

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

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 maxime 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 sale subgrupuri normale 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 și este cel mai mare subgrup normal al lui G conținut în H .

- 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 bijecțiilor 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:

- Există un element $e \in S$ cu proprietatea că $ea = a$ pentru orice $a \in S$;
- 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

- 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:

- S este grup;
- 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. 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.

9. 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 $x \in G$.

10. 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.

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

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

13. 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 $i \in I$.

14. 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*).

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

16. (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 .

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

18. 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.

19. 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

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

produsul direct conținând n factori.

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

21. 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.

22. 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.

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

24. 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.

25. 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.

26. 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.

27. 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.

28. 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 $[L \cap H : L \cap K] \leq [H : K]$.

29. 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.

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 .
Afirmatia (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 29(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;
- (iii) Să se dea un exemplu de grup neabelian G pentru care $|I| = (3/4)|G|$.

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 ciclilor de lungime 3.

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

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 integru*. (Echivalent, dacă $ab = 0$, atunci $a = 0$ sau $b = 0$.) Un inel integru 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 integrabil 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 $s_1, \dots, s_n \in S$, 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.
- a) 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.
 - b) Să se arate că dacă $(a, b) = 1$, atunci inelul $\mathbb{Z}[\sqrt{d}]/(a + b\sqrt{d})$ este izomorf cu inelul $\mathbb{Z}/(a^2 - db^2)$.

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 $\text{grad } f \geq 1$ 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 $0 \leq i \leq n$, $\text{grad}_{X_i}(g_0) < q$ pentru orice $1 \leq i \leq n$, și $\text{grad}(g_0) \leq \text{grad}(f)$.

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 $a \mid_R b$ sau $a \mid b$) 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 $a \mid_R b$ și $b \mid_R a$. 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) $d \mid a$ și $d \mid b$.

(ii) Pentru orice $d' \in R$ care divide a și b avem $d' \mid d$.

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) $a \mid m$ și $b \mid m$.

(ii) Pentru orice $m' \in R$ care se divide prin a și b avem $m \mid m'$.

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) $a \mid bc$ și $(a, b) = 1$ implică $a \mid c$;
- (vi) $a \mid c, b \mid c$ și $(a, b) = 1$ implică $ab \mid c$.

• 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 $p \mid ab$ rezultă $p \mid a$ sau $p \mid b$.

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) $p \mid a_0, p \mid a_1, \dots, p \mid a_{n-1}$.

(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 $a \mid b$, 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) c.m.m.d.c. $(X^2, X^3) = 1$ și c.m.m.m.c. (X^2, X^3) nu există;

(iii) c.m.m.d.c. (X^5, X^6) și 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) Localizatului 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.

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.