq g(B) \subseteq A$.

Dar dacă $u : X \rightarrow Y$ este o funcție injectivă, atunci $X \sim u(X)$. Aplicând această observație de două ori obținem că $A \sim f(A) \sim gf(A)$ și atunci conform punctului (a) rezultă că $A \sim g(B)$. Dar $g(B) \sim B$, de unde $A \sim B$.

27. Fie $\alpha = |A|$ și $\beta = |B|$. Considerăm mulțimea

$$\mathcal{F} = \{(X, f) \mid X \subseteq A \text{ și } f : X \rightarrow B \text{ funcție injectivă}\}.$$

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

X_1 este f_1 . Arătăm că \mathcal{F} este inductiv ordonată cu această relație de ordine. Fie $(X_i, f_i)_{i \in I}$ un lanț (submulțime total ordonată) în \mathcal{F} . Arătăm că el are un majorant în \mathcal{F} . Pentru aceasta fie $X = \bigcup_{i \in I} X_i$ și $f : X \rightarrow B$

funcția definită astfel: dacă $x \in X$, alegem un $i \in I$ cu $x \in X_i$, și definim $f(x) = f_i(x)$. Definiția lui f este corectă. Într-adevăr, fie $x \in X_i$ și $x \in X_j$. 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) știm că f_i este restricția lui f_j la X_i , deci cum $x \in X_i$, avem că $f_j(x) = f_i(x)$.

Funcția f definită mai sus este injectivă, deoarece dacă $x, y \in X$ cu $f(x) = f(y)$, atunci există $i, j \in I$ cu $x \in X_i$ și $y \in X_j$. Presupunem, de exemplu, că $(X_j, f_j) \leq (X_i, f_i)$, și atunci $f(x) = f_i(x)$ și $f(y) = f_j(y) = f_i(y)$. Din injectivitatea lui f_i rezultă că $x = y$. Așadar $(X, f) \in \mathcal{F}$ și $(X_i, f_i) \leq (X, f)$ 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 funcție injectivă $g' : B \rightarrow Y$ și 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 $a \in A - Y$ și definim funcția $f : Y \cup \{a\} \rightarrow B$ prin $f|_Y = g$ și $f(a) = b$. Atunci $(Y \cup \{a\}, f) \in \mathcal{F}$ și această pereche este strict mai mare ca (Y, g) , contradicție. Așadar $Y = A$ și 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 condiții.

28. (a) Fie X o mulțime infinită și $x_0 \in X$. Atunci $X - \{x_0\}$ este nevidă, deci există $x_1 \in X$, $x_1 \neq x_0$. Construim inductiv un șir $(x_n)_{n \in \mathbb{N}}$ astfel: dacă am definit $x_0, \dots, x_n \in X$, oricare două distincte, atunci $X - \{x_0, \dots, x_n\}$ este nevidă (altfel ar rezulta $X = \{x_0, \dots, x_n\}$), deci există $x_{n+1} \in X$ și x_{n+1} să fie diferit de toți x_0, \dots, x_n .

Definim acum funcția injectivă $f : \mathbb{N} \rightarrow X$ prin $f(n) = x_n$ pentru orice $n \in \mathbb{N}$. Rezultă că $|\mathbb{N}| \leq |X|$.

(b) Fie $F = \{y_0, \dots, y_r\}$. Mulțimea $X - F$ este infinită, altfel $X = F \cup (X - F)$ ar fi finită. Atunci, din (i), există o submulțime numărabilă A a lui $X - F$. Fie $A = \{a_0, a_1, \dots\}$. Definim funcția $f : X \rightarrow X - F$ 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 și β putem alege mulțimi A și B cu $|A| = \alpha$, $|B| = \beta$ și $A \cap B = \emptyset$. Într-adevăr, dacă U și V sunt mulțimi cu $|U| = \alpha$ și $|V| = \beta$, putem lua $A = U \times \{1\}$ și $B = V \times \{2\}$.

(a) Dacă $\alpha = |A| = |A'|$ și $\beta = |B| = |B'|$ cu $A \cap B = \emptyset$ și $A' \cap B' = \emptyset$, fie $f : A \rightarrow A'$ și $g : B \rightarrow B'$ bijecții. Atunci funcția $u : A \cup B \rightarrow A' \cup B'$ definită prin $u(x) = f(x)$ dacă $x \in A$, și $u(x) = g(x)$ 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 $\alpha + \beta = |A \cup B| = |B \cup A| = \beta + \alpha$ și $(\alpha + \beta) + \gamma = |(A \cup B) \cup C| = |A \cup (B \cup C)| = \alpha + (\beta + \gamma)$.

(c) Demonstrăm mai întâi că $\alpha + \alpha = \alpha$. Fie $\alpha = |A|$, unde A este mulțime infinită. Considerăm mulțimea

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

Arătăm că \mathcal{F} este nevidă. Pentru aceasta fie o funcție injectivă $u : \mathbb{N} \rightarrow A$ (existența unei astfel de funcții este asigurată de problema 28). Notăm $X = u(\mathbb{N})$ și $x_n = u(n)$ pentru orice $n \in \mathbb{N}$. Atunci aplicația $f : X \times \{0, 1\} \rightarrow X$ definită prin $f(x_n, 0) = x_{2n}$ și $f(x_n, 1) = x_{2n+1}$ pentru orice $n \in \mathbb{N}$, este bijectivă, deci $(X, f) \in \mathcal{F}$.

Definim pe \mathcal{F} o relație de ordine astfel: $(X, f) \leq (Y, g)$ dacă și numai dacă $X \subseteq Y$ și $g(t) = f(t)$ pentru orice $t \in X \times \{0, 1\}$. Atunci (\mathcal{F}, \leq) este o mulțime inductiv ordonată. Într-adevăr, fie $(X_i, f_i)_{i \in I}$ un lanț în \mathcal{F} . Luăm $X = \bigcup_{i \in I} X_i$ și definim $f : X \times \{0, 1\} \rightarrow X$ astfel: dacă $t \in X \times \{0, 1\}$, atunci există $i \in I$ cu $t \in X_i \times \{0, 1\}$ și punem $f(t) = f_i(t)$. Definiția este corectă, deoarece dacă $t \in X_i \times \{0, 1\}$ și $t \in X_j \times \{0, 1\}$, atunci din condiția de lanț putem presupune, de exemplu, că $(X_i, f_i) \leq (X_j, f_j)$ și obținem $f_i(t) = f_j(t)$. Deoarece fiecare f_i este surjectivă, rezultă că și f este surjectivă.

Arătăm că f este injectivă. Dacă $f(t) = f(t')$, fie $i, j \in I$ cu $t \in X_i \times \{0, 1\}$ și $t' \in X_j \times \{0, 1\}$. Ca mai sus putem presupune că $(X_i, f_i) \leq (X_j, f_j)$ și atunci $f(t) = f_i(t) = f_j(t)$ și $f(t') = f_j(t')$. Cum f_j este injectivă, rezultă că $t = t'$.

Prin urmare $(X, f) \in \mathcal{F}$ și această pereche este un majorant pentru lanțul 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 submulțime numărabilă a lui $A - Y$ și $h : C \times \{0, 1\} \rightarrow C$ o bijecție construită

ca în prima parte a soluției. Atunci aplicația $p : (Y \cup C) \times \{0, 1\} \rightarrow (Y \cup C)$ definită prin $p(t) = g(t)$ dacă $t \in Y \times \{0, 1\}$ și $p(t) = h(t)$ dacă $t \in C \times \{0, 1\}$, este bijectivă, deoarece g și h sunt bijecții. Prin urmare $(Y \cup C, p) \in \mathcal{F}$ și $(Y, g) < (Y \cup C, p)$, contradicție cu maximalitatea lui (Y, g) .

Așadar $A - Y$ este finită și 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 $\alpha = |A| = |A'|$ și $\beta = |B| = |B'|$. Considerăm bijecțiile $f : A \rightarrow A'$ și $g : B \rightarrow B'$. Atunci aplicația $u : A \times B \rightarrow A' \times B'$ 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 aplicația $f : (A \times B) \times C \rightarrow A \times (B \times C)$, $f((a, b), c) = (a, (b, c))$ este bijectivă, deci $(\alpha\beta)\gamma = |(A \times B) \times C| = |A \times (B \times C)| = \alpha(\beta\gamma)$.

Apoi $g : A \times B \rightarrow B \times A$, $g(a, b) = (b, a)$, este bijectivă, deci $\alpha\beta = |A \times B| = |B \times A| = \beta\alpha$ și $A \times (B \cup C) = (A \times B) \cup (A \times C)$, deci $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

(c) Dacă α este un număr cardinal infinit, arătăm mai întâi că $\alpha\alpha = \alpha$. Considerăm mulțimea

$$\mathcal{F} = \{(X, f) \mid \emptyset \neq X \subseteq A \text{ și } f : X \times X \rightarrow X \text{ bijecție}\}.$$

Pentru a arăta că \mathcal{F} este nevidă, observăm mai întâi că există o bijecție $u : \mathbb{N}^* \times \mathbb{N}^* \rightarrow \mathbb{N}^*$ definită prin $u(m, n) = 2^{m-1}(2n - 1)$. Considerăm o submulțime numărabilă X a lui A și atunci u induce o bijecție $u' : X \times X \rightarrow X$ via o bijecție între \mathbb{N}^* și X . Rezultă că $(X, u') \in \mathcal{F}$.

Definim pe \mathcal{F} o relație de ordine astfel: $(X, f) \leq (Y, g)$ dacă și numai dacă $X \subseteq Y$ și $g(t) = f(t)$ pentru orice $t \in X \times X$. Arătăm că (\mathcal{F}, \leq) este o mulțime inductiv ordonată. Fie $(X_i, f_i)_{i \in I}$ un lanț din \mathcal{F} . Luăm $X = \bigcup_{i \in I} X_i$

și definim $f : X \times X \rightarrow X$ astfel: dacă $t \in X \times X$, atunci există $i \in I$ cu $t \in X_i \times X_i$ și definim $f(t) = f_i(t)$. Definiția este corectă, deoarece dacă $t \in X_i \times X_i$ și $t \in X_j \times X_j$, atunci din condiția de lanț putem presupune, de exemplu, că $(X_i, f_i) \leq (X_j, f_j)$ și obținem $f_i(t) = f_j(t)$.

Deoarece fiecare f_i este surjectivă, rezultă că și f este surjectivă.

Arătăm că f este injectivă. Dacă $f(t) = f(t')$, fie $i, j \in I$ cu $t \in X_i \times X_i$ și

$t' \in X_j \times X_j$. Ca mai sus putem presupune că $(X_i, f_i) \leq (X_j, f_j)$ și atunci $f(t) = f_i(t) = f_j(t)$ și $f(t') = f_j(t')$. Cum f_j este injectivă, rezultă că $t = t'$. Prin urmare $(X, f) \in \mathcal{F}$ și această pereche este un majorant pentru lanțul dat.

Din lema lui Zorn rezultă că \mathcal{F} are un element maximal (Y, g) . Arătăm că $|A - Y| < |Y|$. Altfel, am avea $|Y| \leq |A - Y|$ și putem alege $D \subseteq A - Y$ cu $|D| = |Y|$. Atunci $(Y \cup D) \times (Y \cup D) = (Y \times Y) \cup (Y \times D) \cup (D \times Y) \cup (D \times D)$ și evident reuniunea din membrul drept al ultimei egalități 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 existența bijecției g , și de asemenea faptul că $|Y| + |Y| = |Y|$, care rezultă din problema 29. Prin urmare există o bijecție $h : (Y \times D) \cup (D \times Y) \cup (D \times D) \rightarrow D$ și atunci putem obține din g și h o bijecție $u : (Y \cup D) \times (Y \cup D) \rightarrow Y \cup D$. Aceasta este o contradicție, deoarece ar rezulta că $(Y \cup D, u)$ este un element din \mathcal{F} mai mare strict ca (Y, g) .

Așadar $|A - Y| < |Y|$ și 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 $\beta \neq |\emptyset|$ și $\beta \leq \alpha$, atunci $\alpha \leq \alpha\beta \leq \alpha\alpha = \alpha$, de unde rezultă că $\alpha\beta = \alpha$.

31. (a) Fie A o mulțime cu $|A| = \alpha$. Cum $|A_i| \leq \alpha$, există o aplicație injectivă $f_i : A_i \rightarrow A$. Definim o funcție $f : \bigcup_{i \in I} A_i \rightarrow A \times I$ astfel: dacă $a \in \bigcup_{i \in I} A_i$, alegem $i \in I$ cu $a \in A_i$ și definim $f(a) = (f_i(a), i)$. Să observăm că se pot obține mai multe astfel de funcții, depinzând de alegerile făcute, dar noi considerăm una dintre aceste funcții. Este clar că f este injectivă și atunci $|\bigcup_{i \in I} A_i| \leq |A \times I| = \alpha|I|$.

(b) Rezultă imediat din (a), considerând $\alpha = |\mathbb{N}|$ și I o mulțime numărabilă.

(c) Aplicația $A \rightarrow \mathcal{P}_f(A)$ 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 submulțime finită S a lui A , $S = \{a_1, \dots, a_n\}$, asociem elementul $(a_1, \dots, a_n) \in A^n$. Aceasta definește o aplicație injectivă $\mathcal{P}_f(A) \rightarrow \bigcup_{n \in \mathbb{N}^*} A^n$, deci $|\mathcal{P}_f(A)| \leq \left| \bigcup_{n \in \mathbb{N}^*} A^n \right| \leq |A| |\mathbb{N}^*| = |A|$, ultima inegalitate rezultând din (a). Aplicăm acum Teorema Cantor-Schröder-Bernstein (vezi problema 26) și obținem $|A| = |\mathcal{P}_f(A)|$.

32. (a) Fie $\alpha = |A| = |A'|$ și $\beta = |B| = |B'|$. Considerăm bijecțiile $u : A \rightarrow A'$ și $v : B \rightarrow B'$. Atunci aplicația $\Phi : \text{Fun}(B, A) \rightarrow \text{Fun}(B', A')$ definită prin $\Phi(f) = ufv^{-1}$ este bijectivă, după cum se poate verifica imediat, și deci definiția lui α^β nu depinde de reprezentanți.

(b) Rezultă din problema 17.

(c) Pentru fiecare submulțime $B \subseteq A$ considerăm funcția caracteristică asociată, mai precis funcția $\chi_B : A \rightarrow \{0, 1\}$, $\chi_B(a) = 0$ dacă $a \notin B$ și $\chi_B(a) = 1$ dacă $a \in B$. Se verifică imediat că funcția $\Psi : \mathcal{P}(A) \rightarrow \text{Fun}(A, \{0, 1\})$, $\Psi(B) = \chi_B$, este bijectivă. De aici rezultă că $|\mathcal{P}(A)| = 2^{|A|}$.

33. Notăm cu A mulțimea 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 funcție surjectivă $f : \mathbb{Z} \times \mathbb{Z}^* \rightarrow \mathbb{Q}$, $f(m, n) = m/n$, și de aici rezultă că $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}^*| = |\mathbb{Z}| |\mathbb{Z}^*| = |\mathbb{Z}| |\mathbb{Z}| = |\mathbb{Z}|$. Cum evident $|\mathbb{Z}| \leq |\mathbb{Q}|$, obținem că $|\mathbb{Z}| = |\mathbb{Q}|$.

Funcția $g : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{C}$, $g(a, b) = a + bi$, este o bijecție, și deci $|\mathbb{C}| = |\mathbb{R} \times \mathbb{R}| = |\mathbb{R}| |\mathbb{R}| = |\mathbb{R}|$.

Funcția $\tan : (-\frac{\pi}{2}, \frac{\pi}{2}) \rightarrow \mathbb{R}$ este bijectivă, deci $|(-\frac{\pi}{2}, \frac{\pi}{2})| = |\mathbb{R}|$. De asemenea pentru orice numere reale $a < b$ și $c < d$, funcția liniară $f : (a, b) \rightarrow (c, d)$, $f(x) = \frac{d-c}{b-a}x + \frac{cb-da}{b-a}$, este bijectivă, deci $|(a, b)| = |(c, d)|$. În consecință 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 $|B| \leq |\mathbb{R}|$ și $|\mathbb{N}| \leq |B|$ (pentru a doua inegalitate observăm, de exemplu, că funcția $g : \mathbb{N} \rightarrow B$, $g(n) = \frac{1}{n+2}$, este injectivă). Arătăm că $|\mathbb{N}| \neq |B|$. Într-adevăr, dacă $|\mathbb{N}| = |B|$, am avea o bijecție $h : \mathbb{N}^* \rightarrow [0, 1)$. Pentru fiecare $n \in \mathbb{N}^*$ considerăm scrierea zecimală a lui $h(n)$, $h(n) = 0, a_{n1}a_{n2} \dots$, 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 $0, u_1u_2 \dots$ cu u_1, u_2, \dots 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 și de a_{nn} . Fie $y = 0, u_1 u_2 \dots \in [0, 1)$. Atunci $y \notin \text{Im}(h)$, 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, contradicție. Rămâne că $|\mathbb{N}| \neq |\mathbb{B}|$. Atunci $|\mathbb{N}| < |\mathbb{B}| \leq |\mathbb{R}|$, deci $|\mathbb{N}| < |\mathbb{R}|$.

34. Să presupunem că ar exista o funcție f cu proprietatea din enunț. Fie $I_n = [n, n+1)$, $n \in \mathbb{Z}$. Atunci $|\text{Im}(f) \cap I_n| \leq 1$, 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 $\text{Im}(f) = \text{Im}(f) \cap \mathbb{R} = \text{Im}(f) \cap \left(\bigcup_{n \in \mathbb{Z}} I_n \right) = \bigcup_{n \in \mathbb{Z}} (\text{Im}(f) \cap I_n)$, care este o reuniune numărabilă de mulțimi de cardinal 0 sau 1, deci este cel mult numărabilă. Dar relația dată arată că f este injectivă, deci \mathbb{R} este în bijecție cu $\text{Im}(f)$. Ar rezulta că \mathbb{R} este cel mult numărabilă, contradicție (ținem 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 $x \in (0, \infty)$ aparține exact unui interval I_k . Definim $g : \mathbb{R} \rightarrow \mathbb{N}$ prin $g(x) = k$, unde k este unicul număr natural pentru care $f(x) \in I_k$. Cum \mathbb{R} este nenumărabilă și $\mathbb{R} = g^{-1}(\mathbb{N}) = \bigcup_{k \in \mathbb{N}} g^{-1}(\{k\})$, 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 $x_1, \dots, x_{k+1} \in g^{-1}(\{k\})$ distincte și obținem că $f(x_1), \dots, f(x_{k+1}) > \frac{1}{k+1}$, deci $f(x_1) + \dots + f(x_{k+1}) > 1$.

36. Notăm cu A mulțimea 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 $p_a < a < q_a$ și definim $g : A \rightarrow \mathbb{Q} \times \mathbb{Q}$ 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 $p_a = p_b = p$ și $q_a = q_b = q$, atunci $(p, q) \subseteq V_a \cap V_b$, de unde $f(b) < f(a)$ și $f(a) < f(b)$, contradicție.

Din injectivitatea lui g rezultă că $|A| \leq |\mathbb{Q} \times \mathbb{Q}|$ și cum $\mathbb{Q} \times \mathbb{Q}$ este numărabilă, rezultă că A este cel mult numărabilă.

Similar mulțimea punctelor de minim local strict ale lui f este cel mult numărabilă, de unde rezultă că mulțimea punctelor de extrem local strict ale lui f este cel mult numărabilă ca reuniune de două mulțimi cel mult

numărăbile.

37. Este imediat că \sim este relație de echivalență.

Să observăm că pentru $x \in \mathbb{R}$ avem $\hat{x} = \{x + q \mid q \in \mathbb{Q}\}$, deci \hat{x} este mulțime numărabilă. Fie $(x_i)_{i \in I}$ un sistem de reprezentanți pentru clasele de echivalență. Atunci $\mathbb{R} = \bigcup_{i \in I} \hat{x}_i$. De aici rezultă că I nu poate fi cel mult numărabilă, altfel \mathbb{R} ar fi reuniune cel mult numărabilă de mulțimi numărabile, deci numărabilă. Așadar $|\mathbb{N}| < |\mathbb{R}/\sim|$. Pe de altă parte este clar că $|\mathbb{R}/\sim| \leq |\mathbb{R}|$. Folosind ipoteza continuului, care spune că între $|\mathbb{N}|$ și $|\mathbb{R}|$ nu mai există alte numere cardinale, obținem că $|\mathbb{R}/\sim| = |\mathbb{R}|$.

38. Este suficient să considerăm o bijecție între \mathbb{N} și \mathbb{Z} și să transferăm relația de ordine uzuală de pe \mathbb{N} (împreună cu care \mathbb{N} este mulțime bine ordonată) la o relație de ordine pe \mathbb{Z} .

De exemplu, scriem elementele lui \mathbb{Z} sub forma unui șir astfel: $0, 1, -1, 2, -2, \dots$. Definim pe \mathbb{Z} relația ρ astfel: $a\rho b$ dacă și numai dacă a este la stânga lui b în acest șir. Atunci ρ este relație de ordine pe \mathbb{Z} și (\mathbb{Z}, ρ) este bine ordonată.

Capitolul 8

Soluții: Legi de compoziție. Semigrupuri și monoizi

1. (i) A defini o lege de compoziție pe M este același lucru cu a da o aplicație $f : M \times M \rightarrow M$. 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 $M = \{x_1, \dots, x_n\}$. A da o lege de compoziție comutativă pe M este același lucru cu a da o aplicație $f : M \times M \rightarrow M$ cu $f(x, y) = f(y, x)$ pentru orice $x, y \in M$. Dar aceasta este tot una cu a da o aplicație $g : \{(x_i, x_j) \mid 1 \leq i \leq j \leq n\} \rightarrow M$. Cum prima mulțime 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 compoziție care are elementul neutru e este același lucru cu a da o funcție $f : M \times M \rightarrow M$ pentru care $f(x, e) = f(e, x) = x$ pentru orice $x \in M$. Aceasta este echivalent cu a da o aplicație $g : \{(x, y) \mid x, y \in M - \{e\}\} \rightarrow M$, ceea ce se poate face în $n^{(n-1)^2}$ moduri. Dar oricare element al lui M poate fi ales ca element neutru și cum elementul neutru este unic rezultă că avem $n^{(n-1)^2+1}$ legi de compoziție cu element neutru definite pe M .

2. Fie T_n numărul de moduri în care se pot pune parantezele în produsul $x_1 x_2 \dots x_n$ pentru $n \geq 2$. Prin convenție notăm $T_1 = 1$. Pentru a stabili o relație de recurență pentru T_n , observăm că atunci când punem corect parantezele în produsul $x_1 x_2 \dots x_n$ avem două posibilități:

- Există o singură pereche de paranteze care nu sunt conținute în interior de alte paranteze. Atunci această pereche conține în interior pe x_1, \dots, x_{n-1} și

lasă în afară pe x_n sau conține în interior pe x_2, \dots, x_n și 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 conținute în interior de alte paranteze, prima pereche conținând în interior pe x_1, \dots, x_k iar a doua pe x_{k+1}, \dots, x_n . Pentru fiecare k parantezele se pot pune în $T_k T_{n-k}$ moduri. Obținem astfel relația de recurență

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

Demonstrăm acum prin inducție 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 $S = T_1 T_{n+1} + 2T_2 T_n + \dots + (n+1)T_{n+1} T_1$. Aplicând ipoteza de inducție obținem că $S = T_{n+1} + 2T_1 T_n + \dots + (4n-2)T_n T_1$. Notăm $R = 2T_1 T_n + \dots + (4n-2)T_n T_1$. Atunci avem

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

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

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

deci $S = \frac{n+2}{2}T_{n+2}$.

Din cele două formule obținute 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 inducție 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 și 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 și $u, v : X \rightarrow A$ verifică $fu = fv$, atunci pentru orice $x \in X$ avem $f(u(x)) = f(v(x))$ și cum f este injectiv obținem $u(x) = v(x)$. Așadar $u = v$ și 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 $(\mathbb{N}, +)$ și morfismele de monoizi $u, v : \mathbb{N} \rightarrow A$ definite prin $u(n) = a^n$ și $v(n) = b^n$ 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 $fu = fv$, contradicție cu faptul că f este monomorfism de monoizi. Rezultă că f este injectiv.

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

Evident, morfismul de monoizi multiplicativi $i : \mathbb{Z} \rightarrow \mathbb{Q}$ nu este surjectiv. Arătăm că i este epimorfism de monoizi. Fie $u, v : \mathbb{Q} \rightarrow Y$ 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 .

și are simetricul $u(1/m)$. Analog, $v(m)$ este simetrizabil și 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 $u = v$ și f este epimorfism de monoizi.

5. Fie S un semigrup. Dacă S este monoid, îl scufundăm pe S în el însuși cu aplicația identică. Dacă S nu are element neutru, fie e un obiect care nu se găsește în S și 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 și $xe = ex = x$ pentru orice $x \in M$. Este clar că M este monoid cu elementul neutru e iar aplicația $f : S \rightarrow M$ definită prin $f(x) = x$, pentru orice $x \in S$, este un morfism injectiv de semigrupuri.

6. Fie S un semigrup cu simplificare și e un element idempotent al lui S . Dacă $x \in S$, avem $ex = e^2x$, deci $ex = e(ex)$ și 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 mulțimea $\{a^p \mid p \in \mathbb{N}^*\}$ 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 $m > p$ și $r \in \mathbb{N}^*$. Alegem r astfel încât $rt > p$ și $m = rt$. Atunci $a^m = a^{m+rt} = a^{2m}$, deci a^m este idempotent.

8. Fie S un semigrup (cu operația 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), și 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 situații:

- 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 $b^2 = a$. Obținem semigrupul $S_3 = \{a, b\}$ cu operația definită de $a^2 = ab = ba = a, b^2 = a$ (este imediat de verificat

asociativitatea și că S_3 nu este monoid).

- S nu are un element zero. Știm din problema 7 că S are cel puțin un idempotent. Presupunem de exemplu că a este idempotent. Dacă $ab = a$, atunci trebuie să avem $ba = b$ (altfel a este un element zero), și în continuare $b^2 = baba = ba^2 = ba = b$. Obținem semigrupul $S_4 = \{a, b\}$ cu operația 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) și în continuare $b^2 = abab = a^2b = ab = b$. Obținem semigrupul $S_5 = \{a, b\}$ cu operația dată de $a^2 = a, ab = b, ba = a, b^2 = b$ (din nou se verifică imediat asociativitatea). Este clar că semigrupurile S_4 și 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 și 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 mulțime 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 și fie $a \in S$. Cum a are ordin finit și $a^n \in S$ 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 operația din S . Fie $a, b \in H_e$. Avem $ea = ae = a$, $eb = be = b$ și există $x, y, x', y' \in S$ cu $xa = ay = e$ și $x'b = by' = e$. Atunci $e(ab) = (ea)b = ab$ și $(ab)e = a(be) = ab$. De asemenea, $x'xab = x'eb = x'b = e$ și $aby'y = aey = ay = e$. Rezultă că $ab \in H_e$. Evident $e \in H_e$, deoarece $ee = e$, și în plus, e este element neutru în H_e . Rămâne să arătăm că orice element din H_e este simetrizabil. Fie $a \in H_e$ și $x, y \in S$ cu $xa = ay = e$. Atunci $(xe)a = xa = e$ și $a(ey) = ay = e$. Apoi $xe = xay = ey$. Arătăm că $xe \in H_e$. Mai întâi observăm că $(xe)e = xe$ și $e(xe) = e(ey) = ey = xe$. Apoi $a(xe) = aey = ay = e$ și $(xe)a = xa = e$. Rezultă că $xe \in H_e$ și acesta este inversul lui a .

(ii) Fie $H \subset S$ astfel încât $e \in H$ și H este grup cu operația 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 conține un idempotent e , atunci mulțimea $\{e\}$ este un subgrup al lui S . Reciproc, dacă S are un subgrup G , atunci elementul neutru e al lui G verifică relația $e^2 = e$.
(ii) Este suficient să dăm un exemplu de semigrup care nu are elemente idempotente. Un astfel de exemplu este $(\mathbb{N}^*, +)$.

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

13. (i) Fie G un subgrup al lui S și 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 $H \cap H_e \neq \emptyset$ și deci $H \subseteq H_e$, de unde se obține că $H = H_e$.
(ii) Fie G și G' două subgrupuri maximale ale lui S . Notăm cu e și respectiv e' elementele neutre ale acestora. Obținem ca la punctul (i) că $G = H_e$ și $G' = H_{e'}$. Dacă G și G' nu sunt disjuncte, aplicăm din nou problema 12(ii) și obținem că $G = H_e \subseteq H_{e'} = G'$ și analog $G' \subseteq G$. Rezultă că $G = G'$.

14. Deoarece S are subgrupuri, rezultă din problema 11 că S are elemente idempotente. Fie I mulțimea acestora. Arătăm că $S = \bigcup_{e \in I} H_e$, unde notațiile 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 și $H_{e'}$ sunt egale sau disjuncte. Ele nu pot fi egale deoarece elementele neutre sunt diferite, deci sunt disjuncte. Am scris așadar pe S ca o reuniune disjunctă de subgrupuri.

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

o lege de compoziție astfel: $e_i e_i = e_i$ pentru orice i și $e_i e_j = e_0$ pentru orice $i \neq j$. Atunci S este semigrup care nu este grup și S este reuniunea subgrupurilor $\{e_i\}$ cu $i \in \{0, \dots, n\}$.

16. Presupunem că există un morfism injectiv de semigrupuri $f : S \rightarrow G$, unde G este grup. Dacă $a, x, y \in S$ și $ax = ay$, atunci $f(ax) = f(ay)$, deci $f(a)f(x) = f(a)f(y)$ și cum G este grup obținem 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 mulțimea $S \times S$ considerăm relația \sim definită astfel:

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

Arătăm că \sim este relație de echivalență 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 și $cb = da$, adică $(c, d) \sim (a, b)$.
- tranzitivitatea: $(a, b) \sim (c, d)$ și $(c, d) \sim (e, f)$ este echivalent cu $ad = bc$ și $cf = de$. Atunci $adf = bcf = deb$ și cum putem simplifica cu d rezultă $af = eb$, adică $(a, b) \sim (e, f)$.

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

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

Arătăm că definiția de mai sus nu depinde de reprezentanți. Într-adevăr, dacă $a/b = a'/b'$ și $c/d = c'/d'$, adică $ab' = ba'$ și $cd' = dc'$, 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 operație definită pe G este asociativă. De asemenea, elementul s/s , $s \in S$, este element neutru în G , deoarece $(a/b)(s/s) = as/b s = a/b$ (aceasta este adevărat pentru că $asb = bsa$) și în mod analog $(s/s)(a/b) = a/b$. Dacă $a/b \in G$, atunci $(a/b)(b/a) = ab/ab = s/s$ (deoarece $abs = abs$) și analog $(b/a)(a/b) = s/s$. Rezultă că orice element al lui G este inversabil, deci G este grup.

Aplicația $f : S \rightarrow G$ 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 $f(a) = f(b) \Rightarrow as/s = bs/s \Rightarrow ass = bss$

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

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

18. (i) Dacă $f, g : X \rightarrow X$ sunt funcții injective, atunci fg este injectivă, deci $I(X)$ este parte stabilă în raport cu compunerea. Știm că această operație este asociativă și 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 $f : S \rightarrow I(X)$ un morfism injectiv de semigrupuri. Dacă $a, b, c \in S$ și $ab = ac$, atunci $f(ab) = f(ac)$, deci $f(a)f(b) = f(a)f(c)$ și cum $f(a)$ este injectivă rezultă că $f(b) = f(c)$, deci $b = c$. Reciproc, dacă S are simplificare la stânga, fie $f : S \rightarrow I(S)$ definită prin $f(s)(a) = sa$. Evident f este injectivă și f este morfism de semigrupuri.

19. (i) Pentru un element $a \in M$ definim funcția $f_a : M \rightarrow M$, $f_a(x) = ax$ pentru orice $x \in M$. Să observăm că $f_a \circ f_b = f_{ab}$ și $f_e = \text{Id}_M$, unde e este elementul identitate al lui M . Definim acum funcția $f : M \rightarrow \text{Fun}(M, M)$, $f(a) = f_a$ pentru orice $a \in M$. Avem că f este morfism de monoizi. Întrădevăr, $f(ab) = f_{ab} = f_a \circ f_b = f(a) \circ f(b)$ pentru orice $a, b \in M$ și $f(e) = f_e = \text{Id}_M$. 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 $(\text{Fun}(M, M), \circ)$, în particular f_b va fi funcție injectivă. Cum M este mulțime finită, rezultă că f_b va fi funcție bijectivă. Așadar, există $g \in \text{Fun}(M, M)$ astfel încât $g \circ f_b = f_b \circ g = \text{Id}_M$. De aici obținem că $f_b(g(x)) = x$ pentru orice $x \in M$. În particular, pentru $x = e$ se obține $bg(e) = e$, deci b este inversabil la dreapta în M . În concluzie, $b \in U(M)$, contradicție.

Considerăm acum monoidul $(\text{Fun}(\mathbb{N}, \mathbb{N}), \circ)$ și elementele $a, b \in \text{Fun}(\mathbb{N}, \mathbb{N})$ definite astfel: $a(n) = n/2$ dacă n este par și $a(n) = 0$ dacă n este impar, respectiv $b(n) = 2n$ pentru orice $n \in \mathbb{N}$. Este evident că a, b nu sunt inversabile, dar $a \circ b = \text{Id}_{\mathbb{N}}$ este element inversabil.

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

monoid, unde operația $*$ 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 $f(0) = f(1) = \dots = f(k) = 0$ și $f(k+i) = i$ 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 și numai dacă $g * f = 1_{\mathbb{N}}$, adică $f \circ g = 1_{\mathbb{N}}$. Aceasta este echivalent cu $g(i) = k+i$ pentru orice $i \in \mathbb{N}^*$ și $g(0) \in \{0, 1, \dots, k\}$. Dar există exact $k+1$ astfel de funcții g , deci f are $k+1$ inverși la stânga.

21. (i) Fie G un grup cu n elemente, de exemplu $(\mathbb{Z}_n, +)$, și 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 și numai dacă g și h sunt inversabile în G , respectiv H . Rezultă că $G \times H$ are exact n elemente inversabile. (Precizăm că operația 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 și 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 poziția a doua se găsește elementul neutru din H .

22. Începem prin a observa că dacă în semigrupul finit M considerăm un element x , iar (k_n) este un șir strict crescător de numere naturale, atunci putem alege un subșir (k_{n_i}) al său astfel încât elementele $x^{k_{n_i}}$, $i \geq 1$, să ia toate aceleași valori. Aceasta este evident, deoarece elementele șirului x^{k_n} pot lua doar un număr finit de valori. Fie $M = \{x_1, \dots, x_r\}$. Aplicăm observația de mai sus elementului x_1 și șirului tuturor numerelor naturale. Obținem un șir $(n_i)_{i \geq 1}$ de numere naturale pentru care toate puterile $x_1^{n_i}$ sunt egale. Aplicăm acum observația de mai sus elementului x_2 și șirului $(n_i)_{i \geq 1}$. Renotând, obținem un șir $(n_i)_{i \geq 1}$ pentru care toți $x_1^{n_i}$ iau aceeași valoare și toți $x_2^{n_i}$ sunt egali. Continuând procedeul obținem după r pași șirul căutat.

23. Fie A mulțimea cu un singur element a . Din construcția monoidului M liber generat de mulțimea A , acesta este format din mulțimea tuturor cuvintelor formate din alfabetul A , adică mulțimea cuvintelor de forma $aa \dots a$ cu n apariții ale lui a , unde $n \in \mathbb{N}^*$ și din cuvântul vid λ . Multiplicarea este dată de alăturarea cuvintelor, elementul neutru fiind λ . Atunci aplicația $f : \mathbb{N} \rightarrow M$ definită astfel: $f(0) = \lambda$ și $f(n) = aa \dots a$ (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 și $a_1, \dots, a_n \in \mathbb{N}^*$ cu proprietatea că $(a_1, \dots, a_n) = 1$. Atunci există $n_0 \in \mathbb{N}^*$ cu proprietatea că pentru orice $x \in \mathbb{N}$, $x \geq n_0$, există $k_1, \dots, k_n \in \mathbb{N}$ astfel încât $x = k_1 a_1 + \dots + k_n a_n$.

Demonstrație. Inducție după n . Dacă $n = 2$, alegem $n_0 = a_1 a_2$ și considerăm șirul de numere $0 \cdot a_2, 1 \cdot a_2, \dots, (a_1 - 1) \cdot a_2$. Să observăm că termenii șirului dau resturi distincte la împărțirea cu a_1 și fiind în număr de a_1 vor apărea toate resturile posibile. Dacă $x \geq n_0$, scriem $x = q a_1 + r$ cu $0 \leq r < a_1$. Din cele de mai sus rezultă că există $l \in \{0, \dots, a_1 - 1\}$ astfel încât $l a_2 = q' a_1 + r$. Deci $x - l a_2 = (q - q') a_1$. Dacă $q - q' < 0$, atunci $x < l a_2$ și rezultă $a_1 a_2 < l a_2$, adică $a_1 < l$, fals. Rezultă că $q - q' \geq 0$ și $r = l a_2 + (q - q') a_1$.

Dacă $n > 2$, notăm $b = (a_1, \dots, a_{n-1})$ și $c = a_n$. Atunci $(b, c) = 1$ și 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 încât $x = kb + lc$. Dar $(a_1/b, \dots, a_{n-1}/b) = 1$ și din ipoteza de inducție rezultă că există $n_2 \in \mathbb{N}$ cu proprietatea că pentru orice $y \in \mathbb{N}$, $y \geq n_2$, există $l_1, \dots, l_{n-1} \in \mathbb{N}$ astfel încât $y = l_1 a_1/b + \dots + l_{n-1} a_{n-1}/b \Rightarrow by = l_1 a_1 + \dots + l_{n-1} a_{n-1}$ pentru $y \geq n_2$. Considerăm $n_0 = n_2 b(1 + c) + n_1$ și arătăm că pentru orice $x \geq n_0$ există $k_1, \dots, k_n \in \mathbb{N}$ astfel ca $x = k_1 a_1 + \dots + k_n a_n$.

Cum $n_0 > n_1$, există $k, l \in \mathbb{N}$ astfel ca $x = kb + lc$. Putem presupune că $k \geq n_2$, altfel $k < n_2 \Rightarrow n_2 b(1 + c) < x = kb + lc < n_2 b + lc \Rightarrow n_2 b c < lc \Rightarrow n_2 b < l \Rightarrow x = (k + n_2 c)b + (l - n_2 b)c$, scriere în care coeficienții lui b și c sunt numere naturale iar coeficientul lui b este mai mare sau egal decât n_2 . Deci $bk = l_1 a_1 + \dots + l_{n-1} a_{n-1}$, unde $l_1, \dots, l_{n-1} \in \mathbb{N}$. În concluzie, $x = kb + lc = l_1 a_1 + \dots + l_{n-1} a_{n-1} + lc$ și nu avem decât să alegem $k_1 = l_1, \dots, k_{n-1} = l_{n-1}, k_n = l$ pentru a obține scrierea dorită.

Să trecem acum la rezolvarea problemei. Fie d cel mai mare divizor comun al elementelor mulțimii $M - \{0\}$. Atunci $(1/d)M \subseteq \mathbb{N}$ este submonoid, deci putem presupune de la început că $d = 1$. Scriem $M - \{0\} = \{a_1, \dots, a_n, \dots\}$ și notăm $q_n = (a_1, \dots, a_n) \Rightarrow \dots | q_n | q_{n-1} | \dots | q_2 | q_1 \Rightarrow \dots \leq q_n \leq q_{n-1} \leq \dots \leq q_2 \leq q_1$, deci există $t \in \mathbb{N}$ astfel încât $q_n = q_{n+1}$ pentru orice $n \geq t$. Notăm $q = q_n$ și cum $q | a_n$ pentru orice $n \in \mathbb{N}^*$, avem că $q = 1$. Deci $(a_1, \dots, a_n) = 1$, 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 $k_1, \dots, k_n \in \mathbb{N}$ astfel încât $x = k_1 a_1 + \dots + k_n a_n \Rightarrow \{x \in \mathbb{N} \mid x \geq n_0\} \subseteq M$, 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 mulțime finită.

Observație. Din demonstrație rezultă că elementele mulțimii A sunt și ele multipli de d .

25. (i) Definim $f : \mathbb{N}^* \rightarrow M_2$ astfel: dacă $n = 2^k m$, $k \in \mathbb{N}$ și m impar, atunci $f(2^k m) = m$. Este ușor de văzut că f este izomorfism de monoizi.
(ii) Este imediat că M_3 și M_5 sunt monoizi în raport cu operația de înmulțire. Să presupunem că ar exista un izomorfism $f : \mathbb{N}^* \rightarrow M_3$. Fie $p \in \mathbb{N}^*$ un număr prim de forma $3k - 1$. Atunci $p^2 \in M_3$ și 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 consecință, $p \in M_3$, contradicție.

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 $f(y) = q^2$ și $f(z) = pq$. Obținem $f(x)f(y) = f(z)^2$ și ținând seama că f este izomorfism de monoizi rezultă că $xy = z^2$. Ținând cont că x, y, z sunt numere prime, deducem că $x = y = z$, contradicție. Deci monoizii \mathbb{N}^* și M_3 nu sunt izomorfi.

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

Presupunem acum că există un izomorfism $f : M_3 \rightarrow M_5$. Să arătăm mai întâi că dacă $x \in M_3$ și 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 $3k + 1$ și v este de forma $3k - 1$ (sau invers), deci $x = u(vb)$ cu $u, vb \in M_3 \Rightarrow x$ reductibil în M_3 , contradicție. Deci a și 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 $(q_1 q_2)^2, (q_1 q_3)^2, (q_2 q_4)^2, (q_3 q_4)^2, q_1 q_2 q_3 q_4 \in M_5$ și există $x, y_1, y_2, z_1, z_2 \in M_3$ distincte și ireductibile astfel încât $f(x) = q_1 q_2 q_3 q_4$, $f(y_1) = (q_1 q_2)^2$, $f(y_2) = (q_3 q_4)^2$, $f(z_1) = (q_1 q_3)^2$, $f(z_2) = (q_2 q_4)^2$. De aici obținem că $f(x)^2 = f(y_1)f(y_2) = f(z_1)f(z_2) \Rightarrow f(x^2) = f(y_1 y_2) = f(z_1 z_2) \Rightarrow x^2 = y_1 y_2 = z_1 z_2$, deci în monoidul M_3 elementul x^2 are trei descompuneri distincte în factori ireductibili, ceea ce este ușor de verificat că nu este posibil (ținând cont de descrierea elementelor ireductibile din M_3).

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

Fie $f : M_m \rightarrow M_n$ 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 $c \in T_n$ și $\bar{c} \in U(\mathbb{Z}_n)$ (unde prin \bar{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 $(f(r)^{\varphi(n)}, f(s)^{\varphi(n)}) = c^{\varphi(n)}$ și deoarece f este surjectivă există $u, v, w \in M_m$ astfel încât $f(u) = c^{\varphi(n)}$, $f(v) = d$ și $f(w) = e$, unde $f(r^{\varphi(n)}) = dc^{\varphi(n)}$ și $f(s^{\varphi(n)}) = ec^{\varphi(n)}$. Să observăm că $d, e \in M_n$. Deci $r^{\varphi(n)} = uv$ și $s^{\varphi(n)} = uw$. De aici obținem $1 = (r^{\varphi(n)}, s^{\varphi(n)}) \geq u$, adică $u = 1$. În consecință, $c^{\varphi(n)} = 1$, de unde $c = 1$, contradicție.

Definim $g : T_m \rightarrow T_n$ astfel: $g(x) = (f(ax), f(bx))$, unde $a, b \in T_m$, $(a, b) = 1$ și $ax, bx \in M_m$ ($x \in T_m \Rightarrow (x, m) = 1 \Rightarrow \hat{x} \in U(\mathbb{Z}_m)$), 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

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

Ultima egalitate rezultă din observația făcută în paragraful anterior, care ne garantează că dacă $(a^{\varphi(m)}, b^{\varphi(m)}) = 1$, atunci $(f(a^{\varphi(m)}), f(b^{\varphi(m)})) = 1$. De aici rezultă imediat faptul că g este bine definită, multiplicativă (adică $g(xy) = g(x)g(y)$ pentru orice $x, y \in T_m$) și 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 $f(x) = uy$ și $f(x') = vy$. 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 $h : U(\mathbb{Z}_m) \rightarrow U(\mathbb{Z}_n)$ prin $h(\hat{x}) = \overline{g(x)}$. Din cele de mai înainte rezultă că h este bine definită, este morfism de grupuri și este surjectivă. Să arătăm că h este și injectivă: $h(\hat{x}) = \bar{1} \Rightarrow \overline{g(x)} = \bar{1} \Rightarrow g(x) \in M_n \Rightarrow$ 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 $f : U(\mathbb{Z}_m) \rightarrow U(\mathbb{Z}_n)$ izomorfism de grupuri și $r = \varphi(m) = \varphi(n)$. Dacă $U(\mathbb{Z}_m) = \{\hat{a}_1, \dots, \hat{a}_r\}$, considerăm $\bar{b}_i = f(\hat{a}_i)$, $1 \leq i \leq r$, și obținem că

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

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

și

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

pentru $1 \leq i \leq r$. Din teorema lui Dirichlet (o progresie aritmetică de numere naturale în care primul termen și rația sunt numere prime între ele, conține o infinitate de numere prime) rezultă că mulțimile A_{m,a_i}, B_{n,b_i} sunt numărabile, deci elementele lor se pot scrie sub forma unui șir crescător.

Se observă că dacă $x \in T_m$, $x = p_1^{r_1} \cdots p_t^{r_t}$ cu p_1, \dots, p_t numere prime distincte, atunci $p_i \in A_{m,a_1} \cup \dots \cup A_{m,a_r}$, pentru orice $1 \leq i \leq t$. Fie $g : T_m \rightarrow T_n$ definită astfel: $g(p) = q$, unde $p \in A_{m,a_i}$ și este al s -lea element în ordine crescătoare al acesteia, iar $q \in B_{n,b_i}$ și 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 și T_n .

Definim acum $h : M_m \rightarrow M_n$ 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. Aceștia nu sunt izomorfi cu monoidul \mathbb{N}^* , fapt care se poate arăta la fel ca la problema precedentă, și 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 aceștia sunt izomorfi cu \mathbb{N}^* . Dacă p_1, \dots, p_n, \dots este șirul numerelor naturale prime, atunci există $t \in \mathbb{N}^*$ astfel încât $p = p_t$. Definim $f : T_p \rightarrow \mathbb{N}^*$ astfel:

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

Este imediat că f este izomorfism de monoizi.

Capitolul 9

Soluții: Grupuri

1. Fie $a \in S$, $a' \in S$ cu $a'a = e$ și $a'' \in S$ astfel încât $a''a' = e$. Atunci $a = ea = a''a'a = a''e$ și $ae = a''ee = a''e = a$, de unde rezultă că e este element neutru. În plus, $a = a''e = a''$, deci $aa' = e$ și $aa' = a''a' = e$, 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 mulțimea \mathbb{R}^* definim legea de compoziție " \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 $a \star a' = 1$. Totuși \mathbb{R}^* cu operația algebrică astfel definită nu este grup, deoarece e nu este element neutru și la dreapta.

2. (ii) \Rightarrow (i) Evident ecuațiile $ax = b$ și $ya = b$ au soluțiile $x = a^{-1}b$, respectiv $y = ba^{-1}$.

(i) \Rightarrow (ii) Fie $a \in S$ și $e \in S$ 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' și e sunt elemente neutre la stânga, respectiv la dreapta, rezultă $e' = e'e = e$, deci e este element neutru pentru S . Fie acum $a \in S$ și $a', a'' \in S$ cu $a'a = e$ și $aa'' = e$. Atunci $a' = a'e = a'aa'' = ea'' = a''$ și acesta este un invers pentru a . Așadar S este grup.

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

problema 2 rezultă că S este grup.

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

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

Dacă $h \in \text{Hom}_{gr}(\mathbb{Q}, \mathbb{Q})$, 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 $h(p/q) = h(p)/q = ap/q$. Așadar $h(x) = ax$ pentru orice $x \in \mathbb{Q}$ și $\text{Hom}_{gr}(\mathbb{Q}, \mathbb{Q}) = \{h_a \mid a \in \mathbb{Q}\}$, unde $h_a : \mathbb{Q} \rightarrow \mathbb{Q}$ este definită prin $h_a(x) = ax$. Deci $\text{Hom}_{gr}(\mathbb{Q}, \mathbb{Q}) \simeq \mathbb{Q}$.

Dacă $h \in \text{Hom}_{gr}(\mathbb{Q}, \mathbb{Z})$, 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 $h(1/2a) = 1/2 \in \mathbb{Z}$, contradicție. Rezultă că $a = 0$ și deci $\text{Hom}_{gr}(\mathbb{Q}, \mathbb{Z}) = \{0\}$ (prin 0 am desemnat morfismul nul).

Pentru a calcula $\text{Hom}_{gr}(\mathbb{Z}_m, \mathbb{Z}_n)$ procedăm ca și în cazul lui $\text{Hom}_{gr}(\mathbb{Z}, \mathbb{Z})$ și obținem că morfismele cerute sunt aplicațiile de forma $f_{\hat{a}} : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ definite prin $f_{\hat{a}}(\hat{x}) = \hat{a}\hat{x}$ pentru orice $x \in \mathbb{Z}$, unde $a \in \{0, 1, \dots, n-1\}$. Deci $\text{Hom}_{gr}(\mathbb{Z}_n, \mathbb{Z}_n) \simeq \mathbb{Z}_n$.

Vom arăta că $\text{Hom}_{gr}(\mathbb{Z}_m, \mathbb{Z}_n) \simeq \mathbb{Z}_d$, unde $d = (m, n)$. Notăm cu \hat{x} clasele din \mathbb{Z}_m , cu \bar{x} clasele din \mathbb{Z}_n și cu \tilde{x} clasele din \mathbb{Z}_d . Considerăm $f \in \text{Hom}_{gr}(\mathbb{Z}_m, \mathbb{Z}_n)$. Atunci $f(\hat{x}) = \bar{a}\bar{x}$ pentru orice $x \in \mathbb{Z}_m$, unde $\bar{a} = f(\hat{1})$. Dar $m\bar{a} = mf(\hat{1}) = f(m\hat{1}) = f(\hat{0}) = \bar{0}$ și cum $(m/d, n/d) = 1$, rezultă că $\frac{n}{d}|\bar{a} \Rightarrow \bar{a} \in \{\bar{0}, n/d, \dots, (d-1)n/d\}$, adică $\bar{a} \in \langle n/d \rangle$. Acum este clar că asocierea $f \mapsto f(\hat{1})$ definește un izomorfism de grupuri între $\text{Hom}_{gr}(\mathbb{Z}_m, \mathbb{Z}_n)$ și $\langle n/d \rangle \simeq \mathbb{Z}_d$.

5. Cum \mathbb{Z} și \mathbb{Q} sunt mulțimi numărabile, iar \mathbb{R} și \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 $(\mathbb{Z}, +)$ și $(\mathbb{Q}, +)$ 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 și nici q , și atunci evident $h \neq a^n$ pentru orice $n \in \mathbb{Z}$. Cu același 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 $a \in \mathbb{Q}$ și $n \in \mathbb{N}^*$ ecuația $nx = a$ are soluție în \mathbb{Q}), dar grupurile (\mathbb{Q}^*, \cdot) și (\mathbb{Q}_+^*, \cdot) nu au această proprietate, ecuația $x^2 = 2$ neavând soluție 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 sfârșit, în (\mathbb{Q}^*, \cdot) ecuația $x^2 = 1$ are două soluții, iar în (\mathbb{Q}_+^*, \cdot) ecuația $x^2 = a$ are cel mult o soluție pentru orice a , de unde rezultă că nici aceste două grupuri nu sunt izomorfe. Așadar orice două grupuri din prima clasă sunt neizomorfe.

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

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

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

În sfârșit, $(\mathbb{R}, +)$ și (\mathbb{C}^*, \cdot) nu sunt izomorfe, deoarece ecuația $z^2 = 1$ are două soluții în \mathbb{C}^* , iar ecuația $2x = 0$ are o singură soluție în $(\mathbb{R}, +)$.

Așadar 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 mulțimile M și M și 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 submulțimea finită H a lui G este parte stabilă. Fie $h \in H$. Atunci $\{h^n \mid n \in \mathbb{N}\} \subseteq H$ și 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 $j - i > 1$ și $h^{-1} = h^{j-i-1} \in H$. Obținem că H este subgrup.

8. Avem $D_4 = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\}$, unde $\text{ord}(r) = 4$, $\text{ord}(s) = 2$ și $sr = r^3s$. Folosind aceste relații între generatori se obține ușor prin calcul că D_4 are două elemente de ordin 4, r și r^2 , un element de ordin 1 (elementul neutru) și 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) și 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 $\langle r \rangle = \{e, r, r^2, r^3\}$. Dacă H este un alt subgrup cu 4 elemente, atunci el nu poate conține pe r sau r^3 care au ordinul 4. Dacă $r^2 \notin H$, atunci H conține trei dintre elementele s, rs, r^2s, r^3s , deci există $i \in \{0, 1, 2\}$ cu $r^i s, r^{i+1} s \in H$. Atunci $r = (r^{i+1} s)(r^i s)^{-1} \in H$, contradicție. Așadar $r^2 \in H$ și obținem două astfel de subgrupuri: $\{e, r^2, s, r^2s\}$ și $\{e, r^2, rs, r^3s\}$.

Subgrupurile $\{e\}$ și 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 intersecție de două subgrupuri normale de ordin 4).

9. Vom arăta mai mult: dacă H și K sunt subgrupuri ale unui grup G , atunci $H \cup K$ este subgrup dacă și numai dacă $H \subseteq K$ sau $K \subseteq H$. Să presupunem că $H \not\subseteq K$ și $K \not\subseteq H$. Fie $h \in H - K$ și $k \in K - H \Rightarrow hk \notin H \cup K$ (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 și 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, $a^2 = b^2 = e$ și $ab = ba$. Atunci $K = \{e, a\} \cup \{e, b\} \cup \{e, ab\}$ este reuniune de trei subgrupuri proprii. De asemenea, ținând cont de descrierea subgrupurilor lui D_4 din problema 8, păstrând notațiile de la soluția 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) și obținem că $xz \notin H$ (altfel $z \in H$, fals), $xz \notin K$ (altfel $z \in K$, fals) și $xz \notin L$ (altfel $x \in L$, fals), contradicție. Deci un element care aparține intersecției a două dintre subgrupurile H, K, L este și în al treilea. Să presupunem acum că $x \in H$ și $x \notin K \cup L$. Fie $z \in L - (H \cup K) \Rightarrow xz \notin H$ și $xz \notin L \Rightarrow xz \in K - (H \cup L) \Rightarrow x(xz) \notin H \cup K \Rightarrow x(xz) \in L \Rightarrow x^2z \in L \Rightarrow x^2 \in L$. Alegând acum $y \in K - (H \cup L)$, obținem că $xy \notin H \cup K \Rightarrow xy \in L - (H \cup K) \Rightarrow x^2y \notin H \cup L \Rightarrow x^2y \in K \Rightarrow x^2 \in K$. În concluzie, $x^2 \in H \cap K \cap L$.

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

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 $x \neq x^{-1}$ și atunci putem scrie $G = \{e\} \cup (\cup_{x \in G} \{x, x^{-1}\})$, deci G ar avea un număr impar de elemente (mulțimile cu câte două elemente care intră în reuniune sunt sau disjuncte sau egale). Obținem astfel o contradicție, deci G are elemente de ordin 2.

13. (i) Aplicația f este morfism de grupuri dacă și numai dacă pentru orice $x, y \in G$ avem $f(xy) = f(x)f(y)$, adică $(xy)^2 = x^2y^2$. Înmulțind cu x^{-1} la stânga și cu y^{-1} la dreapta obținem $xy = yx$, adică G este grup abelian. Reciproc este evident.

(ii) Știm că f este morfism de grupuri. Cum G este grup finit, rezultă că f este izomorfism dacă și numai dacă f este injectiv, deci dacă și numai dacă $\text{Ker}(f) = \{e\}$. Așadar f este izomorfism dacă și 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 $xyxy = e$. Înmulțind cu x^{-1} la stânga și cu y^{-1} la dreapta și ținând cont că $x^2 = y^2 = e$, obținem $yx = xy$.

(ii) Observăm că grupul abelian (G, \cdot) se poate înzestra cu o structură de \mathbb{Z}_2 -spațiu vectorial, înmulțirea cu scalari fiind definită astfel: $\hat{0} \cdot x = e$ și $\hat{1} \cdot x = x$ pentru orice $x \in G$. Verificarea este imediată, observându-se că este esențială condiția $x^2 = e$ 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 -spațiu vectorial, cu $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (în produs intrând n factori). În particular, acesta este și izomorfism de grupuri, deci G are 2^n elemente.

15. Dacă există $g \in G$ de ordin infinit, atunci subgrupul $\langle g \rangle$ generat de g este izomorf cu $(\mathbb{Z}, +)$, deci are o infinitate de subgrupuri. Acestea fiind și subgrupuri ale lui G obținem 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, contradicție. În concluzie G are o infinitate de subgrupuri distincte și 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 și $\{e\}$. Fie $g \in G - \{e\}$. Atunci $\langle g \rangle$ este subgrup netrivial al lui G , deci $\langle g \rangle = G$. Rezultă că G este grup ciclic finit și deci există $n \in \mathbb{N}^*$ cu $G \simeq \mathbb{Z}_n$. Dacă n nu este număr prim, fie p prim cu $p|n$ și atunci $p\mathbb{Z}_n$ este un subgrup propriu și netrivial al lui \mathbb{Z}_n , contradicție. Așadar 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 $\{e\}, H$ și G cele trei subgrupuri. Deoarece $H \neq G$, există $g \in G - H \Rightarrow \langle g \rangle \neq \{e\}, H \Rightarrow \langle g \rangle = G$, 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 distincți, atunci fiecare dintre aceștia ar genera un subgrup propriu și netrivial în \mathbb{Z}_n , deci G ar avea cel puțin patru subgrupuri. Rezultă că $n = p^2$ cu p număr prim și $G \simeq \mathbb{Z}_{p^2}$. Evident aceste grupuri verifică proprietatea

cerută.

(iii) G are exact patru subgrupuri. Fie $\{e\}, H, K$ și G cele patru subgrupuri. Deoarece $H \cup K \neq G$ (vezi problema 9), există $g \in G - (H \cup K) \Rightarrow \langle g \rangle \neq \{e\}, H, K \Rightarrow \langle g \rangle = G$, 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 , obținem că $n = p^3$, p număr prim, sau $n = pq$, unde p și q sunt numere prime distincte.

(iv) G are exact cinci subgrupuri. Fie $\{e\}, H, K, L$ și 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 $g \in G - (H \cup K \cup L) \Rightarrow \langle g \rangle \neq \{e\}, H, K, L \Rightarrow \langle g \rangle = G$, deci G este grup ciclic finit, $G \simeq \mathbb{Z}_n$. Astfel obținem 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 și dacă să zicem $H \cap K \cap L = H$, atunci $H \subseteq K \cap L$ și 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 copii ale lui \mathbb{Z}_2 (vezi problema 14) și cum G are exact cinci subgrupuri rezultă imediat că doar cazul $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ convine.

17. Implicația directă este evidentă din definiția subgrupului normal. Presupunem acum că pentru orice $i \in I$ avem $a_i g a_i^{-1} \in \langle g \rangle$ și $a_i^{-1} g a_i \in \langle g \rangle$. Vrem să arătăm că $x g^p x^{-1} \in \langle g \rangle$ pentru orice $p \in \mathbb{Z}$ și $x \in G$. Cum $x g^p x^{-1} = (x g x^{-1})^p$, rezultă că $a_i u a_i^{-1} \in \langle g \rangle$ și $a_i^{-1} u a_i \in \langle g \rangle$ pentru orice $i \in I$ și $u \in \langle g \rangle$. Acum orice $x \in G$ este de forma $x = b_1 \cdots b_r$ cu $b_i \in \{a_i \mid i \in I\} \cup \{a_i^{-1} \mid i \in I\}$ și afirmația rezultă imediat prin inducție după r .

18. (i) Prin calcul rezultă că $\text{ord}(\mathbf{j}) = \text{ord}(\mathbf{k}) = 4$, $\mathbf{j}^2 = \mathbf{k}^2$ și că $J \cap K = \{I_2, \mathbf{j}^2\}$.

(ii) Avem $\mathbf{j}^{-1} \mathbf{j} \mathbf{j} = \mathbf{j} \mathbf{j} \mathbf{j}^{-1} = \mathbf{j} \in J$, $\mathbf{k} \mathbf{j} \mathbf{k}^{-1} = \mathbf{k}^{-1} \mathbf{j} \mathbf{k} = \mathbf{j}^2 \in J$ și acum din problema 17 rezultă că J este subgrup normal în Q . În mod similar K este subgrup normal (folosind relațiile $\mathbf{j} \mathbf{k} \mathbf{j}^{-1} = \mathbf{j}^{-1} \mathbf{k} \mathbf{j} = \mathbf{k}^2$). Atunci JK este subgrup în Q și cum $\mathbf{j}, \mathbf{k} \in JK$ rezultă că $JK = Q$. Din teorema a doua de izomorfism pentru grupuri obținem $JK/J \simeq K/J \cap K$, deci $|Q| = |JK| = |J||K|/|J \cap K| = 8$.

(iii) Cum J este subgrup de indice 2 în Q și $\mathbf{k} \in J$, rezultă că $Q = J \cup \mathbf{k}J$, deci $Q = \{I_2, \mathbf{j}, \mathbf{j}^2, \mathbf{j}^3, \mathbf{k}, \mathbf{k} \mathbf{j}, \mathbf{k} \mathbf{j}^2, \mathbf{k} \mathbf{j}^3\}$. Folosind relațiile 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 și deci este normal. Dacă $|H| = 2$, folosind (iii) rezultă că $H = \{I_2, \mathbf{j}^2\}$. Atunci $H = \langle \mathbf{j}^2 \rangle$ și cum $\mathbf{j}\mathbf{j}^2\mathbf{j}^{-1} = \mathbf{j}^{-1}\mathbf{j}^2\mathbf{j} = \mathbf{j}^2 \in H$ și $\mathbf{k}\mathbf{j}^2\mathbf{k}^{-1} = \mathbf{k}^{-1}\mathbf{j}^2\mathbf{k} = \mathbf{k}^2 = \mathbf{j}^2 \in H$, 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 $\langle x \rangle \cap \langle y \rangle = \{e\}$, deoarece din teorema lui Lagrange ordinul acestei intersecții divide și pe n și pe m , deci este 1. Acum dacă $(xy)^p = e$, cum x și y comută rezultă că $x^p y^p = e$, deci $x^p = y^{-p} \in \langle x \rangle \cap \langle y \rangle = \{e\}$, deci $x^p = y^{-p} = e$. Atunci n divide p și m divide $-p$. Cum $(n, m) = 1$, rezultă că p se divide cu mn . Pe de altă parte $(xy)^{mn} = (x^n)^m (y^m)^n = e$ și deci $\text{ord}(xy) = nm$.

Dacă n și m nu sunt relativ prime rezultatul nu mai este adevărat. De exemplu, fie x un element de ordin $n > 1$ într-un grup și $y = x^{-1}$. Avem că $\text{ord}(y) = n$, iar $xy = e$ are ordinul 1.

(ii) În grupul $GL(2, \mathbb{R})$ considerăm elementele:

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

care au ordinul 2. În schimb

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

are ordin infinit. În concluzie afirmația de la (i) nu mai este adevărată dacă x și y nu comută.

(iii) Răspunsul este în general negativ. Pentru aceasta fie x un element de ordin infinit într-un grup G și $y = x^{-1}$, care are tot ordin infinit. Atunci $xy = e$ are ordinul 1, dar nici unul dintre $\text{ord}(x)$ și $\text{ord}(y)$ nu este finit.

(iv) Demonstrăm prin inducție după n . Pentru $n = 1$ este clar. Presupunem adevărat pentru n și fie G un grup abelian cu $p_1 \cdots p_{n+1}$ elemente, unde p_1, \dots, 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} . Așadar putem găsi $y \in G$ cu $\text{ord}(y) = p_{n+1}$. Grupul factor $G/\langle y \rangle$ are $p_1 \cdots p_n$

elemente și din ipoteza de inducție 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 $\text{ord}(z) = p_1 \cdots p_n$ și 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 $p_1 \cdots p_{n+1}$ și 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 $x \in G$ și atunci $G = \{e, a, b, ab\}$, unde a, b sunt elemente ale lui G diferite între ele și diferite de e . Este clar că $ba \notin \{e, a, b\}$, deci $ba = ab$ și atunci G este izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_2$, un izomorfism fiind dat de $f: G \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ $f(e) = (\hat{0}, \hat{0}), f(a) = (\hat{1}, \hat{0}), f(b) = (\hat{0}, \hat{1}), f(ab) = (\hat{1}, \hat{1})$.

(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 și din teorema lui Lagrange rezultă că $4|6$, contradicție. Așadar 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 $y = y^4 = x^2$, contradicție, sau $y^2 = x^2$, de unde $y = y^4 = x^4 = x$, din nou contradicție. Deci $\text{ord}(y) = 2$. Dacă $xy = yx$, cum $\text{ord}(x)$ și $\text{ord}(y)$ sunt relativ prime rezultă $\text{ord}(xy) = 2 \cdot 3 = 6$ (vezi problema 19), deci G este ciclic, contradicție. Mai departe obținem $xy = yx^2$, deoarece xy nu poate fi niciunul dintre celelalte cinci elemente. Rezultă că G este izomorf cu S_3 , un izomorfism fiind indus de asocierile $x \rightarrow \sigma$ și $y \rightarrow \tau$ cu σ ciclul de lungime 3 și τ transpoziție.

(iii) Fie G un grup neabelian cu 8 elemente. Atunci G nu are elemente de ordin 8 și nu se poate ca $x^2 = e$ pentru orice $x \in G$ (ar rezulta că G este abelian). Așadar 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 posibilități: $\text{ord}(y) = 2$ 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 $x^2 = y^2 = e$, contradicție. Deci $xy = yx^3$ și atunci $G = < x, y >$ cu $\text{ord}(x) = 4$, $\text{ord}(y) = 2$ și $xy = yx^3$, aceasta determinând în mod unic operația pe G , de unde $G \simeq D_4$ (grupul diedral cu 8 elemente este definit prin aceleași relații ca și G).

Dacă $\text{ord}(y) = 4$, atunci evident $y^2 \notin \{e, y, yx, yx^2, yx^3\}$. Dacă $y^2 = x$, rezultă $x^2 = y^4 = e$, contradicție. Dacă $y^2 = x^3$, atunci $x^2 = x^6 = y^4 =$

e , din nou contradicție. Așadar $y^2 = x^2$. Mai departe este clar că $xy \notin \{e, x, x^2, x^3, yx\}$. Dacă $xy = yx^2$, atunci $xy = y^3$, deci $x = y^2$ și $x^2 = y^4 = e$, contradicție. Rezultă că $xy = yx^3$ și deci $G = \langle x, y \rangle$, unde $\text{ord}(x) = \text{ord}(y) = 4$, $xy = yx^3$, relații care determină în mod unic operația pe G . În consecință G este izomorf cu Q , grupul cuaternionilor, care satisface exact aceste relații.

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 -spațiu vectorial (ca în soluția de la problema 14) și 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 $y \notin \langle x \rangle$ și avem $G = \langle x \rangle \cup y\langle x \rangle = \{e, x, x^2, x^3, y, yx, yx^2, yx^3\}$. Arătăm că există un element $z \notin \langle x \rangle$ de ordin 2. Într-adevăr, dacă y are ordin 2 luăm $z = y$. Dacă nu, atunci $\text{ord}(y) = 4$, deci $\text{ord}(y^2) = 2$ și deci $y \neq x, x^2$ care au ordin 4 și evident $y^2 \notin \{e, y, yx, yx^2, yx^3\}$. Rezultă că $y^2 = x^2$ și atunci $yx \neq e$, iar $(yx)^2 = y^2x^2 = x^4 = e$, de unde $\text{ord}(yx) = 2$ și putem lua $z = yx$. Așadar am găsit $x, z \in G$ cu $\text{ord}(x) = 4$, $\text{ord}(z) = 2$ și $z \notin \langle x \rangle$. Atunci aplicația $f : \mathbb{Z}_2 \times \mathbb{Z}_4 \rightarrow G$ definită prin $f(\hat{i}, \hat{j}) = z^i x^j$ este corect definită, este morfism de grupuri și 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 $\langle x \rangle$ este un subgrup netrivial al lui G și din teorema lui Lagrange rezultă că are p elemente. Atunci $G = \langle x \rangle$, deci este grup ciclic cu p elemente.

21. Fie $x = r/s \in X$, $x \neq 0$. Atunci $0 \neq sx \in X \cap \mathbb{Z}$ și 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 $a \in \mathbb{Z}$ și $y \in X$ cu $1/n = a + y$. Atunci $1 = na + ny \in n\mathbb{Z} + X \subseteq X + X = X$, deci $1 \in X$. Rezultă că $\mathbb{Z} \subseteq X$ și $\mathbb{Q} = \mathbb{Z} + X = X$.

Observație. Mai putem rezolva această problemă și 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, așadar $X = \mathbb{Q}$.

22. Fie $H = \langle p_1/q_1, \dots, p_n/q_n \rangle$ și $q = q_1 \cdots q_n$. 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 $\langle x \rangle = \mathbb{Q}$. Dar $\frac{1}{s+1} \notin \langle \frac{r}{s} \rangle$,

contradicție.

23. Presupunem că S este un sistem de generatori pentru grupul $(\mathbb{Q}, +)$ și fie $s \in S - \{0\}$. Fie H subgrupul generat de $S - \{s\}$. Avem $\mathbb{Q} = \langle S \rangle = H + \mathbb{Z}s$, 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 și $S - \{s\}$ este sistem de generatori pentru \mathbb{Q} . În particular $(\mathbb{Q}, +)$ nu are un sistem minimal de generatori.

24. Procedăm prin inducție după $d(G)$. Dacă $d(G) = 1$, atunci evident $2^{d(G)} = 2 \leq |G|$. Presupunem afirmația adevărată pentru $d(G) \leq k$ și fie G un grup cu $d(G) = k + 1$. Fie $\{x_1, \dots, x_{k+1}\}$ un sistem minimal de generatori pentru G . Notăm cu G' subgrupul lui G generat de x_1, \dots, 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 și pe x_{k+1} am obține un sistem de generatori pentru G cu $r + 1 < d(G)$ elemente, contradicție) și din ipoteza de inducție rezultă că $|G'| \geq 2^{d(G')} = 2^k$. Cum $x_{k+1} \notin G'$, rezultă că mulțimile G' și $x_{k+1}G'$ sunt disjuncte, de unde obținem că $|G| \geq 2|G'| \geq 2^{d(G)}$, ceea ce trebuia demonstrat.

25. Fie σ un ciclu de lungime 3 și τ o transpoziție 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 și 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 $s \equiv i \pmod{3}$. Arătăm că există s astfel încât $s + j \equiv k \pmod{4}$ (va rezulta atunci că $(\sigma, \hat{1})^s (\tau, \hat{1})^j = (f, \hat{k})$). Aceasta este echivalent cu $s \equiv i \pmod{3}$ și $s \equiv k - j \pmod{4}$. Dar un astfel de s există deoarece 4 și 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 (notațiile sunt cele din problema 18).

26. (i) Fie $x, y \in H$ și $i, j \in \mathbb{N}^*$ cu $x \in H_i$, $y \in H_j$. Presupunem de exemplu că $i \leq j$. Atunci $H_i \subseteq H_j$, deci $x, y \in H_j$ și 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, $H = \langle x_1, \dots, x_p \rangle$. Atunci există $n_1, \dots, n_p \in \mathbb{N}^*$ cu $x_i \in H_{n_i}$ pentru orice $i = 1, \dots, p$. Dacă n este cel mai mare dintre numerele n_1, \dots, n_p , rezultă că $x_1, \dots, x_p \in H_n$, de

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

27. Prin calcul rezultă imediat că $g^n(x) = 2^n x$ și $f_n(x) = x + 1/2^n$ pentru orice $n \in \mathbb{N}^*$ și $x \in \mathbb{R}$. Atunci $f_{n+1}^2 = f_n$, de unde rezultă, notând $H_n = \langle f_n \rangle$, 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 $1/2 = p \in \mathbb{Z}$, contradicție. Aplicând acum rezultatul din problema 26 rezultă că $H = \bigcup_{n \leq 1} H_n$ nu este finit generat.

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

28. Alegem un sistem de generatori $S = \{x_1, \dots, x_n\}$ pentru G astfel ca dacă $x \in S$ atunci și $x^{-1} \in S$ (aceasta se poate face considerând un sistem finit de generatori și adăugând inversele tuturor acestor generatori). Atunci orice element din G se poate scrie ca un produs de elemente din S . Fie acum g_1, \dots, g_r un sistem de reprezentanți 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) și eventual renotând, $g_1 = e$. Cum pentru orice $j \in \{1, \dots, r\}$ și $t \in \{1, \dots, n\}$ avem $g_j x_t \in G$, rezultă că există și sunt unic determinate $i \in \{1, \dots, r\}$ și $h_{jt} \in H$ 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 relațiile de mai sus obținem $h = eh = g_1 h = g_1 x_{i_1} \cdots x_{i_k} = h_{1i_1} g_{j_1} x_{i_2} \cdots x_{i_k} = h_{1i_1} h_{j_1 i_2} g_{j_2} x_{i_3} \cdots x_{i_k} = \dots = h_{1i_1} h_{j_1 i_2} \cdots h_{j_{k-1} i_k} g_{j_k}$, unde elementele g_{j_1}, \dots, g_{j_k} sunt unic determinate. Din ultima egalitate rezultă că $g_{j_k} \in H$ și cum reprezentantul ales în H era chiar e , obținem $g_{j_k} = e$. Rezultă că H este generat de toate elementele h_{jt} , deci H este finit generat.

29. (i) Definim pe $H \times K$ relația \sim prin $(h, k) \sim (h', k')$ dacă și 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 echivalență a lui (h, k) este mulțimea $\{(hx^{-1}, xk) \mid x \in H \cap K\}$. Avem astfel $|HK|$ clase de echivalență, fiecare având $|H \cap K|$ elemente. Rezultă că $|H \times K| = |HK||H \cap K|$, deoarece clasele de echivalență formează o partiție a mulțimii $H \times K$.

(ii) Definim $f : (G/H \cap K)_s \rightarrow (G/H)_s \times (G/K)_s$ prin $f(x(H \cap K)) = (xH, xK)$, unde prin $(G/H)_s$ am notat mulțimea claselor la stânga modulo subgrupul H . Aplicația f este corect definită, deoarece $x(H \cap K) = y(H \cap K)$

implică $x^{-1}y \in H \cap K$, deci $x^{-1}y \in H$ și $x^{-1}y \in K$, adică $xH = yH$ și $xK = yK$. Mai mult, f este injectivă, deoarece $xH = yH$ și $xK = yK$ implică $x^{-1}y \in H$ și $x^{-1}y \in K$, deci $x^{-1}y \in H \cap K$, adică $x(H \cap K) = y(H \cap K)$. Cum $|(G/H)_s| = [G : H]$, obținem inegalitatea cerută din existența acestei injecții.

Presupunem acum că $[G : H] = n$ și $[G : K] = m$ sunt finite și $(n, m) = 1$. 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 $m|[G : H \cap K]$ și 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 aplicația f este chiar bijectivă, deoarece este injectivă și domeniul și codomeniul său au același 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 $xH = g^{-1}H$ și $xK = K$. Atunci $x \in K$ și $g^{-1} \in xH$, de unde $g \in H^{-1}x^{-1} = Hx^{-1} \subseteq HK$. Am obținut deci că $G \subseteq HK$, de unde $G = HK$.

(iii) Definim aplicația $f : (L \cap H / L \cap K)_s \rightarrow (H/K)_s$ prin $f(x(L \cap K)) = xK$. În mod similar cu (i) se arată că f este corect definită și este injectivă, de unde rezultă inegalitatea cerută.

30. (i) Să observăm că $(g, h)^p = (e_G, e_H)$ dacă și numai dacă $g^p = e_G$ și $h^p = e_H$, ceea ce este echivalent cu $\text{ord}(g)|p$ și $\text{ord}(h)|p$, de unde rezultă imediat afirmația din problemă.

(ii) Cum ordinul lui $\mathbb{Z}_6 \times \mathbb{Z}_{10}$ este 60 și 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 și numai dacă $[n, m] = 4$, unde $n = \text{ord}(g)$ și $m = \text{ord}(h)$. Cum $n|12$ și $m|15$ rezultă $n = 4$ și $m = 1$. Singurele elemente de ordin 4 din \mathbb{Z}_{12} sunt $\hat{3}$ și $\hat{9}$, deci în grupul inițial există două elemente de ordin 4, și anume $(\hat{3}, \hat{0})$ și $(\hat{9}, \hat{0})$.

În sfârșit, un element $(g, h) \in \mathbb{Z}_{12} \times \mathbb{Z}_{36}$ are ordin 6 dacă și 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 și unul de ordin 1, iar în \mathbb{Z}_{36} avem câte două elemente de ordin 6 și 3 și câte un element de ordin 2 și 1. Corespunzător cu descrierea făcută obținem 24 de elemente de ordin 6 în grupul dat.

31. (i) Presupunem că G este grup ciclic finit. Fără a micșora 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, $|m\mathbb{Z}/n\mathbb{Z}| = n/m$. Așadar

pentru orice divizor pozitiv d al lui n , grupul G are exact un subgrup cu d elemente și 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 $\langle x \rangle$ este unicul subgrup cu d elemente al lui G și deci pentru orice $y \in A_d$ avem $\langle y \rangle = \langle x \rangle$. Atunci elementele de ordin d din G sunt chiar elementele de ordin d din grupul ciclic $\langle x \rangle$ și 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 $H = \mathbb{Z}_n$ și $B_d = \{x \in H \mid \text{ord}(x) = d\}$. Din prima parte a problemei rezultă că $|B_d| = \varphi(d)$ pentru orice $d|n$ și atunci din $\sum_{d|n} |A_d| = \sum_{d|n} |B_d|$ și $|A_d| \leq |B_d|$ pentru orice d , rezultă că $|A_d| = |B_d|$ pentru orice d . În particular, pentru $d = n$ obținem $A_n \neq \emptyset$, 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 și din nou putem considera $G = \mathbb{Z}_n$. Dacă $d|n$, atunci pentru $x \in \{0, \dots, n-1\}$ ecuația $d\hat{x} = \hat{0}$ este echivalentă cu $\frac{n}{d}|x$. Dar există exact d astfel de elemente x , și anume $0, \frac{n}{d}, 2\frac{n}{d}, \dots, (d-1)\frac{n}{d}$.

Reciproc, presupunem că ecuația $x^d = 1$ are cel mult d soluții 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 și atunci din (i) rezultă că G este ciclic.

(iii) Rezultă imediat din (ii) că în cazul în care G este ciclic ecuația $x^p = 1$ are cel mult p soluții în G .

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

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

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

32. Fie G un subgrup finit al grupului multiplicativ (K^*, \cdot) și fie d un divizor natural al lui $n = |G|$. Atunci ecuația $x^d = 1$ are cel mult d soluții 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.

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

33. (i) Scriem $m = p_1^{a_1} \cdots p_r^{a_r}$ și $n = p_1^{b_1} \cdots p_r^{b_r}$ cu p_i numere prime și $a_i, b_i \in \mathbb{N}$. Atunci $[m, n] = p_1^{c_1} \cdots p_r^{c_r}$, $c_i = \max(a_i, b_i)$, $i = 1, \dots, r$. Arătăm că există elementele $z_i \in G$ astfel încât $\text{ord}(z_i) = p_i^{c_i}$, $i = 1, \dots, r$. 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 $x \in G$, $x \neq e$ și $x_0 \in G$ astfel încât $\text{ord}(x_0) = m_0$. Dacă $\text{ord}(x)$ nu divide m_0 , atunci există $y \in G$ astfel încât $\text{ord}(y) = [m_0, \text{ord}(x)] > m_0$, contradicție.

(iii) Din teorema lui Cauchy obținem că există $x_i \in G$ cu $\text{ord}(x_i) = p_i$ pentru orice $i = 1, \dots, n$. 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 conținut în mulțimea rădăcinilor lui f , deci $n \leq m_0$. Dar știm deja că $m_0 \leq n$, deci $m_0 = n$. Asta înseamnă în particular că grupul G conține 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 și U_n au același 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 $z^{p^{n+1}} = 1$ și 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 posibilități: mulțimea $\{m \in \mathbb{N} \mid \text{există } x \in H \text{ cu } \text{ord}(x) = p^m\}$ este mărginită sau nemărginită.

Dacă mulțimea $\{m \in \mathbb{N} \mid \text{există } x \in H \text{ cu } \text{ord}(x) = p^m\}$ este nemărginită, atunci vom avea $H = C_{p^\infty}$. Fie $g \in C_{p^\infty}$, $\text{ord}(g) = p^n$. $\langle g \rangle$ este un subgrup cu p^n elemente al lui C_{p^∞} și din (i) rezultă că $\langle g \rangle = U_{p^n}$. Pe de altă parte, există $m \in \mathbb{N}$, $m > n$ și $x \in H$ cu $\text{ord}(x) = p^m$. Atunci, ca mai sus, $\langle x \rangle = U_{p^m} \supseteq U_{p^n}$, deci $g \in \langle x \rangle \subseteq H$.

Dacă mulțimea $\{m \in \mathbb{N} \mid \text{există } x \in H \text{ cu } \text{ord}(x) = p^m\}$ este mărginită, atunci fie n cel mai mare element al său și $x \in H$ 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 $m \leq n$ și $\langle g \rangle = U_{p^m} \subseteq U_{p^n}$, deci $H \subseteq U_{p^n}$. Pe de altă parte, $H \supseteq \langle x \rangle = U_{p^n}$ și de aici rezultă egalitatea dorită.

(iv) G nu este grup ciclic, altfel G ar fi izomorf cu \mathbb{Z} și nu are proprietatea din enunț. Mai mult, rezultă că $\text{ord}(x) < \infty$ pentru orice $x \in G$, deoarece $\langle x \rangle$ este un subgrup ciclic al lui G și din aceleași 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 $\text{ord}(x_1) = p_1^{a_1}$ și $\text{ord}(x_2) = p_2^{a_2}$, 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 mulțimea $\{k \in \mathbb{N} \mid \text{există } x \in G \text{ cu } \text{ord}(x) = p^k\}$ 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 $x_3 \in G - \langle x_1, x_2 \rangle$ (există un astfel de element, deoarece $\langle x_1, x_2 \rangle$ este subgrup finit al lui G). Dacă $\text{ord}(x_3) = p_1^{k_1} p_2^{k_2}$, atunci $k_1 \leq a_1$ și $k_2 \leq a_2$ (deoarece $\text{ord}(x_3^{p_2^{k_2}}) = p_1^{k_1}$ și $\text{ord}(x_3^{p_1^{k_1}}) = p_2^{k_2}$). Rezultă că $x_3^{p_2^{k_2}} \in \langle x_1 \rangle = U_{p_1^{a_1}}$ și $x_3^{p_1^{k_1}} \in \langle x_2 \rangle = U_{p_2^{a_2}}$, deci $x_3^{p_2^{k_2}} \in \langle x_1, x_2 \rangle$ și $x_3^{p_1^{k_1}} \in \langle x_1, x_2 \rangle$. În particular, obținem $x_3 \in \langle x_1, x_2 \rangle$ (deoarece $(p_1^{k_1}, p_2^{k_2}) = 1$), contradicție. Rezultă că există un număr prim p_3 , diferit de p_1, p_2 , astfel încât $p_3 \mid \text{ord}(x_3)$. 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 obține un șir (x_n) de elemente din G , un șir de numere prime distincte (p_n)

și un șir 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 $\langle x_2, \dots, x_n, \dots \rangle$ este subgrup infinit al lui G și diferit de G (infinit, deoarece $\text{ord}(x_2 \cdots x_n) = p_2^{a_2} \cdots p_n^{a_n}$ pentru orice $n \geq 2$ și diferit de G , deoarece $x_1 \notin \langle x_2, \dots, x_n, \dots \rangle$), contradicție.

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 mulțimea $\{k \in \mathbb{N} \mid \text{există } x \in G \text{ cu } \text{ord}(x) = p^k\}$ ar fi finită, fie k_0 maximul său. Rezultă că $G \subseteq U_{p^{k_0}}$, fals. Deci mulțimea este infinită și în acest caz obținem că $G = C_{p^\infty}$.

(v) Fie $f : C_{p^\infty} \rightarrow C_{p^\infty}$ definită prin $f(z) = z^{p^n}$. Atunci f este morfism de grupuri, $\text{Ker}(f) = U_{p^n}$ și 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 obținem acum izomorfismul cerut.

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

Fie $a \in C_{p^\infty}$, $\text{ord}(a) = p^h$ și $n = p^r m \in \mathbb{N}^*$ cu $(m, p) = 1$. Arătăm că ecuația $x^n = a$ are soluție 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 $x^n = b^m = a$. Așadar (C_{p^∞}, \cdot) este grup divizibil.

(ii) Fie G un grup divizibil netrivial. Dacă prin absurd G ar fi grup finit, fie $|G| = n$ și $a \in G - \{e\}$. Atunci ecuația $x^n = a$ nu are soluție în G , contradicție.

(iii) Fie H un subgrup normal al grupului divizibil G . Fie $\hat{a} \in G/H$ și $n \in \mathbb{N}^*$. Cum G este divizibil există $x \in G$ cu $x^n = a$. Atunci $\hat{x}^n = \hat{a}$, deci și 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, ecuația $2x = 1$ neavând soluție în \mathbb{Z} .

(iv) Pe $\mathbb{R}_+^* \times \mathbb{R}$ definim operația $(a_1, x_1) * (a_2, x_2) = (a_1 a_2, a_1 x_2 + x_1)$. Se verifică ușor că această operație definește o structură de grup. Acest grup nu este abelian, deoarece $(1, 1)(2, 1) = (2, 2)$ și $(2, 1)(1, 1) = (2, 3)$. Arătăm că acest grup este divizibil. Fie $(a, b) \in \mathbb{R}_+^* \times \mathbb{R}$ și $n \in \mathbb{N}^*$. 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 și x cu $c^n = a$ și $(c^{n-1} + \cdots + c + 1)x = b$. Atunci luăm $c = \sqrt[n]{a}$ și $x = b/(c^{n-1} + \cdots + c + 1)$ și acestea verifică relațiile cerute.

(v) Fie G grup divizibil și 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) $H, xH, \dots, x^n H$ nu pot fi distincte, deci există $i, j \in \{0, 1, \dots, n\}$, $j > i$, cu $x^i H = x^j H$, 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 $H = G$.

Observație. O altă soluție, mai puțin elementară, se poate obține folosind problema 75. Deoarece indicele lui H este finit, atunci și indicele lui H_G , interiorul normal al lui H în G , este finit (și 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) și va fi cu necesitate trivial, deci $H_G = G$. De aici rezultă că $H = G$.

(vi) Fie $(G, +)$ un grup divizibil și să presupunem că există H_1, \dots, H_n subgrupuri proprii ale lui G cu proprietatea că $G = \bigcup_{i=1}^n H_i$ și $H_i \not\subseteq \bigcup_{j \neq i} H_j$ pentru orice $i = 1, \dots, n$. Alegem acum două elemente $x_1 \in H_1 - \bigcup_{i \neq 1} H_i$ și $x_2 \in H_2 - \bigcup_{i \neq 2} H_i$. Să observăm că dacă $x_1 = ky_1$, cu $k \in \mathbb{N}^*$ și $y_1 \in G$, atunci

$y_1 \in H_1 - \bigcup_{i \neq 1} H_i$. În mod evident $y_1 \notin \bigcup_{i \neq 1} H_i$ și atunci, deoarece $G = \bigcup_{i=1}^n H_i$, rămâne ca singură posibilitate $y_1 \in H_1$.

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

36 Fie $f : \mathbb{Q} \rightarrow G$ un morfism de grupuri. $H = \text{Ker}(f)$ este subgrup al lui $(\mathbb{Q}, +)$ și există $\bar{f} : \mathbb{Q}/H \rightarrow G$ 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 și astfel obținem că $\text{Hom}_{gr}(\mathbb{Q}, G) = \{0\}$.

37. (i) Considerăm mulțimea

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

Aceasta este o mulțime nevidă, deoarece $X \in \mathcal{F}$, și este ordonată în raport cu incluziunea. Arătăm că este inductiv ordonată. Pentru aceasta fie $(Y_i)_{i \in I}$ o submulțime total ordonată a lui \mathcal{F} și $Y = \bigcup_{i \in I} Y_i$. Atunci Y este sub-

grup al lui G . Într-adevăr, dacă $g, h \in Y$, atunci există $i, j \in I$ cu $g \in Y_i$ și $h \in Y_j$. Avem $Y_i \subseteq Y_j$ sau $Y_j \subseteq Y_i$. Fără a micșora generalitatea presupunem $Y_i \subseteq Y_j$. Atunci $g, h \in Y_j$ și cum acesta este subgrup obținem $gh^{-1} \in Y_j$. 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, \dots, g_p pentru G , rezultă că aceștia se găsesc în Y , deci există $i_1, \dots, i_p \in I$ cu $g_j \in Y_{i_j}$. Din faptul că mulțimea aleasă este total ordonată rezultă că putem găsi un j cu $g_1, \dots, g_p \in Y_{i_j}$. Atunci $Y_{i_j} = G$, contradicție. Evident Y este un majorant pentru familia $(Y_i)_{i \in I}$ și atunci \mathcal{F} este inductiv ordonată. Din Lema lui Zorn rezultă că \mathcal{F} are un element maximal H și acesta este chiar un subgrup maximal în G care conține 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 și 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 și $H \subseteq K \subseteq G$. Dar $K \neq H$ și $K \neq G$, deci H nu este maximal, contradicție. Deci G nu are subgrupuri maximale.

38. Presupunem că G are un singur subgrup maximal, fie acesta H . Fie $x \in G - H$. Dacă $\langle x \rangle \neq G$, din problema 37(i) rezultă că există un subgrup maximal al lui G care îl include pe $\langle x \rangle$. Dar singurul subgrup maximal este H și acesta nu îl include pe $\langle x \rangle$, deoarece nu conține elementul x . Rezultă că $\langle x \rangle = G$, 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 $\langle \hat{p} \rangle$ 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 și deci $m = p^n$ cu $n \geq 2$. Reciproc, dacă $G = \mathbb{Z}_{p^n}$, rezultă din structura subgrupurilor acestui grup că $\langle \hat{p} \rangle$ este unicul subgrup maximal, deci și G are un unic subgrup maximal.

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

40. Scriem $G/Z(G) = \langle \hat{g} \rangle$. Fie $x, y \in G$. Atunci $\hat{x}, \hat{y} \in G/Z(G)$ și 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 $\text{Aut}(G)$ pentru nici un grup G . Presupunem contrariul. Dacă G ar fi grup abelian, atunci $\text{Aut}(G)$ ar conține un element de ordin 2, și anume $f : G \rightarrow G$, $f(x) = x^{-1}$. Dar X nu are elemente de ordin 2, contradicție. Presupunem acum că G este neabelian și că $X \simeq \text{Aut}(G)$. Atunci $\text{Inn}(G)$ este subgrup al unui grup ciclic, deci este ciclic și din problema 39(iii) rezultă că $G/Z(G)$ este grup ciclic. Din problema 40 rezultă atunci că G este grup abelian, contradicție. Așadar X nu este izomorf cu $\text{Aut}(G)$ pentru nici un grup G .

42. (i) Soluția problemei 4 descrie endomorfismele grupului $(\mathbb{Z}, +)$. Este clar că dintre acestea sunt izomorfisme doar identitatea și aplicația $g : \mathbb{Z} \rightarrow \mathbb{Z}$ definită prin $g(x) = -x$. Așadar $\text{Aut}(\mathbb{Z})$ este un grup cu două elemente, deci este izomorf cu \mathbb{Z}_2 .

(ii) Tot în soluția problemei 4 găsim descrise endomorfismele grupului $(\mathbb{Q}, +)$. Se observă că acestea sunt unic determinate de valoarea lor în 1. Așadar putem defini o aplicație $F : \text{Aut}(\mathbb{Q}) \rightarrow (\mathbb{Q}^*, \cdot)$ prin $F(f) = f(1)$. Se verifică ușor că F este izomorfism de grupuri.

(iii) Folosim descrierea endomorfismelor lui \mathbb{Z}_n din soluția problemei 4. Morfismul $f_{\hat{a}} : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ definit prin $f_{\hat{a}}(\hat{x}) = \hat{a}\hat{x}$ este automorfism dacă și numai dacă este surjectiv (deoarece \mathbb{Z}_n este mulțime 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 aplicația $F : U(\mathbb{Z}_n) \rightarrow \text{Aut}(\mathbb{Z}_n)$, $F(\hat{a}) = f_{\hat{a}}$ 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 $\sigma \in S_3$, aplicația $f_\sigma : G \rightarrow G$ definită prin $f_\sigma(e) = e$ și $f_\sigma(x_i) = x_{\sigma(i)}$ este automorfism al lui G . Cum un automorfism duce pe e în e și este bijectiv, rezultă că $\text{Aut}(G) = \{f_\sigma \mid \sigma \in S_3\}$. Mai departe este clar că aplicația $F : S_3 \rightarrow \text{Aut}(G)$, $F(\sigma) = f_\sigma$, este izomorfism de grupuri.

43. Știm că grupul S_3 este generat de $\sigma = (123)$ și $\tau = (12)$. Dacă $f \in \text{Aut}(S_3)$, 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 și trei elemente de ordin 2, rezultă că există cel mult șase automorfisme (un automorfism al lui S_3 este complet determinat de $f(\sigma)$ și $f(\tau)$). Pe de altă parte, $\text{Inn}(S_3) \simeq S_3/Z(S_3) \simeq S_3$ (centrul lui S_3 este trivial, vezi problema 56), deci există șase automorfisme interioare ale lui S_3 și deci $\text{Aut}(S_3) = \text{Inn}(S_3) \simeq S_3$.

Pentru descrierea automorfismelor grupului diedral D_4 să reamintim că $D_4 = \langle r, s \rangle$, cu $\text{ord}(r) = 4$, $\text{ord}(s) = 2$ și $sr = r^3s$. De asemenea, D_4 are două elemente de ordin 4, r și r^3 , și 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 $\text{Im}(h) \subseteq \langle r \rangle$, deci h nu ar fi surjectiv. Deci $h(s)$ poate lua doar patru valori. Se verifică ușor că orice h definit în acest mod (pe generatori) este într-adevăr un automorfism și deci $|\text{Aut}(D_4)| = 8$. Mai departe, dacă notăm cu h automorfismul pentru care $h(r) = r$ și $h(s) = rs$, și cu g automorfismul pentru care $g(r) = r^3$ și $g(s) = s$, avem $\text{ord}(h) = 4$, $\text{ord}(g) = 2$ și $gh = h^3g$, de unde rezultă că $\text{Aut}(D_4) = \langle g, h \rangle \simeq D_4$.

44. (i) Grupul $\mathbb{Z} \times \mathbb{Z}$ nu este ciclic. Într-adevăr, dacă $\mathbb{Z} \times \mathbb{Z} = \langle (a, b) \rangle$, 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 obținem $a = 0$, deci $\langle (0, 0) \rangle = \mathbb{Z} \times \mathbb{Z}$, contradicție. 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 și nu este ciclic, și anume $\mathbb{Z} \times \mathbb{Z}$. Acesta este generat de $(1, 0)$ și $(0, 1)$ și 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} și $\mathbb{Q} \times \mathbb{Q}$ nu sunt izomorfe.

(iii) Aplicația $f : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{C}$, $f(a, b) = a + ib$, este un izomorfism de grupuri. Folosind acum rezultatul de la problema 5 care afirmă că \mathbb{R} și \mathbb{C} sunt grupuri izomorfe, obținem că \mathbb{R} este izomorf cu $\mathbb{R} \times \mathbb{R}$.

45. (i) Fie $f : \mathbb{R} \rightarrow S^1$ definită prin $f(x) = \cos(2\pi x) + i \sin(2\pi x)$. Este imediat că f este morfism surjectiv de grupuri. Mai departe $\text{Ker}(f) = \mathbb{Z}$ și aplicând teorema fundamentală de izomorfism obținem $\mathbb{R}/\mathbb{Z} \simeq S^1$.

(ii) Fie $g : \mathbb{Q} \rightarrow S^1$ definită prin $g(x) = \cos(2\pi x) + i \sin(2\pi x)$. Atunci g este morfism de grupuri, $\text{Im}(g) = U_\infty$ și $\text{Ker}(g) = \mathbb{Z}$. Din nou aplicând teorema fundamentală de izomorfism obținem $\mathbb{Q}/\mathbb{Z} \simeq U_\infty$.

(iii) Grupurile $(\mathbb{R}, +)$ și $(\mathbb{R}/\mathbb{Q}, +)$ pot fi înzestrate cu structuri de \mathbb{Q} -spații vectoriale dacă definim înmulțirea cu scalari prin $q \cdot x = qx$, oricare ar fi $q \in \mathbb{Q}$ și $x \in \mathbb{R}$, pentru primul grup și $q \cdot (x + \mathbb{Q}) = qx + \mathbb{Q}$, oricare ar fi $q \in \mathbb{Q}$ și $x \in \mathbb{R}$, pentru al doilea grup (se observă că definiția nu depinde de reprezentantul x). Ca la problema 5, \mathbb{Q} -spațiul 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 și \mathbb{R}/\mathbb{Q} are o bază de același cardinal. Atunci \mathbb{R} și \mathbb{R}/\mathbb{Q} sunt \mathbb{Q} -spații vectoriale de aceeași dimensiune. Rezultă că ele sunt izomorfe și în particular și grupurile subiacente sunt izomorfe.

(iv) Din cele arătate la (i) avem un izomorfism de grupuri $F : \mathbb{R}/\mathbb{Z} \rightarrow S^1$ 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} și $F(\mathbb{Q}/\mathbb{Z}) = U_\infty$. Obținem 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) și (iv) de la problema 45 rezultă că grupurile \mathbb{R} și 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 $z^2 = 1$ (și 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. Aplicația $f : \mathbb{R}_+^* \times \mathbb{R} \rightarrow \mathbb{C}^*$ definită prin $f(r, a) = r(\cos a + i \sin a)$ este un morfism surjectiv de grupuri și $\text{Ker}(f) = \{1\} \times \mathbb{Z}$. Rezultă că $\mathbb{C}^* \simeq \mathbb{R}_+^* \times (\mathbb{R}/\mathbb{Z})$. Din problema 5 știm că $(\mathbb{R}_+^*, \cdot) \simeq (\mathbb{R}, +)$, deci $\mathbb{C}^* \simeq \mathbb{R} \times (\mathbb{R}/\mathbb{Z})$. Pe de altă parte \mathbb{Q} -spațiile vectoriale \mathbb{R} și $\mathbb{R} \times \mathbb{R}$ au aceeași dimensiune (care este egală cu $|\mathbb{R}|$) și putem găsi astfel un izomorfism $f : \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R}$ cu $f(1) = (0, 1)$ (aceasta se poate face alegând în \mathbb{R} o bază care îl conține pe 1 și în $\mathbb{R} \times \mathbb{R}$ o bază care îl conține pe $(0, 1)$ și construind pe f astfel încât aceste elemente ale bazelor să se corespundă). Atunci f este și izomorfism de grupuri și 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), și de aici rezultă că $\mathbb{C}^* \simeq S^1$.

Deoarece $\mathbb{R} \times \mathbb{R} \simeq \mathbb{C}$ (prin $(a, b) \rightarrow a + ib$) și imaginea lui $\mathbb{Z} \times \{0\}$ prin acest izomorfism este chiar \mathbb{Z} , obținem $(\mathbb{R}/\mathbb{Z}) \times \mathbb{R} \simeq \mathbb{C}/\mathbb{Z}$ și 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 notațiile din problema 8). Atunci $K \trianglelefteq H$ și $H \trianglelefteq G$, deoarece în fiecare caz indicele subgrupului este 2. Însă $K \not\trianglelefteq G$, deoarece $rsr^{-1} = sr^2 \notin K$.

49. (i) Dacă $h \in H$ și $k \in K$ 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) Știm că G/H este grup finit și $HK/H \leq G/H$. Rezultă atunci că $(|HK/H|, |K|) = 1$. Dar $HK/H \simeq K/H \cap K$, deci $(|K/H \cap K|, |K|) = 1$. Acum $|K| = [K : H \cap K]|H \cap K|$ și 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 bijecție $f : (H/H \cap K)_s \rightarrow (HK/K)_s$ definită prin $f(x(H \cap K)) = xK$. Se verifică ușor că f este bine definită și că este bijectivă. Atunci $[HK : K] = [H : H \cap K]$. Acum avem $[G : K] = [G : HK][HK : K] = [G : HK][H : H \cap K]$ și înmulțind 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 obținem $H \subseteq K$.

50. (i) Luăm $G_1 = G_2 = \mathbb{Z}_2 \times \mathbb{Z}_4$, $H_1 = \mathbb{Z}_2 \times \{0\}$ și $H_2 = \{0\} \times \hat{\mathbb{Z}}_4$. Avem $G_1/H_1 \simeq \mathbb{Z}_4$ și $G_2/H_2 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, deci cele două grupuri factor nu sunt izomorfe.

(ii) Fie $G_1 = G_2 = \mathbb{Z}_2 \times \mathbb{Z}_4$, $H_1 = \{0\} \times \mathbb{Z}_4$ și $H_2 = \mathbb{Z}_2 \times \hat{\mathbb{Z}}_4$ (observăm că H_1 și 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 $G = \mathbb{Z}_4$, $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$, $H_1 = \hat{\mathbb{Z}}_4$, $H_2 = \{0\} \times \mathbb{Z}_2$. Atunci $G_1/H_1 \simeq G_2/H_2 \simeq \mathbb{Z}_2$.

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

52. (i) Fie $g \in I$ și $A = g^{-1}I \cap I$. 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 $a \in I$ și $a = g^{-1}b$, 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 și are mai mult de $(1/2)|G|$ elemente, rezultă că $C(g) = G$, deci $g \in Z(G)$. Rezultă $I \subseteq Z(G)$ și cum $|I| > (3/4)|G|$ obținem $|Z(G)| > (3/4)|G|$, 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 aceleași 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 $\sigma \in N$, $\sigma \neq \text{Id}_X$. 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 transpoziția definită de $\tau_{x',y}(x') = y$, $\tau_{x',y}(y) = x'$ și $\tau_{x',y}(z) = z$ 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 $\sigma \neq \text{Id}_X$, avem că $\sigma_y \neq \text{Id}_X$ pentru orice $y \in X$, $y \neq x$. În concluzie, $|X| \leq |N|$.

Revenim acum la rezolvarea problemei. Dacă una dintre mulțimile X, Y este finită, atunci și cealaltă este finită și în mod evident cele două mulțimi vor avea același număr de elemente.

Considerăm că X, Y sunt mulțimi infinite și fie $f : S(X) \rightarrow S(Y)$ un izomorfism. Fie N mulțimea *permutărilor finite* ale lui X , adică permutările lui X care acționează doar asupra unei submulțimi finite F a lui X lăsând neschimbate elementele din $X - F$. Este ușor de arătat că N este subgrup normal al lui $S(X)$. Mai mult, $|N| = |X|$, deoarece mulțimea părților finite ale unei mulțimi infinite are același cardinal cu mulțimea 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 $|Y| \geq |X|$ și 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 și deci orice subgrup al său este normal. Dacă $n \geq 3$, cum $(12) \in H$ și $(1n)(12)(1n) = (2n) \notin H$, rezultă că H nu este subgrup normal.

(iii) Aplicația $f : H \rightarrow S_{n-1}$ definită prin $f(\sigma)(i) = \sigma(i)$ pentru orice $i \in \{1, \dots, n-1\}$ este în mod evident un izomorfism de grupuri.

(iv) Se observă că pentru $\sigma, \tau \in S_n$, $\sigma \equiv \tau \pmod{H}$ dacă și numai dacă $\sigma(n) = \tau(n)$. Fie $\sigma_1, \dots, \sigma_n \in S_n$ cu proprietatea că $\sigma_i(n) = i$ pentru orice $i \in \{1, \dots, n\}$. Mulțimea $\{\sigma_1, \dots, \sigma_n\}$ este un sistem de reprezentanți pentru clasele la stânga modulo H . Cum fiecare σ_i se poate alege în $(n-1)!$ moduri, obținem $[(n-1)!]^n$ sisteme de reprezentanți.

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 $k \neq i, j$ și $\tau = (ijk)$. Atunci $\sigma\tau(i) = i$ și $\tau\sigma(i) = k$, deci $\sigma\tau \neq \tau\sigma$, contradicție. Dacă $\sigma(j) = k \neq i$, atunci avem și $k \neq j$. Fie acum $\tau = (ij)$. Avem $\sigma\tau(i) = k$ și $\tau\sigma(i) = i$, deci $\sigma\tau \neq \tau\sigma$, contradicție. Rezultă că $Z(S_n) = \{e\}$.

Fie acum $\sigma \in Z(A_n)$ și din nou presupunem că $\sigma \neq e$, deci există $i \neq j$ cu $\sigma(i) = j$. Dacă $\sigma(j) = i$ luăm $\tau = (ijk) \in A_n$ și 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 $n \geq 4$) și $\tau = (ij)(kl) \in A_n$. Atunci $\sigma\tau(i) = k$ și $\tau\sigma(i) = i$, deci $\sigma\tau \neq \tau\sigma$ și din nou obținem o contradicție. Așadar $Z(A_n) = \{e\}$.

56. Se știe 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 $f : S_n \rightarrow A_{n+2}$ astfel: dacă $\sigma \in S_n$ este permutare pară, atunci $f(\sigma)(i) = \sigma(i)$ pentru $1 \leq i \leq n$ și $f(\sigma)(i) = i$ pentru $i \in \{n+1, n+2\}$. Dacă σ este permutare impară, definim $f(\sigma)(i) = \sigma(i)$ pentru $1 \leq i \leq n$, $f(\sigma)(n+1) = n+2$ și $f(\sigma)(n+2) = n+1$. Este imediat că această aplicație este corect definită (adică are imaginea în A_{n+2}) și este morfism injectiv de grupuri.

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

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

s/d . Obținem că $\tau^k = \tau_1^{k_1} \cdots \tau_d^{k_1}$ și cum $(k_1, s_1) = 1$ rămâne să arătăm că $\tau_1^{k_1}, \dots, \tau_d^{k_1}$ sunt cicli disjuncți de lungime s_1 și cu aceeași orbită ca τ_1, \dots, τ_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 disjuncți (cu $r \geq 2$), atunci să presupunem că i_1 aparține orbitei ciclului π_1 . Rezultă că $\pi_1^m(i_1) = i_1$, unde m este lungimea ciclului π_1 . De aici obținem $\tau^{km}(i_1) = i_1 \Rightarrow km \equiv 0 \pmod{s} \Rightarrow s|km \Rightarrow s|m$, deoarece $(s, k) = 1$, deci $m \geq s$, contradicție. În concluzie $r = 1$.

58. Fie $n_i = \text{ord}(\pi_i)$ și $m = [n_1, \dots, n_r]$. Cum ciclul disjuncți comută, avem $(\pi_1 \cdots \pi_r)^m = \pi_1^m \cdots \pi_r^m = e$, deoarece $\text{ord}(\pi_i)|m$ pentru orice $i = 1, \dots, r$. Rezultă că $\text{ord}(\sigma)|m$.

Dacă $k \in \mathbb{N}^*$ și $\sigma^k = e$, 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 disjuncți ale căror orbite sunt submulțimi ale orbitei ciclului π_i , $i = 1, \dots, r$. Rezultă că τ_{ij} , $1 \leq j \leq s_i$, $1 \leq i \leq r$, sunt cicli disjuncți 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 $i \in \{1, \dots, r\}$, de unde obținem că $n_i|k$ pentru orice $i \in \{1, \dots, r\}$, deci $m|k$. Așadar $\text{ord}(\sigma) = m$.

59. Presupunem că $n \geq 6$ și 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 disjuncți, unde primii r factori sunt cicli disjuncți de lungime ≥ 3 , iar π este produsul ciclilor de lungime 2. Atunci $\sigma^2 = \pi_1^2 \cdots \pi_r^2$ și 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 disjuncți de lungime egală (vezi problema 57), iar τ conține un singur ciclu de lungime 2, contradicție. Dacă $n \leq 5$, se verifică ușor 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 disjuncți în care scriem și ciclul de lungime 1. Dacă $\sigma = e$, afirmația este evidentă. Altfel avem $p = \text{ord}(\sigma) = [\text{ord}(\pi_1), \dots, \text{ord}(\pi_r)]$, deci $\text{ord}(\pi_i) \in \{1, p\}$ pentru orice $i \in \{1, \dots, r\}$. Dacă $\text{ord}(\pi_i) = p$ pentru orice $i \in \{1, \dots, r\}$, atunci $n = \text{ord}(\pi_1) + \cdots + \text{ord}(\pi_r) = pr$, deci n se divide cu p , contradicție. Rezultă că există un ciclu π_i de lungime 1 și acesta ne dă un punct fix pentru σ .

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

de transpoziții dată. Într-adevăr, dacă $i \neq j$, avem $(ij) = (1i)(1j)(1i)$ și afirmația este demonstrată.

(ii) Este suficient să arătăm că transpozițiile de la (i) sunt în subgrupul generat de familia dată. Pentru aceasta folosim următoarea relație 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 transpozițiile din enunț rezultă prin inducție după i . Pentru $i = 2$, transpoziția (12) apare printre cele date. Presupunem că $(1i)$ este în subgrupul generat de familia de transpoziții dată. Din formulă rezultă că și $(1, i+1)$ se află acolo.

(iii) Să observăm că pentru orice $1 \leq i \leq n-2$ are loc următoarea relație:

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

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

62. Presupunem prin absurd că există $n-2$ transpoziții care generează pe S_n . Fie acestea $\tau_1, \dots, \tau_{n-2}$. Există printre acestea una care îl conține pe 1 în orbită, altfel 1 ar fi fixat de toate aceste transpoziții și deci de toate permutările din S_n , contradicție. Eventual renotând, putem presupune că $\tau_1 = (1, i_1), \dots, \tau_p = (1, i_p)$ sunt toate cele care îl conțin pe 1 în orbită. Dacă $p = n-2$, atunci există $i \in \{1, \dots, n\} - \{1, i_1, \dots, i_p\}$ și acest i este fixat de toate transpozițiile date, deci de toate permutările din S_n , contradicție. Deci $p < n-2$. Acum dacă există $\tau \in \{\tau_{p+1}, \dots, \tau_{n-2}\}$ care conține în orbită unul dintre elementele i_1, \dots, 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 transpozițiile $\tau_{p+1}, \dots, \tau_{n-2}$ nu are în orbită vreun element din mulțimea $\{1, i_1, \dots, i_p\}$. Alegem $j \notin \{1, i_1, \dots, i_p\}$ și atunci transpoziția $(1j)$ nu se poate scrie ca produs de transpoziții din mulțimea $\{\tau_1, \dots, \tau_{n-2}\}$, deoarece un astfel de produs duce pe 1 într-unul din elementele $1, i_1, \dots, i_p$, contradicție.

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

transpoziții este în subgrupul generat de ciclul de lungime 3. Pentru aceasta observăm că au loc formulele: $(ij)(kl) = (ijk)(ikl)$ și $(ij)(il) = (ilj)$ și demonstrația este încheiată.

64. Arătăm mai întâi că dacă N este un subgrup normal netrivial al lui A_n care conține un ciclu de lungime 3, atunci N conține toți ciclul de lungime 3. Să presupunem că $(123) \in N$. Atunci pentru permutarea $\tau \in S_n$ cu $\tau(1) = i, \tau(2) = j, \tau(3) = k$ și $\tau(l) = l$ 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 și diferite de i, j, k .

Vom arăta acum că dacă N este un subgrup normal netrivial al lui A_n , atunci el conține 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 conține în descompunere un ciclu $(ijkl \dots)$ de lungime cel puțin 4. Luăm $\tau = (ijk)$ și obținem $\sigma\tau\sigma^{-1} = (jkl)$ și deci $[\sigma, \tau] = (ilj) \in N$.

b) σ conține în descompunere un ciclu (ijk) de lungime 3. Scriem $\sigma = (ijk)(lm \dots) \dots$, luăm $\tau = (ijl)$ și obținem $\sigma\tau\sigma^{-1} = (jkm)$ și deci $[\sigma, \tau] = (ilkmj) \in N$. Aplicăm acum cazul a) cu $[\sigma, \tau]$ în loc de σ .

c) σ conține în descompunere doar cicluri de lungime 2. Scriem $\sigma = (ij)(kl) \dots$, alegem m diferit de i, j, k, l , luăm $\tau = (ikm)$ și obținem $\sigma\tau\sigma^{-1} = (jl\sigma(m))$. Avem următoarele posibilități pentru $[\sigma, \tau]$: dacă $\sigma(m) = m$, atunci $[\sigma, \tau] = (ijlmk)$ și aplicăm din nou cazul a) cu $[\sigma, \tau]$ în loc de σ . Altfel $[\sigma, \tau] = (jl\sigma(m))(mki)$ și din nou putem aplica cazul b) cu $[\sigma, \tau]$ în loc de σ .

De aici rezultă că N conține toți ciclul de lungime 3, deci conform problemei 63 obținem $N = A_n$, contradicție. Deci A_n este grup simplu.

65. Presupunem că H este un subgrup normal al lui S_n și 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 $A_n \subseteq H \subseteq S_n$ și 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 și conține o permutare impară, deci $HA_n \neq A_n$. Obținem $HA_n = S_n$ și 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 $\sigma = e$, contradicție. 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 și pentru celelalte elemente din K , de unde obținem $K \trianglelefteq S_4$.

(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 și conține un element de ordin 6, fie acesta $\hat{\sigma}$. Dar $\sigma \in S_4$ și deci $\text{ord}(\sigma) \in \{1, 2, 3, 4\}$. Atunci $\hat{\sigma}$ nu poate avea ordin 6, contradicție. Rezultă că $S_4/K \simeq S_3$.

(iii) Observăm că A_4 are un element de ordin 1, trei elemente de ordin 2 și 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 și cum în A_4 există doar trei elemente de ordin 2, cele din $K - \{e\}$, rezultă că $K \subseteq X$ și atunci, din teorema lui Lagrange, obținem $4|6$, contradicție. În concluzie, A_4 nu are subgrupuri cu 6 elemente.

(iv) Un subgrup propriu al lui A_4 are două, trei, patru sau șase elemente. Știm din (iii) că subgrupuri cu șase elemente nu există. Singurul subgrup cu 4 elemente este K , deoarece un grup cu patru elemente nu are elemente de ordin 3 și 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 cicluri de lungime 3 sau de produse de transpoziții disjuncte. În ambele situații, 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 transpoziție sau ciclu de lungime 4. Dacă σ este transpoziție, să zicem $\sigma = (ij)$, atunci $\tau\sigma\tau^{-1} = (\tau(i)\tau(j)) \in X$ pentru orice $\tau \in S_4$, deci X conține toate transpozițiile. De aici obținem că $X = S_4$. Dacă σ este ciclu de lungime 4, $\sigma = (ijkl)$, atunci X va conține toți ciclii de lungime 4. Cum $\sigma^2 = (ik)(jl) \in X$, X va conține și toate produsele de câte două transpoziții disjuncte, deci $K \subseteq X$. Dar $(ijkl)(iljk) = (jlk) \in X$, deci X conține toți ciclii de lungime 3. Rezultă că $A_4 \subsetneq X$, deci $X = S_4$.

67. (i) Dacă $f : S_n \rightarrow \mathbb{Z}$ este un morfism de grupuri, atunci $\text{Im}(f)$ este un subgrup finit al lui \mathbb{Z} , deci este $\{0\}$. Așadar avem numai morfismul nul.

(ii) Fie $f : S_n \rightarrow \mathbb{Q}^*$ 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 și rezultă că \mathbb{Q}^* are un subgrup neabelian (izomorf cu S_n), contradicție. Dacă $\text{Ker}(f) = A_n$,

atunci pentru o transpoziție $\tau \in S_n$ avem $1 = f(e) = f(\tau^2) = f(\tau)^2$, deci $f(\tau) \in \{-1, 1\}$. Cum $\tau \notin \text{Ker}(f)$, rezultă că $f(\tau) = -1$. Atunci $f(\sigma) = -1$ pentru orice permutare impară $\sigma \in S_n$, deci f este morfismul signatură. Dacă $\text{Ker}(f) = S_n$, atunci f este morfismul trivial. Deci există două morfisme, signatura și morfismul trivial.

Discutăm acum cazul $n = 4$. În acest caz, pe lângă $\{e\}$, A_4 și S_4 , grupul S_4 mai are și subgrupul normal K descris în problema 66. Dacă $\text{Ker}(f)$ este unul dintre primele trei subgrupuri, soluția decurge ca mai sus și obținem tot două morfisme, signatura și morfismul trivial. Dacă însă $\text{Ker}(f) = K$, atunci $f((ij)) = -1$ pentru orice $i \neq j$, deoarece $f((ij))^2 = 1$ și $f((ij)) \neq 1$. Avem acum că $f((123)) = f((13))f((12)) = 1$, deci $(123) \in \text{Ker}(f) = K$, contradicție. În concluzie și în acest caz avem tot două morfisme.

(iii) Soluția este similară cu cea de la (ii) și obținem tot două morfisme, morfismul nul și morfismul care duce permutările pare în $\hat{0}$ și permutările impare în $\hat{1}$.

68. (i) Fie $f : S_n \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ 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 ciclul de lungime 3 generează pe A_n (vezi problema 63), rezultă că $A_n \subseteq \text{Ker}(f)$. Atunci $\text{Ker}(f) = A_n$ sau $\text{Ker}(f) = S_n$. Dacă este $\text{Ker}(f) = S_n$, atunci f este morfismul nul. Dacă $\text{Ker}(f) = A_n$, fie σ și τ două permutări impare din S_n . Atunci $f(\sigma) \neq (\hat{0}, \hat{0})$, $f(\tau) \neq (\hat{0}, \hat{0})$ și $f(\sigma) + f(\tau) = (\hat{0}, \hat{0})$, de unde $f(\sigma) = f(\tau)$. Așadar 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 $a \in \mathbb{Z}_2 \times \mathbb{Z}_2$ aplicația $f : S_n \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ definită prin $f(\sigma) = 0$ pentru $\sigma \in A_n$ și $f(\sigma) = a$ pentru $\sigma \in S_n - A_n$, este un morfism de grupuri. Avem deci patru astfel de morfisme.

(ii) Fie $f : S_3 \rightarrow \mathbb{Z}_3$ un morfism de grupuri. Atunci $\text{Ker}(f)$ este subgrup normal al lui S_3 , deci poate fi $\{e\}$, A_3 sau S_3 . Dacă $\text{Ker}(f) = \{e\}$, atunci f este morfism injectiv, imposibil. Dacă $\text{Ker}(f) = A_3$, atunci $S_3/A_3 \simeq \text{Im}(f) \leq \mathbb{Z}_3$, deci \mathbb{Z}_3 are un subgrup cu două elemente, imposibil. Rămâne ca singură posibilitate $\text{Ker}(f) = S_3$ și în acest caz f este morfismul nul.

(iii) Dacă $f : \mathbb{Z}_3 \rightarrow S_3$ este morfism de grupuri, atunci sau $\text{Ker}(f) = \mathbb{Z}_3$ și atunci f este morfismul nul, sau $\text{Ker}(f) = \{\hat{0}\}$ și atunci f este morfism injectiv. În acest caz f este de forma: $f(\hat{0}) = e$, $f(\hat{1}) = \sigma$ și $f(\hat{2}) = \sigma^2$, unde σ este un ciclu de lungime 3, și avem deci două astfel de morfisme.

Avem în total trei morfisme.

69. Fie $f : S_4 \rightarrow S_3$ un morfism de grupuri. Cum $\text{Ker}(f) \trianglelefteq S_4$, rezultă că $\text{Ker}(f)$ poate fi $\{e\}$, K (descrie 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, contradicție. Dacă $\text{Ker}(f) = S_4$, atunci f este morfismul trivial.

Dacă $\text{Ker}(f) = A_4$, atunci $f((12)(34)) = e$, de unde $f((12)) = f((34))$ și sunt egale cu o transpoziție din S_3 . Mai departe $f((12))f((23)) = f((123)) = e$, deci $f((12)) = f((23))$. Procedând analog obținem $f(\sigma) = \tau$ pentru orice $\sigma \in S_4 - A_4$, unde τ este o transpoziție dată din S_3 . Evident, pentru orice astfel de transpoziție, aplicația f definită prin $f(\sigma) = e$ dacă $\sigma \in A_4$ și $f(\sigma) = \tau$ 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 obținem $f((12)) = f((34)) = \tau_1$, $f((13)) = f((24)) = \tau_2$ și $f((14)) = f((23)) = \tau_3$, unde τ_1, τ_2, τ_3 sunt transpoziții distincte din S_3 (dacă nu ar fi distincte am obține o relație de tipul $(ij)(ik) = (jik) \in \text{Ker}(f) = K$, contradicție). Este clar că pentru fiecare alegere a lui τ_1, τ_2, τ_3 distincte, relațiile de mai sus definesc un morfism de grupuri (având f definit pe transpoziții). Cum în S_3 avem exact trei transpoziții, rezultă că avem 6 posibilități 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 transpoziție, 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 . Așadar $f((ijk)) = f((ij))f((jk)) = e$, de unde $f((ij)) = f((jk))$, aceste elemente fiind egale cu inversele lor. Deci există $a \in H$ cu $f(\tau) = a$ pentru orice transpoziție $\tau \in S_n$. Din scrierea unei permutări ca produs de transpoziții 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 obținut că $[G : G \cap A_n] = 2$ și 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 conține o permutare impară, să o notăm cu σ . Rezultă imediat că $G \cap A_n$ și $\sigma(G \cap A_n)$ formează o partiție 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 știm că există un morfism injectiv de grupuri $f : G \rightarrow S(G)$ definit prin $f(x)(y) = xy$ pentru orice $x, y \in G$. (Prin $S(G)$ am notat grupul simetric al mulțimii G , care în acest caz este izomorf cu S_{4n+2}). Să observăm că permutarea $f(g)$ nu are puncte fixe, deoarece $g \neq e$, și că $(f(g))^2 = \text{Id}_G$. Rezultă că descompunerea lui $f(g)$ în produs de cicluri disjuncți constă în produsul a $2n + 1$ transpoziții. Așadar $f(g)$ este o permutare impară și aplicând (i) pentru grupul $\text{Im}(f)$ obținem că $\text{Im}(f)$ are un subgrup de indice 2. Dar f este morfism injectiv, deci $G \simeq \text{Im}(f)$, 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 și 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 $D_n = \{e, r, \dots, r^{n-1}, s, rs, \dots, r^{n-1}s\}$ cu $\text{ord}(r) = n$, $\text{ord}(s) = 2$ și $sr = r^{n-1}s$. Fie $j \in \{1, \dots, n-1\}$. Atunci $r^j \in Z(D_n)$ dacă și numai dacă $r^js = sr^j$, deoarece un element se găsește în centrul unui grup dacă și numai dacă el comută cu generatorii grupului. Această relație este echivalentă cu $r^js = r^{(n-1)j}s$, care la rândul ei se poate scrie $r^{(n-2)j} = e$. Cum $\text{ord}(r) = n$, rezultă că $n|(n-2)j$. Dacă n este impar acest lucru este imposibil, deoarece avem $(n, n-2) = 1$ și 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 $r^js \in Z(D_n)$ cu $1 \leq j \leq n-1$. Pentru că el comută cu r avem $r^jsr = r^{j+1}s \Rightarrow r^{j+n-1}s = r^{j+1}s \Rightarrow r^{n-2} = e$, ceea ce este imposibil.

Așadar 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 poziția (i, j) și 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 enunț 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 și problema 5).

Observație. 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 $GL(2, \mathbb{Z})$ și $GL(3, \mathbb{Z})$ sunt izomorfe. Vom defini acum un morfism injectiv de grupuri $f : GL(2, \mathbb{Z}) \times \{\pm 1\} \rightarrow GL(3, \mathbb{Z})$ 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 și $GL(2, \mathbb{Z})$ este izomorf cu $GL(3, \mathbb{Z})$, rezultă că avem un morfism injectiv de la $GL(2, \mathbb{Z}) \times \mathbb{Z}_2$ la $GL(3, \mathbb{Z})$. Iterând obținem 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 copii ale lui \mathbb{Z}_2) la $GL(3, \mathbb{Z})$. În particular, aceasta înseamnă că pentru orice $n \in \mathbb{N}^*$ există $A_1, \dots, A_n \in GL(2, \mathbb{Z})$ cu proprietatea că $\text{ord}(A_i) = 2$ și $A_i A_j = A_j A_i$, oricare ar fi $i, j \in \{1, \dots, n\}$.

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

Observație. Soluția 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 observație se poate generaliza ducând la concluzia că grupurile $GL(m, \mathbb{Z})$ și $GL(n, \mathbb{Z})$ nu sunt izomorfe pentru $m \neq n$.

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

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

deci H_G este egal cu toți conjugații 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 acțiunea prin translații la stânga a grupului G pe mulțimea $(G/H)_s$ a claselor la stânga modulo H , adică pentru $g \in G$ și $xH \in (G/H)_s$ avem $g(xH) = gxH$. Această acțiune dă naștere unui morfism de grupuri $f : G \rightarrow S((G/H)_s)$ definit prin $f(g)(xH) = g(xH) = gxH$. Să observăm că $g \in \text{Ker}(f)$ dacă și 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 $\text{Ker}(f) = H_G$ și atunci există un morfism injectiv de grupuri între G/H_G și $S((G/H)_s)$. Cum $|(G/H)_s| = [G : H] = n$, rezultă că $S((G/H)_s) \simeq S_n$ și de aici obținem morfismul injectiv căutat. În particular, H_G are indice finit ($\leq n!$) și este subgrup normal al lui G .

76. Vom arăta că $H_G = \{aI_n \mid a \in K^*\}$. Este evident că mulțimea matricelor scalare $\{aI_n \mid a \in K^*\}$ formează un subgrup normal al lui G conținut 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 poziția (i, j) și 0 în rest, și există $1 \leq i \neq j \leq n$ astfel încât $a_{ii} \neq a_{jj}$. Avem $E_{ij}A = \sum_{k=1}^n a_{kk}E_{ij}E_{kk} = a_{jj}E_{ij}$ și $AE_{ij} = \sum_{k=1}^n a_{kk}E_{kk}E_{ij} = a_{ii}E_{ij}$. 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 ușor că H este subgrup. Cum o matrice $\begin{pmatrix} \hat{a} & \hat{b} \\ \hat{0} & \hat{c} \end{pmatrix}$ din H are $\hat{b} \in \mathbb{Z}_3$ și $\hat{a}, \hat{c} \in \mathbb{Z}_3 - \{\hat{0}\}$, rezultă că H are 12 elemente. Știm că $Z(G)$ este format din mulțimea matricelor scalare din G , deci $|Z(G)| = 2$. Avem că $Z(G) \leq H$ și $Z(G) \trianglelefteq G$, 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 $B = \begin{pmatrix} \hat{0} & -\hat{1} \\ \hat{1} & \hat{0} \end{pmatrix}$ și avem că $BAB^{-1} = \begin{pmatrix} \hat{c} & \hat{0} \\ \hat{b} & \hat{a} \end{pmatrix}$, deci $\hat{b} = \hat{0}$. Acum pentru $B = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{1} & \hat{1} \end{pmatrix}$ obținem $BAB^{-1} = \begin{pmatrix} \hat{a} & \hat{0} \\ \hat{a} - \hat{c} & \hat{c} \end{pmatrix}$, deci $\hat{a} = \hat{c}$. În concluzie, $A = \hat{a}I_2 \in Z(G)$.

78. Presupunem că G este un grup simplu infinit și 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) și G (de indice 1), contradicție.

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 $[H : H_G] \mid (p-1)!$. Dacă $H \neq H_G$, atunci există q un divizor prim al lui $[H : H_G]$ și cum $q \mid (p-1)!$ rezultă că $q < p$. Dar $|G| = [G : H_G]|H_G| = [G : H][H : H_G]|H_G|$, deci $q \mid |G|$. Dar aceasta este o contradicție 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 acțiunea prin conjugare a lui G pe H și scriem ecuația claselor pentru această acțiune. 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 $|G|$ și p este cel mai mic număr prim care divide $|G|$, rezultă că $[G : C_G(x)] \geq p$, de unde $p = |H| = 1 + \sum [G : C_G(x)] \geq 1 + p$, contradicție.

80. Știm din problema 75 că dacă H este un subgrup de indice n al lui G , atunci există un morfism injectiv de grupuri $f : G \rightarrow S_n$ cu $\text{Ker}(f) = H_G$. Cum G este finit generat, rezultă că există un număr finit de astfel de morfisme. Într-adevăr, dacă g_1, \dots, g_m generează G și $f_1, f_2 : G \rightarrow S_n$ sunt morfisme de grupuri cu $f_1(g_1) = f_2(g_1), \dots, f_1(g_m) = f_2(g_m)$, atunci $f_1 = f_2$. Cum există doar un număr finit de posibilități pentru $f(g_1), \dots, f(g_m)$, rezultă că există doar un număr finit de morfisme $f : G \rightarrow S_n$. 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 posibilități pentru el.

Acum dacă X este un subgrup normal al lui G , există o corespondență bijectivă între subgrupurile lui G/X și 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 . Așadar există doar un număr finit de posibilități pentru H_G și 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 și fie acestea H_1, \dots, H_r . Dacă $\alpha \in \text{Aut}(G)$ și $H \leq G$ cu $[G : H] = n$, atunci și $[G : \alpha(H)] = n$. Rezultă că $\alpha(H_1), \dots, \alpha(H_r)$ sunt chiar H_1, \dots, 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 ecuația 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 obținem că G este abelian, de unde $Z(G) = G$, contradicție.

(ii) Dacă G are un element de ordin p^2 , atunci este ciclic și deci este izomorf cu \mathbb{Z}_{p^2} . Dacă toate elementele $\neq e$ ale lui G au ordinul p , atunci fie $x \in G$, $x \neq e$ și $y \in G - \langle x \rangle$. Evident $\langle x \rangle \cap \langle y \rangle = \{e\}$. Definim acum $f : G \rightarrow G/\langle x \rangle \times G/\langle y \rangle$ prin $f(a) = (\bar{a}, \bar{a})$. Se verifică ușor că f este morfism de grupuri și din faptul că $\langle x \rangle \cap \langle y \rangle = \{e\}$ rezultă că este injectiv. Cum G și $G/\langle x \rangle \times G/\langle y \rangle$ au același număr de elemente, f va fi și surjectiv, deci f este izomorfism de grupuri. În concluzie, în acest caz G este izomorf cu $\mathbb{Z}_p \times \mathbb{Z}_p$.

82. Știm 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 și ale lui S_4 . Cum pentru A_4 avem $n_3|4$, rezultă că $n_3 = 4$ și H_1, H_2, H_3, H_4 sunt toate 3-subgrupurile Sylow ale lui A_4 . Pentru S_4 avem $n_3|8$ și $n_3 \equiv 1 \pmod{3}$. Cum $n_3 \geq 4$, rezultă că $n_3 = 4$, deci H_1, H_2, H_3, H_4 sunt toate 3-subgrupurile Sylow și în S_4 .

Pentru S_4 avem $n_2 = 3$, deoarece $D_4 = \langle (1234), (12) \rangle$ este subgrup al lui S_4 care nu este normal (și 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 $K \trianglelefteq A_4$ și $|K| = 2^2$.

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 și $k_i \geq 1$. 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 $G_i = \langle x_i \rangle$, deci $\text{ord}(x_i) = p_i^{k_i}$. Deoarece G este grup abelian și numerele $p_i^{k_i}$ sunt oricare două prime între ele, obținem că $\text{ord}(x_1 \cdots x_r) = p_1^{k_1} \cdots p_r^{k_r}$, 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 conține elemente de ordin 2, de unde rezultă că $H \subseteq \langle r \rangle$, 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 $\langle (1234), (12) \rangle$ este un 2-subgrup Sylow al lui S_5 care este izomorf cu D_4 (prin morfismul care asociază (1234) lui r și (12) lui s), ar rezulta că $D_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, contradicție.

85. (i) Cum orice conjugat al lui H este tot un p -subgrup Sylow și există un singur astfel de subgrup, rezultă că H este egal cu toți conjugatii săi, deci este normal.

(ii) Fie H_1, \dots, 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, mulțimea elementelor de ordin p din G este chiar $(H_1 \cup \dots \cup H_{n_p}) - \{e\}$, deoarece orice element de ordin p generează un p -subgrup Sylow, deci această mulțime are $n_p(p - 1)$ elemente.

86. (i) Se verifică ușor că operația este asociativă, admite element neutru pe (e_N, e_H) și orice element este inversabil, inversul unui element (n, h) fiind $(\varphi(h^{-1})(n^{-1}), h^{-1})$.

Fie $p : G \rightarrow H$ definită prin $p(n, h) = h$. Este imediat că p este morfism surjectiv de grupuri și $\text{Ker}(p) = N'$, deci $N' \trianglelefteq G$. Celelalte afirmații rezultă din calcule simple.

(ii) Să observăm mai întâi că orice element al lui G se scrie în mod unic sub forma nh , cu $n \in N$ și $h \in H$. 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 aplicația $\alpha : N \rtimes_{\varphi} H \rightarrow G$ 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 $n_p \in \{1, q\}$ și $n_p \equiv 1 \pmod{p}$. Cum p nu divide $q - 1$, rezultă $n_p = 1$. Apoi $n_q|p$ și $n_q \equiv 1 \pmod{q}$. Cum $p < q$, rezultă că $n_q = 1$. Aplicăm acum problema 85 și obținem că există $p - 1$ elemente de ordin p și $q - 1$ elemente de ordin q în G . Cum $1 + p - 1 + q - 1 < pq$, rezultă că mai există și alte elemente în G . Deoarece p, q sunt prime, divizorii lui pq sunt $1, p, q$ și pq . Atunci acele elemente au ordin pq și deci G este ciclic.

(ii) Să observăm că G admite un q -subgrup Sylow normal (notat în cele ce urmează cu N), deoarece și în acest caz $n_q = 1$. Fie H un p -subgrup Sylow al lui G . Rezultă că $N \cap H = \{e\}$ și deoarece NH are pq elemente avem $NH = G$. Deci G este produs semidirect intern al subgrupurilor N și H . Dar $N \simeq \mathbb{Z}_q$, iar $H \simeq \mathbb{Z}_p$.

Un astfel de produs semidirect este unic definit de morfismul corespunzător de la \mathbb{Z}_p la $\text{Aut}(\mathbb{Z}_q) \simeq \mathbb{Z}_{q-1}$. Se știe din problema 4 că există exact p astfel de morfisme și 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 $\text{Aut}(\mathbb{Z}_q)$, $i = 0, 1, \dots, p - 1$. Produsul semidirect corespunzător G_i se poate descrie prin generatori și relații astfel: fie x un generator al lui \mathbb{Z}_q și y un generator al lui \mathbb{Z}_p . Atunci $G_i = \langle x, y : x^q = y^p = e, yxy^{-1} = \pi^{i(q-1)/p}(x) \rangle$. În particular, dacă $i = 0$, atunci G_0 este abelian și deci ciclic de ordin pq . Dacă $i \neq 0$, atunci G_i este izomorf cu G_1 . Într-adevăr aplicația $G_1 \rightarrow G_i$ care duce pe x în x și pe y în y^i este un izomorfism.

88. Fie G un grup cu p^n elemente, p număr prim și $n > 1$. Dacă G nu este abelian, atunci centrul său, care este netrivial (după cum rezultă din ecuația claselor de conjugare), este un subgrup normal propriu și 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 $\langle g \rangle$ este propriu, netrivial și 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) obținem 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 și 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 $n_q > 1$ și de asemenea $n_q \neq p$, deoarece $n_q \equiv 1 \pmod{q}$. Rezultă că $n_q = p^2$. Din problema 85(ii) obținem că numărul elementelor de ordin q din G este $n_q(q-1) = p^2(q-1)$. Atunci mulțimea $A = \{g \in G \mid g \text{ are ordinul diferit de } q\}$ are exact p^2 elemente. Cum orice p -subgrup Sylow al lui G este inclus în A și are p^2 elemente, rezultă că orice p -subgrup Sylow este egal cu A . Așadar $n_p = 1$, contradicție. 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 puțin $r(q-1)$. În sfârșit, avem $n_p \in \{1, q, r, qr\}$, deci $n_p \geq q$ și numărul elementelor de ordin p este cel puțin $q(p-1)$. Ținând cont și 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 $0 \geq (r-1)(q-1)$, contradicție. Așadar G nu este grup simplu.

89. (i) Fie p un număr prim cu proprietatea că $p || |G|$ și H un p -subgrup Sylow al lui G . Scriem $|G_i| = p^{k_i} m_i$ cu $(p, m_i) = 1$. Fie $\pi_i : G \rightarrow G_i$ proiecția canonică și $H_i = \pi_i(H)$. În mod evident H_i este subgrup al lui G_i și deoarece este izomorf cu un grup factor al lui H (din teorema fundamentală de izomorfism pentru grupuri aplicată restricției lui π_i la H) rezultă că este un p -grup, adică are ordinul o putere a lui p . Notăm $|H_i| = p^{l_i}$ și 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 $|H| \leq |H_1| \cdots |H_n| \Rightarrow p^{k_1 + \cdots + k_n} \leq p^{l_1 + \cdots + l_n} \Rightarrow k_1 + \cdots + k_n \leq l_1 + \cdots + l_n$ și 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 același număr de elemente și 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 $\hat{3}\mathbb{Z}_6 \times \langle \tau \rangle$, unde $\tau \in S_3$ este o transpoziție, iar 3-subgrupurile Sylow sunt $\hat{2}\mathbb{Z}_6 \times \langle \sigma \rangle$, unde $\sigma \in S_3$ este un ciclu de lungime 3.

90. Să începem prin a face următoarea remarcă: dacă G este un grup și $H, K \subseteq G$ sunt subgrupuri normale cu proprietatea că $H \cap K = \{e\}$, atunci oricare ar fi $x \in H$ și $y \in K$ rezultă că $xy = yx$. Aceasta rezultă imediat: se consideră elementul $xyx^{-1}y^{-1}$ și se observă că datorită faptului că H și 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 $i = 1, \dots, n$. Știm că $H_i \trianglelefteq G$. Din remarca de mai sus rezultă că dacă $x \in H_i$ și $y \in H_j$, atunci $xy = yx$, pentru orice $i, j \in \{1, \dots, n\}$. 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 și din teorema a doua de izomorfism pentru grupuri obținem 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 $H_1 \cdots H_n \subseteq G$ și au același număr de elemente obținem $H_1 \cdots H_n = G$, deci G este grup abelian. Acum rezultă imediat că G este izomorf cu $H_1 \times \cdots \times H_n$: definim $f : H_1 \times \cdots \times H_n \rightarrow G$ prin $f(h_1, \dots, h_n) = h_1 \cdots h_n$ și rezultă din cele de mai sus că f este izomorfism.

Observație. În condițiile din problemă rezultă că G este grup ciclic.

Capitolul 10

Soluții: Inele și 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 $\hat{1}$, înmulțirea "•" 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 $\hat{a} \in \mathbb{Z}_p$ înmulțirea $\hat{n} * \hat{m} = \widehat{nma}$ definește 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 $f : (\mathbb{Z}_p, +, \cdot) \rightarrow (\mathbb{Z}_p, +, *)$, $f(\hat{n}) = \widehat{na}$.

Dacă $\hat{a} = \hat{0}$, atunci $(\mathbb{Z}_p, +, *)$ este inelul nul, în care $\hat{n} * \hat{m} = \hat{0}$ pentru orice $\hat{n}, \hat{m} \in \mathbb{Z}_p$, și acesta este evident neizomorf cu $(\mathbb{Z}_p, +, \cdot)$.

Prin urmare există exact două structuri de inel neizomorfe pe o mulțime cu p elemente, și anume inelul nul și 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 $\hat{x}, \hat{y} \in \mathbb{Z}_n$ și se verifică ușor axiomele inelului). Arătăm că $(\mathbb{Z}_n, +, *)$ este inel unitar dacă și numai dacă $(a, n) = 1$. Într-adevăr, \hat{e} este element unitate în raport cu "•" dacă și 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 și numai dacă $(a, n) = 1$. Așadar, există $\phi(n)$ structuri de inel unitar pe $(\mathbb{Z}_n, +)$ și, la fel ca la soluția 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 și $r, s \in R$ două elemente arbitrare. Atunci există $m, p \in \mathbb{N}^*$ cu

$r = ma$ și $s = pa$. Rezultă $rs = (ma)(pa) = mpa^2 = pma^2 = (pa)(ma) = sr$ și 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 și 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 -spațiului vectorial R și $K = \{n \cdot 1_R \mid n \in \mathbb{N}^*\}$ este inclus în centrul lui R . Dacă $r, s \in R$, atunci există $\alpha, \beta, \gamma, \delta$ în K astfel încât $r = \alpha + \beta a$ și $s = \gamma + \delta a$. Efectuând înmulțirile obținem $rs = sr$.

Dacă R nu este inel unitar afirmația nu mai este adevărată. Fie $R = \mathbb{Z}_p \times \mathbb{Z}_p$ cu adunarea pe componente și înmulțirea 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 $(1, 1)(1, 0) = (2, 0)$ și $(1, 0)(1, 1) = (1, 1)$, 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 poziția $(2, 1)$. Atunci R este inel unitar (cu I_2 element unitate), are p^3 elemente și 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 și înmulțirea $(p, a) \cdot (m, b) = (pm, pb + ma + ab)$ pentru orice $p, m \in \mathbb{Z}$ și $a, b \in R$. Se verifică ușor că S este inel unitar cu elementul identitate la înmulțire $(1, 0)$. Aplicația $\phi : R \rightarrow S$, $\phi(r) = (0, r)$ 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 și înmulțirea $(\hat{p}, a) \cdot (\hat{m}, b) = (\hat{p}\hat{m}, pb + ma + ab)$ care este corect definită (se observă ușor că pentru $b \in R$ și $p, q \in \mathbb{Z}$ cu $\hat{p} = \hat{q}$ avem $p = q + ns$ pentru un $s \in \mathbb{Z}$ și cum $nb = 0$ rezultă $pb = qb$).

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

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

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

și $\bar{f}(1, 0) = 1_A$, 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 enunț. Aplicând proprietatea din enunț perechii (S, ϕ) și morfismului de inele $\phi' : R \rightarrow S'$ obținem un morfism unitar de inele $h : S \rightarrow S'$ cu $h\phi = \phi'$. Analog există un morfism unitar de inele $u : S' \rightarrow S$ cu $u\phi' = \phi$. Atunci $uh\phi = u\phi' = \phi$ și aplicând partea de unicitate din proprietatea lui (S, ϕ) pentru morfismul de inele $\phi : R \rightarrow S$ rezultă că $uh = Id_S$. Analog $hu = Id_{S'}$, deci S și 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 și k în \mathbb{Z} cu proprietatea că $ab + nk = 1 \Leftrightarrow (a, n) = 1$. Deci $|U(\mathbb{Z}_n)| = |\{a \in \mathbb{N}^* \mid a < n \text{ și } (a, n) = 1\}|$, iar cardinalul din membrul drept al acestei egalități 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 $c \in \mathbb{Z}$ și atunci $\hat{a}\hat{c} = 0$, deci \hat{a} este divizor al lui zero. Cealaltă implicație 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, \dots, 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 $i \in \{1, 2, \dots, r\}$, adică $p_i|a$ pentru orice $i \in \{1, 2, \dots, r\}$, 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 $\hat{a} = \widehat{p_1 \cdots p_r b} \Leftrightarrow n|a - p_1 \cdots p_r b \Rightarrow p_1 \cdots p_r|a$. Pentru fiecare $i \in \{1, 2, \dots, r\}$ 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 $i \in \{1, 2, \dots, r\}$ 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 $|N(\mathbb{Z}_n)| = |p_1 \cdots p_r \mathbb{Z}_n / n\mathbb{Z}| = n / p_1 \cdots p_r$.

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

9. Fie $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Vom arăta că există o bijecție între mulțimile $\text{Idemp}(\mathbb{Z}_n)$ și $\mathcal{P}(\{p_1, \dots, p_r\})$ și astfel va rezulta că $|\text{Idemp}(\mathbb{Z}_n)| = 2^r$. Se observă că $\hat{x} = \hat{x}^2 \Leftrightarrow n|x(x-1)$ și 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 $\{i_1, \dots, i_k\}$ este o submulțime a lui $\{1, \dots, r\}$ cu proprietatea că $p_i^{\alpha_i}|x \Leftrightarrow i \in \{i_1, \dots, i_k\}$, atunci vom defini $f : \text{Idemp}(\mathbb{Z}_n) \rightarrow \mathcal{P}(\{p_1, \dots, p_r\})$ prin $f(\hat{x}) = \{p_{i_1}, \dots, p_{i_k}\}$.

- f este bine definită: dacă $\hat{x}, \hat{y} \in \text{Idemp}(\mathbb{Z}_n)$ astfel încât $\hat{x} = \hat{y}$ rezultă $n|x-y$, deci $p_i|x-y$ pentru orice $1 \leq i \leq r$. Atunci pentru $j \in \{1, \dots, r\}$ avem că $p_j|x \Leftrightarrow p_j|x - (x-y) = y$, deci f este bine definită.

- f este injectivă: dacă $f(\hat{x}) = f(\hat{y}) = \{i_1, \dots, i_k\}$ avem că $p_{i_1}^{\alpha_{i_1}} \cdots p_{i_k}^{\alpha_{i_k}}|x$ și $p_{i_1}^{\alpha_{i_1}} \cdots p_{i_k}^{\alpha_{i_k}}|y$, deci $p_{i_1}^{\alpha_{i_1}} \cdots p_{i_k}^{\alpha_{i_k}}|x-y$. Dar $p_{j_1}^{\alpha_{j_1}} \cdots p_{j_l}^{\alpha_{j_l}}|x-1$ și $p_{j_1}^{\alpha_{j_1}} \cdots p_{j_l}^{\alpha_{j_l}}|y-1$, unde $\{j_1, \dots, j_l\} = \{1, \dots, r\} \setminus \{i_1, \dots, i_k\}$, de unde rezultă că $p_{j_1}^{\alpha_{j_1}} \cdots p_{j_l}^{\alpha_{j_l}}|(x-1) - (y-1) = x-y$. Așadar, $n|x-y$, deci $\hat{x} = \hat{y}$.

- f este surjectivă: fie $\{i_1, \dots, i_k\} \subseteq \{1, \dots, r\}$ și $\{j_1, \dots, j_l\} = \{1, \dots, r\} \setminus \{i_1, \dots, i_k\}$. 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 $x = p_{i_1}^{\alpha_{i_1}} \cdots p_{i_k}^{\alpha_{i_k}}x'$ și se obține că $n|x(x-1)$, de unde rezultă că $\hat{x} = \hat{x}^2$ și $f(\hat{x}) = \{p_{i_1}, \dots, p_{i_k}\}$.

Observăm că demonstrația faptului că f este surjectivă oferă un algoritm de a găsi idempotenții lui \mathbb{Z}_n . Vom determina în acest fel idempotenții lui \mathbb{Z}_{72} . Avem $72 = 2^3 3^2$, deci vom avea patru idempotenți, fiecare dintre ei fiind corespunzător unei submulțimi a mulțimii $\{2, 3\}$.

Mulțimii vide îi va corespunde $\hat{x} = \hat{1}$, deoarece în relația $1x' + 72y' = 1$ se poate lua $x' = 1, y' = 0$.

Pentru submulțimea $\{2\}$ avem $2^3x' + 3^2y' = 1$. Cum $x' = -1$ și $y' = 1$ este o soluție a ecuației precedente, obținem idempotentul $\hat{x} = \widehat{2^3x'} = \widehat{64}$.

Pentru submulțimea $\{3\}$ avem $3^2x' + 2^3y' = 1$ și idempotentul corespunzător este $\hat{x} = \hat{9}$.

În final, submulțimii $\{2, 3\}$ îi corespunde $\hat{x} = \hat{0}$.

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

injectivă deoarece $f(b) = f(c) \Rightarrow ab + a' - 1 = ac + a' - 1$, de unde $ab = ac$ și înmulțind la stânga cu a' rezultă că $b = c$. Pe de altă parte, $a' \notin \text{Im}(f)$, altfel ar rezulta că există $b \in R$ cu $ab = 1$ și s-ar contrazice faptul că a nu este inversabil la dreapta. Existența funcției $f : M \rightarrow M$ injectivă și nesurjectivă demonstrează că M este infinită (a se vedea problema 4 din Capitolul 1). Partea a doua este o consecință a primei părți, deoarece un element care are doi inverși la stânga nu este inversabil.

11. Fie R un inel unitar finit și $a \in R \setminus \{0\}$ un nondivizor al lui zero, adică a nu este divizor al lui zero nici la stânga și nici la dreapta. Definim $f : R \rightarrow R$ 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 mulțime finită rezultă că f este și surjectivă, deci este bijectivă. Rezultă că există $b \in R$ astfel încât $ba = 1$, deci a este inversabil la stânga. Analog se obține că a este inversabil la dreapta. Rezultă că a este inversabil.

Dacă R este inel integru finit, atunci mulțimea 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 $D = \{a_1, \dots, a_n\}$ mulțimea 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 raționează 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 mulțime infinită de elemente din R , fie acestea r_1, \dots, r_n, \dots , astfel încât $ar_1 = \dots = ar_n = \dots$. 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 și $\phi : R \rightarrow xR$ definită prin $\phi(a) = xa$. Avem că ϕ este morfism surjectiv de grupuri, deci $R/\text{Ker}(\phi) \simeq xR$, de unde obținem $|R| = |\text{Ker}(\phi)||xR|$. Cum mulțimile $\text{Ker}(\phi)$ și 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 raționa 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 și $1 - ab \in R(1 - ab)$, rezultă că $1 = ab + (1 - ab) \in R(1 - ab)$, deci $R(1 - ab) = R$.

și $1 - ab$ este inversabil la stânga.

Observăm că soluția permite și 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) Afirmația 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 înmulțire 1. Atunci aplicația $g : R \rightarrow R$ definită prin $g(r) = 1 - r$ este un izomorfism între monoizii (R, \circ) și (R, \cdot) . Într-adevăr, g este evident bijectivă, $g(0) = 1$ și 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 aplicația $g : S \rightarrow S$, $g(s) = 1 - s$ este un izomorfism de monoizi între (S, \circ) și (S, \cdot) , unde operația "o" a fost definită pe S prin aceeași formulă ca pe R .

Presupunem că $a, b \in R$ și 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 demonstrația problemei 13 rezultă că $1 - ab$ este inversabil la stânga în S și 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 obține $(1 - w) \circ (ab) = 0$, deci ab este quasi-regulat la stânga.

Afirmația similară la dreapta se demonstrează analog.

(iv) Fie $x \in R$ cu $x^n = 0$. Atunci pentru $a = -x - x^2 - \dots - x^{n-1}$ 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 și $b = (a-1)^{-1}a$ verifică relația $a + b = ab$.

(ii) \Rightarrow (i) Fie $r \in R \setminus \{0\}$. Atunci, pentru $a = 1 - r$, există $b \in R$ astfel încât $a + b = ab$. Obținem că $(1 - a)(1 - b) = 1$, deci r este inversabil la dreapta. Așadar, orice element nenul din R este inversabil la dreapta. Fie $r \in R \setminus \{0\}$ și $r', r'' \in R$ 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.

Echivalența (i) \Leftrightarrow (iii) se demonstrează similar.

16. Implicațiile (i) \Rightarrow (ii) și (i) \Rightarrow (iii) sunt clare.

(ii) \Rightarrow (i) $vu^2v = 1 \Rightarrow uvu^2v = u \Rightarrow u^2v = u$. Atunci $1 = vu^2v = vu$ și $1 = vu^2v = vuuv = uv$, deci u este inversabil și are inversul v .

(iii) \Rightarrow (i) $u(v + vu - 1)u = uvu + uvu^2 - u^2 = u + u^2 - u^2 = u$ și 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 $uv = 1$. Așadar u este inversabil și $u^{-1} = v$.

17. Demonstrăm mai întâi următorul rezultat:

Dacă $f : \mathbb{R} \rightarrow \mathbb{R}$ este o funcție care verifică relația $f(x + y) = f(x) + f(y)$ 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 $f(x_1 + \dots + x_n) = f(x_1) + \dots + f(x_n)$ pentru orice $n \in \mathbb{N}^*$, fapt care se obține imediat prin inducție. În particular, pentru $x_1 = \dots = x_n = 1$ 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 $x_1 = \dots = x_q = p/q$ se obține $f(p) = qf(p/q)$, de unde $f(p/q) = f(p)/q = ap/q$. Așadar $f(x) = ax$ pentru orice $x \in \mathbb{Q}$.

Din rezultatul de mai sus se obține că dacă $f : A \rightarrow A$, 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 $f : A \rightarrow A$ 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 $f : \mathbb{Z} \rightarrow \mathbb{Z}$, respectiv $f : \mathbb{Q} \rightarrow \mathbb{Q}$, și anume aplicația identică.

Fie acum un morfism de inele $f : \mathbb{R} \rightarrow \mathbb{R}$. 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 $f : \mathbb{R} \rightarrow \mathbb{R}$, şi anume morfismul identic.

18. (i) Notăm cu F mulţimea morfismelor de inele $f : \mathbb{Z} \rightarrow R$ şi definim $\phi : F \rightarrow \text{Idemp}(R)$ 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 $\psi : \text{Idemp}(R) \rightarrow F$ 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 $f : \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ un morfism de inele. Dacă $p : \mathbb{Z} \rightarrow \mathbb{Z}_m$ este proiecţia canonică, atunci $g = fp : \mathbb{Z} \rightarrow \mathbb{Z}_n$ 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 $\psi : \text{Idemp}(\mathbb{Z}_n) \cap \{e \in \mathbb{Z}_n \mid me = \hat{0}\} \rightarrow F$ prin $\psi(e) = f$, unde $f : \mathbb{Z}_m \rightarrow \mathbb{Z}_n, f(\bar{b}) = be$ 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 $f : \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ 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 $n \mid ma$. Notând $m' = m/d$ şi $n' = n/d$ se obţine că $n' \mid m'a$, deci $n' \mid a$. Aşadar avem de calculat $|\text{Idemp}(\mathbb{Z}_n) \cap \{\hat{a} \in \mathbb{Z}_n \mid n' \mid a\}|$. 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 $f : R \rightarrow S$ un monomorfism. Fie $A = \{(a, b) \mid a, b \in R \text{ și } f(a) = f(b)\}$ care este un inel unitar cu adunarea și înmulțirea pe componente. Aplicațiile $u, v : A \rightarrow R$ definite prin $u(a, b) = a$ și $v(a, b) = b$ sunt morfisme unitare de inele și avem că $fu = fv$. Cum f este monomorfism rezultă că $u = v$. Așadar, dacă $a, b \in R$ verifică $f(a) = f(b)$ atunci $(a, b) \in A$ și $a = u(a, b) = v(a, b) = b$. Prin urmare, f este injectivă.

(ii) Evident, un morfism surjectiv de inele este epimorfism de inele, fiind chiar epimorfism de mulțimi.

Reciproc, arătăm că morfismul de inele $f : \mathbb{Z} \rightarrow \mathbb{Q}$ definit prin $f(x) = x$, $x \in \mathbb{Z}$, este epimorfism, dar în mod clar nu este surjectiv. Fie $u, v : \mathbb{Q} \rightarrow R$ morfisme unitare de inele (R fiind un inel unitar) astfel încât $uf = vf$. Conform problemei 4 din Capitolul 2, f este epimorfism de monoizi și deci $u = v$. Rezultă că f este și 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

$$\begin{aligned} (e * f) * g &= (e + f - 2ef) * g \\ &= (e + f - 2ef) + g - 2(e + f - 2ef)g \\ &= e + f + g - 2ef - 2eg - 2fg + 4efg \end{aligned}$$

și

$$\begin{aligned} e * (f * g) &= e + (f + g - 2fg) - 2e(f + g - 2fg) \\ &= e + f + g - 2fg - 2ef - 2eg + 4efg, \end{aligned}$$

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 și obținem că există $n \in \mathbb{N}^*$ astfel încât $|\text{Idemp}(R)| = 2^n$.

21. (i) Avem $\phi_t(f + g) = (f + g)(t) = f(t) + g(t) = \phi_t(f) + \phi_t(g)$ și $\phi_t(fg) = (fg)(t) = f(t)g(t) = \phi_t(f)\phi_t(g)$. Elementul identitate la înmulțire în inelul C este $u : [0, 1] \rightarrow \mathbb{R}, u(t) = 1$ pentru orice $t \in [0, 1]$. Atunci $\phi_t(u) = u(t) = 1$. Rezultă că ϕ_t este morfism de inele.

(ii) Fie $\phi : C \rightarrow \mathbb{R}$ 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 $g_t \in C, \phi(g_t) = 0$ și $g_t(t) \neq 0$. 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 $[0, 1] \subseteq \bigcup_{t \in [0, 1]} V_t$ și cum $[0, 1]$

este compact, rezultă că există t_1, \dots, t_n astfel încât $[0, 1] \subseteq V_{t_1} \cup \dots \cup V_{t_n}$.

Atunci avem $\sum_{i=1}^n g_{t_i}^2(x) \neq 0$ pentru orice $x \in [0, 1]$, deoarece x aparține unui

V_{t_i} . Rezultă că $g = \sum_{i=1}^n g_{t_i}^2$ este inversabilă în C . Dar $\phi(g) = 0$, contradicție.

22. (i) Fie $x, y \in u^{-1}(J)$. Atunci $u(x)$ și $u(y)$ 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 injecția canonică $i : \mathbb{Z} \rightarrow \mathbb{Q}, i(x) = x$. 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 injecția canonică a lui \mathbb{Z} în \mathbb{Q} (vezi soluția punctului (ii)), constatăm că $(\mathbb{Z}^e)^c = \mathbb{Q} \neq \mathbb{Z}$.

(v) Fie $y \in (J^e)^c$. Atunci, conform (iii), există $b_1, \dots, b_n \in S$ și $x_1, \dots, x_n \in J^c$ astfel încât $y = \sum_{i=1}^n u(x_i)b_i$. Cum $x_1, \dots, x_n \in J^c, u(x_1), \dots, u(x_n) \in J$, prin urmare, $y \in J$.

Considerăm acum injecția canonică $j : \mathbb{Q} \rightarrow \mathbb{Q}[X], j(a) = a$. Dacă punem $J = (X)$, atunci $J^c = (0)$, deci $(J^e)^c = (0) \neq J$.

(vi) Conform punctului (v), $((I^e)^c)^c \subset I^e$. Pentru incluziunea contrară să

considerăm $y \in I^e$. Atunci există $n \in \mathbb{N}^*$, $b_1, \dots, b_n \in S$ și $x_1, \dots, x_n \in I$ astfel încât $y = \sum_{i=1}^n b_i u(x_i)$. Dar, conform punctului (iv), $I \subset (I^e)^c$, deci $x_1, \dots, x_n \in (I^e)^c$. Prin urmare, $y \in ((I^e)^c)^e$.

(vii) Conform punctului (iv) avem că $J^c \subset ((J^e)^e)^c$. Fie acum $x \in ((J^e)^e)^c$. Atunci $u(x) \in (J^e)^e$, deci există $n \in \mathbb{N}^*$, $b_1, \dots, b_n \in S$ și $x_1, \dots, x_n \in J^c$ astfel încât $u(x) = \sum_{i=1}^n b_i u(x_i)$. Cum însă $x_1, \dots, x_n \in J^c$ implică $u(x_1), \dots, u(x_n) \in J$, rezultă că $u(x) \in J$, deci $x \in J^c$.

23. (i) $\hat{x} \in I^e$ dacă și numai dacă există $\hat{a}_1, \dots, \hat{a}_n \in \bar{R}$ și $x_1, \dots, x_n \in I$ astfel încât $\hat{x} = \sum_{i=1}^n \hat{a}_i \pi(x_i)$ (vezi problema 22(iii)). Această relație se rescrie

$\hat{x} = \sum_{i=1}^n \hat{a}_i \hat{x}_i$, iar această expresie este în mod evident în $\bar{I} \bar{R}$.

(ii) Dacă $\hat{x} \in I^e$, atunci \hat{x} este de forma $\sum_{i=1}^n \hat{\alpha}_i \pi(a_i) = \sum_{i=1}^n \widehat{\alpha_i a_i}$ (vezi problema 22(iii)), unde $\alpha_i \in R$, $a_i \in I$, pentru orice $i \in \{1, 2, 3, \dots, n\}$. Cum $\alpha_i a_i \in I$ pentru orice $i \in \{1, 2, 3, \dots, n\}$ și $I \subset I + J$, avem $\hat{x} \in (I + J)/J$.

Reciproc, fie $\hat{x} \in (I + J)/J$. Atunci există $a \in I$ și $b \in J$ astfel încât $\hat{x} = \widehat{a + b} = \hat{a} + \hat{b}$. Cum $b \in J$, avem $\hat{b} = \hat{0}$, deci $\hat{x} = \hat{a} \in \bar{I} \subset I^e$.

(iii) Folosind (i) și (ii),

$$\bar{R}/\bar{I} \bar{R} = \bar{R}/I^e = \frac{R/J}{(I + J)/J}.$$

Aplicând teorema a III-a de izomorfism pentru inele obținem

$$\bar{R}/\bar{I} \bar{R} = \frac{R/J}{(I + J)/J} \simeq R/(I + J).$$

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 obține $I \neq (a_1, \dots, a_n)$, atunci am obține șirul crescător de ideale $(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3) \subsetneq \dots$ care nu este staționar, contradicție. Rămâne că există $n \in \mathbb{N}^*$ așa încât $I = (a_1, \dots, a_n)$. Prin urmare, I este finit generat.

Reciproc, fie un şir crescător $I_1 \subseteq I_2 \subseteq \dots$ 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 $I = (a_1, \dots, a_r)$. Există atunci n_1, \dots, n_r aşa încât $a_j \in I_{n_j}$. Dacă $n = \max\{n_1, \dots, n_r\}$, atunci $I = (a_1, \dots, a_r) \subseteq I_n \subseteq I_{n+1} \subseteq \dots \subseteq I$, de unde $I_n = I_{n+1} = \dots$ 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 $P : a = (c_1, \dots, c_m)$ şi $P + (a) = (d_1, \dots, d_n)$. 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 $\lambda_1, \dots, \lambda_n \in R$ 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 $\mu_1, \dots, \mu_m \in R$ 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 $\{u_1, \dots, u_n, ac_1, \dots, ac_m\}$, 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 $\pi : R \rightarrow R/I$, $\pi(x) = \hat{x}$

proiecția 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, \dots, x_n un sistem de generatori al lui $\pi^{-1}(J)$. Să observăm că $\widehat{x}_1, \dots, \widehat{x}_n \in J$, deci idealul generat de aceste elemente, pe care îl vom nota $(\widehat{x}_1, \dots, \widehat{x}_n)$, este inclus în J . Fie acum $\widehat{x} \in J$. Atunci, $x \in \pi^{-1}(J)$, deci există $a_1, \dots, a_n \in R$ astfel încât $x = a_1x_1 + \dots + a_nx_n$. De aici rezultă că $\widehat{x} = \widehat{a}_1\widehat{x}_1 + \dots + \widehat{a}_n\widehat{x}_n$. Prin urmare, $J \subseteq (\widehat{x}_1, \dots, \widehat{x}_n)$. Rezultă că $J = (\widehat{x}_1, \dots, \widehat{x}_n)$, deci J este ideal finit generat al lui \overline{R} . În concluzie, \overline{R} este inel noetherian.

25. Se ține seama de corespondența bijectivă dintre idealele lui R/I , unde R este un inel comutativ unitar și I este un ideal al său, și idealele lui R care conțin pe I , precum și de corespondențele bijective induse între mulțimea idealelor prime (respectiv maximale) ale lui R/I și mulțimea idealelor prime (respectiv maximale) ale lui R care conțin pe I .

Fie $R = \mathbb{Z}_n$, unde $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ cu p_1, \dots, p_r numere prime diferite și $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$. Idealele lui \mathbb{Z}_n sunt de forma $m\mathbb{Z}/n\mathbb{Z}$, unde m este un divisor 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 și idealele maximale coincid, rezultă că idealele prime și idealele maximale din \mathbb{Z}_n coincid și sunt de forma $p_i\mathbb{Z}/n\mathbb{Z}$, cu $i = 1, \dots, r$, deci sunt în număr de r .

26. (i) Fie $p_i : R \rightarrow R_i$ proiecția lui R pe componenta de pe poziția i , pentru orice $i = 1, \dots, n$. 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 $\alpha = (a_1, \dots, a_n) \in I_1 \times \cdots \times I_n$. Cum $a_i \in I_i$, rezultă că există $\beta_i \in I$ care are pe poziția i chiar pe a_i . Notând cu e_i elementul lui R care are 1 pe poziția i și 0 în rest, se obține că $e_i\beta_i \in I$ este elementul care are a_i pe poziția i și 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 mulțime de această formă este ideal al lui R .

(ii) Notăm cu $\pi_i : R_i \rightarrow R_i/I_i$ proiecția canonică. Definim $f : R \rightarrow R_1/I_1 \times \cdots \times R_n/I_n$ prin $f(r_1, \dots, r_n) = (\pi_1(r_1), \dots, \pi_n(r_n))$. Evident f este morfism surjectiv de inele și $\text{Ker}(f) = I_1 \times \cdots \times I_n$. Aplicând teorema fundamentală de izomorfism se obține izomorfismul cerut.

(iii) Fie $R = \prod_{j \in J} R_j$ un produs direct de inele unitare, unde J este o mulțime infinită. Fie I mulțimea 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 poziția j și 0 pe toate celelalte poziții, acesta este în I , având suport finit, și atunci ar rezulta că $1 \in I_j$, adică $I_j = R_j$. Obținem $I = \prod_{j \in J} R_j = R$, ceea ce este o contradicție, deoarece R conține elemente de suport infinit.

27. (i) Fie $n, m \in \mathbb{N}^*$ astfel încât $I^n = 0$ și $J^m = 0$. Arătăm că $(I + J)^{n+m} = 0$. Într-adevăr, dacă $x_1, \dots, x_{n+m} \in I$ și $y_1, \dots, y_{n+m} \in J$ 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 și că I este generat de elementele x_1, \dots, x_p . Fie $n \in \mathbb{N}$ astfel încât $x_i^n = 0$ pentru orice $i = 1, \dots, p$. Dacă $r \in I$, atunci există $r_1, \dots, r_p \in R$ cu $r = r_1 x_1 + \dots + r_p x_p$. Atunci r^{np} este o sumă de produse de câte np factori de forma $r_i x_i$, deci în fiecare astfel de factor apare cel puțin un x_i la puterea n . Rezultă că orice astfel de produs este 0, deci $r^{np} = 0$.

Dacă I nu este finit generat afirmația 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 poziție au clasa unui multiplu de $p \pmod{p^n}$, nu este nilpotent, dar orice element este nilpotent (explicația este că indicii de nilpotență ai elementelor din I pot fi oricât de mari).

28. Notând cu p_1, \dots, p_n proiecțiile canonice ale lui R pe $R/I_1, \dots, R/I_n$ respectiv, morfismul ϕ se poate descrie prin $\phi(r) = (p_1(r), \dots, p_n(r))$.

(i) Evident $\text{Ker}(\phi) = \bigcap_{i=1}^n \text{Ker}(p_i) = I_1 \cap \dots \cap I_n$.

(ii) Presupunem că ϕ este surjectivă. Fie $j, k \in \{1, \dots, n\}, j \neq k$. Pentru elementul $\alpha \in R/I_1 \times \dots \times R/I_n$ care are $p_j(1)$ pe poziția j și $p_k(0)$ pe poziția k există $r \in R$ astfel încât $\phi(r) = \alpha$, deci $p_j(r) = p_j(1)$ și $p_k(r) = p_k(0)$. Rezultă că $r - 1 \in I_j$ și $r \in I_k$, de unde obținem că $1 = r + (1 - r) \in I_k + I_j$, deci I_k și 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 $(p_1(0), \dots, p_i(1), \dots, p_n(0)) \in \text{Im}(\phi)$ pentru orice $i = 1, \dots, n$.

Ținând cont de faptul că pentru $j \neq i$ avem $I_i + I_j = R$, putem găsi $a_j \in I_i$ și $b_j \in I_j$ 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 $j \neq i$ și $1 - r \in I_i$, deci $\phi(r) = (p_1(0), \dots, p_i(1), \dots, p_n(0))$.
 (iii) Afirmatia rezultă din (i), (ii) și 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 conținut într-un ideal maximal, adică $Ra \subseteq M$. Rezultă că $R \setminus U(R) \subseteq M$ și 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 și $a + b \in R \setminus U(R)$, contradicție. 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 și $a + b \in R \setminus U(R)$. Fie $a \in R \setminus U(R)$ și $r \in R$. Dacă $ar \in U(R)$ rezultă $a, r \in U(R)$, contradicție. Așadar $ar \in R \setminus U(R)$.

Este evident că $R \setminus U(R)$ este ideal maximal și că orice ideal propriu este conținut în $R \setminus U(R)$, deci acesta este unicul ideal maximal.

30. Fie R un inel local și e un idempotent în R . Din $e + (1 - e) = 1$ rezultă $e \in U(R)$ sau $1 - e \in U(R)$. Dar $e(1 - e) = 0$ și unul dintre ele este inversabil, deci $e = 0$ sau $1 - e = 0$. Așadar $e = 0$ 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 idempotenții 0 și 1. Dacă prin absurd n nu ar fi putere a unui număr prim, atunci ar exista $a, b \in R \setminus \{0, 1\}$ cu $n = ab$ și $(a, b) = 1$. Fie $c, d \in \mathbb{Z}$ cu $ca + db = 1$ și $e = \hat{c}\hat{a} \in \mathbb{Z}_n$. 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 $b|c$ și cum $ca + db = 1$ rezultă $b = 1$, contradicție. Analog, dacă $e = \hat{1}$ rezultă $\hat{d}\hat{b} = \hat{0}$ și apoi $a = 1$. Rezultă că n este putere a unui număr prim.

Observație. Putem da acum o altă demonstrație problemei 9 observând că dacă $R = R_1 \times \dots \times R_r$ este un produs direct de inele, atunci idempotenții lui R sunt elementele de forma (e_1, \dots, e_r) , unde fiecare e_i este idempotent în R_i . Fie $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Idealele $I_i = p_i^{\alpha_i} \mathbb{Z}$ sunt oricare două comaximale în \mathbb{Z} , iar $I_1 \cap \dots \cap I_r = n\mathbb{Z}$. Folosind problema 28 obținem $\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{\alpha_1}} \times \dots \times \mathbb{Z}_{p_r^{\alpha_r}}$. Fiecare dintre componentele acestui produs de inele este inel local, deci are

doar doi idempotenți. Rezultă că \mathbb{Z}_n are 2^r idempotenți.

32. (i) Dacă $ab \in U(R)$, nu rezultă neapărat că $a, b \in U(R)$. De exemplu, fie V un spațiu vectorial (peste un corp arbitrar) având o bază numărabilă $(e_n)_{n \geq 1}$ și fie $R = \text{End}_K(V)$ cu structura de inel dată de adunarea obișnuită a morfismelor de spații vectoriale și compunerea morfismelor. Este imediat că R devine inel cu aceste operații. 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 $n \geq 2$ și $g(e_1) = 0$. Evident f nu este surjectivă iar g nu este injectivă, deci nu aparțin lui $U(R)$ care este format din toate automorfismele lui V . Pe de altă parte, $g \circ f$ este aplicația identică pe V , deci $g \circ f \in U(R)$.

(ii) Fie $a^n r = r a^n = 1$. Atunci $a(a^{n-1}r) = (ra^{n-1})a = 1$, deci a este inversabil la stânga și la dreapta, de unde rezultă că a este inversabil.

(iii) Fie $ra = 1$ cu $r \in R$. Atunci $ara = a$, deci $(ar - 1)a = 0$ și cum a nu este divizor al lui zero la dreapta rezultă $ar - 1 = 0$. Se obține $ar = 1$ și 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} și 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 și înmulțirea 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 obține $ae = a$ pentru orice $a \in R$, adică e este element identitate și 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 și $rs \in C_R(A)$. 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 $x \in X$ și $r \in C_R(X)$ avem $xr = rx$, deci $x \in C_R(C_R(X))$. Aplicând ultima relație pentru $X = C_R(A)$ rezultă $C_R(A) \subseteq C_R(C_R(C_R(A)))$. De asemenea $A \subseteq C_R(C_R(A))$ și aplicând prima observație rezultă că $C_R(A) \supseteq C_R(C_R(C_R(A)))$, de unde se obține 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 obține că a este inversabil la stânga și la dreapta, deci este inversabil. Mai mult, deoarece $a \in Z(R)$ rezultă că și $a^{-1} \in Z(R)$, 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 relația $x(xy) - (xy)x = x(xy - yx)$ și cum $xy - yx$ este nenul, el este inversabil și $x = [x(xy) - (xy)x](xy - yx)^{-1}$. Fie $C_R(y) = \{r \in R \mid ry = yr\}$. Cum y comută cu toți comutatorii aditivi obținem că $x(xy) - (xy)x, xy - yx \in C_R(y)$, de unde $(xy - yx)^{-1} \in C_R(y)$ și deci $x \in C_R(y)$, contradicție.

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 relațiile $\delta_a^2(b) = a^2b - 2aba + ba^2 \in K$ și $\delta_{a^2}(b) = a^2b - ba^2 \in K$ se obține prin adunare că $2(a^2b - aba) = 2a\delta_a(b) \in K$. Dacă $\delta_a(b) \neq 0$ rezultă $2\delta_a(b) \in K^*$ și se obține $a \in K$, contradicție. Deci $\delta_a(b) = 0$, adică b comută cu elementele din $D \setminus K$.

Fie acum $c \in K^*$. Atunci a și ac se găsesc în $D \setminus K$, deci din cele de mai sus ele comută cu b . Obținem $(ac)b = b(ac) = (ba)c = abc$ și înmulțind cu a^{-1} rezultă că $cb = bc$, deci b comută și cu elementele din K . Rezultă $b \in Z(D)$, deci $K \subseteq Z(D)$.

39. Fie $c \in D$ un element care comută cu toți 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 $a^{-1}cac^{-1}$ și cu $b^{-1}cbc^{-1}$, de unde, folosind ultima relație, rezultă că c comută și cu a , contradicție.

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 $a(a^{-1}ca - b^{-1}cb) = ca - ab^{-1}cb = c(b+1) - (b+1)b^{-1}cb = c - b^{-1}cb \neq 0$ și cum $a^{-1}ca, b^{-1}cb \in K^*$ rezultă că și $a \in K^*$, ceea ce este o contradicție. 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 și 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 $a^n = 0$. Obținem

$$\begin{aligned}
0 &= (x^2 - x)^n \\
&= \sum_{k=0}^n (-1)^k C_n^k x^{2k} x^{n-k} \\
&= \sum_{k=0}^n (-1)^k C_n^k x^{n+k} \\
&= x^n - x^{n+1} \sum_{k=1}^n (-1)^{k-1} C_n^k x^{k-1}.
\end{aligned}$$

Notând $t = \sum_{k=1}^n (-1)^{k-1} C_n^k x^{k-1}$, avem că $x^n = x^{n+1}t$ și $xt = tx$. Fie $e = x^n t^n$.

Arătăm că e este idempotent și că $f = \hat{e}$. Avem $e = x^n t^n = (x^{n+1}t)t^n = x^{n+1}t^{n+1} = (x^{n+2}t)t^{n+1} = x^{n+2}t^{n+2} = \dots = x^{2n}t^{2n} = (x^n t^n)^2 = e^2$. De asemenea, $\hat{e} = (\hat{x}\hat{t})^n$ și cum $\hat{x} = \widehat{x^{n+1}}$ se obține $\hat{x}\hat{t} = \widehat{x^{n+1}}\hat{t} = \widehat{x^{n+1}t} = \widehat{x^n}$,

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 $x^2 - x = a_1e_1 + \dots + a_ne_n$ cu $a_i \in R$ și $e_i \in P, e_i^2 = e_i$ pentru orice $1 \leq i \leq n$. Avem $(1 - e_1) \dots (1 - e_n)(x^2 - x) = 0$, deoarece pentru fiecare $i = 1, \dots, n$, termenul a_ie_i este anulat de $1 - e_i$. Acum o inducție simplă după n ne conduce la concluzia că $(1 - e_1) \dots (1 - e_n) = 1 - e$ 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 ușor 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 $P \in \text{Spec}(R)$. Există $M \in \text{Max}(R)$ astfel încât $P \subseteq M$. Dacă $P \neq M$ atunci există $x \in M \setminus P$. Dar $x^2 = x \Rightarrow x(1 - x) = 0 \in P \Rightarrow 1 - x \in P \Rightarrow 1 - x \in M \Rightarrow 1 \in M$, contradicție. Deci $P = M \in \text{Max}(R)$.

(iii) Pentru o mulțime X se verifică prin calcul că mulțimea părților sale $\mathcal{P}(X)$ are o structură de inel în raport cu diferența simetrică $A \Delta B = (A \setminus B) \cup (B \setminus A)$ (care joacă rolul adunării în $\mathcal{P}(X)$) și intersecția mulțimilor (care joacă rolul înmulțirii în $\mathcal{P}(X)$). Elementul nul al acestui inel este mulțimea 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 și $2x = 0$ 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 inducție după n că există elementele $a_1, \dots, a_n \in R \setminus \{0, 1\}$ cu proprietatea că $a_ia_j = 0$ pentru orice $i \neq j$.

Pentru $n = 2$ există $e \in R \setminus \{0, 1\}$ și alegem $a_1 = e, a_2 = 1 - e$. Pentru $n > 2$ se consideră $e \in R \setminus \{0, 1\}$ și se scrie $R = Re + R(1 - e)$. Re și $R(1 - e)$ 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 $|Re| = 2^r$ și $|R(1 - e)| = 2^s$ cu $r + s = n$, iar din ipoteza de inducție rezultă că există $b_1, \dots, b_r \in Re$ astfel încât $b_ib_j = 0$ pen-

tru orice $i \neq j$ și $c_1, \dots, c_s \in R(1-e)$ astfel încât $c_k c_l = 0$ pentru orice $k \neq l$. Fie acum $a_1 = b_1, \dots, a_r = b_r, a_{r+1} = c_1, \dots, a_n = c_n$ și cum $e(1-e) = 0$ vom avea $a_i a_j = 0$ pentru orice $i \neq j$.

Arătăm acum că mulțimea tuturor sumelor $a_{i_1} + \dots + a_{i_k}$, cu $1 \leq i_1 < \dots < i_k \leq n$, are 2^n elemente, deci coincide cu R , de unde rezultă că pentru orice $x \in R$ există și sunt unice $1 \leq i_1 < \dots < i_s \leq n$ cu proprietatea că $x = a_{i_1} + \dots + a_{i_s}$. Este suficient să arătăm că dacă avem $1 \leq j_1 < \dots < j_s \leq n$ și $1 \leq k_1 < \dots < k_t \leq n$, atunci $a_{j_1} + \dots + a_{j_s} = a_{k_1} + \dots + a_{k_t} \Leftrightarrow s = t$ și $j_1 = k_1, \dots, j_s = k_s$. Aceasta se demonstrează arătând că $j_1, \dots, j_s \in \{k_1, \dots, k_t\}$ și $k_1, \dots, k_t \in \{j_1, \dots, j_s\}$. Dacă, de exemplu, $j_1 \notin \{k_1, \dots, k_t\}$, atunci din $a_{j_1}(a_{j_1} + \dots + a_{j_s}) = a_{j_1}(a_{k_1} + \dots + a_{k_t})$ rezultă că $a_{j_1}^2 + \dots + a_{j_1} a_{j_s} = a_{j_1} a_{k_1} + \dots + a_{j_1} a_{k_t} \Rightarrow a_{j_1} = 0$, contradicție.

Va fi suficient să considerăm acum aplicația $f : R \rightarrow (\mathcal{P}(\{1, \dots, n\}), \Delta, \cap)$ definită prin $f(x) = \{i_1, \dots, i_s\}$, unde $x = a_{i_1} + \dots + a_{i_s}$, care este izomorfism. (v) Fie $\mathcal{P}_f(X)$ mulțimea părților finite ale lui X și $\mathcal{P}_{cf}(X)$ mulțimea părților lui X care au complementara finită. Este ușor 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 aplicația care duce o mulțime în complementara ei definește o bijecție între $\mathcal{P}_f(X)$ și $\mathcal{P}_{cf}(X)$, 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 bijecție între $\mathcal{P}_f(X) \cup \mathcal{P}_{cf}(X)$ și X . Transportând structura de inel Boole a lui $\mathcal{P}_f(X) \cup \mathcal{P}_{cf}(X)$ prin această bijecție, obținem 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 $S = \{1, x, x^2, x^3, \dots\}$ și

$$\mathcal{F} = \{I \mid I \text{ ideal în } R \text{ și } I \cap S = \emptyset\}.$$

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 $ab \in J$ și $a \notin J, b \notin J \Rightarrow J \subset J+(a)$ și $J \subset J+(b) \Rightarrow (J+(a)) \cap S \neq \emptyset$ și $(J+(b)) \cap S \neq \emptyset \Rightarrow$ există $m, n \in \mathbb{N}$ astfel încât $x^m \in J+(a)$ și $x^n \in J+(b)$

$\Rightarrow x^{m+n} \in (J+(a))(J+(b)) \subseteq J \Rightarrow x^{m+n} \in J \cap S \Rightarrow J \cap S \neq \emptyset$, contradicție. 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 $P \in \text{Spec}(R)$ 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, contradicție.

(iii) Fie $x \in J(R)$ și $a \in R$. Dacă $1 - ax \notin U(R)$ atunci există $M \in \text{Max}(R)$ astfel încât $1 - ax \in M$. Dar $x \in J(R) \Rightarrow x \in M \Rightarrow ax \in M$ și cum $1 - ax \in M$ rezultă $1 \in M$, contradicție. Reciproc, fie $x \in R$ și $1 - ax \in U(R)$ pentru orice $a \in R$ și fie $M \in \text{Max}(R)$. 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 $\text{Spec}(R) \neq \text{Max}(R)$ (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 și numai dacă are un singur termen nenul și acela este inel integru.

(i) " \Rightarrow " Fie P ideal prim al lui R . Rezultă că există $I_1 \leq R_1, \dots, I_n \leq R_n$ astfel încât $P = I_1 \times \dots \times I_n$. Cum P este ideal prim, R/P este integru, prin urmare $R_1/I_1 \times \dots \times R_n/I_n$ este inel integru, deci există un unic $1 \leq i \leq n$ astfel încât $R_i/I_i \neq 0$ și acesta este inel integru. Rezultă $I_j = R_j$ pentru orice $j \neq i$ și I_i este ideal prim în R_i .

" \Leftarrow " Dacă $P = R_1 \times \dots \times R_{i-1} \times P_i \times R_{i+1} \times \dots \times R_n$, 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) și (ii).

46. Idealele lui \mathbb{Z}_{20} sunt $(0), \hat{2}\mathbb{Z}_{20}, \hat{4}\mathbb{Z}_{20}, \hat{5}\mathbb{Z}_{20}, \hat{10}\mathbb{Z}_{20}, \mathbb{Z}_{20}$. Cum \mathbb{Q} și \mathbb{Z}_{19} sunt corpuri, ele au ca ideale doar pe (0) și pe ele însele. Deci R va avea 24 de ideale formate din produsele directe ale idealelor de mai sus. Cum $\text{Spec}(\mathbb{Z}_{20}) = \text{Max}(\mathbb{Z}_{20}) = \{\hat{2}\mathbb{Z}_{20}, \hat{5}\mathbb{Z}_{20}\}$ rezultă că $\text{Spec}(R) = \text{Max}(R) = \{\hat{2}\mathbb{Z}_{20} \times \mathbb{Q} \times \mathbb{Z}_{19}, \hat{5}\mathbb{Z}_{20} \times \mathbb{Q} \times \mathbb{Z}_{19}, \mathbb{Z}_{20} \times (0) \times \mathbb{Z}_{19}, \mathbb{Z}_{20} \times \mathbb{Q} \times (0)\}$. 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 și unul dintre inelele $\mathbb{Q}, \mathbb{Z}_{19}, \mathbb{Q} \times \mathbb{Z}_{19}$.

$J(R) = N(R) = N(\mathbb{Z}_{20}) \times N(\mathbb{Q}) \times N(\mathbb{Z}_{19}) = \hat{10}\mathbb{Z}_{20} \times (0) \times (0)$ și $\text{Idemp}(R) =$

$$\text{Idemp}(\mathbb{Z}_{20}) \times \text{Idemp}(\mathbb{Q}) \times \text{Idemp}(\mathbb{Z}_{19}) = \{\hat{0}, \hat{1}, \hat{5}, \hat{16}\} \times \{0, 1\} \times \{\hat{0}, \hat{1}\}.$$

47. (i) Fie $a, b \in \text{Rad}(I)$. Atunci există $m, n \in \mathbb{N}^*$ cu $a^m \in I$ și $b^n \in I$. Atunci $(a+b)^{m+n} = \sum_{0 \leq i \leq m+n} C_{m+n}^i a^{m+n-i} b^i$ și cum pentru orice $0 \leq i \leq m+n$

avem $i \geq n$ sau $m+n-i \geq m$, rezultă că toți 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 $a^m \in I$, și $r \in R$, 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 definiție 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 $N(R/I) = \bigcap \{P/I \mid P \in \text{Spec}(R), I \subseteq P\}$. Așadar, $\text{Rad}(I)/I = N(R/I) = (\bigcap \{P \mid P \in \text{Spec}(R), I \subseteq P\})/I$, de unde obținem că $\text{Rad}(I) = \bigcap \{P \mid P \in \text{Spec}(R), I \subseteq P\}$.

(iv) Este clar din definiție că dacă $I_1 \subseteq I_2$, atunci $\text{Rad}(I_1) \subseteq \text{Rad}(I_2)$.

Cum $I \subseteq \text{Rad}(I)$, obținem 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 $a^m \in I$ și $a^n \in J$. 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 $u \in \text{Rad}(I)$ și $v \in \text{Rad}(J)$ cu $a^n = u + v$. Fie $m, p > 0$ cu $u^m \in I$ și $v^p \in J$. Atunci

$$a^{n(m+p)} = (u+v)^{m+p} = \sum_{0 \leq i \leq m+p} C_{m+p}^i u^{m+p-i} v^i, \text{ și cum pentru orice } 0 \leq i \leq$$

$m+p$ 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 intersecția tuturor idealelor maximale $J(R) \neq 0$, deoarece idealele maximale ale lui R sunt nenule (pentru că R nu este corp) și produsul acestora (care este conținut în $J(R)$)

este nenul pentru că R este inel integru.

Fie acum $x \in J(R)$, $x \neq 0$ și definim $f : R \rightarrow U(R)$ 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 $|R| \leq |U(R)| \Rightarrow |R| \leq \infty$, contradicție.

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 enunț atunci I este ideal al lui R .

(ii) Fie $P \in \text{Spec}(R)$. 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 $a, b \in \mathbb{N} \setminus \{0, 1\}$, și 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 $m|r - kx$, și cum $k|m$ se obține $k|r$, deci $r = 1$, contradicție. În același mod se obține o contradicție în cazul în care $\widehat{ds} \in P$. Deci k este număr prim.

Să presupunem acum $k|d \Rightarrow d = kt$ pentru un $t \in \mathbb{Z} \Rightarrow \widehat{d^2} = \widehat{dkt} \in P \Rightarrow \widehat{d} \in P \Rightarrow$ există $y \in \mathbb{Z}$ astfel încât $\widehat{d} = \widehat{kdy} \Rightarrow n|d - kdy \Rightarrow m|1 - ky$, și 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, $p|m$ și 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 $\hat{a} = \widehat{dx}$, $\hat{b} = \widehat{dy}$ și $\widehat{d^2xy} = \widehat{pdz}$. Obținem $n|d^2xy - pdz$, deci $m|dxy - pz$, și 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 $M \in \text{Max}(R)$. 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 $M \subset rd\mathbb{Z}/n\mathbb{Z} \subset d\mathbb{Z}/n\mathbb{Z} = R$, contradicție.

Reciproc, să considerăm $M = pd\mathbb{Z}/n\mathbb{Z}$, cu p număr prim și $p|m$. Fie $I \leq R, I \neq R$ astfel încât $M \subseteq I$; rezultă că există $k \in \mathbb{N} \setminus \{0, 1\}$ astfel încât $I = kd\mathbb{Z}/n\mathbb{Z}$ și $pd\mathbb{Z} \subseteq kd\mathbb{Z} \Rightarrow k|p \Rightarrow k = p \Rightarrow I = M$. Deci $M \in \text{Max}(R)$.

50. Se rezolvă asemănător cu problema 49.

51. Fie $R = (\mathbb{Q}, +, *)$, unde multiplicarea se definește astfel: $x * y = 0$ pentru orice $x, y \in \mathbb{Q}$. Se obține astfel un inel neunitar. Idealele lui R coincid cu subgrupurile lui $(\mathbb{Q}, +)$ și cum acest grup nu are subgrupuri maximale (a se vedea problema 37 din Capitolul 3), rezultă că inelul R nu are ideale maximale.

Observație. În problema 30 din Capitolul 5 vom da un exemplu de astfel de inel care va fi chiar integru.

52. Notăm $A = A_1 \times \cdots \times A_m$ și $B = B_1 \times \cdots \times B_n$. Să observăm că $x = (x_1, \dots, x_m) \in \text{Idemp}(A) \Leftrightarrow x_i \in \text{Idemp}(A_i)$ pentru orice $i = 1, \dots, m$ $\Leftrightarrow x_i = 0$ sau $x_i = 1$ pentru orice $i = 1, \dots, m$.

Presupunem $A \simeq B$. Atunci $|\text{Idemp}(A)| = |\text{Idemp}(B)| \Rightarrow 2^m = 2^n \Rightarrow m = n$.

Fie acum $f : A \rightarrow B$ izomorfism de inele. Pentru fiecare $i = 1, \dots, n$ fie $e_i \in A$ (respectiv $f_i \in B$) elementul care are 1 (elementul unitate al inelului A_i , respectiv B_i) pe poziția i și 0 în rest. Observăm că $e_i \in \text{Idemp}(A)$ și $e_i e_j = 0$ pentru orice $i \neq j$. Rezultă că $f(e_i) \in \text{Idemp}(B) \setminus \{0\}$ și $f(e_i)f(e_j) = 0$ 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 $x = (x_1, \dots, x_n)$, 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 $i = 1, \dots, n$.

Rezultă $|\bigcup_{i=1}^n \text{supp}(f(e_i))| = \sum_{i=1}^n |\text{supp}(f(e_i))| \geq n$. Dar $\bigcup_{i=1}^n \text{supp}(f(e_i)) \subseteq$

$\{1, \dots, n\}$ implică $|\bigcup_{i=1}^n \text{supp}(f(e_i))| \leq n$. Deci $|\text{supp}(f(e_i))| = 1$ pentru orice

$i = 1, \dots, n$. Rezultă că există $\sigma \in S_n$ astfel încât $f(e_i) = f_{\sigma(i)}$ pentru orice $i = 1, \dots, n$. Dar $e_i A \simeq A_i$ iar $f_{\sigma(i)} B \simeq B_{\sigma(i)}$ și cum $f(e_i A) = f_{\sigma(i)} B$ rezultă că $A_i \simeq B_{\sigma(i)}$ pentru orice $i = 1, \dots, n$.

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 puțin în număr de $n + 1$, există două astfel de elemente care se află în aceeași 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 obține $1 + \alpha x \in k^* x$, de unde rezultă $1 \in k^* x$, deci $x \in k^*$,

contradicție.

54. Presupunem $K = K_1 \cup \dots \cup K_n$, unde K_1, \dots, 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 $K^* = \langle x \rangle$, 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 $x \in K_1 \setminus \bigcup_{i \neq 1} K_i$

și $y \in K_2 \setminus \bigcup_{i \neq 2} K_i$ arbitrar fixate, mulțimea $\{x + ay \mid a \in \bigcap_{i=1}^n K_i, a \neq 0\} \subseteq K$

are cel puțin n elemente, deci există $1 \leq i \leq n$ și $a, b \in \bigcap_{i=1}^n K_i, a \neq b$, 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 obținem $x \in K_2$, contradicție cu alegerea lui x . Așadar, $|\bigcap_{i=1}^n K_i| \leq n$.

Pe de altă parte, vom arăta că $|\bigcap_{i=1}^n K_i| = \infty$. Deoarece K este infinit, cel puțin unul dintre corpurile K_1, \dots, K_n este infinit, să presupunem (printr-o eventuală renumerotare) că corpul K_1 este infinit. Fie șirul $(a_n)_{n \geq 1} \subseteq K_1$ și 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 conține o infinitate de termeni ai șirului $(\alpha + a_n)_{n \geq 1}$.

Să presupunem $i = 2$, deci K_2 are această proprietate. Deci există un subșir $(a_{n_k})_{k \geq 1}$ al șirului $(a_n)_{n \geq 1}$ 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 șir $(b_n)_{n \geq 1}$ 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 conține o infinitate de termeni ai șirului $(\beta + b_n)_{n \geq 1}$. Să presupunem că $i = 3$, deci K_3 are această proprietate. Obținem acum un șir $(c_n)_{n \geq 1}$ 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 șir care are toți termenii în $K_1 \cap \dots \cap K_n$, deci $|K_1 \cap \dots \cap K_n| = \infty$.

Astfel am obținut o contradicție.

55. Să presupunem, prin absurd, că pentru orice $x, y \in K$ există $a \in K$

astfel încât $x^2 + y^2 = a^2$ și 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 $n \in \mathbb{N}^*$ și $x \in K^*$ cu proprietatea că $|K| = 3^n$ și $K^* = \langle x \rangle$. 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 aplicația $\phi : K \rightarrow K, \phi(x) = x^2$ 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 $|K^*| = 2|L^*|$ și cum L este și el corp finit de caracteristică 3, există $r \in \mathbb{N}^*$ astfel încât $|L| = 3^r$, deci $|L^*| = 3^r - 1$. Obținem că $3^n - 1 = 2(3^r - 1)$, de unde $3^n + 1 = 2 \cdot 3^r$, deci $3 \mid 3^n + 1$, contradicție.

Capitolul 11

Soluții: Construcții de inele: inele de matrice, inele de polinoame, inele de serii formale și inele de fracții

1. Dacă $n = 1$ și 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 $A, B \in M_n(R)$ și 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 condiția (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 $BA = 0$ și

$$AB = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & . \\ ab & 0 & \dots & 0 \end{pmatrix}.$$

Deoarece $AB = BA$, este necesar ca $ab = 0$, deci condiția (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 și numai dacă au loc relațiile

$$a^2 + bc = a, \quad b(a + d) = b, \quad c(a + d) = c, \quad d^2 + bc = d.$$

Dacă $a + d \neq 1$, rezultă că $b = c = 0$ și $a = d = 0$ sau $a = d = 1$, și obținem matricele idempotente $A = 0$ și $A = I_2$.

Dacă $a + d = 1$, avem următoarele posibilități:

- $a = 0$ și atunci $d = 1$, $bc = 0$, de unde $b = 0$ sau $c = 0$. Obținem matricele idempotente $A = \begin{pmatrix} 0 & b \\ 0 & 1 \end{pmatrix}$ cu $b \in \mathbb{Z}_p$ și $A = \begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix}$ cu $c \in \mathbb{Z}_p - \{0\}$, în număr de $p + p - 1 = 2p - 1$.
- $a = 1$ și atunci $d = 0$, $bc = 0$. Obținem matricele idempotente $A = \begin{pmatrix} 1 & b \\ 0 & 0 \end{pmatrix}$ cu $b \in \mathbb{Z}_p$ și $A = \begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix}$ cu $c \in \mathbb{Z}_p - \{0\}$, în număr de $p + p - 1 = 2p - 1$.
- $a \notin \{0, 1\}$ și 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 și b prin formula $c = b^{-1}(a - a^2)$ (unde b^{-1} este inversul lui b în \mathbb{Z}_p). Obținem matricele idempotente

$$A = \begin{pmatrix} a & b \\ b^{-1}(a - a^2) & 1 - a \end{pmatrix}$$

cu $a \in \mathbb{Z}_p - \{0, 1\}$ și $b \in \mathbb{Z}_p - \{0\}$, 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 poziții nenule (deoarece într-o matrice neinvertabilă cu elemente nenule trei poziții pot fi alese fără restricții în $\mathbb{Z}_p - \{0\}$, iar a patra poziție este determinată în mod unic de celelalte trei), $4(p - 1)^3$ matrice inversabile cu exact trei poziții nenule și $2(p - 1)^2$ matrice inversabile cu exact două poziții 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 și 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 $\det(B) = 0$ și relația $B^2 - \text{tr}(B)B + \det(B)I_2 = 0$ devine $B^2 = \alpha B$, unde $\alpha = \text{tr}(B)$. Rezultă mai departe că $B^{q+2} = \alpha^{q+1}B$.

Dacă $\alpha = 0$, atunci $B^2 = 0$ și 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 $\alpha^q = 1$ și 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 $\det(A) = 0$ și sistemul de n ecuații cu n necunoscute

$$A \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix} = 0$$

are o soluție 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, contradicție. 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 poziția (i, j) și 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 $A = \sum_{1 \leq i, j \leq n} a_{ij}e_{ij}$ și avem $Ae_{pq} = \sum_{1 \leq i \leq n} a_{ip}e_{iq}$ și $e_{pq}A = \sum_{1 \leq j \leq n} a_{qj}e_{pj}$. De aici obținem că $Ae_{pq} = e_{pq}A$ dacă și numai dacă $a_{ip} = a_{qj} = 0$ pentru orice $i \neq p$ și $j \neq q$, și $a_{pp} = a_{qq}$. 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 $u \neq v$ și $a_{11} = a_{22} = \dots = a_{nn}$, 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 aplicația $f : R \rightarrow Z(M_n(R))$, $f(a) = aI_n$, este izomorfism de inele.

5. Este ușor de verificat că dacă $f : A \rightarrow B$ este un izomorfism de inele și $Z(A)$ este corp, atunci $Z(B)$ este un corp izomorf cu $Z(A)$, iar $Z(A)$ -spațiul vectorial A și $Z(B)$ -spațiul vectorial B au aceeași 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 $Z(A)$ -spațiul vectorial A , atunci $(f(a_i))_{i \in I}$ este o bază în $Z(B)$ -spațiul vectorial B .

În cazul particular în care $A = M_m(K)$ și $B = M_n(L)$, din problema 4 avem că $Z(A) \simeq K$, rezultă că $K \simeq Z(M_m(K)) \simeq Z(M_n(L)) \simeq L$ și 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 mulțimea tuturor elementelor care apar pe poziția $(1, 1)$ 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 poziția $(1, 1)$ și pentru $r \in R$ matricele $(rI_n)A$ și $A(rI_n)$ din X au pe poziția $(1, 1)$ elementele ra , respectiv ar , de unde $ar, ra \in I$.

Arătăm că $X = M_n(I)$. (Ca și în soluția problemei 4, notăm cu e_{ij} matricea care are 1 pe poziția (i, j) și 0 în rest). Fie $a \in I$ și $A \in X$ care are elementul a pe poziția $(1, 1)$. 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 $A = (a_{ij})_{1 \leq i, j \leq n} \in X$. Pentru orice i, j avem că $e_{1i}Ae_{j1} = a_{ij}e_{11}$ este o matrice din X , de unde $a_{ij} \in I$. Obținem 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 $p : R \rightarrow R/I$ proiecția canonică. Definim $f : M_n(R) \rightarrow M_n(R/I)$ astfel: dacă $A = (a_{ij})_{1 \leq i, j \leq n} \in M_n(R)$, atunci $f(A) = (p(a_{ij}))_{1 \leq i, j \leq n} \in M_n(R/I)$. Se verifică printr-un calcul simplu că f este morfism de inele. Este clar că f este surjectiv și că $\text{Ker}(f) = M_n(I)$. Din teorema fundamentală de izomorfism pentru inele obținem că $M_n(R)/M_n(I) \simeq M_n(R/I)$.

În final, observăm că pentru $n > 1$, mulțimea matricelor din $M_n(R)$ care au 0 pe coloanele $2, 3, \dots, n$ 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 $f : M_n(K) \rightarrow K$. Atunci $\text{Ker}(f)$ 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 și K . Cum $f(I_n) = 1$, nu putem avea $\text{Ker}(f) = M_n(K)$. Rămâne că $\text{Ker}(f) = 0$, adică f este injectiv, și atunci $M_n(K) \simeq \text{Im}(f)$, care este un subinel al lui K . Dar $M_n(K)$ are divizori ai lui zero (pentru că $n \geq 2$) și deci și K are divizori ai lui zero, contradicție.

8. (i) Pentru orice $u, v, z, w \in \mathbb{C}$ avem

$$\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} - \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} = \begin{pmatrix} u-z & v-w \\ -\bar{v}+\bar{w} & \bar{u}-\bar{z} \end{pmatrix} \in \mathbb{H},$$

$$\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} = \begin{pmatrix} uz - v\bar{w} & uw + v\bar{z} \\ -\bar{u}\bar{w} - \bar{v}z & \bar{u}z - \bar{v}w \end{pmatrix} \in \mathbb{H}$$

și $I_2 \in \mathbb{H}$, ceea ce arată că \mathbb{H} este subinel al lui $M_2(\mathbb{C})$. Observăm că dacă $A = \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \in \mathbb{H}$, atunci $\det(A) = |u|^2 + |v|^2$, de unde $A = 0$ dacă și numai dacă $\det(A) = 0$. Atunci pentru orice $A \neq 0$ din \mathbb{H} avem că A este inversabilă în $M_2(\mathbb{C})$ și inversa sa este matricea $\frac{1}{\det(A)} \begin{pmatrix} \bar{u} & -v \\ \bar{v} & u \end{pmatrix}$, care este în \mathbb{H} .

(ii) Aplicația $f : \mathbb{C} \rightarrow \mathbb{H}$, $f(u) = \begin{pmatrix} u & 0 \\ 0 & \bar{u} \end{pmatrix}$, este clar morfism (injectiv) de corpuri.

(iii) Dacă $A = \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}$ cu $u = a + ib$ și $v = c + id$, 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 $a_0I_2 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} = b_0I_2 + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k}$ obținem $a_0 + a_1i = b_0 + b_1i$ și $a_2 + a_3i = b_2 + b_3i$, de unde $a_t = b_t$ pentru orice $0 \leq t \leq 3$.

Fie $A = \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}$ cu $u = a + ib$ și $v = c + id$. Atunci $T(A) = 2aI_2 = \text{tr}(A)I_2$, unde $\text{tr}(A)$ este urma matricei A . Folosind relațiile $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -I_2$, $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$, $\mathbf{jk} = -\mathbf{kj} = \mathbf{i}$ și $\mathbf{ki} = -\mathbf{ik} = \mathbf{j}$, obținem 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 relația $A^2 - T(A)A + N(A) = 0$ nu este altceva decât cunoscuta formulă $A^2 - \text{tr}(A)A + \det(A)I_2 = 0$ pentru matrice pătratice de ordin 2, formulă care rezultă ușor 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 $A\mathbf{i} =$

$a\mathbf{i} - bI_2 - c\mathbf{k} + d\mathbf{j}$ și $\mathbf{i}A = a\mathbf{i} - bI_2 + c\mathbf{k} - d\mathbf{j}$, rezultă că $c = d = 0$. Apoi $\mathbf{j}A = \mathbf{j}(aI_2 + b\mathbf{i}) = a\mathbf{j} - b\mathbf{k}$ și $A\mathbf{j} = a\mathbf{j} + b\mathbf{k}$, 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 și incluziunea inversă, de unde rezultă că $Z(\mathbb{H}) = \mathbb{R}I_2$.

(v) Fie A o soluție a ecuației $x^2 = -1$ în \mathbb{H} , adică $A = aI_2 + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ cu $a, b, c, d \in \mathbb{R}$ și $A^2 = -I_2$. Atunci $\det(A)^2 = \det(-I_2) = 1$ și 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 $A^2\bar{A} = -\bar{A}$, de unde $AN(A) = -\bar{A}$, sau $A = -\bar{A}$. 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 soluție. Într-adevăr, avem $N(A) = I_2$ și $A = -\bar{A}$, de unde $AN(A) = -\bar{A}$, sau $A^2\bar{A} = -\bar{A}$. Cum \mathbb{H} este corp și $\bar{A} \neq 0$, rezultă că $A^2 = -I_2$.

Așadar soluțiile ecuației $x^2 = -1$ 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 poziția (i, j) și 0 în rest. Atunci $\sum_{1 \leq i \leq n} E_{ii} = I_n$ și $E_{ij}E_{kl} = \delta_{jk}E_{il}$ pentru orice $1 \leq i, j, k, l \leq n$.

Dacă $f : M_n(R) \rightarrow S$ este un izomorfism de inele și $e_{ij} = f(E_{ij})$, atunci familia $(e_{ij})_{1 \leq i, j \leq n}$ satisface condițiile 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

$$\begin{aligned} 0 &= e_{pq} \left(\sum_{1 \leq i, j \leq n} r_{ij}e_{ij} \right) e_{kl} \\ &= \sum_{1 \leq i, j \leq n} e_{pq} r_{ij} e_{ij} e_{kl} \\ &= \sum_{1 \leq i, j \leq n} r_{ij} e_{pq} e_{ij} e_{kl} \\ &= r_{qk} e_{pl}. \end{aligned}$$

Atunci $r_{ij} = \sum_{1 \leq p \leq n} r_{ij} e_{pp} = 0$.

Definim acum $f : M_n(R) \rightarrow S$ 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

$$\begin{aligned}
 f(A)f(B) &= \sum_{i, j, p, q} r_{ij} e_{ij} s_{pq} e_{pq} \\
 &= \sum_{i, j, p, q} r_{ij} s_{pq} e_{ij} e_{pq} \\
 &= \sum_{i, j, q} r_{ij} s_{jq} e_{iq} \\
 &= \sum_{i, q} \left(\sum_j r_{ij} s_{jq} \right) e_{iq} \\
 &= f(AB)
 \end{aligned}$$

și $f(I_n) = \sum_{1 \leq i \leq n} e_{ii} = 1$, 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 sfârșit, fie $a \in S$. Arătăm că pentru orice $1 \leq i, j \leq n$, elementul $a_{ij} = \sum_{1 \leq k \leq n} e_{ki} a e_{jk}$ este în R . Într-adevăr

$$\begin{aligned}
 a_{ij} e_{pl} &= \sum_{1 \leq k \leq n} e_{ki} a e_{jk} e_{pl} \\
 &= \sum_{1 \leq k \leq n} \delta_{kp} e_{ki} a e_{jl} \\
 &= e_{pi} a e_{jl}
 \end{aligned}$$

și

$$\begin{aligned}
 e_{pl} a_{ij} &= \sum_{1 \leq k \leq n} e_{pl} e_{ki} a e_{jk} \\
 &= \sum_{1 \leq k \leq n} \delta_{lk} e_{pi} a e_{jk} \\
 &= e_{pi} a e_{jl}.
 \end{aligned}$$

Atunci $A = (a_{ij})_{1 \leq i, j \leq n} \in M_n(R)$ și

$$\begin{aligned}
 f(A) &= \sum_{1 \leq i, j \leq n} a_{ij} e_{ij} \\
 &= \sum_{1 \leq i, j \leq n} \sum_{1 \leq k \leq n} e_{ki} a e_{jk} e_{ij} \\
 &= \sum_{1 \leq i, j \leq n} e_{ii} a e_{jj} \\
 &= \left(\sum_{1 \leq i \leq n} e_{ii} \right) a \left(\sum_{1 \leq j \leq n} e_{jj} \right) \\
 &= a
 \end{aligned}$$

ceea ce arată că f este și 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 condițiile din problema 9(b) este o familie cu aceleași proprietăți și în B . De asemenea familia $(p(e_{ij}))_{1 \leq i, j \leq n}$ din A satisface proprietățile din problema 9(b) pentru A , unde $p : S \rightarrow A$ este proiecția canonică.

11. (i) Verificare imediată.

(ii) Folosind proprietatea de universalitate a inelelor de polinoame, există un morfism de inele $\phi : \mathbb{Z}[X] \rightarrow R_k$ astfel încât $f(a) = aI_2$ pentru orice $a \in \mathbb{Z}$ și $\phi(X) = \begin{pmatrix} 0 & 1 \\ k & 0 \end{pmatrix}$. Atunci ϕ este surjectiv, deoarece $\phi(a+bX) = \begin{pmatrix} a & b \\ kb & a \end{pmatrix}$. Arătăm că $\text{Ker}(\phi) = (X^2 - k)$. Este clar că $\phi(X^2 - k) = 0$, deci $(X^2 - k) \subseteq \text{Ker}(\phi)$. Fie acum $f \in \text{Ker}(\phi)$. Cum $X^2 - k$ are coeficientul dominant 1, putem aplica algoritmul de împărțire cu rest și obținem $f(X) = (X^2 - k)g(X) + r(X)$, unde $r(X) = a + bX$ cu $a, b \in \mathbb{Z}$. Aplicând ϕ obținem că $\phi(r) = 0$, deci $\begin{pmatrix} a & b \\ kb & a \end{pmatrix} = 0$, de unde evident $a = b = 0$. Rezultă că $r = 0$ și $f \in (X^2 - k)$.

(iii) Din (ii) avem că $R_k \simeq R_l$ dacă și numai dacă există un izomorfism $\psi : \mathbb{Z}[X]/(X^2 - k) \rightarrow \mathbb{Z}[X]/(X^2 - l)$. Notăm cu \hat{f} și \bar{f} clasele unui polinom f în inelele factor $\mathbb{Z}[X]/(X^2 - k)$ și $\mathbb{Z}[X]/(X^2 - l)$, respectiv. Este clar că $\psi(\hat{a}) = \bar{a}$ pentru $a \in \mathbb{Z}$. Fie $\psi(\hat{X}) = \overline{a + bX}$. Atunci $\psi(\hat{X})^2 = \psi(\hat{X}^2) = \psi(\hat{k}) = \bar{k}$, de unde $\overline{(a + bX)^2} = \bar{k}$, ceea ce implică $2abX + a^2 + b^2l - k \in (X^2 - l)$. De aici obținem că $ab = 0$ și $a^2 + b^2l = k$. Cum $b \neq 0$ (altfel ψ nu ar fi surjectivă),

rezultă că $a = 0$ și apoi $b^2l = k$. Rezultă că $l|k$ și l, k au același semn. Din motive de simetrie (lucrând cu inversul lui ψ) obținem și $k|l$, de unde $k = l$.

12. Soluția 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 $\phi : M_n(R[X]) \rightarrow M_n(R)[X]$ 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.

Soluția 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 poziția (i, j) și 0 în rest. Considerăm e_{ij} ca pe niște polinoame de grad zero din S . Deoarece familia $(e_{ij})_{1 \leq i, j \leq n}$ verifică condițiile 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 $f \in S$, $f(X) = A_0 + \dots + A_h X^h$. Atunci $f \in T$ dacă și numai dacă $e_{ij}A_k = A_k e_{ij}$ pentru orice $1 \leq i, j \leq n$ și $0 \leq k \leq h$. Dar aceasta este echivalent cu $A_k \in Z(M_n(R)) = RI_n$ pentru orice k . Obținem 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 obținem că există un unic morfism de inele $\phi : R[X_1, \dots, X_n] \rightarrow R$ cu proprietatea că $\phi(r) = r$ pentru $r \in R$ și $\phi(X_i) = a_i$ pentru $1 \leq i \leq n$. Este evident că ϕ este surjectiv. Arătăm prin inducție după n că $\text{Ker}(\phi) = (X_1 - a_1, \dots, X_n - a_n)$. Pentru $n = 1$ rezultă din teorema lui Bézout. Presupunem că afirmația este adevărată pentru $n - 1$ și o demonstrăm pentru n . Din teorema de împărțire cu rest pentru polinoame rezultă că $f(X_1, \dots, X_n) = (X_n - a_n)g(X_1, \dots, X_n) + r(X_1, \dots, X_{n-1})$, deoarece restul r este un polinom de grad zero în X_n . Cum $f(a_1, \dots, a_n) = 0$, rezultă că $r(a_1, \dots, a_{n-1}) = 0$ și din ipoteza de inducție avem că $r \in (X_1 - a_1, \dots, X_{n-1} - a_{n-1})$. De aici rezultă că $f \in (X_1 - a_1, \dots, X_n - a_n)$. Reciproc este evident că dacă $f \in (X_1 - a_1, \dots, X_n - a_n)$, atunci $f \in \text{Ker}(\phi)$. Izomorfismul cerut rezultă acum din teorema fundamentală de izomorfism pentru inele.

14. Notăm cu A inelul $R[X_1, \dots, X_n]$ și cu I^e idealul extins al lui I în A .
(i) Este clar că $I \subset I[X_1, \dots, X_n]$. De aici rezultă că idealul generat de I în

A , adică I^e , este inclus în $I[X_1, \dots, X_n]$. 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 toți coeficienții în I , deci suma lor va avea prin urmare aceeași proprietate. În consecință, $I^e \subset I[X_1, \dots, X_n]$.

(ii) Considerăm proiecția canonică $\pi : R \rightarrow R/I$ și o extindem la un morfism $\bar{\pi} : R[X_1, \dots, X_n] \rightarrow (R/I)[X_1, \dots, X_n]$, conform proprietății de universalitate a inelelor de polinoame. Avem că

$$\bar{\pi}(\sum a_{i_1 \dots i_n} X_1^{i_1} \cdots X_n^{i_n}) = \sum \pi(a_{i_1 \dots i_n}) X_1^{i_1} \cdots X_n^{i_n}$$

și morfismul $\bar{\pi}$ este în mod evident surjectiv. Pe de altă parte, un polinom $f = \sum a_{i_1 \dots i_n} X_1^{i_1} \cdots X_n^{i_n}$ aparține lui $\text{Ker } \bar{\pi}$ dacă și numai dacă $\sum \pi(a_{i_1 \dots i_n}) X_1^{i_1} \cdots X_n^{i_n} = 0$, ceea ce este echivalent cu $\pi(a_{i_1 \dots i_n}) = 0$ pentru orice multiindice $i_1 \dots i_n$, adică $a_{i_1 \dots i_n} \in I$ pentru orice multiindice $i_1 \dots i_n$. În concluzie, $\text{Ker } \bar{\pi} = I[X_1, \dots, X_n]$ și izomorfismul căutat rezultă acum din teorema fundamentală de izomorfism pentru inele.

(iii) Idealul $I[X_1, \dots, X_n]$ este prim în A dacă și numai dacă inelul factor $R[X_1, \dots, X_n]/I[X_1, \dots, X_n]$ este domeniu de integritate. Conform izomorfismului de la punctul (ii), aceasta se întâmplă dacă și numai dacă inelul de polinoame $(R/I)[X_1, \dots, X_n]$ este domeniu de integritate, echivalent cu faptul că R/I este domeniu. În fine, R/I este domeniu dacă și 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 $\phi : \mathbb{Z}[X] \rightarrow \mathbb{Z}[\sqrt{d}]$ cu proprietatea că $\phi(n) = n$ pentru orice $n \in \mathbb{Z}$ și $\phi(X) = \sqrt{d}$. 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 $\text{Ker}(\phi) = (X^2 - d)$. Incluziunea " \supseteq " este evidentă. Invers, dacă $f \in \text{Ker}(\phi)$, adică $f(\sqrt{d}) = 0$, împărțim cu rest pe f la $X^2 - d$ și obținem $f(X) = (X^2 - d)q(X) + r(X)$, $q(X), r(X) \in \mathbb{Z}[X]$ 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 $X = \sqrt{d}$ obținem că $a + b\sqrt{d} = 0$, și cum d este liber de pătrate, deci \sqrt{d} este irațional, trebuie să avem $a = b = 0$. Obținem 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 $\phi : \mathbb{Q}[X] \rightarrow \mathbb{Q}(\varepsilon)$, $\phi(f) = f(\varepsilon)$.

(iii) Similar cu (i), dacă se consideră morfismul de inele $\phi : \mathbb{R}[X] \rightarrow \mathbb{C}$, $\phi(f) = f(i)$.

16. Fie $d \in \mathbb{Z}$ liber de pătrate și $a, b \in \mathbb{Z}$ 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 $\mathbb{Z}[\sqrt{d}]/(a + b\sqrt{d}) = \mathbb{Z}[\sqrt{d}]/(a) = \widehat{\mathbb{Z}[\sqrt{d}]/(a)} = \{u + v\sqrt{d} \mid u, v \in \{0, 1, \dots, |a| - 1\}\}$ (conform teoremei de împărțire cu rest din \mathbb{Z} , pentru orice $x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ există $x', y' \in \mathbb{Z}$ și $r, s \in \{0, 1, \dots, |a| - 1\}$ astfel încât $x + y\sqrt{d} = (ax' + r) + (ay' + s\sqrt{d}) \equiv r + s\sqrt{d} \pmod{I}$). Cum aceste clase sunt distincte, obținem că $\mathbb{Z}[\sqrt{d}]/(a + b\sqrt{d})$ are $a^2 = |a^2 - db^2|$ elemente.

Pentru $b \neq 0$ să notăm $g = (a, b)$. Punem $a = ga'$ și $b = gb'$, cu $a', b' \in \mathbb{Z}$, $(a', b') = 1$, și $m = (a')^2 - d(b')^2$. 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 și $b'\sqrt{d} \equiv -a' \pmod{a' + b'\sqrt{d}}$, 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 $j + k\sqrt{d}$ cu $0 \leq j < g|m|$ și $0 \leq k < g$. 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 relație 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 $a_1 = a'c$ și $b_1 = b'c$. De aici și din $j + k\sqrt{d} = (a + b\sqrt{d})(a_1 + b_1\sqrt{d})$ obținem $j = aa_1 + bb_1\sqrt{d} = gc((a')^2 - (b')^2d)$, 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 și β , și 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 $n = 2$ și $I_1 = (X - \alpha)$, $I_2 = (X - \beta)$ (vezi problema 28 din Capitolul 4) obținem 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 $(X - \alpha)^2 \in P$ și 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 $P = (X - \alpha)$. Obținem că $M = (X - \alpha)/((X - \alpha)^2)$, de unde rezultă că R este inel local.

18. Similar cu soluția 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 $2\mathbb{Z}[i]$, și 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 $\deg(f) = 0$ și $f \in \{1, -1, 3, -3\}$. 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 $X = 1$ obținem că $1 = 3(g(1) + h(1))$, contradicție. Dacă $f = 3$ sau $f = -3$, atunci $I = 3\mathbb{Z}[X]$ și deci $X^3 - X^2 + 2X + 1 \in 3\mathbb{Z}[X]$, din nou contradicție. Așadar 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 $\mathbb{R}[X]$ și că I este ideal al lui R . Fie $\phi : R \rightarrow \mathbb{Q}$ definită prin $\phi(f) = f(0)$. Atunci ϕ este morfism surjectiv de inele și $\text{Ker}(\phi) = I$, 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 $I = (f_1, \dots, f_n)$, unde $f_i = a_1^{(i)}X + a_2^{(i)}X^2 + \dots$ pentru $1 \leq i \leq n$. Atunci pentru orice $a \in \mathbb{R}$ există

$g_1, \dots, g_n \in R$ cu $aX = g_1f_1 + \dots + g_nf_n$. În această relație putem simplifica prin X și apoi, pentru $X = 0$ obținem $a = g_1(0)a_1^{(1)} + \dots + g_n(0)a_1^{(n)}$. Aceasta arată că $\{a_1^{(1)}, \dots, a_1^{(n)}\}$ este sistem de generatori pentru \mathbb{Q} -spațiul vectorial \mathbb{R} , ceea ce este o contradicție cu faptul că \mathbb{R} este mulțime nenumărabilă. Prin urmare I nu este finit generat.

21. Presupunem prin absurd că $I = (f_1, \dots, f_n)$. Polinoamele f_1, \dots, 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, \dots, X_N . Cum $X_{N+1} \in I$, există $g_1, \dots, g_n \in R$ pentru care $X_{N+1} = g_1f_1 + \dots + g_nf_n$. Pentru $X_1 = \dots = X_N = 0$ și $X_{N+1} \neq 0$ obținem o contradicție.

22. Folosind problema 47(v) din Capitolul 4, avem

$$\begin{aligned} \text{Rad}(I) &= \text{Rad}((X^r) + (Y^s)) \\ &= \text{Rad}(\text{Rad}(X^r) + \text{Rad}(Y^s)) \\ &= \text{Rad}((X) + (Y)) \\ &= \text{Rad}(X, Y) \\ &= (X, Y). \end{aligned}$$

Dacă $fg \in I$ și $g \notin \text{Rad}(I)$, 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^uY^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 $X^uY^v \in I$. Considerăm acum polinomul $f_1 = f - a_{uv}X^uY^v$. Avem că $f_1g \in I$ și folosind aceleași argumente ca mai înainte obținem 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 coeficienții lui X^2 în $X^2 - Y^3 = fg$ și rezultă că $g \in K^*$, deci g este inversabil. Similar dacă $\deg_X(g) = 2$ rezultă că f este inversabil. Presupunem că $\deg_X(f) = \deg_X(g) = 1$ și scriem $f = a(Y) + b(Y)X$, $g = c(Y) + d(Y)X$, cu $a, b, c, d \in K[Y]$. Relația $X^2 - Y^3 = fg$ revine la $b(Y)d(Y) = 1$, $a(Y)d(Y) + b(Y)c(Y) = 0$ și $a(Y)c(Y) = -Y^3$. Prima relație arată că $b(Y)$

și $d(Y)$ sunt constante nenule, deci $b(Y) = b$, $d(Y) = b^{-1}$, cu $b \in K^*$. A doua relație arată atunci că $c(Y) = b^{-2}a(Y)$, în particular că $a(Y)$ și $c(Y)$ au același grad. Dar atunci $a(Y)c(Y)$ are grad par și nu poate fi egal cu $-Y^3$. Prin urmare unul dintre f și g este inversabil.

(ii) Folosim proprietatea de universalitate a inelelor de polinoame pentru a construi un morfism de inele $\phi : K[X, Y] \rightarrow k[T]$ pentru care $\phi(a) = a$ pentru orice $a \in K$, $\phi(X) = T^3$ și $\phi(Y) = T^2$. Atunci $\text{Im}(\phi) = B$. Într-adevăr, $\phi(X^i Y^j) = T^{3i+2j} \in B$ pentru orice i, j , deoarece pentru $(i, j) \neq (0, 0)$ avem $3i + 2j \geq 2$. Pe de altă parte $T^m \in \text{Im}(\phi)$ pentru orice $m \geq 2$, deoarece $T^{2i} = \phi(Y^i)$ și $T^{2i+1} = \phi(XY^{i-1})$ pentru $i \geq 1$.

Arătăm acum că $\text{Ker}(\phi) = (X^2 - Y^3)$. Incluziunea " \supseteq " este clară. Invers, fie $f \in K[X, Y]$ cu $f(T^3, T^2) = 0$. Îl privim pe f în $K[Y][X]$ și folosind teorema de împărțire cu rest obținem 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 $r = 0$ și $f \in (X^2 - Y^3)$. Izomorfismul cerut rezultă acum direct din teorema fundamentală de izomorfism. Să observăm că integritatea lui R rezultă direct din (ii), soluția 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 $u = a_0 + a_1X + a_2X^2 + \dots$, atunci $u^2 = 1 + X$ dacă și numai dacă $a_0^2 = 1$, $2a_0a_1 = 1$, $2a_0a_2 + a_1^2 = 0$, $2a_0a_3 + 2a_1a_2 = 0$, \dots . Recurent putem găsi a_0, a_1, a_2, \dots care verifică relațiile de mai sus (aici avem nevoie de caracteristică $\neq 2$) și deci există u cu $u^2 = 1 + X$. Atunci $(Xu)^2 = X^2 + X^3$ și $Y^2 - X^3 - X^2 = Y^2 - (Xu)^2 = (Y - Xu)(Y + Xu)$ nu este element ireductibil în $K[[X, Y]]$. Obținem că $(Y^2 - X^3 - X^2)$ nu este ideal prim în $K[[X, Y]]$, de unde concluzia.

25. (i) Procedăm prin inducție după $n = \deg(f)$. Pentru $n = 0$ este clar. Presupunem afirmația adevărată pentru toate polinoamele de grad mai mic strict decât n . Dacă $\deg(f) = n$, atunci din faptul că f este nilpotent obținem 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 inducție rezultă acum că a_0, a_1, \dots, a_{n-1} sunt nilpotenți.

(ii) " \Leftarrow " Avem că a_0 este inversabil și $a_1X + \dots + a_nX^n$ 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 și un element nilpotent.

" \Rightarrow " Procedăm prin inducție după $\deg(f) = n$. Pentru $n = 0$ este clar. Presupunem afirmația adevărată pentru toate polinoamele de grad mai mic strict decât n și fie f cu $\deg(f) = n$. Fie $g = b_0 + b_1X + \dots + b_mX^m$ inversul lui f . Din $fg = 1$ rezultă că

$$a_nb_m = 0, a_nb_{m-1} + a_{n-1}b_m = 0, \dots, a_0b_0 = 1.$$

Înmulțind a doua relație cu a_n obținem că $a_n^2b_{m-1} = 0$, și apoi prin recurență 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 și un element nilpotent. Din ipoteza de inducție rezultă acum că și elementele a_1, \dots, 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 $g(X) = b_0 + b_1X + \dots + b_mX^m$. Din $fg = 0$ rezultă că $a_nb_m = 0$. Atunci a_ng are gradul mai mic ca m și $(a_ng)f = 0$, de unde obținem că $a_ng = 0$. În particular $a_nb_{m-1} = 0$ și 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 și $(a_{n-1}g)f = 0$, de unde $a_{n-1}g = 0$. Continuăm recurent și obținem 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 demonstrația.

(iv) Dacă f este idempotent, $f^2 = f$, atunci $a_0^2 = a_0$, $2a_0a_1 = a_1$, $2a_0a_2 + a_1^2 = a_2$, și așa mai departe. Înmulțind a doua relație cu a_0 și folosind-o pe prima obținem $2a_0a_1 = a_0a_1$, deci $a_0a_1 = 0$. Rezultă că și $a_1 = 0$. Apoi înmulțind a treia relație cu a_0 și folosind-o pe prima, obținem că $2a_0a_2 = a_0a_2$, deci $a_0a_2 = 0$, ceea ce arată că și $a_2 = 0$. 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 $f - a_0 = X(a_1 + a_2X + \dots)$ și cum $f^t = a_0^t = 0$, cu observația de mai sus avem că $(f - a_0)^{2t} = 0$, deci $f_1^{2t} = 0$, unde $f_1 = a_1 + a_2X + \dots$. Obținem că $a_1^{2t} = 0$, deci a_1 este nilpotent. Recurent obținem că $a_i^{2^t} = 0$

pentru orice $i \geq 0$, deci toți coeficienții sunt nilpotenți (chiar mai mult, avem niște margini pentru indicii de nilpotență ai fiecărui coeficient).

Reciproc este fals. Fie $A = \mathbb{Z}[Y_0, Y_1, \dots]$ inelul de polinoame cu coeficienți întregi într-o infinitate de nedeterminate. Considerăm idealul

$$I = (Y_0, Y_1^{2^2}, \dots, Y_n^{2^{2^n}}, \dots)$$

și 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 $2^{2^i} \leq 2^i t$ 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 $g = b_0 + b_1 X + \dots$ 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 și construim un invers g pentru f . Cum $fg = 1$ este echivalent cu

$$a_0 b_0 = 1, a_0 b_1 + a_1 b_0 = 0, \dots, a_0 b_n + a_1 b_{n-1} + \dots + a_n b_0 = 0, \dots,$$

putem construi pe g astfel: alegem mai întâi $b_0 = a_0^{-1}$. Apoi b_1 se obține 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, \dots , unde $b_n = -a_0^{-1} (a_1 b_{n-1} + \dots + a_n b_0)$.

(iii) Se procedează la fel ca la soluția 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 $M = R[[X]]$, contradicție.

Fie $f = a_0 + a_1 X + \dots \in M$. 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 și fie M un ideal maximal al lui $R[[X]]$. Folosind (i) rezultă că $M \cap R = m$ și $M = mR[[X]] + XR[[X]]$.

(iii) Să presupunem că $R[X]$ ar fi inel local cu idealul maximal M . Atunci X și $1 - X$ sunt în M , altfel ar fi inversabile în $R[X]$ (din problema 28(ii)). Atunci $1 = X + (1 - X) \in M$, contradicție.

28. Fie Q un ideal prim al lui $R[[X]]$. Notăm $P = \{a \in R \mid \text{există } f = a + a_1X + a_2X^2 + \dots \in Q\}$. Cum P este ideal al lui R , rezultă că există $a_1, \dots, a_r \in P$ astfel încât $P = (a_1, \dots, a_r)$.

Dacă $X \in Q$, atunci $Q = (a_1, \dots, a_r, X)$.

Dacă $X \notin Q$, fie $f_1, \dots, f_r \in Q$ serii formale astfel încât termenul liber al lui f_j să fie a_j , $j = 1, \dots, r$. Are loc relația $Q = (f_1, \dots, f_r)$. Într-adevăr, fie $g \in Q$. Atunci termenul liber al lui g se poate scrie sub forma $b_{10}a_1 + \dots + b_{r0}a_r$. Se obține $g - (b_{10}f_1 + \dots + b_{r0}f_r) = Xg_1 \in Q$. Cum $X \notin Q$, rezultă că $g_1 \in Q$, deci, procedînd ca mai sus, putem scrie $g_1 - (b_{11}f_1 + \dots + b_{r1}f_r) = Xg_2 \in Q$. De aici, $g_2 \in Q$. Inductiv găsim b_{1k}, \dots, b_{rk} așa încât $g_k - (b_{1k}f_1 + \dots + b_{rk}f_r) = Xg_{k+1} \in Q$, de unde $g_{k+1} \in Q$. Este clar acum că $h_i = b_{i0} + b_{i1}X + \dots$ verifică relația $g = h_1f_1 + \dots + h_rf_r$.

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 definiția 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 conține pe $(X - 2)$ este $2\mathbb{Z}[[X]] + X\mathbb{Z}[[X]]$ și în mod evident incluziunea este strictă. Așadar $\mathbb{Z}[[X]]/(X - 2)$ 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 toți coeficienții lui f sunt nilpotenți, deci $f \in N(R[X])$. Obținem 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 $f, g \in I$, $f = aX^n + \alpha_{n+1}X^{n+1} + \dots$, $g = bX^n + \beta_{n+1}X^{n+1} + \dots$, și cum $f - g = (a - b)X^n + (\alpha_{n+1} - \beta_{n+1})X^{n+1} + \dots$, 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

$$J = \{f \in R \mid (\exists)\alpha \in G \text{ cu } f = \alpha X^n + \alpha_2 X^{n+1} + \dots\}.$$

Este imediat că J este ideal al lui R și $I \subseteq J$. În plus $J \neq R$, altfel am avea $n = 1$ și $G = K$. 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 obținut 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 $f, g \in I_G$, $f = aX + \alpha_2X^2 + \dots$, $g = bX + \beta_2X^2 + \dots$ cu $a, b \in G$, atunci $f - g = (a - b)X + \dots \in I_G$, și $qf = q_1aX^2 + \dots \in I_G$ pentru orice $q = q_1X + \dots \in R$, 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 $I_G \subseteq J$ și $J \neq R$. Atunci

$$G \subseteq H = \{a \in R \mid (\exists)f \in J \text{ cu } f = aX + \dots\},$$

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 $f = X + a_2X^2 + \dots \in J$. 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 $g = b_2X^2 + \dots$ avem $g = X^2q$ pentru un $q \in K[[X]]$, de unde $g = XuXu^{-1}q \in J$, pentru că $Xu = f \in J$ și $Xu^{-1}q \in R$. Fie acum $h = c_1X + c_2X^2 + \dots \in R$. Atunci $g = c_2X^2 + \dots \in J$. Pe de altă parte $c_1 \in K = H$, deci există $p = c_1X + d_2X^2 + \dots \in J$. Cum $d_2X^2 + \dots \in J$, obținem că $c_1X \in J$. Atunci $h = c_1X + g \in J$, ceea ce înseamnă că $J = R$, contradicție. Prin urmare $H \neq K$.

Obținem $H = G$, deoarece G este maximal. Dacă $f = aX + \dots \in J$, atunci avem că $a \in H$, deci $a \in G$, și deci $f \in I_G$. Obținem $J = I_G$, ceea ce arată că I_G este maximal.

(iii) Rezultă direct din (i) și (ii).

(iv) Dacă grupul $(K, +)$ este divizibil, atunci pentru orice $n \in \mathbb{Z} - \{0\}$ și orice $a \in K$, ecuația $nx = a$ are soluție $x \in K$. În particular, pentru orice p prim ecuația $px = 1$ are soluție în K , de unde $\text{char}(K) \neq p$. Rămâne că $\text{char}(K) = 0$.

Reciproc, dacă $\text{char}(K) = 0$, atunci orice $n \in \mathbb{Z} - \{0\}$ este inversabil în K și atunci ecuația $nx = a$ are soluția $x = n^{-1}a$.

(v) Dacă grupul $(K, +)$ are subgrupuri maximale, atunci, din problema 37(ii) din Capitolul 3, el nu este divizibil și din (iv) rezultă $\text{char}(K) \neq 0$.

Reciproc, dacă $\text{char}(K) = p > 0$, atunci K are un subcorp izomorf cu corpul \mathbb{Z}_p , deci putem să privim pe K ca pe un \mathbb{Z}_p -spațiu vectorial. Atunci K are un \mathbb{Z}_p -subspațiu vectorial maximal (este suficient să luăm o bază B a lui K ,

un element $b \in B$, și atunci \mathbb{Z}_p -subspațiul vectorial generat de $B - \{b\}$ este maximal), care este evident și un subgrup maximal al lui $(K, +)$.

(vi) Rezultă direct din (iii) și (vi).

32. (i) Fie I un ideal propriu al lui $K[[X]]$ și fie $n = \inf\{\text{ord}(f) \mid f \in I\}$. Atunci $n \geq 1$, altfel există $f \in I$ cu $\text{ord}(f) = 0$ și cum un astfel de f este inversabil, rezultă că $I = K[[X]]$, contradicție.

Vom arăta că $I = (X^n)$. Dacă $f \in I$, atunci $\text{ord}(f) \geq n$, deci $f = a_n X^n + a_{n+1} X^{n+1} + \dots = X^n(a_n + a_{n+1}X + \dots) \in (X^n)$, de unde $I \subseteq (X^n)$. Pe de altă parte, există $f \in I$ cu $\text{ord}(f) = n$ și atunci $f = X^n u$, cu $\text{ord}(u) = 0$, adică u este inversabil. Atunci $X^n = X^n u u^{-1} = f u^{-1} \in I$, de unde $(X^n) \subseteq I$. Obținem că $I = (X^n)$.

În particular, singurul ideal maximal al lui $K[[X]]$ este (X) , deci $K[[X]]$ este inel local.

(ii) Este ușor de văzut că dacă $f = a_0 + a_2 X^2 + \dots$ cu $a_0 \neq 0$, atunci f este inversabil în R (într-adevăr, inversul lui f din $K[[X]]$, calculat în soluția problemei 26(ii), se găsește în R). Fie I un ideal propriu nenul al lui R . Atunci $n = \inf\{\text{ord}(g) \mid g \in I\} \geq 2$ și există $f = a_n X^n + a_{n+1} X^{n+1} + \dots \in I$ cu $a_n \neq 0$. Cum $a_n \neq 0$, există $u \in K[[X]]$ cu $(a_n + a_{n+1}X + \dots)u = 1$. Atunci $X^{n+2} = X^2 f u \in I$ și $X^{n+3} = X^3 f u \in I$. De aici rezultă că $a_{n+2} X^{n+2} + a_{n+3} X^{n+3} + \dots = X^{n+2}(a_{n+2} + a_{n+3}X + \dots) + a_{n+3} X^{n+3} \in I$, și mai departe că $a_n X^n + a_{n+1} X^{n+1} \in I$. Avem două cazuri:

1. Există $g \in I$, $g = b_n X^n + b_{n+1} X^{n+1} + \dots$ cu proprietatea că $a_n b_{n+1} \neq a_{n+1} b_n$.

Avem că $b_n X^n + b_{n+1} X^{n+1} \in I$. Într-adevăr, dacă $b_n \neq 0$ rezultă din cele arătate mai sus. Dacă $b_n = 0$, atunci $b_{n+1} \neq 0$ și din nou ca mai sus avem că $b_{n+1} X^{n+1} + b_{n+2} X^{n+2} \in I$. Dar știm deja că $X^{n+2} \in I$ și obținem că $b_{n+1} X^{n+1} \in I$.

Atunci avem că $a_n(b_n X^n + b_{n+1} X^{n+1}) \in I$ și cum $b_n(a_n X^n + a_{n+1} X^{n+1}) \in I$, obținem prin scădere că $(a_n b_{n+1} - a_{n+1} b_n) X^{n+1} \in I$, de unde $X^{n+1} \in I$. În continuare rezultă că $a_n X^n \in I$, deci $X^n \in I$, și obținem că $(X^n, X^{n+1}) \subseteq I$. Dar incluziunea inversă este evidentă din relația $c_n X^n + c_{n+1} X^{n+1} + \dots = X^n(c_n + c_{n+2} X^2 + \dots) + c_{n+1} X^{n+1}$. Rezultă că $I = (X^n, X^{n+1})$.

2. Pentru orice $g = b_n X^n + b_{n+1} X^{n+1} + \dots \in I$ avem $a_n b_{n+1} = a_{n+1} b_n$.

Fie $a = a_n^{-1} a_{n+1}$. Arătăm că $I = (X^n + a X^{n+1})$. Deoarece $a_n X^n + a_{n+1} X^{n+1} \in I$ rezultă că $a_n^{-1}(a_n X^n + a_{n+1} X^{n+1}) \in I$, deci $X^n + a X^{n+1} \in I$. Invers, fie $h \in I$, $h = c_n X^n + c_{n+1} X^{n+1} + \dots$. Atunci se verifică ușor că $g = (X^n + a X^{n+1})(d_0 + d_2 X^2 + \dots)$, unde $d_0 = c_n, d_2 = c_{n+2}, d_i = c_{n+i} - a d_{i-1}$

pentru orice $i \geq 3$ (notăm că relația $ad_0 = c_{n+1}$ este verificată deoarece $a_n c_{n+1} = a_{n+1} c_n$). Așadar $g \in I$ și 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 înmulțirea seriilor formale. Fie $N > 0$. Se arată imediat prin inducție după N că dacă $f = 1 + a_1X + a_2X^2 + \dots$, atunci

$$f^N = 1 + Na_1X + (Na_2 + h_2(a_1))X^2 + (Na_3 + h_3(a_1, a_2))X^3 + \dots$$

pentru niște funcții polinomiale h_2, h_3, \dots care nu depind de f . Fie $g = 1 + b_1X + b_2X^2 + \dots \in U_1(K[[X]])$. Atunci

$$g^N = 1 + Nb_1X + (Nb_2 + h_2(b_1))X^2 + (Nb_3 + h_3(b_1, b_2))X^3 + \dots$$

Dacă $\phi_N(f) = \phi_N(g)$, identificând coeficienții rezultă că

- $Na_1 = Nb_1$ și cum $N1_K \neq 0$, deci este inversabil, obținem că $a_1 = b_1$.
- $Na_2 + h_2(a_1) = Nb_2 + h_2(b_1)$, și cum $a_1 = b_1$, obținem că $Na_2 = Nb_2$, deci $a_2 = b_2$.
- Recurent obținem că $a_i = b_i$ pentru orice $i \geq 1$.

Rezultă că $f = g$, deci ϕ_N este injectivă.

Pentru surjectivitate, fie $u = 1 + u_1X + u_2X^2 + \dots \in U_1(K[[X]])$. Căutăm $f = 1 + a_1X + a_2X^2 + \dots$ cu $f^N = u$. Aceasta este echivalent cu

$$\begin{aligned} Na_1 &= u_1 \\ Na_2 + h_2(a_1) &= u_2 \\ &\dots \end{aligned}$$

sistem în a_1, a_2, \dots care se rezolvă ecuație cu ecuație (începând cu prima) și rezultă soluții pentru a_1, a_2, \dots (din nou folosim la fiecare ecuație faptul că $N1_K$ este inversabil).

Este clar că ϕ_N este morfism de grupuri deoarece $\phi_N(fg) = (fg)^N = f^N g^N = \phi_N(f)\phi_N(g)$. Așadar ϕ_N este izomorfism de grupuri.

Considerăm aplicația $\psi : U_1(K[[X]]) \rightarrow U_1(K[[X]])$, $\psi(f) = f^{-1}$, care este evident izomorfism de grupuri. Atunci $\psi\phi_N = \phi_{-N}$, deci și ϕ_{-N} este izomorfism de grupuri.

34. (i) Primele două formule rezultă ușor prin calcule directe, iar a treia se obține din a doua prin inducție după n .

- (ii) Scriem $A = 1 + a_1X + a_2X^2 + \dots$ și $B = 1 + b_1X + b_2X^2 + \dots$. Dacă egalăm coeficienții în $A'B = AB'$, rezultă că $a_1 = b_1$, $a_1b_1 + 2a_2 = a_1b_1 + 2b_2$, $a_1b_2 + 2a_2b_1 + 3a_3 = a_2b_1 + 2a_1b_2 + 3b_3, \dots$. De aici rezultă printr-o inducție ale cărei detalii sunt ușoare că $a_1 = b_1$, $a_2 = b_2$, $a_3 = b_3, \dots$, deci $A = B$.
- (iii) Rezultă imediat din identificarea coeficienților.

35. (i) Avem $F'_i = \sum_{j \geq 1} ja_{ij}X^{j-1} = \sum_{j \geq 1} (j+1)a_{i,j+1}X^j$, și cum pentru orice j șirul $((j+1)a_{i,j+1})_{i \geq 0}$ conține doar un număr finit de elemente nenule, rezultă că familia $(F'_i)_{i \geq 0}$ este sumabilă. Cum $\sum_{i \geq 0} (j+1)a_{i,j+1} = (j+1)b_{j+1}$, obținem 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}, \dots, F_{i_s} , au coeficientul vreunui X^r , cu $r \leq j$, nenul. Atunci pentru orice $i \neq i_1, \dots, i_s$ seria formală GF_i are coeficienții lui X^r cu $r \leq j$ nuli. Prin urmare familia $(F_iG)_{i \geq 0}$ este sumabilă și egalitatea coeficienților lui X^j din $(\sum_{i \geq 0} F_i)G$ și $\sum_{i \geq 0} F_iG$ rezultă din egalitatea $(F_{i_1} + \dots + F_{i_s})G = F_{i_1}G + \dots + F_{i_s}G$.

36. (i) Deoarece familia $(\frac{1}{n!}f^n)_{n>0}$ este sumabilă, rezultă din problema 35(ii) că și familia $(\frac{1}{(n-1)!}f^{n-1}f')_{n>0}$, care constă din derivatele seriilor formale din prima familie, este sumabilă și 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 $\log(g) = -\sum_{n>0} \frac{1}{n}f^n$ și aplicând problema 35(ii) obținem 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. Obținem 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 $(\exp(\log(g)))' = \exp(\log(g))(\log(g))'$ și 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 $g = \exp(f)$ obținem 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

$$\begin{aligned} \exp(f+h) &= 1 + \sum_{n>0} \frac{1}{n!} (f+h)^n \\ &= \sum_{n \geq 0} \frac{1}{n!} (f+h)^n \\ &= \sum_{n \geq 0} \sum_{0 \leq i \leq n} \frac{1}{i!(n-i)!} f^i h^{n-i} \\ &= \left(\sum_{m \geq 0} \frac{1}{m!} f^m \right) \left(\sum_{p \geq 0} \frac{1}{p!} h^p \right) \\ &= \exp(f) \exp(h). \end{aligned}$$

(vi) Din (iii) și (iv) rezultă că \exp și \log sunt funcții inverse una celeilalte, iar din (v) rezultă că \exp (deci și \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 $g^M = \phi_N^{-1}(1+X)$, și 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 $Ma = Nb$ și atunci $(\phi_N^{-1}(1+X))^a = g^{Ma} = g^{Nb} = (\phi_M^{-1}(1+X))^b$, adică definiția lui $(1+X)^\alpha$ nu depinde de reprezentarea lui α ca fracție rațională.

(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 $f \in U_1(K[[X]])$, obținem că $\log(f^{\frac{1}{N}}) = \frac{1}{N} \log(f)$, de unde pentru orice a întreg avem $\frac{a}{N} \log(f) = \log(f^{\frac{a}{N}})$. Așadar $\log(f^\alpha) = \alpha \log(f)$ 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 $\alpha \log(1+X) = -\sum_{m>0} \frac{\alpha}{m} (-X)^m$ și

$$\begin{aligned} (1+X)^\alpha &= \exp(\alpha \log(1+X)) \\ &= 1 + \sum_{n>0} \frac{\alpha^n}{n!} \left(\sum_{m>0} \frac{(-X)^m}{m} \right)^n. \end{aligned}$$

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 funcție polinomială de α .

(iv) Din (iii) avem că există polinoame $P_1, P_2, \dots \in K[T]$ astfel încât

$$(1+X)^\alpha = 1 + P_1(\alpha)X + P_2(\alpha)X^2 + \dots$$

pentru orice $\alpha \in \mathbb{Q}$. Fixăm un $j > 0$ și arătăm că $P_j(T) = \frac{1}{j!} T(T-1) \dots (T-j+1)$. Deoarece pentru orice $n \geq j$ avem din binomul lui Newton că $(1+X)^n = 1 + C_n^1 X + C_n^2 X^2 + \dots + C_n^n X^n$, privind coeficientul lui X^j obținem că $P_j(n) = C_n^j = \frac{1}{j!} n(n-1) \dots (n-j+1)$. Prin urmare dacă notăm $F(T) = \frac{1}{j!} T(T-1) \dots (T-j+1)$, avem că $P_j(n) = F(n)$ pentru orice n întreg, $n \geq j$. Deoarece funcțiile polinomiale atașate polinoamelor P_j și F sunt egale pentru o infinitate de valori, rezultă că $P_j = F$, deci $P_j(\alpha) = \frac{\alpha(\alpha-1) \dots (\alpha-j+1)}{j!} = \binom{\alpha}{j}$ pentru orice α rațional, ceea ce încheie soluția.

38. (i) Avem

$$\begin{aligned} F^2 &= X^2 + (T_1 T_2 + T_2 T_1) X^3 + \dots + (T_1 T_{n-1} + \dots + T_{n-1} T_1) X^n + \dots \\ &= T_2 X^2 + T_3 X^3 + \dots + T_n X^n + \dots \\ &= F - X \end{aligned}$$

(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

$$(1 + Y)^{1/2} = 1 + \binom{1/2}{1}Y + \dots + \binom{1/2}{n}Y^n + \dots$$

care rezultă din Problema 37(iv) pentru $\alpha = 1/2$ în inelul $\mathbb{Q}[[Y]]$ și facem "schimbarea de variabilă" $Y = -4X$. Obținem formula

$$\phi_2^{-1}(1 - 4X) = 1 + (-4)\binom{1/2}{1}X + \dots + (-4)^n\binom{1/2}{n}X^n + \dots \quad (11.1)$$

Riguros, această "schimbare de variabilă" se poate explica astfel. Rezultă printr-o verificare imediată că aplicația $\Psi : \mathbb{Q}[[Y]] \rightarrow \mathbb{Q}[[X]]$ definită prin

$$\Psi(a_0 + a_1Y + \dots + a_nY^n + \dots) = a_0 + (-4)a_1X + \dots + (-4)^na_nX^n + \dots$$

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 $\phi_2^{-1}(1 - 4X) = \Psi((1 + Y)^{1/2})$. Ținând cont de formula pentru $(1 + Y)^{1/2}$ din Problema 37(iv) și de definiția lui Ψ , obținem formula (11.1). Atunci coeficientul lui X^n din $\phi_2^{-1}(1 - 4X)$ este

$$\begin{aligned} (-4)^n \binom{1/2}{n} &= \frac{\frac{1}{2}(\frac{1}{2} - 1) \dots (\frac{1}{2} - n + 1)}{n!} \cdot (-4)^n \\ &= \frac{1 \cdot (-1) \cdot (-3) \cdot \dots \cdot (-(2n - 3))}{2^n \cdot n!} \cdot (-4)^n \\ &= \frac{(-1)^{n-1} \cdot 1 \cdot 3 \cdot \dots \cdot (2n - 3)}{n!} \cdot (-1)^n \cdot 2^n \\ &= -\frac{1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot (2n - 3) \cdot (2n - 2)}{n! \cdot 2 \cdot 4 \cdot \dots \cdot (2n - 2)} \cdot 2^n \\ &= -\frac{(2n - 2)!}{n! \cdot 2^{n-1} \cdot (n - 1)!} \cdot 2^n \\ &= -\frac{2}{n} C_{2n-2}^{n-1} \end{aligned}$$

ceea ce demonstrează formula dorită.

(iv) Rezultă imediat prin identificarea coeficienților lui X^n în $F = \frac{1}{2} -$

$\frac{1}{2}\phi_2^{-1}(1 - 4X)$, dacă ținem 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 relație modulo (f) , obținem $\widehat{0} = \widehat{g}\widehat{h}$. Inelul K fiind corp, rezultă că $\widehat{g} = \widehat{0}$ sau $\widehat{h} = \widehat{0}$, adică $f|g$ (și h este inversabil) sau $f|h$ (și 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 așadar $\widehat{g} \in K \setminus \{\widehat{0}\}$. 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 obține $\widehat{g}\widehat{G} = \widehat{1}$, 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 aplicația $j : Q \rightarrow L$, $j(a) = \widehat{a}$ pentru orice $a \in Q$, este morfism de corpuri. Considerăm acum o mulțime M disjunctă de L și pentru care există o bijecție $u : M \rightarrow L \setminus j(Q)$ (există astfel de mulțimi, de exemplu $(L \setminus j(Q)) \times \{L\}$). Definim $v : Q \cup M \rightarrow L$,

$$v(x) = \begin{cases} u(x), & x \in M \\ j(x), & x \in Q \end{cases}$$

Din definiția lui v și din proprietățile funcțiilor u și j rezultă imediat că v este bijectivă. Pe mulțimea $k = Q \cup M$ definim operațiile $x \oplus y = v^{-1}(v(x) + v(y))$ și $x \otimes y = v^{-1}(v(x)v(y))$. Se arată fără dificultate că aceste operații definesc pe k o structură de corp comutativ.

Prezentăm ca exemplu verificarea distributivității. Fie $x, y, z \in k$. Atunci

$$\begin{aligned} x \otimes (y \oplus z) &= v^{-1}(v(x)v(y \oplus z)) \\ &= v^{-1}(v(x)v(v^{-1}(v(y) + v(z)))) \\ &= v^{-1}(v(x)(v(y) + v(z))) \\ &= v^{-1}(v(x)v(y) + v(x)v(z)) \\ &= v^{-1}(v(v^{-1}(v(x)v(y))) + v(v^{-1}(v(x)v(z)))) \\ &= v^{-1}(v(x \otimes y) + v(x \otimes z)) \\ &= (x \otimes y) \oplus (x \otimes z). \end{aligned}$$

Să observăm acum că v este izomorfism de corpuri. Într-adevăr, pentru orice $x, y \in k$ avem $v(x \oplus y) = v(v^{-1}(v(x) + v(y))) = v(x) + v(y)$ și $v(x \otimes y) =$

$v(v^{-1}(v(x)v(y))) = v(x)v(y)$. În plus, $v(1) = j(1) = 1$.

Prin urmare, v este morfism de corpuri. Cum v este și bijecție, rezultă că v este izomorfism. În consecință, (k, \oplus, \otimes) este un corp comutativ. Cum pentru orice $x, y \in Q$ avem $x \oplus y = x + y$ și $x \otimes y = xy$, rezultă că Q este subcorp al lui k . Dacă punem acum $g = a_0 + a_1X + \cdots + a_rX^r$, atunci

$$\begin{aligned} g(v^{-1}(\hat{X})) &= a_0 \oplus a_1 \otimes v^{-1}(\hat{X}) \oplus \cdots \oplus a_r \otimes v^{-1}(\hat{X})^r \\ &= v^{-1}(j(a_0) + j(a_1)\hat{X} + \cdots + j(a_r)\hat{X}^r) \\ &= v^{-1}(\hat{a}_0 + \hat{a}_1\hat{X} + \cdots + \hat{a}_r\hat{X}^r) \\ &= v^{-1}(a_0 + a_1\widehat{X} + \cdots + a_rX^r) \\ &= 0. \end{aligned}$$

În concluzie, $v^{-1}(\hat{X}) \in k$ este rădăcină pentru g (deci și pentru f).

(iii) Procedăm prin inducție după $n = \text{grad } f$. Dacă $n = 1$, atunci putem lua $K = Q$. Fie acum $n > 1$. Presupunem afirmația adevărată pentru toate polinoamele de grad mai mic decât n . Conform punctului (ii), există un corp K_1 care conține Q ca subcorp și în care f are cel puțin 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 inducție, există un corp K în care f_1 are toate rădăcinile și care conține pe K_1 ca subcorp. Deci K conține pe Q ca subcorp și întrucât f are drept rădăcini exact pe a și 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 $a = p^t a'$, $t \in \mathbb{N}^*$, $a' \in \mathbb{Z}$ și $(a', p) = 1$. 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 $X^n - a$ 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 $p | x$ și fie $x = p^s y$, cu $y \in \mathbb{Z}$ și $(p, y) = 1$. Cum $p^t | m$, avem și $p^t | x^n - a = p^{ns} y^n - p^t a'$, de unde $p^t | p^{ns} y^n$, ceea ce garantează că $t \leq ns$. Atunci avem și $hn < ns$, de unde deducem că $h < s$. Deci $h+1 \leq s$. Dar $p^{ns} | x^n$, deci și $p^{n(h+1)} | x^n$, adică $m | x^n$. Cum $m | x^n - a$, obținem că $m | a$, adică $(h+1)n < t$, contradicție. Așadar t trebuie să fie multiplu de n .

41. Procedăm prin inducție după n . Dacă $n = 1$, se știe că un polinom nenul într-o nedeterminată peste un domeniu de integritate are un număr de

rădăcini $\leq \deg(f)$, deci funcția polinomială asociată are doar un număr finit de zerouri.

Presupunem adevărat pentru $n - 1$ și demonstrăm pentru n . Scriem

$$f(X_1, \dots, X_n) = \sum_{0 \leq i \leq m} f_i(X_1, \dots, X_{n-1})X_n^i$$

unde $f_i(X_1, \dots, X_{n-1}) \in K[X_1, \dots, X_{n-1}]$ pentru orice $0 \leq i \leq m$. Rezultă că pentru orice $a_1 \in A_1, \dots, a_{n-1} \in A_{n-1}$, funcția polinomială asociată polinomului

$$f(a_1, \dots, a_{n-1}, X_n) = \sum_{0 \leq i \leq m} \tilde{f}_i(a_1, \dots, a_{n-1})X_n^i \in R[X_n]$$

se anulează pentru orice $a_n \in A_n$. Cum mulțimea A_n este infinită, rezultă că polinomul $f(a_1, \dots, a_{n-1}, X_n)$ este nul, deci $\tilde{f}_i(a_1, \dots, a_{n-1}) = 0$ pentru orice $0 \leq i \leq m$. Din ipoteza de inducție rezultă că $f_i(X_1, \dots, X_{n-1}) = 0$ pentru orice $0 \leq i \leq m$. Atunci evident $f = 0$.

Dacă \tilde{f} se anulează într-o mulțime infinită care nu mai este de forma $A_1 \times \dots \times A_n$ 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 afirmația în cazul în care f constă dintr-un singur monom (prin sumare se obține apoi rezultatul pentru un polinom arbitrar). Fie $X_1^{k_1} \dots X_n^{k_n}$ un monom care apare în scrierea lui f . Pentru fiecare $1 \leq i \leq n$ folosim teorema de împărțire cu rest și obținem $X_i^{k_i} = (X_i^q - X_i)q_i(X_i) + r_i(X_i)$, unde $q_i, r_i \in K[X_i]$ cu $\text{grad } r_i < q$. Înmulțind aceste relații obținem $f = \sum_{1 \leq i \leq n} (X_i^q - X_i)g_i + r_1 \dots r_n$, și notând $g_0 = r_1 \dots r_n$, toate condițiile dorite sunt satisfăcute.

43. Procedăm prin inducție după n la fel ca la problema 41.

44. Rezultă imediat din problemele 41 și 42 dacă ținem cont de faptul că $x^q = x$ pentru orice $x \in K$.

45. Fie $|K| = q$. Numărul funcțiilor de la K^n la K este q^{q^n} . Pe de altă parte orice funcție 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 și cu ele putem forma q^{q^n} polinoame cu coeficienți în K . Dar funcțiile polinomiale asociate acestor polinoame sunt distincte din problema 42, de unde rezultă că avem exact q^{q^n} funcții polinomiale de la K^n la K . De aici rezultă că orice funcție $\phi : K^n \rightarrow K$ este polinomială.

46. (i) Presupunem că $\tilde{f}(a) \neq 0$ pentru orice $a \neq (0, \dots, 0)$. Fie polinoamele $g = 1 - f^{q-1}$ și $h = (1 - X_1^{q-1}) \cdots (1 - X_n^{q-1})$. Atunci, pentru orice $a \neq (0, \dots, 0)$ avem $\tilde{h}(a) = 0$ (deoarece $x^{q-1} = 1$ pentru orice $x \in K$, $x \neq 0$) și $\tilde{g}(a) = 1 - (\tilde{f}(a))^{q-1} = 0$ (deoarece $\tilde{f}(a) \in K - \{0\}$). Pentru $a = (0, \dots, 0)$ 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 $g_i \in K[X_1, \dots, X_n]$

pentru orice $0 \leq i \leq n$, $\deg_{X_i}(g_0) < q$ pentru orice $1 \leq i \leq n$, și $\deg(g_0) \leq \deg(g) = d(q-1)$. Este clar că $\tilde{g}_0 = \tilde{g}$, de unde $\tilde{g}_0 = \tilde{h}$. Aplicând problema 42 (observăm că g_0 și h satisfac condițiile impuse asupra gradelor, căci și $\deg_{X_i}(h) < q$), rezultă că $g_0 = h$. Dar $\deg(g_0) \leq \deg(g) < \deg(h)$, contradicție. Așadar presupunerea făcută este falsă.

(ii) Am văzut în soluția punctului (i) că $\tilde{g}(a) = 1$ dacă $\tilde{f}(a) = 0$ iar $\tilde{g}(a) = 0$ dacă $\tilde{f}(a) \neq 0$. Așadar $N1_K = \sum_{a \in K^n} \tilde{g}(a)$. Dar $\tilde{g} = \tilde{g}_0$ și din soluția problemei

41 știm că $g_0 = r_1 \cdots r_n$, unde $r_1 \in K[X_1], \dots, r_n \in K[X_n]$, toate de grad mai mic decât q . Rezultă că g_0 se poate scrie sub forma

$$g_0 = \sum_{0 \leq i_1, \dots, i_n < q} c_{i_1} \cdots c_{i_n} X_1^{i_1} \cdots X_n^{i_n}$$

și de aici rezultă că

$$\begin{aligned} N1_K &= \sum_{(a_1, \dots, a_n) \in K^n} \left(\sum_{0 \leq i_1, \dots, i_n < q} c_{i_1} \cdots c_{i_n} a_1^{i_1} \cdots a_n^{i_n} \right) \\ &= \sum_{0 \leq i_1, \dots, i_n < q} c_{i_1} \cdots c_{i_n} \left(\sum_{(a_1, \dots, a_n) \in K^n} a_1^{i_1} \cdots a_n^{i_n} \right). \end{aligned}$$

Dar $\sum_{(a_1, \dots, a_n) \in K^n} a_1^{i_1} \cdots a_n^{i_n} = \left(\sum_{a_1 \in K} a_1^{i_1} \right) \cdots \left(\sum_{a_n \in K} a_n^{i_n} \right)$ și cum $\deg(g_0) \leq \deg(g) =$

$d(q-1) < n(q-1)$, rezultă că nu toți indicii i_1, \dots, 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 $K^* = \{1, \alpha, \alpha^2, \dots, \alpha^{q-2}\}$. Avem $\alpha^i - 1 \neq 0$ pentru orice $i \geq 0$ și

$$\begin{aligned} \sum_{x \in K} x^i &= \sum_{0 \leq j \leq q-2} \alpha^{ij} \\ &= (\alpha^{(q-1)i} - 1)(\alpha^i - 1)^{-1} \\ &= ((\alpha^{(q-1)})^i - 1)(\alpha^i - 1)^{-1} \\ &= 0. \end{aligned}$$

Rezultă că $\sum_{(a_1, \dots, a_n) \in K^n} a_1^{i_1} \dots a_n^{i_n} = 0$ pentru orice i_1, \dots, i_n . Obținem că $N1_K = 0$, deci $p|N$.

47. Fie $K^* = \{b_1, \dots, b_{q-1}\}$. Avem că $b_i^{q-1} = 1$ pentru orice i . Considerăm matricea

$$B = \begin{pmatrix} 1 & b_1 & \dots & b_1^{q-2} \\ \dots & \dots & \dots & \dots \\ 1 & b_{q-1} & \dots & b_{q-1}^{q-2} \end{pmatrix} \in M_{q-1}(K).$$

Atunci avem

$$BA = \begin{pmatrix} f(b_1) & b_1^{-1}f(b_1) & \dots & b_1^{-(q-2)}f(b_1) \\ \dots & \dots & \dots & \dots \\ f(b_{q-1}) & b_{q-1}^{-1}f(b_{q-1}) & \dots & b_{q-1}^{-(q-2)}f(b_{q-1}) \end{pmatrix}.$$

$N = |\{a \in K^* \mid \tilde{f}(a) = 0\}|$ este numărul de zerouri din șirul $f(b_1), \dots, f(b_{q-1})$. Să presupunem de exemplu că ultimii N termeni ai acestui șir 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 și primele $(q-1-N)$ coloane este nenul (determinantul este un determinant de tip Vandermonde înmulțit cu elementele nenule $f(b_1), \dots, f(b_{q-1-N})$), deci $\text{rang}(BA) = q-1-N$. Cum B este inversabilă, rezultă că $\text{rang}(A) = q-1-N$. De aici obținem că $N = q-1-\text{rang}(A)$.

48. (i) ” \Rightarrow ” Fie $s \in S$ și 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, contradicție.

" \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, obținem 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 și surjectivă.

49. (i) Se verifică imediat că $S^{-1}I$ este ideal în $S^{-1}R$. Fie $\phi : R \rightarrow S^{-1}R$, $\phi(a) = a/1$, morfismul canonic, și 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 $a \in I$, și atunci $a/s \in S^{-1}I$. Invers, dacă $a \in I$ și $s \in S$, atunci $a/1 = \phi(a) \in J$ și $a/s = (1/s)(a/1) \in J$.

(ii) Dacă $S^{-1}I = S^{-1}R$, atunci $1/1 \in S^{-1}I$, deci există $a \in I$ și $s \in S$ cu $a/s = 1/1$. De aici rezultă că există $t \in S$ cu $t(a-s) = 0$, deci $ta = ts \in I \cap S$ și obținem 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 $\pi : R \rightarrow R/I$ proiecția canonică și $\psi : R/I \rightarrow T^{-1}(R/I)$ 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 $T^{-1}(R/I)$), și aplicând proprietatea de universalitate a inelelor de fracții obținem un morfism $v : S^{-1}R \rightarrow T^{-1}(R/I)$ astfel încât $v(a/s) = \hat{a}/\hat{s}$. Este clar că v este surjectiv și

$$\begin{aligned} \text{Ker}(v) &= \{a/s \mid \hat{a}/\hat{s} = \hat{0}/\hat{1}\} \\ &= \{a/s \mid \text{există } t \in S \text{ cu } \hat{t}\hat{a} = \hat{0}\} \\ &= \{a/s \mid \text{există } t \in S \text{ cu } ta \in I\} \\ &= S^{-1}I. \end{aligned}$$

Rezultă că v induce un izomorfism de inele între $S^{-1}R/S^{-1}I$ și $T^{-1}(R/I)$.

(iv) Verificare imediată.

50. (i) Din problema 48(ii) obținem că $S^{-1}p \neq S^{-1}R$, iar din punctul (iii) al aceleiași probleme avem că $S^{-1}R/S^{-1}p \simeq T^{-1}(R/p)$. Dar R/p este inel integru, deci orice inel de fracții 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 $P \in \text{Spec}(S^{-1}R)$. 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 $c \in p$ și $s \in S$ 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 aplicația $p \mapsto S^{-1}p$ este o corespondență bijectivă între $\text{Spec}(R) \cap \Sigma$ și $\text{Spec}(S^{-1}R)$.

(iii) Fie $P \in \text{Spec}(S^{-1}R)$. Atunci există $q \in \text{Spec}(R)$, $q \cap S = \emptyset$, cu $P = S^{-1}q$. Deoarece $S = R - p$ și $q \cap S = \emptyset$, 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 fracții al inelului R/p . În particular $S^{-1}p \in \text{Max}(S^{-1}R)$. În consecință $S^{-1}p$ este unicul ideal maximal al lui $S^{-1}R$.

51. Fie R inel noetherian, S un sistem multiplicativ al său și 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 $I = (a_1, \dots, a_n)$. Evident, $(\frac{a_1}{1}, \dots, \frac{a_n}{1}) \subseteq J$. Dacă $y \in J$, atunci există $a \in I$ și $s \in S$ astfel ca $y = \frac{a}{s}$. Dar x fiind în I se poate scrie sub forma $\alpha_1 a_1 + \dots + \alpha_n a_n$, unde $\alpha_1, \dots, \alpha_n \in R$. De aici rezultă că $y = \frac{\alpha_1}{s} \cdot \frac{a_1}{1} + \dots + \frac{\alpha_n}{s} \cdot \frac{a_n}{1}$. Prin urmare, $J = (\frac{a_1}{1}, \dots, \frac{a_n}{1})$, 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 $m \in \text{Max}(R)$, avem $R \subseteq \bigcap_{m \in \text{Max}(R)} R_m$. Reciproc, fie $x \in \bigcap_{m \in \text{Max}(R)} R_m$. Atunci pentru orice $m \in \text{Max}(R)$ există $a_m \in R$, $b_m \in R - m$, cu $x = a_m/b_m$. Pe de altă parte, idealul I generat de

mulțimea $\{b_m \mid m \in \text{Max}(R)\}$ este egal cu R , altfel ar exista $n \in \text{Max}(R)$ cu $I \subseteq n$, și atunci $b_n \in n$, contradicție. Obținem că $1 = \sum_{1 \leq i \leq s} c_i b_{m_i}$, unde $m_1, \dots, m_s \in \text{Max}(R)$ și $c_1, \dots, c_s \in R$. 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 $u : R \rightarrow R[X]/(aX - 1)$ morfismul obținut prin compunerea proiecției canonice $R[X] \rightarrow R[X]/(aX - 1)$ cu incluziunea canonică $R \rightarrow R[X]$. În inelul $R[X]/(aX - 1)$ avem $\hat{a}\hat{X} = \hat{1}$, deci \hat{a} este un element inversabil și inversul său este \hat{X} . Rezultă că $u(S) \subseteq U(R[X]/(aX - 1))$. Din proprietatea de universalitate a inelelor de fracții există un morfism de inele $\bar{u} : S^{-1}R \rightarrow R[X]/(aX - 1)$ cu $\bar{u}(r/a^n) = \hat{r}\hat{X}^n$.

Din proprietatea de universalitate a inelelor de polinoame rezultă că există un morfism de inele $v : R[X] \rightarrow S^{-1}R$ cu $v(X) = 1/a$. Este evident că $(aX - 1) \subseteq \text{Ker}(v)$, deci există un morfism de inele $\bar{v} : R[X]/(aX - 1) \rightarrow S^{-1}R$ cu $\bar{v}(\hat{X}) = 1/a$.

Un calcul simplu arată că $\bar{u} \circ \bar{v}$ și $\bar{v} \circ \bar{u}$ sunt aplicațiile identice, deci \bar{u} este izomorfism între $S^{-1}R$ și $R[X]/(aX - 1)$.

56. Fie $\pi : R \rightarrow R/\text{Ker}(\phi)$ proiecția canonică. Atunci avem $\pi(S) \subseteq U(R/\text{Ker}(\phi))$, altfel ar exista $s \in S$ cu $\hat{s} \notin U(R/\text{Ker}(\phi))$, și atunci \hat{s} este divizor al lui zero în $R/\text{Ker}(\phi)$ (deoarece într-un inel comutativ finit orice element este sau inversabil sau divizor al lui zero), deci ar exista $a \in R - \text{Ker}(\phi)$ cu $\hat{s}\hat{a} = 0$. Aceasta înseamnă că $sa \in \text{Ker}(\phi)$, deci există $t \in S$ cu $t\hat{s}\hat{a} = 0$. Cum $ts \in S$, obținem că $a \in \text{Ker}(\phi)$, contradicție.

Acum folosind proprietatea de universalitate a inelelor de fracții găsim un morfism $\psi : S^{-1}R \rightarrow R/\text{Ker}(\phi)$. Este clar că $\bar{\phi}\psi = \text{Id}$, unde $\bar{\phi} : R/\text{Ker}(\phi) \rightarrow S^{-1}R$ este morfismul canonic care se obține din ϕ . Deci $\bar{\phi}$ este un morfism surjectiv (chiar izomorfism), de unde $\phi = \bar{\phi}\pi$ este surjectiv.

Considerăm acum $R = \mathbb{Z}_{12}$ și $d = 2$. Presupunem că ar exista un sistem multiplicativ S al lui R cu $S^{-1}R \simeq \mathbb{Z}_2$. Cum $S^{-1}R \simeq R/\text{Ker}(\phi)$, unde $\phi : R \rightarrow S^{-1}R$ este morfismul canonic, rezultă că $\text{Ker}(\phi) = \hat{2}\mathbb{Z}_{12}$. Atunci $\hat{2} \in \text{Ker}(\phi)$, deci există $s \in S$ cu $\hat{2}\hat{s} = \hat{0}$. Aceasta arată că $2s \in 12\mathbb{Z}$, adică $s \in 6\mathbb{Z}$, și atunci $\hat{0} = \hat{s}^2 \in S$, contradicție.

57. Fie $S = \{a \in R \mid a \neq 0 \text{ și } 1/a \in A\}$. Este clar că S este sistem

multiplicativ al lui R și că $S^{-1}R \subseteq A$. Arătăm acum că $A \subseteq S^{-1}R$. Fie $x \in A$. Atunci $x = a/b$ pentru niște $a, b \in R$, $b \neq 0$. Cum idealul (a, b) este principal, există $c \in R$ cu $(a, b) = (c)$. Atunci există $a', b', \alpha, \beta \in R$ cu $a = ca'$, $b = cb'$ și $c = a\alpha + b\beta$. Obținem că $x = a'/b'$ și $1a'\alpha + b'\beta$, 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 $R = \mathbb{Z}[i\sqrt{3}]$ și $A = \mathbb{Z}[(1 + i\sqrt{3})/2]$. Calcule directe arată că $U(R) = \{-1, 1\}$ și $U(A) = \{-1, 1, \frac{1}{2} + i\sqrt{3}, -\frac{1}{2} + i\sqrt{3}, \frac{1}{2} - i\sqrt{3}, -\frac{1}{2} - i\sqrt{3}\}$. 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 $A = R$, contradicție.

58. Folosind proprietatea de universalitate a inelelor de polinoame găsim un morfism de inele $u : R[X] \rightarrow (S^{-1}R)[X]$ astfel încât $u(a) = a/1$ pentru orice $a \in R$ și $u(X) = X$. Deoarece $u(S) \subseteq U((S^{-1}R)[X])$, din proprietatea de universalitate a inelelor de fracții deducem că există un morfism de inele $\bar{u} : S^{-1}(R[X]) \rightarrow (S^{-1}R)[X]$ care extinde pe u .

Fie $q : R \rightarrow R[X]$ morfismul canonic și $v : S^{-1}R \rightarrow S^{-1}(R[X])$ morfismul definit prin $v(a/s) = q(a)/s$. Folosind proprietatea de universalitate a inelelor de polinoame obținem că există un morfism de inele $\bar{v} : (S^{-1}R)[X] \rightarrow S^{-1}(R[X])$ care extinde pe v și pentru care $\bar{v}(X) = X$.

Este imediat că $\bar{u} \circ \bar{v} = \text{Id}$ și $\bar{v} \circ \bar{u} = \text{Id}$, ceea ce arată că $S^{-1}(R[X])$ și $(S^{-1}R)[X]$ sunt izomorfe canonic.

Pentru serii formale putem defini un morfism canonic $\psi : S^{-1}(R[[X]]) \rightarrow (S^{-1}R)[[X]]$ prin $\psi(f/s) = \sum_{n \geq 0} (a_n/s)X^n$, unde $f = \sum_{n \geq 0} a_nX^n$. 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, $R = K[Y_0, Y_1, \dots, Y_n, \dots]/(Y_0Y_1, Y_0^2Y_2, \dots, Y_0^nY_n, \dots)$, $S = \{\hat{Y}_0^n \mid n \in \mathbb{N}\}$ și $f = \sum_{n \geq 0} \hat{Y}_nX^n$. 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 și $g = \sum_{n \geq 0} (1/p^n)X^n \in \mathbb{Q}[[X]]$.

Dacă ar exista $f \in \mathbb{Z}[[X]]$, $f = \sum_{n \geq 0} a_nX^n$, și $s \in S$ 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 $s = 0$, contradicție. Rezultă că ψ nu este surjectiv.

59. Este evident că S este sistem multiplicativ al lui R . Fie $\phi_i : R_i \rightarrow$

$S_i^{-1}R_i$, $i \in I$, morfismele canonice și fie $\phi = \prod_{i \in I} \phi_i : R \rightarrow \prod_{i \in I} (S_i^{-1}R_i)$. Deoarece $\phi(S) \subseteq U(\prod_{i \in I} (S_i^{-1}R_i))$, putem folosi proprietatea de universalitate a inelelor de fracții și obținem că există un morfism $u : S^{-1}R \rightarrow \prod_{i \in I} (S_i^{-1}R_i)$ 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 $m \in \text{Max}(R)$ avem $(a/1)^n = 0$ în R_m , și 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 raționament similar cu cel de la problema 53 arată că $a = 0$.

Proprietatea nu mai rămâne adevărată dacă în loc de redus considerăm integrul. Fie K un corp comutativ și $R = K \times K$. Idealele maximale ale lui R sunt $K \times \{0\}$ și $\{0\} \times K$. Pentru $m = K \times \{0\}$ avem $S = R - m = K^* \times K$. Atunci este ușor de văzut că pentru $(a, b), (c, d) \in R$ și $(\alpha, \beta), (\gamma, \delta) \in S$ avem că $(a, b)/(\alpha, \beta) = (c, d)/(\gamma, \delta)$ dacă și numai dacă $a\gamma - c\alpha = 0$, adică $a/\alpha = c/\gamma$. Aceasta arată că asocierea $(a, b)/(\alpha, \beta) \mapsto a/\alpha$ definește un izomorfism de inele între $R_m = S^{-1}R$ și K , în particular R_m este inel integrul. La fel, dacă $m = \{0\} \times K$, rezultă că $R_m \simeq K$, care este inel integrul. Este clar însă că R nu este inel integrul.

61. (i) Din definiție rezultă că $D_n(X_{\sigma(1)}, \dots, X_{\sigma(n)})$ este produs după toate perechile (i, j) cu $1 \leq i < j \leq n$ de niște 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

$$\begin{aligned} \Delta_n(X_{\sigma(1)}, \dots, X_{\sigma(n)}) &= (D_n(X_{\sigma(1)}, \dots, X_{\sigma(n)}))^2 \\ &= (\varepsilon(\sigma) D_n(X_1, \dots, X_n))^2 \\ &= (D_n(X_1, \dots, X_n))^2 \\ &= \Delta_n(X_1, \dots, X_n). \end{aligned}$$

(iii) Cum $f(X_1, \dots, X_i, \dots, X_j, \dots, X_n) = -f(X_1, \dots, X_j, \dots, X_i, \dots, X_n)$, rezultă că $2f(X_1, \dots, X_i, \dots, X_i, \dots, X_n) = 0$ și cum $\text{char}(K) \neq 2$ obținem că $f(X_1, \dots, X_i, \dots, X_i, \dots, X_n) = 0$. Atunci $X_i - X_j | f$ pentru orice $i < j$, de unde $D_n | f$. Rezultă că există $g \in K[X_1, \dots, X_n]$ cu $f = gD_n$. Este imediat că g este polinom simetric.

(iv) Fie $\tau \in S_n - A_n$. Definim

$$f_1(X_1, \dots, X_n) = 2^{-1}(f(X_1, \dots, X_n) + f(X_{\tau(1)}, \dots, X_{\tau(n)})).$$

Atunci pentru orice $\sigma \in S_n$ avem

$$f_1(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = 2^{-1}(f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) + f(X_{\tau\sigma(1)}, \dots, X_{\tau\sigma(n)})).$$

Dacă $\sigma \in A_n$, avem $\tau\sigma = (\tau\sigma\tau^{-1})\tau$ și $\tau\sigma\tau^{-1} \in A_n$, de unde

$$f_1(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = 2^{-1}(f(X_1, \dots, X_n) + f(X_{\tau(1)}, \dots, X_{\tau(n)})).$$

Dacă $\sigma \in S_n - A_n$, atunci $\sigma = (\sigma\tau^{-1})\tau$, cu $\sigma\tau^{-1} \in A_n$, și $\tau\sigma \in A_n$, de unde

$$f_1(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = 2^{-1}(f(X_{\tau(1)}, \dots, X_{\tau(n)}) + f(X_1, \dots, X_n)).$$

În ambele situații rezultă că $f_1(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = f_1(X_1, \dots, X_n)$, 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 $f - f_1 = f_2D_n$.

62. (i) Urmăm algoritmul din demonstrația teoremei fundamentale a polinoamelor simetrice. Polinomul dat este simetric și omogen de grad 6, și scăzând din el polinoame simetrice omogene de grad 6 vom obține 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 $k_1 \geq k_2 \geq k_3$ și $k_1 + k_2 + k_3 = 6$, 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. Așadar polinomul se scrie ca $s_1^2s_2^2 + as_1^3s_3 + bs_2^3 + cs_1s_2s_3 = ds_3^2$, și dând valori particulare nedeterminatelor obținem că $a = -4, b = -4, c = 18, d = -27$.

(ii) Se obține $(X_1^2 + X_2^2)(X_1^2 + X_3^2)(X_2^2 + X_3^2) = s_1^2s_2^2 - 2s_1^3s_3 - 2s_2^3 + 4s_1s_2s_3 - s_3^2$.

(iii) Notând cu f polinomul din enunț 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 $X_1^3 + \dots + X_n^3 = s_1^3 + as_1s_2 + bs_3$ și dând valori particulare nedeterminatelor găsim că $a = -3$, $b = 3$.

63. (i) Din relațiile $X_i^n - s_1X_i^{n-1} + \dots + (-1)^{n-1}s_{n-1}X_i + (-1)^n s_n = 0$, $1 \leq i \leq n$, obținem că $X_i^k - s_1X_i^{k-1} + \dots + (-1)^{n-1}s_{n-1}X_i^{k-n+1} + (-1)^n s_nX_i^{k-n} = 0$ pentru orice $k \geq n$. Sumând aceste relații obținem relația dorită.

(ii) Arătăm mai întâi că dacă un polinom $f \in K[X_1, \dots, X_n]$ este omogen de grad $q < n$ și are proprietatea că atunci când dăm valoarea zero la oricare $n - q$ dintre nedeterminatele X_1, \dots, 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 $aX_{i_1}^{k_1} \dots X_{i_s}^{k_s}$ cu $k_j \geq 1$ pentru orice $1 \leq j \leq s$ și $k_1 + \dots + k_s = q$. De aici rezultă în particular că $s \leq q$. Făcând X_i zero pentru orice $i \notin \{i_1, \dots, i_s\}$, obținem un polinom nenul, contradicție.

Considerăm acum polinomul simetric $f(X_1, \dots, X_n) = p_k - s_1p_{k-1} + \dots + (-1)^{k-1}s_{k-1}p_1 + (-1)^k ks_k$ pentru $k < n$. Avem că f este polinom omogen de grad k . Dar $f(X_1, \dots, X_k, 0, \dots, 0) = p'_k - s'_1p'_{k-1} + \dots + (-1)^{k-1}s'_{k-1}p'_1 + (-1)^k ks'_k$, unde $s'_j = s_j(X_1, \dots, X_k, 0, \dots, 0)$ și $p'_j = p_j(X_1, \dots, X_k, 0, \dots, 0)$. Cum s'_1, \dots, s'_k sunt polinoamele simetrice fundamentale în nedeterminatele X_1, \dots, X_k , rezultă din punctul (i), aplicat pentru $n = k$, că avem $f(X_1, \dots, X_k, 0, \dots, 0) = 0$. Cum f este polinom simetric, obținem că polinomul care rezultă atunci când dăm valoarea zero la oricare $n - k$ dintre nedeterminatele X_1, \dots, X_n este nul. Aceasta arată că $f = 0$.

64. Avem că polinoamele p_1, \dots, p_n evaluate pentru $X_1 = x_1, \dots, X_n = x_n$ sunt zero. Din formulele lui Newton rezultă că și polinoamele s_1, \dots, s_n evaluate pentru $X_1 = x_1, \dots, X_n = x_n$ sunt zero (de fapt, obținem că ks_k este zero când este evaluat pentru $X_1 = x_1, \dots, X_n = x_n$, și cum K are caracteristică zero rezultă că $s_k = 0$ pentru aceste valori). Aceasta înseamnă că x_1, \dots, x_n sunt rădăcini ale polinomului $X^n = 0$, deci $x_1 = \dots = x_n = 0$.

Concluzia nu mai este adevărată dacă $x_1^k + \dots + x_n^k = 0$ pentru n valori ale lui k care nu sunt neapărat consecutive. De exemplu, luăm $n = 2$, $x_1 = 1$, $x_2 = -1$ și atunci $x_1 + x_2 = 0$ și $x_1^3 + x_2^3 = 0$.

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 $x_1 + x_2 = \hat{0}$ și $x_1^2 + x_2^2 = \hat{0}$, dar $x_1, x_2 \neq \hat{0}$.

65. Folosim formulele lui Newton și obținem că, evaluat în x_1, x_2, x_3 ,

$$p_{10} = 621.$$

66. (i) Folosim formulele lui Newton și obținem că $x_1^i + \dots + x_n^i = -(a^i + b^i)$ pentru i impar și $x_1^i + \dots + x_n^i = -(a^{i/2} + b^{i/2})$ pentru i par.
- (ii) Înmulțim polinomul cu $(X - a)(X - b)$ și folosim formulele lui Newton pentru rădăcinile acestuia. Obținem că $x_1^i + \dots + x_n^i = -(a^i + b^i)$.

Capitolul 12

Soluții: Aritmetică în inele integre

1. Frațiile pe care le vom scrie sunt elemente din corpul de fracții al domeniului în care lucrăm.

(i) Notăm $R = \mathbb{Z}[i]$, $a = 1 + i$, $b = 2 + i$, $c = 1 - i$, $d = 1 + 2i$, $e = 1 - 2i$ și $f = -2 + i$. Vom studia relațiile între elementele a și b .

Metoda I. $\frac{a}{b} = \frac{(1+i)(2-i)}{5} = \frac{3}{5} + \frac{1}{5}i \notin R$. Prin urmare, $b \nmid a$ și $b \not\sim a$.

$\frac{b}{a} = \frac{5}{3+i} = \frac{3}{2} - \frac{1}{2}i \notin R$, deci $a \nmid b$.

Metoda II. Avem (vezi problema 2) $N(a) = 2 \nmid_{\mathbb{Z}} 5 = N(b)$, deci conform problemei 3(i), $a \nmid b$ (și, evident, $a \not\sim b$). De asemenea, $N(b) \nmid_{\mathbb{Z}} N(a)$, deci $b \nmid a$.

Cu considerații similare obținem $a \sim c$, $a \nmid d$, $b \nmid d$, $b \sim e$, $d \nmid a$, $d \nmid b$, $d \sim f$. Celelalte relații între elementele date se deduc imediat din cele deja menționate.

(ii) Procedând ca la punctul (i) obținem că nu există nicio pereche de elemente diferite a, b din mulțimea 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 și c . Avem: $\frac{b}{c} = \frac{\rho}{\rho+1} = \frac{\rho(1+\bar{\rho})}{(1+\rho)(1+\bar{\rho})} = \rho(1 - 1 - \rho) = -\rho^2 = 1 + \rho$.

Metoda I. $\frac{b}{c} = 1 + \rho \in R$, deci $c|b$; $\frac{c}{b} = \frac{1}{1+\rho} = \frac{1+\bar{\rho}}{(1+\rho)(1+\bar{\rho})} = 1 - 1 - \rho = -\rho \in R$, 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 considerații de același tip obținem $a \sim b \sim c|d \sim e$ și $d \nmid c$. 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 și nici nu se divide cu vreunul (cu excepția lui însuși). O afirmație similară este valabilă și 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, obținem $a \sim d$, $b \sim c$, și nu există nicio altă pereche de elemente diferite α, β din listă cu $\alpha|\beta$.

(v) Notăm $R = \mathbb{Q}[[X]]$. Se știe (vezi problema 26 din Capitolul 5) că elementele inversabile din R sunt seriile formale cu termen liber nenul.

Vom studia cazul elementelor $f = a_r X^r + a_{r+1} X^{r+1} + \dots$ și $g = b_s X^s + b_{s+1} X^{s+1} + \dots$. Avem $f = X^r \bar{f}$, unde $\bar{f} = a_r + a_{r+1} X + \dots \in U(R)$ și $g = X^s \bar{g}$, unde $\bar{g} = b_s + b_{s+1} X + \dots \in U(R)$. Dacă $r \leq s$, atunci $g = (X^{s-r} \bar{f}^{-1} \bar{g}) f$, deci $f|g$. Dacă $r > s$, $f = (X^{r-s} \bar{g}^{-1} \bar{f}) g$, deci $g|f$.

Prin urmare $f|g$ dacă și numai dacă $r \leq s$, iar $f \sim g$ dacă și numai dacă $r = s$. Toate relațiile care trebuie studiate se deduc de aici.

(vi) Notăm $R = \mathbb{Q} + X\mathbb{R}[X]$, $a = 2 + X$, $b = \frac{3}{7} + \frac{3}{14}X$, $c = 2\pi X + \pi X^2$, $d = \frac{\pi}{5}X + \frac{\pi}{10}X^2$, $e = 3\pi^2 X + \frac{3\pi^2}{2}X^2$ și $f = 2 + 3X + X^2$.

Avem $b = \frac{3}{14}a$ și $a = \frac{14}{3}b$, deci $a \sim b$. $c = \pi X \cdot a$, deci $a|c$. Presupunând $c|a$, ar exista $g \in R$ cu $a = cg$, relație valabilă și 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 divizibilității coincide cu cea a lui a . $d = \frac{1}{10}c$ și $c = 10 \cdot d$, 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 $\frac{3\pi}{2} \notin \mathbb{Q}$, contradicție. 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 relația în $\mathbb{R}[X]$, constatăm că grad $g = 0$, deci $g \in \mathbb{R} \cap R = \mathbb{Q}$. Pe de altă parte, comparând coeficienții dominanți din relația $f = gc$, obținem $g = \frac{1}{\pi}$, contradicție. Rămâne deci că $c \nmid f$. Analog se arată relațiile $f \nmid c$, $e \nmid f$ și $f \nmid e$. Cum $d \sim c$, comportarea lui d din punctul de vedere al divizibilității 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

$$\begin{aligned}
N(z_1 z_2) &= N(a_1 a_2 + db_1 b_2 + (a_1 b_2 + a_2 b_1)\sqrt{d}) \\
&= |(a_1 a_2 + db_1 b_2)^2 - d(a_1 b_2 + a_2 b_1)^2| \\
&= |a_1^2 a_2^2 + d^2 b_1^2 b_2^2 - da_1^2 b_2^2 - da_2^2 b_1^2| \\
&= |(a_1^2 - db_1^2)(a_2^2 - db_2^2)| \\
&= N(z_1)N(z_2).
\end{aligned}$$

Mai simplu, $N(z_1 z_2) = |z_1 z_2 \overline{z_1 z_2}| = |z_1 z_2 \overline{z_1} \overline{z_2}| = |z_1 \overline{z_1}| |z_2 \overline{z_2}| = N(z_1)N(z_2)$.

(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, și $z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$ cu $z = z_1 z_2$. 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. Așadar 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 aceștia 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 $N(z) = |z\overline{z}| = \left| \left(a + b\frac{1+\sqrt{d}}{2}\right) \left(a + b\frac{1-\sqrt{d}}{2}\right) \right| = \left| a^2 + ab + \frac{1-d}{4}b^2 \right| \in \mathbb{N}$.

Demonstrațiile date la punctele (iv) și (v) rămân valabile și 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 $a \in \mathbb{Z}$;

$b = \pm 1$, care duce la $a^2 = 109$, imposibil, pentru că $a \in \mathbb{Z}$;

$b = \pm 2$, care duce la $a^2 = 100$, de unde $z = \pm 10 \pm 2\sqrt{3}$;

$b = \pm 3$, care duce la $a^2 = 85$, imposibil, pentru că $a \in \mathbb{Z}$;

$b = \pm 4$, care duce la $a^2 = 64$, de unde $z = \pm 8 \pm 4\sqrt{3}$;

$b = \pm 5$, care duce la $a^2 = 37$, imposibil, pentru că $a \in \mathbb{Z}$;

$b = \pm 6$, care duce la $a^2 = 4$, de unde $z = \pm 2 \pm 6\sqrt{3}$, și

$|b| > 6$, care duce la $a^2 < 0$, imposibil.

Prin urmare, elementele de ordin 112 din $\mathbb{Z}[i\sqrt{3}]$ sunt $\pm 10 \pm 2\sqrt{3}$, $\pm 8 \pm 4\sqrt{3}$ și $\pm 2 \pm 6\sqrt{3}$.

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 $a \in \mathbb{Z}$ și $|b| > 4$, care duce la $a^2 < 0$, imposibil.

Prin urmare, în $\mathbb{Z}[i\sqrt{11}]$ nu există elemente de normă 112.

Fie $z = a + b\frac{1+i\sqrt{7}}{2} \in \mathbb{Z}\left[\frac{1+i\sqrt{7}}{2}\right]$ 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 $2a+b = 7k$. Relația 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 $b^2 = 36$ și $2a+b = \pm 14$;

$k = \pm 3$, care duce la $b^2 = 1$ și $2a+b = \pm 21$.

Înlocuind, deducem că elementele de normă 112 din inelul $\mathbb{Z}\left[\frac{1+i\sqrt{7}}{2}\right]$ sunt $\pm 4i\sqrt{7}, \pm 7 \pm 3i\sqrt{7}$ și $\frac{\pm 21 \pm i\sqrt{7}}{2}$.

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)) obținem $N(b) = N(a)N(c)$, deci $N(a)|N(b)$.

(ii) Notăm $R = \mathbb{Z}[i\sqrt{2}]$ și considerăm elementele $a = 3$ și $b = 1 + 2i\sqrt{2}$ 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 $a|_R b$ și $N(a) = N(b)$; există $c \in R$ astfel încât $b = ac$. Trecând la norme obținem $N(b) = N(a)N(c)$. Cum $N(a) = N(b)$, rezultă că $N(c) = 1$, deci $c \in U(R)$. Prin urmare, $a \sim_R b$.

(iv) Evident, $1|a$ și $1|b$. Fie acum $f \in \mathbb{Z}[\sqrt{d}]$ cu proprietatea că $f|a$ și $f|b$. Trecând la norme, obținem (conform (i)) $N(f)|N(a)$ și $N(f)|N(b)$, 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 și b în $\mathbb{Z}[\sqrt{d}]$.

(v) Nu neapărat. Să considerăm, de exemplu, elementele $a = 2$ și $b = 1 + i\sqrt{5}$ din inelul $R = \mathbb{Z}[i\sqrt{5}]$. Dacă $d \in R$ divide a și b , atunci, conform (i),

$N(d)|N(a)$ și $N(d)|N(b)$, 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 $1|_R a$ și $1|_R b$, rezultă că 1 e un c.m.m.d.c. pentru a și b în R . Avem însă $N(1) = 1 \neq 2 = (N(a), N(b))$.

(vi) Demonstrațiile de la punctele (i), (iii) și (iv) rămân valabile și 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 și numai dacă $N(z) = 1$, condiție care se rescrie $a^2 - db^2 = 1$. Procedând ca la problema 2(vii), constatăm că pentru $d = -1$ se obțin valorile $a = \pm 1, b = 0$ și $a = 0, b = \pm 1$, în timp ce pentru $d < -1$ relația de mai sus e posibilă numai pentru $a = \pm 1, b = 0$. În concluzie, pentru $d \in \mathbb{Z}$, $d < 0$ și d liber de pătrate

$$U(\mathbb{Z}[\sqrt{d}]) = \begin{cases} \{1, -1, i, -i\} & \text{dacă } d = -1 \\ \{1, -1\} & \text{dacă } d < -1 \end{cases}.$$

(ii) Să notăm $R = \mathbb{Z}[\sqrt{2}]$, $G = U(R)$, $u = 1 + \sqrt{2} \in G$ și $\mathcal{N} = \{a + b\sqrt{2} \mid a, b \in \mathbb{N}\} \cap G$. 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 multiplicativității 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 $xu^{-n} > 0$, obținem $r > 0$ și $s > 0$. Deci $r \geq 1$ și $s \geq 1$. Rezultă $x = (r + s\sqrt{2})u^n \geq u^{n+1}$, contradicție. Dacă $rs = 0$, atunci $xu^{-n} \in \mathcal{N}$ implică $r = 1$ și $s = 0$, 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 $|r| + |s|\sqrt{2} \geq u$, obținem $x \leq u^{n-1}$, din nou contradicție.

În concluzie, $\mathcal{N} = \{u^n \mid n \in \mathbb{N}\}$.

Să constatăm în continuare că dacă $x = a + b\sqrt{2} \in G$ și $x > 0$, avem posibilitățile:

- 1) $a, b \in \mathbb{N}$, caz în care $x \in \mathcal{N}$.
- 2) $ab < 0$, situație 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, obținem $G_+ = \{u^n \mid n \in \mathbb{Z}\}$. Cum $x \in G_- = \{x \in G \mid x < 0\} \Leftrightarrow -x \in G_+$, se obține $G = \{\pm u^n \mid n \in \mathbb{Z}\}$.

Acum este clar că funcția $f : \mathbb{Z}_2 \times \mathbb{Z} \rightarrow G, f(\hat{a}, n) = (-1)^a u^n$ este corect definită și izomorfism de grupuri.

5. Să notăm $\varepsilon = \frac{1+i\sqrt{3}}{2}$ și $R = \mathbb{Z}[\varepsilon]$. 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 $N(z) = z\bar{z} = (a + \frac{1}{2}b)^2 + \frac{3b^2}{4} = a^2 + ab + b^2 \in \mathbb{N}$. Procedând ca la soluția problemei 2, se arată că N este multiplicativă și că $z \in R$ este inversabil dacă și numai dacă $N(z) = 1$, condiție care se rescrie $(a + \frac{1}{2}b)^2 + \frac{3b^2}{4} = 1$. Pot apărea cazurile: $b = 0$, caz în care obținem $a = \pm 1$; $b = 1$, caz în care $(a + \frac{1}{2})^2 = \frac{1}{4}$, deci $a \in \{-1, 0\}$; $b = -1$, caz în care $(a - \frac{1}{2})^2 = \frac{1}{4}$, deci $a \in \{0, 1\}$. Prin urmare, $U(\mathbb{Z}[\varepsilon]) = \{1, -1, \varepsilon, -\varepsilon, 1 - \varepsilon\}$. Constatăm că $\varepsilon^2 = -1 + \varepsilon \neq 1$, $\varepsilon^3 = -1 \neq 1$, $\varepsilon^4 = -\varepsilon \neq 1$, $\varepsilon^5 = 1 - \varepsilon \neq 1$ și $\varepsilon^6 = 1$. Prin urmare, ordinul lui ε în $U(\mathbb{Z}[\varepsilon])$ este 6. În consecință, $U(\mathbb{Z}[\varepsilon]) = \langle \varepsilon \rangle$. Așadar $U(\mathbb{Z}[\varepsilon])$ 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 $a = X^2$ și $b = \sqrt{2}X^2$, $a, b \in R$. Fie d un divizor comun pentru a și b . Atunci, $\text{grad}(d) \leq 2$. Scriind $a = d\alpha$, $\alpha \in R$, obținem, după identificarea coeficienților, 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 și b . Prin urmare, un eventual c.m.m.d.c. în R al elementelor a și b trebuie să fie de forma AX , $A \in \mathbb{R}$ și să se dividă în R cu X și cu $\sqrt{2}X$. Însă R nu conține astfel de elemente. Rămâne deci că a și 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 este număr prim din $\mathbb{Z} \subset R$, fie este ireductibil în $\mathbb{R}[X]$ și 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 situații f este reductibil. Dacă $f \in R$, nenul și neinvertibil, are gradul 0 și nu e număr prim, atunci pentru orice număr prim $p \in \mathbb{Z}$ care divide pe f obținem descompunerea relevantă $f = p \cdot \frac{f}{p}$, deci f este reductibil în R .)

Fie acum $f \in R$ ireductibil și $g, h \in R$ 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 $f|_Rg$ sau $f|_Rh$, respectiv.
2. f este ireductibil în $\mathbb{R}[X]$ și $f(0) \in \{-1, 1\}$. Cum $f|_Rgh$, 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 $f|_Rg$. Cazul $f|_{\mathbb{R}[X]}h$ se tratează analog. În concluzie, f este prim în R și demonstrația e încheiată.

8. Notăm $R = \mathbb{Z}[i\sqrt{n}]$, $n \geq 3$ impar. În R avem relația $2 \cdot \frac{n+1}{2} = n+1 = (1+i\sqrt{n})(1-i\sqrt{n})$. 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 soluția problemei 2(vii)) în R nu există elemente de normă 2, contradicție. 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 $a = 2(1+i\sqrt{5})$ și $b = 6$ au un c.m.m.d.c. în R , fie el d . Atunci, $d|_Ra$ și $d|_Rb$, deci $N(d)|_{\mathbb{Z}}N(a) = 24$ și $N(d)|_{\mathbb{Z}}N(b) = 36$. Prin urmare, $N(d)|_{\mathbb{Z}}12$. Pe de altă parte, 2 și $1+i\sqrt{5}$ divid a și b în R , deci ele divid d . Rezultă că $4 = N(2)|_{\mathbb{Z}}N(d)$ și $6 = N(1+i\sqrt{5})|_{\mathbb{Z}}N(d)$, deci $12|_{\mathbb{Z}}N(d)$. Prin urmare, $N(d) = 12$. Procedând ca în soluția problemei 2(vii), obținem că în R nu există elemente de normă 12, contradicție. Rămâne că $2(1+i\sqrt{5})$ și 6 nu au un c.m.m.d.c. în R .

În ceea ce privește elementele $1+i\sqrt{5}$ și 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 $1 + i\sqrt{5}$ și 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 situațiile: $N(x) = 1, N(y) = 36$. 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 soluția problemei 2(vii)).

$N(x) = 3, N(y) = 12$. Imposibil, căci R nu are elemente de normă 3.

$N(x) = 4, N(y) = 9$. Obținem $x \sim_R 2$ și $y \sim_R 3$ (vezi problema 2(vii)).

$N(x) = 6, N(y) = 6$. Obținem $x \sim_R 1 + i\sqrt{5}$ și $y \sim_R 1 - i\sqrt{5}$ sau invers.

Să constatăm că $2 \cdot 3 = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$. Această relație arată că $2 \mid_R (1 + i\sqrt{5})(1 - i\sqrt{5})$. 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, $1 + i\sqrt{5}$ și $1 - i\sqrt{5}$ 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, contradicție.

În concluzie, 6 se descompune în factori ireductibili în R ca $2 \cdot 3$ și $(1 + i\sqrt{5})(1 - i\sqrt{5})$, 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, contradicție. 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 și $1 + i\sqrt{3}$ trebuie să dividă 4. Dacă această normă ar fi 4, ar rezulta (conform problemei 3(iii)) că $d \sim_R 2$ și $d \sim_R 1 + i\sqrt{3}$, deci $2 \sim_R 1 + i\sqrt{3}$, contradicție (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 $1 + i\sqrt{3}$ și 2, rezultă că 2 și $1 + i\sqrt{3}$ 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 $a = 2(1 + i\sqrt{3})$ și $b = 4$ au un c.m.m.d.c. în R , fie el d . Atunci, $d|_Ra$ și $d|_Rb$, deci $N(d)|_{\mathbb{Z}}N(a)$ și $N(d)|_{\mathbb{Z}}N(b)$. Cum $N(a) = N(b) = 16$, rezultă că $N(d)|_{\mathbb{Z}}16$. Pe de altă parte, 2 divide a și 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 soluția problemei 2(vii)), rezultă că $N(d) \in \{4, 16\}$. Dacă $N(d) = 4$, obținem $d = \pm 2$ sau $d = \pm 2 \pm i\sqrt{3}$.

Dacă $N(d) = 16$, procedând ca la problema 2(vii), obținem $d = \pm 4$ sau $d = \pm 2 \pm 2i\sqrt{3}$.

Se observă (ca la soluția problemei 1) că $\pm 4 \nmid_R a$, iar $\pm 2 \pm 2i\sqrt{3} \nmid_R b$.

Pe de altă parte, $1 + i\sqrt{3}|_Ra$ și $1 + i\sqrt{3}|_Rb$, dar $1 + i\sqrt{3} \nmid_R \pm 2$; $2|_Ra$ și $2|_Rb$, 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 și b . Rămâne că $2(1 + i\sqrt{3})$ și 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 $a = 4 + i\sqrt{5}$ și $b = 1 + 3i\sqrt{5}$. Atunci, $N(d)|N(a) = 21$ și $N(d)|N(b) = 46$. Prin urmare, $N(d)|(21, 46)_{\mathbb{Z}} = 1$, deci $N(d) = 1$. Rezultă că $d \in U(R)$, deci $d|_R1$. Cum 1 divide în R pe a și pe b , rezultă că $1 = (a, b)_R$.

(ii) Fie d un divizor comun în R pentru $a = 6 + 2i\sqrt{5}$ și $b = 14$. Atunci, $N(d)|N(a) = 56$ și $N(d)|N(b) = 196$. Prin urmare, $N(d)|(56, 196)_{\mathbb{Z}} = 28$. Presupunem că d este chiar un c.m.m.d.c. pentru a și b în R . Cum $2|_Ra$ și $2|_Rb$, rezultă $2|_Rd$, de unde $4 = N(2)|_{\mathbb{Z}}N(d)$. Avem și $3 + i\sqrt{5}|_Ra$ și $3 + i\sqrt{5}|_Rb$, deci $3 + i\sqrt{5}|_Rd$, 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 $u, v \in \mathbb{Z}$, obținem $u^2 + 5v^2 = 28$, de unde $u^2 \equiv 3 \pmod{5}$, contradicție. Așadar a și b nu au un c.m.m.d.c. în R .

(iii) Fie d un divizor comun în R pentru $a = 4 + i\sqrt{5}$ și $b = 1 + 2i\sqrt{5}$. Atunci $N(d)|_{\mathbb{Z}}N(a) = N(b) = 21$. Vom avea deci $N(d) \in \{1, 3, 7, 21\}$. Procedând ca la soluția problemei 2(vii) se constată că în R nu există elemente de normă 3 sau 7. Dacă $N(d) = 21$, atunci se obține (vezi problema 2(vii)) $d \sim_R a$ sau $d \sim_R \bar{a}$ sau $d \sim_R b$ sau $d \sim_R \bar{b}$. Dar $a \nmid_R b$, $\bar{a} \nmid_R a$, $b \nmid_R a$ și $\bar{b} \nmid_R b$. Rămâne prin urmare că $N(d) = 1$. Rezultă că $d \in U(R)$, deci $d|_R1$. Cum 1 divide în R pe a și pe b , rezultă că $1 = (a, b)_R$.

(iv) Fie d un divizor comun în R pentru $a = 6 + 3i\sqrt{5}$ și $b = 9$. Cum $N(a) = N(b) = 81$, rezultă $N(d)|81$. Presupunem acum că $d = (a, b)_R$; constatăm că $3|_Ra$ și $3|_Rb$, de unde $3|_Rd$, 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 situațiile $N(d) = 9$ și $N(d) = 81$.

Dacă $N(d) = 9$, atunci $d \sim 3$ sau $d \sim 2 \pm i\sqrt{5}$. Dar (ca la soluția 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 $2 + i\sqrt{5}$ și 3 sunt divizori comuni în R pentru a și b și 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 și 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 și b nu admit un c.m.m.d.c. în R .

(v) Fie d un divizor comun în R pentru $a = 2 + 8i\sqrt{5}$ și $b = 18$. Atunci, $N(d) | N(a) = N(b) = 324$. Presupunem că d este chiar un c.m.m.d.c. pentru a și b în R . Cum $2 |_{Ra}$ și $2 |_{Rb}$, rezultă $2 |_{Rd}$, 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 și b (și se divide și prin divizorul comun 2 de la cazul precedent).

Dacă $N(d) = 324$, atunci, din $d |_{Ra}$ și $N(d) = N(a)$ rezultă (vezi problema 3(iii)) $d \sim_R a$; analog obținem $d \sim_R b$, deci $a \sim_R b$, contradicție.

Prin urmare, singurul (până la o asociere în divizibilitate) element care poate fi c.m.m.d.c. în R pentru a și b este $4 - 2i\sqrt{5}$.

Rămâne să verificăm dacă $4 - 2i\sqrt{5}$ se divide într-adevăr prin toți divizorii comuni ai elementelor a și b . Fie c un astfel de divizor. S-a arătat mai sus că $N(c) |_{\mathbb{Z}} 324$. Ținând cont de considerațiile 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 și $2 + i\sqrt{5}$ nu divid în R pe a , iar $2 - i\sqrt{5}$, care este divizor comun pentru a și 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 sfârșit, 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 și 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:

$$f = \sum_{k=0}^{\lfloor \frac{n}{3} \rfloor} a_{3k} X^{3k} + \sum_{k=1}^{\lfloor \frac{n-1}{3} \rfloor} a_{3k+1} X^{3k+1} + \sum_{k=0}^{\lfloor \frac{n-2}{3} \rfloor} a_{3k+2} X^{3k+2}.$$

Dacă punem

$$F(U, V) = \sum_{k=0}^{\lfloor \frac{n}{3} \rfloor} a_{3k} V^k + \sum_{k=1}^{\lfloor \frac{n-1}{3} \rfloor} a_{3k+1} V^{k-1} U^2 + \sum_{k=0}^{\lfloor \frac{n-2}{3} \rfloor} a_{3k+2} V^k U \in \mathbb{Z}[U, V],$$

atunci $f = F(X^2, X^3)$, deci $f \in \mathbb{Z}[X^2, X^3]$.

(ii) Dacă $d|_R X^2$ și $d|_R X^3$, atunci aceste divizibilități au loc și 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 și X^3 în R , deci $1 = (X^2, X^3)_R$.

Presupunem acum că X^2 și X^3 admit un c.m.m.m.c. în R , fie el m . Cum X^2 și X^3 divid în R pe X^5 , rezultă că $m|_R X^5$, deci $m|_{\mathbb{Z}[X]} X^5$. Avem și $X^3|_R m$, deci $X^3|_{\mathbb{Z}[X]} m$. Prin urmare, $m \in \{\pm X^3, \pm X^4, \pm X^5\}$. Dar $X^2 \nmid_R \pm X^3$ și $X^3 \nmid_R \pm X^4$. A rămas de investigat numai cazul $m = \pm X^5$; nici acesta nu este însă c.m.m.m.c. pentru X^2 și X^3 în R , căci $X^2|_R X^6$ și $X^3|_R X^6$, dar $X^5 \nmid_R X^6$. Rămâne așadar că X^2 și X^3 nu admit c.m.m.m.c. în R .

(iii) Presupunem că X^5 și 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, $X^3|_R X^5$ și $X^3|_R X^6$, deci $X^3|_R d$, prin urmare $X^3|_{\mathbb{Z}[X]} d$. În consecință, $d \in \{\pm X^3, \pm X^4, \pm X^5\}$. Dar $X^5 \nmid_R \pm X^6$ și $X^4 \nmid_R \pm X^5$. A rămas de investigat numai cazul $d = \pm X^3$; nici acesta nu este însă c.m.m.d.c. pentru X^5 și X^6 în R , căci $X^2|_R X^5$ și $X^2|_R X^6$, dar $X^2 \nmid_R \pm X^3$.

Presupunem acum că X^5 și X^6 admit un c.m.m.m.c. în R , fie el m . Cum X^5 și X^6 divid în R pe X^8 , rezultă că $m|_R X^8$, deci $m|_{\mathbb{Z}[X]} X^8$. Avem și $X^6|_R m$, deci $X^6|_{\mathbb{Z}[X]} m$. Prin urmare, $m \in \{\pm X^6, \pm X^7, \pm X^8\}$. Dar $X^5 \nmid_R \pm X^6$ și $X^6 \nmid_R \pm X^7$. A rămas de investigat numai $m = \pm X^8$; nici acesta nu este însă c.m.m.m.c. pentru X^5 și X^6 în R , căci $X^5|_R X^9$ și $X^6|_R X^9$, dar $\pm X^8 \nmid_R X^9$. Rămâne așadar că X^5 și X^6 nu admit c.m.m.m.c. în R .

(iv) Dacă $X^2 = fg$ în R , atunci această relație are loc și în $\mathbb{Z}[X]$. Prin urmare, $f = \pm 1$ și $g = \pm X^2$ (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 $f = a_0 + a_1X + \dots + a_nX^n \in R[X]$. Pentru orice $i \in \{0, 1, \dots, n\}$ punem $a_i = \alpha_i c(f)$. Notăm $\bar{f} = \alpha_0 + \alpha_1X + \dots + \alpha_nX^n$. Dacă un element $d \in R$ divide toți coeficienții lui \bar{f} , atunci $dc(f)$ divide toți coeficienții lui f . Prin urmare, $dc(f)$ va divide și c.m.m.d.c. al acestora, adică pe $c(f)$. Rezultă că $d \in U(R)$. Prin urmare, $c(\bar{f}) = 1$.

(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 $c(f)$ și 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 consecință, $c(f)c(g)|c(fg)$. Scriem $c(fg) = ac(f)c(g)$, $a \in R$. Cum $c(f)c(g)\bar{f}\bar{g} = fg = c(fg)\bar{f}\bar{g}$, rezultă $\bar{f}\bar{g} = a\bar{f}\bar{g}$.

Notăm $I = aR$, $S = R/I$, $\pi : R \rightarrow S$ proiecția canonică și $\bar{\pi} : R[X] \rightarrow S[X]$, $\bar{\pi}(c_0 + \dots + c_t X^t) = \pi(c_0) + \dots + \pi(c_t)X^t$ extinsul lui π la inelele de polinoame corespunzătoare. Atunci $\bar{\pi}(\bar{f})\bar{\pi}(\bar{g}) = 0$.

• Dacă $\bar{\pi}(\bar{f}) = 0$, atunci toți coeficienții lui \bar{f} sunt în I , deci se divid cu a . Cum $c(\bar{f}) = 1$, rezultă $a \in U(R)$, deci $c(f)c(g) = c(fg)$.

• Dacă $\bar{\pi}(\bar{f}) \neq 0$, atunci $\bar{\pi}(\bar{g})$ este divizor al lui zero în $S[X]$. Conform problemei 25 din Capitolul 5, există $\hat{b} \in S \setminus \{0\}$ astfel ca $\hat{b}\bar{\pi}(\bar{g}) = 0$. Notând $d = (a, b)$, $a = \alpha d$ și $b = \beta d$, din considerațiile anterioare rezultă că $\alpha \notin U(R)$ și $\alpha|\beta\bar{g}$. Dar $(\alpha, \beta) = 1$, deci α divide toți coeficienții lui \bar{g} . Prin urmare, $\alpha|c(\bar{g})$, contradicție. Așadar acest caz este imposibil.

(iii) Rezultă din relația $c(f)c(g)\bar{f}\bar{g} = fg = c(fg)\bar{f}\bar{g}$ și din punctul (ii).

(iv) Este clar că dacă $f|g$ în $R[X]$, atunci $f|g$ și 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 coeficienții lui h_1 la același numitor, găsim $h \in R[X]$ și $s \in R \setminus \{0\}$ astfel ca $h_1 = \frac{h}{s}$. Obținem $sg = fh$, de unde $sc(g) = c(f)c(h)$ și $s = c(h)$. Atunci $g = f \frac{h}{s} = f\bar{h}$. 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) obținem $c(g) = c(f)c(h)$, deci $c(f)|_R c(g)$. Conform punctului (iii), $\bar{g} = u\bar{f} \cdot \bar{h}$, $u \in U(R)$. Prin urmare, $\bar{f}|_{R[X]}\bar{g}$.

Reciproc, dacă $c(g) = c(f)\gamma$, $\gamma \in R$, și $\bar{g} = \bar{f}\bar{h}$, $h \in R[X]$, atunci $g = c(g)\bar{g} = c(f)\gamma\bar{f}\bar{h} = (\gamma h)f$, deci $f|_{R[X]}g$.

(vi) Este echivalent cu (v) conform (iv).

14. Vom folosi în soluția acestei probleme notațiile din problema 13. Deseptăm prin Q corpul de fracții al lui R . Fie $f, g \in R[X]$. Cum $Q[X]$ este inel euclidian, f și g admit un c.m.m.d.c. în $Q[X]$, fie el d'' . Aducând coeficienții lui d'' la același numitor, putem scrie $d'' = \frac{d'}{\delta}$ cu $d' \in R[X]$, $\delta \in R$ și $(c(d'), \delta)_R = 1$. Să considerăm acum $a = (c(f), c(g))_R$ și $d = ad'$. Avem $\frac{f}{d} = \frac{c(f)}{c(d)} \frac{\bar{f}}{\bar{d}} = \frac{c(f)}{a} \frac{\bar{f}}{\bar{d}}$. Dar $d''|_{Q[X]} f \Rightarrow d'|_{Q[X]} f \Rightarrow \bar{d}'|_{Q[X]} \bar{f}$. Cum $\bar{d}', \bar{f} \in R[X]$ și $c(\bar{d}') = c(\bar{f}) = 1$, rezultă din problema 13(iv) că $\bar{d}'|_{R[X]} \bar{f}$, adică $\frac{\bar{f}}{\bar{d}'} \in R[X]$. Cum $a|c(f)$, obținem 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 și pe g . Conform problemei 13(v), $c(D)|_R c(f)$, $c(D)|_R c(g)$, $\bar{D}|_{R[X]} \bar{f}$ și $\bar{D}|_{R[X]} \bar{g}$. De aici rezultă că $c(D)|_R (c(f), c(g))_R$ și $\bar{D}|_{Q[X]} (\bar{f}, \bar{g})_{Q[X]}$; această ultimă relație dă imediat și $\bar{D}|_{Q[X]} \bar{d}'$. Conform problemei 13(vi), obținem $D|_{R[X]} d$. Prin urmare, d este un c.m.m.d.c. în $R[X]$ pentru f și g .

15. Să începem cu observația că pentru orice $f \in R \setminus \{0\}$ există și sunt unice $a_f \in \mathbb{Q}$, $r_f \in \mathbb{N}$ și $\bar{f} \in R$ cu $\bar{f}(0) = 1$ astfel încât $f = a_f X^{r_f} \bar{f}$. 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 situația în care $r_f \leq r_g$, $f|_R g \Rightarrow f|_{Q[X]} g$. Cum $\frac{g}{f} = \frac{a_g}{a_f} X^{r_g - r_f} \frac{\bar{g}}{\bar{f}}$, obținem $\bar{f}|_{Q[X]} \bar{g}$, deci există $h \in Q[X]$ astfel ca $\bar{g} = \bar{f}h$. Rezultă $h(0) = \bar{f}(0)h(0) = \bar{g}(0) = 1 \in \mathbb{Z}$, deci $h \in R$. Prin urmare, $\bar{f}|_R \bar{g}$. În concluzie, în cazul în care $r_f < r_g$, avem $f|_R g \Leftrightarrow \bar{f}|_R \bar{g}$.

În cazul $r_f = r_g$ avem

$$f|_R g \Leftrightarrow \frac{g}{f} \in R \Leftrightarrow \frac{a_g}{a_f} \cdot \frac{\bar{g}}{\bar{f}} \in R \Leftrightarrow \bar{f}|_R \bar{g} \text{ și } \frac{a_g}{a_f} \in \mathbb{Z}.$$

Aceste preliminarrii fiind încheiate, să arătăm că inelul R are proprietatea c.m.m.d.c. Fie $f, g \in R \setminus \{0\}$. Notăm $h = (\bar{f}, \bar{g})_{Q[X]}$ și $\bar{h} = \frac{1}{h(0)}h$.

Dacă $r_f < r_g$, punem $d = a_f X^{r_f} \bar{h}$. Avem $\frac{f}{d} = \frac{\bar{f}}{\bar{h}} \in R$, deci $d|_R f$, și $\frac{g}{d} = \frac{a_g}{a_f} X^{r_g - r_f} \frac{\bar{g}}{\bar{h}} \in R$, deci $d|_R g$.

Fie acum $d' \in R$ astfel încât $d'|_R f$ și $d'|_R g$. Pot apărea cazurile:

1. $r_{d'} < r_f$. Atunci $d'|_R f \Rightarrow \bar{d}'|_R \bar{f}$; $d'|_R g \Rightarrow \bar{d}'|_R \bar{g}$. Urmează că $d'|_R \bar{h} = \bar{d}$. Prin urmare, $d'|_R d$.

2. $r_{d'} = r_f$. Atunci $d'|_R f \Rightarrow \bar{d}'|_R \bar{f}$ și $\frac{a_f}{a_{d'}} \in \mathbb{Z}$; $d'|_R g \Rightarrow \bar{d}'|_R \bar{g}$. Urmează că

$d'|_R \bar{h} = \bar{d}$ și $\frac{a_d}{a_{d'}} = \frac{a_f}{a_{d'}} \in \mathbb{Z}$. Prin urmare, $d'|_R d$.

Dacă $r_f = r_g$, pot apărea situațiile:

1. $r_f = r_g = 0$. Punem $d = (a_f, a_g)_{\mathbb{Z}} \bar{h}$. Avem

$$\frac{f}{d} = \frac{a_f \bar{f}}{(a_f, a_g)_{\mathbb{Z}} \bar{h}} \in R \Rightarrow d|_R f; \quad \frac{g}{d} = \frac{a_g \bar{g}}{(a_f, a_g)_{\mathbb{Z}} \bar{h}} \in R \Rightarrow d|_R g.$$

Fie acum $d' \in R$ astfel încât $d'|_R f$ și $d'|_R g$. Atunci $r_{d'} = 0$. Avem

$$d'|_R f \Rightarrow \frac{a_f}{a_{d'}} \cdot \frac{\bar{f}}{d'} \in R \Rightarrow a_{d'}|_{\mathbb{Z}} a_f \text{ și } \bar{d}'|_R \bar{f}$$

și

$$d'|_R g \Rightarrow \frac{a_g}{a_{d'}} \cdot \frac{\bar{g}}{d'} \in R \Rightarrow a_{d'}|_{\mathbb{Z}} a_g \text{ și } \bar{d}'|_R \bar{g},$$

de unde obținem $a_{d'}|_{\mathbb{Z}}(a_f, a_g) = a_d$ și $\bar{d}'|_R(\bar{f}, \bar{g})_{\mathbb{Q}[X]} = \bar{h} = \bar{d}$. De aici rezultă $d'|_R d$.

2. $r_f = r_g > 0$. Punem $a_f = \frac{s_f}{t}$ și $a_g = \frac{s_g}{t}$ cu $(s_f, s_g, t) = 1$ și considerăm $d = \frac{(s_f, s_g)}{t} X^{r_f} \bar{h}$. Avem

$$\frac{f}{d} = \frac{\frac{s_f}{t} X^{r_f} \bar{f}}{\frac{(s_f, s_g)}{t} X^{r_f} \bar{h}} = \frac{s_f}{(s_f, s_g)} \frac{\bar{f}}{\bar{h}} \in R \Rightarrow d|_R f$$

și

$$\frac{g}{d} = \frac{\frac{s_g}{t} X^{r_g} \bar{g}}{\frac{(s_f, s_g)}{t} X^{r_g} \bar{h}} = \frac{s_g}{(s_f, s_g)} \frac{\bar{g}}{\bar{h}} \in R \Rightarrow d|_R g.$$

Fie acum $d' \in R$ astfel încât $d'|_R f$ și $d'|_R g$. Dacă $r_{d'} < r_f$, atunci, cum $d'|_R f \Rightarrow \bar{d}'|_R \bar{f}$ și $d'|_R g \Rightarrow \bar{d}'|_R \bar{g}$, obținem $\bar{d}'|_R \bar{h}$, deci $d'|_R d$. Dacă $r_{d'} = r_f$, atunci $d'|_R f \Rightarrow \bar{d}'|_R \bar{f}$ și $\frac{a_f}{a_{d'}} \in \mathbb{Z}$ și $d'|_R g \Rightarrow \bar{d}'|_R \bar{g}$ și $\frac{a_g}{a_{d'}} \in \mathbb{Z}$. Din aceste relații rezultă că $\bar{d}'|_R \bar{h} = \bar{d}$ și că există $c_f, c_g \in \mathbb{Z}$ cu proprietățile

$$(**) \quad c_f a_{d'} = \frac{s_f}{t} \text{ și } c_g a_{d'} = \frac{s_g}{t}.$$

Din ultimele relații obținem $\frac{s_g}{c_g t} = \frac{s_f}{c_f t}$, de unde $c_f s_g = c_g s_f$. Punând $s_f = (s_f, s_g) u_f$ și $s_g = (s_f, s_g) u_g$, ajungem la $c_f u_g = c_g u_f$. Cum $(u_f, u_g) = 1$, deducem existența unor numere întregi c'_f, c'_g pentru care $c_f = c'_f u_f$ și $c_g =$

$c'_g u_g$. Introducând în $(**)$ obținem $c'_f a_{d'} = \frac{(s_f, s_g)}{t}$, 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 obținuserăm $\bar{d}'|_R \bar{d}$, 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 și neinvertibil în R , vor exista $n \in \mathbb{N}^*$ și elementele p_1, \dots, 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 relație în $\mathbb{Q}[X]$, rezultă $a, b \in \mathbb{Q}^*$. Dar $a, b \in R$, deci $a, b \in \mathbb{Z}$. Din $2 = ab$ obținem că unul dintre elementele a și b este invertibil, contradicție. 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 relația $X = 2^{n+1} \left(\frac{1}{2^{n+1}} X \right)$, deducem că $2^{n+1}|_R X = p_1 \cdots p_n$. De aici rezultă că $p_1 = \dots = p_n = 2$ și $2|_R 1$, contradicție. Rămâne că R nu este factorial.

16. Să notăm $S = \left\{ \frac{r}{s} \mid r \in \mathbb{Z}, s \in 2\mathbb{Z} + 1, (r, s) = 1 \right\} \subset \mathbb{Q}$. 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 și sunt unice $r_f \in \mathbb{N}$ și $u_f \in \mathbb{Q}[[X]]$ astfel încât $f = X^{r_f} u_f$ și $\widetilde{u_f} \neq 0$. 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 situația $r_f < r_g$ 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 și numai dacă $\frac{\widetilde{u_g}}{\widetilde{u_f}} \in S$.

Am arătat deci că $f|g$ în R dacă și numai dacă sunt într-una din următoarele două situații:

- a) $r_f < r_g$ sau
- b) $r_f = r_g$ și $\frac{\widetilde{u_g}}{\widetilde{u_f}} \in S$.

Trecem acum la demonstrația 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 însuși și 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 $\widetilde{u_f} = \frac{a_f}{s_f} \cdot 2^{v_f}$ și $\widetilde{u_g} = \frac{a_g}{s_g} \cdot 2^{v_g}$, unde $a_f, s_f, a_g, s_g \in 2\mathbb{Z} + 1$, iar $v_f, v_g \in \mathbb{Z}$. Notăm $v = \min\{v_f, v_g\}$ și 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 obținem $d|g$.

Fie acum $d' \in R$ cu $d'|f$ și $d'|g$. Dacă $r_{d'} < r_f$, atunci $d'|d$. Dacă $r_{d'} = r_f$, din $d'|f$ și $d'|g$ deducem $\frac{\widetilde{u}_f}{\widetilde{u}_{d'}}, \frac{\widetilde{u}_g}{\widetilde{u}_{d'}} \in S$, deci există $\lambda_f, \lambda_g \in \mathbb{N}$ și $\alpha_f, \alpha_g, \sigma \in 2\mathbb{Z} + 1$, $(\alpha_f, \alpha_g, \sigma) = 1$, astfel încât $\frac{\widetilde{u}_f}{\widetilde{u}_{d'}} = 2^{\lambda_f} \frac{\alpha_f}{\sigma}$ și $\frac{\widetilde{u}_g}{\widetilde{u}_{d'}} = 2^{\lambda_g} \frac{\alpha_g}{\sigma}$. Deducem $\frac{a_f}{s_f} \cdot 2^{v_f} = 2^{\lambda_f} \frac{\alpha_f}{\sigma} \widetilde{u}_{d'}$ și $\frac{a_g}{s_g} \cdot 2^{v_g} = 2^{\lambda_g} \frac{\alpha_g}{\sigma} \widetilde{u}_{d'}$. 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 consecință, $2^{v_f - \lambda_f} a_f s_g \alpha_g = 2^{v_g - \lambda_g} a_g s_f \alpha_f$. Obținem de aici $v_f - \lambda_f = v_g - \lambda_g$, deci $v_f - \lambda_f \leq v_g$. Atunci $d = 2^v X^{r_f} \sim_R 2^{\min\{v_f, v_g\}} \frac{s_f \alpha_f}{a_f \sigma \cdot 2^{v_f - \lambda_f}} d' = 2^{\min\{v_f, v_g\} - (v_f - \lambda_f)} \frac{s_f \alpha_f}{a_f \sigma} \cdot d'$. 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 și g vor avea ordin zero. Dacă notăm $\widetilde{u}_f = \frac{a_f}{s_f}$ și $\widetilde{u}_g = \frac{a_g}{s_g}$, cu $s_f, s_g \in 2\mathbb{Z} + 1$ și $(a_f, s_f) = (a_g, s_g) = 1$, avem $2 = \frac{a_f a_g}{s_f s_g}$, deci $2|a_f$ și $2 \nmid a_g$ 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, și există elementele prime $p_1, \dots, p_n \in R$ astfel încât $X = p_1 \cdots p_n$. Dar $X = 2^{n+1} \cdot (\frac{1}{2^{n+1}} X)$, de unde $2^{n+1} | p_1 \cdots p_n$. De aici deducem $p_1 = \dots = p_n = 2$ și $2|1$, contradicție. Rămâne așadar că R nu este inel factorial.

17. Notăm $R = \mathbb{Z}[\sqrt{2}]$ și definim $N : \mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}$, $N(a + b\sqrt{2}) = |a^2 - 2b^2|$. Conform problemei 2(ii),(iii), N este multiplicativă și $N(\mathbb{Z}[\sqrt{2}]) \subset \mathbb{N}$. Fie $x = a + b\sqrt{2}$ și $y = c + d\sqrt{2}$, $y \neq 0$, 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

$$\alpha = \frac{ac - 2bd}{c^2 - 2d^2} \text{ și } \beta = \frac{bc - ad}{c^2 - 2d^2},$$

iar cu A și B întregii cei mai apropiați de α , respectiv de β . Prin urmare, $|A - \alpha| \leq \frac{1}{2}$ și $|B - \beta| \leq \frac{1}{2}$. Cu aceste notații se obține

$$\frac{x}{y} = A + B\sqrt{2} + (\alpha - A) + (\beta - B)\sqrt{2},$$

deci $x = (A + B\sqrt{2})y + [(\alpha - A) + (\beta - B)\sqrt{2}]y$. Cum x, y și $q = A + B\sqrt{2}$ sunt în R , din relația anterioară rezultă că $r = [(\alpha - A) + (\beta - B)\sqrt{2}]y \in R$.

Avem deci în R scrierea $x = qy + r$. În plus, datorită multiplicativității lui N , $N(r) = N((\alpha - A) + (\beta - B)\sqrt{2})N(y) = N(y)|(\alpha - A)^2 - 2(\beta - B)^2|$. Avem însă $0 \leq (\alpha - A)^2 \leq \frac{1}{4}$ și $-\frac{1}{2} \leq -2(\beta - B)^2 \leq 0$. Adunând membru cu membru aceste relații, obținem $-\frac{1}{2} \leq (\alpha - A)^2 - 2(\beta - B)^2 \leq \frac{1}{4}$, 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 $N : \mathbb{Q}[\sqrt{5}] \rightarrow \mathbb{Q}$, $N(u + v\sqrt{5}) = |a^2 - 5b^2|$. Conform problemei 2(ii), N este multiplicativă. Observăm și că $N(a + b\omega) = |a^2 + ab - b^2|$, de unde $N(R) \subset \mathbb{N}$. Se constată imediat prin dublă incluziune că $R = \{\frac{a+b\sqrt{5}}{2} \mid a, b \in \mathbb{Z} \text{ au aceeași paritate}\}$. Fie $x = \frac{a+b\sqrt{5}}{2}$ și $y = \frac{c+d\sqrt{5}}{2} \neq 0$ 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

$$\alpha = \frac{ac - 5bd}{c^2 - 5d^2} \text{ și } \beta = \frac{bc - ad}{c^2 - 5d^2}$$

și alegem B cel mai apropiat întreg de 2β (deci, $|\beta - \frac{B}{2}| \leq \frac{1}{4}$) și A cel mai apropiat întreg de aceeași paritate cu B de 2α (deci, $|\alpha - \frac{A}{2}| \leq \frac{1}{2}$). Cu aceste notații se obține

$$\frac{x}{y} = \frac{A + B\sqrt{5}}{2} + (\alpha - \frac{A}{2}) + (\beta - \frac{B}{2})\sqrt{5},$$

deci $x = (\frac{A+B\sqrt{5}}{2})y + [(\alpha - \frac{A}{2}) + (\beta - \frac{B}{2})\sqrt{5}]y$. Cum x, y și $q = \frac{A+B\sqrt{5}}{2}$ sunt în R , din relația 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 multiplicativității 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 $\varphi : R \setminus \{0\} \rightarrow \mathbb{N}$ astfel încât oricare ar fi $a, b \in R$, $b \neq 0$, există $q, r \in R$ cu proprietățile $a = bq + r$ și $r = 0$ sau $\varphi(r) < \varphi(b)$. Considerăm și 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 soluția problemei 4, obținem $U(R) = \{-1, 1\}$. 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 proprietăților lui φ , există $q, r \in R$ cu proprietățile $z = q\alpha + r$ și $r = 0$ sau $\varphi(r) < \varphi(\alpha)$. Conform definiției lui α , ultima inegalitate nu este posibilă decât dacă $r \in \{-1, 0, 1\}$.

În consecință, 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 $\alpha \mid 3$ sau $\alpha \mid 2$ sau $\alpha \mid 1$. Ultimul caz este însă imposibil deoarece $\alpha \notin U(R)$. Trecând la norme în celelalte două relații obținem (vezi problema 3(i)) că $N(\alpha) \mid 9$ sau $N(\alpha) \mid 4$. Cum α nu este inversabil, el nu poate avea norma 1 . Prin urmare, $N(\alpha) \in \{2, 3, 4, 9\}$. Reamintind că $R = \left\{\alpha + \beta\frac{1+i\sqrt{d}}{2} \mid \alpha, \beta \in \mathbb{Z}\right\} = \left\{\frac{a+bi\sqrt{d}}{2} \mid a, b \in \mathbb{Z} \text{ au aceeași paritate}\right\}$, notăm $\alpha = \frac{a+bi\sqrt{d}}{2}$, unde $a, b \in \mathbb{Z}$ au aceeași paritate.

Dacă $N(\alpha) \in \{2, 3\}$, rezultă $a^2 + db^2 \in \{8, 12\}$. Dacă $b = 0$, obținem $a^2 \in \{8, 12\}$, iar dacă $|b| \geq 1$ găsim $a^2 < 0$, contradicție.

Dacă $N(\alpha) = 4$, vom avea $a^2 + db^2 = 16$; dacă $b = 0$ obținem $\alpha = \pm 2 \sim 2$. 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 relație 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 $1 = 2v$, contradicție.

Dacă $|b| = 1$, avem variantele $d > 15$ (în care obținem $a^2 = 4 - db^2 < 0$, contradicție) și $d = 15$ (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 $\frac{1 \pm i\sqrt{15}}{2} \sim 2$, contradicție.) Dacă $|b| > 1$, obținem $a^2 = 4 - db^2 < 0$, contradicție.

Dacă $N(\alpha) = 9$, vom avea $a^2 + db^2 = 36$; pentru $b = 0$ obținem $\alpha = \pm 3 \sim 3$; constatăm însă că dacă $i\sqrt{d}$ ar da rest $-1, 0$ sau 1 modulo 3 , atunci ar avea loc în R o relație de tipul $\frac{1+i\sqrt{d}}{2} = 3\frac{u+vi\sqrt{d}}{2} + \varepsilon$ cu $\varepsilon \in \{-1, 0, 1\}$, de unde $1 = 3v$, contradicție.

Dacă $|b| = 1$, distingem cazurile:

$d = 15$, în care obținem $a^2 = 21$, contradicție;

$d = 19$, în care obținem $a^2 = 17$, contradicție;

$d = 23$, în care obținem $a^2 = 13$, contradicție;
 $d = 31$, în care obținem $a^2 = 5$, contradicție;
 $d = 35$, în care obținem $a^2 = 1$, 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 $\frac{1 \pm i\sqrt{35}}{2} \sim 3$, contradicție.
 $d \geq 39$, în care obținem $a^2 < 0$, contradicție.
 Dacă $|b| > 1$, obținem $a^2 = 36 - db^2 < 0$, contradicție.
 Rămâne așadar că inelul R nu este euclidian.
 ” \Leftarrow ” Fie $d \in \{3, 7, 11\}$. Definim $N : \mathbb{Q}[i\sqrt{d}] \rightarrow \mathbb{Q}$, $N(a + bi\sqrt{d}) = a^2 + db^2$. Conform problemei 2, N este multiplicativă și $N(R) \subset \mathbb{N}$. Fie $x = \frac{a + bi\sqrt{d}}{2}$ și $y = \frac{c + ei\sqrt{d}}{2} \neq 0$ 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

$$\alpha = \frac{ac + dbe}{c^2 + de^2} \text{ și } \beta = \frac{bc - ae}{c^2 + de^2}$$

și alegem B cel mai apropiat întreg de 2β (deci, $|\beta - \frac{B}{2}| \leq \frac{1}{4}$) și A cel mai apropiat întreg de aceeași paritate cu B de 2α (deci, $|\alpha - \frac{A}{2}| \leq \frac{1}{2}$). Cu aceste notații, se obține

$$\frac{x}{y} = \frac{A + Bi\sqrt{d}}{2} + \left(\alpha - \frac{A}{2}\right) + \left(\beta - \frac{B}{2}\right)i\sqrt{d},$$

deci $x = \left(\frac{A + Bi\sqrt{d}}{2}\right)y + \left[\left(\alpha - \frac{A}{2}\right) + \left(\beta - \frac{B}{2}\right)i\sqrt{d}\right]y$. Cum x, y și $q = \frac{A + Bi\sqrt{d}}{2}$ sunt în R , din relația anterioară rezultă că $r = \left[\left(\alpha - \frac{A}{2}\right) + \left(\beta - \frac{B}{2}\right)i\sqrt{d}\right]y \in R$.
 Avem deci în R scrierea $x = qy + r$. În plus, datorită multiplicativității lui N , $N(r) = N\left(\left(\alpha - \frac{A}{2}\right) + \left(\beta - \frac{B}{2}\right)i\sqrt{d}\right)N(y) = N(y)\left(\alpha - \frac{A}{2}\right)^2 + d\left(\beta - \frac{B}{2}\right)^2 \leq \frac{4+d}{16}N(y) \leq \frac{15}{16}N(y) < N(y)$. Prin urmare, R este euclidian în raport cu N .

19. (i) \Rightarrow (ii) Fie \mathfrak{p} un ideal prim nenul al lui R și $a \in \mathfrak{p} \setminus \{0\}$. 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 conține

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 și neinvertibil. Dacă $(a) \cap S \neq \emptyset$, atunci ar exista $\alpha \in R$ astfel ca $a\alpha = p_1 \cdots p_n$ cu p_1, \dots, p_n prime și $n \geq 1$ minim. Dacă $n = 1$, atunci $\alpha \in U(R)$, iar relația $a = \alpha^{-1}p_1$ arată că $a \in S$, contradicție. Pentru $n \geq 2$, dacă nici unul dintre factorii din membrul drept nu divide pe α , atunci $p_1 \cdots p_n \nmid a$; punând $a = bp_1 \cdots p_n$, obținem $b\alpha = 1$, 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, contradicție. Dacă pe de altă parte vreunul dintre elementele p_1, \dots, p_n , să zicem p_n , divide pe α , atunci, punând $\alpha = \beta p_n$, am avea scrierea $a\beta = p_1 \cdots p_{n-1}$, contradicție cu minimalitatea lui n . Rămâne așadar că $(a) \cap S = \emptyset$. Prin urmare, mulțimea idealelor lui R care conțin pe (a) și nu intersectează S este nevidă. Această mulțime 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 $\mathfrak{p} + (x)$ și $\mathfrak{p} + (y)$ conțin strict pe \mathfrak{p} , deci ele trebuie să intersecteze pe S . Fie $u = \pi + \alpha x \in (\mathfrak{p} + (x)) \cap S$ și $v = \rho + \beta y \in (\mathfrak{p} + (y)) \cap S$, unde $\pi, \rho \in \mathfrak{p}$, $\alpha, \beta \in R$. Atunci $uv = \pi\rho + \pi\beta y + \rho\alpha x + \alpha\beta xy \in \mathfrak{p} \cap S$, contradicție.

Rămâne deci că \mathfrak{p} este ideal prim. Atunci, conform ipotezei, el trebuie să conțină un element prim, care se va afla însă și în S . Prin urmare, $\mathfrak{p} \cap S \neq \emptyset$, contradicție.

Presupunerea că există elemente nenule și neinvertibile în afara lui S este deci incorectă. Prin urmare, toate elementele nenule și neinvertibile ale lui R se scriu ca produs de elemente prime. În consecință, R este inel factorial.

20. Se știe că orice inel de fracții al unui domeniu de integritate este de asemenea domeniu de integritate.

Considerăm pentru început că R este inel euclidian în raport cu φ . Definim

$$\overline{\varphi} : S^{-1}R \setminus \{0\} \rightarrow \mathbb{N}, \quad \overline{\varphi}\left(\frac{a}{s}\right) = \min \left\{ \varphi(\alpha) \mid \exists \sigma \in S \text{ cu } \frac{a}{s} = \frac{\alpha}{\sigma} \right\}.$$

Fie $\frac{a}{s}$ și $\frac{b}{t} \neq 0$ din $S^{-1}R$ și $\frac{\beta}{\tau} = \frac{b}{t}$ astfel ca $\overline{\varphi}\left(\frac{b}{t}\right) = \varphi(\beta)$. Cum R e euclidian, există $q, r \in R$ astfel ca $a = \beta q + r$ și $r = 0$ 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 și 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 și neinvertibil ($\frac{p}{1} \cdot \frac{a}{s} = \frac{1}{1}$ înseamnă $pa = s$, adică $p|_R s$, contradicție) 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 și 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 același 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 și în $S^{-1}R$. Fie acum un element nenul și neinvertibil $x = \frac{a}{s} \in S^{-1}R$. Atunci a este și el nenul și neinvertibil în R , deci se poate scrie sub forma $a = p_1 \cdots p_n$, $n \geq 1$, unde p_1, \dots, p_n sunt elemente prime din R . După o eventuală renumerotare, putem considera că p_1, \dots, p_r ($0 \leq r < n$) divid elemente din S , iar $p_{r+1}, p_{r+2}, \dots, p_n$ 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 invertibil), 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, \dots, p_n sunt elemente prime din R . Cum \mathfrak{p} este ideal prim, cel puțin 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 $S^{-1}\mathfrak{p}$

conține 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 $p_{i_1} \notin \mathfrak{p}$ și $p_{i_1} \in U(S^{-1}R)$, deci $q_1 \in \mathfrak{p}$ și $\frac{q}{1} \sim_{S^{-1}R} \frac{q_1}{1}$. 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 $p_{i_2} \notin \mathfrak{p}$ și $p_{i_2} \in U(S^{-1}R)$, deci $q_2 \in \mathfrak{p}$ și $\frac{q_1}{1} \sim_{S^{-1}R} \frac{q_2}{1}$. Continuând în acest mod, obținem șirul q, q_1, q_2, \dots de elemente din \mathfrak{p} , cu $q_1|_R q$, $q_2|_R q_1$, ș.a.m.d. În termeni de ideale aceasta înseamnă că $qR \subset q_1R \subset q_2R \subset \dots$. Conform ipotezei, acest șir ascendent de ideale principale este staționar; prin urmare, există un rang n pentru care $q_n \sim_R q_{n+1}$. Deci $\frac{q_n}{1} \sim_{S^{-1}R} \frac{q}{1}$, așadar $\frac{q_n}{1}$ este prim în $S^{-1}R$, și 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 $c = p_{i_1} \cdots p_{i_r}d$, $d \in R$. Obținem $a = q_nd$, deci $q_n|_R a$. Pentru $\frac{q_n}{1}|_{S^{-1}R} \frac{b}{1}$ se procedează analog și se obține $q_n|_R b$. Prin urmare, $q_n \in \mathfrak{p}$ este element prim.

În concluzie, orice ideal prim nenul al lui R conține 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 $\Phi : \mathbb{C}[X, Y] \rightarrow \mathbb{C}[U, V]$ cu proprietățile $\Phi(a) = a$ pentru orice $a \in \mathbb{C}$, $\Phi(X) = \frac{1}{2}(U + V)$, $\Phi(Y) = \frac{1}{2}i(V - U)$ și $\Psi : \mathbb{C}[U, V] \rightarrow \mathbb{C}[X, Y]$ cu proprietățile $\Psi(a) = a$ pentru orice $a \in \mathbb{C}$, $\Psi(U) = X + iY$ și $\Psi(V) = X - iY$ (existența morfismelor Φ și Ψ e asigurată de proprietatea de universalitate a inelelor de polinoame).

Se constată imediat că Φ și Ψ sunt inverse unul celuilalt, deci sunt izomorfisme. Dacă notăm cu π proiecția canonică a lui $\mathbb{C}[U, V]$ pe $\mathbb{C}[U, V]/(UV - 1)$, constatăm imediat că $w = \pi \circ \Phi$ este morfism surjectiv și $\text{Ker } w = (X^2 + Y^2 - 1)$. Aplicând teorema fundamentală de izomorfism pentru inele, obținem

$$\frac{\mathbb{C}[X, Y]}{(X^2 + Y^2 - 1)} \simeq \frac{\mathbb{C}[U, V]}{(UV - 1)}.$$

Cum inelul din membrul drept al relației anterioare este inel euclidian conform punctului (i), demonstrația este încheiată.

23. Să notăm $A = R[X_1, \dots, X_n]$.

„ \Rightarrow ”: Presupunem pentru început că R nu este corp. Atunci există un element $a \in R$ nenul și neinvertibil. 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 $g \in A$ așa 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 $\text{grad}_{X_1}(a) \geq 1$, contradicție. Dacă $\text{grad}_{X_1}(f) = 0$ și $\text{grad}_{X_1}(g) = 1$, avem că $f \in R[X_2, \dots, X_n]$ și $g = P_0 + P_1X_1$, $P_0, P_1 \in R[X_2, \dots, X_n]$. Rezultă $P_0f = 0$ și $P_1f = 1$, de unde $P_0 = 0$ și (constatând că P_1 și 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 relație, obținem $a \in U(R)$, contradicție. Prin urmare, pentru ca A să fie principal, este necesar ca R să fie corp.

Presupunând că $n \geq 2$, considerăm $A = R[X_n][X_1, \dots, X_{n-1}]$. Cum $R[X_n]$ nu este corp, A nu este inel principal conform cazului deja discutat, contradicție. Rămâne așadar că $n = 1$.

„ \Leftarrow ”: Dacă R este corp și $n = 1$, se știe că A este inel euclidian, deci și principal.

24. (i) „ \subseteq ” Fie $x \in P$. Există $\alpha = s + ti\sqrt{3}$ și $\beta = u + vi\sqrt{3}$ astfel încât $x = 2\alpha + (1 + i\sqrt{3})\beta$. După efectuarea calculelor, se obține $x = 2s + u - 3v + (2t + u + v)i\sqrt{3}$. Dacă punem $a = 2s + u - 3v$ și $b = 2t + u + v$, avem $a, b \in \mathbb{Z}$ și $2|2s - 2t - 4v = a - b$.

„ \supseteq ” Dacă $x \in R$ se scrie sub forma $a + bi\sqrt{3}$ cu $a, b \in \mathbb{Z}$ de aceeași 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 \hat{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 $(X^2 + 3) \subset (2, X + 1)$, obținem

$$\frac{R}{P} \simeq \frac{\mathbb{Z}[X]/(X^2 + 3)}{(2, X + 1)/(X^2 + 3)}.$$

Aplicând de două ori teorema a III-a de izomorfism pentru inele deducem

$$\frac{R}{P} \simeq \frac{\mathbb{Z}[X]}{(2, X+1)} \simeq \frac{\mathbb{Z}[X]/(2)}{(2, X+1)/(2)} \stackrel{(*)}{\simeq} \frac{\mathbb{Z}[X]/2\mathbb{Z}[X]}{(0, X+1)} \stackrel{(**)}{\simeq} \frac{\mathbb{Z}_2[X]}{(X+1)} \stackrel{(***)}{\simeq} \mathbb{Z}_2,$$

unde izomorfismele $(*)$ și $(**)$ sunt consecințe ale problemei 14 din Capitolul 5, iar $(***)$ rezultă din problema 13, Capitolul 5. În consecință, R/P este inel integru (chiar corp), deci P este ideal prim (chiar maximal).

Să presupunem acum că P ar fi ideal principal și 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 conține elemente de normă 2. Rămâne că $N(x) = 4$. Cum avem $x|_R 2$, $x|_R 1 + i\sqrt{3}$ și $N(x) = 4 = N(2) = N(1 + i\sqrt{3})$, deducem, conform problemei 3(iii), că $x \sim_R 2$ și $x \sim_R 1 + i\sqrt{3}$. De aici rezultă însă că $2 \sim_R 1 + i\sqrt{3}$, deci $2|_R 1 + i\sqrt{3}$, contradicție. Rămâne așadar 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 și 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 aceeași paritate. Cum 2 și $1 + i\sqrt{3}$ sunt în PR_P , rezultă că există $c, d, e, f, s, t, u, v \in \mathbb{Z}$ astfel încât

$$2 = \frac{c + di\sqrt{3}}{s + ti\sqrt{3}}(a + bi\sqrt{3}), \quad 1 + i\sqrt{3} = \frac{e + fi\sqrt{3}}{u + vi\sqrt{3}}(a + bi\sqrt{3}),$$

unde c, d au aceeași paritate, e, f au aceeași paritate, s, t au parități diferite, u, v au parități diferite. Dacă a și b ar fi pare, cum din a doua relație de mai sus rezultă că $u + v = af + be$, ar rezulta că $u + v$ e par, contradicție. Trebuie deci ca a și b să fie impare. Cum relația $2 = \frac{c+di\sqrt{3}}{s+ti\sqrt{3}}(a + bi\sqrt{3})$ conduce la $ac - 3bd = 2s$ și $ad + bc = 2t$, c și d trebuie să fie impare (altfel, din cele două relații anterioare am obține că s și t au aceeași paritate, absurd). Tot din relația $2 = \frac{c+di\sqrt{3}}{s+ti\sqrt{3}}(a + bi\sqrt{3})$ obținem 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 (ținând cont că s și t au parități diferite) este imposibil.

Rămâne așadar că PR_P nu este ideal principal în R_P . În consecință, R_P nu este inel principal.

(iv) Presupunem că R_P admite cel puțin 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 aceeași paritate.

Dacă a și b sunt pare, atunci 2 divide π în R , deci și în R_P . Rezultă că $\pi = 2x$, cu $x \in R_P$, și singura variantă pentru ca π să fie prim ar fi $\pi \sim_{R_P} 2$. Dacă a și b sunt impare și dau același rest modulo 4, atunci $\pi = a + bi\sqrt{3} = (1 + i\sqrt{3})\left(\frac{a+3b}{4} + \frac{b-a}{4}i\sqrt{3}\right)$. Prin urmare, $1 + i\sqrt{3}$ divide π în R , deci și în R_P . Rezultă că $\pi = (1 + i\sqrt{3})x$, cu $x \in R_P$, și 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 situația în care a și b sunt impare și 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 $1 + i\sqrt{3}$ (și atunci ar exista $c, d \in \mathbb{Z}$ de aceeași paritate și $s, t \in \mathbb{Z}$ de parități diferite astfel ca $2 \cdot \frac{c+di\sqrt{3}}{s+ti\sqrt{3}} = 1 + i\sqrt{3}$, de unde $s + t = 2d$, contradicție) sau pe $1 - i\sqrt{3}$ (și atunci ar exista $c, d \in \mathbb{Z}$ de aceeași paritate și $s, t \in \mathbb{Z}$ de parități diferite astfel ca $2 \cdot \frac{c+di\sqrt{3}}{s+ti\sqrt{3}} = 1 - i\sqrt{3}$, de unde $t - s = 2d$, contradicție). 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 $1 + i\sqrt{3}$ și $1 - i\sqrt{3}$ 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 $\varphi(y) = \min\{\varphi(z) | z \in I \setminus \{0\}\}$. Mulțimea \mathbb{N} fiind bine ordonată, minimum de mai sus există și este număr natural nenul. Fie x un element arbitrar nenul al lui I . Să presupunem că $y \nmid x$. Conform proprietății (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 proprietății (i) și inegalității $\varphi(xu - yv) > 0$. 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 așadar că $I = Ry$. Prin urmare, R este inel principal.

26. Pentru a demonstra că inelele din enunț sunt principale, vom aplica criteriul din problema 25.

Notăm $R = \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ și $N : R \rightarrow \mathbb{N}$, $N(z) = z\bar{z}$. Este evident că, pentru $a \in R$, $N(a) = 0$ dacă și numai dacă $a = 0$. Fie acum $x, y \in R$, $y \neq 0$, $y \nmid x$. Conform problemei 25, demonstrația se încheie dacă arătăm că există $u, v \in R$ astfel ca $0 < N(xu - yv) < N(y)$. Conform problemei 2, N se prelungește la funcția multiplicativă $N : \mathbb{Q}[i\sqrt{19}] \rightarrow \mathbb{Q}$, $N(z) = z\bar{z}$. Relația anterioară se rescrie atunci $0 < N\left(\frac{x}{y}u - v\right) < 1$. 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 $a, b \in \mathbb{Z}$ și $c \in \mathbb{N}$ 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 împărțirii cu rest deducem existența întregilor γ și r cu proprietățile $a\alpha - 19b\beta = c\gamma + r$ și $|r| \leq \frac{c}{2}$.

Dacă $c \geq 6$, alegem $u = \alpha + \beta i\sqrt{19}$ și $v = \gamma + \delta i\sqrt{19}$. Obținem $zu - v = \frac{r+i\sqrt{19}}{c}$, 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 aceleași 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 și b nu pot fi simultan pare. Avem prin urmare de studiat următoarele două cazuri:

1. Dacă a și b sunt de parități diferite, constatăm că $a^2 + 19b^2 \equiv s \pmod{4}$, $s \in \{1, 3\}$. Scriem $a^2 + 19b^2 = 4q + s$ și alegem $u = a - bi\sqrt{19}$ și $v = q$. Rezultă $zu - v = \frac{s}{4}$, deci $N(zu - v) \in (0, 1)$.

2. Dacă a și b sunt impare, atunci $a^2 + 19b^2 \equiv 4 \pmod{8}$. Scriem $a^2 + 19b^2 = 8q + 4$ și alegem $u = \frac{a-bi\sqrt{19}}{2}$ și $v = q$. Rezultă $zu - v = \frac{1}{2}$, deci $N(zu - v) = \frac{1}{4} \in (0, 1)$.

Dacă $c = 3$, să presupunem că $3 \nmid a^2 + 19b^2$. Dacă 3 divide unul dintre numerele a și b , rezultă că îl divide și pe celălalt, contradicție cu $(a, b, c) = 1$. Prin urmare, $3 \nmid a$ și $3 \nmid b$. De aici obținem însă $a^2 + 19b^2 \equiv 2 \pmod{3}$, contradicție. Rămâne așadar că $3 \nmid a^2 + 19b^2$. Scriem $a^2 + 19b^2 = 3q + r$, $r \in \{1, 2\}$ și alegem $u = a - bi\sqrt{19}$ și $v = q$. Rezultă $zu - v = \frac{r}{3}$, deci $N(zu - v) \in (0, 1)$.

Dacă $c = 2$, atunci numerele a și b trebuie să aibă parități diferite (altfel am avea $z \in R$). Atunci $a^2 + 19b^2 \equiv 1 \pmod{4}$. Scriem $a^2 + 19b^2 = 4q + 1$ și

alegem $u = a - bi\sqrt{19}$ și $v = q$. Rezultă $zu - v = \frac{1}{2}$, deci $N(zu - v) = \frac{1}{4} \in (0, 1)$.

Notăm $R = \mathbb{Z}\left[\frac{1+i\sqrt{43}}{2}\right]$ și $N : R \rightarrow \mathbb{N}$, $N(z) = z\bar{z}$. Este evident că, pentru $a \in R$, $N(a) = 0$ dacă și numai dacă $a = 0$; Fie acum $x, y \in R$, $y \neq 0$, $y \nmid x$. Conform problemei 25, demonstrația se încheie dacă arătăm că există $u, v \in R$ astfel ca $0 < N(xu - yv) < N(y)$. Conform problemei 2, N se prelungește la funcția multiplicativă $N : \mathbb{Q}[i\sqrt{43}] \rightarrow \mathbb{Q}$, $N(z) = z\bar{z}$. Relația 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 $a, b \in \mathbb{Z}$ și $c \in \mathbb{N}$ 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 împărțirii cu rest deducem existența întregilor γ și r cu proprietățile $a\alpha - 43b\beta = c\gamma + r$ și $|r| \leq \frac{c}{2}$.

Dacă $c \geq 8$, alegem $u = \alpha + \beta i\sqrt{43}$ și $v = \gamma + \delta i\sqrt{43}$. Obținem $zu - v = \frac{r+i\sqrt{43}}{c}$, 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 $c \mid a^2 + 43b^2$. Dacă c divide unul dintre numerele a și b , rezultă că îl divide și pe celălalt, contradicție cu $(a, b, c) = 1$.

Prin urmare, $c \nmid a$ și $c \nmid b$. De aici obținem 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 și am obținut astfel o contradicție.

Rămâne așadar că $c \nmid a^2 + 43b^2$. Scriem $a^2 + 43b^2 = cq + r$, $r \in \{1, \dots, c-1\}$ și alegem $u = a - bi\sqrt{43}$ și $v = q$. Rezultă $zu - v = \frac{r}{c}$, deci $N(zu - v) \in (0, 1)$.

Dacă $c = 6$, putem face aceleași alegeri de la cazul precedent. Faptul că $6 \nmid a^2 + 43b^2$ rezultă din relația $3 \nmid a^2 + 43b^2$ demonstrată în cazul anterior.

Dacă $c = 4$, observăm că a și b nu pot fi simultan pare. Avem prin urmare de studiat următoarele două cazuri:

1. Dacă a și b sunt de parități diferite, constatăm că $a^2 + 43b^2 \equiv s \pmod{4}$, $s \in \{1, 3\}$. Scriem $a^2 + 43b^2 = 4q + s$ și alegem $u = a - bi\sqrt{43}$ și $v = q$. Rezultă $zu - v = \frac{s}{4}$, deci $N(zu - v) \in (0, 1)$.

2. Dacă a și b sunt impare, atunci $a^2 + 43b^2 \equiv 4 \pmod{8}$. Scriem $a^2 + 43b^2 = 8q + 4$ și alegem $u = \frac{a-bi\sqrt{43}}{2}$ și $v = q$. Rezultă $zu - v = \frac{1}{2}$, deci $N(zu - v) = \frac{1}{4} \in (0, 1)$.

Dacă $c = 2$, atunci numerele a și b trebuie să aibă parități diferite (altfel am avea $z \in R$). Atunci $a^2 + 43b^2 \equiv 1 \pmod{4}$. Scriem $a^2 + 43b^2 = 4q + 1$ și alegem $u = a - bi\sqrt{43}$ și $v = q$. Rezultă $zu - v = \frac{1}{2}$, deci $N(zu - v) = \frac{1}{4} \in (0, 1)$.

Notăm $R = \mathbb{Z}\left[\frac{1+i\sqrt{67}}{2}\right]$ și $N : R \rightarrow \mathbb{N}$, $N(z) = z\bar{z}$. Este evident că, pentru $a \in R$, $N(a) = 0$ dacă și numai dacă $a = 0$; Fie acum $x, y \in R$, $y \neq 0$, $y \nmid x$. Conform problemei 25, demonstrația se încheie dacă arătăm că există $u, v \in R$ astfel ca $0 < N(xu - yv) < N(y)$. Conform problemei 2, N se prelungește la funcția multiplicativă $N : \mathbb{Q}[i\sqrt{67}] \rightarrow \mathbb{Q}$, $N(z) = z\bar{z}$. Relația 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 $a, b \in \mathbb{Z}$ și $c \in \mathbb{N}$ 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 împărțirii cu rest deducem existența întregilor γ și r cu proprietățile $a\alpha - 67b\beta = c\gamma + r$ și $|r| \leq \frac{c}{2}$.

Dacă $c \geq 10$, alegem $u = \alpha + \beta i\sqrt{67}$ și $v = \gamma + \delta i\sqrt{67}$. Obținem $zu - v = \frac{r+i\sqrt{67}}{c}$, 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 și b , rezultă că îl divide și pe celălalt, contradicție cu $(a, b, c) = 1$. Prin urmare, $3 \nmid a$ și $3 \nmid b$. De aici obținem însă $a^2 + 67b^2 \equiv 2 \pmod{3}$, contradicție.

Rămâne așadar că $3 \nmid a^2 + 67b^2$, de unde obținem și $6 \nmid a^2 + 67b^2$ și $9 \nmid a^2 + 67b^2$. Putem deci scrie $a^2 + 67b^2 = cq + r$ cu $r \in \{1, \dots, c-1\}$. Alegem $u = a - bi\sqrt{67}$ și $v = q$. Rezultă $zu - v = \frac{r}{c}$, deci $N(zu - v) \in (0, 1)$.

Dacă $c = 8$, observăm că a și 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 $a^2 + 67b^2 = 8q + s$ și alegem $u = a - bi\sqrt{67}$ și $v = q$. Obținem $zu - v = \frac{s}{8}$, 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 și b , rezultă că îl divide și pe celălalt, contradicție cu $(a, b, c) = 1$.

Prin urmare, $c \nmid a$ și $c \nmid b$; de aici obținem însă $\widehat{-67} = (\widehat{ab^{-1}})^2$ 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 și am obținut astfel o contradicție.

Rămâne așadar că $c \nmid a^2 + 67b^2$. Scriem $a^2 + 67b^2 = cq + r$, $r \in \{1, \dots, c-1\}$ și alegem $u = a - bi\sqrt{67}$ și $v = q$. Rezultă $zu - v = \frac{r}{c}$, deci $N(zu - v) \in (0, 1)$. Dacă $c = 4$, observăm că a și b nu pot fi simultan pare. Avem prin urmare de studiat următoarele două cazuri:

1. Dacă a și b sunt de parități diferite, constatăm că $a^2 + 67b^2 \equiv s \pmod{4}$, $s \in \{1, 3\}$. Scriem $a^2 + 67b^2 = 4q + s$ și alegem $u = a - bi\sqrt{67}$ și $v = q$. Rezultă $zu - v = \frac{s}{4}$, deci $N(zu - v) \in (0, 1)$.

2. Dacă a și b sunt impare, atunci $a^2 + 67b^2 \equiv 4 \pmod{8}$. Scriem $a^2 + 67b^2 = 8q + 4$ și alegem $u = \frac{a-bi\sqrt{67}}{2}$ și $v = q$. Rezultă $zu - v = \frac{1}{2}$, deci $N(zu - v) = \frac{1}{4} \in (0, 1)$.

Dacă $c = 2$, atunci numerele a și b trebuie să aibă parități diferite (altfel am avea $z \in R$). Atunci $a^2 + 67b^2 \equiv 1 \pmod{4}$. Scriem $a^2 + 67b^2 = 4q + 1$ și alegem $u = a - bi\sqrt{67}$ și $v = q$. Rezultă $zu - v = \frac{1}{2}$, deci $N(zu - v) = \frac{1}{4} \in (0, 1)$.

Notăm $R = \mathbb{Z}\left[\frac{1+i\sqrt{163}}{2}\right]$ și $N : R \rightarrow \mathbb{N}$, $N(z) = z\bar{z}$. Este evident că, pentru $a \in R$, $N(a) = 0$ dacă și numai dacă $a = 0$. Fie acum $x, y \in R$, $y \neq 0$, $y \nmid x$. Conform problemei 25, demonstrația se încheie dacă arătăm că există $u, v \in R$ astfel ca $0 < N(xu - yv) < N(y)$. Conform problemei 2, N se prelungește la funcția multiplicativă $N : \mathbb{Q}[i\sqrt{163}] \rightarrow \mathbb{Q}$, $N(z) = z\bar{z}$. Relația 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 $a, b \in \mathbb{Z}$ și $c \in \mathbb{N}$ 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 împărțirii cu rest deducem existența întregilor γ și r cu proprietățile $a\alpha - 163b\beta = c\gamma + r$ și $|r| \leq \frac{c}{2}$.

Dacă $c \geq 15$, alegem $u = \alpha + \beta i\sqrt{163}$ și $v = \gamma + \delta i\sqrt{163}$. Obținem $zu - v = \frac{r+i\sqrt{163}}{c}$, 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 $c \mid a^2 + 163b^2$. Dacă c divide unul dintre numerele a și b , rezultă că îl divide și pe celălalt, contradicție cu $(a, b, c) = 1$. Prin urmare, $c \nmid a$ și $c \nmid b$. De aici obținem însă $\widehat{-163} = \widehat{(ab^{-1})}^2$ 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 și am obținut astfel o contradicție.

Rămâne așadar că $c \nmid a^2 + 163b^2$. Scriem $a^2 + 163b^2 = cq + r$, $r \in \{1, \dots, c-1\}$ și alegem $u = a - bi\sqrt{163}$ și $v = q$. Rezultă $zu - v = \frac{r}{c}$, deci $N(zu - v) \in (0, 1)$. Dacă $c = 14$, din afirmația $7 \nmid a^2 + 163b^2$ demonstrată la cazul anterior rezultă $14 \nmid a^2 + 163b^2$. Scriem $a^2 + 163b^2 = 14q + r$, $r \in \{1, \dots, 13\}$ și alegem $u = a - bi\sqrt{163}$ și $v = q$. Rezultă $zu - v = \frac{r}{14}$, deci $N(zu - v) \in (0, 1)$.

Dacă $c = 10$, din afirmația $5 \nmid a^2 + 163b^2$ demonstrată anterior rezultă $10 \nmid a^2 + 163b^2$. Scriem $a^2 + 163b^2 = 10q + r$, $r \in \{1, \dots, 9\}$ și alegem $u = a - bi\sqrt{163}$ și $v = q$. Rezultă $zu - v = \frac{r}{10}$, deci $N(zu - v) \in (0, 1)$.

Dacă $c \in \{3, 6, 9, 12\}$, să presupunem că $3 \mid a^2 + 163b^2$.

Dacă 3 divide unul dintre numerele a și b , rezultă că îl divide și pe celălalt, contradicție cu $(a, b, c) = 1$. Prin urmare, $3 \nmid a$ și $3 \nmid b$. De aici obținem însă $a^2 + 163b^2 \equiv 2 \pmod{3}$, contradicție.

Rămâne așadar că $3 \nmid a^2 + 163b^2$, de unde obținem și relațiile $6 \nmid a^2 + 163b^2$, $9 \nmid a^2 + 163b^2$ și $12 \nmid a^2 + 163b^2$. Putem deci scrie $a^2 + 163b^2 = cq + r$ cu $r \in \{1, \dots, c-1\}$. Alegem $u = a - bi\sqrt{163}$ și $v = q$. Rezultă $zu - v = \frac{r}{c}$, deci $N(zu - v) \in (0, 1)$.

Dacă $c = 8$, observăm că a și b nu pot fi simultan pare (altfel am avea $2 \mid (a, b, c) = 1$). Prin urmare, $a^2 + 163b^2$ este congruent cu $s \in \{1, 3, 4\}$ modulo 8. Scriem $a^2 + 163b^2 = 8q + s$ și alegem $u = a - bi\sqrt{163}$ și $v = q$. Obținem $zu - v = \frac{s}{8}$, de unde $N(zu - v) \in [\frac{1}{8}, \frac{1}{4}] \subset (0, 1)$.

Dacă $c = 4$, observăm că a și b nu pot fi simultan pare. Avem prin urmare de studiat următoarele două cazuri:

1. Dacă a și b sunt de parități diferite, constatăm că $a^2 + 163b^2 \equiv s \pmod{4}$, $s \in \{1, 3\}$. Scriem $a^2 + 163b^2 = 4q + s$ și alegem $u = a - bi\sqrt{163}$ și $v = q$. Rezultă $zu - v = \frac{s}{4}$, deci $N(zu - v) \in (0, 1)$.

2. Dacă a și b sunt impare, atunci $a^2 + 163b^2 \equiv 4 \pmod{8}$. Scriem $a^2 + 163b^2 = 8q + 4$ și alegem $u = \frac{a - bi\sqrt{163}}{2}$ și $v = q$. Rezultă $zu - v = \frac{1}{2}$, deci $N(zu - v) = \frac{1}{4} \in (0, 1)$.

Dacă $c = 2$, atunci numerele a și b trebuie să aibă parități diferite (altfel am avea $z \in R$). Atunci $a^2 + 163b^2 \equiv 1 \pmod{4}$. Scriem $a^2 + 163b^2 = 4q + 1$ și alegem $u = a - bi\sqrt{163}$ și $v = q$. Rezultă $zu - v = \frac{1}{2}$, deci $N(zu - v) = \frac{1}{4} \in (0, 1)$.

Faptul că inelele din enunț nu sunt euclidiene rezultă din problema 18.

Observație. 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 $d \in \{1, 2\}$ și că singurele inele principale de forma $\mathbb{Z}\left[\frac{1+i\sqrt{d}}{2}\right]$, $d \in \mathbb{N}$ de forma $4k + 3$ și liber de pătrate, sunt cele corespunzătoare valorilor

$d \in \{3, 7, 11, 19, 43, 67, 163\}$.

27. Notăm $A = R[[X]]$ și definim $u : R[[X]] \rightarrow R$ 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 conține un element prim.

Fie P un ideal prim nenul al lui A . X fiind element prim în A , afirmația 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 $f = a + a_1X + a_2X^2 + \dots$. Cum $f \in P$, $Af \subset P$. Fie acum $g = b_0 + b_1X + \dots \in P$. 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 și 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 șirurile $(g_n)_{n \geq 1}$, $g_n \in P$ și $(c_n)_{n \geq 0}$, $c_n \in A$, astfel: g_1 și c_0 sunt cele de mai sus. Presupunem construiți c_0, c_1, \dots, c_{k-1} și g_k astfel încât $g = (c_0 + c_1X + \dots + c_{k-1}X^{k-1})f + X^k g_k$. Atunci există $c_k \in R$ astfel încât $u(g_k) = c_k a$. Deci $g_k - c_k f$ nu are termen liber. Definim g_{k+1} astfel încât $g_k - c_k f = Xg_{k+1}$; cum $g_k, c_k f \in P$, obținem $Xg_{k+1} \in P$; dar $X \notin P$, deci $g_{k+1} \in P$. În plus, $g = (c_0 + c_1X + \dots + c_{k-1}X^{k-1})f + X^k(c_k f + Xg_{k+1}) = (c_0 + \dots + c_k X^k)f + X^{k+1}g_{k+1}$.

Dacă notăm acum $h = c_0 + c_1X + c_2X^2 + \dots \in A$, atunci g și hf vor avea aceiași coeficienți pentru $1, X, X^2, \dots, X^k$, pentru orice $k \in \mathbb{N}$ și prin urmare $g = hf$.

În concluzie, $P = Af$. Cum P este ideal prim, rezultă că f este element prim și demonstrația este încheiată.

28. Vom nota clasele elementelor X, Y și Z modulo $(X^r + Y^s + Z^t)$ cu x, y , respectiv z .

(i) Dacă t este impar, considerăm morfismul $\varphi : k[X, Y, Z] \rightarrow k[X, Y, Z]$, $\varphi(f) = f(X, Y, -Z)$, a cărui existență 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 și s impare. Reluăm atunci raționamentul anterior folosind $\psi : k[X, Y, Z] \rightarrow k[X, Y, Z]$, $\psi(f) = f(-X, -Y, Z)$ și 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, $z = x^r w^{t-1} + y^s w^{t-1}$, 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 $u = w^{\alpha s} x$ și $v = w^{\alpha r} y$. 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, $x = u z^{\alpha s} = u(u^r + v^s)^{\alpha s} \in k[u, v, (u^r + v^s)^{-1}]$, $y = v z^{\alpha r} = v(u^r + v^s)^{\alpha r} \in k[u, v, (u^r + v^s)^{-1}]$, iar $w = (u^r + v^s)^{-1} \in k[u, v, (u^r + v^s)^{-1}]$. Obținem și 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 $P = \sum_{i,j} a_{ij} U^i V^j \in k[U, V]$. 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 același numitor și obținem o relație de tipul $\sum_{i,j} a_{ij} x^i y^j z^{n-\alpha(si+rj)} = 0$, ceea ce înseamnă că există $F \in k[X, Y, Z]$

astfel ca $\sum_{i,j} a_{ij} X^i Y^j Z^{n-\alpha(si+rj)} = (X^r + Y^s - Z^t) F$. Conform proprietății de universalitate a inelelor de polinoame, există un morfism de inele $\chi : k[X, Y, Z] \rightarrow k[C, D, Z]$, $\chi(f) = f(C^{\alpha s}, D^{\alpha r}, Z)$. Aplicând χ în relația de mai sus, obținem $\sum_{i,j} a_{ij} C^{\alpha is} D^{\alpha jr} Z^{n-\alpha(si+rj)} = (C^{t-1} + D^{t-1} - Z^t) \chi(F)$.

Cum polinomul din membrul stâng al relației 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 $\sum_{i,j} a_{ij} X^i Y^j Z^{n-\alpha(si+rj)} = 0$, de unde $P = 0$. În consecință, morfismul $\phi : k[U, V] \rightarrow k[u, v]$, $\phi(P) = P(u, v)$, 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 $u^r + v^s$, obținem, conform problemei 20, că și 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 și teorema a III-a de izomorfism pentru

inele, obținem izomorfisme

$$\frac{R}{zR} \simeq \frac{\frac{k[X,Y,Z]}{(X^r+Y^s-Z^t)}}{\frac{(Z, X^r+Y^s-Z^t)}{(X^r+Y^s-Z^t)}} \simeq \frac{k[X,Y,Z]}{(X^r+Y^s, Z)} \simeq \frac{\frac{k[X,Y,Z]}{(Z)}}{\frac{(X^r+Y^s, Z)}{(Z)}} \simeq \frac{k[X,Y]}{(X^r+Y^s)}.$$

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, obținem (vezi problema 24 din capitolul 4) că R este și el noetherian, deci orice lanț ascendent de ideale principale este staționar. Conform criteriului lui Nagata (vezi problema 21), R este inel factorial.

(ii) Considerăm în R sistemul multiplicativ $S = \{1, x, x^2, \dots\}$. Notăm $S' = \{a_0 + a_1X + \dots \in R[[X]] \mid a_0 \in S\}$. S' este în mod clar un sistem multiplicativ al lui R . Notăm $A = R[[X]]$, $B = S^{-1}A$, $B' = (S')^{-1}A$ și $\widehat{B} = (S^{-1}R)[[X]]$. Incluziunile $A \subset B \subset B'$ sunt evidente. Pe de altă parte, dacă $a_0 + a_1X + \dots \in S'$, atunci există $n_0 \in \mathbb{N}$ astfel încât $a_0 = x^{n_0}$. Dacă considerăm sistemul de relații $c_0^{n_0}b_0 = 1$ și $\sum_{i+j=n} a_i b_j = 0$ pentru fiecare

$n \in \mathbb{N}^*$, atunci $b_0 = \frac{1}{c_0^{n_0}}$, iar dacă presupunem pentru $n \geq 1$ că toți b_j , $j \in \{0, 1, \dots, m-1\}$, sunt de forma $\frac{\alpha_j}{c_0^{n_j}}$, din relația $\sum_{i+j=m} a_i b_j = 0$ deducem $b_m = - \sum_{\substack{i+j=m \\ j \neq m}} \frac{a_i \alpha_j}{c_0^{n_j}}$. Aducând fracțiile din suma din membrul drept la

același numitor rezultă că există $n_m \in \mathbb{N}$ și $\alpha_m \in R$ așa încât $b_m = \frac{\alpha_m}{c_0^{n_m}}$. Am demonstrat deci prin inducție că există un șir $(b_n)_{n \in \mathbb{N}}$ de elemente din $S^{-1}R$ cu proprietatea că $(a_0 + a_1X + \dots)(b_0 + b_1X + \dots) = 1$. De aici rezultă, folosind proprietatea de universalitate a inelelor de fracții, 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 $y + a_1X + a_2X^2 + \dots$ cu $a_i \in R$ pentru fiecare $i \in \mathbb{N}^*$.

Într-adevăr, să presupunem contrariul. Atunci putem scrie o relație de tipul

$(xy - z^{t-1}X) \left(\frac{c_0}{x^{n_0}} + \frac{c_1}{x^{n_1}}X + \dots \right) = y + a_1X + a_2X^2 + \dots$, unde pentru fiecare $i \in \mathbb{N}$ $c_i \in R$ și $n_i \in \mathbb{N}$. Rezultă $\frac{c_0}{x^{n_0}} = \frac{1}{x}$ și $c_1yx^{1-n_1} - z^{t-1}x^{-1} = a_1 \in R$, 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 și teorema a III-a de izomorfism pentru inele, obținem

$$\frac{R}{yR} \simeq \frac{k[X, Y, Z]}{(Y, X^r + Y^s - Z^t)} \simeq \frac{\frac{k[X, Y, Z]}{(Y)}}{(Y, X^r + Y^s - Z^t)} \simeq \frac{k[X, Z]}{(X^r - Z^t)}.$$

Dacă t este impar, considerăm morfismul $\varphi : k[X, Z] \rightarrow k[X, Z]$, $\varphi(f) = f(X, -Z)$, a cărui existență 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 raționamentul anterior folosind $\psi : k[X, Z] \rightarrow k[X, Z]$, $\psi(f) = f(-X, Z)$ și 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 $x \notin yR$, relația $dx^{n_1-2} \in Ry$ ne dă $d \in Ry$. Există deci $e \in R$ astfel ca $d = ey$. Înlocuind în $c_1y - x^{n_1-2}z^{t-1} \in Rx^{n_1-1}$, obținem $eyx^{n_1-2} - x^{n_1-2}z^{t-1} \in Rx^{n_1-1}$, 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 relație nedeterminatelor X și Y valoarea 0, obținem contradicția $Z^t | Z^{t-1}E(0, 0, Z)$ și demonstrația afirmației pasului I este încheiată.

Pasul II: Demonstrăm că există un număr natural a și o serie formală $v' = y^a x^{-1} + b_1 x^{-2} X + \dots + b_m X^{-m-1} X^m + \dots \in \widehat{B}$, 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, \dots ale lui R astfel încât coeficienții lui u să fie în R . În scrierea lui u avem termenul liber $y^{t+1} \in R$, coeficientul lui X egal cu $b_1 y x^{-1} - z^{t-1} y^a x^{-1}$, iar pentru $l \geq 2$ coeficientul lui X^l egal cu $b_l y x^{-l} - b_{l-1} z^{t-1} x^{-l}$. Pentru ca acești coeficienți să se afle în R , este necesar și suficient ca $b_1 y - z^{t-1} y^a \in Rx$ și $b_l y - z^{t-1} b_{l-1} \in Rx^l$ pentru orice $l \geq 2$. Realizăm acum construcția inductivă a șirului $(b_m)_{m \geq 1}$: Alegem $b_1 = z^{t-1} y^{a-1}$, $b_2 = z^{2(t-1)} y^{a-2}$, \dots , $b_{rt-1} = z^{(rt-1)(t-1)} y^{a-rt+1}$ și numărul natural $a \geq rt$ și constatăm că $b_1, \dots, b_{rt-1} \in R$. Pentru alegerea lui b_{rt} , vom ține cont că trebuie îndeplinită relația $b_{rt} y - z^{rt(t-1)} y^{a-rt+1} = b_{rt} y - z^{t-1} b_{rt-1} \in$

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 $f_1(U, V) = \sum_{k=0}^t C_{n(t-1)}^k U^k V^{t-k} \in R[U, V]$ este evident un polinom omogen

de grad t . Relația anterioară se scrie atunci $b_{rt}y - y^{s(rt-r-t)-rt+a+1} f_1(x^r, y^s) \in Rx^{rt}$ și se vede că putem alege $b_{rt} = y^{rst-rs-rt-st+a} f_1(x^r, y^s)$. Cum $r, s \geq 2$ și $r \neq s$, avem $t(rs - r - s) \geq t$. În plus, din $t \equiv 1 \pmod{rs}$ se obține $t > rs$. În consecință, exponentul lui y din scrierea lui b_{rt} este mai mare decât a .

Să presupunem acum că am construit $b_1, b_2, \dots, b_{(l-1)rt}$, $l \geq 2$, în așa 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 coeficienți în R , iar $\varphi(l-1)$ este un număr natural cu proprietatea $\varphi(l-1) \geq a \geq rt$. Pentru fiecare $j \in \{1, \dots, rt-1\}$ alegem $b_{(l-1)rt+j} = z^{j(t-1)} y^{\varphi(l-1)-j} f_{l-1}(x^r, y^s)$ și constatăm că aceste valori verifică relațiile $b_{(l-1)rt+j} - z^{t-1} b_{(l-1)rt+j-1} \in Rx^{(l-1)rt+j}$. Pentru alegerea lui b_{lrt} , vom ține cont că trebuie îndeplinită relația $b_{lrt}y - z^{t-1} b_{lrt-1} \in Rx^{lrt}$, 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 relația pe care dorim să o obținem 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 și y^s . Termenii din această expresie în care x apare la putere cel mult lrt vor avea exponentul lui y^s cel puțin $r(t-1) + (l-1)t - lt$, 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 coeficienți în R . În consecință, 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 inducție și demonstrația afirmației 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 $F \in B'$ și $m, n \in \mathbb{N}$ avem relația $(F + (X)^m) \cap (F + (X)^n) = F + (X)^{\max\{m,n\}}$. 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 vecinătăți.

Fie acum $F \in v\widehat{B} \cap B'$. Există atunci $G = \frac{a_0}{x^{n_0}} + \frac{a_1}{x^{n_1}} X + \dots \in \widehat{B}$ așa încât

Fie acum $F \in \overline{vB'}$. Atunci trebuie ca pentru orice $n \in \mathbb{N}$ să existe $F_n \in vB'$ așa încât $F_n \in F + (X)^n$, altfel spus, $F \in vB' \cap (X)^n$ pentru fiecare $n \in \mathbb{N}$. Deducem că $\overline{vB'} \subset \bigcap_{n \in \mathbb{N}} (vB' + (X)^n)$.

$I = \bigcap_{n \in \mathbb{N}} (\tilde{X})^n$. Dacă $\tilde{F} \in I$, atunci $\tilde{F} \in (\tilde{X})$, deci există $G \in B'$ astfel încât $\tilde{F} = \tilde{X}\tilde{G}$. Fie $n \in \mathbb{N}^*$. Atunci există $F_n \in B'$ astfel ca $\tilde{F} = \tilde{X}^n \widetilde{F_n}$, de unde $XG - X^n F_n \in vB'$. Scriind $XG - X^n F_n = vH$, $H \in B'$, constatăm folosind o observație 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 $\tilde{G} = \tilde{X}^{n-1} \widetilde{F_n}$. Am obținut deci $\tilde{G} \in I$. În consecință, $I \subset (X)I$. Incluziunea contrară fiind evidentă, obținem $I = (X)I$.

$$\begin{aligned} (1 - \widetilde{XG}_{11})\widetilde{F}_1 - \widetilde{G}_{12}\widetilde{F}_2 - \cdots - \widetilde{G}_{1k}\widetilde{F}_k &= 0 \\ -\widetilde{G}_{21}\widetilde{F}_1 + (1 - \widetilde{XG}_{22})\widetilde{F}_2 - \cdots - \widetilde{G}_{2k}\widetilde{F}_k &= 0 \\ \vdots & \\ -\widetilde{G}_{k1}\widetilde{F}_1 - \widetilde{G}_{k2}\widetilde{F}_2 - \cdots + (1 - \widetilde{XG}_{kk})\widetilde{F}_k &= 0 \end{aligned}$$

Considerăm aceste relații ca fiind un sistem de ecuații cu necunoscutele $\widetilde{F}_1, \dots, \widetilde{F}_k$. Matricea acestui sistem este

$$M = \begin{pmatrix} (1 - \widetilde{X}\widetilde{G}_{11}) & -\widetilde{G}_{12} & \dots & -\widetilde{G}_{1k} \\ -\widetilde{G}_{21} & (1 - \widetilde{X}\widetilde{G}_{22}) & \dots & -\widetilde{G}_{2k} \\ \dots & \dots & \dots & \dots \\ -\widetilde{G}_{k1} & -\widetilde{G}_{k2} & \dots & (1 - \widetilde{X}\widetilde{G}_{kk}) \end{pmatrix}$$

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 fracție și aducem la același numitor, constatăm că numărătorul obținut este în S' . Prin urmare, $1 + XH \in U(B')$, de unde $\det M \in U(\frac{B'}{vB'})$. Scriind sistemul sub formă matriceală și înmulțind cu adjuncta lui M , obținem $(\det M) \cdot \widetilde{F}_i = 0$ pentru fiecare $i = \overline{1, k}$. De aici rezultă că toți generatorii lui I sunt nuli, deci $I = (0)$. Rezultă $\bigcap_{n \in \mathbb{N}} (vB' + (X)^n) = \pi^{-1}(I) = vB'$. Folosind și relațiile obținute anterior, obținem $v\widehat{B} \cap B' \subset vB'$ și relația $v\widehat{B} \cap B' = vB'$ 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 $u = y^{a+1} + a_1X + a_2X^2 + \dots$ cu $a_i \in R$ pentru orice $i \in \mathbb{N}^*$. Fie $u = u_1u_2 \dots u_m$ 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 $\theta : A \rightarrow \frac{R}{yR}[[X]]$, $\theta(a_0 + a_1X + \dots) = \overline{a_0} + \overline{a_1}X + \dots$, și constatăm că nucleul său este yA . Prin urmare, $A/yA \simeq \frac{R}{yR}[[X]]$, iar inelul din membrul drept este integru. Se obține că yA este ideal prim al lui A , deci y este prim și 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 soluției problemei 20, elementele $u_j, j = \overline{1, m}$ sunt prime și în B' . Cum $v' \in \widehat{B}$, obținem 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 obține $v(v' - v'') = 0$, de unde, \widehat{B} fiind domeniu, $v' = v'' \in B'$. Observăm că v este element ireductibil al lui B' (dacă $v = \frac{a_0 + a_1X + \dots}{x^p + b_1X + \dots} \cdot \frac{c_0 + c_1X + \dots}{x^q + d_1X + \dots}$, atunci $x^{p+q+1}y = a_0c_0$, de unde, ținând cont de factorialitatea lui R , unul dintre elementele a_0 și c_0 este putere de x , iar factorul corespunzător este inversabil în B'). Din relația $vv' = u_1 \dots u_m$ și din factorialitatea lui B' rezultă că v este asociat în B' cu

unul dintre u_1, \dots, u_m , fie el u_j . Dacă ținem 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 $y + a_1X + a_2X^2 + \dots$ cu $a_i \in R$ pentru fiecare $i \in \mathbb{N}^*$, ceea ce contrazice pasul I și încheie demonstrația.

29. Notăm $R = \mathbb{Z}[i\sqrt{6}]$. Relația $-i\sqrt{6} \cdot i\sqrt{6} = 6 = 2 \cdot 3$ ne arată că $i\sqrt{6} \mid_R 2 \cdot 3$; este clar însă (vezi problema 1) că $i\sqrt{6}$ nu divide în R nici unul din acești 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 obține $6 = N(a)N(b)$, de unde $N(a) = 2$ și $N(b) = 3$ (sau viceversa). Dar în R nu există elemente de normă 2 (și nici de normă 3), contradicție. Așadar $i\sqrt{6}$ este ireductibil în R , dar nu este prim. De aici rezultă că R nu este inel factorial.

Notăm $R = \mathbb{Z}[\sqrt{10}]$. Relația $(\sqrt{10})^2 = 10 = 2 \cdot 5$ ne arată că $2 \mid_R (\sqrt{10})^2$; 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 obține $4 = N(a)N(b)$, de unde $N(a) = N(b) = 2$. Cum însă niciun pătrat perfect nu se termină în 2 sau în 8, relația $|x^2 - 10y^2| = 2$ este imposibilă în numere întregi, prin urmare în R nu există elemente de normă 2, contradicție. Așadar, 2 este ireductibil în R , dar nu este prim. De aici rezultă că R nu este inel factorial.

Notăm $R = \mathbb{Z}[\sqrt{26}]$. Relația $(\sqrt{26} - 1)(\sqrt{26} + 1) = 25 = 5 \cdot 5$ ne arată că $5 \mid_R (\sqrt{26} - 1)(\sqrt{26} + 1)$; este clar însă (vezi problema 1) că 5 nu divide în R nici unul din acești 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 obține $5 = N(a)N(b)$, 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 așa încât $|x^2 - 26y^2| = 5$, deci $x^2 \equiv \pm 5 \pmod{13}$, ceea ce ar însemna că unul dintre elementele $\widehat{5}$ și $\widehat{8}$ este pătrat în \mathbb{Z}_{13} , absurd) și ajungem astfel la o contradicție. Prin urmare, 5 este ireductibil în R , dar nu este prim. De aici rezultă că R nu este inel factorial.

Notăm $R = K[X, Y, Z, T]/(XT - YZ)$ și $x = \widehat{X}$, $y = \widehat{Y}$, $z = \widehat{Z}$, $t = \widehat{T}$. Avem că $R = K[x, y, z, t]$ și $xt = yz$. Polinomul $XT - YZ \in K[X, Y, Z, T] \simeq K[Y, Z, T][X]$ este de gradul întâi și 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 și prin urmare R este inel integru.

Vom prezenta două soluții pentru faptul că R nu este inel factorial.

Soluția 1. Polinoamele din $K[X, Y]$ se scriu în mod unic ca sumă de polinoame omogene. Această proprietate se transmite și 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 privește unicitatea, este suficient să demonstrăm că dacă $f_0(x, y, z, t) + f_1(x, y, z, t) + \dots + f_n(x, y, z, t) = 0$ (unde f_j este polinom omogen de grad j pentru fiecare $j \in \{0, 1, \dots, n\}$), atunci $f_0(x, y, z, t) = f_1(x, y, z, t) = \dots = f_n(x, y, z, t) = 0$. Dar $f_0(x, y, z, t) + \dots + f_n(x, y, z, t) = 0$ înseamnă $XT - YZ|_{K[X, Y, Z, T]} f_0(X, Y, Z, T) + f_1(X, Y, Z, T) + \dots + f_n(X, Y, Z, T)$. Există deci $g = g_0 + g_1 + \dots + g_m \in K[X, Y, Z, T]$, g_i omogen de grad i pentru orice $i \in \{0, 1, \dots, m\}$, astfel ca $f_0(X, Y, Z, T) + f_1(X, Y, Z, T) + \dots + f_n(X, Y, Z, T) = (XT - YZ)g$. Identificând componentele omogene din cei doi membri obținem $m = n - 2$, $f_0(X, Y, Z, T) = 0$, $f_1(X, Y, Z, T) = 0$ și $f_j(X, Y, Z, T) = (XT - YZ)g_{j-2}(X, Y, Z, T)$ pentru orice $j \in \{2, 3, \dots, n\}$. 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 $j \in \{0, 1, \dots, n\}$.

Fie acum $x = fg$ o scriere a lui x ca produs de elemente din R . Constatăm că f și g trebuie să fie omogene, deoarece dacă unul din ele ar avea cel puțin două componente omogene, produsul lor (și deci și x) ar avea aceeași proprietate, absurd. În plus, $\text{grad } f = 0$ și $\text{grad } g = 1$ sau invers. Rezultă așadar că unul din factorii produsului considerat este inversabil. Prin urmare, x este ireductibil în R .

Relația $xt = yz$ 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 $XT - YZ|_{K[X, Y, Z, T]} uX - Z$, 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.

Soluția 2. Să demonstrăm pentru început că orice element din R se scrie în mod unic sub forma $\overline{F_1(X)} + \overline{T F_2(T)}$ cu $F_1, F_2 \in K[Y, Z][U]$. Cum $K[X, Y, Z, T] \simeq K[Y, Z][X, T]$, orice element \bar{f} din R se poate scrie sub forma $\sum a_{ij} X^i T^j$ cu $a_{ij} \in K[Y, Z]$. Cum $\overline{XT} = \overline{YZ}$, \bar{f} se rescrie $\sum_{i \geq j} a_{ij} Y^j Z^j X^{i-j} + \sum_{i < j} a_{ij} Y^i Z^i T^{j-i} = \sum_{i \geq j} a_{ij} Y^j Z^j X^{i-j} + \overline{T \sum_{i < j} a_{ij} Y^i Z^i T^{j-i-1}}$ și am probat astfel existența unei scrieri de tipul menționat. Pentru a proba unicitatea acestui tip de scriere, considerăm egalitatea $\overline{F_1(X)} + \overline{T F_2(T)} = \overline{F'_1(X)} +$

$\overline{TF'_2(T)}$. 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 coeficienților polinoamelor $F_1 - F'_1, F_2 - F'_2 \in K[Y, Z][U]$ și $\Phi \in K[Y, Z][X, T]$; punem $F_1 - F'_1 = DG_1$, $F_2 - F'_2 = DG_2$ și $\Phi = D\Psi$ și obținem $G_1(X) + TG_2(T) = (XT - YZ)\Psi$. Făcând $T = 0$, obținem $G_1(X) = YZ\Psi(X, Y, Z, 0)$, de unde $YZ|G_1(X)$. Făcând $X = 0$, obținem $G_1(0) + TG_2(T) = YZ\Psi(0, Y, Z, T)$. Cum din relația anterioară avem $YZ|G_1(0)$, obținem și $YZ|G_2(T)$. Urmează că $YZ|\Phi$, contradicție. Rămâne deci că $F_1 = F'_1$, ceea ce duce imediat și la $F_2 = F'_2$.

Să observăm acum că $\text{grad}_X(\overline{F_1(X)} + \overline{TF_2(T)})(\overline{F'_1(X)} + \overline{TF'_2(T)}) =$
 $= \text{grad}_X(\overline{F_1(X)F'_1(X)} + \overline{TF_1(X)F'_2(T)} + \overline{TF'_1(X)F_2(T)} + \overline{T^2F_2(T)F'_2(T)})$
 $= \text{grad}_X \overline{F_1(X)} + \text{grad}_X \overline{F'_1(X)}$
 $= \text{grad}_X(\overline{F_1(X)} + \overline{TF_2(T)}) + \text{grad}_X(\overline{F'_1(X)} + \overline{TF'_2(T)})$
 Analog se arată că $\text{grad}_T(\overline{F_1(X)} + \overline{TF_2(T)})(\overline{F'_1(X)} + \overline{TF'_2(T)}) =$
 $= \text{grad}_T(\overline{F_1(X)} + \overline{TF_2(T)}) + \text{grad}_T(\overline{F'_1(X)} + \overline{TF'_2(T)})$.

Considerăm acum o descompunere $\overline{X} = fg$, cu $f = \overline{F_1(X)} + \overline{TF_2(T)}$ și $g = \overline{F'_1(X)} + \overline{TF'_2(T)}$, a lui \overline{X} în R . Conform proprietății demonstrate mai sus vom avea $\text{grad}_X f = 1$ și $\text{grad}_X g = 0$ (sau viceversa) și $\text{grad}_T f = \text{grad}_T g = 0$. Prin urmare, $f = a\overline{X} + b$ cu $a, b \in K[Y, Z]$ și $g \in K[Y, Z]$. Din relația $\overline{X} = fg$ rezultă acum $ag = 1$, deci g este inversabil în R . Aceste considerații 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 $\overline{X}|_R \overline{Y}$, aceasta ar însemna că $\overline{X}(F(X) + \overline{TG(T)}) = \overline{Y}$, 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 $YZ - XT|_{K[X, Y, Z, T]} Y(\alpha Z - 1)$, contradicție. 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 consecință, 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 relațiile $-2i \cdot 2i = 2 \cdot 2$, 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 situații R nu este euclidian, deci putem considera $d \geq 10$.

Cum R este inel euclidian, există $\varphi : R \setminus \{0\} \rightarrow \mathbb{N}$ astfel încât oricare ar fi $a, b \in R$, $b \neq 0$, există $q, r \in R$ cu proprietățile $a = bq + r$ și $r = 0$ sau $\varphi(r) < \varphi(b)$. Considerăm și norma $N : R \rightarrow \mathbb{N}$, $N(x + yi\sqrt{d}) = x^2 + dy^2$. 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 $\varphi(\alpha) = \min\{\varphi(a) \mid a \in R \setminus \{-1, 0, 1\}\}$. (Remarcăm că acest minim este atins, întrucât \mathbb{N} este bine ordonat.) Dacă z este un element arbitrar din R , atunci, conform proprietăților lui φ , există $q, r \in R$ cu proprietățile $z = q\alpha + r$ și $r = 0$ sau $\varphi(r) < \varphi(\alpha)$. Conform definiției lui α , ultima inegalitate nu este posibilă decât dacă $r \in \{-1, 0, 1\}$.

În consecință, 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 $\alpha \mid 3$ sau $\alpha \mid 2$ sau $\alpha \mid 1$. Ultimul caz este însă imposibil deoarece $\alpha \notin U(R)$. Trecând la norme în celelalte două relații obținem (vezi problema 3(i)) că $N(\alpha) \mid 9$ sau $N(\alpha) \mid 4$. 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 $b = 0$, obținem $a^2 \in \{2, 3\}$, iar dacă $|b| \geq 1$ găsim $a^2 < 0$, contradicție.

Dacă $N(\alpha) = 4$, vom avea $a^2 + db^2 = 4$; dacă $b = 0$ obținem $\alpha = \pm 2 \sim 2$. Constatăm însă că dacă $i\sqrt{d}$ ar da rest $-1, 0$ sau 1 modulo 2 , atunci ar avea loc în R o relație de forma $i\sqrt{d} = 2(u + vi\sqrt{d}) + \varepsilon$ cu $\varepsilon \in \{-1, 0, 1\}$, de unde $1 = 2v$, contradicție. Dacă $|b| \geq 1$, obținem $a^2 = 4 - db^2 < 0$, contradicție.

Dacă $N(\alpha) = 9$, vom avea $a^2 + db^2 = 9$; pentru $b = 0$ obținem $\alpha = \pm 3 \sim 3$. Constatăm însă că dacă $i\sqrt{d}$ ar da rest $-1, 0$ sau 1 modulo 3 , atunci ar avea loc în R o relație de tipul $i\sqrt{d} = 3(u + vi\sqrt{d}) + \varepsilon$ cu $\varepsilon \in \{-1, 0, 1\}$, de unde $1 = 3v$, contradicție. Dacă $|b| \geq 1$, obținem $a^2 = 9 - db^2 < 0$, contradicție.

Rămâne așadar că inelul R nu este euclidian.

" \Leftarrow " Fie $d \in \{1, 2\}$. Definim $N : \mathbb{Q}[i\sqrt{d}] \rightarrow \mathbb{Q}$, $N(a + bi\sqrt{d}) = a^2 + db^2$. Conform problemei 2(ii),(iii), N este multiplicativă și $N(\mathbb{Z}[i\sqrt{d}]) \subset \mathbb{N}$. Fie $x = a + bi\sqrt{d}$ și $y = c + ei\sqrt{d} \neq 0$ elemente din R . Avem în \mathbb{C}

$$\frac{x}{y} = \frac{ac + dbe}{c^2 + de^2} + \frac{bc - ae}{c^2 + de^2}i\sqrt{d} \in \mathbb{Q}[i\sqrt{d}]. \text{ Notăm } \alpha = \frac{ac + dbe}{c^2 + de^2} \text{ și } \beta = \frac{bc - ae}{c^2 + de^2},$$

iar cu A și B întregii cei mai apropiați de α , respectiv de β . Prin urmare, $|A - \alpha| \leq \frac{1}{2}$ și $|B - \beta| \leq \frac{1}{2}$. Cu aceste notații se obține

$$\frac{x}{y} = A + Bi\sqrt{d} + (\alpha - A) + (\beta - B)i\sqrt{d},$$

deci $x = (A + Bi\sqrt{d})y + [(\alpha - A) + (\beta - B)i\sqrt{d}]y$. Cum x, y și $q = A + Bi\sqrt{d}$ sunt în R , din relația anterioară rezultă că $r = [(\alpha - A) + (\beta - B)i\sqrt{d}]y \in R$. Avem deci în R scrierea $x = qy + r$. În plus, datorită multiplicativității 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 $0 \leq (\alpha - A)^2 \leq \frac{1}{4}$ și $0 \leq (\beta - B)^2 \leq \frac{1}{4}$. 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 și care are doar un număr finit de elemente inversabile. Presupunem că R are doar un număr finit de elemente prime neasociate și considerăm un sistem p_1, \dots, p_n de reprezentanți ai acestora (în raport cu relația de asociere în divizibilitate). Avem $n > 0$ deoarece R conține elemente nenule și neinvertabile. 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 mulțimii $\mathcal{X} = \{x_n | n \in \mathbb{N}^*\}$ sunt distincte două câte două, ceea ce arată că \mathcal{X} e infinită, deci \mathcal{X} conține cel puțin un element neinvertabil, fie el x_m . Presupunerea că elementul prim $p \in R$ ar divide x_m ne-ar conduce la contradicția $p|1$. Rezultă că x_m nu are divizori primi, contradicție. Rămâne așadar că R are o infinitate de elemente prime neasociate.

(ii) Considerăm un domeniu de integritate R și 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 și fie p_1, \dots, p_n un sistem de reprezentanți ai acestora (în raport cu relația 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 puțin 1 deoarece unul din factorii p_1, \dots, 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, coeficienții lui f diferiți de $f(0)$ trebuie să fie nilpotenți; cum R este domeniu, înseamnă că acești coeficienți sunt nuli. Prin urmare, f este constant, contradicție.

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 $\widehat{f} = \sum a_{ij}x^i y^j \in R$. Punând $P(T) = \sum a_{i,2j}T^i(1-T^2)^j$ și $Q(T) = \sum a_{i,2j+1}T^i(1-T^2)^j$, 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 $P_1 = P_2$ și $Q_1 = Q_2$. Prin urmare, elementele lui R se scriu în mod unic sub forma $P + yQ$, cu $P, Q \in K[x]$.

Definim $\mathcal{N} : R \rightarrow K[X]$, $\mathcal{N}(P + yQ) = P^2(X) + (X^2 - 1)Q^2(X)$. 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 $P + yQ \in U(R)$ și $P' + yQ'$ 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 $P + yQ \in U(R)$. Așadar $P + yQ \in R$ e inversabil dacă și numai dacă $\mathcal{N}(P + yQ)$ este un element din $K \setminus \{0\}$.

Ipoteza că $x = \widehat{X}$ este element reductibil înseamnă că există $a = P_1 + yQ_1$ și $b = P_2 + yQ_2$ în $R \setminus U(R)$ astfel încât $x = ab$. Rezultă că $X^2 = \mathcal{N}(x) = \mathcal{N}(a)\mathcal{N}(b)$. Cum $a, b \notin U(R)$, $\mathcal{N}(a)$ și $\mathcal{N}(b)$ trebuie să aibă gradul cel puțin 1. Din condiția ca produsul lor să fie X^2 deducem că există $\alpha \in R \setminus \{0\}$ astfel încât $\mathcal{N}(a) = \alpha X$ și $\mathcal{N}(b) = \alpha^{-1}X$. Aceste condiții 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) "⇒" 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 acești 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 $X = 0$, obținem că $Y^2 - 1|_{K[Y]}Y \pm 1$, contradicție. Rămâne că x nu e prim în R , ceea ce, amintindu-ne că x este ireductibil, înseamnă că R nu este inel factorial, contradicție.

” \Leftarrow ” Să notăm cu i o rădăcină din K a lui $Z^2 + 1 \in K[Z]$. Conform proprietății de universalitate a inelelor de polinoame, există morfisme de K -algebre $\Phi, \Psi : K[X, Y] \rightarrow K[X, Y]$ astfel încât $\Phi(X) = X + iY, \Phi(Y) = X - iY, \Psi(X) = 2^{-1}(X + Y)$ și $\Psi(Y) = (2i)^{-1}(X - Y)$. Se constată imediat că $\Phi = \Psi^{-1}$, deci Φ și Ψ sunt izomorfisme. Avem relația $\Psi((X^2 + Y^2 - 1)) = \Psi(((X + iY)(X - iY) - 1)) = (XY - 1)$. Rezultă că $R \simeq K[X, Y]/(XY - 1)$, care, conform problemei 22, este inel euclidian, deci R este inel euclidian. În consecință, 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 $R = \mathbb{R}[X, Y]/(X^2 + Y^2 + 1)$, $x = \hat{X}$ și $y = \hat{Y}$.

Cum polinomul $X^2 + Y^2 + 1$ este ireductibil în $\mathbb{R}[X, Y] \simeq \mathbb{R}[Y][X]$ (aplicăm criteriul lui Eisenstein cu $p = Y^2 + 1$) și $\mathbb{R}[X, Y]$ 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 și η imaginile lui x , respectiv y , prin proiecția canonică $R \rightarrow R/\mathfrak{p}$. Cum $f(x, y) \in \mathfrak{p}$, rezultă $f(\xi, \eta) = 0$. Pe de altă parte, relația $x^2 + y^2 + 1 = 0$ implică $\xi^2 + \eta^2 + 1 = 0$.

Sistemul de condiții $\xi^2 + \eta^2 + 1 = 0$ și $f(\xi, \eta) = 0$ este echivalent cu un sistem de forma $\xi^2 + \eta^2 + 1 = 0$ și $P(\xi) + Q(\xi)\eta = 0$, $P, Q \in \mathbb{R}[T]$. Într-adevăr, afirmația este evidentă în situația în care $n = \text{grad}_Y f \in \{0, 1\}$. Dacă $n \geq 2$, să presupunem afirmația adevărată pentru polinoamele de grad mai mic decât n . Punând $f(X, Y) = a_0(X) + a_1(X)Y + \dots + a_n(X)Y^n$, sistemul dat este echivalent cu $\xi^2 + \eta^2 + 1 = 0$ și $g(\xi, \eta) = 0$, unde $g(X, Y) = a_0(X) + a_1(X)Y + \dots + a_{n-1}(X)Y^{n-1} - a_n(X)Y^{n-2}(X^2 + 1) = f(X, Y) - a_n(X)Y^{n-2}(X^2 + Y^2 + 1)$. Gradul în Y al lui g fiind cel mult $n - 1$, putem aplica ipoteza de inducție și afirmația este demonstrată. Remarcăm în plus că în pasul de inducție prezentat mai sus avem $f \equiv g \pmod{X^2 + Y^2 + 1}$. Prin urmare, ecuația $P(\xi) + Q(\xi)\eta = 0$ se realizează pentru P și Q nu simultan nule. Evident, ξ și η vor satisface și relația $(P(\xi) + Q(\xi)\eta)(P(\xi) - Q(\xi)\eta) = 0$, 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 $P = Q = 0$, contradicție). Aceeași proprietate o va avea deci și 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 și are rădăcina ξ .

Prin urmare, există polinoame nenule cu coeficienți 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 $\text{grad } P = 1$, 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 $\mathbb{R} \rightarrow R/\mathfrak{p}$, $a \mapsto \hat{a} + \mathfrak{p}$, n-ar fi injectiv atunci ar exista $a \in \mathbb{R}^*$ cu $\hat{a} \in \mathfrak{p}$. Cum $\hat{a} + \mathfrak{p}$ e inversabil în R , ar rezulta $\mathfrak{p} = R$, contradicție.)

Prin urmare, $\xi \in \mathbb{R}$ sau ξ este rădăcină a unui polinom (monic) de grad 2 cu coeficienți reali.

În mod analog se demonstrează că $\eta \in \mathbb{R}$ sau η este rădăcină a unui polinom (monic) de grad 2 cu coeficienți reali.

Să mai observăm că ξ și 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 fracții al lui R). Scriem $T^2 + AT + B = (\sigma T + \tau)(T - \xi)$, dezvoltăm și identificăm coeficienții. Obținem $\sigma = 1$ și $\tau - \xi = A$, de unde $\tau = A + \xi \in R/\mathfrak{p}$. Prin urmare, $\sigma T + \tau = T + (A + \xi) \in (R/\mathfrak{p})[T]$ și a doua rădăcină a lui $T^2 + AT + B$ este $-(A + \xi) \in R/\mathfrak{p}$; notăm $\bar{\xi} = -(A + \xi)$. În mod similar a doua rădăcină a lui $T^2 + CT + D$ este tot în R/\mathfrak{p} și o notăm cu $\bar{\eta}$.

Să constatăm acum că $A^2 - 4B < 0$ (altfel $T^2 + AT + B$ ar fi reductibil peste \mathbb{R}) și să punem $i = \frac{1}{\sqrt{4B-A^2}}(\xi - \bar{\xi})$. Observăm că $i^2 = \frac{1}{4B-A^2}(\xi - \bar{\xi})^2 = \frac{1}{4B-A^2}[(\xi + \bar{\xi})^2 - 4\xi\bar{\xi}] = \frac{1}{4B-A^2}(A^2 - 4B) = -1$ și din această relație deducem că $i \in U(R/\mathfrak{p})$, deci și $\xi - \bar{\xi} \in U(R/\mathfrak{p})$.

Dacă notăm $\alpha = \frac{1}{2}(\xi - \bar{\xi})$, $\beta = \frac{1}{2}i^{-1}(\xi - \bar{\xi})$, $\gamma = \frac{1}{2}(\eta + \bar{\eta})$, $\delta = \frac{1}{2}i^{-1}(\eta - \bar{\eta})$, atunci $\alpha = -\frac{1}{2}A \in \mathbb{R} \subset R/\mathfrak{p}$ și $\beta = \frac{1}{2}i^{-1}(\xi - \bar{\xi}) = \frac{1}{2}\left(\frac{1}{\sqrt{4B-A^2}}(\xi - \bar{\xi})\right) = \frac{\sqrt{4B-A^2}}{2} \in \mathbb{R} \subset R/\mathfrak{p}$. Analog $C, D \in R/\mathfrak{p}$.

Avem $\alpha + i\beta = \frac{1}{2}(\xi - \bar{\xi}) + i\frac{1}{2}i^{-1}(\xi - \bar{\xi}) = \xi$ și analog $\eta = \gamma + i\delta$.

Punând acum $a = \delta$, $b = -\beta$ și $c = \beta\gamma - \alpha\delta$, obținem $a\xi + b\eta + c = 0$, cu $a, b, c \in \mathbb{R}$ și a și b nu simultan nuli. Relația $a\xi + b\eta + c = 0$ 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 analoag.

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 și 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 și 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 $a' = -\frac{a}{b}$ și $b' = -\frac{c}{b}$ și ținând 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 considerațiilor anterioare, orice ideal prim nenul al lui R intersectează pe S . Cum idealele prime ale lui $S^{-1}R$ sunt în corespondență 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 șir ascendent de ideale principale ale lui R este staționar. 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 $\text{grad}_Y f \in \{0, 1\}$, afirmația este evidentă. Dacă $\text{grad}_Y f = n \geq 2$, să presupunem afirmația adevărată pentru toate elementele $g(x, y) \in R$ cu $\text{grad}_Y g < n$. Dacă scriem $f = a_n(X)Y^n + \dots + a_0(X)$, atunci, notând $g = a_0(X) + a_1(X)Y + \dots + a_{n-1}(X)Y^{n-1} - a_n(X)Y^{n-2}(X^2 + 1) \in \mathbb{R}[X, Y]$, avem în mod clar $\text{grad}_Y g \leq n - 1 < n$. Conform ipotezei de inducție, 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 $f(x, y) = a_0(x) + \cdots + a_n(x)y^n = a_0(x) + a_1(x)y + \cdots + a_{n-1}(x)y^{n-1} - a_n(x)y^{n-2}(x^2 + 1) = g(x, y) = P(x) + Q(x)y$ și existența scrierii este demonstrată. În ceea ce privește unicitatea, să remarcăm că pentru $P_1, P_2, Q_1, Q_2 \in \mathbb{R}[X]$, relația $P_1(x) + Q_1(x)y = P_2(x) + Q_2(x)y$ înseamnă $Y^2 + X^2 + 1 \mid (P_1 - P_2) + Y(Q_1 - Q_2)$, de unde deducem $P_1 = P_2$ și $Q_1 = Q_2$. Definim acum $N : R \rightarrow \mathbb{R}[X]$, $N(P(x) + Q(x)y) = P^2 + (X^2 + 1)Q^2$. Remarcăm că pentru elementele arbitrare $w_1 = P_1(x) + Q_1(x)y$ și $w_2 = P_2(x) + Q_2(x)y$ ale lui R avem $N(w_1 w_2) = N(P_1(x)P_2(x) - (x^2 + 1)Q_1(x)Q_2(x) + y(P_1(x)Q_2(x) + P_2(x)Q_1(x))) = P_1^2 P_2^2 + (X^2 + 1)^2 Q_1^2 Q_2^2 + (X^2 + 1)P_1 Q_2 + (X^2 + 1)P_2 Q_1 = (P_1^2 + (X^2 + 1)Q_1^2)(P_2^2 + (X^2 + 1)Q_2^2) = N(w_1)N(w_2)$. Fie acum $w \in U(R)$. Atunci există $w' \in R$ cu $ww' = 1$. Aplicând N acestei relații, obținem $N(w)N(w') = 1$, 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 , obținem $1 = \frac{1}{\alpha}(P^2(x) + (x^2 + 1)Q^2(x)) = P^2(x) - y^2 Q^2(x) = w \frac{1}{\alpha}(P(x) - yQ(x))$, prin urmare $w \in U(R)$. În concluzie, un element $w \in R$ este inversabil dacă și numai dacă $N(w) \in \mathbb{R}^*$.

Dacă $w_1 \mid_R w_2$, atunci există $\lambda \in R$ astfel ca $w_2 = \lambda w_1$. Utilizând multiplicativitatea lui N , obținem $N(w_2) = N(\lambda)N(w_1)$, de unde $N(w_1) \mid_{\mathbb{R}[X]} N(w_2)$. 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 $w_1 \mid_R w_2$, $w_2 = \lambda w_1$, și 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 $w_2 R \subset w_1 R$, atunci $N(w_2)\mathbb{R}[X] \subset N(w_1)\mathbb{R}[X]$, iar aceste incluziuni sunt fie ambele stricte, fie ambele egalități.

Fie acum $w_1 R \subset w_2 R \subset \cdots$ un lanț ascendent de ideale principale ale lui R . Conform celor de mai sus, el induce lanțul 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 lanț este însă staționar deoarece $\mathbb{R}[X]$ este inel principal. Prin urmare, lanțul $w_1 R \subset w_2 R \subset \cdots$ este de asemenea staționar.

Inelul R verifică așadar condițiile 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 $\pi\bar{\pi} = p_1 \cdots p_n$, deci π divide măcar unul din acești 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, obținem $p_1^2 = N(\pi)N(x)$, de unde $p_1^2 = p_1 \cdots p_n N(x)$. Această relație nu este posibilă decât într-unul din următoarele două cazuri:

$n = 2$, $p_2 = p_1$ și $N(x) = 1$. Atunci (vezi problema 2(iv)) x este inversabil în R . În consecință, $\pi \sim p_1$.

$n = 1$ și $N(x) = p_1$. Atunci $\pi\bar{\pi} = N(\pi) = p_1$.

(ii) Demonstrația 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 $p|\mathbb{Z}a$ și $p|\mathbb{Z}b$, deci $p|\mathbb{Z}(a, b) = 1$, contradicție.

" \Leftarrow " Conform problemei 16 din Capitolul 5, inelul $R/(x)$ are $|a^2 - b^2d| = N(x)$ elemente. Folosind problema 2 din Capitolul 4 (pe o mulțime 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 și 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} și să decidem care rămân prime în R și care sunt norme de prime din R . Să remarcăm pentru început că $2 = (1+i)(1-i)$ și $N(1+i) = N(1-i) = 2$, deci $2 \in R$ nu este prim. Pe de altă parte, $1+i$ și $1-i$ sunt ireductibile (vezi problema 2(v)), deci, cum R este euclidian, ele sunt prime. Observăm și 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 relații nu poate fi congruent cu 3 modulo 4, rezultă că primele de forma $4k+3$ din \mathbb{N} rămân prime și în R .

Fie acum un prim $p \in \mathbb{N}$ de forma $4k + 1$. Considerăm relațiile:

$$\begin{aligned} p-1 &\equiv -1 \pmod{p} \\ p-2 &\equiv -2 \pmod{p} \\ &\dots\dots\dots \\ \frac{p+1}{2} &\equiv -\frac{p-1}{2} \pmod{p}, \end{aligned}$$

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 $(a+bi)(c+di)$, obținem $N(a+bi) = N(c+di) = p$, deci $(a+bi)(a-bi) = p$; în plus, conform problemei 2(v), $a \pm bi$ sunt prime în R și demonstrația este completă.

37. Notăm $R = \mathbb{Z}[i\sqrt{2}]$, care este inel euclidian. Prin urmare, un element din R este prim dacă și 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} și să decidem care rămân prime în R și care sunt norme de prime din R . Să remarcăm pentru început că $2 = (-i\sqrt{2}) \cdot i\sqrt{2}$ și $N(i\sqrt{2}) = 2$, 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 relații nu poate fi congruent cu 5 sau 7 modulo 8, rezultă că primele de forma $8k + 5$ și cele de forma $8k + 7$ din \mathbb{N} rămân prime și în R .

În cele ce urmează vom avea nevoie de următorul rezultat:

Lemă Fie $p \in \mathbb{N}$ un număr prim impar și $a \in \mathbb{Z}$ cu $(a, p) = 1$. Următoarele afirmații sunt echivalente:

1. Există $x \in \mathbb{Z}$ astfel încât $x^2 \equiv a \pmod{p}$.
2. $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Demonstrație 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 $p-1$. Așadar pătratele din $\mathbb{Z}_p \setminus \{0\}$

sunt rădăcini pentru G . Pe de altă parte, pentru $i, j \in \{\widehat{1}, \widehat{2}, \dots, \widehat{\frac{p-1}{2}}\}$ avem $i^2 = j^2 \Leftrightarrow p|(i-j)(i+j)$. Este clar că $p \nmid i+j$ și $p|i-j$ doar dacă $i=j$; prin urmare $i^2 = j^2 \Leftrightarrow i=j$. Așadar 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 și numai dacă este rădăcină a lui G , deci dacă și 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 $k = \left\lfloor \frac{p-1}{4} \right\rfloor$, $a_j = 2j$ pentru fiecare $j = \overline{1, k}$ și $b_j = 2j$ pentru fiecare $j = \overline{k+1, \frac{p-1}{2}}$. Să observăm că $0 \leq a_1, a_2, \dots, a_k \leq \frac{p-1}{2}$, $\frac{p-1}{2} < b_{k+1}, \dots, b_{\frac{p-1}{2}} \leq p-1$ și elementele $a_1, a_2, \dots, a_k, p-b_{k+1}, \dots, p-b_{\frac{p-1}{2}}$ 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, $\{a_1, a_2, \dots, a_k, p-b_{k+1}, \dots, p-b_{\frac{p-1}{2}}\} = \{1, 2, \dots, \frac{p-1}{2}\}$. Considerăm relațiile:

$$\begin{aligned} 2 \cdot 1 &\equiv a_1 \pmod{p}, \\ 2 \cdot 2 &\equiv a_2 \pmod{p}, \\ &\dots\dots\dots \\ 2 \cdot k &\equiv a_k \pmod{p}, \\ 2 \cdot (k+1) &\equiv b_{k+1} \pmod{p}, \\ &\dots\dots\dots \\ 2 \cdot \frac{p-1}{2} &\equiv b_{\frac{p-1}{2}} \pmod{p}. \end{aligned}$$

Înmulțindu-le membru cu membru obținem $2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{p-1}{2}-k} \left(\frac{p-1}{2}\right)! \pmod{p}$ de unde deducem că $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}-\left\lfloor \frac{p-1}{4} \right\rfloor} \pmod{p}$, deci $(-2)^{\frac{p-1}{2}} \equiv (-1)^{p-1-\left\lfloor \frac{p-1}{4} \right\rfloor} \pmod{p}$. Dar pentru p de forma $8k+1$ sau $8k+3$ numărul $p-1-\left\lfloor \frac{p-1}{4} \right\rfloor$ 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 , obținem $N(a+bi\sqrt{2}) = N(c+di\sqrt{2}) = p$, 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) și demonstrația e completă.

38. Notăm $R = \mathbb{Z}[\sqrt{2}]$, care este inel euclidian. Prin urmare, un element din R este prim dacă și 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} și să decidem care rămân prime în R și care sunt norme de prime din R . Să remarcăm pentru început că $2 = \sqrt{2}^2$ și $N(\sqrt{2}) = 2$, 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 relații nu poate fi congruent cu 3 sau 5 modulo 8, rezultă că primele de forma $8k + 3$ și cele de forma $8k + 5$ din \mathbb{N} rămân prime și în R . Fie acum un prim $p \in \mathbb{N}$ de forma $8k + 1$ sau $8k + 7$. Notăm $k = \left\lfloor \frac{p-1}{4} \right\rfloor$, $a_j = 2j$ pentru fiecare $j = \overline{1, k}$ și $b_j = 2j$ pentru fiecare $j = \overline{k+1, \frac{p-1}{2}}$. Să observăm că $0 \leq a_1, a_2, \dots, a_k \leq \frac{p-1}{2}$, $\frac{p-1}{2} < b_{k+1}, \dots, b_{\frac{p-1}{2}} \leq p-1$ și elementele $a_1, a_2, \dots, a_k, p - b_{k+1}, \dots, p - b_{\frac{p-1}{2}}$ 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, $\{a_1, a_2, \dots, a_k, p - b_{k+1}, \dots, p - b_{\frac{p-1}{2}}\} = \{1, 2, \dots, \frac{p-1}{2}\}$. Considerăm relațiile:

$$\begin{aligned} 2 \cdot 1 &\equiv a_1 \pmod{p}, \\ 2 \cdot 2 &\equiv a_2 \pmod{p}, \\ &\dots\dots\dots \\ 2 \cdot k &\equiv a_k \pmod{p}, \\ 2 \cdot (k+1) &\equiv b_{k+1} \pmod{p}, \\ &\dots\dots\dots \\ 2 \cdot \frac{p-1}{2} &\equiv b_{\frac{p-1}{2}} \pmod{p}. \end{aligned}$$

Înmulțindu-le membru cu membru, obținem $2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{p-1}{2}-k} \left(\frac{p-1}{2}\right)! \pmod{p}$ de unde deducem că $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}-\left\lfloor \frac{p-1}{4} \right\rfloor} \pmod{p}$. Dar pentru p de forma $8k + 1$ sau $8k + 7$ numărul $\frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor$ este par, deci, conform lemei din soluția 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 , obținem $N(a + b\sqrt{2}) = N(c + d\sqrt{2}) = p$, 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) și demonstrația este completă.

39. Notăm $R = \mathbb{Z}[\sqrt{3}]$, care este inel euclidian. Prin urmare, un element din R este prim dacă și 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} și să decidem care rămân prime în R și 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 și 3 nu sunt prime în R , iar $\sqrt{3} \pm 1$ și $\sqrt{3}$ 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 relații nu poate fi congruent cu 5 sau 7 modulo 12, rezultă că primele din \mathbb{N} de forma $12k + 5$ și cele de forma $12k + 7$ rămân prime și în R . Fie acum un prim $p \in \mathbb{N}$ de forma $12k + 1$ sau $12k + 11$. Notăm $k = \left\lfloor \frac{p-1}{6} \right\rfloor$ și $l = \left\lfloor \frac{p-1}{3} \right\rfloor$. Considerăm relațiile:

$$\begin{aligned}
3 \cdot 1 &\equiv 3 \stackrel{\text{not}}{=} a_1 \pmod{p}, \\
3 \cdot 2 &\equiv 6 \stackrel{\text{not}}{=} a_2 \pmod{p}, \\
&\dots\dots\dots \\
3 \cdot k &\equiv 3k \stackrel{\text{not}}{=} a_k \pmod{p}, \\
3 \cdot (k+1) &\equiv 3(k+1) \stackrel{\text{not}}{=} b_{k+1} \pmod{p}, \\
&\dots\dots\dots \\
3 \cdot l &\equiv 3l \stackrel{\text{not}}{=} b_l \pmod{p}, \\
3 \cdot (l+1) &\equiv 3(l+1) \stackrel{\text{not}}{=} c_{l+1} \pmod{p}, \\
&\dots\dots\dots \\
3 \cdot \frac{p-1}{2} &\equiv \frac{3(p-1)}{2} \stackrel{\text{not}}{=} c_{\frac{p-1}{2}} \pmod{p}.
\end{aligned}$$

Să observăm că $0 \leq a_1, a_2, \dots, a_k \leq \frac{p-1}{2}$, $\frac{p-1}{2} < b_{k+1}, \dots, b_l \leq p-1$, $p+1 \leq c_{l+1}, c_{l+2}, \dots, c_{\frac{p-1}{2}} \leq \frac{3(p-1)}{2}$ și elementele $a_1, a_2, \dots, a_k, p-b_{k+1}, \dots, p-b_l, c_{l+1}-p, \dots, c_{\frac{p-1}{2}}-p$ sunt distincte două câte două (procedând ca în soluția problemei 37). Prin urmare, $\{a_1, a_2, \dots, a_k, p-b_{k+1}, \dots, p-b_l, c_{l+1}-p, \dots, c_{\frac{p-1}{2}}-p\} = \{1, 2, \dots, \frac{p-1}{2}\}$. Înmulțind membru cu membru relațiile anterioare, obținem $3^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{l-k} \left(\frac{p-1}{2}\right)! \pmod{p}$ de unde deducem că $3^{\frac{p-1}{2}} \equiv (-1)^{\left\lfloor \frac{p-1}{3} \right\rfloor - \left\lfloor \frac{p-1}{6} \right\rfloor} \pmod{p}$. Dar pentru p de forma $12k + 1$ sau $12k + 11$ numărul $\left\lfloor \frac{p-1}{3} \right\rfloor - \left\lfloor \frac{p-1}{6} \right\rfloor$ este par, deci, conform lemei din soluția problemei 37, există $a \in \mathbb{Z}$ cu proprietatea $a^2 \equiv 3 \pmod{p}$. Avem deci $p|a^2 - 3$, prin

urmare $p \mid_R (a - \sqrt{3})(a + \sqrt{3})$. 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 $(a + b\sqrt{3})(c + d\sqrt{3})$, obținem $N(a + b\sqrt{3}) = N(c + d\sqrt{3}) = p$, 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 și demonstrația 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 și, dacă da, în ce mod.

Dacă $p = 3$, atunci $p = (1 - \rho)(1 - \bar{\rho}) = (1 - \rho)(2 + \rho)$; cum $N(1 - \rho) = N(2 + \rho) = 3$, elementele $1 - \rho$ și $2 + \rho$ sunt neinvertabile 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 și 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, $a^2 - ab + b^2 = (a - \frac{b}{2})^2 + \frac{3b^2}{4} = 3$. Dacă $b = 0$, obținem $a^2 = 3$, imposibil. Dacă $b = 1$ rezultă $(a - \frac{1}{2})^2 = \frac{9}{4}$, deci $a \in \{-1, 2\}$. Dacă $b = -1$ rezultă $(a + \frac{1}{2})^2 = \frac{9}{4}$, deci $a \in \{-2, 1\}$. Dacă $b = 2$ obținem $(a - 1)^2 = 0$, 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 $-1 + \rho$, $-1 - 2\rho$, $1 - \rho$, $1 + 2\rho$, $2 + \rho$ și $-2 - \rho$.

Cum $|\{(1 - \rho)a \mid a \in U(R)\}| \subset |\{x \in R \mid N(x) = 3\}|$ și aceste mulțimi 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 și oricare dintre acestea este asociat în divizibilitate cu $1 - \rho$.

Dacă numărul prim p este de forma $3k + 1$, $k \in \mathbb{N}^*$, utilizăm relația

$$3^{\frac{p-1}{2}} \equiv (-1)^{[\frac{p-1}{3}] - [\frac{p-1}{6}]} \pmod{p},$$

pe care am demonstrat-o în soluția problemei 39. Din această relație deducem

$$(-3)^{\frac{p-1}{2}} \equiv (-1)^{[\frac{p-1}{3}] - [\frac{p-1}{6}] + (\frac{p-1}{2})} \pmod{p}.$$

Numărul p fiind prim și de forma $3k + 1$, el nu poate da prin împărțire 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 soluția problemei 37, există $a \in \mathbb{Z}$ astfel ca $a^2 \equiv -3 \pmod{p}$. Atunci $p \mid_{\mathbb{Z}} a^2 + 3$, de unde $p \mid_R a^2 + 3 = (a - i\sqrt{3})(a + i\sqrt{3})$; este însă evident că p nu divide în R niciunul dintre acești factori. Prin urmare, p nu este prim în R , deci nu există elemente prime din R asociate cu el. Există în schimb, conform considerațiilor de mai sus, elemente $\pi \in R$ pentru care $N(\pi) = \pi\bar{\pi} = p$ și orice astfel de element este, conform problemei 2(v), ireductibil. Prin urmare, orice astfel de element este și prim, căci știm 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 $x, y \in R \setminus U(R)$. Obținem $p^2 = N(p) = N(x)N(y)$, de unde $N(x) = N(y) = p$. Punând $x = a + b\rho$, $a, b \in \mathbb{Z}$, obținem $(2a - b)^2 + 3b^2 = 4p$, deci $(2a - b)^2 \equiv p \pmod{3}$, de unde $(2a - b)^2 \equiv 2 \pmod{3}$, contradicție. Rămâne așadar că p este ireductibil în R . Cum R este inel euclidian, obținem că p este element prim în R .

41. Să observăm pentru început că dacă (x, y, z) este o soluție pentru ecuația din enunț cu $d = (x, y, z) \neq 1$, atunci $\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$ este și ea soluție. E suficient prin urmare să găsim soluțiile (x, y, z) cu $(x, y, z) = 1$ pentru ecuația considerată, celelalte obținându-se apoi prin multiplicarea acestora cu constante. Apoi, singurele soluții cu componentă nulă sunt cele din $\{(0, k, \pm k) \mid k \in \mathbb{Z}\}$ și $\{(k, 0, \pm k) \mid k \in \mathbb{Z}\}$. În al treilea rând, să constatăm că, dată fiind soluția (x, y, z) , $(|x|, |y|, |z|)$ este la rândul-i soluție, deci soluțiile cu componente întregi se obțin din cele cu componente naturale luând toate combinațiile posibile de semne.

Rămâne prin urmare să rezolvăm ecuația dată în numere naturale nenule cu cel mai mare divizor comun 1. Privim ecuația 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 $x + iy$ și $x - iy$, atunci el divide și suma și diferența acestora, deci $\pi \mid_R (2x, 2iy)$. Dar $(x, y) = 1$, căci dacă ar exista un număr prim p care să dividă și pe x și pe y , atunci din ecuație ar rezulta că p îl divide și

pe z , contradicție 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 și y nu pot fi simultan pare, căci ar rezulta și z par, deci $2|(x, y, z)$, contradicție, și nici simultan impare, căci s-ar obține contradicția $z^2 = x^2 + y^2 \equiv 2 \pmod{4}$. Faptul că $1 + i|x + iy$ este așadar contradictoriu. Prin urmare, $x + iy$ și $x - iy$ nu au divizori primi comuni, deci sunt prime între ele în R .

Relația $(x + iy)(x - iy) = z^2$ împreună cu faptul că $x + iy$ și $x - iy$ nu au divizori primi comuni conduce la concluzia că $x + iy$ și $x - iy$ sunt asociate cu pătrate din R . avem de considerat cazurile:

1. Există $a, b \in \mathbb{Z}$ astfel ca $x + iy = (a + bi)^2$. Obținem $x = a^2 - b^2$, $y = 2ab$ iar din ecuație deducem $z = a^2 + b^2$. Să observăm că această soluție convine doar dacă $a^2 - b^2 > 0$, a și b sunt de același semn (căci $y = 2ab \in \mathbb{N}$), situație în care ele pot fi luate numere naturale cu $a > b$, iar a și b sunt prime între ele, căci altfel $(x, y, z) \neq 1$.

2. Există $a, b \in \mathbb{Z}$ astfel ca $x + iy = -(a + bi)^2$. Obținem $x = |b|^2 - |a|^2$, $y = 2|a||b|$ iar din ecuație deducem $z = |a|^2 + |b|^2$. Pentru $|b| \leq |a|$, acest caz nu dă soluții.

3. Există $a, b \in \mathbb{Z}$ astfel ca $x + iy = i(a + bi)^2$. Obținem $x = 2|a||b|$, $y = |a|^2 - |b|^2$, $y = 2ab$ iar din ecuație deducem $z = |a|^2 + |b|^2$. Pentru $|a| \leq |b|$, acest caz nu dă soluții.

4. Există $a, b \in \mathbb{Z}$ astfel ca $x + iy = -i(a + bi)^2$. Obținem $x = 2|a||b|$, $y = |b|^2 - |a|^2$, $y = 2ab$ iar din ecuație deducem $z = |a|^2 + |b|^2$. Pentru $|b| \leq |a|$, acest caz nu dă soluții.

Prin urmare, soluțiile netriviabile ale ecuației date, numită și *ecuația lui Pitagora*, sunt $(\pm d(a^2 - b^2), \pm 2dab, \pm d(a^2 + b^2))$ și $(\pm 2dab, \pm d(a^2 - b^2), \pm d(a^2 + b^2))$, unde $a > b$ sunt numere naturale prime între ele, $d \in \mathbb{N}^*$, iar alegerea semnelor \pm poate fi făcută în toate combinațiile posibile.

42. Să constatăm pentru început că singura soluție care are componente nule este $(0, 0, 0)$. În continuare, pentru orice soluție (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 soluție dacă și numai dacă $(\frac{x}{d^2}, \frac{y}{d}, \frac{z}{d})$ e soluție. Prin urmare, este suficient să găsim soluțiile cu componentele prime între ele. Fie $(x, y, z) \in (\mathbb{Z}^*)^3$ o astfel de soluție. Notăm $R = \mathbb{Z}[i\sqrt{2}]$ (care, conform problemei 17, este un inel euclidian) și căutăm pentru ecuația dată soluții din R^3 . Ecuația devine $(x + y^2i\sqrt{2})(x - y^2i\sqrt{2}) = 17z^4$. Fie δ un divizor prim (în R !) comun pentru $x + y^2\sqrt{2}$ și $x - y^2i\sqrt{2}$. Atunci $\delta|2x$ și $\delta|2y^2i\sqrt{2}$. Rezultă (vezi

problema 31) că $\delta = i\sqrt{2}$. Există deci un element $a + bi\sqrt{2} \in R$ astfel ca $x + y^2i\sqrt{2} = i\sqrt{2}(a + bi\sqrt{2})$, de unde $x = -2b$. Rezultă imediat din ecuația inițială că z e par, și apoi că y e par, contradicție. Rămâne deci că $x + y^2i\sqrt{2}$ și $x - y^2i\sqrt{2}$ sunt prime între ele în R . Acum, în R are loc relația $17 = (3 + 2i\sqrt{2})(3 - 2i\sqrt{2})$. Cum (vezi problema 31) $3 \pm 2i\sqrt{2}$ sunt prime în R , rezultă că $3 + 2i\sqrt{2}$ divide $x + y^2i\sqrt{2}$ sau $x - y^2i\sqrt{2}$. Să presupunem pentru a fixa ideile că $3 + 2i\sqrt{2} \mid_R x + y^2i\sqrt{2}$. Rezultă imediat că $3 - 2i\sqrt{2} \mid_R x - y^2i\sqrt{2}$; avem

$$\frac{x + y^2i\sqrt{2}}{3 + 2i\sqrt{2}} \cdot \frac{x - y^2i\sqrt{2}}{3 - 2i\sqrt{2}} = z^4;$$

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 $\pm(x + y^2i\sqrt{2}) = (3 + 2i\sqrt{2})(c + di\sqrt{2})^4$. Dezvoltând și identificând coeficienții, obținem

$$\pm x = 3c^4 - 36c^2d^2 + 12d^4 - 16c^3d + 32cd^3 \quad (12.1)$$

și

$$\pm y^2 = 2c^4 - 24c^2d^2 + 8d^4 + 12c^3d - 24cd^3.$$

Din ultima relație rezultă că y e par; punem $y = 2y_1$ și obținem

$$\pm 2y_1^2 = c^4 - 12c^2d^2 + 4d^4 + 6c^3d - 12cd^3,$$

de unde obținem c par; din relația (12.1) rezultă acum că x e par, contradicție cu faptul că x și y sunt prime între ele. Prin urmare, ecuația considerată admite numai soluția $(0, 0, 0)$.

43. Vom începe cu câțiva pași preliminari și apoi vom trece la rezolvarea problemei. Notăm $\rho = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $R = \mathbb{Z}[\rho]$ și $\lambda = 1 - \rho$ (conform problemei 40, λ este prim în R). Toate literele grecești din demonstrație vor desemna elemente din R ; $\alpha|\beta$ va avea semnificația " 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 știe că $a + b$ este de forma $3k + r$, cu $k \in \mathbb{Z}$ și $r \in \{-1, 0, 1\}$. 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 și ± 1 sunt resturi distincte modulo λ deoarece (vezi problema 1) λ nu divide în R elementele ± 1 și ± 2 .

2. Dacă $\omega \in R$ și $\lambda \nmid_R \omega$, 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 mulțimea $\{-\omega, \omega\}$ care este congruent cu 1 $\pmod{\lambda}$. Există așadar $\beta \in R$ astfel încât $\alpha = 1 + \beta\lambda$. Ținând cont și 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 $\beta - 1, \beta$ și $\beta + 1$ 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 $\lambda^4|3 \sim_R \lambda^2$, contradicție.

Trecem acum la rezolvarea problemei. Să remarcăm că tripletele de forma $(k, 0, k)$ și $(k, k, 0)$, $k \in \mathbb{Z}$, reprezintă soluții ale ecuației din enunț (ele sunt așa-numitele "soluții triviale" ale ecuației considerate).

Ne propunem în continuare să arătăm că nu mai există și alte soluții. Aceasta este o consecință a faptului că ecuația $\xi^3 + \eta^3 + \zeta^3 = 0$ nu are soluții netriviale (adică cu toate componentele nenule) în inelul R , afirmație pe care o vom demonstra în cele ce urmează. Fie (ξ, η, ζ) o soluție netrivială a acestei ecuații. Putem considera că ξ, η și ζ sunt prime două câte două în R (altfel, simplificăm relația 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 $n \in \mathbb{N}^*$ și $\gamma \in R$ astfel încât $\zeta = \lambda^n \gamma$, $\lambda \nmid \gamma$. În plus, $\lambda \nmid \xi$ și $\lambda \nmid \eta$. Ținând cont de aceste constatări, avem practic de demonstrat că relația $\xi^3 + \eta^3 + \lambda^{3n} \gamma^3 = 0$ este imposibilă în condițiile în care ξ, η, γ nu se divid prin λ , iar $(\xi, \eta) = 1$. Vom arăta ceva mai mult, și anume că relația $\xi^3 + \eta^3 + \varepsilon \lambda^{3n} \gamma^3 = 0$ este imposibilă în condițiile în care ξ, η, γ nu se divid prin λ , $\varepsilon \in U(R)$, iar $(\xi, \eta) = 1$. Presupunem că relația $\xi^3 + \eta^3 + \varepsilon \lambda^{3n} \gamma^3 = 0$, $\varepsilon \in U(R)$, este satisfăcută de ξ, η, γ care îndeplinesc condițiile de mai sus.

Constatăm pentru început că $n \geq 2$: Relația considerată duce la $-\varepsilon \lambda^{3n} \gamma^3 \equiv \xi^3 + \eta^3 \equiv \pm 1 \pmod{\lambda^4}$. Dar $\lambda \nmid \pm 2$, deci $-\varepsilon \lambda^{3n} \gamma^3 \equiv 0 \pmod{\lambda^4}$ și cum $\lambda \nmid \gamma$, obținem $n \geq 2$.

Revenim la relația $\xi^3 + \eta^3 + \varepsilon \lambda^{3n} \gamma^3 = 0$, pe care o rescriem $-\varepsilon \lambda^{3n} \gamma^3 = (\xi + \eta)(\xi + \rho\eta)(\xi + \rho^2\eta)$. Diferențele dintre factorii din membrul drept al acestei relații sunt $\eta\lambda$, $\rho\eta\lambda$ și $\rho^2\eta\lambda$, toate asociate cu $\eta\lambda$. Cum $\lambda \nmid \eta$, aceste diferențe 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 ; ceilalți se vor divide cu λ (căci diferențele se divid cu λ), dar nu se vor divide cu λ^2 (căci diferențele 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 $\xi + \eta = \lambda^{3n-2} \kappa_1$, $\xi + \rho\eta = \lambda \kappa_2$ și $\xi + \rho^2\eta = \lambda \kappa_3$. Dacă $\delta \in R$ ar divide κ_2 și κ_3 , atunci δ ar divide $\rho\eta = \kappa_2 - \kappa_3$ și $\rho\xi = \rho\kappa_3 - \rho^2\kappa_2$, deci δ ar divide η și ξ , ceea ce (dat fiind că η și 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 observații, relația $-\varepsilon \lambda^{3n} \gamma^3 = (\xi + \eta)(\xi + \rho\eta)(\xi + \rho^2\eta)$ conduce la $-\varepsilon \gamma^3 = \kappa_1 \kappa_2 \kappa_3$. Prin urmare, κ_1, κ_2 și κ_3 sunt asociate cu cuburi din R . Există deci $\theta, \phi, \psi \in R$ și $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in U(R)$ astfel încât $\kappa_1 = \varepsilon_1 \theta^3$, $\kappa_2 = \varepsilon_2 \phi^3$ și $\kappa_3 = \varepsilon_3 \psi^3$. 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 $\varepsilon_4 = \varepsilon_3 \varepsilon_2^{-1} \rho$ și $\varepsilon_5 = \varepsilon_1 (\varepsilon_2 \rho)^{-1}$ sunt evident unități 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 $\lambda \nmid \phi$ și $\lambda \nmid \psi$, avem, conform pasului 2, $\phi^3 \equiv \pm 1 \pmod{\lambda^4}$ și $\psi^3 \equiv \pm 1 \pmod{\lambda^4}$; cu atât mai mult $\phi^3 \equiv \pm 1 \pmod{\lambda^2}$ și $\psi^3 \equiv \pm 1 \pmod{\lambda^2}$. Prin urmare, $\pm 1 \pm \varepsilon_4 \equiv 0 \pmod{\lambda^2}$. Dar elementele $\pm 1 \pm \rho$ și $\pm 1 \pm \rho^2$ sunt asociate fie cu 1, fie cu λ , prin urmare nu sunt divizibile cu λ^2 . Rămâne deci că $\varepsilon_4 = \pm 1$.

Obținem prin urmare $\phi^3 + (\pm \psi)^3 + \varepsilon_5 \lambda^{3(n-1)} \theta^3 = 0$, adică o nouă relație de

tipul considerat, dar în care însă exponentul lui λ a scăzut cu 3. Aplicând acest procedeu de încă $n - 2$ ori, vom obține o relație de același tip, dar în care exponentul lui λ este 3, contradicție cu observația făcută mai devreme că în orice astfel de relație exponentul lui λ este cel puțin 6. Prin urmare, presupunerea că ecuația considerată are soluții netriviale în R este falsă. În concluzie, ecuația $x^3 + y^3 = z^3$ nu are soluții netriviale în R^3 (și cu atât mai puțin în numere întregi).

44. Notățiile pe care le vom folosi sunt cele din soluția problemei 43. Să observăm mai întâi că dacă în R are loc o relație de forma $\xi^3 + \eta^3 + 5\zeta^3 = 0$ cu ξ, η și ζ prime două câte două, atunci ζ se divide prin λ : Să presupunem că ζ nu se divide prin λ . Atunci avem fie că $\lambda \nmid \xi$ și $\lambda \nmid \eta$, deci (vezi soluția problemei 43) cuburile acestora sunt congruente cu $\pm 1 \pmod{\lambda^4}$ și rezultă $\pm 1 \pm 1 \pm 5 \equiv 0 \pmod{\lambda^4}$, deci $\lambda^4 | 5$ sau $\lambda^4 | 7$, de unde $81 = N(\lambda^4) | N(5) = 25$ sau $81 = N(\lambda^4) | N(7) = 49$, contradicție, fie că unul dintre elementele ξ și 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 $\pm 1 \pm 5 \equiv 0 \pmod{\lambda^3}$. Se obține $\lambda^3 | 4$ 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 soluții ale ecuației din enunț (ele sunt așa-numitele "soluții triviale" ale ecuației considerate). Ne propunem în continuare să arătăm că nu există alte soluții. Aceasta este o consecință a faptului că ecuația $\xi^3 + \eta^3 + 5\zeta^3 = 0$ nu are soluții netriviale (adică cu toate componentele nenule) în inelul R , afirmație pe care o vom demonstra în cele ce urmează. Fie (ξ, η, ζ) o soluție netrivială a acestei ecuații. Putem considera că ξ, η și ζ sunt prime două câte două în R (altfel, simplificăm relația prin cubul c.m.m.d.c.-ului lor). Conform celor de mai sus, λ trebuie să dividă ζ . Atunci, există $n \in \mathbb{N}^*$ și $\gamma \in R$ astfel încât $\zeta = \lambda^n \gamma$, $\lambda \nmid \xi$ și $\lambda \nmid \eta$. Ținând cont de aceste constatări, avem practic de demonstrat că relația $\xi^3 + \eta^3 + 5\lambda^{3n}\gamma^3 = 0$ este imposibilă în condițiile în care ξ, η, γ nu se divid prin λ , iar $(\xi, \eta) = 1$. Vom arăta ceva mai mult, și anume că relația $\xi^3 + \eta^3 + 5\varepsilon\lambda^{3n}\gamma^3 = 0$ este imposibilă în condițiile în care ξ, η, γ nu se divid prin λ , $\varepsilon \in U(R)$, iar $(\xi, \eta) = 1$. Presupunem că relația $\xi^3 + \eta^3 + 5\varepsilon\lambda^{3n}\gamma^3 = 0$, $\varepsilon \in U(R)$, este satisfăcută de ξ, η, γ care îndeplinesc condițiile de mai sus.

Constatăm pentru început că $n \geq 2$: Relația considerată duce la $-5\varepsilon\lambda^{3n}\gamma^3 = \xi^3 + \eta^3 \equiv \pm 1 \pm 1 \pmod{\lambda^4}$. Dar $\lambda \nmid \pm 2$, deci $-5\varepsilon\lambda^{3n}\gamma^3 \equiv 0 \pmod{\lambda^4}$ și cum $\lambda \nmid \gamma$, obținem $n \geq 2$.

Revenim la relația $\xi^3 + \eta^3 + 5\varepsilon\lambda^{3n}\gamma^3 = 0$, pe care o rescriem $-5\varepsilon\lambda^{3n}\gamma^3 =$

$(\xi + \eta)(\xi + \rho\eta)(\xi + \rho^2\eta)$. Diferențele dintre factorii din membrul drept al acestei relații sunt $\eta\lambda$, $\rho\eta\lambda$ și $\rho^2\eta\lambda$, toate asociate cu $\eta\lambda$. Cum $\lambda \nmid \eta$, aceste diferențe 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 ; ceilalți se vor divide cu λ (căci diferențele se divid cu λ), dar nu se vor divide cu λ^2 (căci diferențele nu se divid cu λ^2). Înlocuind eventual η cu $\rho\eta$ sau cu $\rho^2\eta$, putem presupune că $\lambda^2 \mid \xi + \eta$. Există prin urmare $\kappa_1, \kappa_2, \kappa_3 \in R$, nedivizibile cu λ , astfel ca $\xi + \eta = \lambda^{3n-2}\kappa_1$, $\xi + \rho\eta = \lambda\kappa_2$ și $\xi + \rho^2\eta = \lambda\kappa_3$. Dacă $\delta \in R$ ar divide κ_2 și κ_3 , atunci δ ar divide $\rho\eta = \kappa_2 - \kappa_3$ și $\rho\xi = \rho\kappa_3 - \rho^2\kappa_2$, deci δ ar divide η și ξ , ceea ce (dat fiind că η și 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 observații, relația $-5\varepsilon\lambda^{3n}\gamma^3 = (\xi + \eta)(\xi + \rho\eta)(\xi + \rho^2\eta)$ ne conduce la $-5\varepsilon\gamma^3 = \kappa_1\kappa_2\kappa_3$. Prin urmare, există $\theta, \phi, \psi \in R$ și $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in U(R)$ astfel încât să aibă loc una dintre următoarele situații:

1. $\kappa_1 = 5\varepsilon_1\theta^3$, $\kappa_2 = \varepsilon_2\phi^3$ și $\kappa_3 = \varepsilon_3\psi^3$,
2. $\kappa_1 = \varepsilon_1\theta^3$, $\kappa_2 = 5\varepsilon_2\phi^3$ și $\kappa_3 = \varepsilon_3\psi^3$,
3. $\kappa_1 = \varepsilon_1\theta^3$, $\kappa_2 = \varepsilon_2\phi^3$ și $\kappa_3 = 5\varepsilon_3\psi^3$.

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 obține din această relație în fiecare din cazurile de mai sus.

În cazul 1 se obține $5\varepsilon_1\lambda^{3n-2}\theta^3 + \varepsilon_2\rho\lambda\phi^3 + \varepsilon_3\rho^2\lambda\psi^3 = 0$. Prin urmare, $\phi^3 + \varepsilon_4\psi^3 + 5\varepsilon_5\lambda^{3n-3}\theta^3 = 0$, unde $\varepsilon_4 = \varepsilon_3\varepsilon_2^{-1}\rho$ și $\varepsilon_5 = \varepsilon_1(\varepsilon_2\rho)^{-1}$ sunt evidente unități 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 $\lambda \nmid \phi$ și $\lambda \nmid \psi$, avem (vezi soluția problemei 43) $\phi^3 \equiv \pm 1 \pmod{\lambda^4}$ și $\psi^3 \equiv \pm 1 \pmod{\lambda^4}$; cu atât mai mult $\phi^3 \equiv \pm 1 \pmod{\lambda^2}$ și $\psi^3 \equiv \pm 1 \pmod{\lambda^2}$. Prin urmare, $\pm 1 \pm \varepsilon_4 \equiv 0 \pmod{\lambda^2}$. Dar elementele $\pm 1 \pm \rho$ și $\pm 1 \pm \rho^2$ 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 obține $\varepsilon_1\lambda^{3n-2}\theta^3 + 5\varepsilon_2\rho\lambda\phi^3 + \varepsilon_3\rho^2\lambda\psi^3 = 0$ și prin urmare, $\phi^3 + 5\varepsilon_4\psi^3 + \varepsilon_5\lambda^{3n-3}\theta^3 = 0$, unde $\varepsilon_4 = \varepsilon_3\varepsilon_2^{-1}\rho$ și $\varepsilon_5 = \varepsilon_1(\varepsilon_2\rho)^{-1}$ sunt evidente unități 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 $\lambda \nmid \phi$ și $\lambda \nmid \psi$, avem (vezi soluția problemei 43) $\phi^3 \equiv \pm 1 \pmod{\lambda^4}$ și $\psi^3 \equiv \pm 1 \pmod{\lambda^4}$; cu atât mai mult $\phi^3 \equiv \pm 1 \pmod{\lambda^3}$ și $\psi^3 \equiv \pm 1 \pmod{\lambda^3}$. Prin urmare, $\pm 1 \pm 5\varepsilon_4 \equiv 0 \pmod{\lambda^3}$. Dar elementele $\pm 1 \pm 5$, $\pm 1 \pm 5\rho$ și $\pm 1 \pm 5\rho^2$ 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 și se trage concluzia că nici acest caz nu este posibil.

Singura variantă rămasă în discuție este prin urmare cea obținută în cazul 1. Ea conduce la relația $\phi^3 + (\pm\psi)^3 + 5\varepsilon_5\lambda^{3(n-1)}\theta^3 = 0$, adică o nouă relație de tipul considerat, în care însă exponentul lui λ a scăzut cu 3. Aplicând acest procedeu de încă $n - 2$ ori, vom obține o relație de același tip, dar în care exponentul lui λ este 3, contradicție cu observația făcută mai sus că în orice astfel de relație exponentul lui λ este cel puțin 6. Prin urmare, presupunerea că ecuația considerată are soluții netriviiale în R este falsă.

În concluzie, ecuația $x^3 + y^3 = z^3$ nu are soluții netriviiale în R^3 (și cu atât mai puțin în numere întregi).

45. (i) Considerăm polinoamele în $K[Y, Z][X]$. Ele sunt monice, deci primitive. Pentru $X^2 - Y$ și $X^2 - YZ^2$ 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 $K[X, Y] \simeq K[Y][X]$ și 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 $g, h \in K[X, Y]$ neinvertibile. Scriem $g = g_0 + g_1X + \dots + g_kX^k$ și $h = h_0 + h_1X + \dots + h_lX^l$, unde $g_i \in K[Y]$ pentru orice $i \in \{1, \dots, k\}$, $h_j \in K[Y]$ pentru orice $j \in \{1, \dots, l\}$ și constatăm că $l = \text{grad}_X(h) \leq r$ și $k = \text{grad}_X(g) \leq r$. Cu considerații similare găsim $m = \text{grad}_Y(g) \leq s$ și $n = \text{grad}_Y(h) \leq s$. De fapt, inegalitățile apărute sunt chiar stricte, căci dacă, de exemplu $f = g(X)h(X, Y)$, rezultă că $\text{grad}_Y(h) = s$ și, dacă notăm coeficientul dominant al lui $h \in K[X][Y]$ cu $\bar{h}(X)$, $g(X)\bar{h}(X) = 1$, ceea ce arată că $g(X)$ este inversabil, contradicție.

Acum scriem $g = \sum_{0 \leq i \leq k, 0 \leq j \leq l} g_{ij}X^iY^j$ și $h = \sum_{0 \leq i \leq m, 0 \leq j \leq n} h_{ij}X^iY^j$, $g_{ij}, h_{ij} \in K$.

Cum r și s sunt prime între ele, unul dintre ele este impar, să zicem s . Atunci, în inelul de polinoame $K[U]$ avem relația $g(U^s, -U^r)h(U^s, -U^r) = f(U^s, -U^r) = 0$. 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 $i_1 \equiv i_2 \pmod{r}$ și $j_1 \equiv j_2 \pmod{s}$. Dar

$i_1, i_2 \in \{0, 1, \dots, r-1\}$ și $j_1, j_2 \in \{0, 1, \dots, s-1\}$, deci în situația dată $i_1 s + j_1 r = i_2 s + j_2 r \Leftrightarrow i_1 = i_2$ și $j_1 = j_2$. În concluzie, la termeni diferiți din g și h corespund termeni diferiți în $g(U^s, -U^r)$ și $h(U^s, -U^r)$. Prin urmare, termenii din g , respectiv h nu se pot reduce când facem $X = U^r$ și $Y = -U^s$. Atunci $g(U^s, -U^r) \neq 0 \neq h(U^s, -U^r)$, contradicție 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 $\varphi : K[Y, Z] \rightarrow K[Y], \varphi(g) = g(Y, 0)$. Extindem pe φ la un morfism $\bar{\varphi} : K[Y, Z][X] \rightarrow K[Y][X]$ cu proprietatea $\bar{\varphi}(X) = X$ și observăm că $\bar{\varphi}(f) = X^r + Y^s$. Din $r \equiv 1 \pmod{st}$ rezultă că $(r, s) = 1$, deci, conform (i), $\bar{\varphi}(f) \in K[Y][X]$ este ireductibil. În plus, $\text{grad}_X(\bar{\varphi}(f)) = r = \text{grad}_X(f)$, 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 $p = 5$ și obținem ireductibilitatea lui f în $\mathbb{Q}[\sqrt{3}][X]$. Cum $(\sqrt{3}, 25) = 1$, f este și primitiv, deci este ireductibil și în $\mathbb{Z}[\sqrt{3}][X]$.

(ii) Începem prin a observa că polinomul $X^3 + 6X + 2$ este ireductibil în $\mathbb{Q}[X]$ (are gradul 3 și nu are rădăcini raționale) și 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 coeficienții $X+1$ și $-2(X^3 + 6X + 2)$ sunt primi între ei, f este și 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} și elementul prim $p = 2$). Cum în plus f este primitiv, rezultă că el este ireductibil și în $\mathbb{Z}[X]$.

(ii) Aplicația $\Phi : \mathbb{Z}[X] \rightarrow \mathbb{Z}[X], \Phi(h) = h(X+1)$ este evident un morfism de inele unitare. Analog $\Psi : \mathbb{Z}[X] \rightarrow \mathbb{Z}[X], \Psi(h) = h(X-1)$ este morfism de inele unitare și este inversul lui Φ , deci Φ este izomorfism. Prin urmare, f este ireductibil dacă și 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 obține $j(j-1) \cdots 1 \cdot C_p^j = p(p-1) \cdots (p-j+1)$ și deci p divide unul din factorii produsului din membrul stâng al egalității iar singurul posibil este C_p^j . În concluzie, $p | C_p^j$ pentru orice $j \in \{1, \dots, p-1\}$. Prin urmare, $f(X+1) \in \mathbb{Z}[X]$ verifică condițiile pentru aplicarea criteriului lui Eisenstein (în raport cu elementul prim $p \in \mathbb{Z}$). Se obține că $f(X+1)$ este ireductibil peste \mathbb{Q} . Fiind monic este și primitiv, deci este ireductibil peste \mathbb{Z} . Conform celor de mai sus, $f \in \mathbb{Z}[X]$ este la rândul său ireductibil.

(iii) Cu notațiile de la punctul (ii), $\Phi(f) = \sum_{k=1}^{p^n} C_{p^n}^k X^k + p$. Pentru $j \in \{1, 2, \dots, p^n - 1\}$ 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 $i \in \{1, 2, \dots, j\}$ 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 relației 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 și p^{t_j} . Prin urmare, după ce facem toate simplificările posibile, obținem un număr întreg divizibil prin p^{n-t_j} . Cum $t_j < n$, tragem concluzia că fiecare coeficient binomial $C_{p^n}^j$, $j \in \{1, \dots, p^n - 1\}$, este divizibil cu p . În consecință, 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 și primitiv, deci este ireductibil și peste \mathbb{Z} . Rezultă așadar că $f \in \mathbb{Z}[X]$ este la rândul său ireductibil.

(iv) Aplicăm criteriul reducerii. Considerăm morfismul canonic $\pi : \mathbb{Z} \rightarrow \mathbb{Z}_p$, $\pi(x) = \hat{x}$ și extinsul său $\bar{\pi} : \mathbb{Z}[X] \rightarrow \mathbb{Z}_p[X]$. Este suficient să demonstrăm că polinomul $\bar{f} = \bar{\pi}(f)$, $\bar{f} = X^p - X + \hat{a}$ este ireductibil în $\mathbb{Z}_p[X]$. Fie K o extindere a lui \mathbb{Z}_p în care \bar{f} are o rădăcină (vezi problema 39 din Capitolul 5) și fie $\alpha \in K$ o rădăcină a lui \bar{f} . În grupul multiplicativ $\mathbb{Z}_p \setminus \{0\}$ (de ordin $p-1$) orice element \hat{x} are proprietatea $\hat{x}^{p-1} = 1$, deci pentru orice $\hat{k} \in \mathbb{Z}_p$

avem relația $\widehat{k}^p = \widehat{k}$. De aici rezultă că $\alpha, \alpha + \widehat{1}, \dots, \alpha + \widehat{p-1}$ sunt și 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 obținem $(X - \alpha)(X - \alpha - \widehat{1}) \cdots (X - \alpha - \widehat{p-1}) = gh$, 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 , aparține 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 $p|a$, contradicție.

49. (i) Considerăm morfismul canonic $\pi : \mathbb{Z} \rightarrow \mathbb{Z}_2$, $\pi(a) = \widehat{a}$, și extinsul său $\overline{\pi} : \mathbb{Z}[X] \rightarrow \mathbb{Z}_2[X]$ (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 coeficienții 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 $\overline{g} = (X^4 + X^3 + 1)^p$ și $\overline{h} = (X^4 + X^3 + 1)^q$. Rezultă că $f = [(X^4 + X^3 + 1)^p + 2g_1][(X^4 + X^3 + 1)^q + 2h_1]$. Înmulțim și obținem $(X^4 + X^3 + 1)^n + 4(X^4 + X^3 + 1)^m + 2 = (X^4 + X^3 + 1)^{p+q} + 2(X^4 + X^3 + 1)^p h_1 + 2(X^4 + X^3 + 1)^q g_1 + 4g_1 h_1$, de unde $2(X^4 + X^3 + 1)^m + 1 = (X^4 + X^3 + 1)^p h_1 + (X^4 + X^3 + 1)^q g_1 + 2g_1 h_1$. Aplicând din nou $\overline{\pi}$, obținem în $\mathbb{Z}_2[X]$ relația contradictorie $1 = (X^4 + X^3 + 1)^p \overline{h}_1 + (X^4 + X^3 + 1)^q \overline{g}_1$. Rămâne așadar că f este ireductibil peste \mathbb{Z} (deci și peste \mathbb{Q}).

(ii) Polinomul $f = X^4 + 3X^3 + 3X^2 - 5$ nu are rădăcini raționale, deoarece nici unul dintre divizorii lui 5 nu este rădăcină. Prin urmare, el fiind și 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 relație modulo 2 și obținem în $\mathbb{Z}_2[X]$ relația $X^4 + X^3 + X^2 + 1 = \overline{f} = \overline{g}\overline{h}$. Cum $4 = \text{grad}\overline{g} + \text{grad}\overline{h} \leq \text{grad}g + \text{grad}h = 4$, obținem $\text{grad}\overline{g} = \text{grad}\overline{h} = 2$. Pe de altă parte, în inelul euclidian $\mathbb{Z}_2[X]$ polinomul \overline{f} are descompunerea unică în factori primi $\overline{f} = (X + 1)(X^3 + X + 1)$, contradicție. 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 $f \in K[X_1, X_2][X_3]$ și, 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 $X_1^2 + \dots + X_k^2$ este ireductibil în $K[X_1, \dots, X_k]$. Atunci, lui $X_1^2 + \dots + X_{k+1}^2 = X_{k+1}^2 + (X_1^2 + \dots + X_k^2) \in K[X_1, X_2, \dots, X_{k+1}] \simeq K[X_1, X_2, \dots, X_k][X_{k+1}]$, care constatăm că este primitiv deoarece este monic, îi aplicăm criteriul lui Eisenstein cu $p = X_1^2 + \dots + X_k^2$ și constatăm că este ireductibil, ceea ce încheie pasul de inducție și demonstrația.

51. Să notăm $f = X^4 + 1 \in \mathbb{Z}[X]$. Este evident că funcția $\Phi : \mathbb{Z}[X] \rightarrow \mathbb{Z}[X]$, $\Phi(g) = g(X + 1)$ este un automorfism al inelului $\mathbb{Z}[X]$. Prin urmare, un polinom g este ireductibil dacă și 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 și 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 soluția 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 soluția 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 situațiile de mai sus, atunci (vezi demonstrația lemei din soluția problemei 37) $(-1)^{\frac{p-1}{2}} \equiv 2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ și 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 $X^4 + 1 = X^4 - 2X^2 + 1 - (-2X^2) = (X^2 + cX + 1)(X^2 - cX + 1)$ și demonstrația este încheiată.

52. Procedăm prin inducție după n . Pentru $n = 1$, $f_1 = X_{11}$, care este în mod evident ireductibil. Presupunem acum că f_k este ireductibil. Avem relația $f_{k+1} = X_{k+1,1}A_{k+1,1} + \dots + X_{k+1,k+1}A_{k+1,k+1}$, unde A_{ij} desemnează complementul algebric al lui X_{ij} din matricea

$$\begin{pmatrix} X_{11} & X_{12} & \dots & X_{1,k+1} \\ X_{21} & X_{22} & \dots & X_{2,k+1} \\ \vdots & \vdots & & \vdots \\ X_{k+1,1} & X_{k+1,2} & \dots & X_{k+1,k+1} \end{pmatrix}.$$

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 $Q(\mathbb{Z}[\{X_{ij}|i, j \in \{1, \dots, k+1\}\} \setminus \{X_{k+1,k+1}\}][X_{k+1,k+1}])$. Este suficient deci să arătăm că este primitiv în $\mathbb{Z}[\{X_{ij}|i, j \in \{1, \dots, k+1\}\} \setminus \{X_{k+1,k+1}\}][X_{k+1,k+1}]$. Presupunând că nu este primitiv, rezultă (ținând cont că f_k este ireductibil din ipoteza de inducție) că $f_k | X_{k+1,1}A_{k+1,1} + \dots + X_{k+1,k}A_{k+1,k}$, ceea ce revine la $f_k | A_{k+1,j}$ pentru orice $j \in \{1, \dots, k\}$. Dar aceste relații sunt contradictorii, deoarece dacă facem $X_{1j} = \dots = X_{kj} = 0$, f_k se anulează, iar $A_{k+1,j}$ nu se anulează. Rămâne că f_{k+1} este primitiv în $\mathbb{Z}[\{X_{ij}|i, j \in \{1, \dots, k+1\}\} \setminus \{X_{k+1,k+1}\}][X_{k+1,k+1}]$ și demonstrația este încheiată.

53. Procedăm prin inducție după n . Pentru $n = 1$, $f_1 = X_{11}$, care este în mod evident ireductibil. Presupunem acum că f_k este ireductibil. Avem relația $f_{k+1} = X_{1,k+1}A_{k+1,1} + \dots + X_{k+1,k+1}A_{k+1,k+1}$, unde A_{ij} desemnează complementul algebric al elementului de pe poziția i, j din matricea

$$\begin{pmatrix} X_{11} & X_{12} & \dots & X_{1,k+1} \\ X_{12} & X_{22} & \dots & X_{2,k+1} \\ \vdots & \vdots & & \vdots \\ X_{1,k+1} & X_{2,k+1} & \dots & X_{k+1,k+1} \end{pmatrix}.$$

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 $Q(\mathbb{Z}[\{X_{ij}|i, j \in \{1, \dots, k+1\}, i \leq j\} \setminus \{X_{k+1,k+1}\}][X_{k+1,k+1}])$. Este deci suficient să arătăm că este primitiv în $\mathbb{Z}[\{X_{ij}|i, j \in \{1, \dots, k+1\}, i \leq j\} \setminus \{X_{k+1,k+1}\}][X_{k+1,k+1}]$. Presupunând că nu este primitiv, rezultă (ținând cont că f_k este ireductibil din ipoteza de inducție) că $f_k | X_{1,k+1}A_{k+1,1} + \dots + X_{k,k+1}A_{k+1,k}$, ceea ce revine la $f_k | A_{j,k+1}$ pentru orice $j \in \{1, \dots, k\}$. Dar aceste relații sunt contradictorii, deoarece, dacă facem $X_{1j} = \dots = X_{jj} = X_{j,j+1} = \dots = X_{jk} = 0$, f_k se anulează, iar $A_{k+1,j}$ nu se anulează. Rămâne că f_{k+1} este primitiv în $\mathbb{Z}[\{X_{ij}|i, j \in \{1, \dots, k+1\}, i \leq j\} \setminus \{X_{k+1,k+1}\}][X_{k+1,k+1}]$ și demonstrația este încheiată.

54. Procedăm prin inducție după n . Pentru $n = 1$, $f_1 = X_1$, care este în mod evident ireductibil. Presupunem acum că f_k este ireductibil. Avem relația $f_{k+1} = X_{k+1}A_{k+1,1} + \dots + X_{2k+1}A_{k+1,k+1} + X_{2k+1}A_{k+1,k+1}$, unde A_{ij} desemnează complementul algebric al elementului de pe poziția 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 (ținând cont că f_k este ireductibil din ipoteza de inducție) 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 relații 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 $\mathbb{Z}[X_1, \dots, X_{2k}][X_{2k+1}]$ și demonstrația este încheiată.

55. Notăm $g_n = \sum_{i=1}^n T_i f_i$. Vom demonstra afirmația prin inducție 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 $(T_1 f_1, f_2) = 1$ și 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 $g_{n+1} = f_{n+1}T_{n+1} + g_n \in k[X_1, \dots, X_q][T_1, \dots, T_n][T_{n+1}]$, ținem seama de faptul că are loc izomorfismul

$$k[X_1, \dots, X_q][T_1, \dots, T_n][T_{n+1}] \simeq k[X_1, \dots, X_q, T_1, \dots, T_n][T_{n+1}]$$

și 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} și g_n trebuie să dividă $(f_1, \dots, f_{n+1}) = 1$) și 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 inducție și demonstrația.

Bibliografie

- [1] T. Albu, I. D. Ion, *Capitole de teoria algebrică a numerelor*, Editura Academiei R. S. R., 1984.
- [2] T. Albu, Ș. Raianu, *Lecții de algebră comutativă*, Tipografia Universității din București, 1984.
- [3] M. Becheanu, C. Vraciu, *Probleme de teoria grupurilor*, Tipografia Universității din București, 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 Universității din București, 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 și pedagogică, București, 1981.
- [10] I. D. Ion, C. Niță, N. Radu, D. Popescu, *Probleme de algebră*, Editura didactică și pedagogică, București, 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 mulțimilor*, Editura didactică și pedagogică, București, 1974.
- [15] C. Năstăsescu, *Inele. Module. Categorii*, Editura Academiei R. S. R., 1976.
- [16] C. Năstăsescu, C. Niță, C. Vraciu, *Bazele Algebrei*, Editura Academiei R. S. R., 1986.
- [17] L. Panaitopol, A. Gica, *O introducere în aritmetică și teoria numerelor*, Editura Universității din București, 2001.
- [18] P. Samuel, *Anneaux factoriels*, Publicação do instituto de pesquisas matematicas da Universidade de Sao Paolo e da sociedade matematica de Sao Paolo, 1963.
- [19] I. Tomescu, *Probleme de combinatorică și teoria grafurilor*, Editura didactică și pedagogică, București, 1981.