Link-uri utile

- Grup tutoriat
- Cursurile de la Băețica
- Cursurile de an trecut de la Mincu

Exerciții

Exercițiul 1. Scrieți elementele mulțimii $\mathscr{P}(\mathscr{P}(\mathscr{P}(\varnothing)))$.

Demonstrație.

$$\begin{aligned}\mathscr{P}(\varnothing) &= \{\ \varnothing\ \}\\ \mathscr{P}(\mathscr{P}(\varnothing)) &= \{\ \varnothing, \{\ \varnothing\ \}\ \}\\ \mathscr{P}(\mathscr{P}(\mathscr{P}(\varnothing))) &= \{\ \varnothing, \{\ \varnothing\ \}, \{\ \{\ \varnothing\ \}\ \}, \{\ \varnothing, \{\ \varnothing\ \}\ \}\ \}\end{aligned}$$

□

Exercițiul 2. Arătați că relația de congruență modulo n este relație de echivalență, folosind definiția.

Demonstrație. Fie $n \in \mathbb{N}^*$ fixat. Atunci spunem că $a \equiv b \mod n$ dacă $n \mid (a-b)$.

Pentru a demonstra că este relație de echivalență, trebuie să demonstrăm că este *reflexivă*, *simetrică* și *tranzitivă*.

1. Fie $a \in \mathbb{N}$. Atunci $n \mid (a-a) = 0$. Deci $a \equiv a \mod n$. Deci $\equiv$ este reflexivă.
2. Fie $a, b \in \mathbb{N}$ cu $a \equiv b \mod n$. Din definiție, $n \mid (a-b)$. Atunci $n \mid -(a-b)$. De unde rezultă că $n \mid (b-a)$. Deci $b \equiv a \mod n$. Deci $\equiv$ este simetrică.
3. Fie $a, b, c \in \mathbb{N}$ cu $a \equiv b \mod n$ și $b \equiv c \mod n$. Din definiție avem că $n \mid (a-b)$ și $n \mid (b-c)$. Atunci facem suma și avem că $n \mid ((a-b)+(b-c)) \implies n \mid (a-c)$. Deci $a \equiv c \mod n$. Deci $\equiv$ este tranzitivă.

Din acestea rezultă că $\equiv$ este relație de echivalență. □

Exercițiul 3. Demonstrați că relația $x \rho y \iff x^2 + 7x = y^2 + 7y$ este de echivalență.

Demonstrație. Demonstrația este similară cu cea de la exercițiul precedent, iar proprietățile decurg din faptul că egalitatea este reflexivă, simetrică și tranzitivă. □

Exercițiul 4. Fie A și A' submulțimi ale lui T. Arătați că:

1. $\chi_{A \cap A'} = \chi_A \cdot \chi_{A'}$
2. $\chi_{A \cup A'} = \chi_A + \chi_{A'} - \chi_A \cdot \chi_{A'}$
   În particular, dacă A și A' sunt disjuncte avem că $X_{A \cup A'} = \chi_A + \chi_{A'}$.
3. $\chi_{A \setminus A'} = \chi_A \cdot (1 - \chi_{A'})$

Demonstrație. Putem demonstra aceste egalități construind tabelul de valori pentru funcțiile χ.

1.

χ_A	$\chi_{A'}$	$\chi_{A\cap A'}$	$\chi_A \cdot \chi_{A'}$
0	0	0	$0 \cdot 0 = 0$
0	1	0	$0 \cdot 1 = 0$
1	0	0	$1 \cdot 0 = 0$
1	1	1	$1 \cdot 1 = 1$

2.

χ_A	$\chi_{A'}$	$\chi_{A\cup A'}$	$\chi_A + \chi_{A'} - \chi_A \cdot \chi_{A'}$
0	0	0	$0 + 0 - 0 \cdot 0 = 0$
0	1	1	$0 + 1 - 0 \cdot 1 = 1$
1	0	1	$1 + 0 - 1 \cdot 0 = 1$
1	1	1	$1 + 1 - 1 \cdot 1 = 1$

3.

χ_A	$\chi_{A'}$	$\chi_{A\setminus A'}$	$\chi_A \cdot (1 - \chi_{A'})$
0	0	0	$0 \cdot (1 - 0) = 0$
0	1	0	$0 \cdot (1 - 1) = 0$
1	0	1	$1 \cdot (1 - 0) = 1$
1	1	0	$1 \cdot (1 - 1) = 0$

□

Exercițiul 5. Dați exemplu de funcții $f, g : \mathbb{N} \to \mathbb{N}$ cu proprietatea că $g \circ f = 1_{\mathbb{N}}$, dar g nu este injectivă, iar f nu este surjectivă.

Demonstrație. O pereche de funcții care îndeplinesc aceste condiții sunt

$$g(n) = \begin{cases} 0, & \text{dacă } n = 0 \\ n - 1, & \text{dacă } n \geq 1 \end{cases}$$

$$f(n) = n + 1, \forall n \in \mathbb{N}$$

□

Link-uri utile

- Grup tutoriat
- Cursurile de la Băețica
- Cursurile de anul acesta de la Mincu
- Cursurile de an trecut de la Mincu

Exerciții

Exercițiul 1. Fie $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 + x$. Găsiți preimaginea lui $[6, 12]$ (mai multe exemple pe acest site).

Demonstrație. Aplicăm definiția preimaginii:

$$\begin{aligned} f^{-1}([6,12]) &= \{\, x \in \mathbb{R} \mid f(x) \in [6,12] \,\} \\ &= \{\, x \in \mathbb{R} \mid 6 \le f(x) \le 12 \,\} \\ &= \left\{\, x \in \mathbb{R} \;\middle|\; 6 \le x^2 + x \le 12 \,\right\} \end{aligned}$$

Deci problema se reduce la a găsi soluțiile inecuației $6 \le x^2 + x \le 12$.

- Rezolvăm $6 \le x^2 + x \iff 0 \le x^2 + x - 6$:

$$\begin{aligned} \Delta &= 1 + 4 \cdot 6 = 25 \\ x_1 &= \frac{-1+5}{2} = 2 \\ x_2 &= \frac{-1-5}{2} = -3 \end{aligned}$$

  Soluția este $x \in (-\infty, -3] \cup [2, +\infty)$.

- Rezolvăm $x^2 + x \le 12 \iff x^2 + x - 12 \le 0$:

$$\begin{aligned} \Delta &= 1 + 4 \cdot 12 = 49 \\ x_1 &= \frac{-1+7}{2} = 3 \\ x_2 &= \frac{-1-7}{2} = -4 \end{aligned}$$

  Soluția este $x \in [-4, 3]$.

Punând laolaltă rezultatele, obținem că preimaginea lui $[6, 12]$ este

$$((-\infty, -3] \cup [2, +\infty)) \cap [-4, 3] = [-4, -3] \cup [2, 3]$$

□

Exercițiul 2. Fie $f : [1, \infty) \to (0, 1]$, unde

$$f(x) = \frac{2x}{1 + x^2}$$

Demonstrați că f este bijectivă și găsiți f^{-1}.

Demonstrație. Ca să arătăm că f este bijectivă arătăm, pe rând, că este injectivă și surjectivă:

- f injectivă $\iff$ pentru orice $x_1, x_2 \in [1, \infty)$ avem că $f(x_1) = f(x_2) \implies x_1 = x_2$. Fie $x_1, x_2 \in [1, \infty)$.

$$\begin{aligned} & f(x_1) = f(x_2) \\ \iff & \frac{2x_1}{1+x_1^2} = \frac{2x_2}{1+x_2^2} \\ \iff & x_1(1+x_2^2) = (1+x_1^2)x_2 \\ \iff & x_1 + x_1x_2^2 = x_2 + x_1^2x_2 \\ \iff & x_1 - x_2 + x_1x_2^2 - x_1^2x_2 = 0 \\ \iff & (x_1 - x_2)(1 - x_1x_2) = 0 \\ \iff & \begin{cases} x_1 = x_2 \\ x_1x_2 = 1 \iff x_1 = \frac{1}{x_2} \\ \qquad \iff x_1 = x_2 = 1 \\ \qquad \text{pentru că } x_1, x_2 \in [1, \infty) \end{cases} \end{aligned}$$

- f surjectivă $\iff$ pentru orice $y \in (0, 1]$ există un $x \in [1, \infty)$ astfel încât $f(x) = y$. Trebuie să ne gândim cum ar arăta un x pentru care $f(x) = y$. Am avea că

$$\begin{aligned} & \frac{2x}{1+x^2} = y \\ \iff & yx^2 - 2x + y = 0 \\ & \Delta = 4 - 4y^2 \geq 0 \text{ pentru că } y \in (0, 1] \\ & x_1 = \frac{2 + \sqrt{4-4y^2}}{2y} = \frac{1 + \sqrt{1-y^2}}{y} \\ & x_2 = \frac{2 - \sqrt{4-4y^2}}{2y} = \frac{1 - \sqrt{1-y^2}}{y} \end{aligned}$$

  Dintre cele două posibilități, dacă încercăm să introducem valoarea $y = \frac{1}{2}$ doar prima convine. Acum trebuie să și demonstrăm că aceasta ar fi formula potrivită pentru x.

  Fie $y \in (0, 1]$. Luăm $x = \frac{1+\sqrt{1-y^2}}{y}$. Avem că

$$\begin{aligned} f\left(\frac{1+\sqrt{1-y^2}}{y}\right) &= \frac{2\frac{1+\sqrt{1-y^2}}{y}}{1 + \left(\frac{1+\sqrt{1-y^2}}{y}\right)^2} = \frac{2+2\sqrt{1-y^2}}{y} \cdot \frac{1}{\frac{y^2}{y^2} + \frac{1+2\sqrt{1-y^2}+1-y^2}{y^2}} \\ &= \frac{2+2\sqrt{1-y^2}}{y} \cdot \frac{y^2}{2+2\sqrt{1-y^2}} = y \end{aligned}$$

Din cele de mai sus rezultă că f este bijectivă.

Conform definiției, inversa unei funcții $f : A \to B$ este o funcție $g : B \to A$ cu proprietatea că $f \circ g = \mathbb{1}_B$ și $g \circ f = \mathbb{1}_A$.

Luăm $g : (0, 1] \to [1, \infty)$, $g(y) = \frac{1+\sqrt{1-y^2}}{y}$. Atunci avem că $f \circ g = \mathbb{1}_{[1,\infty)}$ (conform calculelor de la surjectivitate), și putem arăta și că $g \circ f = \mathbb{1}_{(0,1]}$ (prin alte calcule asemănătoare). □

Exercițiul 3. Fie $G = (V, E)$ un graf neorientat (respectiv orientat). Definim relația de echivalență pe noduri $n \rho m \iff n$ este vecin cu m. Ce reprezintă închiderea tranzitivă a lui ρ în acest caz?

Demonstrație. Conform definiției, închiderea tranzitivă a lui ρ este

$$\rho' = \bigcup_{n=1}^{+\infty} \rho^n$$

Să vedem ce reprezintă ρ^n pentru un anumit n.

Dacă există o muchie între nodul a și nodul b ($(a, b) \in \rho$), și o muchie între b și c ($(b, c) \in \rho$), atunci în ρ^2 vom avea perechea $(a, c) \in \rho^2$. Cu alte cuvinte, spunem că două noduri se află în relația $x \rho^2 y$ dacă există un drum de lungime doi între x și y.

Reunind toate drumurile de lungime $1, 2, \ldots, \infty$ obținem că $x \rho' y$ dacă există un drum de orice lungime între x și y.

Acum să vedem ce reprezintă clasele de echivalență pentru ρ'. Toate nodurile între care există un drum sunt echivalente. O mulțime maximală de noduri care sunt conectate se numește componentă conexă. □

Exercițiul 4. Pe mulțimea $\mathbb{C}^*$ (numere complexe în afară de 0) definim relația $\sim$ cu $z \sim w$ dacă 0, z, și w sunt coliniare. Arătați că $\sim$ este relație de echivalență și găsiți un sistem de reprezentanți.

Demonstrație. Pentru a demonstra că este relație de echivalență trebuie să arătăm că este

- *reflexivă*: Fie $z \in \mathbb{C}^*$. Atunci z se află pe dreapta $(0, z)$. Deci $z \sim z$.
- *simetrică*: Fie $z, w \in \mathbb{C}^*$ astfel încât $z \sim w$. Atunci $0, z, w$ sunt coliniare. Putem spune că și $0, w, z$ sunt coliniare. Deci $w \sim z$.
- *tranzitivă*: Fie $z, w, v \in \mathbb{C}^*$ astfel încât $z \sim w$ și $w \sim v$.

Deoarece toate punctele aflate pe o dreaptă care trece prin origine, am putea lua ca sistem de reprezentanți dreptele:

$$S = \{\ d \text{ dreaptă care trece prin } 0\ \}$$

Dacă ne dăm seama că singurul lucru care contează pentru a distinge aceste drepte este panta lor, putem să luăm ca sistem de reprezentanți unghiul pe care îl fac cu O_x:

$$S = \{\ u \text{ unghi } \mid u \in [0, 2\pi)\ \}$$

Să mai observăm și că obținem aceeași dreaptă dacă luăm două unghiuri la distanță π între ele. Așa că sistemul se poate reduce la

$$S = \{\ u \text{ unghi } \mid u \in [0, \pi)\ \}$$

□

Exercițiul 5. Fie $\sim$ relația pe $\mathbb{N} \times \mathbb{N}$ definită prin $(a,b) \sim (c,d)$ dacă $a + d = b + c$. Arătați că $\sim$ este o relație de echivalență și identificați un sistem de reprezentanți.

Demonstrație. Arătăm mai întâi că $\sim$ este de echivalență:

- *reflexivă*: Fie $(a,b) \in \mathbb{N} \times \mathbb{N}$. Avem că $a + b = b + a$. Deci $(a,b) \sim (a,b)$.
- *simetrică*: Fie $(a,b),(c,d) \in \mathbb{N} \times \mathbb{N}$ astfel încât $(a,b) \sim (c,d)$.
- *tranzitivă*: Fie $(a,b),(c,d),(e,f) \in \mathbb{N} \times \mathbb{N}$, cu

$$\left.\begin{array}{l}(a,b) \sim (c,d) \iff a + d = b + c \iff a - b = c - d \\ (c,d) \sim (e,f) \iff c + f = d + e \iff c - d = e - f\end{array}\right\} \implies$$
$$\implies a - b = e - f$$
$$\iff a + f = b + e$$
$$\iff (a,b) \sim (e,f)$$

Acum trebuie să alegem reprezentanți pentru fiecare clasă de echivalență. Observăm că dacă plecăm de la, de exemplu $(2,3)$ obținem

$$(0,1) \sim (1,2) \sim (2,3) \sim (3,4) \sim \cdots \sim (n, n+1)$$

Sau dacă plecăm de la $(7,4)$ obținem

$$(3,0) \sim \cdots \sim (6,3) \sim (7,4) \sim (8,5) \sim \cdots \sim (n+3, n)$$

Deci clasele de echivalență sunt de forma $(n, n+k)$ sau $(n+k, n)$. Luăm separat și cazul (n,n). Deci un sistem de reprezentanți ar fi

$$S = \left\{ (0,k) \;\middle|\; k \in \mathbb{N}^* \right\} \cup \left\{ (k,0) \;\middle|\; k \in \mathbb{N}^* \right\} \cup \{ (0,0) \}$$

O idee ar fi să identificăm perechile de forma $(k,0)$ cu $+k$ și cele de forma $(0,k)$ cu simbolul $-k$. Astfel aceste clase de echivalență se identifică cu $\mathbb{Z}$. Dacă avem o pereche oarecare (a,b), dacă $a > b$ atunci aceasta reprezintă numărul pozitiv cu modulul $a - b$, dacă $a < b$ reprezintă numărul negativ cu modulul $b - a$.

Regulile de calcul pentru $\mathbb{Z}$ funcționează și când lucrăm pe aceste perechi. Dacă luăm $(5,3)$ (care ar însemna $+2$) și adunăm $(1,6)$ (care ar însemna -5) obținem $(6,9)$ (care ar însemna (-3)). □

Exercițiul 6. Fie X o mulțime. Demonstrați că mulțimea funcțiilor $f : X \to X$ formează un monoid în raport cu operația de compunere a funcțiilor.

Demonstrație. Pentru a forma un monoid, operația $\circ$ trebuie să îndeplinească două cerințe:

- să fie asociativă (știm deja asta despre compunerea funcțiilor)
- să admită un element neutru: să existe o funcție $h : X \to X$ cu proprietatea că

$$f \circ h = h \circ f = f, \forall f : X \to X$$

Observăm că în cazul nostru elementul neutru este funcția identică $\mathbb{1}_X$.

□

Link-uri utile

- Grup tutoriat
- Cursurile de la Băețica
- Cursurile de anul acesta de la Mincu
- Cursurile de an trecut de la Mincu

Exerciții

Exercițiul 1. Fie $A = \{ 3, 6, 7, 9 \}$. Definim funcția $f : A \to \mathscr{P}(A)$, unde $f(x) =$ complementul mulțimii $\{ x \}$. Scrieți explicit cât este $f(3), f(6), f(7), f(9)$.

Demonstrație.

$$f(3) = C_A \{ 3 \} = \{ 6, 7, 9 \}$$
$$f(6) = C_A \{ 6 \} = \{ 3, 7, 9 \}$$
$$f(7) = C_A \{ 7 \} = \{ 3, 6, 9 \}$$
$$f(9) = C_A \{ 9 \} = \{ 3, 6, 7 \}$$

□

Exercițiul 2. Fie A o mulțime. Demonstrați că nu poate exista nicio funcție *surjectivă* de la A la $\mathscr{P}(A)$.

Demonstrație. Demonstrăm afirmația prin reducere la absurd.

Fie o mulțime A pentru care există o funcție surjectivă $f : A \to \mathscr{P}(A)$.

Din definiție, $f(x)$ este o submulțime a lui A. Atunci, pentru orice $x \in A$, avem două cazuri:

- fie $x \in f(x)$
- fie $x \notin f(x)$

Notăm cu $T = \{ x \in A \mid x \notin f(x) \}$.
Știm că T este o submulțime a lui A. Deci $T \in \mathscr{P}(A)$.
Deoarece f este surjectivă, există un $a \in A$ pentru care $f(a) = T$.
Acum ne punem întrebarea dacă $a \in T$:

- dacă $a \in T$, atunci din definiția lui T avem că $a \notin f(a)$, deci $a \notin T$
- dacă $a \notin T$, atunci din definiția lui T avem că $a \in f(a)$, deci $a \in T$

În ambele cazuri, ajungem la **contradicție**. Deci nu poate exista o astfel de funcție. □

Exercițiul 3. Fie $f : A \to B$ o funcție. Demonstrați că relația $a \, \rho_f \, b \iff f(a) = f(b)$ este de echivalență. Aceasta se numește *relația de echivalență asociată funcției* f.

Demonstrație. Pentru a arăta că ρ_f este relație de echivalență, arătăm că este:

- *reflexivă*: fie $a \in A$, avem că $f(a) = f(a)$, deci $a \, \rho_f \, a$.

- *simetrică*: fie $a, b \in A$ astfel încât $a \rho_f b$. Atunci $f(a) = f(b)$, de unde și $f(b) = f(a)$. Deci $b \rho_f a$.
- *tranzitivă*: fie $a, b, c \in A$ astfel încât $a \rho_f b$ și $b \rho_f c$. Atunci avem că $f(a) = f(b)$ și $f(b) = f(c)$. Deci și $f(a) = f(c)$, de unde rezultă că $a \rho_f c$.

□

Exercițiul 4. Fie $f : A \to B$. Demonstrați că f este injectivă dacă și numai dacă relația asociată ρ_f conține numai elemente de forma (x, x) (adică $x \rho_f y$ doar dacă x, y sunt egale).

Demonstrație. Mai întâi demonstrăm implicația directă.

Fie f o funcție injectivă. Vrem să arătăm că toate numerele care sunt în relație sunt egale, deci că nu există $x \rho_f y$ cu $x \neq y$. Să presupunem prin reducere la absurd că ar exista $x \neq y \in A$ pentru care $x \rho_f y$. Din definiția relației, avem că $f(x) = f(y)$. Din definiția injectivității, trebuie ca $x = y$. Ajungem la o contradicție.

Acum demonstrăm implicația inversă.

Știm că relația este $\rho_f = \{ (x, x) \mid x \in A \}$. Fie $x, y \in A$ pentru care $f(x) = f(y)$. Atunci din definiția lui ρ_f avem că $x \rho_f y$. Toate elementele din relație sunt de forma (x, x), deci $x = y$. De aici rezultă că f este injectivă. □

Exercițiul 5. Fie $A = \{ 3, -2, 7, 15, 21 \}$.

Verificați care dintre următoarele sunt partiții ale lui A:

- $P_1 = \{ \{ 3, 21 \}, \{ -2, 7, 15 \} \}$
- $P_2 = \{ \{ -2, 3 \}, \varnothing, \{ 7 \}, \{ 15, 21 \} \}$
- $P_3 = \{ \{ -2, 15 \}, \{ 7, 21 \} \}$
- $P_4 = \{ \{ 15, 21 \}, \{ -2, 7 \}, \{ 3, -2 \} \}$

Demonstrație.

- Este partiție, avem o mulțime de submulțimi nevide, disjuncte două câte două, iar reuniunea lor este toată mulțimea.
- Nu este partiție pentru că partiția este formată doar din mulțimi nevide.
- Nu este partiție pentru că elementul 3 nu apare în nicio submulțime.
- Nu este partiție pentru că elementul -2 apare în două submulțimi.

□

Exercițiul 6. Fie relația de echivalență $x \rho y \iff x^2 = y^2$ pentru $x, y \in \mathbb{R}$. Scrieți cât este mulțimea factor $\frac{\mathbb{R}}{\rho}$.

Demonstrație. Observăm că pentru această relație de echivalență, pentru orice $x \in \mathbb{R}$, $x \rho (-x)$. O să notăm clasa de echivalență a lui x cu $\hat{x} = \{ x, -x \}$. Pentru 0 avem o clasă de echivalență cu un singur element: $\hat{0} = \{ 0 \}$. Reunind toate clasele de echivalență, obținem mulțimea factor:

$$\frac{\mathbb{R}}{\rho} = \{ \hat{x} \mid x \in [0, +\infty) \}$$

□

Exercițiul 7. Considerăm pe $\mathbb{R}$ relația $x \rho y \iff x^2 + 7x = y^2 + 7y$.

Determinați $\frac{2}{\rho}$, $\frac{\mathbb{R}}{\rho}$, și găsiți un sistem complet și independent de reprezentanți pentru relația ρ.

Demonstrație.

1. Pentru a găsi clasa de echivalență a elementului 2 trebuie să găsim toate elementele care sunt echivalente cu el:

$$\begin{aligned}\frac{2}{\rho} &= \{\, x \in \mathbb{R} \mid x \rho 2 \,\} \\ &= \left\{\, x \in \mathbb{R} \;\middle|\; x^2 + 7x = 2^2 + 7 \cdot 2 \,\right\} \\ &= \left\{\, x \in \mathbb{R} \;\middle|\; x^2 + 7x - 18 = 0 \,\right\} \\ &= \{\, 2, -9 \,\} = \hat{2}\end{aligned}$$

2. Fie $y \in \mathbb{R}$ fixat. Atunci

$$\begin{aligned}\frac{y}{\rho} &= \{\, x \in \mathbb{R} \mid x \rho y \,\} \\ &= \left\{\, x \in \mathbb{R} \;\middle|\; x^2 + 7x = y^2 + 7y \,\right\} \\ &= \left\{\, x \in \mathbb{R} \;\middle|\; x^2 + 7x - (y^2 + 7y) = 0 \,\right\} \\ &= \{\, y, -y - 7 \,\} = \hat{y}\end{aligned}$$

   Deci $\frac{\mathbb{R}}{\rho} = \left\{\, \frac{y}{\rho} \;\middle|\; y \in \mathbb{R} \,\right\} = \{\, \{\, y, -y - 7 \,\} \mid y \in \mathbb{R} \,\}$.

3. Pentru a construi un sistem de reprezentanți, trebuie să alegem un element din fiecare clasă de echivalență.

   Am putea să luăm ca sistem de reprezentanți tot $\mathbb{R}$: $S = \{\, \hat{x} \mid x \in \mathbb{R} \,\}$. Acest sistem este complet, dar nu independent. De exemplu, $\hat{2} = \widehat{-9}$.

   Dacă încercăm să luăm câteva câteva clase de echivalențe găsim că:

$$\begin{aligned}\hat{5} &= \widehat{-5 - 7} = \widehat{-12} \\ \widehat{-4} &= -\widehat{(-4)} - 7 = \widehat{-3} \\ \hat{1} &= \widehat{-1 - 7} = \widehat{-8} \\ \widehat{-2} &= -\widehat{(-2)} - 7 = \widehat{-5}\end{aligned}$$

   Observăm că -3.5 este singur în clasa lui de echivalență, $\widehat{-3.5} = \{\, -3.5 \,\}$, deoarece $-3.5 = -(-3.5) - 7$.

   Bănuim că un sistem complet și independent de reprezentanți ar fi $S = [-3.5, \infty)$. Trebuie să și demonstrăm asta:

   - S este *complet*: fie $x \in \mathbb{R}$. Dacă $x \geq -3.5$ atunci reprezentantul lui x este $\hat{x}$. Dacă $x < -3.5$, atunci $-x - 7 > -3.5$, deci reprezentantul o să fie $\widehat{-x - 7}$.
   - S este *independent*: să presupunem că există două clase de echivalență $\hat{x}, \hat{y} \in S$ astfel încât $\hat{x} = \hat{y}$ cu $x \neq y$. Singura posibilitate este ca $x = -y - 7$ (sau viceversa). Dar $y > 3.5$, deci $-y - 7 < -3.5$.

□

Exercițiul 8. Demonstrați că pentru orice partiție P a unei mulțimi A există o unică relație de echivalență ρ astfel încât $\frac{A}{\rho} = P$.

Demonstrație. Fie P o partiție a mulțimii A.

Definim relația ρ în felul următor: $a \rho b \iff \exists U \in P$ astfel încât $a, b \in U$ (adică a, b se află în aceeași mulțime în partiție). Se poate arăta ușor că această relație este de echivalență:

- *reflexivă*: fie $x \in A$. Deoarece P este o partiție, trebuie să existe o submulțime U în care apare x. Deci putem spune că $x, x \in U$, deci $x \rho x$.
- *simetrică*: fie $x, y \in A$ astfel încât $x \rho y$. Din definiția lui ρ avem că $x, y \in U$. Atunci și $y, x \in U$. Deci $y \rho x$.
- *tranzitivă*: fie $x, y, z \in A$ astfel încât $x \rho y$ și $y \rho z$. Deci $x, y \in U$ și $y, z \in V$. Avem că $U \cap V = \{ y \}$. P fiind partiție, trebuie ca $U = V$. Deci $x, z \in U \iff x \rho z$.

Trebuie să mai arătăm că $\frac{A}{\rho} = P$. Avem că

$$\begin{aligned}\frac{A}{\rho} &= \{ \{ y \in A \mid x \rho y \} \mid x \in A \} \\ &= \{ \{ y \in A \mid y \in U \} \mid U \in P \} \\ &= \{ U \in P \} = P\end{aligned}$$

Pentru unicitate: să presupunem că ar exista o altă relație ρ', diferită de ρ, astfel încât $\frac{A}{\rho} = \frac{A}{\rho'} = P$. Dacă relațiile diferă, trebuie să existe cel puțin o pereche (x, y) astfel încât $(x, y) \in \rho$ și $(x, y) \notin \rho'$ (sau vice versa). Dar asta ar însemna că x și y se află în aceeași mulțime în $\frac{A}{\rho}$ și în mulțimi diferite în $\frac{A}{\rho'}$. Însă asta înseamnă că ρ și ρ' definesc partiții diferite. □

Link-uri utile

- Grup tutoriat
- Cursurile de la Băețica
- Cursurile de anul acesta de la Mincu
- Cursurile de an trecut de la Mincu

Exerciții

Exercițiul 1. Fie $x \in \mathbb{Z}$. Notăm cu $\hat{a} \in \mathbb{Z}_3$ clasa de resturi modulo 3 corespunzătoare lui a. Fie corespondența $x \mapsto \widehat{x+1}$. Demonstrați că această corespondență definește o funcție.

Demonstrație. Pentru a fi funcție, corespondența trebuie să atribuie fiecărui x un singur rezultat, și să fie definită pentru orice $x \in \mathbb{Z}$.

Definim $f : \mathbb{Z} \to \mathbb{Z}_3$, $f(x) = \widehat{x+1}$. Pentru fiecare x, obținem o clasă de resturi. De asemenea, expresia $\widehat{x+1}$ este definită pentru orice număr întreg. □

Exercițiul 2. Fie $f : \mathbb{Z}_3 \to \mathbb{Z}$, $f(\hat{x}) = 3x + 2$. Demonstrați că această funcție nu este bine definită.

Demonstrație. Să calculăm funcția pentru un x anume:

$$f(\hat{1}) = 3 \cdot 1 + 2 = 5$$

Să calculăm funcția pentru un alt reprezentant din aceeași clasă de resturi:

$$f(\hat{7}) = 3 \cdot 7 + 2 = 23$$

Observăm că $\hat{1} = \hat{7}$, dar $f(\hat{1}) \neq f(\hat{7})$.

Valoarea expresiei depinde de ce reprezentant alegem pentru clasa de resturi. □

Exercițiul 3. Fie $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$. Această funcție nu este nici injectivă, nici surjectivă.

Propuneți o modificare (care ar putea fi aplicată pentru orice funcție) pentru ca aceasta să devină surjectivă, respectiv injectivă.

Demonstrație. Pentru surjectivitate, putem întotdeauna să **restrângem codomeniul** funcției la imaginea ei. Definim deci $f' : \mathbb{R} \to [0, +\infty)$, unde $f'(x) = x^2$.

Pentru injectivitate, am putea alege să **restrângem domeniul**, dar apar două probleme:

- în acest caz este ușor să determinăm la ce să restrângem domeniul, dar pe cazul general nu e clar cum am putea alege submulțimea pe care funcția ar fi injectivă
- vrem să putem cumva să continuăm să calculăm funcția pentru toate valorile din domeniul inițial

Putem rezolva ambele probleme prin *mulțimi factor*. Ne vom folosi de relația de echivalență asociată unei funcții.

Reamintim că relația ρ_f este definită ca

$$x \,\rho_f\, y \iff f(x) = f(y)$$

Pentru funcția noastră:

$$x \,\rho_f\, y \iff x^2 = y^2 \iff |x| = |y|$$

Să vedem care sunt clasele de echivalență pentru ρ_f:

$$\begin{aligned}
\mathbb{R}/\rho_f &= \left\{ \left\{ y \in \mathbb{R} \;\middle|\; x \,\rho_f\, y \right\} \;\middle|\; x \in \mathbb{R} \right\} \\
&= \{\, \{\, y \in \mathbb{R} \mid |x| = |y| \,\} \mid x \in \mathbb{R} \,\} \\
&= \{\, \{\, x, -x \,\} \mid x \in \mathbb{R} \,\} \\
&= \{\, \hat{x} \mid x \in [0, \infty) \,\}
\end{aligned}$$

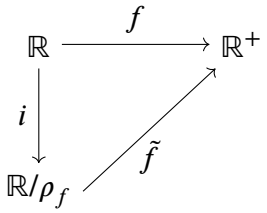
unde cu $\hat{x}$ am notat $\{ x, -x \}$.

Vom defini funcția $\tilde{f} : \mathbb{R}/\rho_f \to \mathbb{R}$, $\tilde{f}(\hat{x}) = x^2$. Fiind o funcție de la o mulțime factor la o mulțime obișnuită (adică o funcție în care „dăm jos căciula" lui x) ne punem problema dacă este bine-definită.

Pentru a demonstra asta mai ușor acest lucru ne putem folosi de *proprietatea de universalitate a mulțimii factor*.

Introducem acum și funcția numită *injecția canonică*, $i : \mathbb{R} \to \mathbb{R}/\rho_f$, unde $i(x) = \hat{x}$ (intuitiv, i îi „pune căciula" lui x). Pe cazul general, i e o funcție de la o mulțime la o mulțime factor obținută de la mulțimea inițială, care duce un element în clasa de echivalență corespunzătoare.

Putem rescrie f în funcție de celelalte funcții ca $f = \tilde{f} \circ i$.



Relația dintre funcțiile construite

Proprietatea de universalitate ne garantează că în acest caz $\tilde{f}$ este corect definită. □

Exercițiul 4. Fie M o mulțime și $\cdot$ o lege de compoziție binară astfel încât $(M, \cdot)$ este monoid. Notăm cu e elementul neutru al acestui monoid.

Demonstrați că $(M, \odot)$ este tot monoid, unde am definit $x \odot y = y \cdot x$.

Demonstrație. Trebuie să arătăm că legea de compoziție „$\odot$":

- este *asociativă*:

$$\begin{aligned}
(x \odot y) \odot z = x \odot (y \odot z) &\iff \\
(y \cdot x) \odot z = x \odot (z \cdot y) &\iff \\
z \cdot (y \cdot x) = (z \cdot y) \cdot x &
\end{aligned}$$

  Ultima egalitate este adevărată deoarece „$\cdot$" este asociativă.

- admite *element neutru*, care este chiar elementul neutru pentru „$\cdot$”:

$$x \bigodot e = e \bigodot x = x \iff e \cdot x = x \cdot e = x$$

□

Exercițiul 5. Fie $(M, \cdot)$ un monoid. Notăm cu $U(M)$ mulțimea *unităților* lui M, adică mulțimea elementelor inversabile în raport cu $\cdot$ din M.

Demonstrați că $(U(M), \cdot)$ formează un grup.

Demonstrație. Arătăm mai întâi că $(U(M), \cdot)$ este parte stabilă în raport cu „$\cdot$”.

Fie $x, y \in U(M)$. Vrem să arătăm că și $xy \in U(M)$, deci că este inversabil.

Inversul lui xy este $y^{-1}x^{-1}$:

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xx^{-1} = e$$
$$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}y = e$$

Observăm că $y^{-1}x^{-1}$ aparține lui $U(M)$ (inversul este xy).

Din faptul că este parte stabilă rezultă că $(U(M), \cdot)$ este monoid.

De asemenea, toate elementele din $U(M)$ sunt inversabile, din definiția acestei submulțimi.

Deci $(U(M), \cdot)$ formează un grup. □

Exercițiul 6. Fie un număr întreg $n > 1$. Lucrăm cu monoidul $(\mathbb{Z}_n, \cdot)$. Fie $0 \leq a < n$.

Demonstrați că a este inversabil în $\mathbb{Z}_n$ dacă și numai dacă $(a, n) = 1$.

Demonstrație. Implicația „ $\Longrightarrow$ ”: Plecăm de la faptul că $\hat{a} \in \mathbb{Z}_n$ este inversabil. Deci există $\hat{b}$ pentru care

$$\hat{a}\hat{b} = \hat{1}$$

Înlocuind clasele de resturi cu reprezentanți în egalitate. Pentru $p, q, k \in \mathbb{Z}$ avem că:

$$\begin{aligned} (pn + a)(qn + b) &= kn + 1 \\ pqn^2 + qna + pnb + ab - kn &= 1 \\ ab + (pqn + q + p - k)n &= 1 \\ ab + k'n &= 1 \qquad \text{(notăm coeficientul lui } n \text{ cu } k') \end{aligned}$$

Notăm cu $d \in \mathbb{Z}$ c.m.m.d.c.-ul lui a și n. Deoarece d divide și pe a și pe n, avem că $d \mid ab + k'n$. Deci d divide și pe 1. Dar asta înseamnă că $d = 1$.

Implicația „ $\Longleftarrow$ ”: Știm din ipoteză că $(a, n) = 1$. Ne folosim de identitatea lui Bézout, care ne spune că există $p, q \in \mathbb{Z}$ astfel încât

$$pa + qn = (a, n) = 1$$

Trecând totul la clase de resturi modulo n obținem că:

$$\begin{aligned} \widehat{pa + qn} = \hat{1} &\iff \widehat{pa} + \widehat{qn} = \hat{1} \\ &\iff \hat{p}\hat{a} + \hat{q}\hat{n} = \hat{1} \iff \hat{p}\hat{a} + \hat{q}\hat{0} = \hat{1} \\ &\iff \hat{p}\hat{a} = \hat{1} \end{aligned}$$

Din ultima egalitate rezultă că $\hat{p}$ din identitatea lui Bézout este inversul lui $\hat{a}$.

Importanța teoretică a acestui rezultat este că avem un mod de a găsi inverse modulare folosind algoritmul lui Euclid extins (care ne ajută să calculăm p, q din identitatea lui Bézout). □

Exercițiul 7. Fie $(G, \cdot)$ un grup în care $(ab)^2 = a^2b^2$, $\forall a, b \in G$.

Demonstrați că $(G, \cdot)$ este abelian (comutativ).

Demonstrație. Un grup este comutativ dacă $ab = ba, \forall a, b \in G$.

Plecând de la relație, și folosindu-ne de faptul că toate elementele dintr-un grup sunt inversabile, obținem echivalențele:

$$\begin{aligned} (ab)^2 = a^2b^2 &\iff \\ abab = aabb &\iff \\ (a^{-1}a)ba(bb^{-1}) = (a^{-1}a)ab(bb^{-1}) &\iff \\ ba = ab & \end{aligned}$$

□

Exercițiul 8. Fie $(\mathbb{Z}, +)$ grupul numerelor întregi cu adunarea. Arătați că toate subgrupurile acestuia sunt de forma $n\mathbb{Z}$ pentru un $n \in \mathbb{Z}$, adică multiplii de n.

Demonstrație. Un **subgrup** al unui grup $(G, \cdot)$ este

- o **submulțime** H a lui G
- la rândul ei **grup**, în raport cu aceeași operație

În mod echivalent, un subgrup este o submulțime care:

- este **parte stabilă** în raport cu operația „$\cdot$”: dacă $a, b \in H$, atunci $a \cdot b \in H$
- conține **elementul neutru** al lui G
- pentru orice element x din H, și **inversul** x^{-1} este în H

Observăm că $n\mathbb{Z} = \{ kn \mid k \in \mathbb{Z} \}$ formează un subgrup.

Fie H un subgrup al lui $n\mathbb{Z}$. Lucrând pe cazul general, nu știm ce elemente conține.

Fiind subgrup, cu siguranță conține elementul neutru 0. Dacă îl conține doar pe 0, atunci $H = \{ 0 \} = 0\mathbb{Z}$. Dacă nu, observăm că trebuie să conțină cel puțin un număr pozitiv și un număr negativ (dacă îl conține pe x îl conține și pe inversul său la adunare $-x$).

Îl notăm cu a pe cel mai mic număr din H care este strict pozitiv. Deoarece H este subgrup, trebuie să îl conțină și pe $a + a$, $a + a + a$, ..., adică $ka, \forall k \in \mathbb{Z}$.

Să presupunem că mai există un $b \in H, b > 0$, care nu este multiplu de a. Deoarece a este cel mai mic număr strict pozitiv din H, avem că $b > a$. Putem împărți cu rest pe b la a. Atunci relația din teorema împărțirii cu rest se scrie ca

$$b = p \cdot a + r$$

Deoarece r este restul la împărțire, avem că $0 \leq r < a$.

Putem rescrie formula ca

$$r = b - p \cdot a$$

Am plecat de la faptul că $b \in H$, $p \cdot a$ este multiplu de a deci este în H, și deoarece un subgrup este parte stabilă avem că și $r \in H$.

Deci avem în H un număr strict pozitiv r care este mai mic decât a. Asta contrazice presupunerea că a ar fi cel mai mic număr din H. Deci b nu poate să fie în H; toate elementele din H trebuie să fie multiplii de a. □

Link-uri utile

- Grup tutoriat
- Cursurile de la Băețica
- Cursurile de anul acesta de la Mincu
- Cursurile de an trecut de la Mincu

Exerciții

Exercițiul 1. Demonstrați că grupurile $\mathbb{Z}$ și $\mathbb{Z}_6$ sunt ciclice.

Demonstrație. Un grup este ciclic dacă poate fi generat de un singur element.

- Pentru $\mathbb{Z}$, 1 generează toată mulțimea. Putem obține orice număr pozitiv k ca $k = 1 + \cdots + 1$, orice număr negativ este opusul unui număr pozitiv, iar $0 = 1 + (-1)$.
- Pentru $\mathbb{Z}_6$, $\hat{1}$ este un generator:

$$\begin{aligned}\hat{1} + \hat{1} &= \hat{2}\\ \hat{2} + \hat{1} &= \hat{3}\\ \hat{3} + \hat{1} &= \hat{4}\\ \hat{4} + \hat{1} &= \hat{5}\\ \hat{5} + \hat{1} &= \hat{6} = \hat{0}\end{aligned}$$

□

Exercițiul 2. Demonstrați că grupul $\mathbb{Q}$ nu este ciclic.

Demonstrație. Demonstrăm prin reducere la absurd. Presupunem că $\mathbb{Q}$ ar fi ciclic. Fie $a \in \mathbb{Q}$ un generator al său. Scriem a sub formă de fracție rațională ireductibilă: $a = \frac{p}{q}$, cu $p, q \in \mathbb{Z}^*$.

Observăm că fracția $\frac{p}{q+1}$ nu poate fi obținută din $\frac{p}{q}$. Oricum am aduna sau scădea fracțiile care sunt multiplu de $\frac{p}{q}$, nu putem ajunge la o fracție cu numitor mai mare. □

Exercițiul 3. Determinați dacă grupurile $\mathbb{Z}_{28} \times \mathbb{Z}_{29}$, $\mathbb{Z}_{28} \times \mathbb{Z}_{30}$, respectiv $\mathbb{R}$ sunt sau nu ciclice.

Demonstrație. Pentru a simplifica demonstrațiile în problemele în care apar $\mathbb{Z}_n \times \mathbb{Z}_m$, ne folosim de o teoremă care ne spune că $\mathbb{Z}_n \times \mathbb{Z}_m$ este izomorf cu $\mathbb{Z}_{n \times m}$ dacă și numai dacă n este prim față de m. În acest fel, se poate arăta că $\mathbb{Z}n \times m$ este ciclic dacă și numai dacă $(n, m) = 1$.

- Pentru $\mathbb{Z}_{28} \times \mathbb{Z}_{29}$, avem că 28 este prim față de 29.
- Pentru $\mathbb{Z}_{28} \times \mathbb{Z}_{30}$, numerele nu sunt prime între ele, deci grupul nu este izomorf cu $\mathbb{Z}_{28 \times 29}$.

- Să presupunem că $\mathbb{R}$ ar fi ciclic, și $a \in \mathbb{R}$ ar fi un generator. Elementul a poate genera doar multiplii de a. Asta înseamnă că toate numerele din $\mathbb{R}$ sunt de forma na, pentru un $n \in \mathbb{Z}$. Dar $\mathbb{R}$ este o mulțime infinită nenumărabilă, deci trebuie să mai existe elemente care nu sunt generate de a.

În fine, teorema de structură a grupurilor ciclice ne spune că orice grup ciclic este izomorf cu $\mathbb{Z}_n$ (dacă este finit), respectiv $\mathbb{Z}$ dacă este infinit. Deci în general la un astfel de exercițiu putem arăta că un grup este/nu este izomorf cu unul dintre grupurile $\mathbb{Z}_n$ sau $\mathbb{Z}$. □

Exercițiul 4. Pe mulțimea $[-3, 1)$ definim relația de echivalență $a \rho b \iff a^4 = b^4$.

Determinați clasa de echivalență a elementului $\frac{\sqrt{2}}{2}$ și scrieți un sistem complet și independent de reprezentanți ai elementelor lui $[-3, 1)$ în raport cu ρ.

Demonstrație. Pentru a determina clasa de echivalență a lui $\frac{\sqrt{2}}{2}$, trebuie să găsim toate elementele din $[-3, 1)$ care sunt în relație cu el:

$$\begin{aligned} & x \rho \frac{\sqrt{2}}{2} \\ \iff & x^4 = \left(\frac{\sqrt{2}}{2}\right)^4 \\ \iff & x^4 = \frac{1}{4} \end{aligned}$$

Singurele soluții ale acestei ecuații în $[-3, 1)$ sunt $\pm\frac{\sqrt{2}}{2}$. Deci

$$\widehat{\frac{\sqrt{2}}{2}} = \left\{ \frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2} \right\}$$

Pe cazul mai general, observăm că pentru $x \in (-1, 1)$:

$$\hat{x} = \{ x, -x \}, \forall x \in (-1, 1)$$

Dacă $x \in [-3, -1]$, atunci x este singur în clasa sa de echivalență (pentru că $-x$ ar fi în afara mulțimii):

$$\hat{x} = \{ x \}, \forall x \in [-3, -1]$$

Când vine vorba de ales un sistem de reprezentanți, nu putem alege toată mulțimea, deoarece de exemplu $\widehat{-0.5} = \widehat{0.5}$, deci sistemul nu ar fi independent. Așa că alegem ca sistem de reprezentanți pe $S = [-3, 0]$.

Justificăm că S este

- *complet*: Fie $x \in [-3, 1)$. Dacă $x \leq 0$, atunci x este reprezentat de $\hat{x}$. Dacă $x > 0$, x este reprezentant de $\widehat{-x}$.

- *independent*: Dacă alegem un element $x \leq -1$, atunci acesta se află singur în clasa lui, deci aceste clase de echivalență sunt independente. Dacă luăm $x \neq y \in (-1, 0]$, este imposibil ca $\hat{x} = \hat{y}$, deoarece în clasa lui $\hat{x}$ se află doar el și $-x$ care este în $(0, 1)$ (deci diferit sigur de y).

O altă soluție ar fi fost să alegem ca sistem de reprezentanți $[-3,-1] \cup [0,1)$. □

Exercițiul 5. Fie permutarea

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 3 & 12 & 13 & 2 & 7 & 9 & 5 & 6 & 8 & 4 & 11 & 10 & 1 \end{pmatrix}$$

- Descompuneți τ în produs de ciclii disjuncți și în produs de transpoziții.
- Determinați τ^2, τ^{-1}, $\epsilon(\tau)$, $\text{ord}(\tau)$ și τ^{2010}.

Demonstrație.

- Luăm fiecare element de la 1 la 13 și încercăm să scriem ciclul în care se află (de exemplu, 1 merge în 3, care merge în 13, care se întoarce în 1, ș.a.m.d.):

  $$\tau = (1,3,13)(2,12,10,4)(5,7)(6,9,8)$$

  Observați că nu am mai scris ciclul de lungime 1 format de 11, pentru că nu afectează rezultatul.

  Pentru transpoziții, rupem fiecare ciclu în perechi de elemente consecutive:

  $$\tau = (1,3)(3,13)(2,12)(12,10)(10,4)(5,7)(6,9)(9,8)$$

- Când ridicăm la puterea k, luăm fiecare ciclu și numărăm din k în k. Ciclii ale căror lungimi au factori în comun cu k se rup în mai multe bucăți. Ciclii ale căror lungimi sunt egale cu sau divid puterea dispar.

  În cazul nostru, ciclul de lungime 4 s-a rupt în doi cicli de lungime 2.

  $$\tau^2 = (1,13,3)(2,10)(12,4)(6,8,9)$$

  Pentru a calcula inversa, putem să ne uităm pe permutare și să luăm elementele de jos în sus și să le reordonăm. Însă mult mai simplu este să ne folosim de descompunerea în cicli și să scriem fiecare ciclu invers.

  $$\tau^{-1} = (13,3,1)(4,10,12,2)(7,5)(8,9,6)$$

  Semnul permutării este fie $+1$ (pentru permutări pare) fie -1 (pentru permutări impare). Îl putem determina în funcție de numărul de transpoziții (paritatea permutării este aceeași cu paritatea numărului de transpoziții în care se descompune).

  $$\epsilon(\tau) = (-1)^8 = 1$$

  Ordinul unei permutări τ este cel mai mic număr $k \in \mathbb{N}^*$ pentru care $\tau^k = e$. Ordinul unui ciclu (care este tot o permutare) este egal cu lungimea ciclului. Ordinul unei permutări este egal cu c.m.m.m.c.-ul lungimilor ciclilor.

  În cazul nostru,

  $$\text{ord}(\tau) = [3,4,2,3] = 12$$

  Pentru a determina τ^{2010} ne folosim de faptul că

  $$\tau^{2010} = (\tau^{12})^{167} \cdot \tau^6 = \tau^6$$

  Putem calcula τ^6 pe ciclii:

  $$\tau^6 = (2,10)(12,4)$$

□

Exercițiul 6. Fie permutarea

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 7 & 4 & 5 & 6 & 1 & 8 & 3 & 10 & 12 & 2 & 13 & 9 & 11 \end{pmatrix}$$

- Descompuneți τ în produs de ciclii disjuncți, în produs de transpoziții.
- Determinați τ^{-2}, $\epsilon(\tau)$, și $\text{ord}(\tau)$.
- Rezolvați în S_{13} ecuația
$$x^{20} = \tau$$

Demonstrație.

- Produs de ciclii disjuncți:
$$\tau = (1, 7, 3, 5)(2, 4, 6, 8, 10)(9, 12)(11, 13)$$
Produs de transpoziții:
$$\tau = (1, 7)(7, 3)(3, 5)(2, 4)(4, 6)(6, 8)(8, 10)(9, 12)(11, 13)$$
- Calculăm utilizând aceleași metode ca la exercițiul precedent:
$$\begin{aligned} \tau^{-2} &= (\tau^2)^{-1} \\ &= ((1, 3)(7, 5)(2, 6, 10, 4, 8))^{-1} \\ &= (3, 1)(5, 7)(8, 4, 10, 6, 2) \\ \epsilon(\tau) &= (-1)^9 = -1 \\ \text{ord}(\tau) &= [4, 5, 2, 2] = 20 \end{aligned}$$
- Dacă ne uităm la semne, observăm că $\epsilon(\tau)$ este -1 (τ este impară), dar în stânga, semnul lui x^{20} este $+1$, fiind o putere pară. Deci ecuația nu are soluții.

  În cazul în care ecuația ar avea soluții, trebuie să luăm o permutare oarecare din S_{13} și să potrivim indicii pentru a rezolva ecuația.

□

Link-uri utile

- Grup tutoriat
- Cursurile de la Băețica
- Cursurile de anul acesta de la Mincu
- Cursurile de an trecut de la Mincu

Exerciții

Exercițiul 1. Demonstrați că următoarele grupuri (cu adunarea) nu sunt izomorfe:

- $\mathbb{Z}_2 \times \mathbb{Z}_2$ și $\mathbb{Z}_4$.
- $\mathbb{Z}$ și $\mathbb{Q}$
- $\mathbb{Q}$ și $\mathbb{R}$

Demonstrație. Pentru a demonstra că două grupuri nu sunt izomorfe, putem folosi procedeul reducerii la absurd. Presupunem că ar exista un izomorfism f și ajungem la o contradicție.

- În unele cazuri ne putem gândi la ordinele elementelor. Reamintim că ordinul elementului x este cel mai mic număr natural nenul k pentru care $\underbrace{x + \cdots + x}_{k \text{ ori}} = 0$.

  Un izomorfism păstrează ordinul unui element: $f(\underbrace{x + \cdots + x}_{k \text{ ori}}) = \underbrace{f(x) + \cdots + f(x)}_{k \text{ ori}}$.

  - În $\mathbb{Z}_2 \times \mathbb{Z}_2$ toate elementele au ordin cel mult 2.
  - În $\mathbb{Z}_4$ avem și un element de ordin 4 (și anume $\hat{1}$). Pentru elementul de ordin 4 nu am avea corespondent.

- O altă proprietate care trebuie păstrată de izomorfisme este cea de a fi grup ciclic. $\mathbb{Z}$ este un grup ciclic, în timp ce $\mathbb{Q}$ nu este (am demonstrat acest lucru în tutoriatul anterior).

- Dacă ar exista un izomorfism f, acesta ar fi funcție bijectivă. Asta ar însemna că $\mathbb{Q}$ și $\mathbb{R}$ ar avea același cardinal. Dar $\mathbb{Q}$ este mulțime numărabilă, iar $\mathbb{R}$ este nenumărabilă.

□

Exercițiul 2. Fie $f : \mathbb{Q} \to \mathbb{C}^*$, definită prin

$$f(\frac{m}{n}) = \cos 2\pi\frac{m}{n} + i \sin 2\pi\frac{m}{n}$$

și notăm cu U mulțimea $U = \left\{ z \in \mathbb{C}^* \;\middle|\; \exists n \in \mathbb{N}^*, z^n = 1 \right\}$

1. Arătați că f este morfism de grupuri.
2. Determinați $\ker f$ și $\operatorname{im} f$.
3. Arătați că $\mathbb{Q}/\mathbb{Z} \cong U$.

Demonstrație. Facem observația că în acest caz, grupurile sunt $\mathbb{Q}$ cu adunarea (elementul neutru este 0) și $\mathbb{C}$ cu înmulțirea (elementul neutru este 1).

De asemenea, dacă luăm formula din definiția lui U și aplicăm modulul obținem:

$$\begin{aligned} & z^n = 1 \\ \implies & |z^n| = 1 \\ \implies & |z|^n = 1 \\ \implies & |z| = 1 \end{aligned}$$

Deci U este mulțimea punctelor aflate la distanță 1 de origine, sau cu alte cuvinte este cercul de centru 0 și rază 1.

1. Condiția ca f să fie morfism este ca

$$\begin{gathered} f(x+y) = f(x) \cdot f(y) \iff \\ \cos 2\pi(x+y) + i \sin 2\pi(x+y) = (\cos 2\pi x + i \sin 2\pi x) \cdot (\cos 2\pi y + i \sin 2\pi y) \end{gathered}$$

   Ultima egalitate este adevărată din formulele lui de Moivre.

2. Ne bazăm pe definițiile acestor mulțimi:

$$\begin{aligned} \ker f &= \{\, x \in \mathbb{Q} \mid f(x) = 1 \,\} \\ &= \{\, x \in \mathbb{Q} \mid \cos 2\pi x + i \sin 2\pi x = 1 \,\} \\ &= \{\, x \in \mathbb{Q} \mid x \in \mathbb{Z} \,\} = \mathbb{Z} \end{aligned}$$

$$\begin{aligned} \operatorname{im} f &= \left\{ y \in \mathbb{C}^* \;\middle|\; \exists x \in \mathbb{Q}, f(x) = y \right\} \\ &= \left\{ y \in \mathbb{C}^* \;\middle|\; \exists x \in \mathbb{Q}, \cos 2\pi x + i \sin 2\pi x = y \right\} \\ &= \left\{ y \in \mathbb{C}^* \;\middle|\; |y| = 1 \right\} = U \end{aligned}$$

3. Putem demonstra că grupul factor $\frac{\mathbb{Q}}{\mathbb{Z}}$ este izomorf cu U foarte ușor folosindu-ne de **teorema fundamentală de izomorfism**.

   Pe cazul general, teorema spune că, dacă $f : G \to H$ este un morfism de grupuri, avem că

$$\frac{G}{\ker f} \cong \operatorname{im} f$$

   Aplicând teorema pe cazul nostru avem că:

$$\frac{\mathbb{Q}}{\mathbb{Z}} \cong U$$

□

Exercițiul 3. Scrieți subgrupurile lui $\mathbb{Z}_{12}$ și grupurile factor ale lui $\mathbb{Z}_{12}$.

Demonstrație. Putem găsi subgrupurile lui $\mathbb{Z}_{12}$ generând subgrupul corespunzător fiecărui element:

$$\begin{aligned}
\langle \hat{0} \rangle &= \{ \hat{0} \} \\
\langle \hat{1} \rangle &= \left\{ \hat{0}, \hat{1}, \ldots, \widehat{11} \right\} \\
&= \langle \hat{5} \rangle = \langle \hat{7} \rangle = \widehat{\langle 11 \rangle} \\
\langle \hat{2} \rangle &= \left\{ \hat{0}, \hat{2}, \hat{4}, \ldots, \widehat{10} \right\} = \left\langle \widehat{10} \right\rangle \\
\langle \hat{3} \rangle &= \{ \hat{0}, \hat{3}, \ldots, \hat{9} \} = \langle \hat{9} \rangle \\
\langle \hat{4} \rangle &= \{ \hat{0}, \hat{4}, \hat{8} \} = \langle \hat{8} \rangle \\
\langle \hat{6} \rangle &= \{ \hat{0}, \hat{6} \}
\end{aligned}$$

Nu mai există alte subgrupuri în afară de acestea. Dacă luăm două numere $\hat{a}, \hat{b}$ și încercăm să vedem ce subgrup generează, fie au un factor în comun și generează subgrupul generat de c.m.m.d.c.-ul lor $\langle \hat{a}, \hat{b} \rangle = \left\langle \widehat{(a, b)} \right\rangle$.

În ceea ce privește grupurile factor, să luăm de exemplu subgrupul normal $H = \{ \hat{0}, \hat{6} \}$. Atunci avem

$$\frac{\mathbb{Z}_{12}}{H} = \left\{ \left\{ \hat{y} \in \mathbb{Z}_{12} \;\middle|\; \hat{x} - \hat{y} \in \mathbb{Z}_{12} \right\} \;\middle|\; \hat{x} \in \mathbb{Z}_{12} \right\}$$

Pentru a determina clasele de echivalență din grupul factor, ne folosim de definiția că două clase de resturi $\hat{x}, \hat{y}$ sunt echivalente dacă $\hat{x} - \hat{y} \in \{ \hat{0}, \hat{6} \}$.

Obținem clasele de echivalență:

$$\begin{aligned}
\hat{0} + H &= \{ \hat{0}, \hat{6} \} \\
\hat{1} + H &= \{ \hat{1}, \hat{7} \} \\
&\ldots \\
\hat{5} + H &= \left\{ \hat{5}, \widehat{11} \right\}
\end{aligned}$$

Adunarea pe aceste șase clase de echivalență funcționează ca în $\mathbb{Z}_6$. Dacă notăm cu $\overline{x} = \hat{x} + H$ avem, de exemplu:

$$\begin{aligned}
\overline{1} + \overline{3} &= \overline{4} \\
\overline{5} + \overline{4} &= \overline{3} \\
&\ldots
\end{aligned}$$

De fapt, un rezultat mai general ne spune că, pentru orice $n \in \mathbb{Z}^*$ și pentru orice d divizor al lui n, avem:

$$\frac{\mathbb{Z}_n}{d\mathbb{Z}_n} \cong \mathbb{Z}_d$$

□

Exercițiul 4. Fie G grupul factor $(\mathbb{Q}, +)/\mathbb{Z}$. Arătați că:

1. dacă $a, b \in \mathbb{N}^*$ sunt prime între ele, atunci $\operatorname{ord}\left(\widehat{\frac{a}{b}}\right) = b$
2. orice subgrup finit generat este ciclic
3. G nu este finit generat

Demonstrație. Să încercăm mai întâi să înțelegem din ce este format grupul factor $\frac{\mathbb{Q}}{\mathbb{Z}}$. În primul rând, observăm că toate numerele întregi se află în clasa lui 0, deoarece

$$\hat{0} = \{\, x \in \mathbb{Q} \mid x - 0 \in \mathbb{Z} \,\} \iff \hat{0} = \mathbb{Z}$$

1. Observăm că dacă adunăm o fracție $\widehat{\frac{a}{b}}$ cu ea însăși de b ori, obținem un număr întreg, care este în $\hat{0}$:
$$\underbrace{\widehat{\frac{a}{b}} + \cdots + \widehat{\frac{a}{b}}}_{b \text{ ori}} = \widehat{b \cdot \frac{a}{b}} = \hat{a} = \hat{0}$$
Pentru a justifica că b este chiar ordinul lui $\widehat{\frac{a}{b}}$, trebuie să arătăm că nu poate exista un $c < b, c \in \mathbb{N}^*$ pentru care $\widehat{c\frac{a}{b}} = \hat{0}$. Ca să se întâmple așa ceva, ar trebui ca $b \mid c \cdot a$. Însă știm că $(a, b) = 1$ și că $c < b$, ajungem la o contradicție.

2. Fie un subgrup $H \leq G$ care este generat de $\widehat{\frac{a_1}{b_1}}, \ldots, \widehat{\frac{a_n}{b_n}}$. Orice element din H se obține ca o combinație liniară dintre acești generatori:
$$\forall x \in H, x = k_1 \widehat{\frac{a_1}{b_1}} + \cdots + k_n \widehat{\frac{a_n}{b_n}}$$
Să zicem că q ar fi numitorul comun al $\widehat{\frac{a_1}{b_1}}, \ldots, \widehat{\frac{a_n}{b_n}}$. Atunci putem rescrie relația de mai sus ca
$$\begin{aligned} x &= k_1' \widehat{\frac{1}{q}} + \cdots + k_n' \widehat{\frac{1}{q}} \\ &= (k_1' + \cdots + k_n') \widehat{\frac{1}{q}} \end{aligned}$$
Deci H este ciclic, fiind generat de un singur element, $\widehat{\frac{1}{q}}$.

3. Presupunem că ar exista un sistem de generatori finit pentru $G = \left\langle \widehat{\frac{a_1}{b_1}}, \ldots \widehat{\frac{a_n}{b_n}} \right\rangle$. Analog cu ce am făcut la subpunctul anterior, am ajunge la concluzia că acest sistem de generatori poate fi înlocuit de un singur $\widehat{\frac{1}{q}}$. Dar nu avem cum să generăm, de exemplu, fracția $\widehat{\frac{1}{q+1}}$.

□

Link-uri utile

- Grup tutoriat
- Cursurile de la Băețica
- Cursurile de anul acesta de la Mincu
- Cursurile de an trecut de la Mincu

Exerciții

Exercițiul 1. Determinați toate morfismele de monoizi de la $(\mathbb{N}, +)$ la $(\mathbb{N}, \max)$.

Demonstrație. Fie $f : \mathbb{N} \to \mathbb{N}$ un morfism. Atunci f are proprietatea că $f(0) = 0$ și $f(a+b) = \max(f(a), f(b))$.

Putem scrie $f(2)$ ca

$$f(2) = f(1+1) = \max(f(1), f(1)) = \max(f(1)) = f(1)$$

Notând $f(1) = a \in \mathbb{N}$, ajungem la concluzia că

$$\begin{aligned} f(0) &= 0 \\ f(n) &= \max(\underbrace{f(1), \dots, f(1)}_{n \text{ ori}}) = f(1) = a \end{aligned}$$

Deci toate morfismele sunt de forma

$$f(x) = \begin{cases} 0, & \text{dacă } x = 0 \\ a, & \text{altfel} \end{cases}$$

pentru un $a \in \mathbb{N}$. □

Exercițiul 2. Determinați $\boldsymbol{Hom}(\mathbb{Z}_8, \mathbb{Q})$, adică mulțimea morfismelor de la $(\mathbb{Z}_8, +)$ la $(\mathbb{Q}, +)$.

Demonstrație. Fie $f : \mathbb{Z}_8 \to \mathbb{Q}$ un morfism de grupuri. Din proprietățile morfismelor, știm că

$$\begin{aligned} f(\hat{0}) &= 0 \\ f(\hat{a} + \hat{b}) &= f(\hat{a}) + f(\hat{b}) \end{aligned}$$

Să luăm de exemplu $f(\hat{3})$. Acesta poate fi scris ca

$$f(\hat{3}) = f(\hat{1} + \hat{1} + \hat{1}) = f(\hat{1}) + f(\hat{1}) + f(\hat{1}) = 3f(\hat{1})$$

Pe același principiu, pentru orice $\hat{k} \in \mathbb{Z}_8$ avem că

$$f(\hat{k}) = kf(\hat{1})$$

Să luăm acum două clase din $\mathbb{Z}_8$ care adunate dau $\hat{0}$, cum ar fi $\hat{3}$ și $\hat{5}$:

$$\begin{aligned} f(\hat{3} + \hat{5}) &= f(\hat{0}) = 0 \\ f(\hat{3} + \hat{5}) &= 3f(\hat{1}) + 5f(\hat{1}) = 8f(\hat{1}) \end{aligned}$$

Deci $8f(\hat{1}) = 0$. De aici obținem că $f(\hat{1}) = 0$, și de fapt că $f(\hat{k}) = 0$, $\forall \hat{k} \in \mathbb{Z}_8$.

Singurul morfism de la $\mathbb{Z}_8$ la $\mathbb{Q}$ este morfismul nul. □

Model de examen rezolvat

Subiectul 1

Considerăm grupul diedral $\mathrm{D}_5 = \left\{ 1, \rho, \rho^2, \rho^3, \rho^4, \sigma, \rho\sigma, \rho^2\sigma, \rho^3\sigma, \rho^4\sigma \right\}$. Se știe că în el au loc relațiile $\rho^5 = 1$, $\sigma^2 = 1$, $\sigma\rho = \rho^4\sigma$.

Grupul diedral de ordin n se referă la simetriile unui poligon regulat cu n laturi. În acest caz, D_5 se referă la simetriile unui pentagon regulat. ρ reprezintă o rotație, iar σ este pentagonul "oglindit".

(a) **Teorie**: Construcția grupului factor

(b) Arătați că $\left\{ 1, \rho^3\sigma \right\} \leq \mathrm{D}_5$.

Demonstrație. Notăm mulțimea cu $A = \left\{ 1, \rho^3\sigma \right\}$.

Oricum am compune între ele elementele, rămânem în mulțime:

$$\begin{aligned} 1 \cdot 1 &= 1 \in A \\ 1 \cdot \rho^3\sigma &= \rho^3\sigma \in A \\ \rho^3\sigma \cdot 1 &= \rho^3\sigma \in A \\ (\rho^3\sigma) \cdot (\rho^3\sigma) &= \rho^3(\sigma\rho)\rho^2\sigma = \rho^3\rho^4\sigma\rho^2\sigma \\ &= \rho^7(\sigma\rho)\rho\sigma \\ &= \rho^{11}(\sigma\rho)\sigma \\ &= \rho^{15}\sigma^2 = (\rho^5)^3 \cdot 1 \\ &= 1 \in A \end{aligned}$$

Pentru fiecare element, inversul elementului este conținut în mulțime:

$$\begin{aligned} 1 \cdot 1 = 1 &\iff 1^{-1} = 1 \in A \\ (\rho^3\sigma) \cdot (\rho^3\sigma) = 1 &\iff (\rho^3\sigma)^{-1} = \rho^3\sigma \in A \end{aligned}$$

□

(c) Arătați că $\langle\rho\rangle \trianglelefteq \mathrm{D}_5$.

Demonstrație. Trebuie să scriem subgrupul generat de ρ:

$$\langle\rho\rangle = \left\{ \rho, \rho^2, \rho^3, \rho^4, \rho^5 = 1 \right\}$$

Deoarece $\rho^5 = 1$, orice putere mai mare a lui ρ este conținută în această listă.

Pentru a arăta că este subgrup normal, cel mai simplu este să observăm că $\langle\rho\rangle$ are exact 5 elemente, iar D_5 are 10. Deci $\langle\rho\rangle$ are indice $2 = \frac{10}{5}$. Ne folosim de o proprietate din curs care zice că orice subgrup de indice 2 al unui grup este normal.

Dacă nu ținem minte această observație, trebuie să calculăm toate clasele de resturi la stânga $1H, \rho H, \ldots, \sigma H$ și toate clasele de resturi la dreapta $H1, H\rho, \ldots, H\sigma$, și să arătăm că au același număr și corespund unu-la-unu. □

(d) Descrieți grupul factor $D_5/\langle\rho\rangle$.

Demonstrație. Notăm $H = \langle\rho\rangle$. Clasele de resturi obținute ar fi $1H$, ρH, $\rho^2 H, \dots, \sigma H, \dots, \rho^4\sigma H$. Unele dintre acestea sunt echivalente:

$$H = \rho H = \cdots = \rho^4 H$$
$$\sigma H = \cdots = \rho^4\sigma H$$

Legea de compoziție pe subgrup:

$$H \cdot H = H$$
$$H \cdot \sigma H = \sigma H$$
$$\sigma H \cdot H = \sigma H$$
$$\sigma H \cdot \sigma H = H$$

Acest grup factor este izomorf cu $(\mathbb{Z}_2, +)$: H este elementul neutru $\hat{0}$, iar σH este $\hat{1}$. □

Subiectul 2

(a) **Teorie**: Definiția morfismului și izomorfismul de grupuri

(b) Elementele de ordin 8 din $\mathbb{Z}_{10} \times \mathbb{Z}_{36}$

Demonstrație. Ordinul grupului este $10 \cdot 36 = 360$.

Fie $(\hat{a}, \tilde{b})$ un element arbitrar din grup, cu $\hat{a} \in \mathbb{Z}_{10}$ și $\tilde{b} \in \mathbb{Z}_{36}$. Din teorema lui Lagrange trebuie ca ordinul lui $(\hat{a}, \tilde{b})$ să dividă 360, și $\operatorname{ord}\hat{a} \mid 10$, $\operatorname{ord}\tilde{b} \mid 36$.

Știm că

$$\operatorname{ord}_{\mathbb{Z}_{10}\times\mathbb{Z}_{36}}(\hat{a}, \tilde{b}) = [\operatorname{ord}_{\mathbb{Z}_{10}}\hat{a}, \operatorname{ord}_{\mathbb{Z}_{36}}\tilde{b}]$$

unde $[\cdot,\cdot]$ reprezintă c.m.m.m.c.-ul celor două ordine.

Din ipoteză, $\operatorname{ord}_{\mathbb{Z}_{10}\times\mathbb{Z}_{36}}(\hat{a}, \hat{b})$ trebuie să fie 8. Pentru a obține acest c.m.m.m.c. ar trebui ca unul dintre $\hat{a}, \tilde{b}$ să aibă ordin 8.

Deoarece $8 \nmid 10$ și $8 \nmid 36$, nu există soluții. □

(c) Elementele de ordin 20 din $\mathbb{Z}_{10} \times \mathbb{Z}_{36}$

Demonstrație. Asemănător exercițiului precedent, ajungem la concluzia că pentru a avea c.m.m.m.c.-ul 20, trebuie ca ordinele elementelor să fie 5 și 4 sau 10 și 4.

Ne folosim de faptul că în $\mathbb{Z}_n$:

$$\operatorname{ord}\hat{x} = \frac{n}{(x, n)}$$

unde $(\cdot,\cdot)$ reprezintă c.m.m.d.c.-ul celor două numere.

Rearanjând obținem

$$\operatorname{ord}\hat{x} \cdot (x, n) = n$$

Înlocuim în expresie valorile noastre:

$$\begin{aligned} 5 \cdot (x, 10) = 10 &\iff (x, 10) = 2 \\ 10 \cdot (x, 10) = 10 &\iff (x, 10) = 1 \\ 4 \cdot (x, 36) = 36 &\iff (x, 36) = 9 \end{aligned}$$

Elementele de ordin 5 în $\mathbb{Z}_{10}$ sunt $\left\{ \hat{2}, \hat{4}, \hat{6}, \hat{8} \right\}$, iar de ordin 10 sunt $\hat{1}, \hat{3}, \hat{7}, \hat{9}$. Elementele de ordin 4 în $\mathbb{Z}_{36}$ sunt $\left\{ \tilde{9}, \widetilde{27} \right\}$.

Deci elementele de ordin 20 sunt toate combinațiile posibile:

$$\left\{ (\hat{2}, \tilde{9}), \ldots, (\hat{8}, \widetilde{27}), (\hat{1}, \tilde{9}), \ldots, (\hat{9}, \widetilde{27}) \right\}$$

□

Subiectul 3

(a) **Teorie**: Definiți ce este o transpoziție. Demonstrați că orice transpoziție este permutare impară.

(b) Fie $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 4 & 5 & 6 & 7 & 8 & 9 & 11 & 12 & 3 & 13 & 1 & 2 & 10 \end{pmatrix} \in S_{13}$

Trebuie descompusă în produs de ciclii disjuncți, găsit inversul permutării, calculat σ^2, calculat ordinul permutării, calculat σ^{2019}.

Demonstrație. Descompunem permutarea în produs de ciclii disjuncți:

$$\sigma = (1, 4, 7, 11)(2, 5, 8, 12)(3, 6, 9)(10, 13)$$

Putem calcula σ^2 mai ușor folosindu-ne de această reprezentare:

$$\sigma^2 = (1, 7)(4, 11)(2, 8)(5, 12)(3, 9, 6)$$

Orice ciclu de lungime 4 s-a spart în doi ciclii de lungime 2. Ciclul de lungime 2 a dispărut complet.

Pentru σ^{-1}, putem inversa ordinea fiecărui ciclu:

$$\sigma^{-1} = (11, 7, 4, 1)(12, 8, 5, 2)(9, 6, 3)(13, 10)$$

Ordinul permutării este c.m.m.m.c.-ul lungimilor ciclului. Deci este $[4, 4, 3, 2]$, adică 12.

Pentru a calcula σ^{2019}, ne folosim de faptul că de fiecare dată când compunem permutarea cu ea însăși de 12 ori (ordinul ei), obținem permutarea identică. Deci

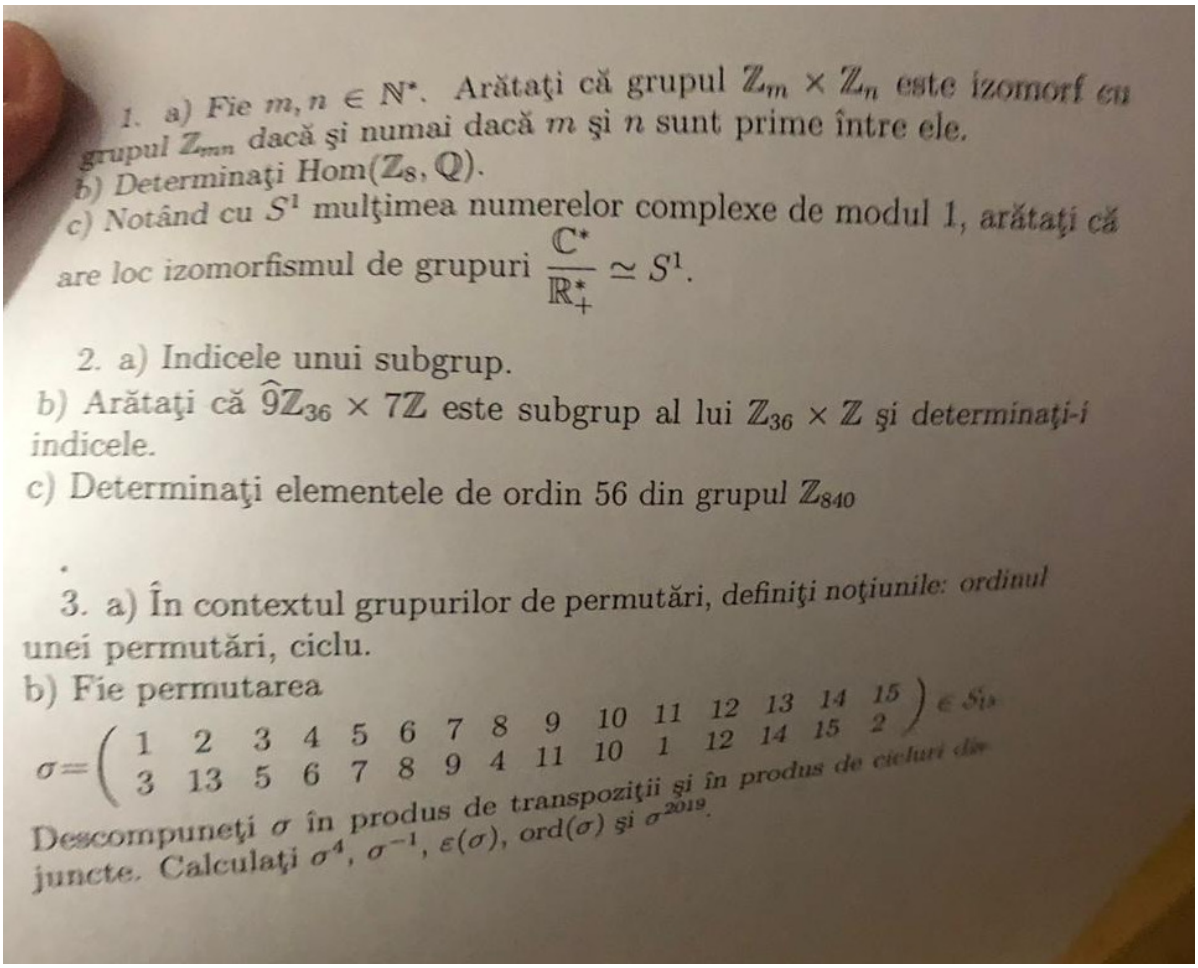
$$\sigma^{2019} = \sigma^{168 \cdot 12 + 3} = (\sigma^{12})^{168} \sigma^3 = \sigma^3$$

Răspunsul este

$$\sigma^{2019} = \sigma^3 = (1, 11, 7, 4)(2, 12, 8, 5)(10, 13)$$

□

Subiectul de la restanță la Mincu, pentru cei care vor să-și testeze cunoștințele:



1. a) Fie $m, n \in \mathbb{N}^*$. Arătaţi că grupul $\mathbb{Z}_m \times \mathbb{Z}_n$ este izomorf cu grupul $\mathbb{Z}_{mn}$ dacă şi numai dacă m şi n sunt prime între ele.
b) Determinaţi $\mathrm{Hom}(\mathbb{Z}_8, \mathbb{Q})$.
c) Notând cu S^1 mulţimea numerelor complexe de modul 1, arătaţi că are loc izomorfismul de grupuri $\dfrac{\mathbb{C}^*}{\mathbb{R}_+^*} \simeq S^1$.

2. a) Indicele unui subgrup.
b) Arătaţi că $\widehat{9}\mathbb{Z}_{36} \times 7\mathbb{Z}$ este subgrup al lui $\mathbb{Z}_{36} \times \mathbb{Z}$ şi determinaţi-i indicele.
c) Determinaţi elementele de ordin 56 din grupul $\mathbb{Z}_{840}$

3. a) În contextul grupurilor de permutări, definiţi noţiunile: ordinul unei permutări, ciclu.
b) Fie permutarea

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 3 & 13 & 5 & 6 & 7 & 8 & 9 & 4 & 11 & 10 & 1 & 12 & 14 & 15 & 2 \end{pmatrix} \in S_{15}$$

Descompuneţi σ în produs de transpoziţii şi în produs de cicluri disjuncte. Calculaţi σ^4, σ^{-1}, $\varepsilon(\sigma)$, $\mathrm{ord}(\sigma)$ şi σ^{2019}.

Link-uri utile

- Grup tutoriat
- Cursurile de la Băețica
- Cursurile de anul acesta de la Mincu
- Cursurile de an trecut de la Mincu

Exerciții

Exercițiul 1. Arătați că orice grup de 4 elemente este izomorf cu $\mathbb{Z}_4$ sau cu $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Demonstrație. Fie $(G, +)$ un grup cu $|G| = 4$.

O consecință a teoremei lui Lagrange este că ordinul unui element dintr-un grup trebuie să dividă ordinul (cardinalul) grupului. Deci elementele lui G trebuie să aibă ordinele $\operatorname{ord} x \in \{ 1, 2, 4 \}$.

Avem mai multe cazuri posibile:

1. Există cel puțin un element de ordin 4. Fie $a \in G$, cu $\operatorname{ord} a = 4$. Atunci observăm că a generează tot grupul, deci G este ciclic. Din *teorema de structură a grupurilor ciclice*, acesta este izomorf cu $\mathbb{Z}_4$.

2. Toate elementele au ordin cel mult 2. Să le notăm cu $0, a, b, c$. Atunci

$$0 + 0 = a + a = b + b = c + c = 0$$

Dacă $a + b = a$ sau $a + b = b$, ar rezulta că $a = 0$ sau că $b = 0$, ceea ce nu se poate. Deci $a + b = c$.

Analog obținem că $a + c = c + a = b$ și că $b + c = c + b = a$.

Tabelul pentru acest grup ar fi:

	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

Dacă realizăm corespondența $0 \to (\hat{0}, \hat{0})$, $a \to (\hat{0}, \hat{1})$, $b \to (\hat{1}, \hat{0})$ și $c \to (\hat{1}, \hat{1})$ observăm că tabelul se potrivește cu adunarea pe $\mathbb{Z}_2 \times \mathbb{Z}_2$.

□

Exercițiul 2. Arătați că orice grup de 6 elemente este izomorf cu $\mathbb{Z}_6$ sau S_3.

Demonstrație. Fie $(G, \cdot)$ un grup cu $|G| = 4$.

1. Dacă grupul are un element de ordin 6, atunci este ciclic, deci este izomorf cu $\mathbb{Z}_6$.

2. Grupul are cel puțin un element de ordin 3. Să-l notăm pe acesta a. Știm că a și a^2 sunt distincte, iar $a^3 = 1$.

   Să notăm cu b un alt element din grup, diferit de 1, a, sau a^2. Acesta trebuie să aibă ordin 2, altfel am obține distincte elementele ab, a^2b, ab^2, a^2b^2 și am depăși cardinalul lui G.

   Mai facem observația că $ab \neq ba$, altfel completând tabelul am obține că $\operatorname{ord} a = 6$, și G izomorf cu $\mathbb{Z}_6$.

   Completăm tabelul:

	1	a	a^2	b	ab	a^2b
1	1	a	a^2	b	ab	a^2b
a	a	a^2	1	ab	a^2b	b
a^2	a^2	1	a	a^2b	b	ab
b	b	a^2b	ab	1	a^2	a
ab	ab	b	a^2b	a	1	a^2
a^2b	a^2b	ab	b	a^2	a	1

   Acesta se potrivește cu cel al lui S_3.

3. Cazul în care are doar elemente de ordin cel mult 2 ar implica că grupul este comutativ, deoarece

$$\left.\begin{array}{l}(xy)^2 = 1 \implies xy = (xy)^{-1} \\ (xy)^{-1} = y^{-1}x^{-1} = yx\end{array}\right\} \implies xy = yx$$

□

Exercițiul 3. Arătați că orice grup de 8 elemente este izomorf cu $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2^3$, D_4, sau cu Q (grupul cuaternionilor).

Demonstrație. Fie $(G, \cdot)$ un grup cu $|G| = 8$.

1. Dacă are cel puțin un element de ordin 8, atunci G este ciclic, deci izomorf cu $\mathbb{Z}_8$.

2. Dacă toate elementele au ordin cel mult 2, atunci G este izomorf cu $\mathbb{Z}_2^3$.

3. Fie $a \in G$ un element de ordin 4. Acesta va genera subgrupul $\langle a \rangle = \{ 1, a, a^2, a^3 \}$.

   Trebuie să mai existe cel puțin un element, pe care îl notăm b, care să nu aparțină lui $\langle a \rangle$. Elementele grupului sunt

$$G = \{ 1, a, a^2, a^3, b, ab, a^2b, a^3b \}$$

Știm că b^2 trebuie să fie egal cu unul din primele patru elemente scrise mai sus:

(a) Dacă $b^2 = 1$, atunci $\operatorname{ord} b = 2$. Trebuie să vedem cu cât este egal ba:

i. Dacă $ba = ab$ atunci G este comutativ și izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_4$.

ii. Dacă $ba = a^2b$, înmulțind cu inversul obținem $a = b^{-1}a^2b$. Ridicând la pătrat ajungem la contradicția $a^2 = (b^{-1}a^2b)(b^{-1}a^2b) = 1$.

iii. Dacă $ba = a^3b$, regăsim grupul diedral $\mathrm{D}4$.

(b) Dacă $b^2 = a^2$, atunci $\operatorname{ord} b = 4$.

i. Dacă $ba = ab$ regăsim $\mathbb{Z}_2 \times \mathbb{Z}_4$.

ii. Dacă $ba = a^2b$ ajungem la contradicția $ba = b^3 \iff a = b^2 = a^2$.

iii. Dacă $ba = a^3b$ obținem un grup care se numește *grupul cuaternionilor*. Cuaternionii se notează de obicei cu

$$Q = \{ \pm 1, \pm i, \pm j, \pm k \}$$

cu proprietatea că $i^2 = j^2 = k^2 = ijk = -1$.

(c) $b^2 = a$ și $b^2 = a^3$ duc la contradicția că $\operatorname{ord} b \notin \{ 2, 4 \}$

□

Exercițiu. Găsiți elementele inversabile, divizorii lui 0, elementele nilpotente și elementele idempotente din $\mathbb{Z}_{63}$.

Demonstrație.

- Elementele au invers la înmulțire în $\mathbb{Z}_n$ dacă și numai dacă sunt prime față de n. În acest caz, $U(\mathbb{Z}_{63}) = \{\, \hat{1}, \hat{2}, \hat{4}, \hat{5}, \dots \,\}$.

- Divizorii lui 0 dintr-un inel R sunt elementele $a \in R$ pentru care $\exists b \neq 0$ astfel încât $ab = 0$. Din acest motiv, elementele care sunt inversabile sigur nu pot fi divizori ai lui 0.

  În $\mathbb{Z}_n$, toate numerele care au un factor în comun cu n sunt divizori ai lui 0. Răspunsul este $\{\, \hat{3}, \hat{6}, \hat{7}, \hat{9}, \hat{12}, \dots \,\}$.

- Elementele nilpotente sunt cele pentru care $\exists n \in \mathbb{N}^*$ astfel încât $a^n = 0$. 0 este întotdeauna nilpotent, dar este posibil să mai existe și alte elemente de acest fel.

  În $\mathbb{Z}_n$, elementele nilpotente sunt cele care conțin cel puțin toți factorii primi distincți ai lui n. Pentru $n = 63$, avem $63 = 3^2 \cdot 7$, deci trebuie să găsim numere care să fie multiplii de $3 \cdot 7$. Răspunsul este $\mathcal{N}(\mathbb{Z}_{63}) = \{\, \hat{0}(= 3 \cdot 7 \cdot 0), \hat{21}(= 3 \cdot 7 \cdot 1), \hat{42}(= 3 \cdot 7 \cdot 2) \,\}$.

- Elementele idempotente sunt cele pentru care $a^2 = a$. Atât 0 cât și 1 sunt întotdeauna idempotente. De asemenea, dacă a este idempotent, atunci și $1 - a$ este idempotent, deci odată ce am găsit jumătate dintre idempotente putem obține mai ușor și cealaltă jumătate.

  Ideea este să descompunem n în produs de r numere prime sau puteri de numere prime, $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ și să descompunem $\mathbb{Z}_n$ în $\mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \dots \times \mathbb{Z}_{p_r^{k_r}}$. Singurele elemente idempotente din fiecare $\mathbb{Z}_{p^k}$ sunt $\bar{0}$ și $\bar{1}$.

  În acest caz $\mathbb{Z}_{63} = \mathbb{Z}_7 \times \mathbb{Z}_9$. Trebuie să scriem toate cele 2^r șiruri posibile de 0 și 1 de lungime r (fiecare corespunde unui idempotent):

  - $(\bar{0}, \bar{\bar{0}}) \implies$ numere care dau rest 0 la împărțirea cu 7 și rest 0 la împărțirea cu 9 $\implies \hat{0}$
  - $(\bar{1}, \bar{\bar{1}}) \implies$ numere care dau rest 1 la împărțirea cu 7 și rest 1 la împărțirea cu 9 $\implies \hat{1}$
  - $(\bar{0}, \bar{\bar{1}}) \implies$ numere care dau rest 0 la împărțirea cu 7 și rest 1 la împărțirea cu 9 $\implies \hat{28}$

– Din moment ce deja știm că $\hat{28}$ este idempotent, știm că și $1-28 \equiv -27 \equiv 36 \mod 63$ este idempotent. Dacă nu observăm acest lucru, putem să calculăm ca mai înainte:
$(\bar{1}, \bar{\bar{0}}) \implies$ numere care dau rest 1 la împărțirea cu 7 și rest 0 la împărțirea cu 9 $\implies \hat{36}$

Deci $\text{Idemp}(\mathbb{Z}_{63}) = \{ \hat{0}, \hat{1}, \hat{28}, \hat{36} \}$.

□

Exercițiu. Găsiți idealele lui $\mathbb{C} \times M_4(\mathbb{Z}_6 \times \mathbb{R})$.

Demonstrație. Ne folosim de una sau mai multe dintre următoare proprietăți (în rezolvare, trebuie enunțate înainte de folosirea lor):

- Idealele lui $R_1 \times R_2 \times \cdots \times R_n$ sunt $I_1 \times I_2 \times \cdots \times I_n$, unde $I_1, I_2, \ldots, I_n$ sunt ideale ale lui $R_1, R_2, \ldots,$ respectiv R_n.
- Idealele lui $\mathbb{Z}$ sunt $n\mathbb{Z}, \forall n \in \mathbb{N}^*$.
- Idealele lui $\mathbb{Z}_n$ sunt $\hat{d}\mathbb{Z}_n$ unde $d \mid n$.
- Dacă R este corp, atunci singurele lui ideale sunt $\{ 0 \}$ și R.
- Idealele lui $M_n(R)$ sunt $M_n(I)$ unde I este un ideal al lui R.

În acest caz:

- Fiind corpuri, idealele lui $\mathbb{C}$ și $\mathbb{R}$ sunt $\{ 0 \}$ și ele însăși.
- Idealele lui $\mathbb{Z}_6$ sunt $\hat{d}\mathbb{Z}_6$ unde $d \mid 6$, deci $\hat{1}\mathbb{Z}_6, \hat{2}\mathbb{Z}_6, \hat{3}\mathbb{Z}_6, \hat{6}\mathbb{Z}_6$.
- Ne folosim de prima proprietate pentru idealele produsului de inele.
- Ne folosim de ultima proprietate pentru idealele inelelor de matrici.

În concluzie, idealele căutate sunt:

- $\{ 0 \} \times M_4(\hat{1}\mathbb{Z}_6 \times \{ 0 \})$
- $\{ 0 \} \times M_4(\hat{1}\mathbb{Z}_6 \times \mathbb{R})$
- $\{ 0 \} \times M_4(\hat{2}\mathbb{Z}_6 \times \{ 0 \})$
- $\{ 0 \} \times M_4(\hat{2}\mathbb{Z}_6 \times \mathbb{R})$
- ...

- $\mathbb{C} \times M_4(\hat{6}\mathbb{Z}_6 \times \{\,0\,\})$
- $\mathbb{C} \times M_4(\hat{6}\mathbb{Z}_6 \times \mathbb{R})$

□

Exercițiu. Găsiți idealele inelului $R = \mathbb{Z}_8 \times \mathbb{Q}$ și, până la izomorfism, inelele factor obținute prin împărțirea la aceste ideale.

Demonstrație. Asemănător exercițiului anterior, găsim idealele acestui inel: $\hat{1}\mathbb{Z}_8 \times \{\,0\,\}, \hat{1}\mathbb{Z}_8 \times \mathbb{Q}, \ldots, \hat{8}\mathbb{Z}_8 \times (\{\,0\,\}), \hat{8}\mathbb{Z}_8 \times \mathbb{Q}$.

Pentru a doua parte ne vom folosi și de următoarele proprietăți:

- Dacă $I_1 \trianglelefteq R_1$ și $I_2 \trianglelefteq R_2$, $(R_1 \times R_2)/(I_1 \times I_2) \cong (R_1/I_1) \times (R_2/I_2)$
- Dacă $I, J \trianglelefteq R$ și $J \subset I$, atunci $(R/J)/(I/J) \cong (R/I)$.
- $(R/R) \cong \{\,0\,\}, (R/\{\,0\,\}) \cong R$
- $\{\,0\,\} \times R \cong R \times \{\,0\,\} \cong R$
- $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$

Acum trebuie să scriem toate inelele factor de forma $\frac{\mathbb{Z}_8 \times \mathbb{Q}}{I \times J}$, unde $I \in \{\,\hat{1}\mathbb{Z}_8, \ldots, \hat{8}\mathbb{Z}_8\,\}$ și $J \in \{\,\{\,0\,\}, \mathbb{Q}\,\}$. Trebuie de asemenea să "simplificăm" aceste inele până la forma în care se vede care sunt izomorfe între ele.

- $$\frac{\mathbb{Z}_8 \times \mathbb{Q}}{\hat{1}\mathbb{Z}_8 \times \{\,0\,\}} \cong \frac{\mathbb{Z}_8}{\mathbb{Z}_8} \times \frac{\mathbb{Q}}{\{\,0\,\}} \cong \{\,\hat{0}\,\} \times \mathbb{Q} \cong \mathbb{Q}$$
- $$\frac{\mathbb{Z}_8 \times \mathbb{Q}}{\hat{1}\mathbb{Z}_8 \times \mathbb{Q}} \cong \frac{\mathbb{Z}_8}{\mathbb{Z}_8} \times \frac{\mathbb{Q}}{\mathbb{Q}} \cong \{\,\hat{0}\,\} \times \{\,0\,\} \cong \{\,0\,\}$$
- $$\ldots$$
- $$\frac{\mathbb{Z}_8 \times \mathbb{Q}}{\hat{4}\mathbb{Z}_8 \times \mathbb{Q}} \cong \frac{\mathbb{Z}_8}{\hat{4}\mathbb{Z}_8} \times \frac{\mathbb{Q}}{\mathbb{Q}} \cong \frac{\mathbb{Z}/8\mathbb{Z}}{4\mathbb{Z}/8\mathbb{Z}} \times \{\,0\,\} \cong \frac{\mathbb{Z}}{4\mathbb{Z}} \times \{\,0\,\} \cong \mathbb{Z}_4 \times \{\,0\,\} \cong \mathbb{Z}_4$$
- $$\ldots$$
- $$\frac{\mathbb{Z}_8 \times \mathbb{Q}}{\hat{8}\mathbb{Z}_8 \times \mathbb{Q}} \cong \frac{\mathbb{Z}_8}{\hat{8}\mathbb{Z}_8} \times \frac{\mathbb{Q}}{\mathbb{Q}} \cong \frac{\mathbb{Z}_8}{\{\,0\,\}} \times \{\,0\,\} \cong \mathbb{Z}_8 \times \{\,0\,\} \cong \mathbb{Z}_8$$

□

Link-uri utile

- Grup tutoriat
- Cursurile de la Băețica
- Cursurile de anul acesta de la Mincu
- Cursurile de an trecut de la Mincu

Exerciții

Exercițiul 1. Fie $Q = \{ 1, -1, i, -i, j, -j, k, -k \}$ grupul cuaternionilor.

1. Arătați că $\{ 1, -1 \} \leq Q$
2. Arătați că $\{ 1, -1 \} \trianglelefteq Q$
3. Descrieți grupul factor $\frac{Q}{\{ 1, -1 \}}$

Demonstrație. Enunțăm aici regulile de calcul pentru cuaternioni:

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Vom nota $A = \{ -1, 1 \}$ ca să nu ne tot repetăm.

1. Mai întâi arătăm că A este parte stabilă în raport cu operația „$\cdot$”:

$$\begin{aligned} 1 \cdot 1 = 1 \in A \\ 1 \cdot (-1) = -1 \in A \\ (-1) \cdot 1 = -1 \in A \\ (-1) \cdot (-1) = 1 \in A \end{aligned}$$

   A este finită deoarece $|A| = 2$.

   Avem o propoziție care ne zice că A este subgrup.

2. Construim clasele de resturi la stânga și la dreapta pentru A și vedem că acestea se potrivesc unu-la-unu:

$$\begin{aligned} 1 \cdot A = -1 \cdot A &= \{ 1, -1 \} = A \cdot 1 = A \cdot (-1) \\ i \cdot A = -i \cdot A &= \{ i, -i \} = A \cdot i = A \cdot (-i) \\ j \cdot A = -j \cdot A &= \{ j, -j \} = A \cdot j = A \cdot (-j) \\ k \cdot A = -k \cdot A &= \{ k, -k \} = A \cdot k = A \cdot (-k) \end{aligned}$$

   Deci $\{ 1, -1 \}$ este subgrup normal.

3. Grupul factor cerut este format din

$$\frac{Q}{\{1,-1\}} = \{\{1,-1\},\{i,-i\},\{j,-j\},\{k,-k\}\}$$

Vom nota cu $\hat{x}$ clasa corespunzătoare elementului $x \in \{1,i,j,k\}$. Obținem o descriere echivalentă a grupului factor:

$$\frac{Q}{\{1,-1\}} = \{\hat{1},\hat{i},\hat{j},\hat{k}\}$$

Fiind un grup cu 4 elemente, trebuie să fie izomorf fie cu $\mathbb{Z}_4$ fie cu $\mathbb{Z}_2 \times \mathbb{Z}_2$. Ne putem da seama mai ușor cu care este izomorf dacă construim tabelul:

$\cdot$	$\hat{1}$	$\hat{i}$	$\hat{j}$	$\hat{k}$
$\hat{1}$	$\hat{1}$	$\hat{i}$	$\hat{j}$	$\hat{k}$
$\hat{i}$	$\hat{i}$	$\hat{1}$	$\hat{k}$	$\hat{j}$
$\hat{j}$	$\hat{j}$	$\hat{k}$	$\hat{1}$	$\hat{i}$
$\hat{k}$	$\hat{k}$	$\hat{j}$	$\hat{i}$	$\hat{1}$

Se observă ușor că acest tabel corespunde lui $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$.

□

Exercițiul 2. Definiția noțiunea de transpoziție și demonstrați că orice transpoziție este o permutare impară.

Demonstrație. O transpoziție este un ciclu de lungime doi. Ne va ajuta în demonstrație să scriem cum arată la cazul general o transpoziție.

Fie o transpoziție $\sigma \in S_n$. Aceasta se scrie ca

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n-1 & n \\ 1 & 2 & \dots & j & \dots & i & \dots & n-1 & n \end{pmatrix}$$

unde $1 \leq i < j \leq n$, și $\sigma(k) = k$ pentru orice k diferit de i și j.

O *inversiune* a unei permutări este orice pereche de indici i, j cu $i < j$ dar $\sigma(i) > \sigma(j)$. Prin definiție, o permutare se numește *impară* dacă are un număr impar de inversiuni. Deci trebuie să numărăm inversiunile dintr-o transpoziție pentru a vedea dacă este impară.

Să scriem din nou partea care ne interesează din transpoziție:

$$\sigma = \begin{pmatrix} \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots \\ \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots \end{pmatrix}$$

Să numărăm inversiunile cu un capăt în i: avem $i < i+1$ dar $j > i+1$, $i < i+2$ dar $j > i+2$ etc. De la i la $j-1$ inclusiv avem un total de $j-i$ inversiuni.

Analog numărăm inversiunile cu un capăt în j: avem $i+1 < j$ dar $i+1 > i$, $i+2 < j$ dar $i+2 > i$ etc. Aici mai avem încă $j-i$ inversiuni.

Mai trebuie să numărăm și inversiunea (i, j). În total avem un număr impar de inversiuni:

$$(j-i) + (j-i) + 1 = 2(j-i) + 1 = 2m + 1$$

□

Exercițiul 3. Demonstrați că

$$S_n = \langle (1,2), (2,3), (3,4), \ldots, (n-1,n) \rangle$$

(adică că pornind de la acele transpoziții putem genera orice permutare de ordin n)

Demonstrație. De obicei când avem o submulțime și vrem să arătăm că aceasta poate genera tot grupul, este suficient să arătăm că poate genera un generator/sistem de generatori știut al grupului.

La permutări, știm că mulțimea tuturor transpozițiilor poate genera orice permutare. Dacă reușim să plecăm de la transpozițiile date și să obținem orice transpoziție, am rezolvat problema.

Să vedem ce se întâmplă când facem următoarea compunere de permutări:

$$(1,2) \circ (2,3) \circ (1,2) = (1,3)$$

Luăm permutarea generată și calculăm:

$$(1,3) \circ (3,4) \circ (1,3) = (1,4)$$

Prin inducție, se poate arăta că astfel generăm toate transpozițiile de forma $(1,i)$ cu $\forall i \in \overline{2,n}$.

Acum încercăm următoarele:

$$(1,2) \circ (1,3) \circ (1,2) = (2,3)$$
$$(1,2) \circ (1,4) \circ (1,2) = (2,4)$$
$$(1,2) \circ (1,5) \circ (1,2) = (2,5)$$

Generalizând:

$$(1,2) \circ (1,i) \circ (1,2) = (2,i), \forall i \in \overline{3,n}$$

Putem obține orice transpoziție:

$$(1,i) \circ (1,j) \circ (1,i) = (i,j), \forall i,j \in \overline{3,n}$$

Din moment ce mulțimea transpozițiilor generează S_n, am demonstrat că

$$\{ (1,2), (2,3), \ldots, (n-1,n) \}$$

generează tot S_n. □

Link-uri utile

- Grup tutoriat
- Exerciții rezolvate
- Cursurile de la Băețica
- Cursurile de la Mincu

Sfaturi

- La ambii profesori este important să scrii toată rezolvarea **pas cu pas**, și să fie **corect** din punct de vedere logic.
  - Dacă omiți pași care ți se par evidenți, profesorul ar putea să întrebe la corectură cum de ai obținut un anume rezultat.
  - În special la Mincu: În cazul în care nu ești sigur dacă e nevoie să arăți/verifici ceva ca parte a unei demonstrații, nu pierzi nimic dacă scrii în plus.
  - Mare grijă la diferența dintre $p \implies q$ și $p \iff q$! De asemenea, e important să pui conectori logici ($\implies$, *așadar*, *deci*) între propozițiile pe care le scrii, altfel nu ar fi clar cum decurge rezolvarea.
- Întotdeauna trebuie să ai în minte **ce îți cere problema** (concluzia). Multă lume ajunge să dea răspunsul corect dar la cu totul altă întrebare. Dacă nu înțelegi ce vrea enunțul de la tine, poți cere clarificări de la profesor.

Exerciții

Exercițiul 1. Fie polinoamele $f = X^2 + \hat{2}X + \hat{1}$, $g = X^2 + \hat{2}X + \hat{2}$ din $\mathbb{Z}_3[X]$.
Demonstrați că

$$\mathbb{Z}_3[X]/(f) \ncong \mathbb{Z}_3[X]/(g)$$

Demonstrație. Vrem să găsim o justificare de ce nu ar putea fi izomorfe inelele factor.
Observăm că polinomul f este reductibil:

$$\begin{aligned} &f(\hat{0}) = \hat{1} \\ &f(\hat{1}) = \hat{1} \\ &f(\hat{2}) = \hat{0} \implies f = (X - \hat{2})(X - \hat{2}) \end{aligned}$$

În timp ce polinomul g este ireductibil:

$$\begin{aligned} g(\hat{0}) &= \hat{2} \\ g(\hat{1}) &= \hat{2} \\ g(\hat{2}) &= \hat{1} \end{aligned}$$

Din curs avem o proprietate care ne zice că atunci când factorizăm printr-un polinom ireductibil, cum avem în cazul $\mathbb{Z}_3[X]/(g)$, obținem un *corp*. Ar fi suficient să arătăm că $\mathbb{Z}_3[X]/(f)$ nu e corp.

Când polinomul prin care factorizăm este reductibil, putem să îi scriem descompunerea în factori în inelul factor ca să obținem *divizori ai lui zero*:

$$\overline{(\underbrace{X-\hat{2}}_{\neq 0})(\underbrace{X-\hat{2}}_{\neq 0})} = \overline{X^2+\hat{2}X+\hat{1}} = \bar{\hat{0}}$$

Deoarece are divizori al lui zero, $\mathbb{Z}_3[X]/(f)$ nu este corp. Deci nu poate fi izomorf cu $\mathbb{Z}_3[X]/(g)$. □

Exercițiul 2. Fie $J = (X^3+1)$ un ideal al inelului $\mathbb{Q}[X]$. Determinați elementele nilpotente și idempotente ale lui $\mathbb{Q}[X]/J$.

Demonstrație. Elementele inelului factor sunt de forma

$$\frac{\mathbb{Q}[X]}{J} = \left\{ aX^2+bX+c \;\middle|\; a,b,c \in \mathbb{Q} \right\}$$

și mai știm și că $\widehat{X^3} = \widehat{-1}$.

Pentru ca un polinom să fie nilpotent trebuie ca

$$(aX^2\widehat{+bX}+c)^n = \hat{0} \text{ pentru un } n \in \mathbb{N}$$

Dacă dezvoltăm și ne uităm doar la termenul liber, obținem că

$$\hat{c^n} = \hat{0}$$

deci trebuie ca c să fie nilpotent, în cazul nostru singura posibilitate este $c = 0$.

Repetăm raționamentul pentru

$$(a\widehat{X^2+bX})^n = \hat{0} \iff \hat{X}^n(\widehat{aX+b})^n = \hat{0}$$

Dacă ne uităm doar la termenul de grad n obținem că $\widehat{X^n b^n} = \hat{0}$, de unde b este nilpotent, deci este 0.

Analog obținem că $a = 0$. Singurul nilpotent al inelului factor este $\hat{0}$.

Pentru ca un polinom să fie idempotent trebuie ca

$$(aX^2\widehat{+bX}+c)^2 = aX^2\widehat{+bX}+c$$

Desfăcând paranteza și folosindu-ne de identitatea de mai sus obținem

$$\widehat{a^2X^4}+\widehat{b^2X^2}+\hat{c^2}+\widehat{2abX^3}+\widehat{2acX^2}+\widehat{2bcX} = \widehat{aX^2}+\widehat{bX}+\hat{c}$$
$$\widehat{-a^2}\hat{X}+\hat{b^2}\widehat{X^2}+\hat{c^2}-\widehat{2ab}+\widehat{2ac}\widehat{X^2}+\hat{bc}\hat{X} = \widehat{aX^2}+\widehat{bX}+\hat{c}$$
$$\widehat{X^2}(\hat{b^2}+\widehat{2ac})+X(\widehat{-a^2}+\hat{bc})+\hat{c^2}-\widehat{2ab} = \widehat{aX^2}+\widehat{bX}+\hat{c}$$
$$\begin{cases} b^2+2ac = a \\ -a^2+bc = b \\ c^2-2ab = c \end{cases}$$

Singurele soluții ale acestui sistem sunt $a = b = c = 0$ și $a = b = 0$, $c = 1$. Deci singurii idempotenți din inelul factor sunt 0 și 1. □

Exercițiul 3. Se dă polinomul $f = X^4 + X^2 + 1$. Notăm cu $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ rădăcinile complexe ale polinomului. Scrieți un polinom care să aibă rădăcinile $2\alpha_1+1, 2\alpha_2+1, 2\alpha_3+1, 2\alpha_4+1$.

Demonstrație. Vrem să obținem un nou polinom f' în Y care să aibă acele rădăcini. Pentru asta notăm $Y = 2X + 1$ și extragem X-ul:

$$Y = 2X + 1 \iff Y - 1 = 2X \iff \frac{Y-1}{2} = X$$

Înlocuind, obținem polinomul

$$f' = \left(\frac{Y-1}{2}\right)^4 + \left(\frac{Y-1}{2}\right)^2 + 1$$

În această formă se vede că $f'(2\alpha_k + 1)$ este egal cu $f(\alpha_k) = 0$, $\forall k \in \overline{1,4}$. Mai rămâne să desfacem parantezele ca să scriem polinomul în forma lui obișnuită (ca să fie mai ușor, putem înmulți cu $\frac{1}{16}$, vom avea aceleași rădăcini). □

Rezolvarea exercițiilor din cursul de algebră

Cursul scris de dl. prof. Cornel Băețica
Rezolvări scrise de Gabriel Majeri *

Cuprins

*Mulțumiri dlui. prof. Gabriel Mincu pentru cursul de la seria 14 și explicațiile de la seminarii, Antoniei Biro-Bălan pentru materiale, feedback și explicații, și celorlalți colegi pentru feedback și susținere.

1 Inele

1.1 Generalități

Exercițiul (1.3)**.** Să se determine numărul structurilor:

(a) de inel, neizomorfe între ele, care pot fi definite pe grupul $(\mathbb{Z}_p, +)$, unde p este un număr prim.

Demonstrație. În acest exercițiu o să notăm cu $*$ legea de înmulțire pe care trebuie să o definim.

Pentru a defini în mod unic această lege de compoziție, este suficient să fixăm valoarea pentru $\hat{1} * \hat{1}$, deoarece $\hat{k} = \underbrace{\hat{1} + \cdots + \hat{1}}_{\text{de } k \text{ ori}}, \forall \hat{k} \in \mathbb{Z}_p$, și avem că

$$\begin{aligned}\hat{a} * \hat{b} &= (\underbrace{\hat{1} + \cdots + \hat{1}}_{\text{de } a \text{ ori}}) * (\underbrace{\hat{1} + \cdots + \hat{1}}_{\text{de } b \text{ ori}}) \\ &= \underbrace{\hat{1} * \hat{1} + \cdots + \hat{1} * \hat{1}}_{\text{de } a \cdot b \text{ ori}} \\ &= (ab)(\hat{1} * \hat{1})\end{aligned}$$

Dacă $\hat{1} * \hat{1} = \hat{0}$, atunci avem înmulțirea nulă pe $\mathbb{Z}_p$, $\hat{a} * \hat{b} = \hat{0}, \forall \hat{a}, \hat{b} \in \mathbb{Z}_p$.

Dacă $\hat{1} * \hat{1} = \hat{u} \neq \hat{0}$, atunci $\hat{a} * \hat{b} = (ab)\hat{u}$.

Putem să arătăm că pentru orice $\hat{u}$ toate aceste structuri sunt izomorfe între ele, arătând că toate sunt izomorfe cu $\mathbb{Z}_p$ cu înmulțirea obișnuită modulo p, definind izomorfismul $f \colon (\mathbb{Z}_p, +, *) \to (\mathbb{Z}_p, +, \cdot)$, $f(\hat{x}) = \hat{u}^{-1}\hat{x}$. □

(b) de inel unitar ce pot fi definite pe grupul $(\mathbb{Z}_n, +)$ și să se arate că acestea sunt izomorfe.

Demonstrație. Deoarece avem nevoie de inele unitare, excludem din start înmulțirea nulă ($a * b = 0, \forall a, b \in \mathbb{Z}_n$).

Toate elementele care sunt prime față de n au invers la înmulțire în $\mathbb{Z}_n$. Folosind morfismul de la sub punctul precedent, putem arăta că toate acestea sunt izomorfe cu $(\mathbb{Z}_n, +, \cdot)$, adică $\mathbb{Z}_n$ cu înmulțirea obișnuită modulo n. □

Exercițiul (1.4)**.** Arătați că pe grupul $(\mathbb{Q}/\mathbb{Z}, +)$ nu se poate defini o structură de inel unitar.

Demonstrație. Clasele de resturi din acest grup factor sunt de forma $\hat{\frac{1}{a}}$, cu $a \in \mathbb{Z}$. Observăm că pentru orice $n \in \mathbb{N}^*$, elementul $\widehat{\frac{1}{n}}$ are ordin n, deoarece $\underbrace{\widehat{\frac{1}{n}} + \cdots + \widehat{\frac{1}{n}}}_{\text{de } n \text{ ori}} = \widehat{\frac{n}{n}} = \hat{1} = \hat{0}$.

Presupunem că am definit o înmulțire pe acest inel, și că avem elementul unitate $\hat{\frac{1}{k}}, k \in \mathbb{Z}$. Atunci pentru orice $\widehat{1/a} \in \mathbb{Q}/\mathbb{Z}$:

$$\underbrace{\widehat{\frac{1}{a}} + \cdots + \widehat{\frac{1}{a}}}_{\text{de } k \text{ ori}} = \widehat{\frac{k}{a}} = \widehat{\frac{1}{k}} \cdot \widehat{\frac{k}{a}} = \hat{0}$$

Asta înseamnă că ordinul oricărui element este cel mult k, dar asta ar contrazice faptul că putem avea elemente cu ordin orice număr natural. □

Exercițiul (1.6)**.** Să se arate că $(\mathbb{R}^{\mathbb{R}}, +, \circ)$ nu este inel.

Demonstrație. Presupunem că această structură ar fi inel. Atunci compunerea ar trebui să fie distributivă față de adunare. Luăm contra exemplul $f, g, h \colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2, g(x) = 2x, h(x) = 3x$.

$$f \circ (g + h) = f(g(x) + h(x)) = f(2x + 3x) = (5x)^2 = 25x^2$$

$$f \circ g + f \circ h = f(g(x)) + f(h(x)) = f(2x) + f(3x) = 4x^2 + 9x^2 = 13x^2$$

Avem că $25x^2 \neq 13x^2$, deci $f \circ (g+h) \neq f \circ g + f \circ h$, deci nu este inel. □

Exercițiul (1.7)**.** Fie R un inel și $n \geq 2$. Să se arate că inelul de matrice $M_n(R)$ este comutativ dacă și numai dacă $ab = 0$ pentru orice $a, b \in R$.

Demonstrație. $\implies$ Fie $a, b \in R$. Considerăm matricile din $A, B \in M_n(R)$, unde A este matricea care îl are pe a pe poziția $(2, 1)$ și zerouri în rest, și B îl are pe b pe $(1, 2)$.

Dacă calculăm produsul AB, obținem matricea care îl are pe ab în poziția (2, 2), iar din produsul BA obținem 0 în acea poziție.

Deoarece știm din ipoteză că $AB = BA$, rezultă că $ab = 0$.

$\impliedby$ Fie $A, B \in M_n(R)$. Când calculăm produsul AB, respectiv BA, calculăm expresii de forma $\sum a_i b_j$. Deoarece știm din ipoteză că $ab = 0, \forall a, b \in R$, aceste expresii vor fi toate 0. Deci $AB = BA = \mathbf{0}_n$.

□

Exercițiul (1.10)**.** Arătați că dacă un inel are un divizor al lui zero la stânga (dreapta) nenul, atunci are un divizor al lui zero nenul.

Demonstrație. Fie $a \in R$, $a \neq 0$ un divizor al lui zero la stânga, nenul. Atunci, din definiție $\exists b \in R$, $b \neq 0$ astfel încât $a \cdot b = 0$. Asta înseamnă că b este un divizor al lui zero *la dreapta* nenul.

Considerăm acum elementul $b \cdot a$. Dacă acesta este 0, atunci înseamnă că a este un divizor al lui zero și la dreapta, deci am terminat demonstrația. Altfel, observăm ce se întâmplă când înmulțim acest element cu b la dreapta, respectiv cu a la stânga:

$$(b \cdot a) \cdot b = b \cdot (a \cdot b) = b \cdot 0 = 0$$
$$a \cdot (b \cdot a) = (a \cdot b) \cdot a = 0 \cdot a = 0$$

Deci $b \cdot a$ este sigur divizor al lui zero.

Demonstrația decurge analog dacă pornim cu un divizor al lui zero la dreapta nenul. □

Exercițiul (1.11)**.** Arătați că în inelul $M_n(R)$ orice divizor al lui zero la stânga (dreapta) este divizor al lui zero la dreapta (stânga).

Demonstrație. Fie $A \in M_n(R)$, $A \neq 0$ o matrice care este divizor al lui zero la stânga.

Fiind divizor al lui zero, sigur nu este inversabilă, deci $\det A = 0$. De asemenea, $\det A^\top = 0$.

Considerând matricea $A^\top$ o transformare liniară între spații vectoriale, din teorema dimensiunii, trebuie să existe cel puțin un vector nenul $v \in R^n$ pentru care $A^\top v = 0$.

Construim matricea V punând copii ale vectorului v pe fiecare coloană. Avem că $A^\top V = 0$. Atunci $(A^\top V)^\top = 0 \iff V^\top A = 0$.

Deci A este divizor al lui zero și la dreapta. □

Exercițiul (1.15)**.**

- Arătați că $f \in \mathbb{R}^\mathbb{R}$ este divizor al lui zero dacă și numai dacă există $x_0 \in \mathbb{R}$ astfel încât $f(x_0) = 0$.

  Demonstrație. $\implies$ Deoarece f este divizor al lui zero, înseamnă că există un $g \in \mathbb{R}^\mathbb{R}, g \neq 0$ astfel încât $(f \cdot g)(x) = 0, \forall x \in \mathbb{R}$.
  Putem rescrie $g \neq 0$ ca $\exists x_0$ astfel încât $g(x_0) \neq 0$. Atunci:

  $$(f \cdot g)(x_0) = 0 \implies f(x_0)g(x_0) = 0 \implies f(x_0) = 0$$

$\Longleftarrow$ Definim $g\colon \mathbb{R} \to \mathbb{R}$, $g \neq 0$,

$$g(x) = \begin{cases} 1, \, x = x_0 \\ 0, \text{ altfel} \end{cases}$$

Se observă că $f(x)g(x) = (f \cdot g)(x) = 0, \forall x \in \mathbb{R}$. Deci f este divizor al lui 0.

□

- Fie $C(\mathbb{R}) = \{ \, f\colon \mathbb{R} \to \mathbb{R} \mid \text{f este continuă} \, \}$ cu operațiile de adunare și înmulțire a funcțiilor. Arătați că $f \in C(\mathbb{R})$ este divizor al lui zero dacă și numai dacă există $(a, b) \subseteq \mathbb{R}$ astfel încât $f(x) = 0$ pentru orice $x \in (a, b)$.

  Demonstrație. $\Longrightarrow$ Fie $f\colon \mathbb{R} \to \mathbb{R}$ continuă și divizor al lui zero. Asemenea sub-punctului precedent, trebuie să existe un $x_0 \in \mathbb{R}$ astfel încât $f(x_0) = 0$. Dar deoarece f este continuă, trebuie să fie 0 pe o vecinătate deschisă a lui x_0, și anume $(a, b) \subseteq \mathbb{R}$.

  $\Longleftarrow$ Trebuie să găsim o funcție continuă care înmulțită cu f să fie peste tot 0. Pentru a face acest lucru, funcția va fi 0 în afara lui (a, b), și în (a, b) va fi o parabolă care intersectează O_x în a, respectiv b. Definim $g\colon \mathbb{R} \to \mathbb{R}$ continuă,

  $$g(x) = \begin{cases} (x - a)(x - b), \, x \in (a, b) \\ 0, \text{ altfel} \end{cases}$$

  Atunci $g \neq 0$, dar $f(x)g(x) = 0$, $\forall x \in \mathbb{R}$. Deci f este divizor al lui 0.

  □

Exercițiul (1.17)**.** Arătați că în inelul $M_n(R)$ orice element inversabil la stânga (dreapta) este inversabil la dreapta (stânga).

Demonstrație. Fie $A \in M_n(R)$ o matrice inversabilă la stânga. Atunci există $B \in M_n(R)$ cu $BA = I_n$.

Dacă ne uităm la determinanți, $\det(BA) = \det I_n = 1$, deci atât $\det B$ cât și $\det A$ sunt nenuli.

Avem că

$$B = (BA)B = B(AB)$$

Din $B = B(AB)$ obținem că $B(AB - I_n) = 0_n$. Deoarece $\det B \neq 0$, știm că B nu este divizor al lui zero, deci îl putem simplifica. Rămâne că $AB = I_n$. De aici am obținut că A este inversabilă și la dreapta. □

Exercițiul (1.22)**.** Să se determine elementele nilpotente în inelul $\mathbb{Z}_n$ și să se afle numărul acestora.

Demonstrație. Elementele nilpotente sunt cele pentru care $\exists k \in \mathbb{N}$ astfel încât $\hat{x}^k = \hat{0}$. Deci $n \mid x^k$. Ridicând la putere, nu pot apărea noi factori primi, doar crește puterea celor deja existenți. Deci trebuie ca x să conțină toți factorii primi ai lui n, la puteri mai mici.

Fie descompunerea lui n în m factori primi $n = p_1^{r_1} \cdot \dots \cdot p_m^{r_m}$. Atunci $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_m^{r_m}}$. Nilpotenții din inelul inițial corespund perechilor care conțin nilpotenți în inelele din produs.

În $\mathbb{Z}_{p_i^{r_i}}$ se vede mult mai clar câți nilpotenți avem. Înmulțim cu p_i tot inelul original $\mathbb{Z}_{p_i^{r_i}}$ ca să obținem numere în care apare factorul prim p_i, și obținem un sub inel

$$p_i\mathbb{Z}_{p_i^{r_i}} = p_i(\mathbb{Z}/p_i^{r_i}\mathbb{Z}) = \mathbb{Z}/p_i^{r_i-1}\mathbb{Z} = \mathbb{Z}_{p_i^{r_i-1}}$$

care are $p_i^{r_i-1}$ elemente.

Per total, în $\mathbb{Z}_n$ avem

$$p_1^{r_1-1} \cdot \dots \cdot p_m^{r_m-1} = \frac{p_1^{r_1} \cdot \dots \cdot p_m^{r_m}}{p_1 \cdot \dots \cdot p_m} = \frac{n}{p_1 \cdot \dots \cdot p_m}$$

nilpotenți. □

Exercițiul (1.23)**.** Fie R un inel și $x, y \in R$ elemente nilpotente.

1. Dacă $xy = yx$ atunci xy și $x + y$ sunt nilpotente.

   Demonstrație. Fie $x, y \in R$ nilpotente. Atunci $\exists n, m \in \mathbb{N}^*$ astfel încât $x^n = 0$, $y^m = 0$. Vrem să găsim o putere pentru care atât x și y să fie 0. Alegem $k = \max(n, m)$. Atunci $x^k = y^k = 0$.

   Luăm prima expresie și vedem ce se întâmplă când o ridicăm la k:

   $$(xy)^k = \underbrace{(xy) \dots (xy)}_{\text{k ori}}$$

   Deoarece $xy = yx$ putem să rearanjăm termenii: $(xy)^k = x^k y^k = 0$. Deci xy nilpotent.

   Pentru $x+y$ ne folosim de binomul lui Newton pentru a ridica la putere (avem voie deoarece $xy = yx$). Deoarece vrem ca toți termenii să se

anuleze, nu este suficient să ridicăm la puterea k, ci cel puțin la puterea $2k$. Dezvoltăm $(x+y)^{2k}$ după binomul lui Newton:

$$(x+y)^{2k} = \sum_{i=0}^{2k} \binom{2k}{i} a^{2k-i} b^i$$

Termenii cu i de la 0 până la k se anulează deoarece avem $k-i \geq 0$, putem rescrie $a^{2k-i} = a^k a^{k-i} = 0$, cei de la $k+1$ până la $2k$ se anulează deoarece avem $i-k \geq 0$, putem rescrie $b^i = b^k b^{i-k} = 0$. Deci $x+y$ nilpotent. □

2. Dați exemple care să arate că proprietatea 1 nu mai rămâne adevărată dacă $xy \neq yx$.

Demonstrație. De exemplu, în $M_2(\mathbb{R})$, avem nilpotenții $X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ și $Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, cu $X^2 = Y^2 = \mathbf{0}_2$, care nu comută: $XY \neq YX$. Suma lor nu este nilpotentă: $X+Y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $(X+Y)^2 = \mathbf{I}_2$, $(X+Y)^3 = (X+Y)$. □

Exercițiul (1.27)**.** Fie R un inel boolean. Să se arate că R este comutativ.

Demonstrație. Din definiția inelului boolean, toate elementele sunt idempotente: $x^2 = x$, $\forall x \in R$.

Observăm că avem următoarele identități:

$$\left.\begin{aligned} &x+x = (x+x)^2 = (x+x)(x+x) = x^2+x^2+x^2+x^2 \\ &x+x = (x^2)+(x^2) \end{aligned}\right\} \implies$$
$$\implies x^2+x^2+x^2+x^2 = x^2+x^2$$
$$\implies x^2+x^2 = 0$$
$$\implies x^2 = -x^2$$
$$\implies x = -x, \forall x \in R$$

Deci orice element este propriul său invers la adunare.

Pentru a arăta că acest inel este comutativ, trebuie să obținem cumva că $xy = yx$, $\forall x, y \in R$, folosindu-ne de proprietățile pe care le știm deja.

$$\left.\begin{aligned} &x + y = (x + y)^2 = x^2 + xy + yx + y^2 \\ &x + y = x^2 + y^2 \end{aligned}\right\} \implies$$
$$\implies (x^2 + y^2) + (xy + yx) = x^2 + y^2$$
$$\implies xy + yx = 0$$
$$\implies xy = -yx$$
$$\implies xy = yx$$

□

Exercițiul (1.28)**.**

- Se consideră numărul natural $n \geq 2$ care are r factori primi distincți în descompunerea sa. Să se arate că numărul idempotenților lui $\mathbb{Z}_n$ este 2^r.

  Demonstrație. Descompunem pe n în factori primi, $n = p_1^{q_1} p_2^{q_2} \dots p_r^{q_r}$. Atunci $\mathbb{Z}_n$ este izomorf cu $\mathbb{Z}_{p_1^{q_1}} \times \cdots \times \mathbb{Z}_{p_r^{q_r}}$.

  Singurele elemente idempotente în $\mathbb{Z}_{p_i^{r_i}}$ sunt $\overline{0}$ și $\overline{1}$. Deci idempotentele lui $\mathbb{Z}_n$ corespund prin izomorfism elementelor de forma $(0, \dots, 0, 0)$, $(0, \dots, 0, 1)$, ..., $(1, \dots, 1, 1)$. Există 2^r astfel de r-tupluri.

  Pentru a găsi idempotenții în inelul inițial, construim un sistem de congruențe liniare. De exemplu, pentru $(1, 0, \dots, 0, 1)$ sistemul ar fi:

$$\begin{cases} x \equiv 1 \mod p_1^{q_1} \\ x \equiv 0 \mod p_2^{q_2} \\ \vdots \\ x \equiv 0 \mod p_{r-1}^{q_{r-1}} \\ x \equiv 1 \mod p_r^{q_r} \end{cases}$$

  Din lema chineză a resturilor și din faptul că toți factorii primi sunt numere prime între el, acest sistem sigur are soluții. □

- Să se determine idempotenții inelului $\mathbb{Z}_{36}$.

Demonstrație. Pe baza descompunerii în factori primi avem că

$$\mathbb{Z}_{36} \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2}$$

În inelul produs, avem idempotenții $(\overline{0}, \overline{\overline{0}})$, $(\overline{1}, \overline{\overline{1}})$, $(\overline{0}, \overline{\overline{1}})$ și $(\overline{1}, \overline{\overline{0}})$.

Primii doi idempotenți corespund lui $\hat{0}$, respectiv $\hat{1}$. Pentru a afla corespondenții ultimilor doi idempotenți trebuie să rezolvăm două sisteme de congruențe:

$$\begin{cases} x \equiv 0 \mod 4 \\ x \equiv 1 \mod 9 \end{cases} \qquad \begin{cases} x \equiv 1 \mod 4 \\ x \equiv 0 \mod 9 \end{cases}$$

Soluția primei ecuații este $\widehat{28}$. Putem rezolva și a doua ecuație, sau ne putem folosi de faptul că $\hat{1} - \widehat{28}$ este tot idempotent, de unde obținem că $\widehat{1-28} = \widehat{-27} = \hat{9}$ este cealaltă soluție. □

Exercițiul (1.29)**.** Fie $R = M_2(\mathbb{Z}_2)$.

- Să se determine numărul elementelor lui R.

  Demonstrație. Elementele lui R sunt matrici 2×2 cu elemente din $\mathbb{Z}_2$:

  $$A = \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix} \in R$$

  În R avem $|\mathbb{Z}_2|^4 = 2^4 = 16$ matrici distincte. □

- Să se determine numărul divizorilor lui zero ai lui R.

  Demonstrație. Dacă o matrice are determinantul $\hat{0}$, atunci există un vector nenul astfel încât $Av = 0$, și dacă punem copii ale acestui vector pentru a obține o matrice, obținem că $AB = 0$. Deci este suficient să găsim matricile cu determinant nul.

  Avem 10 matrici cu determinant nul:

  $$\begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{1} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix},$$
  $$\begin{pmatrix} \hat{1} & \hat{1} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{1} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{0} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{1} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix}$$

  □

- Aflați câte elemente nilpotente are R.

  Demonstrație. Pentru ca A să fie nilpotent, trebuie ca $A^k = 0$. Din proprietățile determinantului, obținem că $\det A$ trebuie să fie $\hat{0}$. Putem să plecăm de la lista de divizori ai lui zero / matrici cu determinant nul, și să verificăm fiecare matrice dacă este nilpotentă.

  Obținem 4 nilpotenți:

$$\begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{1} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix}$$

  □

- Aflați câte elemente idempotente are R.

  Demonstrație. Din faptul că vrem ca $A^2 = A$, ajungem la concluzia că fie nu este inversabilă și are determinant zero, fie este inversabilă, și atunci este matricea unitate (deoarece $A^2 = A \iff A^{-1}A^2 = A^{-1}A \iff A = I$).

  Verificând matricile cu determinant nul, obținem 8 idempotenți:

$$\begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix},$$
$$\begin{pmatrix} \hat{1} & \hat{1} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{1} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{0} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{1} & \hat{1} \end{pmatrix}$$

  □

1.2 Subinele. Ideale

Exercițiul (2.7)**.** Fie R_1, R_2 inele unitare $R = R_1 \times R_2$. Să se arate că idealele la stânga (la dreapta, bilaterale) ale lui R sunt de forma $I = I_1 \times I_2$ unde I_1, I_2 sunt ideale la stânga (la dreapta, bilaterale) în R_1, respectiv R_2.

Demonstrație. $\implies$ Presupunem că avem două ideale $I_1 \trianglelefteq R_1$, $I_2 \trianglelefteq R_2$. Trebuie să arătăm că $I_1 \times I_2 = I \trianglelefteq R$.

Avem că $I = I_1 \times I_2 = \{\, (a, b) \in R \mid a \in I_1, b \in I_2 \,\}$.

Arătăm că această mulțime este închisă la adunare:

$$(a, b) + (c, d) = (\underbrace{a + c}_{\in I_1}, \underbrace{b + d}_{\in I_2}) \in I$$

și la înmulțirea cu un element din inel:

$$(m,n)(a,b) = (\underbrace{ma}_{\in I_1}, \underbrace{nb}_{\in I_2}) \in I$$

(ne-am folosit de faptul că I_1 și I_2 sunt ideale în inelele respective, și adunarea/înmulțirea se face pe componente).

Deci I este ideal (la stânga, la dreapta, sau bilateral, în funcție de cum erau I_1 și I_2).

$\Longleftarrow$ Presupunem că avem $I \trianglelefteq R$. Trebuie să arătăm că există două ideale $I_1 \trianglelefteq R_2$, $I_2 \trianglelefteq R_2$ astfel încât $I_1 \times I_2 = I$.

Observație: dacă perechea (a,b) aparține lui I, atunci și perechile $(a,0)$, respectiv $(0,b)$ aparțin idealului: putem să înmulțim (a,b) cu $(1,0)$, respectiv $(0,1)$ (avem voie, I este ideal).

Definim două mulțimi

$$I_1 = \{\, a \in R_1 \mid \exists y \in R_2 \text{ a.î. } (a,y) \in I \,\} \subseteq R_1$$

$$I_2 = \{\, b \in R_2 \mid \exists x \in R_1 \text{ a.î. } (x,b) \in I \,\} \subseteq R_2$$

Vrem să arătăm că acestea sunt ideale în inelele de care aparțin. Se arată ușor prin calcule că sunt închise la adunare. În ceea ce privește închiderea la înmulțirea cu un element din inel:

Fie $r \in R_1$, $a \in I_1$. Pentru ca $ra \in I_1$ trebuie să existe un y' astfel încât $(ra, y') \in I$. Noi știm că $a \in I_1 \implies \exists y$ astfel încât $(a,y) \in I$. Pe baza observației de mai sus, $(a,0) \in I$. Atunci și $(ra,0) \in I$. Deci $y' = 0$ și $ra \in I_1$.

Demonstrația decurge analog pentru I_2, dar interschimbăm componentele.

Mai rămâne de arătat că $I_1 \times I_2 = I$ (prin dublă incluziune):

1. Dacă avem $a \in I_1$, $b \in I_2$, înseamnă că există $x \in I_1, y \in I_2$ astfel încât $(a,y) \in I$ și $(x,b) \in I$, deci sigur $(a,b) \in I$
2. Pentru orice $(a,b) \in I$, avem $a \in I_1$ și $b \in I_2$.

□

1.3 Morfisme de inele

Exercițiul (3.9)**.** Arătați că avem următoarele izomorfisme de grupuri:

- $\text{End}((\mathbb{Z}, +)) \cong \mathbb{Z}$

  Demonstrație. Fie $f \colon \mathbb{Z} \to \mathbb{Z}$ un morfism. Știm că $f(0) = 0$. Notăm $f(1) = a \in \mathbb{Z}$.

  Atunci, pentru un k pozitiv

  $$f(k) = f(\underbrace{1 + \cdots + 1}_{k \text{ ori}}) = f(1) + \cdots + f(1) = k \cdot f(1) = k \cdot a, \forall k > 0$$

  Pentru un k negativ, ne folosim de faptul că pentru orice morfism de grupuri $f(-x) = -f(x)$. Atunci

  $$f(k) = -f(-k) = -k \cdot a, \forall k < 0$$

  Deci $f(k) = k \cdot a, \forall k \in \mathbb{Z}$. Fiecare dintre aceste morfisme este identificat prin valoarea lui a, deci avem câte unul pentru fiecare număr din $\mathbb{Z}$.

  De asemenea, acestea formează un grup în raport cu compunerea. Fie $f_a \colon \mathbb{Z} \to \mathbb{Z}$ morfismul cu $f_a(k) = k \cdot a$, $\forall k \in \mathbb{Z}$. Atunci:

  $$(f_a \circ f_b)(k) = f_a(f_b(k)) = k \cdot ab = f_{ab}$$
  $$f_{-a}(k) = k \cdot (-a) = -k \cdot a = -f_a$$

  Deci $\text{End}((\mathbb{Z}, +)) \cong \mathbb{Z}$. □

- $\text{End}((\mathbb{Q}, +)) \cong \mathbb{Q}$

  Demonstrație. Asemănător cu exercițiul precedent, endomorfismele lui $\mathbb{Q}$ sunt de forma $f_{\frac{p}{q}}(x) = \frac{p}{q}x$. □

- $\text{End}((\mathbb{Z}_n, +)) \cong \mathbb{Z}_n$

  Demonstrație. Asemănător cu exercițiile precedente, endomorfismele sunt de forma $f_{\hat{k}}(\hat{x}) = \hat{k} \cdot \hat{x}$. □

- $\text{End}((\mathbb{Z} \times \mathbb{Z}, +)) \cong M_2(\mathbb{Z})$

Demonstrație. Plecând de la cunoștințele pe care le avem legate de endomorfismele lui $\mathbb{Z}$, putem construi endomorfisme scriind combinații liniare ale celor două componente:

$$f((x,y)) = (ax + by, cx + dy)$$

Dacă scriem fiecare pereche din $\mathbb{Z} \times \mathbb{Z}$ ca un vector coloană, obținem:

$$f(\begin{pmatrix} x \\ y \end{pmatrix}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

□

Exercițiul (3.10)**.** Determinați endomorfismele (și automorfismele) următoarelor inele:

- $(\mathbb{Z}, +, \cdot)$

  Demonstrație. Plecăm de la endomorfismele grupului $(\mathbb{Z}, +)$, și punem condiția și ca $f(a \cdot b) = f(a) \cdot f(b)$, $\forall a, b \in \mathbb{Z}$. Dacă înlocuim cu forma generală a unui morfism pe $\mathbb{Z}$ obținem

  $$k \cdot ab = ka \cdot kb = k^2 \cdot ab$$

  Din $k = k^2$ ajungem la concluzia că singurele endomorfisme de inele sunt morfismul identitate, $f(x) = x$, și morfismul nul, $f(x) = 0$. Dintre acestea, morfismul identitate este și automorfism. □

- $(\mathbb{Q}, +, \cdot)$

  Demonstrație. Asemănător cu exercițiul precedent. □

- $(\mathbb{R}, +, \cdot)$

  Demonstrație. Asemănător cu exercițiile precedente. □

- $(\mathbb{Z}_n, +, \cdot)$

  Demonstrație. Din faptul că vrem ca $\hat{k} = \hat{k}^2$, trebuie ca $\hat{k}$ să fie element idempotent. Deci putem obține un endomorfism diferit pentru fiecare idempotent al lui $\mathbb{Z}_n$. □

- $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$

  Demonstrație. Asemănător exercițiilor precedente, trebuie să căutăm morfisme ale grupului $(\mathbb{Z} \times \mathbb{Z}, +)$ care să se comporte bine și cu înmulțirea.

  Deoarece deja știm că aceste morfisme sunt unic determinate de o matrice din $M_2(\mathbb{Z})$, endomorfismele inelului $\mathbb{Z} \times \mathbb{Z}$ sunt cele care corespund matricilor idempotente. □

Exercițiul (3.11)**.**

- Arătați că există un morfism *unitar* de inele $\mathbb{Z}_m \to \mathbb{Z}_n$ dacă și numai dacă $n \mid m$.

  Demonstrație. Vom nota cu $\hat{a}$ clasele de resturi din $\mathbb{Z}_m$ și cu $\tilde{b}$ clasele de resturi din $\mathbb{Z}_n$.

  Observație: la acest sub-punct contează foarte mult că ne referim numai la morfisme *unitare*. Indiferent de n și m, întotdeauna avem de exemplu morfismul neunitar $f(\hat{x}) = \tilde{0}$.

  $\Longrightarrow$ Fie $f \colon \mathbb{Z}_m \to \mathbb{Z}_n$ morfism unitar de inele. Atunci avem proprietățile:

  $$f(\hat{0}) = \tilde{0} \qquad (f \text{ este morfism de inele})$$
  $$f(\hat{1}) = \tilde{1} \qquad (f \text{ este morfism } \textit{unitar} \text{ de inele})$$

  Acum vedem ce se întâmplă când introducem clasa lui m în morfism:

  $$f(\widehat{m}) = f(\hat{0}) = \tilde{0} \qquad (\text{restul lui } m \text{ la împărțirea cu } m \text{ este } 0)$$
  $$f(\widehat{m}) = f(\underbrace{\hat{1} + \cdots + \hat{1}}_{m \text{ ori}})$$
  $$f(\widehat{m}) = \underbrace{f(\hat{1}) + \cdots + f(\hat{1})}_{m \text{ ori}} = \underbrace{\tilde{1} + \cdots + \tilde{1}}_{m \text{ ori}} = \widetilde{m}$$

  Punând totul la un loc, obținem că $\widetilde{m} = \tilde{0}$. Cu alte cuvinte, m este multiplu de n, deci $n \mid m$.

$\Longleftarrow$ Presupunem că $n \mid m$. Definim $f\colon \mathbb{Z}_m \to \mathbb{Z}_n$, cu legea $f(\hat{x}) = \tilde{\hat{x}} = \tilde{x}$. Cu alte cuvinte, f ia fiecare rest la împărțirea cu m și îi face restul la împărțirea cu n.

Trebuie să arătăm mai întâi că această funcție este bine definită. Indiferent de ce reprezentanți am alege pentru aceeași clasă de resturi, trebuie să ne asigurăm că funcția ia aceeași valoare. Altfel spus, $\forall \hat{x}, \hat{y} \in \mathbb{Z}_m$ cu $\hat{x} = \hat{y}$ și $x \neq y$, vrem ca $f(\hat{x}) = f(\hat{y})$.

$$\left.\begin{array}{l} \hat{x} = \hat{y} \iff m \mid (x-y) \\ n \mid m \end{array}\right\} \implies n \mid (x-y)$$
$$\iff \tilde{x} = \tilde{y}$$
$$\iff f(\hat{x}) = f(\hat{y})$$

Acum trebuie să demonstrăm că f este morfism unitar de inele. Acest lucru se poate face destul de simplu, deoarece "căciula" comută cu operațiile uzuale. Deci $f(\hat{a} + \hat{b}) = f(\widehat{a+b}) = \widetilde{a+b} = \tilde{a} + \tilde{b}$, și analog pentru înmulțire.

□

- Arătați că un morfism de inele $f\colon \mathbb{Z}_m \to \mathbb{Z}_n$ este unic determinat de condițiile: $mf(\hat{1}) = \tilde{0}$ și $f(\hat{1}) = f(\hat{1})^2$.

Demonstrație. Cerința poate fi rescrisă ca $f\colon \mathbb{Z}_m \to \mathbb{Z}_n$ morfism de inele dacă și numai dacă $mf(\hat{1}) = \tilde{0}$ și $f(\hat{1}) = f(\hat{1})^2$.

$\Longrightarrow$ Fie $f\colon \mathbb{Z}_m \to \mathbb{Z}_n$ morfism de inele. Atunci

$$\begin{aligned} & \widehat{m} = \hat{0} \\ \Longrightarrow\ & f(\widehat{m}) = f(\hat{0}) \\ \Longrightarrow\ & f(\hat{1} + \cdots + \hat{1}) = \tilde{0} \\ \Longrightarrow\ & f(\hat{1}) + \cdots + f(\hat{1}) = \tilde{0} \\ \Longrightarrow\ & mf(\hat{1}) = \tilde{0} \end{aligned}$$

Pentru a doua condiție, avem că

$$f(\hat{1}) = f(\hat{1} \cdot \hat{1}) = f(\hat{1}) \cdot f(\hat{1}) = f(\hat{1})^2$$

$\Longleftarrow$ Fie $f\colon \mathbb{Z}_m \to \mathbb{Z}_n$, $f(\hat{k}) = kf(\hat{1})$. Notăm $f(\hat{1}) = \tilde{a}$. Știm că $m\tilde{a} = \tilde{0}$ și $\tilde{a} = \tilde{a}^2$.

Trebuie să arătăm mai întâi că această funcție este bine definită. Fie $\hat{k}, \hat{l} \in \mathbb{Z}_m$ cu $k \neq l$ și $\hat{k} = \hat{l}$. Vrem să arătăm că

$$\begin{aligned} & f(\hat{k}) = f(\hat{l}) \\ \Longleftrightarrow\ & k\tilde{a} = l\tilde{a} \\ \Longleftrightarrow\ & k\tilde{a} - l\tilde{a} = \tilde{0} \\ \Longleftrightarrow\ & (k-l)\tilde{a} = \tilde{0} \end{aligned}$$

Din $\hat{k} = \hat{l}$ avem că $\hat{k} - \hat{l} = \hat{0}$, deci $k - l$ este multiplu de m. Deoarece $m\tilde{a} = \tilde{0}$, avem că $(k-l)\tilde{a} = \tilde{0}$.

Ca să arătăm că este morfism, ne folosim de cealaltă proprietate:

$$\begin{aligned} f(\hat{k} \cdot \hat{l}) &= f(\widehat{k \cdot l}) \\ &= (k \cdot l)\tilde{a} = (k \cdot l)\tilde{a}^2 \qquad \text{(din proprietatea } \tilde{a}^2 = \tilde{a}) \\ &= k\tilde{a} \cdot l\tilde{a} \\ &= f(\hat{k}) \cdot f(\hat{l}) \end{aligned}$$

□

- Să se determine toate morfismele de inele de la $\mathbb{Z}_{12}$ la $\mathbb{Z}_{28}$.

Demonstrație. Fie $f\colon \mathbb{Z}_{12} \to \mathbb{Z}_{28}$. Notăm $f(\hat{1}) = \tilde{a}$. Atunci, conform subpunctului anterior, $\tilde{a}$ trebuie să îndeplinească condițiile:

$$\begin{cases} \tilde{a}^2 = \tilde{a} \\ 12\tilde{a} = \tilde{0} \end{cases}$$

Trebuie să găsim toate $\tilde{a} \in \mathbb{Z}_{28}$ pentru care $\tilde{a}^2 = \tilde{a}$. Cu alte cuvinte, căutăm elementele idempotente.

Avem că $\mathbb{Z}_{28} = \mathbb{Z}_4 \times \mathbb{Z}_7$. Idempotenții corespund perechilor $(\overline{0}, \overline{\overline{0}})$, $(\overline{0}, \overline{\overline{1}})$, $(\overline{1}, \overline{\overline{0}})$ și $(\overline{1}, \overline{\overline{1}})$. Idempotenții lui $\mathbb{Z}_{28}$ sunt $\left\{ \tilde{0}, \tilde{1}, \tilde{8}, \widetilde{21} \right\}$.

Dintre aceștia, doar $\tilde{0}$ și $\widetilde{21}$ îndeplinesc și a doua condiție. Deci singurele morfisme sunt $f(\hat{k}) = \tilde{0}$ și $f(\hat{k}) = \widetilde{21}\tilde{k}$. □

1.4 Inele factor

Exercițiul (4.8)**.** Fie R_1, R_2 inele unitare, $R = R_1 \times R_2$ și $I = I_1 \times I_2$ unde I_1, I_2 sunt ideale bilaterale în R_1, respectiv R_2. Să se arate că inelele R/I și $R_1/I_1 \times R_2/I_2$ sunt izomorfe.

Demonstrație. Se poate rezolva definind $f \colon R/I \to R_1/I_1 \times R_2/I_2$, cu

$$f(\widehat{(a,b)}) = (\overline{a}, \overline{\overline{b}})$$

și demonstrând că această funcție este izomorfism. □

Exercițiul (4.9)**.** Fie R un inel unitar și I ideal bilateral al lui R. Să se arate că inelele $M_2(R)/M_2(I)$ și $M_2(R/I)$ sunt izomorfe.

Demonstrație. Vrem să folosim teorema fundamentală de izomorfism pentru inele. Avem nevoie de un morfism f pentru care $\ker f = M_2(I)$.

- Definim $f \colon M_2(R) \to M_2(R/I)$, $f(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix}, \forall a, b, c, d \in R$.
- Se arătă prin calcule că f este morfism unitar de inele.
- Studiem nucleul morfismului:

$$f(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix} \iff \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix} = \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}$$

$$\iff \begin{cases} \hat{a} = \hat{0} \\ \hat{b} = \hat{0} \\ \hat{c} = \hat{0} \\ \hat{d} = \hat{0} \end{cases} \iff a, b, c, d \in I$$

  Deci $\ker f = M_2(I)$.
- Imaginea lui f este întregul codomeniul $M_2(R/I)$, f este surjectiv.

  Fie $y \in M_2(R/I)$, $y = \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix}$. Atunci luăm $x \in M_2(R)$, $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Se observă că $f(x) = y$.
- Din teorema fundamentală de izomorfism, $M_2(R)/M_2(I) \cong M_2(R/I)$.

□

1.5 Teorema chineză a resturilor pentru ideale

Exercițiul (5.4)**.** Arătați că

- $\mathbb{Q}[X]/(X^2-1) \cong \mathbb{Q} \times \mathbb{Q}$

  Demonstrație. Putem rescrie $\mathbb{Q}[X]/(X^2-1) = \mathbb{Q}[X]/((X-1)(X+1))$.

  Pentru a arăta că $(X-1)$ și $(X+1)$ sunt comaximale, trebuie să arătăm că suma lor generează tot $\mathbb{Q}[X]$. Este suficient să arătăm că suma idealelor conține elementul unitate.

  Observăm că $(X+1)-(X-1) = 2$. Înmulțind cu $\frac{1}{2}$ (avem voie, deoarece lucrăm în $\mathbb{Q}$) obținem 1.

  Putem aplica **Remarca 5.2** din curs, și obținem că

  $$\mathbb{Q}[X]/((X-1)(X+1)) = \mathbb{Q}[X]/((X-1) \cap (X+1))$$

  Acum ne folosim de **Teorema 5.3** din curs. Obținem că

  $$\mathbb{Q}[X]/((X-1) \cap (X+1)) \cong \mathbb{Q}[X]/(X-1) \times \mathbb{Q}[X]/(X+1)$$

  Clasele de echivalență ale lui $\mathbb{Q}[X]/(X-1)$ sunt resturile obținute prin împărțirea oricărui polinom la $X-1$, deci sunt polinoame de grad 0, de forma $\{\, \hat{a} \mid a \in \mathbb{Q} \,\}$, deci $\mathbb{Q}[X]/(X-1) \cong \mathbb{Q}$. Analog pentru $\mathbb{Q}[X]/(X+1) \cong \mathbb{Q}$.

  În concluzie, $\mathbb{Q}[X]/(X^2-1) \cong \mathbb{Q} \times \mathbb{Q}$. □

- $\mathbb{Z}[X]/(X^2-X) \cong \mathbb{Z} \times \mathbb{Z}$

  Demonstrație. Demonstrația decurge asemănător pentru $\mathbb{Z}[X]/(X^2-X)$, cu observația că $X^2-X = X(X-1)$. Sunt comaximale deoarece $X-(X-1) = 1$. □

- $\mathbb{Z}[X]/(X^2-1) \ncong \mathbb{Z} \times \mathbb{Z}$

  Demonstrație. Demonstrația începe la fel ca prima, însă nu mai putem să înmulțim cu $\frac{1}{2}$ deoarece lucrăm în $\mathbb{Z}$, deci nu mai putem folosi această metodă pentru a arăta că sunt izomorfe.

  Presupunem că inelul factor ar fi izomorf cu $\mathbb{Z} \times \mathbb{Z}$. Ne uităm la elementele idempotente ale acestor două inele.

  Observație: deoarece X^2-1 aparține idealului prin care factorizăm, avem că $\widehat{X^2-1} = \hat{0}$, de unde $\widehat{X^2} = \hat{1}$.

– În $\mathbb{Z}[X]/(X^2-1)$, fie $\hat{a}\widehat{X}+\hat{b}$ un idempotent. Atunci

$$\begin{aligned}
&(\hat{a}\widehat{X}+\hat{b})^2 = \hat{a}\widehat{X}+\hat{b}\\
\iff &\hat{a}^2\widehat{X}^2 + \widehat{2ab}\widehat{X} + \hat{b}^2 = \hat{a}\widehat{X}+\hat{b}\\
\iff &\hat{a}^2\cdot\hat{1} + \widehat{2ab}\widehat{X} + \hat{b}^2 = \hat{a}\widehat{X}+\hat{b}\\
\iff &\begin{cases}\widehat{a^2}+\widehat{b^2}=\hat{b}\\ \widehat{2ab}=\hat{a}\end{cases}
\end{aligned}$$

Singura soluție care convine în $\mathbb{Z}$ este $a=0$ și $b\in\{0,1\}$. Deci singurii idempotenți sunt $\hat{0}$ și $\hat{1}$.

– În $\mathbb{Z}\times\mathbb{Z}$, avem idempotenții $(0,0)$, $(0,1)$, $(1,0)$ și $(1,1)$.

Cele două inele nu pot fi izomorfe, având un număr diferit de idempotenți. □

2 Corpuri

2.1 Generalități

Exercițiul (1.4)**.** Orice inel unitar ($1\neq 0$) integru și finit este corp.

Demonstrație. Fie $a\in R$ un element diferit de 0. Trebuie să arătăm că are invers la înmulțire.

Luăm în considerare puterile lui a: a^n, $\forall n\in\mathbb{N}^*$. Inelul fiind finit, acestea nu pot fi toate distincte. La un moment dat trebuie să existe $m\neq n$ pentru care $a^m=a^n$. Să presupunem că $m<n$.

Atunci $a^m-a^n=0 \iff a^m(1-a^{n-m})=0$.

Fiind inel integru, rezultă că $a^m=0$ sau $a^{n-m}-1=0$. Prima posibilitate este exclusă deoarece un inel integru nu are nilpotenți netriviali.

Rămâne deci că $a^{n-m}-1=0 \iff a^{n-m}=1 \iff a\cdot a^{n-m-1}=1$.

Astfel am găsit un invers multiplicativ pentru a, și anume a^{n-m-1}. □

3 Inele de polinoame

3.1 Inele de polinoame într-o nedeterminată

Exercițiul (2.4)**.** Fie R un inel comutativ și unitar, și fie $\alpha\in R$. Atunci $R[X]/(X-\alpha)\cong R$.

Demonstrație. Vrem să ne folosim de teorema fundamentală de izomorfism.

Trebuie să găsim un morfism de inele al cărui nucleu să fie exact idealul generat de $X - \alpha$, iar imaginea acestuia să fie întreg R-ul. Cu alte cuvinte, vrem să avem un morfism $\varphi\colon R[X] \to R$ surjectiv pentru care $\varphi(f) = 0 \iff f$ este multiplu de $X - \alpha, \forall f \in R[X]$. Acesta este chiar morfismul care evaluează polinomul în α: $\varphi(f) = f(\alpha)$.

Morfismul este și surjectiv, deoarece $\forall y \in R$, y este și element în $R[X]$, iar $\varphi(y) = y$. Acum trebuie să îi determinăm nucleul:

$$\begin{aligned}
& f \in \ker \varphi \\
\iff & \varphi(f) = 0 \\
\iff & f(\alpha) = 0 \\
\iff & X - \alpha \mid f && \text{(din Bézout)} \\
\iff & f \text{ multiplu de } X - \alpha \\
\iff & f \in (X - \alpha)
\end{aligned}$$

Deci $\ker \varphi = (X - \alpha)$, $\operatorname{im} \varphi = R$.

Aplicăm teorema fundamentală de izomorfism pentru inele:

$$R[X]/\ker \varphi \cong \operatorname{im} \varphi \iff R[X]/(X - \alpha) \cong R$$

□

3.2 Teorema de împărțire cu rest pentru polinoame într-o nedeterminată

Exercițiul (2.5)**.** Arătați că:

1. $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$

   Demonstrație. Definim $\varphi\colon \mathbb{R}[X] \to \mathbb{C}$, $\varphi(f) = f(i)$, adică funcția care evaluează polinomul în i. Aceasta este morfism unitar de inele.

   Demonstrăm că $\ker \varphi = (X^2 + 1)$ prin dublă incluziune:

   - Dacă f este multiplu de $X^2 + 1$, atunci $f(i) = 0$, deci $f \in \ker \varphi$.
   - Fie $f \in \ker \varphi$.
     $\varphi(f) = 0 \implies f(i) = 0 \implies i$ este o rădăcină a polinomului f
     Deoarece lucrăm cu polinoame cu coeficienți reali, și conjugatul $-i$ este o rădăcină a polinomului f.
     Din Bézout, f se divide prin $X - i$ și prin $X + i$, deci se divide și prin $(X - i)(X + i) = X^2 + 1$.
     Deci $f \in (X^2 + 1)$.

Pentru orice număr complex $z = a + bi$, avem că $\varphi(a + bX) = a + bi$, deci φ este surjectiv. Imaginea lui φ este $\mathbb{C}$.

Aplicăm teorema fundamentală de izomorfism pentru inele și avem că

$$\mathbb{R}[X]/\ker\varphi \cong \operatorname{im}\varphi \iff \mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$$

□

2. $\mathbb{Z}[X]/(X^2-2) \cong \mathbb{Z}[\sqrt{2}]$

Demonstrație. Aplicăm teorema fundamentală de izomorfism pentru

$$\varphi\colon \mathbb{Z}[X] \to \mathbb{Z}[\sqrt{2}]$$

$$\varphi(f) = f(\sqrt{2})$$

□

Exercițiul (2.6)**.** Să se arate că $R = \mathbb{Z}[X]/(2, X^2+1)$ este un inel cu 4 elemente, dar nu este izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Demonstrație. Factorizând prin (2), toți coeficienții polinoamelor sunt înlocuiți cu resturi modulo 2. Deci $\mathbb{Z}[X]/(2, X^2+1) \cong \mathbb{Z}_2[X]/(\widehat{X^2+1})$.

Factorizând mai departe prin $(\widehat{X^2+1})$, clasele de resturi obținute sunt de forma $\hat{a}X + \hat{b}$. De aceea R are $2^2 = 4$ elemente:

$$R = \mathbb{Z}[X]/(2, X^2+1) = \left\{\hat{0}, \hat{1}, \widehat{X}, \widehat{X}+\hat{1}\right\}$$

Pentru a demonstra că nu este izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_2$, ne uităm la numărul de nilpotenți ale acestor inele.

- În R avem $\hat{0}^2 = \hat{0}$ și $(\widehat{X}+\hat{1})^2 = \widehat{X^2} + \hat{2}\widehat{X} + \hat{1} = \hat{0}$.
- În $\mathbb{Z}_2 \times \mathbb{Z}_2$ singurul nilpotent este $(\hat{0}, \hat{0})$.

Deci aceste două inele nu sunt izomorfe. □

Exercițiul (2.7)**.** 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 inel integru.

Demonstrație. Dacă I ar fi ideal principal, atunci ar exista un singur polinom f astfel încât $I = (f)$. Ar însemna că f poate să genereze ambii generatori ai lui I. Deci $f \mid 3$ și $f \mid X^3 - X^2 + 2X + 1$.

Ar rezulta că $f = 1$, deci $I = (f) = \mathbb{Z}[X]$. Însă de exemplu $2 \in \mathbb{Z}[X]$, însă 2 nu poate fi scris ca o combinație liniară de 3 și $X^3 - X^2 + 2X + 1$.

Inelul factor rezultat este izomorf cu $\mathbb{Z}_3[X]/(X^3 - X^2 + \hat{2}X + \hat{1})$.

În inelul obținut, încercăm să scriem $X^3 - X^2 + \hat{2}X + \hat{1}$ (care corespunde lui 0) ca produs de alte polinoame. Avem că

$$(X + \hat{1})(X^2 + X + \hat{1}) = X^3 + \hat{2}X^2 + \hat{2}X + \hat{1} = X^3 - X^2 + \hat{2}X + \hat{1}$$

Deci inelul factor nu este integru, avem cel puțin doi divizori ai lui zero: $X + \hat{1}$ și $X^2 + X + \hat{1}$. □

Exercițiul (2.8)**.** Aflați inversul lui $\widehat{4X + 3}$ în inelul factor $R = \mathbb{Z}_{11}[X]/(X^2 + 1)$.

Demonstrație. Asemănător exercițiilor anterioare ajungem la concluzia că clasa asociată fiecărui polinom din $\mathbb{Z}_{11}[X]$ se poate găsi calculând restul la împărțirea cu $\widehat{X^2 + 1}$:

$$\mathbb{Z}_{11}[X]/(X^2 + 1) = \left\{ \hat{a}\widehat{X} + \hat{b} \;\middle|\; \hat{a}, \hat{b} \in \mathbb{Z}_{11} \right\}$$

Exercițiul ne cere să găsim un invers multiplicativ pentru $\widehat{4X + 3}$, adică un polinom de forma $\widehat{aX + b} \in R$ pentru care

$$(\widehat{4X + 3})(\widehat{aX + b}) = \hat{1} \iff (\hat{4}\widehat{X} + \hat{3})(\hat{a}\widehat{X} + \hat{b}) = \hat{1}$$

Dacă desfacem parantezele avem că

$$\widehat{4a}\widehat{X^2} + \widehat{3a}\widehat{X} + \widehat{4b}\widehat{X} + \widehat{3b} = \hat{1}$$

Deoarece lucrăm cu idealul generat de $X^2 + 1$, știm că $\widehat{X^2 + 1} = \hat{0}$ deoarece $X^2 + 1$ aparține idealului. Observăm că

$$\widehat{X^2 + 1} = \hat{0} \iff \widehat{X^2} + \hat{1} = \hat{0} \iff \widehat{X^2} = \widehat{-1}$$

Putem să rescriem rezultatul să fie de grad cel mult 1:

$$(\widehat{3a} + \widehat{4b})\widehat{X} + (\widehat{-4a} + \widehat{3b}) = \hat{1}$$

În acest moment, găsirea inversului se reduce la rezolvarea sistemului de ecuații

$$\begin{cases} \widehat{3a} + \widehat{4b} = \hat{0} \\ \widehat{-4a} + \widehat{3b} = \hat{1} \end{cases}$$

După calcule ajungem la soluția $\hat{a} = \hat{6}$ și $\hat{b} = \hat{1}$.

Deci inversul lui $\widehat{4X + 3}$ este $\widehat{6X + 1}$. □

3.3 Inele de polinoame într-un număr finit de nedeterminate

Exercițiul (3.9)**.** Fie R un inel comutativ și unitar, și fie $\alpha_1, \dots, \alpha_n \in R$. Atunci $R[X_1, \dots, X_n]/(X_1 - \alpha_1, \dots, X_n - \alpha_n)$ și R sunt izomorfe.

Demonstrație. Demonstrația decurge similar ca la exercițiul 2.4, dar vom defini $\varphi(f) = f(\alpha_1, \dots, \alpha_n)$, și ne folosim de proprietatea de universalitate a inelelor de polinoame într-un număr finit de nedeterminate. □

3.4 Polinoame simetrice

Exercițiul (4.19)**.** Să se arate că următoarele polinoame sunt simetrice și să se scrie fiecare dintre ele ca polinom de polinoame simetrice fundamentale:

1. $X_1^3X_2 + X_1^3X_3 + X_1X_2^3 + X_1X_3^3 + X_2^3X_3 + X_2X_3^3$

   Demonstrație. Notăm cu f polinomul din enunț. Pentru a arăta că este simetric, este suficient să verificăm că rămâne la fel dacă permutăm necunoscutele cu transpozițiile $(1, 2)$ și $(2, 3)$.

   $$f(X_2, X_1, X_3) = X_2^3X_1 + X_2^3X_3 + X_2X_1^3 + X_2X_3^3 + X_1^3X_3 + X_1X_3^3 = f$$

   $$f(X_1, X_3, X_2) = X_1^3X_3 + X_1^3X_2 + X_1X_3^3 + X_1X_2^3 + X_3^3X_2 + X_3X_2^3 = f$$

   Îl descompunem în polinom de polinoame simetrice fundamentale folosind algoritmul lui Newton.

   Polinoamele simetrice în 3 necunoscute sunt

   $$\begin{aligned} s_1 &= X_1 + X_2 + X_3 \\ s_2 &= X_1X_2 + X_1X_3 + X_2X_3 \\ s_3 &= X_1X_2X_3 \end{aligned}$$

   Termenul principal (primul în ordine lexicografică) este $X_1^3X_2$. Acesta este de grad 4 și are coeficientul 1. Scriem toate monoamele de grad 4 cu exponenții necunoscutelor descrescători, și le ordonăm lexicografic:

   $$\underbrace{X_1^3X_2}_{(3,1,0)} > \underbrace{X_1^2X_2^2}_{(2,2,0)} > \underbrace{X_1^2X_2X_3}_{(2,1,1)}$$

   Trebuie să obținem aceste monoame din produse de polinoame simetrice. Notăm coeficienții acestor polinoame simetrice cu a, b:

   $$f = s_1^2s_2 + as_2^2 + bs_1s_3$$

Acum putem să dăm valori convenabile lui X_1, X_2, X_3, astfel încât polinomul să fie 0, și să se anuleze unele dintre polinoamele simetrice fundamentale.

- Pentru $X_1 = 1, X_2 = -1, X_3 = 0$ avem $f = -2$ și $s_1 = 0, s_2 = -1, s_3 = 0$. Atunci $a(-1)^2 = -2 \iff \boxed{\text{a = -2}}$.
- Pentru $X_1 = 1, X_2 = 1, X_3 = 1$ avem $f = 6$ și $s_1 = 3, s_2 = 3, s_3 = 1$. Atunci $3^2 \cdot 3 - 2 \cdot 3^2 + b \cdot 3 \cdot 1 = 6 \iff 3b = -3 \iff \boxed{\text{b = -1}}$.

Deci $f = s_1^2 s_2 - 2s_2^2 - s_1 s_3$. □

2. $(X_1^2 + X_2^2)(X_1^2 + X_3^2)(X_2^2 + X_3^2)$

Demonstrație. Notăm polinomul dat cu f. Vedem ce se întâmplă când îl permutăm cu transpozițiile $(1, 2)$ și $(2, 3)$:

$$f(X_2, X_1, X_3) = (X_2^2 + X_1^2)(X_2^2 + X_3^2)(X_1^2 + X_3^2) = f$$

$$f(X_1, X_3, X_2) = (X_1^2 + X_3^2)(X_1^2 + X_2^2)(X_3^2 + X_2^2) = f$$

Deci f este polinom simetric.

Termenii pe care îi putem obține dacă desfacem parantezele o să fie de grad cel mult 6, iar $X_1^4 X_2^2$ este primul lexicografic. Monoamele de grad 6 ar veni, în ordine:

$$(4, 2, 0) > (4, 1, 1) > (3, 3, 0) > (3, 2, 1) > (2, 2, 2)$$

Care ar corespunde lui

$$f = s_1^2 s_2^2 + a s_1^3 s_3 + b s_2^3 + c s_1 s_2 s_3 + d s_3^2$$

- Pentru $X_1 = 1, X_2 = i, X_3 = 0$ avem $f = 0$ și $s_1 = 1 + i, s_2 = i, s_3 = 0$. Atunci $(1 + i)^2 \cdot (i^2) + b \cdot (i^3) = 0 \iff -2i - bi = 0 \iff \boxed{\text{b = -2}}$.
- Pentru $X_1 = 2, X_2 = -1, X_3 = -1$ avem $f = 50$ și $s_1 = 0, s_2 = -3, s_3 = 2$. Atunci $-2 \cdot (-3)^3 + d \cdot 2^2 = 50 \iff 54 + 4d = 50 \iff \boxed{\text{d = -1}}$.
- Pentru $X_1 = 2, X_2 = 2, X_3 = -1$ avem $f = 200$ și $s_1 = 3, s_2 = 0, s_3 = -4$. Atunci $a \cdot 3^3 \cdot (-4) - (-4)^2 = 200 \iff -108a = 216 \iff \boxed{\text{a = -2}}$.

- Pentru $X_1 = 1, X_2 = i, X_3 = -i$ avem $f = 0$ și $s_1 = 1, s_2 = 1, s_3 = 1$. Atunci $1 - 2 - 2 + c - 1 = 0 \iff \boxed{c = 4}$.

Deci $f = s_1^2 s2^2 - 2s_1^3 s_3 - 2s_2^3 + 4s_1 s_2 s_3 - s_3^2$. □

Exercițiul (4.22)**.** Să se calculeze:

1. $x_1^5 + x_2^5 + x_3^5$, unde x_1, x_2, x_3 sunt rădăcinile polinomului $X^3 - 3X + 1$.

Demonstrație. Dacă x_i este una dintre rădăcinile polinomului, atunci

$$x_i^3 - 3x_i + 1 = 0 \iff x_i^3 = 3x_i - 1$$

Înlocuind, expresia care trebuie calculată devine

$$\begin{gathered} x_1^2 x_1^3 + x_2^2 x_2^3 + x_3^2 x_3^3 \\ = x_1^2(3x_1 - 1) + x_2^2(3x_2 - 1) + x_3^2(3x_3 - 1) \\ = 3x_1^3 - x_1^2 + 3x_2^3 - x_2^2 + 3x_3^3 - x_3^2 \\ = 3(3x_1 - 1) + 3(3x_2 - 1) + 3(3x_3 - 1) - (x_1^2 + x_2^2 + x_3^2) \\ = (9x_1 - 3) + (9x_2 - 3) + (9x_3 - 3) - (x_1^2 + x_2^2 + x_3^2) \\ = 9(x_1 + x_2 + x_3) - 9 - (x_1^2 + x_2^2 + x_3^2) \end{gathered}$$

Din relațiile lui Viète avem $x_1 + x_2 + x_3 = 0$, $x_1x_2 + x_2x_3 + x_1x_3 = -3$ și

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_1x_3) = 6$$

Valoarea expresiei $x_1^5 + x_2^5 + x_3^5$ este $9 * 0 - 9 - 6 = -15$. □

2. $x_1^3 + x_2^3 + x_3^3 + x_4^3$, unde x_1, x_2, x_3, x_4 sunt rădăcinile polinomului $X^4 + X^3 + 2X^2 + X + 1$.

Exercițiul (4.23)**.** Considerăm elementele $x_1, \dots, x_n \in \mathbb{C}$ cu proprietatea că $x_1^k + \cdots + x_n^k = 0, \forall k \in \overline{1, n}$. Arătați că $x_1 = \cdots = x_n = 0$.

Demonstrație. În cele ce urmează notăm cu s_i polinoamele simetrice fundamentale. Încercăm să vedem ce obținem dacă îi dăm diferite valori lui k.

Pentru $k = 1$ avem că $x_1 + \cdots + x_n = 0 \iff s_1 = 0$.

Pentru $k = 2$ obținem

$$\begin{aligned} & x_1^2 + \cdots + x_n^2 = 0 \\ \iff & (\underbrace{x_1 + \cdots + x_n}_{=0 \text{ din } k=1})^2 - 2(x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n) = 0 \\ \iff & x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n = 0 \\ \iff & s_2 = 0 \end{aligned}$$

Prin inducție, putem demonstra că $s_i = 0, \forall i \in \overline{1,n}$. Din relațiile lui Viète obținem că $x_1 = x_2 = \cdots = x_n = 0$. □

Exercițiul (4.24)**.** Să se rezolve în $\mathbb{R}$ ecuația $\sqrt[4]{97 - x} + \sqrt[4]{x} = 5$.

Demonstrație. **Condiții de existență.** Observăm că numerele de sub radicalul de ordin 4 trebuie să fie pozitive. Deci pentru început $0 \leq x \leq 97$.

Fie $t = \sqrt[4]{x}$. Atunci ecuația devine:

$$\begin{aligned} & \sqrt[4]{97 - t^4} + t = 5 \\ \iff & \sqrt[4]{97 - t^4} = 5 - t && \text{Condiție de existență: } t \leq 5 \\ \iff & 97 - t^4 = t^4 - 20t^3 + 150t^2 - 500t + 625 \\ \iff & 2t^4 - 20t^3 + 150t^2 - 500t + 528 = 0 \\ \iff & t^4 - 10t^3 + 75t^2 - 250t + 264 = 0 \end{aligned}$$

În acest moment, știm că dacă acest polinom are soluții reale, acestea sunt în intervalul $t \in [0, 5]$. Prin încercări, găsim soluțiile $t = 2$ și $t = 3$. Dacă factorizăm polinomul la $t - 2$ și la $t - 3$ obținem:

$$(t - 2)(t - 3)(t^2 - 5t + 44) = 0$$

Calculând Δ pentru polinomul de grad 2 rămas, observăm că este negativ, deci nu mai avem alte soluții în $\mathbb{R}$.

Scoatem x din t și avem soluțiile $x = 16$, respectiv $x = 81$. □

Exercițiul (4.25)**.** Să se rezolve în $\mathbb{R}$ sistemul de ecuații

$$\begin{cases} x + y = 3 \\ x^5 + y^5 = 33 \end{cases}$$

Demonstrație. Toate polinoamele care apar în acest sistem sunt simetrice. O să le descompunem în polinoame simetrice fundamentale.

Notăm polinoamele simetrice fundamentale în două necunoscute cu $S = x + y$, $P = xy$.

Din prima ecuație avem că $x + y = 3 \implies S = 3$.
Încercăm să descompunem $x^5 + y^5$:

$$\begin{aligned} x^5 + y^5 &= \underline{(x+y)}^5 - (5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4) \\ &= S^5 - 5\underline{xy}(x^3 + 2x^2y + 2xy^2 + y^3) \\ &= S^5 - 5P(\underline{(x+y)}^3 - (x^2y + xy^2)) \\ &= S^5 - 5P(S^3 - \underline{xy}\underline{(x+y)}) \\ &= S^5 - 5P(S^3 - PS) \end{aligned}$$

Sistemul devine:

$$\begin{aligned} &\begin{cases} S = 3 \\ S^5 - 5P(S^3 - PS) = 33 \end{cases} \\ &\iff 3^5 - 5P(3^3 - 3P) = 33 \\ &\iff 243 - 5P(27 - 3P) = 33 \\ &\iff 5P^2 - 45P + 70 = 0 \\ &\iff P \in \{ 2, 7 \} \end{aligned}$$

Acum trebuie să găsim două numere reale care să aibă suma egală cu 3 și produsul egal cu 2 (respectiv, suma 3 și produsul 7). Putem să le ghicim, sau putem să aplicăm invers relațiile lui Viète.

Numerele care au suma S și produsul P sunt soluțiile ecuației $x^2 - Sx + P = 0$.

$$x^2 - 3x + 2 = 0 \iff x \in \{ 1, 2 \}$$

$$x^2 - 3x + 7 = 0 \iff \text{nu are soluții pe } \mathbb{R}$$

Deci soluțiile găsite sunt $(x = 1, y = 2)$ și $(x = 2, y = 1)$.

(Sistemul fiind simetric, dacă (a, b) este soluție, atunci și (b, a) este soluție) □

4 Aritmetica în $\mathbb{Z}$ și $K[X]$

4.1 Divizibilitate. Algoritmul lui Euclid

Exercițiul (1.15)**.** Calculați $(24, 54)$ în $\mathbb{Z}$ cu algoritmul lui Euclid.

Demonstrație. Împărțim cu rest pe 54 la 24 (dacă am urma exact algoritmul ar trebui să împărțim pe 24 la 54 mai întâi, dar apoi tot la pasul acesta ajungem):

$$54 = 24 \cdot 2 + 6$$

Acum împărțim cu rest pe 24 la 6:

$$24 = 6 \cdot 4 + 0$$

Deoarece restul obținut este 0, algoritmul se termină. În concluzie, un c.m.m.d.c. al lui 24 și 54 este 6. □

Exercițiul (1.16)**.** Calculați $(X^4 - 4X^3 + 1, X^3 - 3X^2 + 1)$ în $\mathbb{R}[X]$ cu algoritmul lui Euclid.

Demonstrație. Notăm $f = X^4 - 4X^3 + 1$, $g = X^3 - 3X^2 + 1$. Împărțim cu rest pe f la g:

$$\begin{array}{rr} X^4 - 4X^3 & +1 \\ \hline -X^4 + 3X^3 & -X \\ \hline -X^3 & -X+1 \\ X^3 - 3X^2 & +1 \\ \hline -3X^2 & -X+2 \end{array} \quad = \left(X^3 - 3X^2 + 1\right)\left(X - 1\right) - 3X^2 - X + 2$$

Deci $f = (X-1)g + (-3X^2 - X + 2)$. Notăm $r_1 = -3X^2 - X + 2$. Acum împărțim cu rest pe g la r_1:

$$\begin{array}{rr} X^3 - 3X^2 & +1 \\ \hline -X^3 - \frac{1}{3}X^2 & +\frac{2}{3}X \\ \hline -\frac{10}{3}X^2 & +\frac{2}{3}X+1 \\ \frac{10}{3}X^2 + \frac{10}{9}X & -\frac{20}{9} \\ \hline \frac{16}{9}X & -\frac{11}{9} \end{array} \quad = \left(-3X^2 - X + 2\right)\left(-\tfrac{1}{3}X + \tfrac{10}{9}\right) + \tfrac{16}{9}X - \tfrac{11}{9}$$

Deci $g = \left(-\frac{1}{3}X + \frac{10}{9}\right) r_1 + \left(\frac{16}{9}X - \frac{11}{9}\right)$.

Dacă înmulțim un polinom cu un element inversabil din inelul de coeficienți, noul polinom este asociat în divizibilitate cu cel precedent. Deci o să înmulțim cu numitorul comun (care este inversabil, deoarece lucrăm în $\mathbb{R}$) și notăm $r_2 = 16X - 11$ pentru a simplifica calculele.

Împărțim cu rest pe r_1 la r_2:

$$\begin{array}{rr} -3X^2 & -X+2 \\ \hline 3X^2 - \frac{33}{16}X & \\ \hline -\frac{49}{16}X & +2 \\ \frac{49}{16}X - \frac{539}{256} & \\ \hline -\frac{27}{256} & \end{array} \quad = \left(16X - 11\right)\left(-\tfrac{3}{16}X - \tfrac{49}{256}\right) - \tfrac{27}{256}$$

Deci $r_1 = \left(-\frac{3}{16}X - \frac{49}{256}\right) r_2 + \left(-\frac{27}{256}\right)$. O să înmulțim restul obținut cu $-\frac{256}{27}$. Notăm $r_3 = 1$.

Împărțim cu rest pe r_2 la r_3:

$$\begin{array}{r} 16X-11 = 1\cdot\big(16X-11\big) \\ \underline{-\,16X} \\ -\,11 \\ \underline{\quad 11} \\ 0 \end{array}$$

De unde rezultă $r_2 = 1 \cdot r_3 + 0$. Ultimul rest nenul este 1, deci cele două polinoame sunt prime între ele: $(X^4 - 4X^3 + 1, X^3 - 3X^2 + 1) = 1$. □

Exercițiul (1.22)**.** Determinați $(X^2 - 1)\mathbb{Q}[X] \cap (X^3 - 1)\mathbb{Q}[X]$ și $(X^2 - 1)\mathbb{Q}[X] + (X^3 - 1)\mathbb{Q}[X]$.

Demonstrație. Ne folosim de proprietățile din curs: intersecția a două ideale generate de un singur element este idealul generat de c.m.m.m.c.-ul al celor două elemente, respectiv pentru adunare de c.m.m.d.c.-ul celor două elemente.

Pentru a fi mai ușor să găsim c.m.m.d.c.-ul și c.m.m.m.c.-ul, descompunem polinoamele în factori ireductibili din $\mathbb{Q}[X]$:

$$X^2 - 1 = (X - 1)(X + 1)$$
$$X^3 - 1 = (X - 1)(X^2 + X + 1)$$

Obținem $[X^2-1, X^3-1] = (X-1)(X+1)(X^2+X+1)$ și $(X^2-1, X^3-1) = X - 1$.

Deci

$$(X^2 - 1)\mathbb{Q}[X] \cap (X^3 - 1)\mathbb{Q}[X] = ((X - 1)(X + 1)(X^2 + X + 1))\mathbb{Q}[X]$$
$$(X^2 - 1)\mathbb{Q}[X] + (X^3 - 1)\mathbb{Q}[X] = (X - 1)\mathbb{Q}[X]$$

□

4.2 Elemente prime. Elemente ireductibile

Exercițiul (2.10)**.** Determinați polinoamele ireductibile de grad ≤ 5 din $\mathbb{Z}_2[X]$.

Demonstrație. Sunt cel mult $2^6 = 64$ polinoame de grad ≤ 5 în $\mathbb{Z}_2[X]$. Ca să nu fie nevoie să le încercăm pe toate, facem câteva observații ajutătoare:

1. Polinoamele de grad ≤ 1 sunt sigur ireductibile: $\hat{0}, \hat{1}, \widehat{X}, \widehat{X+1}$.

2. Polinoamele de grad ≥ 2 care nu au un termen liber $\hat{1}$ sunt sigur reductibile, pentru că se divid prin $\widehat{X}$.

3. Dacă un polinom are rădăcina α, atunci sigur este reductibil (din Bézout, se divide prin $X - \alpha$). Deoarece lucrăm în $\mathbb{Z}_2$, este suficient să încercăm să înlocuim X cu $\hat{0}$ și $\hat{1}$.

4. Pentru că $\mathbb{Z}_2$ este corp de caracteristică 2 (deoarece $\hat{1} + \hat{1} = \hat{0}$), avem că $(a+b)^2 = a^2 + b^2$ (sau mai general, $(\sum x)^2 = \sum(x^2)$).

   Deci orice polinom din $\mathbb{Z}_2[X]$ cu toate monoamele de grad par este reductibil. De exemplu, $X^4 + X^2 + \hat{1} = (X^2 + X + \hat{1})^2$.

5. În $\mathbb{Z}_2[X]$, dacă suma coeficienților unui polinom este un număr par, atunci acel polinom sigur are rădăcina $\hat{1}$, deci este reductibil.

6. Pe măsură ce construim lista, dacă observăm că un polinom este egal cu produsul altor polinoame deja scrise, atunci este reductibil.

Lista polinoamelor ireductibile de grad ≤ 5 din $\mathbb{Z}_2[X]$:

- Grad ≤ 1: 0, 1, X, $X+1$
- Grad 2: $X^2 + X + 1$
- Grad 3: $X^3 + X^2 + 1$, $X^3 + X + 1$
- Grad 4: $X^4 + X^3 + X^2 + X + 1$, $X^4 + X^3 + 1$, $X^4 + X + 1$
- Grad 5: $X^5 + X^2 + 1, X^5 + X^3 + 1, X^5 + X^3 + X^2 + X + 1, X^5 + X^4 + X^2 + X + 1, X^5 + X^4 + X^3 + X + 1, X^5 + X^4 + X^3 + X^2 + 1$

□

Exercițiul (2.11)**.** Descompuneți polinomul $f = X^{56} - X^{49} - X^7 + \hat{1}$ în produs de polinoame ireductibile în $\mathbb{Z}_7[X]$.

Demonstrație. Notăm $Y = X^7$. Polinomul inițial este $f = Y^8 - Y^7 - Y + \hat{1}$.

Observăm că $\hat{1}$ este o rădăcină (multiplă) a polinomului. Tot împărțim prin $Y - \hat{1}$ și obținem:

$$\begin{aligned}
f &= Y^8 - Y^7 - Y + 1 \\
&= (Y - \hat{1})(Y^7 - \hat{1}) \\
&= (Y - \hat{1})^2(Y^6 + Y^5 + Y^4 + Y^3 + Y^2 + Y + \hat{1}) \\
&= (Y - \hat{1})^3(Y^5 + \hat{2}Y^4 + \hat{3}Y^3 + \hat{4}Y^2 + \hat{5}Y - \hat{1}) \\
&= (Y - \hat{1})^4(Y^4 + \hat{3}Y^3 + \hat{6}Y^2 + \hat{3}Y + \hat{1}) \\
&= (Y - \hat{1})^5(Y^3 + \hat{4}Y^2 + \hat{3}Y - \hat{1}) \\
&= (Y - \hat{1})^6(Y^2 + \hat{5}Y + \hat{1}) \\
&= (Y - \hat{1})^7(Y - \hat{1}) \\
&= (Y - \hat{1})^8
\end{aligned}$$

Deci polinomul inițial este $f = (Y - \hat{1})^8 = (X^7 - \hat{1})^8$. Pe baza calculelor deja efectuate pentru Y, acesta este egal cu $((X - \hat{1})^7)^8 = (X - \hat{1})^{56}$. □

Exercițiul (2.17)**.** Determinați c.m.m.d.c. și c.m.m.m.c. pentru polinoamele $f = (X-1)(X^2-1)(X^3-1)(X^4-1)$ și $g = (X+1)(X^2+1)(X^3+1)(X^4+1)$ din $\mathbb{Q}[X]$.

Demonstrație. Deoarece polinoamele sunt deja scrise ca produs de alte polinoame, începem prin a descompune cele două polinoame în produs de factori ireductibili peste $\mathbb{Q}[X]$. Avem că

$$\begin{aligned}
f &= (X-1)(X-1)(X+1)(X-1)(X^2+X+1)(X-1)(X+1)(X^2+1) \\
&= (X-1)^3(X+1)^2(X^2+1)(X^2+X+1) \\
g &= (X+1)(X^2+1)(X^3+1)(X^4+1)
\end{aligned}$$

Pentru a găsi c.m.m.d.c.-ul, luăm toți factorii primi comuni la puterea cea mai mică.

$$(f, g) = (X+1)(X^2+1)$$

Pentru c.m.m.m.c., luăm toți factorii primi o singură dată, la puterea cea mai mare.

$$[f, g] = (X-1)^3(X+1)^2(X^2+1)(X^3+1)(X^2+X+1)(X^4+1)$$

□

4.3 Teorema fundamentală a algebrei

Exercițiul (3.7)**.** Arătați că polinomul X^n-2 este ireductibil în $\mathbb{Q}[X]$ pentru orice $n \geq 1$.

Demonstrație.

- Pentru $n = 1$, $X - 2$ este polinom de grad 1, deci ireductibil.
- Pentru $n = 2$, rădăcinile polinomului sunt $\pm\sqrt{2}$, care nu aparțin lui $\mathbb{Q}$, deci polinomul este ireductibil.
- Pentru $n \geq 3$, facem observația că polinomul este reductibil peste $\mathbb{C}[X]$, soluțiile fiind rădăcinile de ordin n ale lui 2. Deci $X^n - 2$ mai poate fi scris ca
$$X^n - 2 = (X - \varepsilon_0) \dots (X - \varepsilon_{n-1})$$
unde $\varepsilon_k = \sqrt[n]{2}(\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n})$. De aici rezultă că $(-1)^n \cdot \varepsilon_0 \cdot \dots \cdot \varepsilon_n = -2$.

  Să presupunem că putem scrie $X^n - 2$ ca produs de polinoame ireductibile peste $\mathbb{Q}[X]$:
$$X^n - 2 = (X^{k_1} + \dots + a_1) \dots (X^{k_r} + \dots + a_r)$$
  Toate aceste polinoame trebuie să fie de grad cel puțin 2, pentru că rădăcinile polinomului nu sunt numere raționale.

  Dacă egalăm cele două descompuneri, și ne uităm la termenii liberi care apar când calculăm produse dintre unii termeni, am obține că un produs de numere raționale $a_{i_1} \dots a_{i_p}$ este egal cu un produs de numere complexe $\varepsilon_{j_1} \dots \varepsilon_{j_r}$. Deci polinomul nu poate fi descompus peste $\mathbb{Q}$.

□

Exercițiul (3.8)**.** Descompuneți polinomul $X^n - 1, 1 \leq n \leq 6$, în produs de polinoame ireductibile în $\mathbb{Q}[X]$, $\mathbb{R}[X]$, respectiv $\mathbb{C}[X]$.

Demonstrație.

- Pentru $n = 1$, polinomul $X - 1$ este deja ireductibil, fiind de grad 1.
- Pentru $n = 2$, polinomul $X^2 - 1$ se descompune ca $(X - 1)(X + 1)$.
- Pentru $n = 3$, polinomul $X^3 - 1$ se descompune ca $(X-1)(X^2+X+1)$. Peste $\mathbb{Q}$ și $\mathbb{R}$, factorul $X^2 + X + 1$ este ireductibil, fiind de gradul 2, cu $\Delta < 0$.

  Peste $\mathbb{C}$, descompunerea completă este $(X - 1)(X - e^{i\frac{2\pi}{3}})(X - e^{i\frac{2\pi}{3}})$.

- Pentru $n = 4$, polinomul $X^4 - 1$ se descompune ca $(X^2 - 1)(X^2 + 1) = (X - 1)(X + 1)(X^2 + 1)$. Aceasta este descompunerea în factori ireductibili peste $\mathbb{Q}$ și $\mathbb{R}$.

  Peste $\mathbb{C}$ polinomul se descompune ca $(X - 1)(X + 1)(X - i)(X + i)$.

- Pentru $n = 5$, polinomul $X^5 - 1$ se descompune ca $(X - 1)(X^4 + X^3 + X^2 + X + 1)$. Această descompunere este ireductibilă peste $\mathbb{Q}$.

  Peste $\mathbb{R}$ mai putem descompune polinomul în $(X - 1)(X^2 + \frac{1-\sqrt{5}}{2}X + 1)(X^2 + \frac{1+\sqrt{5}}{2}X + 1)$.

  Peste $\mathbb{C}$ polinomul se descompune complet în $(X - \varepsilon_0) \dots (X - \varepsilon_4)$, unde $\varepsilon_k = \cos\frac{2k\pi}{5} + i \sin\frac{2k\pi}{5}$.

- Pentru $n = 6$, putem scrie $X^6 - 1$ ca $(X^3 - 1)(X^3 + 1)$. Deja am analizat descompunerea lui $X^3 - 1$.

  În ceea ce privește $X^3 + 1$, acest polinom se descompune în $(X + 1)(X^2 - X + 1)$. Aceasta este descompunerea finală peste $\mathbb{Q}$ și $\mathbb{R}$, dar peste $\mathbb{C}$ mai putem descompune $X^2 - X + 1$ în $(X - \varepsilon_1)(X - \varepsilon_2)$, unde $\varepsilon_k = -(\cos\frac{2k\pi}{3} + i \sin\frac{2k\pi}{3})$.

□

4.4 Teorema chineză a resturilor

Exercițiul (4.1)**.** Să se afle cea mai mică soluție pozitivă a sistemului de congruențe

$$\begin{cases} x \equiv 5 \mod 18 \\ x \equiv 27 \mod 35 \end{cases}$$

Demonstrație. Deoarece 18 și 35 sunt prime între ele, putem aplica teorema chineză a resturilor. Începem prin a găsi inversul modular al lui 18 în $\mathbb{Z}_{35}$, respectiv al lui 35 în $\mathbb{Z}_{18}$ (putem face asta folosind algoritmul lui Euclid extins):

$$\begin{cases} 18 \cdot 2 \equiv 1 \mod 35 \\ 35 \cdot 17 \equiv 1 \mod 18 \end{cases}$$

Atunci $x = 27 \cdot (18 \cdot 2) + 5 \cdot (35 \cdot 17)$ este o soluție pozitivă a sistemului. Pentru a găsi cea mai mică soluție pozitivă, calculăm restul împărțirii lui x la $18 \cdot 35$:

$$27 \cdot (18 \cdot 2) + 5 \cdot (35 \cdot 17) \equiv 167 \mod 18 \cdot 35$$

Verificare:

$$\begin{cases} 167 & \equiv 5 \mod 18 \\ 167 & \equiv 27 \mod 35 \end{cases}$$

□

Exercițiul (4.2)**.** Rezolvați sistemul de congruențe

$$\begin{cases} 6x \equiv 2 \mod 8 \\ 5x \equiv 5 \mod 6 \end{cases}$$

Demonstrație. Deoarece 8 și 6 nu sunt prime între ele, nu putem aplica teorema chineză a resturilor. Încercăm să mai simplificăm sistemul pentru a găsi o soluție manual.

În prima ecuație putem simplifica cu 2:

$$\begin{cases} 3x \equiv 1 \mod 4 \\ 5x \equiv 5 \mod 6 \end{cases}$$

Putem înmulți prima ecuație cu inversul modulo 4 al lui 3, și a doua ecuație cu inversul modulo 6 al lui 5. Sistemul devine:

$$\begin{cases} x \equiv 3 \mod 4 \\ x \equiv 1 \mod 6 \end{cases}$$

Trebuie să găsim soluția care este de forma $x = 4p + 3 = 6q + 1$ pentru un $p, q \in \mathbb{Z}$. De asemenea, este suficient să căutăm soluția printre numerele cuprinse între 0 și $4 \cdot 6 = 24$.

Observăm că 19 este o soluție:

$$\begin{cases} 19 \equiv 3 \mod 4 \\ 19 \equiv 1 \mod 6 \end{cases}$$

De asemenea, toate numerele de forma $24k + 19, \forall k \in \mathbb{Z}$ sunt soluții. □

5 Algebră liniară

Exercițiile alese de domnul profesor sunt din cartea "Algebra 1" de Tiberiu Dumitrescu, disponibilă pe internet.

5.1 Determinanți

Exercițiul (176)**.** Fie x_1, x_2, x_3 rădăcinile ecuației $x^3+px+q=0$. Calculați Δ^2 în funcție de p și q, unde

$$\Delta = \begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{vmatrix}$$

Demonstrație. Putem să dezvoltăm Δ ca un determinant Vandermonde, și astfel trebuie să calculăm $(x_2-x_1)^2(x_3-x_1)^2(x_3-x_2)^2$. Acesta este un polinom simetric, deci poate fi scris în funcție de polinoamele simetrice fundamentale s_1, s_2, s_3, pe care apoi le exprimăm în funcție de p și q.

Altfel, putem să ne folosim de faptul că $\det A = \det A^\top$, de unde

$$(\det A) \cdot (\det A^\top) = (\det A) \cdot (\det A) = (\det A)^2$$

Deci

$$\begin{aligned} \Delta^2 &= \det \left(\begin{pmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{pmatrix} \cdot \begin{pmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{pmatrix} \right) \\ &= \begin{vmatrix} 3 & x_1+x_2+x_3 & x_1^2+x_2^2+x_3^2 \\ x_1+x_2+x_3 & x_1^2+x_2^2+x_3^2 & x_1^3+x_2^3+x_3^3 \\ x_1^2+x_2^2+x_3^2 & x_1^3+x_2^3+x_3^3 & x_1^4+x_2^4+x_3^4 \end{vmatrix} \end{aligned}$$

Acum trebuie să obținem unele dintre aceste expresii în funcție de p și q.

$$\begin{aligned} x_1+x_2+x_3 &= 0 \\ x_1x_2+x_1x_3+x_2x_3 &= p \\ x_1x_2x_3 &= -q \\ x_1^2+x_2^2+x_3^2 &= -2p \\ x_1^3+x_2^3+x_3^3 &= -3q \\ x_1^4+x_2^4+x_3^4 &= 2p^2 \end{aligned}$$

Determinantul devine

$$\begin{aligned} \Delta^2 &= \begin{vmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{vmatrix} \\ &= -4p^3 - 27q^2 \end{aligned}$$

□

Exercițiul (179)**.** Calculați determinantul

$$\Delta = \begin{vmatrix} a_1 & x & x & ... & x \\ x & a_2 & x & ... & x \\ x & x & a_3 & ... & x \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x & x & x & ... & a_n \end{vmatrix}$$

Demonstrație. Scădem prima linie din toate celelalte și scoatem factorii comuni:

$$\Delta = \begin{vmatrix} a_1 & x & x & ... & x \\ x-a_1 & a_2-x & 0 & ... & 0 \\ x-a_1 & 0 & a_3-x & ... & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x-a_1 & 0 & 0 & ... & a_n-x \end{vmatrix}$$

$$= (a_1-x)...(a_n-x) \begin{vmatrix} \frac{a_1}{a_1-x} & \frac{x}{a_2-x} & \frac{x}{a_3-x} & ... & \frac{x}{a_n-x} \\ -1 & 1 & 0 & ... & 0 \\ -1 & 0 & 1 & ... & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & 0 & 0 & ... & 1 \end{vmatrix}$$

Adunăm toate coloanele la prima și dezvoltăm după prima linie:

$$= (a_1-x)...(a_n-x) \begin{vmatrix} \frac{a_1}{a_1-x}+\cdots+\frac{x}{a_n-x} & \frac{x}{a_2-x} & ... & \frac{x}{a_n-x} \\ 0 & 1 & ... & 0 \\ 0 & 0 & ... & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & ... & 1 \end{vmatrix}$$

$$= (a_1-x)...(a_n-x)\left(\frac{a_1}{a_1-x}+\frac{x}{a_2-x}+\cdots+\frac{x}{a_n-x}\right)$$

În cazul în care $x \in \{ a_1, ..., a_n \}$, trebuie să desfacem acel produs. Fracțiile dispar și formula rămâne validă. □

Exercițiul (180)**.** Calculați următorul determinant prin dezvoltare Laplace după liniile 1 și 2:

$$\Delta = \begin{vmatrix} 5 & 3 & 0 & 0 & 0 \\ 2 & 5 & 3 & 0 & 0 \\ 0 & 2 & 5 & 3 & 0 \\ 0 & 0 & 2 & 5 & 3 \\ 0 & 0 & 0 & 2 & 5 \end{vmatrix}$$

Demonstrație. Dezvoltăm cu regula lui Laplace după primele două linii:

$$\begin{aligned}\Delta = &\underbrace{(-1)^{1+1+2+2}}_{1}\underbrace{\begin{vmatrix}5 & 3\\ 2 & 5\end{vmatrix}}_{19}\underbrace{\begin{vmatrix}5 & 3 & 0\\ 2 & 5 & 3\\ 0 & 2 & 5\end{vmatrix}}_{95-30}\\ &+\underbrace{(-1)^{1+1+2+3}}_{-1}\underbrace{\begin{vmatrix}5 & 0\\ 2 & 3\end{vmatrix}}_{15}\underbrace{\begin{vmatrix}2 & 3 & 0\\ 0 & 5 & 3\\ 0 & 2 & 5\end{vmatrix}}_{2\cdot 19}\\ &+\underbrace{(-1)^{1+2+2+3}}_{1}\underbrace{\begin{vmatrix}3 & 0\\ 5 & 3\end{vmatrix}}_{9}\underbrace{\begin{vmatrix}0 & 3 & 0\\ 0 & 5 & 3\\ 0 & 2 & 5\end{vmatrix}}_{0}\\ &= 95\cdot 19 - 30\cdot 19 - 30\cdot 19\\ &= 19\cdot 35\end{aligned}$$

□

Exercițiul (185)**.** Determinați numărul de matrici inversabile din $M_3(\mathbb{Z}_2)$. Generalizare.

Demonstrație. Construim matricea în așa fel încât determinantul ei să nu fie $\hat{0}$.

1. Pentru a construi prima coloană, trebuie să alegem trei elemente din mulțimea $\left\{\hat{0}, \hat{1}\right\}$. Acestea nu pot fi toate $\hat{0}$, altfel determinantul ar fi nul. Deci avem $2^3 - 1$ posibilități.

2. A doua coloană trebuie să fie diferită de coloana nulă, și diferită de prima coloană (dacă două coloane sunt egale sau proporționale, determinantul este nul). Atunci avem $2^3 - 2$ posibilități.

3. Ultima coloană trebuie să fie diferită de coloana nulă, diferită de primele două, și să nu fie combinație liniară de primele două coloane. Singura combinație liniară posibilă în $\mathbb{Z}_2$ ar fi suma primelor două coloane. Astfel avem $2^3 - 4$ posibilități.

În concluzie, sunt $(2^3 - 1)(2^3 - 2)(2^3 - 4) = 168$ moduri de a construi o matrice inversabilă în $M_3(\mathbb{Z}_2)$.

Pe cazul general de matrici din $M_n(\mathbb{Z}_2)$ numărul de matrici inversabile este $(2^n - 2^0)\cdot(2^n - 2^1)\cdot\cdots\cdot(2^n - 2^{n-1})$. □

5.2 Eșalonare. Metoda lui Gauss

Exercițiul (212)**.** Eșalonați matricea

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

și găsiți baze în subspațiile generate de liniile, respectiv coloanele matricei.

Demonstrație.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

$$\overset{\substack{L_2-L_1 \\ \sim \\ L_3-2L_1}}{} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & -1 \\ 0 & -1 & -5 & -4 \end{pmatrix}$$

$$\overset{\substack{(-1)L_3 \\ \sim \\ L_2 \leftrightarrow L_3}}{} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 5 & 4 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

$$\overset{L_1-2L_2}{\sim} \begin{pmatrix} 1 & 0 & -7 & -4 \\ 0 & 1 & 5 & 4 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

$$\overset{\substack{L_1+7L_3 \\ \sim \\ L_2-5L_3}}{} \begin{pmatrix} 1 & 0 & 0 & -11 \\ 0 & 1 & 0 & 9 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

Vectorii coloană ai matricei sunt

$$C = \{(1,0,0), (0,1,0), (0,0,1), (-11,9,-1)\}$$

Aceștia generează întreg $\mathbb{R}^3$, deci o bază pentru ei este baza canonică $B_0 = \{ (1,0,0), (0,1,0), (0,0,1) \}$.

Vectorii linie sunt $L = \{(1,0,0,-11), (0,1,0,9), (0,0,1,-1)\}$. Deoarece avem 3 vectori din $\mathbb{R}^4$ care sunt și linear independenți, ei generează un hiperplan 3-dimensional în $\mathbb{R}^4$, și îi putem lua și ca bază pentru acest subspațiu. □

Exercițiul (213)**.** Rezolvați sistemul de ecuații liniare

$$\begin{cases} x - 2y + z + t = 1 \\ x - 2y + z - t = -1 \\ x - 2y + z + 5t = 5 \end{cases}$$

Demonstrație. Construim matricea extinsă a sistemului:

$$A^e = \left(\begin{array}{cccc|c} 1 & -2 & 1 & 1 & 1 \\ 1 & -2 & 1 & -1 & -1 \\ 1 & -2 & 1 & 5 & 5 \end{array}\right)$$
$$\overset{\substack{L_2-L_1 \\ L_3-L_1}}{\sim} \left(\begin{array}{cccc|c} 1 & -2 & 1 & 1 & 1 \\ 0 & 0 & 0 & -2 & -2 \\ 0 & 0 & 0 & 4 & 4 \end{array}\right)$$
$$\overset{\substack{L_3+2L_2 \\ (-\frac{1}{2})L_2}}{\sim} \left(\begin{array}{cccc|c} 1 & -2 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$
$$\overset{L_1-L_2}{\sim} \left(\begin{array}{cccc|c} 1 & -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Acum putem rescrie sistemul echivalent din matrice:

$$\begin{cases} x - 2y + z = 0 \\ t = 1 \end{cases}$$

Rescriem necunoscutele principale x și t (necunoscutele pe coloanele cărora avem pivoții) în funcție de celelalte necunoscute (adică y, z).

Mulțimea soluțiilor este $S = \{\ (2y - z, y, z, 1) \mid y, z \in \mathbb{R}\ \}$.

Pentru a găsi soluția particulară, separăm termenii liberi de cei care depind de o variabilă, și rescriem vectorial ecuațiile:

$$S = (0, 0, 0, 1) + (2y + z, y, z, 0)$$

Pentru a determina o bază care să genereze subspațiul vectorial al soluțiilor, separăm componentele care depind de y, respectiv z:

$$\begin{aligned} S &= (0, 0, 0, 1) + y(2, 1, 0, 0) + z(-1, 0, 1, 0) \\ &= (0, 0, 0, 1) + \langle (2, 1, 0, 0), (-1, 0, 1, 0) \rangle \end{aligned}$$

□

Exercițiul (214)**.** Rezolvați sistemul de ecuații liniare

$$\begin{cases} x + y - 3z = -1 \\ 2x + y - 2z = 1 \\ x + y + z = 3 \\ x + 2y - 3z = 1 \end{cases}$$

Demonstrație. Scriem matricea extinsă a sistemului și rezolvăm prin metoda lui Gauss:

$$\left(\begin{array}{cccc|c} 1 & 1 & -3 & & -1 \\ 1 & 1 & -2 & & 1 \\ 1 & 1 & 1 & & 3 \\ 1 & 2 & -3 & & 1 \end{array}\right)$$

$$\begin{array}{l} L_2-L_1 \\ L_3-L_1 \\ \sim \\ L_4-L_1 \end{array} \left(\begin{array}{cccc|c} 1 & 1 & -3 & & -1 \\ 0 & 0 & 1 & & 2 \\ 0 & 0 & 4 & & 4 \\ 0 & 1 & 0 & & 2 \end{array}\right)$$

$$\begin{array}{l} (\frac{1}{4})L_3 \\ \sim \\ L_3-L_2 \end{array} \left(\begin{array}{cccc|c} 1 & 1 & -3 & & -1 \\ 0 & 0 & 1 & & 2 \\ 0 & 0 & 0 & & -1 \\ 0 & 1 & 0 & & 2 \end{array}\right)$$

Deoarece deja am obținut o contradicție pe linia 3 ($0 = -1$), sistemul este incompatibil. □

5.3 Inversa unei matrici prin eșalonare

Exercițiul (215)**.** Calculați inversa matricei următoare prin eșalonare

$$A = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 3 & 2 & 0 & 0 \\ 1 & 1 & 3 & 4 \\ 2 & -1 & 2 & 3 \end{pmatrix}$$

Demonstrație. Scriem matricea extinsă, cu I_4 pe partea dreaptă:

$$\left(\begin{array}{cccc|cccc} 2 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 3 & 2 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 3 & 4 & 0 & 0 & 1 & 0 \\ 2 & -1 & 2 & 3 & 0 & 0 & 0 & 1 \end{array}\right)$$

$$\overset{L_1 \leftrightarrow L_3}{\sim} \left(\begin{array}{cccc|cccc} 1 & 1 & 3 & 4 & 0 & 0 & 1 & 0 \\ 3 & 2 & 0 & 0 & 0 & 1 & 0 & 0 \\ 2 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 3 & 0 & 0 & 0 & 1 \end{array}\right)$$

$$\begin{array}{l} L_2-3L_1 \\ (-1)L_2 \\ \sim \\ L_3-2L_1 \\ L_4-2L_1 \end{array} \left(\begin{array}{cccc|cccc} 1 & 1 & 3 & 4 & 0 & 0 & 1 & 0 \\ 0 & 1 & 9 & 12 & 0 & -1 & 3 & 0 \\ 0 & -1 & -6 & -8 & 1 & 0 & -2 & 0 \\ 0 & -3 & -4 & -5 & 0 & 0 & -2 & 1 \end{array}\right)$$

$$\begin{array}{l} L_3+L_2 \\ \sim \\ L_4+L_2 \end{array} \left(\begin{array}{cccc|cccc} 1 & 0 & -6 & -8 & 0 & 1 & -2 & 0 \\ 0 & 1 & 9 & 12 & 0 & -1 & 3 & 0 \\ 0 & 0 & 3 & 4 & 1 & -1 & 1 & 0 \\ 0 & 0 & 23 & 31 & 0 & -3 & 7 & 1 \end{array}\right)$$

$$\begin{array}{l} L_1+2L_3 \\ L_2-3L_3 \\ \sim \\ 8L_3 \end{array} \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -3 & 2 & 0 & 0 \\ 0 & 0 & 24 & 32 & 8 & -8 & 8 & 0 \\ 0 & 0 & 23 & 31 & 0 & -3 & 7 & 1 \end{array}\right)$$

$$\overset{L_3-L_4}{\sim} \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -3 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 & 8 & -5 & 1 & -1 \\ 0 & 0 & 23 & 31 & 0 & -3 & 7 & 1 \end{array}\right)$$

$$\overset{L_4-23L_4}{\sim} \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -3 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 & 8 & -5 & 1 & -1 \\ 0 & 0 & 0 & 8 & -184 & 112 & -16 & 24 \end{array}\right)$$

$$\overset{\frac{1}{8}L_4}{\sim} \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -3 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 & 8 & -5 & 1 & -1 \\ 0 & 0 & 0 & 1 & -23 & 14 & -2 & 3 \end{array}\right)$$

$$\overset{L_3-L_4}{\sim} \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -3 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 31 & -19 & 3 & -4 \\ 0 & 0 & 0 & 1 & -23 & 14 & -2 & 3 \end{array}\right)$$

□

Rezolvare Examen Mincu 2020

Fiecare student a primit un k și un l diferit.
Vom lua ca exemplu $k = 73$ și $l = 38$.

1. Considerăm corespondențele $f, g, h \colon \mathbb{Q} \to \mathbb{Q}$ date astfel:

$$f\left(\frac{a}{b}\right) = \frac{a^{2k}}{b^{2l+1}} \text{ pentru orice } (a,b) \in \mathbb{Z} \times \mathbb{Z}^*,$$

$$g\left(\frac{a}{b}\right) = \frac{a^{2k}}{b^{2l+1}} \text{ pentru orice } (a,b) \in \mathbb{Z} \times \mathbb{Z}^* \text{ pentru care } (a,b) = 1,$$

$$h\left(\frac{a}{b}\right) = \frac{a^{2k}}{b^{2l+1}} \text{ pentru orice } (a,b) \in \mathbb{Z} \times \mathbb{N}^* \text{ pentru care } (a,b) = 1.$$

   (a) Care dintre aceste corespondențe este funcție? Justificați!

   Rezolvare. În toate aceste cazuri, numitorul este diferit de zero, deci fracțiile care apar sunt bine definite pe întreg domeniul.
   O proprietate a unei funcții este că, atâta timp cât îi dăm același input, o să aibă același rezultat.
   Dacă ne uităm la f, putem avea aceași fracție scrisă în două moduri, de exemplu $\frac{1}{2} = \frac{2}{4}$, dar rezultatul diferă:

$$f\left(\frac{1}{2}\right) = \frac{1}{2^{77}} \neq \frac{1}{2^7} = \frac{2^{146}}{4^{77}} = f\left(\frac{2}{4}\right)$$

   Pentru g, observăm că apare o problemă legată de semne. Să zicem că luăm $\frac{-1}{-1} = \frac{1}{1}$. Atunci avem:

$$g\left(\frac{-1}{-1}\right) = \frac{1}{-1} \neq \frac{1}{1} = g\left(\frac{1}{1}\right)$$

   La h, modul în care este definită funcția garantează că nu întâmpinăm vreuna dintre probleme. Fracția este ireductibilă și semnul rezultatului este întotdeauna pozitiv. □

   (b) Pentru acelea dintre ele care sunt funcții, precizați (cu justificare!) dacă sunt sau nu injective, respectiv surjective.

   Rezolvare. Pentru h:

   - nu este injectivă, dacă luăm $\frac{-1}{1}$ și $\frac{1}{1}$ obținem același rezultat, dar parametrii sunt diferiți.

- nu este surjectivă, deoarece rezultatul este mereu pozitiv, deci nu acoperă tot $\mathbb{Q}$.

□

2. Considerăm grupul $G = \mathbb{Z}_k \times S_l$ (în cazul nostru $\mathbb{Z}_{73} \times S_{38}$).

   (a) Decideți dacă G este sau nu ciclic.

   Rezolvare. Vom arată că nu este ciclic bazându-ne pe faptul că S_n pentru $n \geq 3$ nu este ciclic.
   Să presupunem prin reducere la absurd că G este ciclic, deci există un generator $(\hat{a}, \tilde{b}) \in G$. Asta implică că $n(\hat{a}, \tilde{b})$ atinge toate valorile lui G, deci și $n\hat{a}$ și $\tilde{b}^n$ ating, eventual, toate valorile din $\mathbb{Z}_{73}$, respectiv din S_{38}.
   Deci $\tilde{b}$ este un generator pentru S_{38}, deci S_{38} este ciclic. Dar asta contrazice faptul că S_{38} nu este ciclic. □

   (b) Determinați $\hom_{\text{Grp}}(\mathbb{Q}, G)$.

   Rezolvare. Fie $f \colon \mathbb{Q} \to G$ un morfism. Notăm $f(1) = a = (\hat{x}, \tilde{y}) \in G$.
   Atunci

$$f(2) = f(1+1) = f(1) + f(1) = (\hat{x}, \tilde{y}) + (\hat{x}, \tilde{y}) = (\hat{x} + \hat{x}, \tilde{y} \circ \tilde{y}) = 2a$$

   Analog

$$f(-1) = -f(1) = -(\hat{x}, \tilde{y}) = (-\hat{x}, \tilde{y}^{-1}) = -a$$

   Deci $f(n) = na, \forall n \in \mathbb{Z}$.
   De asemenea, avem

$$a = f(1) = f\left(\frac{1}{2} + \frac{1}{2}\right) = 2f\left(\frac{1}{2}\right)$$

   Dacă ne uităm la numerele de forma $\frac{1}{k}$, obținem asemănător că

$$a = kf\left(\frac{1}{k}\right), \forall k \in \mathbb{N}^*$$

   Atunci, pentru $k = 73$ avem

$$a = 73f\left(\frac{1}{73}\right) \implies \hat{x} = 73 \cdot \cdots = \hat{0}$$

   Facem același lucru pentru $k = |S_{38}|$ și obținem că $\tilde{y} = \tilde{1}$ (permutarea identică).
   Deci $a = (\hat{0}, \tilde{1})$, iar $f(q) = (\hat{0}, \tilde{1}), \forall q \in \mathbb{Q}$. □

   (c) Determinați un subgrup H normal, propriu și netrivial al lui G.

   Rezolvare. $\mathbb{Z}_{73}$ este un subgrup normal al lui $\mathbb{Z}_{73}$.
   A_{38} (subgrupul permutărilor pare) este un subgrup normal, propriu și netrivial al lui S_{38}.
   $H = \mathbb{Z}_{73} \times A_{38}$ este un subgrup normal, propriu și netrivial al lui G. □

(d) Descrieți, eventual până la izomorfism, grupul factor G/H.

Rezolvare. Când factorizăm S_{38} prin A_{38} obținem două clase de resturi: clasa permutărilor pare și clasa permutărilor impare. Având exact două elemente, grupul factor este izomorf cu $\mathbb{Z}_2$.

$$\frac{G}{H} = \frac{\mathbb{Z}_{73} \times S_{38}}{\mathbb{Z}_{73} \times A_{38}} \cong \frac{\mathbb{Z}_{73}}{\mathbb{Z}_{73}} \times \frac{S_{38}}{A_{38}} \cong \{1\} \times \mathbb{Z}_2 \cong \mathbb{Z}_2$$

□

3. (a) Determinați numărul elementelor de ordin $10k$ din grupul $\mathbb{Z}_{2020k}$.

Rezolvare. Trebuie să găsim numărul elementelor de ordin 730 din grupul $\mathbb{Z}_{2020 \cdot 73}$.
Observăm că $730 \mid (2020 \cdot 73)$, deci există elemente de acest ordin.
Ne folosim de raționamentul de aici, care ne spune că numărul cerut este fix $\phi(730)$, adică numărul de numere de la 1 la 729 inclusiv prime față de 730.
Putem calcula $\phi(730)$ foarte rapid descompunând numărul în factori primi: $730 = 2 \cdot 5 \cdot 73$. Atunci $\phi(730) = \phi(2 \cdot 5 \cdot 73)$, care după multe calcule iese ca fiind 288. □

(b) Considerăm permutarea σ a literelor alfabetului românesc scrisă ca produs de cicluri astfel: luați (toate) numele și toate prenumele dvs. (așa cum apar în actul de identitate, fără inițiala tatălui, dar cu diacritice) și scrieți-le pe un rând, fără spații. Descompuneți apoi șirul de caractere obținut în blocuri, cu ajutorul parantezelor, închizând fiecare paranteză exact înaintea literei care ar genera o primă repetiție în blocul închis de acea paranteză.
De exemplu, numele Dulgeru Iancu R.D. Mihaela Florica generază permutarea

$$\sigma = (dulger)(uianc)(umihael)(afloric)(a)$$

Descompuneți σ în produs de transpoziții și în produs de cicluri disjuncte. Calculați σ^3, σ^{-1}, $\varepsilon(\sigma)$, $ord(\sigma)$ și σ^{2020}.

Rezolvare. Vom lucra cu permutarea dată ca exemplu.
Descompunerea ca transpoziții se poate face destul de ușor, doar spargem ciclurile:

$$\begin{gathered}\sigma = (du)(ul)(lg)(ge)(er)\\(ui)(ia)(an)(nc)\\(um)(mi)(ih)(ha)(ae)(el)\\(af)(fl)(lo)(or)(ri)(ic)\end{gathered}$$

Nu am mai scris ultimul ciclu (a) pentru că fiind un ciclu cu un singur element, era practic permutarea identică.
Deși permutarea este deja descompusă în cicluri, acestea **nu** sunt disjuncte. Trebuie să înmulțim pe rând transpozițiile, urmărim parcursul fiecărei litere să vedem ce cicluri disjuncte obținem.
De exemplu, dacă am avea $(abc)(ad)$, am observa că:

- a se duce în d, care nu e afectat de (abc)
- b nu e afectat de (ad), se duce în c
- c nu e afectat de (ad), se duce în a
- d se duce în a, care se duce în b

Deci scris ca ciclu disjunct ar fi $(adbc)$.

Dacă la unul dintre acești pași ne întoarcem la începutul ciclului pe care îl calculăm, deschidem un nou ciclu cu una dintre literele rămase și continuăm algoritmul.

Efectuând calcule asemănătoare, obținem pe rând:

$$(dulger)(uianc) = (duianclger)$$
$$(duianclger)(umihael) = (dumar)(ihncl)(ge)$$
$$(dumar)(ihncl)(ge)(afloric) = (dumafilo)(hncr)(ge)$$

Avem 3 cicluri disjuncte de lungimi 8, 4, și 2.

Pentru a calcula σ^3, e suficient să parcurgem din 3 în 3 ciclurile:

$$\sigma^3 = (dalufomi)(hrcn)(ge)$$

Pentru a calcula σ^{-1}, citim invers ciclurile:

$$\sigma^{-1} = (olifamud)(rcnh)(eg)$$

Pentru a calcula $\varepsilon(\sigma)$, numărăm câte transpoziții avem: 21, deci permutarea este impară.

Pentru a calcula $ord(\sigma)$, calculăm cel mai mic multiplu comun al lui 8, 4 și 2, adică 8.

Pentru a calcula σ^{2020}, observăm că $2 \mid 2020$ și $4 \mid 2020$, deci ciclurile de aceste lungime dispar. De asemenea, $2020 = 2016 + 4$, deci este suficient să calculăm puterea a 4-a a ciclului de lungime 8:

$$\sigma^{2020} = (df)(ao)(lm)(ui)$$

□